Algebra & Number Theory

Volume 9
2015
No. 10

msp

Algebra & Number Theory

msp.org/ant

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

The subscription price for 2015 is US $255/year for the electronic version, and $440/year (+$55, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscribers address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

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

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

msp

ALGEBRA AND NUMBER THEORY 9:10 (2015)
dx.doi.org/10.2140/ant.2015.9.2197

Equivariant torsion and base change

Michael Lipnowski

What is the true order of growth of torsion in the cohomology of an arithmetic group? Let D be a quaternion algebra over an imaginary quadratic field F. Let E/F be a cyclic Galois extension with $\Gamma_{E/F} = \langle\sigma\rangle$. We prove lower bounds for "the Lefschetz number of σ acting on torsion cohomology" of certain Galois-stable arithmetic subgroups of $D_E^\times$. For these same subgroups, we unconditionally prove a would-be-numerical consequence of the existence of a hypothetical base change map for torsion cohomology.

A list of symbols can be found on page 2237.

0. Introduction

Let $\boldsymbol{H}/\mathbb{Q}$ be a semisimple group. Let $K \subset H = \boldsymbol{H}(\mathbb{R})$ be a maximal compact subgroup and $X = X_{\boldsymbol{H}} = H/K$ the symmetric space of maximal compact subgroups of H. Fix an arithmetic subgroup $\Gamma \subset \boldsymbol{H}(\mathbb{Q})$. Let $\rho : \boldsymbol{H} \to \mathrm{GL}(V)$ be a homomorphism of algebraic groups over $\mathbb{Q}$ and let $M \subset V$ be a Γ-stable lattice.

MSC2010: primary 11F75; secondary 11F72, 11F70.

Keywords: torsion, cohomology, Reidemeister torsion, analytic torsion, Ray–Singer torsion, locally symmetric space, trace formula, base change, equivariant, twisted.

Suppose that $\boldsymbol{H}/\mathbb{Q}$ is anisotropic and that $M_{\mathbb{R}}$ is strongly acyclic [Bergeron and Venkatesh 2013, §4]. Let $\Gamma_n \subset \Gamma$ be a sequence of subgroups for which the injectivity radius of $\Gamma_n \backslash X$ approaches infinity. Bergeron and Venkatesh [2013] prove that if the fundamental rank[1] of X equals 1, then

$$\liminf_n \frac{\sum_i \log|H^i(\Gamma_n, M)_{\mathrm{tors}}|}{[\Gamma : \Gamma_n]} > 0.$$

Little is known about the true order of growth of $\log|H^*(\Gamma_n, M)_{\mathrm{tors}}|$ for X of fundamental rank $\neq 1$.

Let F be an imaginary quadratic field and let E/F be a cyclic Galois extension of degree p. Let D be a quaternion algebra over F. One goal of this paper is to prove lower bounds for the amount of torsion in the cohomology of locally symmetric spaces for $X_{\mathrm{PGL}_1(D_E)}$, which has fundamental rank $p > 1$.

Calegari and Venkatesh [2012, §2] have proposed an analogue of Langlands functoriality for torsion cohomology. The hypothetical existence of torsion base change functoriality leads one to predict that torsion cohomology on locally symmetric spaces for $X_{\mathrm{PGL}_1(D)}$ — proven to be abundant in [Bergeron and Venkatesh 2013] — can be lifted to torsion cohomology on locally symmetric spaces for $X_{\mathrm{PGL}_1(D_E)}$. A second goal of this paper is to unconditionally prove a numerical relationship between the cohomology of certain locally symmetric spaces for $X_{\mathrm{PGL}_1(D_E)}$ and "matching" locally symmetric spaces for $X_{\mathrm{PGL}_1(D)}$ which is consistent with base change for torsion.

0A. *Notational setup for statement of main results.*

0A1. *Analytic torsion and Reidemeister torsion.* Let $\mathcal{L} \to \mathcal{M}$ be a local system of $\mathbb{C}$-vector spaces, equipped with a Hermitian metric, over a compact Riemannian manifold $\mathcal{M}$. Let σ, of prime order p, act equivariantly by isometries on $\mathcal{L} \to \mathcal{M}$. Let $\Delta_{\mathcal{L}}$ denote the Laplace operator for $\mathcal{L}$. Let $\tau_\sigma(\mathcal{M}, \mathcal{L})$ denote the σ-equivariant analytic torsion of $\mathcal{L} \to \mathcal{M}$; it is a spectral quantity defined purely in terms of the action of σ on the eigenspaces of $\Delta_{\mathcal{L}}$ (see Section 3A).

We define the untwisted analytic torsion of a metrized local system $L \to M$ to be $\tau(M, L) := \tau_1(M, L)$.

We let $\mathrm{RT}_\sigma(\mathcal{M}, \mathcal{L})$ denote the equivariant Reidemeister torsion of $\mathcal{L} \to \mathcal{M}$; it is an equivariant topological invariant, described in a manner tailored to our needs in [Lipnowski 2014, §1.3].

We let $\mathrm{RT}(M, L) := \mathrm{RT}_1(M, L)$ denote untwisted Reidemeister torsion.

[1]The fundamental rank of H/K is $\mathrm{rank}(H) - \mathrm{rank}(K)$, where rank denotes the dimension of any maximal torus, not necessarily split.

0A2. *The locally symmetric spaces.* Let D be a quaternion algebra over an imaginary quadratic field F. Let E/F be a cyclic Galois extension of prime degree p, with Galois group $\Gamma_{E/F}$; we fix a generator σ for $\Gamma_{E/F}$. Let $\boldsymbol{G}$ denote the adjoint group of $\underline{D}^\times$, the unit group of D considered as an F-algebraic group. We form the associated locally symmetric space

$$\mathcal{M}_{\mathcal{U}} = \boldsymbol{G}(E)\backslash\boldsymbol{G}(\mathbb{A}_E)/\mathcal{K}\mathcal{U}, \quad M_U = \boldsymbol{G}(F)\backslash\boldsymbol{G}(\mathbb{A}_F)/KU,$$

where $\mathcal{U}$ is a compact open Galois-stable subgroup of $\boldsymbol{G}(\mathbb{A}_E^{\mathrm{fin}})$; U is a compact open subgroup of $\boldsymbol{G}(\mathbb{A}_F^{\mathrm{fin}})$; $\mathcal{K}$ is a Galois-stable maximal compact subgroup of $\boldsymbol{G}(E_{\mathbb{R}})$; and $K = \mathcal{K}^{\Gamma_{E/F}}$ is a maximal compact subgroup of $\boldsymbol{G}(F_{\mathbb{R}})$. There is a $\boldsymbol{G}(E_{\mathbb{R}}) \rtimes \Gamma_{E/F}$-invariant metric on $\boldsymbol{G}(E_{\mathbb{R}})/\mathcal{K}$ and a $\boldsymbol{G}(F_{\mathbb{R}})$-invariant metric on $\boldsymbol{G}(F_{\mathbb{R}})/K$ which descend to metrics on $\mathcal{M}_{\mathcal{U}}$ and M_U respectively; these invariant metrics are unique up to scaling. For a discussion of normalization of these metrics, see Section 2.

0A3. *The local systems.* Let N/F be a finite extension and V an N-vector space. Let $\tilde{\rho} : \mathrm{Res}_{E/F}\boldsymbol{G} \rtimes \Gamma_{E/F} \to \mathrm{Res}_{N/F}\mathrm{GL}(V)$ and $\rho : \boldsymbol{G} \to \mathrm{Res}_{N/F}\mathrm{GL}(W)$ be algebraic representations (over F). We fix "integral structures" within V and W, i.e., O_N-lattices inside V and W; let $\mathcal{U}_0$ and U_0 be their respective stabilizers inside $\boldsymbol{G}(\mathbb{A}_E^{\mathrm{fin}})$ and $\boldsymbol{G}(\mathbb{A}_F^{\mathrm{fin}})$.

The representation $\tilde{\rho}$ gives rise to a local system of N-vector spaces $\mathcal{L}_{\tilde{\rho}} \to \mathcal{M}_{\mathcal{U}}$ with an action of $\Gamma_{E/F}$. Similarly, the representation ρ gives rise to a local system of N-vector spaces $L_\rho \to M_U$. Let $\mathcal{L}_{\tilde{\rho}_\iota}$, L_{ρ_ι} denote the scalar extensions of $\mathcal{L}_{\tilde{\rho}}$, L_ρ by the complex embedding $\iota : N \hookrightarrow \mathbb{C}$. If $\mathcal{U} \subset \mathcal{U}_0$ and $U \subset U_0$, the integral structures on V, W yield integral structures on these local systems, i.e., local systems of O_N-modules, which we denote by

$$\mathcal{L}^0_{\tilde{\rho}} \to \mathcal{M}_{\mathcal{U}}, \quad L^0_\rho \to M_U.$$

We discuss the integral structures and scalar extensions in greater detail in Section 2B.

0B. ***Statements of main results.*** Let

$$M_U = \boldsymbol{G}(F)\backslash\boldsymbol{G}(\mathbb{A}_F)/KU, \quad \text{where } K = \mathcal{K} \cap \boldsymbol{G}(F_{\mathbb{R}}),\ U = \mathcal{U} \cap \boldsymbol{G}(\mathbb{A}_F^{\mathrm{fin}}).$$

Sample Theorem (comparison of analytic torsion). *Let E/F be an everywhere unramified Galois extension of odd prime degree. Suppose that $\mathcal{U}$ is a parahoric level structure* (see Definition 5.1) *and that ρ and $\tilde{\rho}$ match* (see Section 4C). *Then, for any complex embedding $\iota : N \hookrightarrow \mathbb{C}$,*

$$\tau_\sigma(\mathcal{M}_{\mathcal{U}}, \mathcal{L}_{\tilde{\rho}_\iota}) = \tau(M_U, L_{\rho_\iota})^p.$$

A more general statement, which allows any E/F that is everywhere tamely ramified, is proven in Sections 4D and 6. The relationship in the more general case between $\tau_\sigma(\mathcal{M}_{\mathcal{U}}, \mathcal{L}_{\tilde{\rho}_\iota})$ and $\tau(M_U, L_{\rho_\iota})$ has the same flavor but is not as simply stated.

Spectral comparisons such as the sample theorem, in conjunction with Cheeger–Müller theorems (see Section 0C), have consequences for torsion in the cohomology of $\mathcal{L}^0_{\tilde{\rho}}$. In order to describe these implications, we use the following notational shorthand:

- $\sum^*$ denotes an alternating sum.
- P denotes the p-cyclotomic polynomial $P(x) = x^{p-1} + x^{p-2} + \cdots + 1$.
- For any $\mathbb{Z}[\sigma]$-module A and any polynomial $h \in \mathbb{Z}[x]$, we let $A^{h(\sigma)}$ be the set $\{a \in A : h(\sigma)a = 0\}$.

Sample Theorem (relationship between sizes of torsion subgroups). *Let E/F be an everywhere tamely ramified Galois extension of odd prime degree with $\Gamma_{E/F} = \langle\sigma\rangle$. Let the places where E/F is ramified and the places where D is ramified be disjoint. Suppose that*:

- *$\rho, \tilde{\rho}$ are matching representations of the sort described in Section 7A.*
- *The level structure $\mathcal{U}$ is* tamely parahoric *at each unramified place of E/F* (see Definition 6.16).

Then there is an explicit finite collection of compact open subgroups $U \subset \boldsymbol{G}(\mathbb{A}_F^{\mathrm{fin}})$ and explicit constants c_U such that

$$\sum{}^* \log|H^i(\mathcal{M}_{\mathcal{U}}, \mathcal{L}^0_{\tilde{\rho}})^{\sigma-1}_{\mathrm{tors}}| - \frac{1}{p-1}\log|H^i(\mathcal{M}_{\mathcal{U}}, \mathcal{L}^0_{\tilde{\rho}})^{P(\sigma)}_{\mathrm{tors}}| = \sum_U c_U \sum{}^* \log|H^i(M_U, L^0_{\rho})_{\mathrm{tors}}| + n\log p$$

for some integer n. Furthermore, n can be bounded linearly by $\dim_{\mathbb{F}_p} H^i(\mathcal{M}^{\sigma}_{\mathcal{U}}, \mathcal{L}^0_{\rho,\mathbb{F}_p})$.

For a more precise statement, see Theorem 7.4. An appropriate generalization of the sample theorem also has consequences for growth of torsion in the cohomology of the spaces $\mathcal{M}_{\mathcal{U}}$.

Corollary (growth of torsion for fundamental rank > 1). *Let E/F be everywhere tamely ramified with $[E : F]$ odd. Let the places where E/F is ramified and the places where D is ramified be disjoint. Let $\mathcal{U}_n \subset \mathcal{U}_0$ denote a sequence of compact open subgroups of $\boldsymbol{G}(\mathbb{A}_E^{\mathrm{fin}})$ such that*:

- *The injectivity radius of $\mathcal{M}_{\mathcal{U}_n}$ approaches ∞.*
- *The level structures $\mathcal{U}_n$ are* tamely parahoric *at each unramified place of E/F* (see Definition 6.16).
- *Let $U_n \subset \boldsymbol{G}(\mathbb{A}_F^{\mathrm{fin}})$ denote the matching level structure implicit in the definition of tamely parahoric* (see Definition 6.16). *For every complex embedding $\iota : N \hookrightarrow \mathbb{C}$, the local systems $L_{\rho_\iota} \to M_{U_n}$ form a strongly acyclic family* (see Section 8A), *where ρ and $\tilde{\rho}$ are matching representations* (see Section 4C).

Then

$$\limsup_n \frac{\log\left|H^*(\mathcal{M}_{\mathcal{U}_n}, \mathcal{L}^0_{\tilde{\rho}})\right|}{\mathrm{vol}(\mathcal{M}_{\mathcal{U}_n})^{1/p}} > 0.$$

In fact, we prove an asymptotic formula for the "Lefschetz numbers of σ acting on $H^*(\mathcal{M}_{\mathcal{U}_n}, \mathcal{L}^0_{\tilde{\rho}})_{\mathrm{tors}}$" (see Section 8C).

0C. ***Main tools.*** Three main inputs are used to prove these theorems:

(a) *Cheeger–Müller theorems.* Let $\mathcal{L} \to \mathcal{M}$ be a local system of metrized $\mathbb{C}$-vector spaces acted on equivariantly by an isometry σ of finite order p. A *Cheeger–Müller theorem* is an identity

$$\tau_\sigma(\mathcal{M}, \mathcal{L}) = \mathrm{RT}_\sigma(\mathcal{M}, \mathcal{L})$$

valid for some class of metrized local systems $\mathcal{L}$ and some class of equivariant isometries σ. This remarkable formula was originally fathomed, for $\sigma = 1$ and $\mathcal{L}$ unitarily flat, by Ray and Singer [1971]. When σ equals 1 and $\mathcal{L}$ is unitarily flat, it was proven independently by Cheeger [1979] and Müller [1978]. An extension to $\sigma = 1$ and general unimodular $\mathcal{L}$ was proven by Müller [1993].

A general version of this theorem for $\sigma \neq 1$ is proven by Bismut and Zhang [1994]. This general version expresses the difference between $\log \mathrm{RT}_\sigma(\mathcal{M}, \mathcal{L})$ and $\log \tau_\sigma(\mathcal{M}, \mathcal{L})$ in terms of auxiliary differential geometric data on a germ of the fixed point set of σ. The author proves in [Lipnowski 2014] that this difference equals zero in the cases to be studied in this paper.

Cheeger–Müller theorems provide a bridge between the analytic expression $\tau_\sigma(\mathcal{M}, \mathcal{L})$ and the quantity $\mathrm{RT}_\sigma(\mathcal{M}, \mathcal{L})$. In the case where $\mathcal{L}$ is the complexification of a local system of $\mathbb{Z}$-modules $\mathcal{L}^0$, the latter can concretely be related to the σ-module $H^*(\mathcal{M}, \mathcal{L}^0)_{\mathrm{tors}}$ [Lipnowski 2014, Corollary 3.8].

(b) *Trace formula comparison.* Using Cheeger–Müller theorems, torsion in cohomology of arithmetic groups related by base change can be compared by instead comparing analytic torsions. In the case of compact quotient, the equivariant analytic torsion of $(\mathcal{M}, \mathcal{L})$ is determined by the spectral side of the twisted Arthur–Selberg trace formula for an appropriate family of test functions (see Section 3). The analytic torsion of (M, L) is determined by the spectral side of the untwisted trace formula for a matching family of test functions.

Comparing these spectral quantities uses the methods of [Langlands 1980] together with some local representation theory for PGL_2. In particular, we need to prove a "fundamental lemma for the spherical unit" for tamely ramified base change of PGL_2.

(c) *The results of Bergeron and Venkatesh* [2013] *on growth of untwisted analytic torsion for sequences of locally symmetric spaces with universal cover of fundamental rank 1.*

Combining (a) with (b) proves an identity relating sizes of torsion cohomology for arithmetic groups related by base change (see Theorem 7.4). The resulting identity is consistent with implications of torsion base change functoriality (see Section 1).

Combining (a) with (c) proves the growth of "Lefschetz numbers for torsion". See Theorem 8.5 for a more precise statement.

0D. ***Outline.*** In Section 1, we discuss base change functoriality over $\mathbb{Z}$. Base change functoriality over $\mathbb{Z}$ predicts one of the main results of this paper, a relationship between the sizes of torsion subgroups on locally symmetric spaces related by base change.

In Section 2, we discuss (equivariant) local systems over locally symmetric spaces. We explain in Section 2B how, for finite extensions N/F, algebraic homomorphisms $\boldsymbol{G} \to R_{N/F}\,\mathrm{GL}(V)$ over F give rise to local systems of O_N-modules over M_U for appropriate compact open subgroups $U \subset \boldsymbol{G}(\mathbb{A}_F^{\mathrm{fin}})$.

In Section 3, we express the σ-twisted analytic torsion of $\mathcal{L}_{\tilde{\rho}_\iota} \to \mathcal{M}_{\mathcal{U}}$ and the untwisted analytic torsion of $L_{\rho_\iota} \to M_U$ in purely representation theoretic terms.

In Section 4, we use Langlands' representation theoretic statement of base change to prove an abstract matching Section 4D, which will ultimately imply identities of the flavor

$$\tau_\sigma(\mathcal{M}_{\mathcal{U}}, \mathcal{L}_{\tilde{\rho}_\iota}) = \tau(M_U, L_{\rho_\iota})^p$$

of the aforementioned sample theorem. In order to apply this matching theorem, we need to find instances of matching test functions, which will be the objective of Sections 5 and 6.

In Section 5, we describe some circumstances under which the desired matching test functions can be found. This matching only applies at places v where E_v/F_v is unramified. Here is where we finally define and discuss parahoric level structure.

In Section 6, we prove a matching theorem at places v where E_v/F_v is tamely ramified. In Section 6D, we define tamely parahoric level structures, those level structures which occur in the matching theorem (Theorem 6.17) and the numerical cohomology comparison theorem (Theorem 7.4).

In Section 7, we prove the numerical cohomology comparison theorem (Theorem 7.4) for the local systems introduced in Section 7A.

In Section 8, we use the main comparison corollary for analytic torsion (Corollary 4.19) together with [Bergeron and Venkatesh 2013, Theorem 4.5] to prove that, for appropriate equivariant local systems $\mathcal{L}$ and level structures $\mathcal{U}$ (see Definition 5.1), the twisted analytic torsion $\log \tau_\sigma(\mathcal{M}_{\mathcal{U}}, \mathcal{L})$ is asymptotic to $\mathrm{vol}(\mathcal{M}_{\mathcal{U}})^{1/p}$. Combined with the results of [Lipnowski 2014, §§1–5] — which relate equivariant Reidemeister torsion to cohomology — asymptotic growth of cohomology is proven. The results of [Bergeron and Venkatesh 2013] prove asymptotic growth of Reidemeister

torsion, which one might loosely think of as an "Euler characteristic for torsion in cohomology". In the same vein, the results of Section 8 prove "asymptotic growth of Lefschetz numbers for torsion in cohomology".

1. A priori predictions via torsion base change functoriality

Calegari and Venkatesh [2012, §2] have conjectured an analogue of Langlands functoriality for mod p and torsion cohomology of arithmetic locally symmetric spaces. In this section, we explain how one of our main results, Theorem 7.4, is roughly predicted by their conjecture applied to base change.

1A. ***Base change functoriality over*** $\mathbb{Z}$**.** For a more general discussion of functoriality over $\mathbb{Z}$, we refer the reader to [Calegari and Venkatesh 2012, §2].

Let F be any number field and E/F a cyclic Galois extension of odd prime degree p. Let $\boldsymbol{G}_1/F$ be any group and let $\boldsymbol{G}_2 = R_{E/F}\boldsymbol{G}_1$. In accordance with functoriality over $\mathbb{Z}$, the diagonal map of L-groups [Buzzard and Gee 2015]

$$^L\boldsymbol{G}_1 \xrightarrow{\phi} {}^L\boldsymbol{G}_2, \quad (g, \sigma) \mapsto (g, \dots, g) \times \sigma$$

is expected to give rise to a Hecke-equivariant map ϕ_* on cohomology, torsion or otherwise. For certain groups such as $\boldsymbol{G}_1$, the unit group of a semisimple algebra over F, this correspondence is known for characteristic zero cohomology.

One main purpose of this paper is to unconditionally prove certain would-be-numerical consequences of the existence of the hypothetical map ϕ_*. The analogue of this program was carried out for Jacquet–Langlands functoriality for PGL_2 in [Calegari and Venkatesh 2012].

1B. ***Conjectures on torsion base change.*** This highly speculative section discusses implications of the existence of a base change map ϕ_*, as above. The discussion uses the language of Langlands' theory of base change, to be reviewed in Section 4A.

Let D be a quaternion algebra over a number field F. Let $\boldsymbol{G}$ denote the adjoint group of its group of units. Let E/F be a cyclic Galois extension with $\Gamma_{E/F} = \langle\sigma\rangle$. Let $\mathcal{U} \subset \boldsymbol{G}(\mathbb{A}_E^{\mathrm{fin}})$ and $U \subset \boldsymbol{G}(\mathbb{A}_F^{\mathrm{fin}})$ be compact open subgroups with $\mathcal{U}$ Galois-invariant. Let $\mathcal{U}$ and U have respective volume-1 Haar measures $d\tilde{u}$ and du. Let $K \subset \boldsymbol{G}(F_{\mathbb{R}})$ be a maximal compact subgroup and $\mathcal{K} \subset \boldsymbol{G}(E_{\mathbb{R}})$ a Galois-invariant maximal compact subgroup. Let

$$\mathcal{M}_{\mathcal{U}} = \boldsymbol{G}(E)\backslash\boldsymbol{G}(\mathbb{A}_E)/\mathcal{K}\mathcal{U} \quad \text{and} \quad M_U = \boldsymbol{G}(F)\backslash\boldsymbol{G}(\mathbb{A}_F)/KU.$$

For compact open subgroups $J \subset \boldsymbol{G}(\mathbb{A}_F^{\mathrm{fin}})$ and $\mathcal{J} \subset \boldsymbol{G}(\mathbb{A}_E^{\mathrm{fin}})$, let

$$W^J = L^2(\boldsymbol{G}(F)\backslash\boldsymbol{G}(\mathbb{A}_F)/J) \quad \text{and} \quad \mathcal{W}^{\mathcal{J}} = L^2(\boldsymbol{G}(E)\backslash\boldsymbol{G}(\mathbb{A}_E)/\mathcal{J}).$$

Definition 1.1. We say that $\mathbf{1}_{\mathcal{U}}\, d\tilde{u}$ and $\sum_U c_U \mathbf{1}_U\, du$ (finite sum) are *matching level structures* if

$$\operatorname{tr}\{\sigma \,|\, \tilde{\pi}_{\mathrm{fin}}^{\mathcal{U}}\} = \sum_U c_U \dim \pi_{\mathrm{fin}}^U$$

for every pair of representations $\tilde{\pi}$ of $\boldsymbol{G}(\mathbb{A}_E) \rtimes \Gamma_{E/F}$ and π of $\boldsymbol{G}(\mathbb{A}_F)$ which match by base change (see Section 4A). If E'/F is a second cyclic Galois extension and $\mathcal{U}' \subset \boldsymbol{G}(\mathbb{A}_{E'})$ and $\mathcal{U} \subset \boldsymbol{G}(\mathbb{A}_E)$ both match a common level structure, we say that $\mathcal{U}$ and $\mathcal{U}'$ are *related*.

Lemma 1.2. *Matching level structures satisfy the identity of traces in cohomology*

$$\operatorname{tr}\{\sigma \,|\, H^*(\mathcal{M}_{\mathcal{U}}, \mathcal{L}_{\mathbb{C}})\} = \sum_U c_U \dim H^*(M_U, L_{\mathbb{C}}) \tag{1}$$

for local systems $\mathcal{L}$, L associated to compatible representations $\tilde{\rho}$ of $R_{E/F}\boldsymbol{G} \rtimes \Gamma_{E/F}$ and ρ of $\boldsymbol{G}$ (see Section 4C for a discussion of matching representations and matching local systems).

Proof. We can decompose

$$H^*(M_U, L_{\mathbb{C}}) = \bigoplus \dim \operatorname{Hom}_{\boldsymbol{G}(\mathbb{A}_F)}(\pi, W) \dim \pi_{\mathrm{fin}}^U \cdot H^*(\pi_\infty \otimes \rho)$$

in accordance with Matsushima's formula [Borel and Wallach 2000, Chapter VII, Theorem 5.2], where $H^*(\pi_\infty \otimes \rho)$ denotes $(\mathfrak{g}, K)$-cohomology; this is a representation theoretic incarnation of Hodge theory. Because the level structures match, we are reduced to proving that

$$\operatorname{tr}\{\sigma \,|\, H^*(\tilde{\pi}_\infty \otimes \tilde{\rho})\} = \dim H^*(\pi_\infty \otimes \rho)$$

for pairs of representations $\tilde{\pi}$ of $\boldsymbol{G}(\mathbb{A}_E) \rtimes \Gamma_{E/F}$ and π of $\boldsymbol{G}(\mathbb{A}_F)$ which match by local base change. In this particular situation, $\boldsymbol{G}(E_{\mathbb{R}})$ is isomorphic to $\boldsymbol{G}(F_{\mathbb{R}})^p$, and $\tilde{\pi}_\infty \cong \pi_\infty^{\boxtimes p}$, where σ acts by cyclic permutation. By the Künneth formula for $(\mathfrak{g}, K)$-cohomology, $H^*(\tilde{\pi}_\infty \otimes \tilde{\rho}) \cong H^*(\pi_\infty \otimes \rho)^{\otimes p}$ (graded tensor product), where σ again acts by cyclic permutation. The result then follows by the elementary fact that, for any finite dimensional V,

$$\operatorname{tr}\{\text{cyclic permutation} \,|\, V^{\otimes p}\} = \dim V. \qquad \square$$

Corollary 1.3. *If $\mathcal{U} \subset \boldsymbol{G}(\mathbb{A}_E)$ and $\mathcal{U}' \subset \boldsymbol{G}(\mathbb{A}_{E'})$ are related level structures, then*

$$\operatorname{tr}\{\sigma \,|\, H^*(\mathcal{M}_{\mathcal{U}}, \mathcal{L}_{\mathbb{C}})\} = \operatorname{tr}\{\sigma \,|\, H^*(\mathcal{M}'_{\mathcal{U}'}, \mathcal{L}'_{\mathbb{C}})\}.$$

We optimistically conjecture that an analogous conjecture is true of torsion cohomology.

Conjecture 1.4 (Galois structure). *For related rationally acyclic local systems $\mathcal{L}^0 \to \mathcal{M}_{\mathcal{U}}$, $\mathcal{L}'^0 \to \mathcal{M}_{\mathcal{U}'}$, the graded $\mathbb{Z}[\sigma]$-modules $H^*(\mathcal{M}'_{\mathcal{U}'}, \mathcal{L}'^0)$ and $H^*(\mathcal{M}_{\mathcal{U}}, \mathcal{L}^0)$ are isomorphic.*

Let $E' = F \times \cdots \times F/F$ be a split extension of degree p and E/F a cyclic Galois extension of degree p. For simplicity, suppose that there are compact open subgroups $\mathcal{U} \subset \boldsymbol{G}(\mathbb{A}_E^{\mathrm{fin}})$, $J \subset \boldsymbol{G}(\mathbb{A}_F^{\mathrm{fin}})$ for which $\mathbf{1}_{\mathcal{U}}\, du$ matches $\mathbf{1}_J\, dj$; examples of this sort are constructed in Section 5. If we simply take $\mathcal{U}' = J \times \cdots \times J$, then $\mathcal{U}$ and $\mathcal{U}'$ are related and we have $\mathcal{M}'_{\mathcal{U}'} = M_J \times \cdots \times M_J$. Suppose that $\mathcal{L}^0 \to \mathcal{M}_{\mathcal{U}}$ and $L^0 \to M_J$ are matching (rationally acyclic) local systems (see Section 4C). Then Conjecture 1.4 predicts that

$$H^*(\mathcal{M}_{\mathcal{U}}, \mathcal{L}^0) \cong_{\mathbb{Z}[\sigma]} H^*(\mathcal{M}'_{\mathcal{U}'}, (L^0)^{\boxtimes p}) = H^*(M_J \times \cdots \times M_J, (L^0)^{\boxtimes p}) \cong (H^*(M_J, L^0))^{\widehat{\otimes} p},$$

where $\widehat{\otimes} p$ denotes the p-fold left-derived tensor product. For example, suppose the ℓ-primary part of $H^*(M_J, L^0)$ is isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$ in degree d, generated by $c \in H^d(M_J, L^0)$. Conjecture 1.4 predicts the existence of a graded $\mathbb{Z}[\sigma]$-submodule $\widetilde{C} \subset H^*(\mathcal{M}_{\mathcal{U}}, \mathcal{L}^0)$ isomorphic to $H^*((\mathbb{Z} \xrightarrow{\ell} \mathbb{Z})[d]^{\otimes p})$; the action of σ on the latter group is induced by cyclic permutation of the tensor factors.

Remark 1.5. One computes that $H^*((\mathbb{Z} \xrightarrow{\ell} \mathbb{Z})[d]^{\otimes p})$ is isomorphic, as a graded $\mathbb{Z}[\sigma]$-module, to the exterior algebra on the $\mathbb{Z}/\ell\mathbb{Z}$-vector space

$$(\mathbb{Z}/\ell\mathbb{Z})[\sigma]/\langle \sigma^{p-1} + \cdots + \sigma + 1 \rangle$$

starting in degree $p(d-1)+1$.

We mention, in passing, an even more speculative conjecture, pertaining to Hecke-equivariance of this correspondence on cohomology.

Conjecture 1.6 (Hecke-equivariance of base change). *Suppose c, $\widetilde{C}$ are as above. Suppose that c is a $\boldsymbol{G}$-Hecke eigenclass, i.e., for every v where $\boldsymbol{G}/F_v$ is split and J_v is hyperspecial and for every $\rho \in \mathrm{Rep}({}^L\boldsymbol{G})$,*

$$T_\rho(c) = a_\rho c;$$

here, $T_\rho \in \mathcal{H}_v$ denotes the image of ρ under the Satake isomorphism $\mathcal{H}_v \cong \mathrm{Rep}({}^L\boldsymbol{G})$. Then, for every $\tilde{c} \in \widetilde{C}$ and every $\tau \in \mathrm{Rep}({}^L R_{E/F}\boldsymbol{G})$,

$$T_\tau \tilde{c} = a_{\tau \circ \phi} \tilde{c}.$$

1C. ***A numerical consequence to be expected of torsion base change.*** Let $\mathcal{U}, \mathcal{U}'$, $\mathcal{L}$, L, E, E', F be as in the previous section.

For Galois-equivariant, rationally acyclic local systems $\mathcal{L}^0 \to \mathcal{M}_\mathcal{U}$ as above, where $\Gamma_{E/F} = \langle\sigma\rangle$, we consider the alternating product

$$R_\sigma(\mathcal{L}) := \prod\nolimits^* \frac{|H^i(\mathcal{M}_\mathcal{U}, \mathcal{L}^0)^{\sigma-1}|}{|H^i(\mathcal{M}_\mathcal{U}, \mathcal{L}^0)^{P(\sigma)}|^{\frac{1}{p-1}}}.$$

In support of Conjecture 1.4 and Remark 1.5, we compute in [Lipnowski 2014, Lemma 5.3] that

$$R_\sigma(\mathcal{L}) = R_\sigma(L^{\boxtimes p}) = R(L)^p, \quad R(L) := \prod\nolimits^* |H^i(M_J, L^0)|, \tag{2}$$

at least up to powers of p.

The invariant $R_\sigma(\mathcal{L})$ is very closely related to the twisted Reidemeister torsion of $\mathcal{L}$ (see [Lipnowski 2014, §1.3]). It is a miraculous fact (see [Bismut and Zhang 1994, Theorem 0.2; Lipnowski 2014, Theorem 1.23]) that the twisted Reidemeister torsion is closely related to the twisted analytic torsion $\tau_\sigma(\mathcal{L})$, an equivariant spectral invariant of the metrized, equivariant local system $\mathcal{L}$ (described in [Lipnowski 2014, §1.1]). The main content of this paper is comparing $\tau_\sigma(\mathcal{L})$ to the untwisted analytic torsion $\tau(L)$ of a matching (see Section 4C) local system. A prototypical example:

Sample Theorem (comparison of analytic torsion). *Let E/F be everywhere unramified. Let $\mathcal{U} \subset \boldsymbol{G}(\mathbb{A}_E^{\mathrm{fin}})$ be a parahoric level structure* (see Definition 5.1) *and $U \subset \boldsymbol{G}(\mathbb{A}_F^{\mathrm{fin}})$ an associated level structure* (see Definition 5.3). *Then*

$$\tau_\sigma(\mathcal{M}_\mathcal{U}, \mathcal{L}) = \tau(M_U, L)^p$$

(see Corollary 4.19 combined with Theorem 6.17 for a more general statement). *By applying appropriate versions, both twisted and untwisted, of the Cheeger–Müller theorem* (see [Lipnowski 2014, §§1–2]), *we arrive at the equalities*

$$R_\sigma(\mathcal{M}_\mathcal{U}, \mathcal{L}) \sim \tau_\sigma(\mathcal{M}_\mathcal{U}, \mathcal{L}) = \tau(M_U, L)^p = R(M_U, L)^p,$$

where $\sim$ denotes equality up to powers of p. This reasoning is applicable to those matching pairs $\mathcal{L}$, L of local systems described in Section 7A.

2. Local systems over locally symmetric manifolds

2A. ***Complex local systems over locally symmetric spaces.*** Let $\boldsymbol{H}$ be a semisimple group over a number field F. Let $K \subset H = \boldsymbol{H}(F_\mathbb{R})$ be a maximal compact subgroup and $U \subset \boldsymbol{H}(\mathbb{A}_F^{\mathrm{fin}})$ a compact open subgroup. Assume U is small enough that $\boldsymbol{H}(F)$ acts freely on $\boldsymbol{H}(\mathbb{A}_F)/KU$. Then the quotient $M_U = \boldsymbol{H}(F)\backslash\boldsymbol{H}(\mathbb{A}_F)/KU$ is a manifold.

Let W be a complex vector space and $\rho : H \to \mathrm{GL}(W)$ an irreducible representation. We form the local system

$$L_\rho = \boldsymbol{H}(F)\backslash(\boldsymbol{H}(\mathbb{A}_F)/KU \times W) \to M_U, \tag{3}$$

where $\boldsymbol{H}(F)$ acts by $h \cdot (h'KU, w) = (hh'KU, \rho(h_\infty)w)$ and the bundle map is given by the first coordinate projection.

2A1. *Equivariant local systems.* Let Γ be a finite group of automorphisms of $\boldsymbol{H}$. Suppose the action of Γ preserves both U and K. Then Γ acts on the manifold M_U. Suppose further that the representation $\rho : H \to \mathrm{GL}(W)$ extends to a representation $\tilde{\rho} : H \rtimes \Gamma \to \mathrm{GL}(W)$. The action

$$\Gamma \times L_\rho \to L_\rho, \quad (hKU, w) \mapsto (\sigma(h)KU, \tilde{\rho}(\sigma)(w)) \tag{4}$$

covers the action of Γ on M_U. The action (4) gives L_ρ the structure of an equivariant local system.

2A2. *Riemannian structure.* We refer to [Bergeron and Venkatesh 2013, §3.4] for a discussion of the normalizations used here.

Let θ be the Cartan involution corresponding to K with associated decomposition $\mathfrak{h} := \mathrm{Lie}(\boldsymbol{H}(F_\mathbb{R})) = \mathfrak{k} \oplus \mathfrak{p}$ into the $+1$-eigenspace $\mathfrak{k} = \mathrm{Lie}(K)$ and the -1-eigenspace $\mathfrak{p}$.

By Weyl's unitary trick, the irreducible representation $\rho : \boldsymbol{H}(F_\mathbb{R}) \to \mathrm{GL}(W)$ corresponds to a unique representation, which we also call ρ, of the compact dual group S of H; more precisely S is the normalizer in $\boldsymbol{H}(F_\mathbb{C})$ of the real Lie algebra $\mathfrak{k} \oplus i\mathfrak{p}$. There is a unique Hermitian metric on W_ι which is S-invariant, up to scaling. Fix such a choice of metric $\langle \cdot, \cdot \rangle_0$. We use this choice to define a metric $\| \cdot \|$ on the bundles L_ρ:

$$\|(hKU, v)\|^2 = \|\rho(h_\infty^{-1})v\|_0^2 \quad \text{for } (h, v) \in L_\rho.$$

Suppose a finite group Γ acts on $\boldsymbol{H}$ by automorphisms and normalizes K and U. Then Γ also normalizes S and so automatically preserves the metric $\| \cdot \|_0$. If the representation ρ extends to a representation $\tilde{\rho} : H \rtimes \Gamma \to \mathrm{GL}(W)$, then Γ acts on L_ρ, as in Section 2A1, by isometries.

2B. ***Rational and integral structures on local systems.*** Let W be an N-vector space with N/F a finite extension of number fields and let $\mathcal{O} \subset W$ be an O_N-lattice. Let $\rho : \boldsymbol{H} \to R_{N/F}\,\mathrm{GL}(W)$ be an algebraic representation *defined over* F. Let $U \subset \boldsymbol{H}(\mathbb{A}_F^{\mathrm{fin}})$ be a compact open subgroup and $K \subset \boldsymbol{H}(F_\mathbb{R})$ a maximal compact subgroup with $X = \boldsymbol{H}(F_\mathbb{R})/K$. Assume U is small enough that $\boldsymbol{H}(F)$ acts freely on $\boldsymbol{H}(\mathbb{A}_F)/KU$. We form an associated local system of N-vector spaces

$$L_\rho = \boldsymbol{H}(F)\backslash((\boldsymbol{H}(\mathbb{A}_F)/KU) \times W) \to M_U = \boldsymbol{H}(F)\backslash\boldsymbol{H}(\mathbb{A}_F)/KU$$

where $h \cdot (x, w) = (hx, \rho(h)w)$ for $h \in \boldsymbol{H}(F)$.

Now suppose that $\mathcal{O} \subset W$ is an O_N-lattice. The group $\boldsymbol{H}(\mathbb{A}_F^{\mathrm{fin}})$ acts through ρ on the space of O_N lattices of W, and we suppose that U stabilizes $\mathcal{O}$. Consider the local system of O_N-lattices over $X \times \boldsymbol{H}(\mathbb{A}_F^{\mathrm{fin}})/U$ given by

$$\Lambda_\rho^0 := \{(x, hU, v) : v \in \rho(h)\mathcal{O}\} \to X \times \boldsymbol{H}(\mathbb{A}_F^{\mathrm{fin}})/U$$

with the bundle projection given by projection onto the first two factors. The group $\boldsymbol{H}(F)$ acts on Λ_ρ^0 diagonally: $h \cdot (x, gU, v) = (h_\infty x, h_{\mathrm{fin}} gU, \rho(h)v)$. We let

$$L_\rho^0 := \boldsymbol{H}(F)\backslash\Lambda_\rho^0 \to M_U \tag{5}$$

denote the quotient, which satisfies the following properties:

(1) L_ρ^0 is a local system of O_N-modules.

(2) $L_\rho^0 \otimes_{O_N} N = L_\rho$.

(3) Let $\iota : N \hookrightarrow \mathbb{C}$ be a complex embedding. Let $\rho_\iota : \boldsymbol{H}(F_\mathbb{R}) \to \mathrm{GL}(W_\iota)$ be the composition

$$\rho_\iota = \boldsymbol{H}(F_\mathbb{R}) \to \boldsymbol{H}(F_\mathbb{C}) \to \mathrm{GL}(W_\iota).$$

Then

$$(L_\rho^0) \otimes_\iota \mathbb{C} = L_{\rho_\iota}.$$

Here, L_{ρ_ι} denotes the local system of $\mathbb{C}$-vector spaces associated to the complex representation ρ_ι in Section 2A.

Remark 2.1. Given an algebraic representation $\tilde{\rho} : R_{E/F}\boldsymbol{H} \rtimes \Gamma_{E/F} \to R_{N/F}\,\mathrm{GL}(W)$ defined over F, the constructions of this section apply equally well and give rise to $\mathcal{L}_{\tilde{\rho}}$ and $\mathcal{L}_{\tilde{\rho}}^0$, respectively equivariant local systems of O_N-modules and N-vector spaces satisfying

$$\mathcal{L}_{\tilde{\rho}}^0 \otimes_{O_N} N = \mathcal{L}_{\tilde{\rho}} \quad \text{and} \quad \mathcal{L}_{\tilde{\rho}} \otimes_\iota \mathbb{C} = \mathcal{L}_{\tilde{\rho}_\iota},$$

where the latter is the equivariant local system of complex vector spaces constructed in Section 2A1.

3. Zeta functions and analytic torsion of equivariant, metrized local systems

3A. ***Equivariant analytic torsion over general manifolds.*** Let $\mathcal{M}$ be a compact Riemannian manifold and $\mathcal{L} \to \mathcal{M}$ a local system of $\mathbb{C}$-vector spaces equipped with a Hermitian metric. Let σ act compatibly on $\mathcal{M}$ and $\mathcal{L}$ by a finite order isometry.

Remark 3.1. We *do not* require the parallel transport associated to the flat structure $\mathcal{L} \to \mathcal{M}$ to be unitary.

Let $d_{\mathcal{L}} : \Omega^\bullet(\mathcal{M}, \mathcal{L}) \to \Omega^\bullet(\mathcal{M}, \mathcal{L})$ denote the exterior derivative, defined on local sections by $d_{\mathcal{L}}(\omega \otimes s) = dw \otimes s$. Let $d_{\mathcal{L}}^*$ denote the formal adjoint of $d_{\mathcal{L}}$. Then $\Delta = d_{\mathcal{L}} d_{\mathcal{L}}^* + d_{\mathcal{L}}^* d_{\mathcal{L}}$ is the *Laplace operator* associated to $\mathcal{L}$. We let Δ_j denote its restriction to $\Omega^j(\mathcal{M}, \mathcal{L})$.

Definition 3.2 (cf. [Lück 1993, (1.12)]). The *j-th equivariant zeta function of* $(\mathcal{L} \to \mathcal{M}, \sigma)$ is defined by

$$\zeta_{j,\mathcal{L},\sigma}(s) = \sum_{\lambda > 0} \operatorname{tr}(\sigma | E_\lambda) \lambda^{-s},$$

where the sum runs over the positive eigenvalues λ of Δ_j, with corresponding eigenspace E_λ.

The *j-th zeta function of the metrized local system of complex vector spaces* $L \to M$ over a compact Riemannian manifold is defined by

$$\zeta_{j,L} := \zeta_{j,L,\mathrm{id}}.$$

Each $\zeta_{j,\mathcal{L},\sigma}$ admits a meromorphic continuation to the entire complex plane which is regular at $s = 0$ [Lück 1993, Lemma 1.13].

Definition 3.3 [Lück 1993, Definition 1.14]. The *equivariant analytic torsion* of the triple $(\mathcal{L} \to \mathcal{M}, \sigma)$ is the quantity

$$\tau_\sigma(\mathcal{L}) := \exp\left(-\frac{1}{2} \sum_{j=0}^{\dim M} (-1)^j j \cdot \zeta'_{j,\mathcal{L},\sigma}(0) \right).$$

The *untwisted analytic torsion* (or simply *analytic torsion*) of a metrized local system $L \to M$ over a compact Riemannian manifold M is defined to be $\tau(L) := \tau_{\mathrm{id}}(L)$.

3B. ***Equivariant analytic torsion over locally symmetric manifolds.*** Let $\boldsymbol{H}$ be a semisimple algebraic group over a number field F. Let E/F be a cyclic Galois extension of degree p with Galois group $\Gamma_{E/F} = \langle \sigma \rangle$.

Let $\mathcal{K} \subset \widetilde{H} := \boldsymbol{H}(E_{\mathbb{R}})$ be maximal compact with corresponding Cartan decomposition $\tilde{\mathfrak{h}} = \tilde{\mathfrak{k}} \oplus \tilde{\mathfrak{p}}$.

If the Casimir operator of a group $\bullet$ acts on a representation r of $\bullet$ by a scalar, let λ_r denote this scalar.

Let $\mathcal{U} \subset \boldsymbol{H}(\mathbb{A}_E^{\mathrm{fin}})$ be compact open. Assume that both $\mathcal{K}$ and $\mathcal{U}$ are Galois-stable. Assume that $\mathcal{U}$ is small enough that the quotient $\mathcal{M}_{\mathcal{U}} := \boldsymbol{H}(E) \backslash \boldsymbol{H}(\mathbb{A}_E) / \mathcal{K}\mathcal{U}$ is a manifold. Assume that $\boldsymbol{H}$ is anisotropic over E; this is equivalent to $\mathcal{M}_{\mathcal{U}}$ being compact.

Let $\tilde{\rho} : \widetilde{H} \rtimes \Gamma_{E/F} \to \mathrm{GL}(W)$ be a complex representation. Let $\mathcal{L}_{\tilde{\rho}} \to \mathcal{M}_{\mathcal{U}}$ be the $\Gamma_{E/F}$-equivariant local system associated to $\tilde{\rho}$ (see Section 2A1) endowed with the Hermitian structure described in Section 2A2.

Denote the $\boldsymbol{H}(\mathbb{A}_E) \rtimes \Gamma_{E/F}$-isotypic decomposition of $L^2(\boldsymbol{H}(E)\backslash\boldsymbol{H}(\mathbb{A}_E))$ by

$$L^2(\boldsymbol{H}(E)\backslash\boldsymbol{H}(\mathbb{A}_E)) = \bigoplus_{\tilde{\pi}} \mathcal{W}[\tilde{\pi}].$$

The equivariant zeta functions $\zeta_{j,L,\sigma}$ can be expressed purely in terms of the $\tilde{\pi}$. Before stating a precise result, we set some representation theory notation.

Notation for trace. For a σ-module A, we let $\langle A\rangle$ denote $\mathrm{tr}\{\sigma\,|\,A\}$.

Definition 3.4. An admissible, irreducible representation $\tilde{\pi}$ of $\boldsymbol{H}(\mathbb{A}_E) \rtimes \Gamma_{E/F}$ is called *essential* if $\tilde{\pi}|_{\boldsymbol{H}(\mathbb{A}_E)}$ is irreducible. It is called *inessential* otherwise.

Suppose that $\tilde{\pi} = \tilde{\pi}_\infty \otimes \tilde{\pi}_{\mathrm{fin}}$ is a representation of $\boldsymbol{H}(\mathbb{A}_E)$. Suppose further that *the action of σ on $\tilde{\pi}$ factorizes as $\tilde{\pi}(\sigma) = \tilde{\pi}_\infty(\sigma_\infty) \otimes \tilde{\pi}_{\mathrm{fin}}(\sigma_{\mathrm{fin}})$.*

Remark 3.5. Let $\boldsymbol{H}$ be the adjoint group of $\underline{D}^\times$ for a quaternion algebra over F. For every essential representation $\tilde{\pi}$ of $\boldsymbol{H}(\mathbb{A}_E) \rtimes \langle\sigma\rangle$, we have that $\tilde{\pi}(\sigma)$ admits a preferred factorization $\tilde{\pi}(\sigma) = \otimes'_v \tilde{\pi}_v(\sigma_v)$. See our discussion of base change, especially Theorem 4.11.

Lemma 3.6. *The j-th equivariant zeta function of $(\mathcal{L}_{\tilde{\rho}} \to \mathcal{M}_{\mathcal{U}}, \sigma)$ equals*

$$\zeta_{j,\mathcal{M}_{\mathcal{U}},\mathcal{L}_{\tilde{\rho}},\sigma}(s) = \sum_{\lambda} \lambda^{-s} \sum_{\substack{\tilde{\pi}\ \text{essential} \\ \lambda_{\tilde{\rho}} - \lambda_{\tilde{\pi}_\infty} = \lambda}} m(\tilde{\pi}) \cdot \langle \tilde{\pi}_{\mathrm{fin}}^{\mathcal{U}} \rangle \cdot \langle \mathrm{Hom}_{\mathcal{K}}(\wedge^j \tilde{\mathfrak{p}}, \tilde{\pi}_\infty \otimes \tilde{\rho}) \rangle, \tag{6}$$

where $m(\tilde{\pi}) := \dim \mathrm{Hom}_{\boldsymbol{H}(\mathbb{A}_E)\rtimes\Gamma_{E/F}}(\tilde{\pi}, \mathcal{W})$.

Proof. See [Fung 2002, §2.3; Speh 1994]. The key inputs are as follows:

- The $\mathcal{L}_{\tilde{\rho}}$-valued differential forms on $\mathcal{M}_{\mathcal{U}}$ decompose as a (Hilbert) direct sum:

  $$\Omega^j(\mathcal{M}_{\mathcal{U}}) = \bigoplus_{\tilde{\pi}} \mathrm{Hom}_{\mathcal{K}}(\wedge^j \tilde{\mathfrak{p}}, \mathcal{W}[\tilde{\pi}]^{\mathcal{U}} \otimes \tilde{\rho}).$$

  Kuga's lemma [Borel and Wallach 2000, Chapter II, §2] states that $\Delta_{\mathcal{L}_{\tilde{\rho}}}$ acts on $\mathrm{Hom}_{\mathcal{K}}(\wedge^j \tilde{\mathfrak{p}}, \mathcal{W}[\tilde{\pi}]^{\mathcal{U}} \otimes \tilde{\rho})$ by the scalar $\lambda_{\tilde{\rho}} - \lambda_{\tilde{\pi}}$.

- If $\tilde{\pi}$ is inessential, then $\tilde{\pi}|_{\boldsymbol{H}(\mathbb{A}_E)}$ decomposes as a direct sum of p (irreducible) representations $V_1 \oplus \cdots \oplus V_p$ where $\tilde{\pi}(\sigma)$ cyclically permutes the V_i. In particular, because no summand V_i is preserved,

  $$\langle \mathrm{Hom}_{\mathcal{K}}(\wedge^j \tilde{\mathfrak{p}}, \mathcal{W}[\tilde{\pi}]^{\mathcal{U}} \otimes \tilde{\rho}) \rangle = 0 \quad \text{for inessential } \tilde{\pi}. \qquad \square$$

Corollary 3.7. *The j-th zeta function of the metrized local system $L_\rho \to M_U$ equals*

$$\zeta_{j,M_U,L_\rho}(s) = \sum_{\lambda} \lambda^{-s} \sum_{\substack{\pi \\ \lambda_{\rho_\iota} - \lambda_{\pi_\infty} = \lambda}} m(\pi) \cdot \dim \pi_{\mathrm{fin}}^U \cdot \dim(\mathrm{Hom}_K(\wedge^j \mathfrak{p}, \pi_\infty \otimes \rho)). \tag{7}$$

Proof. Lemma 3.6 specializes to the corollary statement when $E = F$, $\sigma = \mathrm{id}$, $\mathcal{U} = U$, $\mathcal{K} = K$, $\tilde{\rho} = \rho$. □

4. Base change for quaternion algebras and analytic torsion

Let $\boldsymbol{G}$ be the adjoint group of a quaternion algebra D over a number field F. Let E/F be a cyclic Galois extension of *odd* prime degree p with Galois group $\Gamma_{E/F} = \langle\sigma\rangle$. Assume that D_E is not split. Then $\boldsymbol{G}(E)\backslash\boldsymbol{G}(\mathbb{A}_E)$ and $\boldsymbol{G}(F)\backslash\boldsymbol{G}(\mathbb{A}_F)$ are compact.

Let $\mathcal{M}_{\mathcal{U}} = \boldsymbol{G}(E)\backslash\boldsymbol{G}(\mathbb{A}_E)/\mathcal{K}\mathcal{U}$ for some Galois-stable maximal compact subgroup $\mathcal{K} \subset \boldsymbol{G}(E_{\mathbb{R}})$ and some Galois-stable compact open subgroup $\mathcal{U} \subset \boldsymbol{G}(\mathbb{A}_E^{\mathrm{fin}})$. Let $M_U = \boldsymbol{G}(F)\backslash\boldsymbol{G}(\mathbb{A}_F)/KU$ for some maximal compact $K \subset \boldsymbol{G}(F_{\mathbb{R}})$ and some compact open $U \subset \boldsymbol{G}(\mathbb{A}_F^{\mathrm{fin}})$.

One main goal of this paper is to prove a spectral comparison of the flavor

$$\log \tau_\sigma(\mathcal{M}_{\mathcal{U}}, \mathcal{L}) = p \log \tau(M_U, L) \tag{8}$$

for appropriate pairs of matching local systems of complex vector spaces $\mathcal{L} \to \mathcal{M}_{\mathcal{U}}$ and $L \to M_U$.

We will prove such spectral identities using trace formula techniques, by comparing the trace of a twisted convolution operator on $L^2(\boldsymbol{G}(E)\backslash\boldsymbol{G}(\mathbb{A}_E))$ to that of an untwisted convolution operator on $L^2(\boldsymbol{G}(F)\backslash\boldsymbol{G}(\mathbb{A}_F))$, exactly in the spirit of Langlands' book [1980] on base change for GL_2.

In Section 4A, we will discuss those elements of the theory of base change needed to prove the comparison (8). In Section 4B, we discuss local-global compatibility of base change and a consequence for "multiplicities". In Section 4C, we discuss matching representations and matching local systems. Such matching pairs occur in the abstract matching theorem proved in Section 4D. Later, in Sections 5 and 6, instances of test functions satisfying the hypotheses of the abstract matching theorem will be described.

4A. ***Preliminaries on base change.*** For general references on base change, see [Langlands 1980] for GL_2 and [Arthur and Clozel 1989] for GL_n. For a comprehensive treatment of the twisted trace formula formalism, see [Labesse and Waldspurger 2013].

4A1. *Twisted convolution and convolution.*

Definition 4.1. Let $\mathrm{SM}_c(\boldsymbol{G}(\mathbb{A}_E))$ denote the space of *smooth compactly supported measures on* $\boldsymbol{G}(\mathbb{A}_E)$. More precisely, these are all finite linear combinations of measures of the form $\tilde{f}\, d\tilde{g}$ for a Haar measure $d\tilde{g}$ on $\boldsymbol{G}(\mathbb{A}_E)$ and a function $f = \prod_v f_v$. We require that f_∞ be smooth and compactly supported, that f_v be compactly supported and locally constant, and that $f_v = \mathbf{1}_{\boldsymbol{G}(O_{E_v})}$ for almost all places v of F. We define $\mathrm{SM}_c(\boldsymbol{G}(\mathbb{A}_F))$ similarly.

For any smooth, compactly supported measure $\tilde{f}\,d\tilde{g}$ on $\boldsymbol{G}(\mathbb{A}_E)$, let

$$\mathcal{R}(\tilde{f}\,d\tilde{g}) = \int_{\boldsymbol{G}(\mathbb{A}_E)} \tilde{f}(g)\mathcal{R}(g)\,d\tilde{g} \circlearrowleft L^2(\boldsymbol{G}(E)\backslash\boldsymbol{G}(\mathbb{A}_E)),$$

where $\mathcal{R}$ denotes the right regular representation of $\boldsymbol{G}(\mathbb{A}_E)$ acting on $\boldsymbol{G}(E)\backslash\boldsymbol{G}(\mathbb{A}_E)$. Note that the larger group $\boldsymbol{G}(\mathbb{A}_E) \rtimes \Gamma_{E/F}$ acts on $\boldsymbol{G}(E)\backslash\boldsymbol{G}(\mathbb{A}_E)$.

Similarly, for a smooth, compactly supported measure $f\,dg$ on $\boldsymbol{G}(\mathbb{A}_F)$, we let

$$r(f\,dg) = \int_{\boldsymbol{G}(\mathbb{A}_F)} f(g)r(g)\,dg \circlearrowleft L^2(\boldsymbol{G}(F)\backslash\boldsymbol{G}(\mathbb{A}_F)),$$

where r denotes the right regular representation of $\boldsymbol{G}(\mathbb{A}_F)$.

4A2. *Twisted conjugacy and the norm map.* Suppose that $E_v = E \otimes F_v$ is unramified over F_v, i.e., is either a split extension or an unramified field extension. We define the *norm map* [Langlands 1980, §4]

$$N : \boldsymbol{G}(E_v) \to \boldsymbol{G}(E_v), \quad x \mapsto x\sigma(x)\cdots\sigma^{p-1}(x). \tag{9}$$

Lemma 4.2 (cf. [Arthur and Clozel 1989, Lemma 1.1(i)]). *If $x \in \boldsymbol{G}(E_v)$, then Nx is $\boldsymbol{G}(E_v)$-conjugate to an element of y of $\boldsymbol{G}(F_v)$, where y is uniquely defined modulo $\boldsymbol{G}(F_v)$-conjugation.*

Proof. Lift x to $\tilde{x}$ in $D_{E_v}^\times$. We can define a norm map on $D_{E_v}^\times$ using formula (9); we also denote it by N. If $\tilde{u} = N(\tilde{x})$, then

$$\sigma(\tilde{u}) = \tilde{x}^{-1}\tilde{u}\tilde{x}.$$

The characteristic polynomial $p_{\tilde{u}}(t) = t^2 - \mathrm{trd}(\tilde{u})t + \mathrm{nrd}(\tilde{u}) \in E_v[t]$ is thus preserved by $\Gamma_{E/F}$. Therefore, $p_{\tilde{u}}(t) \in F_v[t]$.

If $\tilde{u} \in F_v^\times \subset D_{F_v}^\times$, we are done. Otherwise, the polynomial $p_{\tilde{u}}$ is irreducible. Since the quaternion algebra D_{F_v} contains all quadratic extensions of F_v, there is some element $\tilde{u}' \in D_{F_v}$ with the same characteristic polynomial as $N\tilde{x} \in D_{E_v}$. By the Noether–Skolem theorem for D_{E_v}, we know that $N\tilde{x}$ and $\tilde{u}'$ are conjugate in $D_{E_v}^\times$, implying that the image of $\tilde{u}'$ in $\boldsymbol{G}(F_v)$ and Nx are conjugate by $\boldsymbol{G}(E_v)$. By a second application of the Noether–Skolem theorem, any two elements of $\boldsymbol{G}(F_v)$ which are $\boldsymbol{G}(E_v)$-conjugate are $\boldsymbol{G}(F_v)$-conjugate. □

Lemma 4.3 (cf. [Arthur and Clozel 1989, Lemma 1.1(ii)]). *If Nx and Ny are $\boldsymbol{G}(E_v)$-conjugate, then x and y are σ-conjugate.*

Proof. Applying σ-conjugation to x and y as necessary, we may suppose that $Nx = Ny \in \boldsymbol{G}(F_v)$. Lift x, y to $\tilde{x}$, $\tilde{y} \in D_{E_v}^\times$. Then

$$N\tilde{x} = cN\tilde{y}$$

for some $c \in E_v^\times$. This implies that

$$c^2 = \mathrm{Norm}_{E_v/F_v}(\mathrm{nrd}(\tilde{x}\tilde{y}^{-1})) \in \mathrm{Norm}_{E_v/F_v}(E_v^\times) \subset F_v^\times.$$

Since $[E_v : F_v] = p$ is odd, we have $c \in F_v^\times$. Furthermore, $F_v^\times / \mathrm{Norm}_{E_v/F_v}(E_v^\times)$ is isomorphic to $\mathrm{Gal}(E_v/F_v)$ by class field theory. Since $\mathrm{Gal}(E_v/F_v)$ has odd order p, it follows that $c = \mathrm{Norm}_{E_v/F_v}(c')$ for some $c' \in E_v^\times$. Replace $\tilde{y}$ by $\tilde{y}' = c'\tilde{y}$. By Noether–Skolem, $N\tilde{y}'$ and $N\tilde{x}$ are $D_{F_v}^\times$-conjugate. The argument from [Langlands 1980, Lemma 4.2] then shows that $\tilde{x}$ and $\tilde{y}'$ are σ-conjugate. □

Corollary 4.4. *The norm map induces a well-defined injection*

$$N : \{\sigma\text{-twisted conjugacy classes in } \boldsymbol{G}(E_v)\} \to \{\text{conjugacy classes in } \boldsymbol{G}(F_v)\},$$
$$[x] \mapsto [N(x)] \cap \boldsymbol{G}(F_v).$$

Proof. The norm map converts σ-twisted conjugacy to conjugacy because of the fact that $N(g^{-1}x\sigma(g)) = g^{-1}N(x)g$. The rest follows from Lemmas 4.2 and 4.3. □

Corollary 4.5. *If $x, y \in \boldsymbol{G}(F_v)$ are $\boldsymbol{G}(\bar{F}_v)$-conjugate, then they are $\boldsymbol{G}(F_v)$-conjugate. If $x', y' \in \boldsymbol{G}(E_v)$ are $\boldsymbol{G}(\bar{E}_v)\sigma$-conjugate, then they are $\boldsymbol{G}(E_v)\sigma$-conjugate.*

Proof. The first part follows by the same result for $\underline{D}_{F_v}^\times$; this in turn follows by the Noether–Skolem theorem.

For the second part, the assumptions imply that $Nx', Ny' \in \boldsymbol{G}(F_v)$ are $\boldsymbol{G}(\bar{F}_v)$-conjugate. By the first part, it follows that Nx' and Ny' are $\boldsymbol{G}(F_v)$-conjugate. By Lemma 4.3, it follows that x', y' are $\boldsymbol{G}(E_v)\sigma$-conjugate. □

4A3. *Matching orbital integrals.* See [Langlands 1980, §6] for a discussion of orbital integrals in the context of base change for GL_2.

For a σ-twisted conjugacy class $c = [x]$ of $\boldsymbol{G}(E_v)$, a conjugacy class $c' = [x']$ of $\boldsymbol{G}(F_v)$, and test measures $f\,dg$ on $\boldsymbol{G}(F_v)$ and $\tilde{f}\,d\tilde{g}$ on $\boldsymbol{G}(E_v)$, we let

$$\mathcal{O}_{\sigma,c}(\tilde{f}\,d\tilde{g}) = \int_{\boldsymbol{G}_{\sigma\ltimes x}(F_v)\backslash \boldsymbol{G}(E_v)} \tilde{f}(g^{-1}x\sigma(g))\,\frac{d\tilde{g}}{dz_\sigma},$$
$$\mathcal{O}_{c'}(f\,dg) = \int_{\boldsymbol{G}_{x'}(F_v)\backslash \boldsymbol{G}(F_v)} f(g^{-1}x'g)\,\frac{dg}{dz},$$

where $\boldsymbol{G}_{\sigma\ltimes x}$ denotes the twisted centralizer of x and $\boldsymbol{G}_{x'}$ denotes the centralizer of x'. See Remark 4.7 for a discussion of the Haar measures dz and dz_σ.

Definition 4.6. We say that $\tilde{f}\,d\tilde{g}$ and $f\,dg$ *match* if

$$\mathcal{O}_{c'}(f\,dg) = \begin{cases} \mathcal{O}_{\sigma,c}(\tilde{f}\,d\tilde{g}) & \text{if } c \text{ is a regular twisted conjugacy class and } c' = Nc, \\ 0 & \text{if } c' \neq Nc \text{ for any twisted conjugacy class } c. \end{cases}$$

Similarly, we say that the pure tensors $\tilde{f}\,d\tilde{g} = \prod_v \tilde{f}_v\,d\tilde{g}_v \in \mathrm{SM}_c(\boldsymbol{G}(\mathbb{A}_E))$ and $f\,dg = \prod_v f_v\,dg_v \in \mathrm{SM}_c(\boldsymbol{G}(\mathbb{A}_F))$ match if they match everywhere locally.

Remark 4.7. The definitions of $\mathcal{O}_{\sigma,\delta}$ and $\mathcal{O}_\gamma$ depend on choices of Haar measures dz_σ on $\boldsymbol{G}_{\sigma\rtimes\delta}(F_v)$ and dz on $\boldsymbol{G}_\gamma(F_v)$. However, if $\gamma = N\delta$, then the F-algebraic groups $\boldsymbol{G}_\gamma$ and $\boldsymbol{G}_{\sigma\rtimes\delta}$ are inner forms. Therefore, a choice of Haar measure dz_σ on $\boldsymbol{G}_{\sigma\rtimes\delta}(F_v)$ determines a compatible Haar measure dz on $\boldsymbol{G}_\gamma(F_v)$ (see [Kottwitz 1982, Lemma 5.8]). The equality from Definition 4.6 is to be taken with respect to this compatible choice. Though the individual orbital integrals depend on choices of Haar measure, this convention ensures that the notion of $\tilde{f}\,d\tilde{g}$ and $f\,dg$ matching is independent of all choices.

Example 4.8 [Langlands 1980, §8]. Say that E_v/F_v is split, i.e., $E_v = F_v^p$. Then for any test function $f_1\,dg_1 \times \cdots \times f_p\,dg_p$ on $\boldsymbol{G}(E_v) = \boldsymbol{G}(F_v)^p$, the convolution product $(f_1\,dg_1) * \cdots * (f_p\,dg_p)$ on $\boldsymbol{G}(F_v)$ matches.

4A4. *Statement of base change.* For this section, let $W = L^2(\boldsymbol{G}(F)\backslash\boldsymbol{G}(\mathbb{A}_F))$ and $\mathcal{W} = L^2(\boldsymbol{G}(E)\backslash\boldsymbol{G}(\mathbb{A}_E))$.

Theorem 4.9 (Saito, Shintani, Langlands). *Let $\tilde{f}\,d\tilde{g} = \prod_v \tilde{f}_v\,d\tilde{g}_v \in \mathrm{SM}_c(\boldsymbol{G}(\mathbb{A}_E))$ and $f\,dg = \prod_v f_v\,dg_v \in \mathrm{SM}_c(\boldsymbol{G}(\mathbb{A}_F))$ be matching test functions. Then*

$$\mathrm{tr}\{\mathcal{R}(\sigma)\mathcal{R}(\tilde{f}\,d\tilde{g})|\mathcal{W}\} = \mathrm{tr}\{r(f\,dg)|W\}. \tag{10}$$

Of course, the onus is on us to produce interesting examples of matching test functions. The identity (10) can be leveraged to give a more refined identity.

Corollary 4.10 [Gelbart and Jacquet 1979]. *Let E/F be a cyclic Galois extension of number fields of* odd *prime degree. There is a bijection between irreducible automorphic representations π of $\boldsymbol{G}$ and essential* (see Definition 3.4) *automorphic representations $\tilde{\pi}$ of $R_{E/F}\boldsymbol{G}\rtimes\Gamma_{E/F}$. This bijection is uniquely defined by an equality of traces: π and $\tilde{\pi}$ match if and only if*

$$\mathrm{tr}\{\mathcal{R}(\sigma)\mathcal{R}(\tilde{f}\,d\tilde{g})|\mathcal{W}[\tilde{\pi}]\} = \mathrm{tr}\{r(f\,dg)|W[\pi]\} \tag{11}$$

for all pairs of matching test functions $\tilde{f}\,d\tilde{g}$ and $f\,dg$ as above. Here, $\mathcal{W}[\tilde{\pi}]$ denotes the $\tilde{\pi}$ isotypic subspace of $\mathcal{W}$ and $W[\pi]$ the π-isotypic subspace of W.

4B. ***Local-global compatibility for base change and a consequence for multiplicities.*** The groups $R_{E/F}\boldsymbol{G}_E$ and $\boldsymbol{G}$ satisfy multiplicity one, by the Jacquet–Langlands correspondence and multiplicity one for GL_2. Therefore, the equality of (11) is equivalent to

$$\mathrm{tr}\{\tilde{\pi}(\sigma)\tilde{\pi}(\tilde{f}\,d\tilde{g})\} = \mathrm{tr}\{\pi(f\,dg)\} \tag{12}$$

for all pairs of matching test functions $\tilde{f}\,d\tilde{g}$ and $f\,dg$. Using (12), Langlands proves a local version of base change and local-global compatibility.

Theorem 4.11 [Langlands 1980, §7]. *Let E/F be a cyclic Galois extension of odd prime degree p. There is a bijection between irreducible representations π_v*

of $\boldsymbol{G}(F_v)$ and representations $\tilde{\pi}_v$ of $\boldsymbol{G}(E_v) \rtimes \Gamma_{E/F}$ which are irreducible after restricting to $\boldsymbol{G}(E_v)$. This bijection is determined by the equality of traces

$$\mathrm{tr}\{\tilde{\pi}_v(\sigma_v)\tilde{\pi}_v(\tilde{f}_v\tilde{g}_v)\} = \mathrm{tr}\{\pi_v(f_v\,dg_v)\}$$

for all pairs of matching test functions $\tilde{f}_v\,d\tilde{g}_v$ and $f_v\,dg_v$. The image of $\tilde{\pi}_v$ under this bijection is often denoted $\mathrm{BC}(\pi_v)$ *and referred to as the* base change of π_v. *This base change bijection is compatible with the global bijection of Corollary 4.10 in the sense that $\pi = \otimes'\pi_v$ globally matches the unique essential representation $\tilde{\pi} = \otimes'\tilde{\pi}_v$.*

Remark 4.12. As promised in Remark 3.5, the above local-global compatibility theorem has the following consequence: for any essential representation $\tilde{\pi} = \otimes'\tilde{\pi}_v$ of $\boldsymbol{G}(\mathbb{A}_E) \rtimes \Gamma_{E/F}$ matching the representation $\pi = \otimes'\pi_v$ of $\boldsymbol{G}(\mathbb{A}_F)$, there is a canonical factorization

$$\tilde{\pi}(\sigma) = \otimes'\tilde{\pi}(\sigma_v).$$

4B1. *Local base change and "trace matching".*

Definition 4.13. Let $\tilde{f}\,d\tilde{g}$ be a smooth measure on $\boldsymbol{G}(E_v)$ and let $f\,dg$ be a smooth measure on $\boldsymbol{G}(F_v)$. We say that $\tilde{f}\,d\tilde{g}$ and $f\,dg$ are *trace-matching* if, for every irreducible admissible representation π of $\boldsymbol{G}(F_v)$ with base change representation $\mathrm{BC}(\pi)$ of $\boldsymbol{G}(E_v)$, there is an equality

$$\mathrm{tr}\{\mathrm{BC}(\pi)(\sigma)\,\mathrm{BC}(\pi)(\tilde{f}\,d\tilde{g})\} = \mathrm{tr}\{\pi(f\,dg)\}.$$

Example 4.14. If $\tilde{f}\,d\tilde{g}$ and $f\,dg$ have matching orbital integrals in the sense of Definition 4.6, then they are trace-matching.

We record one straightforward consequence that Theorem 4.11 on local-global compatibility of base change has for comparing "multiplicities":

Lemma 4.15. *Let S be any set of places. Let $\mathcal{U} = \prod_{v\in S}\mathcal{U}_v$ be a compact open subgroup of the restricted tensor product $\prod'_{v\in S}\boldsymbol{G}(E_v)$. Suppose that $\mathbf{1}_{\mathcal{U}_v}\,du_v$ trace-matches m_v for each $v \in S$ and that $\prod_{v\in S} m_v = \sum c_U \mathbf{1}_U\,du$. Then for matching representations $\tilde{\pi} = \otimes'_v\tilde{\pi}_v$ of $\boldsymbol{G}(\mathbb{A}_E) \rtimes \Gamma_{E/F}$ and $\pi = \otimes\pi_v$ of $\boldsymbol{G}(\mathbb{A}_F)$, there is an equality*

$$\langle \tilde{\pi}_S^{\mathcal{U}} \rangle = \sum_U c_U \dim \pi_S^U,$$

where $\bullet_S$ denotes the (restricted) tensor or cartesian product over all places $v \in S$.

Proof. This follows directly by Theorem 4.11 and Section 4B1 of trace-matching:

$$\langle \tilde{\pi}_S^{\mathcal{U}} \rangle := \operatorname{tr}\{\tilde{\pi}_S(\sigma)\tilde{\pi}_S(\mathbf{1}_{\mathcal{U}}\, du)\} = \prod_{v\in S} \operatorname{tr}\{\tilde{\pi}_v(\sigma)\tilde{\pi}_v(\mathbf{1}_{\mathcal{U}_v}\, d\tilde{u}_v)\}$$
$$= \prod_{v\in S} \operatorname{tr}\{\pi(m_v)\} = \operatorname{tr}\Big\{\pi_S\Big(\sum c_U \mathbf{1}_U\, du\Big)\Big\} = \sum_U c_U \dim \pi_S^U. \qquad \square$$

4C. ***Local systems and matching representations.*** Let $\boldsymbol{H}$ be a semisimple group over the number field F. Let $i_E : F \hookrightarrow E$ be a cyclic Galois extension of prime degree p. Note that $(R_{E/F}\boldsymbol{H})_E = \prod_{\Gamma_{E/F}} \boldsymbol{H}_E$, where $\Gamma_{E/F}$ acts by permuting the factors according to its left translation action on itself. Let $i_N : F \hookrightarrow N$ be a second finite extension. Let $R_{E/F}\boldsymbol{H} \to R_{N/F}\,\mathrm{GL}(V)$, for V a finite dimensional N-vector space, be an algebraic homomorphism defined over F.

4C1. *Definition and examples of matching representations and local systems.* Suppose $\iota : N \hookrightarrow \mathbb{C}$ is a complex embedding and suppose $\mathbb{C}_\iota = N \otimes_\iota \mathbb{C}$. Then $R_{E/F}\boldsymbol{H}(\mathbb{C}_\iota) = \prod_{\iota'} \boldsymbol{H}(\mathbb{C}_{\iota'})$ where the product runs over all $\iota' : E \hookrightarrow \mathbb{C}$ extending $\iota \circ i_N$. The Galois group $\Gamma_{E/F}$ acts on this product by permuting the factors according to its action on the set $\{\iota' | \iota \circ i_N\}$. Furthermore, the induced homomorphism $R_{E/F}\boldsymbol{H}(F\otimes\mathbb{R}) \to \mathrm{GL}(V)(\mathbb{C}_\iota)$ factors as

$$R_{E/F}\boldsymbol{H}(F\otimes\mathbb{R}) \to R_{E/F}\boldsymbol{H}(F\otimes\mathbb{C}) \to R_{E/F}\boldsymbol{H}(\mathbb{C}_\iota) \to \mathrm{GL}(V)(\mathbb{C}_\iota),$$

the second map being induced by the projection $F\otimes\mathbb{C} \to \mathbb{C}_\iota$.

Definition 4.16 (matching representations for different coefficient fields). Suppose $\tilde{\rho} : R_{E/F}\boldsymbol{H} \rtimes \Gamma_{E/F} \to R_{N/F}\,\mathrm{GL}(V_{\tilde{\rho}})$ and $\rho : \boldsymbol{H} \to R_{N/F}\,\mathrm{GL}(V_\rho)$ are representations of algebraic groups over F. Let $\iota : N \hookrightarrow \mathbb{C}$ be a complex embedding. We say that $\tilde{\rho}$ *ι-matches* ρ if

$$\tilde{\rho}_\iota = \otimes_{\iota'|\iota}\rho_\iota,$$

with $\Gamma_{E/F}$ acting by permutations on the set $\{\iota' | \iota \circ i_N\}$. When no confusion will result, we abbreviate "ι-match" to "match". For local systems $V_{\tilde{\rho}}$ and V_ρ of N-vector spaces arising in the manner of Section 2B, we say that $V_{\tilde{\rho}}$ and V_ρ match exactly when $\tilde{\rho}$ and ρ match.

Definition 4.17 (matching representations for the same coefficient field). Suppose $\tilde{\rho} : R_{E/F}\boldsymbol{H} \rtimes \Gamma_{E/F} \to R_{E/F}\,\mathrm{GL}(V_{\tilde{\rho}})$ and $\rho : \boldsymbol{H} \to \mathrm{GL}(V_\rho)$ are representations of algebraic groups over F. Let $\iota : E \hookrightarrow \mathbb{C}$ be a complex embedding. We say that $\tilde{\rho}$ *ι-matches* ρ if

$$\tilde{\rho}_\iota = \otimes_{\iota'|\iota}\rho_\iota,$$

with $\Gamma_{E/F}$ acting by permutations on the set $\{\iota' | \iota \circ i_E\}$. When no confusion will result, we abbreviate "ι-match" to "match". For local systems $V_{\tilde{\rho}}$ of E-vector spaces

and V_ρ of F-vector spaces arising in the manner of Section 2B, we say that $V_{\tilde\rho}$ and V_ρ match exactly when $\tilde\rho$ and ρ match.

Main examples of matching representations. (a) Let $\rho : \boldsymbol{H} \to R_{N/F}\,\mathrm{GL}(V)$ be any representation over F. Suppose that N is a Galois closure of F containing E. For any F-algebra A, the representation ρ induces a homomorphism

$$\boldsymbol{H}(A \otimes_F E) \to \mathrm{GL}((V \otimes_F A) \otimes_F E \otimes_F N) \to \prod_i \mathrm{GL}((V \otimes_F A) \otimes_F N) \to \mathrm{GL}\Big(\bigotimes_i (V \otimes_F A) \otimes_F N\Big)$$

where the product runs over all i for which $F \xrightarrow{i_E} E \xrightarrow{i} N$ and $i \circ i_E = i_N$ where i_E and i_N are the embeddings defining E/F and N/F. The second map above is induced by the ring map

$$A \otimes_F E \otimes_F N \to A \otimes_F N, \quad a \otimes_F e \otimes_F n \mapsto (a \otimes_F i(e) \cdot n)_i.$$

The above homomorphisms are functorial in A and so define a map

$$R_{E/F}\boldsymbol{H} \to R_{F/N}\,\mathrm{GL}\Big(\bigotimes_i V\Big).$$

This map extends naturally to

$$\tilde\rho : R_{E/F}\boldsymbol{H} \rtimes \Gamma_{E/F} \to R_{F/N}\,\mathrm{GL}\Big(\bigotimes_i V\Big),$$

where $\Gamma_{E/F}$ acts by permuting the embeddings i. For every complex embedding $\iota : N \hookrightarrow \mathbb{C}$, the representations ρ and $\tilde\rho$ ι-match.

(b) Let $\rho : \boldsymbol{H} \to \mathrm{GL}(V)$ be any representation over F. There is a natural map

$$\boldsymbol{H}(A \otimes_F E) \rtimes \Gamma_{E/F} \to \mathrm{GL}(V \otimes_F A \otimes_F E)$$

given by composing ρ on $(A \otimes_F E)$-valued points with the F-algebra homomorphism

$$A \otimes_F E \to A \otimes_F E, \quad a \otimes_F e \mapsto a \otimes_F \sigma(e)$$

for each $\sigma \in \Gamma_{E/F}$. This collection of maps is functorial in F-algebras A and so defines an algebraic group homomorphism over F,

$$\tilde\rho : R_{E/F}\boldsymbol{H} \rtimes \Gamma_{E/F} \to R_{E/F}\,\mathrm{GL}(V).$$

For every complex embedding $\iota : E \hookrightarrow \mathbb{C}$, the representations ρ and $\tilde\rho$ ι-match.

4D. *An abstract matching theorem.*

4D1. *Notational setup for the matching theorem.* Let $\mathcal{M}_{\mathcal{U}} = \boldsymbol{G}(E)\backslash\boldsymbol{G}(\mathbb{A}_E)/\mathcal{K}\mathcal{U}$, where $\mathcal{K}, \mathcal{U}$ are chosen to be $\Gamma_{E/F}$-stable. This locally symmetric space is acted on by $\Gamma_{E/F} = \langle\sigma\rangle$, which is cyclic of prime degree p, by isometries. Similarly, for compact open $U \subset \boldsymbol{G}(\mathbb{A}_F^{\mathrm{fin}})$ and maximal compact K, we let $M_U = \boldsymbol{G}(E)\backslash\boldsymbol{G}(\mathbb{A}_F)/KU$. Let $\rho : \boldsymbol{G} \to R_{N/F}\,\mathrm{GL}(V_\rho)$ and $\tilde{\rho} : R_{E/F}\boldsymbol{G} \to R_{N/F}\,\mathrm{GL}(V_{\tilde{\rho}})$ be matching representations and let $\iota : N \hookrightarrow \mathbb{C}$ be a complex embedding.

For any compact group J, we let dj denote its volume-1 Haar measure.

4D2. *Statement and proof of the matching theorem.*

Theorem 4.18. *Assume that*

$$\prod \mathbf{1}_{\mathcal{U}_v}\, du_v = \mathbf{1}_{\mathcal{U}}\, d\tilde{u} \quad \textit{and} \quad \prod m_v = \sum_{\Pi(\mathcal{U})} c_U \mathbf{1}_U\, du$$

are trace-matching test functions (see Definition 4.13), *where* $\Pi(\mathcal{U})$ *is a finite set of compact open subgroups of* $\boldsymbol{G}(\mathbb{A}_F^{\mathrm{fin}})$. *Let* $\tilde{\rho}$ *and* ρ *be matching representations of* $R_{E/F}\boldsymbol{G}_E \rtimes \Gamma_{E/F}$ *and* $\boldsymbol{G}$ (*defined in Section 4C*). *Then*

$$\zeta_{j,\mathcal{M}_{\mathcal{U}},\mathcal{L}_{\tilde{\rho}_\iota},\sigma}(s) = \begin{cases} p(-1)^{a^2(p-1)} \displaystyle\sum_{\Pi(U)} c_U \zeta_{a,M_U,L_{\rho_\iota}}(s) \cdot p^{-s} & \text{if } j = pa, \\ 0 & \text{if } j \neq 0 \pmod p. \end{cases} \tag{13}$$

Proof. Because the groups $\boldsymbol{G}$ and $R_{E/F}\boldsymbol{G}$ satisfy multiplicity one, we can rewrite the above zeta functions from equations (6) and (7) as

$$\zeta_{j,\mathcal{M}_{\mathcal{U}},\mathcal{L}_{\tilde{\rho}_\iota},\sigma}(s) = \sum_{\lambda} \lambda^{-s} \sum_{\substack{\tilde{\pi} \text{ essential} \\ \lambda_{\tilde{\rho}_\iota} - \lambda_{\tilde{\pi}_\infty} = \lambda}} \langle \tilde{\pi}_{\mathrm{fin}}^{\mathcal{U}} \rangle \cdot \langle \mathrm{Hom}_{\mathcal{K}}(\wedge^j \tilde{\mathfrak{p}}, \tilde{\pi}_\infty \otimes \tilde{\rho}_\iota) \rangle, \tag{14}$$

$$\zeta_{j,M_U,L_{\rho_\iota}}(s) = \sum_{\lambda} \lambda^{-s} \sum_{\substack{\pi \\ \lambda_{\rho_\iota} - \lambda_{\pi_\infty} = \lambda}} \dim \pi_{\mathrm{fin}}^U \cdot \dim(\mathrm{Hom}_K(\wedge^j \mathfrak{p}, \pi_\infty \otimes \rho_\iota)). \tag{15}$$

We now discuss matching for the multiplicities, the Casimir eigenvalues, and the $(\mathfrak{g}, K)$-cochain groups in turn.

By Lemma 4.15, for any matching pair of an essential representation $\tilde{\pi}$ of $\boldsymbol{G}(\mathbb{A}_E) \rtimes \Gamma_{E/F}$ and an irreducible representation π of $\boldsymbol{G}(\mathbb{A}_F)$, there is an equality

$$\langle \tilde{\pi}_{\mathrm{fin}}^{\mathcal{U}} \rangle = \sum_U c_U \dim \pi_{\mathrm{fin}}^U. \tag{16}$$

We can relate the Casimir eigenvalues of $\tilde{\pi}_\infty$ and π_∞ by being more explicit about the relationship between $\tilde{\pi}_\infty$ and π_∞. Because $[E : F]$ is odd, we have $E_{\mathbb{R}} \cong (F_{\mathbb{R}})^p$. A choice of isomorphism determines an isomorphism $\boldsymbol{G}(E_{\mathbb{R}}) = \boldsymbol{G}(F_{\mathbb{R}})^p$. Langlands [1980, §8] calculates that the representation π_∞ corresponds to the representation $\tilde{\pi}_\infty = \pi_\infty^{\boxtimes p}$ of $\boldsymbol{G}(E_{\mathbb{R}}) \rtimes \Gamma_{E/F}$ equipped with intertwining isomorphism given by

a cyclic shift. Similarly, $\tilde{\rho}_\iota$ is isomorphic to $\rho_\iota^{\boxtimes p}$ with intertwining isomorphism given by the same cyclic shift. Therefore,

$$\lambda_{\tilde{\rho}_\iota} - \lambda_{\tilde{\pi}_\infty} = p(\lambda_{\rho_\iota} - \lambda_{\pi_\infty}). \tag{17}$$

Finally, note that because $\tilde{\pi}_\infty \otimes \tilde{\rho}_\iota \cong \pi_\infty^{\boxtimes p} \otimes \rho_\iota^{\boxtimes p}$ the $(\mathfrak{g}, K)$-chain complexes obey a "Künneth relationship",

$$\mathrm{Hom}_{\mathcal{K}}(\wedge^\bullet \tilde{\mathfrak{p}}, \tilde{\pi}_\infty \otimes \tilde{\rho}_\iota) = \mathrm{Hom}_K(\wedge^\bullet \mathfrak{p}, \pi_\infty \otimes \rho_\iota)^{\otimes p} \quad \text{(graded tensor product)}$$

(see [Borel and Wallach 2000, Chapter I, §1.3]) which is equivariant for the cyclic shift on the right and the σ action on the left. Exactly as in our calculations from [Lipnowski 2014, Proposition 5.1], it follows that

$$\begin{aligned}&\langle \mathrm{Hom}_{\mathcal{K}}(\wedge^j \tilde{\mathfrak{p}}, \tilde{\pi}_\infty \otimes \tilde{\rho}_\iota)\rangle \\ &= \begin{cases} (-1)^{a^2(p-1)} \cdot \dim(\mathrm{Hom}_K(\wedge^a \mathfrak{p}, \pi_\infty \otimes \rho_\iota)) & \text{if } j = pa, \\ 0 & \text{if } j \text{ is not a multiple of } p. \end{cases}\end{aligned} \tag{18}$$

By Langlands' formulation of base change (see Corollary 4.10), there is a bijection between irreducible subrepresentations $\pi \subset W$ of $\boldsymbol{G}(\mathbb{A}_F)$ and essential representations $\tilde{\pi} \subset \mathcal{W}$ of $\boldsymbol{G}(\mathbb{A}_E) \rtimes \Gamma_{E/F}$. Multiplying (16), $(17)^{-s}$ and (18) together and summing over all subrepresentations π of W therefore gives the result. □

An immediate corollary concerning analytic torsion is as follows:

Corollary 4.19.

$$\log \tau_\sigma(\mathcal{M}_\mathcal{U}, \mathcal{L}_{\tilde{\rho}_\iota}) = p\left(\sum c_U \log \tau(M_U, V_{\rho_\iota})\right) - p\log(p)\left(\sum_j (-1)^j j \cdot \zeta_{j, M_U, L_{\rho_\iota}}(0)\right).$$

Remark 4.20. The second summand on the right-hand side is a red herring. It would disappear by scaling the metric on M_U by p. In particular, if $L_{\rho,\mathbb{Q}}$ is acyclic, the analytic torsion is metric independent and so the second summand automatically vanishes.

5. Matching at places where E/F is unramified

We recall our notational setup: let $\boldsymbol{G}$ be the adjoint group of the group of units of a quaternion algebra D over a number field F. Say E/F is a cyclic Galois extension of prime degree p. The Galois group $\Gamma_{E/F} = \langle\sigma\rangle$ acts on $\boldsymbol{G}(\mathbb{A}_E)$.

The goal of this section is to describe instances of local trace-matching (see Section 4B1) at places v for which E_v/F_v is unramified (see, in particular, Theorem 5.4); this will enable us to prove relationships between twisted analytic torsion on locally symmetric spaces related by base change — see Theorem 4.18.

5A. ***Parahoric level structure.*** Throughout this section, assume that E/F is everywhere unramified.

The argument for proving Theorem 4.18 and Corollary 4.19 which relates $\tau_\sigma(\mathcal{L}_{\tilde{\rho}_i})$ to $\tau(L_{\rho_i})$ hinges on the fact that $\mathbf{1}_{\mathcal{U}}\, d\tilde{u}$ and $m = \mathbf{1}_{U^\Sigma}\, du^\Sigma \times \prod_{v\in\Sigma} m_v$ are matching test functions, for an appropriate finite set of nonarchimedean places Σ of F and corresponding measures m_v on $\boldsymbol{G}(F_v)$. We introduce a type of level structure for which we will be able to prove such a matching theorem.

Definition 5.1 (parahoric level structure). A compact open subgroup $\mathcal{U}_v \subset \boldsymbol{G}(E_v)$ is called *locally parahoric* if it satisfies the following conditions:

- If D is ramified at v, then $\mathcal{U}_v$ should equal the image of the units of the maximal order of D_v in $\boldsymbol{G}(E_v)$.
- Suppose E_v is split and D is unramified at v. Identify $\boldsymbol{G}(E_v) = \boldsymbol{G}(F_v)^p$. Then $\mathcal{U}_v = U_v^p$ for an arbitrary compact open $U_v \subset \boldsymbol{G}(F_v)$.
- Say E_v/F_v is unramified and cyclic of degree p, and say D is unramified at v. The tree of $\boldsymbol{G}/F_v$ injects into the tree of $\boldsymbol{G}/E_v$ with image identified as the Galois-invariants. We insist that $\mathcal{U}_v = J$, where J is the pointwise stabilizer in $\boldsymbol{G}(E_v)$ of either a vertex or an edge of the tree of $\boldsymbol{G}/F_v$.

If $\mathcal{U} = \prod \mathcal{U}_v$ is locally parahoric at all places v of F, then we call $\mathcal{U}$ (*globally*) *parahoric*. If $\mathcal{U}$ is locally parahoric for all $v \notin \Sigma$, then we call $\mathcal{U}$ *parahoric outside* Σ.

Remark 5.2. The above definition does not apply at places v where E_v/F_v is ramified. We extend the definition of parahoric level structure, for places v where E_v/F_v is tamely ramified, in Definition 6.16.

To every parahoric level structure $\mathcal{U} \subset \boldsymbol{G}(\mathbb{A}_E^{\mathrm{fin}})$, we associate a matching level structure $U \subset \boldsymbol{G}(\mathbb{A}_F^{\mathrm{fin}})$.

Definition 5.3. Let $\mathcal{U}_v \subset \boldsymbol{G}(E_v)$ be parahoric at v. We say that U_v is *associated to* $\mathcal{U}_v$ if $U_v = \mathcal{U}_v \cap \boldsymbol{G}(F_v)$. Specifically:

- Suppose D_v is ramified. We require that U_v equals the image of the units of the maximal order of D_v in $\boldsymbol{G}(F_v)$.
- Suppose that E_v is split. Then $\mathcal{U}_v = (U_v')^p$ for some $U_v' \subset \boldsymbol{G}(F_v)$, and we require that $U_v = U_v'$.
- Suppose that E_v/F_v is an unramified field extension and that D_v is unramified. Then $\mathcal{U}_v$ equals the pointwise stabilizer in $\boldsymbol{G}(E_v)$ of some simplex of the tree of $\boldsymbol{G}/F_v$, viewed as a subset of the tree of $\boldsymbol{G}/E_v$. We require that U_v be the stabilizer of that same simplex in $\boldsymbol{G}(F_v)$.

We say that $U = \prod U_v$ is associated to $\mathcal{U} = \prod U_v$ if U_v is *associated to* $\mathcal{U}_v$ for all places v.

With these notions in hand, we now throw the kitchen sink at the issue of matching $\mathbf{1}_{\mathcal{U}}\, d\tilde{u} \leftrightarrow \mathbf{1}_U\, du$.

Theorem 5.4 (Kottwitz). *Let U_v be associated to a parahoric level structure $\mathcal{U}_v$ at v. Then the test functions $\mathbf{1}_{\mathcal{U}_v}\, d\tilde{u}_v$ and $\mathbf{1}_{U_v}\, du_v$ geometrically match, where $d\tilde{u}_v$ and du_v are volume-1 Haar measures. In particular, $\mathbf{1}_{\mathcal{U}_v}\, d\tilde{u}_v$ and $\mathbf{1}_{U_v}\, du_v$ are trace-matching* (see Definition 4.13).

Proof. Kottwitz [1986a] proves that

$$\mathrm{SO}_{\delta,\sigma}(\mathbf{1}_{\mathcal{U}_v}\, d\tilde{u}_v) = \mathrm{SO}_{N\delta}(\mathbf{1}_{U_v}\, du_v)$$

for any regular semisimple $\delta \in \boldsymbol{G}(E_v)$. Here SO denotes the stable orbital integral, whose definition is given in [Kottwitz 1986a]. Let c be a $\boldsymbol{G}(F_v)$-conjugacy class in $\boldsymbol{G}(F_v)$. Suffice it to say that if

$$\{\boldsymbol{G}(\bar{F}_v) \text{ conjugacy class of } c\} \cap \boldsymbol{G}(F_v) = c,$$
$$\{\boldsymbol{G}(\bar{E}_v)\sigma\text{-twisted conjugacy class of } c'\} \cap \boldsymbol{G}(E_v) = c'$$

for every regular semisimple conjugacy class c and regular semisimple σ-twisted conjugacy class c', then $\mathrm{SO}_{\delta,\sigma} = O_{\delta,\sigma}$ and $\mathrm{SO}_\gamma = O_\gamma$.

Corollary 4.5 shows that, if $\boldsymbol{G}$ is the adjoint group of the units of a quaternion algebra over F_v, then $\boldsymbol{G}(\bar{F}_v)$-conjugacy collapses to $\boldsymbol{G}(F_v)$-conjugacy and $\boldsymbol{G}(\bar{E}_v)\sigma$-conjugacy collapses to $\boldsymbol{G}(E_v)\sigma$-conjugacy. Thus, $\mathbf{1}_{\mathcal{U}_v}\, d\tilde{u}_v$ and $\mathbf{1}_{U_v}\, du_v$ match, as claimed. □

6. Matching at places where E/F is tamely ramified

To broaden the applicability of Section 4D, we need to prove matching theorems at places v where E_v/F_v is ramified. We assume throughout this chapter that E_v/F_v is *tamely ramified*. Our immediate goals:

(1) Characterize all (possibly ramified) representations π of $\mathrm{PGL}_2(F_v)$ for which $\mathrm{BC}(\pi)$ is unramified.

(2) Find a test function on $f\, dg$ on $\mathrm{PGL}_2(F_v)$ which trace-matches $\mathbf{1}_{\mathrm{PGL}_2(E_v)}\, d\tilde{g}$.

Characterizing those representations as in (1) will be relatively straightforward; this is done in Section 6A. We will say that representations as in (1) are *E_v-potentially unramified*. For (2), the main content is an analysis of J-fixed vectors in principal series representations for various compact open subgroups $J \subset \mathrm{PGL}_2(O_F)$; this is accomplished in Section 6C3. A test function which serves as an indicator function for E_v-potentially unramified representations is constructed in Theorem 6.15.

Notation for local fields. To ease notation in what follows, we will denote E_v/F_v by E/F. So for the remainder of this chapter, E/F will denote a tamely ramified, cyclic Galois extension of local fields, *not* an extension of global fields.

6A. ***Tamely ramified and E-potentially unramified Langlands parameters.*** Fix a rational prime ℓ not equal to the residue characteristic of F. We want to characterize continuous representations

$$\sigma : W_F \to \mathrm{SL}_2(\overline{\mathbb{Q}_\ell})$$

such that $\sigma|_{W_E}$ is unramified. Since E/F is tamely ramified, such representations σ are tamely ramified. But the tame Weil group has the very simple description

$$W_F^{\mathrm{tame}} = I_F^{\mathrm{tame}} \rtimes \langle f \rangle,$$

where I_F^{tame} is procyclic and generated by a single element u, and f is any lift of the arithmetic Frobenius. The generators f and u satisfy the single relation

$$fuf^{-1} = u^q, \quad \text{where } q = \#k_F.$$

Remark 6.1. Because $\Gamma_{E/F}$ is an abelian quotient of W_F^{tame} of prime order p, it follows that $p|(q-1)$.

Lemma 6.2. *All E-potentially unramified Langlands parameters are either unramified or conjugate to*

$$\sigma = \sigma_{a,\zeta} := f \mapsto \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \quad u \mapsto \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}$$

for $a, \zeta \in \overline{\mathbb{Q}_\ell}^\times$ *and* $\zeta^p = 1$.

Proof. Note that $I_F^{\mathrm{tame}}/I_E^{\mathrm{tame}}$ equals $\Gamma_{E/F}$, which is a cyclic group of order p. Thus, I_E^{tame} must be the unique closed subgroup of index p in I_F^{tame}. In particular, $u^p \in I_E^{\mathrm{tame}}$. It follows that if $\sigma(f) = A,\ \sigma(u) = B$, then

$$ABA^{-1} = B^q \quad \text{and} \quad B^p = 1.$$

After conjugation if necessary, we may suppose that $B = \left(\begin{smallmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{smallmatrix}\right)$, where $\zeta^p = 1$.

Assume that $\zeta \neq 1$, and let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Using the fact that $ABA^{-1} = B^q$ and that $\zeta^{q-1} = 1$, we see that $b = c = 0$. These give rise to the Langlands parameters

$$\sigma = \sigma_{a,\zeta} := f \mapsto \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \quad u \mapsto \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}.$$

These parameters correspond, by the local Langlands correspondence, to the representations $I_{s,\chi} := \mathrm{Ind}_B^G(|\cdot|^s \cdot \chi)$ where χ is a nontrivial character of $F^\times/N(E^\times)$.

If $\zeta = 1$, the resulting parameter corresponds to an unramified representation. □

6B. ***A closer look at local base change.*** Let E/F be a tamely ramified extension of local fields. The goal of this section is to construct a smooth, compactly supported test measure $m_{E,\mathrm{ur}}$ on $\mathrm{PGL}_2(F)$ such that $\mathbf{1}_{\mathrm{PGL}_2(O_E)}\,d\tilde{k}$ trace-matches $m_{E,\mathrm{ur}}$ (see Definition 4.13).

In Section 6B1, we explain how to recover the matching of orbital integrals in a more representation theoretic manner. In Section 6B2, we discuss the action of $\Gamma_{E/F}$ on the $\mathrm{PGL}_2(O_E)$-fixed vectors of a representation of $\mathrm{PGL}_2(E)$ of the form $\mathrm{BC}(\pi)$.

6B1. *Strategy for proving the local base change trace identity.* Recall the following definition from Section 4 on base change:

Definition 6.3. A representation $\tilde{\pi}$ of $\mathrm{PGL}_2(E) \rtimes \langle\sigma\rangle$ *matches* the representation π of $\mathrm{PGL}_2(F)$ if the following equality of traces holds:

$$\mathrm{tr}\{\tilde{\pi}(\sigma)\tilde{\pi}(\tilde{f}\,d\tilde{g})\} = \mathrm{tr}\{\pi(f\,dg)\} \tag{19}$$

for every pair of matching test functions $\tilde{f}\,d\tilde{g} \in \mathrm{SM}_c(\boldsymbol{G}(E))$, $f\,dg \in \mathrm{SM}_c(\boldsymbol{G}(F))$. We write $\tilde{\pi} = \mathrm{BC}(\pi)$.

Remark 6.4. The intertwining isomorphism $\tilde{\pi}(\sigma) : \pi \to \pi^\sigma$ is a priori only well-defined up to a p-th root of unity. However, the equality of traces in the above definition uniquely determines $\tilde{\pi}(\sigma)$.

For the particular choices of test functions $\tilde{f}_0\,d\tilde{g}_0$ and $f_0\,dg_0$ that we will make in the sequel, rather than proving that (19) holds by demonstrating an equality of orbital integrals, we prove it directly by using explicitly understood features of local base change for $\mathrm{PGL}_2(F)$.

6B2. *Action of σ on $\mathrm{PGL}_2(O_E)$-fixed vectors.* Let μ be the inflation to the upper triangular Borel subgroup $B \subset \mathrm{PGL}_2(F)$ of a character $T \to \mathbb{C}^\times$, where T is the diagonal torus of $\mathrm{PGL}_2(F)$, and let δ denote the modulus character of B. We let (ρ_μ, I_μ) denote the normalized principal series representation, i.e., the space of locally constant functions $f : \mathrm{PGL}_2(F) \to \mathbb{C}$ which transform by the rule $f(bg) = \mu(b)\delta(b)^{1/2} f(g)$ where ρ_μ acts by right translation.

We define $I_{\tilde{\mu}}$ similarly for characters of the upper triangular Borel subgroup $\widetilde{B} \subset \mathrm{PGL}_2(E)$. If $\tilde{\mu}^\sigma = \tilde{\mu}$, then we extend $I_{\tilde{\mu}}$ to a representation of $\mathrm{PGL}_2(E) \rtimes \Gamma_{E/F}$ by the formula

$$\rho_{\tilde{\mu}}(\sigma) f(g) = f(g^{\sigma^{-1}}).$$

Proposition 6.5 [Langlands 1980, Corollary 7.3]. *Let $N : E^\times \to F^\times$ denote the norm map. The representations $I_{\mu\circ N}$ and I_μ match. That is, for any pair $\tilde{f}\,d\tilde{g}$ and $f\,dg$ of matching test functions on $\mathrm{PGL}_2(E)$ and $\mathrm{PGL}_2(F)$ respectively, there is an equality*

$$\mathrm{tr}\{\rho_{\mu\circ N}(\sigma)\rho(\tilde{f}\,d\tilde{g})\} = \mathrm{tr}\{\rho_\mu(f\,dg)\}.$$

Corollary 6.6. *For every irreducible admissible representation π of* $\mathrm{PGL}_2(F)$, *there is an equality*

$$\mathrm{tr}\{\mathrm{BC}(\pi)(\sigma)\,\mathrm{BC}(\pi)(\mathbf{1}_{\mathrm{PGL}_2(O_E)}\,d\tilde{k})\}$$
$$= \mathrm{tr}\{\mathrm{BC}(\pi)(\mathbf{1}_{\mathrm{PGL}_2(O_E)}\,d\tilde{k})\} = \begin{cases} 1 & \text{if } \mathrm{BC}(\pi) \text{ is unramified,} \\ 0 & \text{otherwise.} \end{cases}$$

Proof. The claim is vacuously true if $\mathrm{BC}(\pi)$ is ramified. If it is unramified, then it can be embedded in an unramified principal series representation V; indeed, any representation with an Iwahori fixed vector can be embedded into an unramified principal series representation.

If V is irreducible, then $\mathrm{BC}(\pi) = V$. But Proposition 6.5 shows that for such principal series representations, in the image of base change, the action of $\Gamma_{E/F}$ on the $\mathrm{PGL}_2(O_E)$-fixed vector is trivial.

If V is reducible, then $\mathrm{BC}(\pi)$ is either Steinberg, which is ramified, or the trivial representation. One readily checks that the trivial representations of $\mathrm{PGL}_2(F)$ and $\mathrm{PGL}_2(E) \rtimes \Gamma_{E/F}$ match because each has character given by the constant function 1. Therefore, $\Gamma_{E/F}$ again acts trivially on the $\mathrm{PGL}_2(O_E)$-fixed vector of $\mathrm{BC}(\pi)$. □

6C. ***Constructing an indicator test function for E-potentially unramified representations.*** According to Corollary 6.6, finding a function on $\mathrm{PGL}_2(F)$ which trace-matches the volume-1 Haar measure on $\mathrm{PGL}_2(O_E)$ is equivalent to finding a test measure $m_{E,\mathrm{ur}}$ on $\mathrm{PGL}_2(F)$ satisfying

$$\mathrm{tr}\,\pi(m_{E,\mathrm{ur}}) = \begin{cases} 1 & \text{if } \pi \text{ is } E\text{-potentially unramified,} \\ 0 & \text{otherwise.} \end{cases}$$

The Langlands parameters for all E-potentially unramified representations are, in particular, tamely ramified. By the local Langlands correspondence, they therefore have Iwahori fixed vectors. Therefore, a natural place to start constructing such a test measure $m_{E,\mathrm{ur}}$ is to modify the measure $\mathbf{1}_J\,dj$ for congruence subgroups of Iwahori subgroups.

6C1. *Fixed vectors for congruence subgroups of Iwahori subgroups of* $\mathrm{PGL}_2(F)$. Let $\boldsymbol{B} \subset \mathrm{PGL}_2/O_F$ be a Borel subgroup and $\boldsymbol{N}$ its unipotent radical, and let $\boldsymbol{T} = \boldsymbol{B}/\boldsymbol{N}$. Let k_F denote the residue field of O_F, and let C be any subgroup of $\boldsymbol{T}(k_F)$. Let $I_C \subset \mathrm{PGL}_2(O_F)$ denote the preimage of C under the reduction map. The subgroup I_1 is one such example.

6C2. *Supercuspidal representations have no I_C-fixed vectors.* We quote the following theorem:

Proposition 6.7 [Bushnell and Henniart 2006, §14.3]. *If V is a supercuspidal representation of* $\mathrm{PGL}_2(F)$, *then $V^{I_1} = 0$. In particular, $V^{I_C} = 0$ for any C as above.*

6C3. *I_C-fixed vectors for principal series representations of* $\mathrm{PGL}_2(F)$. Suppose $B = \boldsymbol{B}(F),\ N = \boldsymbol{N}(F),\ T = \boldsymbol{T}(F),\ G = \mathrm{PGL}_2(F)$. We prove a simple lemma concerning the space of J-fixed vectors, for an arbitrary compact open J, in principal series representations $I_\chi = \mathrm{Ind}_B^G \chi$, where $\chi : B \to \mathbb{C}^\times$ is the inflation of a character of T.

Lemma 6.8. *The dimension of the space of J-fixed vectors $(I_\chi)^J$ equals the number of double cosets $g \in B\backslash G/J$ for which $\chi|_{B\cap gJg^{-1}} = 1$.*

Proof. Let $V = I_\chi$. If $f \in V^J$, then $f(bgj) = \chi(b) f(g)$ for $b \in B,\ j \in J$. In order for this equality to hold for all $b \in B,\ j \in J$, it is necessary and sufficient that either $\chi|_{B\cap gJg^{-1}} = 1$ or $f(g) = 0$. Therefore, $f \in V^J$ is uniquely specified by its values on those double cosets g for which $\chi_{B\cap gJg^{-1}} = 1$. □

By choosing $J = I_C$ well, we can essentially isolate all those E-potentially unramified representations, i.e., those whose Langlands parameters were classified in Section 6A.

Corollary 6.9. *Let $T_C = \{t \in \boldsymbol{T}(O_F) : t \pmod{\pi} \in C \subset \boldsymbol{T}(k_F)\}$ and let $J = I_C$. Then*

$$\dim(I_\chi)^J = \begin{cases} 2 & \text{if } \chi|_{T_C} = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Observe that the elements

$$1 \quad \text{and} \quad w = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

form a full set of coset representatives for $B\backslash G/J$. But we readily compute that the image of both $B \cap wJw^{-1}$ and $B \cap J$ in T is T_C. The result then follows immediately by Lemma 6.8. □

Corollary 6.10. *Let*

$$C_0 = \left\{ \begin{pmatrix} a^p & 0 \\ 0 & 1 \end{pmatrix} : a \in k_F^\times \right\}.$$

Then

$$\dim(I_\chi)^{I_{C_0}} = \begin{cases} 2 & \text{if } \chi|_{N(O_E^\times)} = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Remark 6.11. As pointed out in Section 6A, the E-potentially unramified principal series representations are exactly those with Langlands parameters corresponding to χ for which $\chi|_{N(O_E^\times)} = 1$, as in the first case of the above corollary.

6C4. *I_{C_0}-fixed vectors in arbitrary representations.*

Proposition 6.12. *Let π be an irreducible admissible representation of* $\mathrm{PGL}_2(F)$. *Then*

$$\operatorname{tr}\pi(1_{C_0}\,dj) = \begin{cases} 0 & \text{if } \pi \text{ is supercuspidal,} \\ 0 & \text{if } \pi = I_\chi,\ \chi|_{N(O_E^\times)} \neq 1, \\ 2 & \text{if } \pi = I_\chi,\ \chi|_{N(O_E^\times)} = 1, \\ 1 & \text{if } \pi = \mathbf{1}, \\ 1 & \text{if } \pi = \mathrm{St}, \end{cases}$$

*where dj denotes the volume-*1 *Haar measure on I_{C_0}.*

Proof. Irreducible admissible representations π of $\mathrm{PGL}_2(F)$ are of three possible types:

- π is supercuspidal. As discussed in Section 6C2, no supercuspidal representation has an I_{C_0}-fixed vector.
- By definition, if π is not supercuspidal then it is a subquotient of a principal series representation. All of the principal series representations I_χ, where $\chi \neq |\cdot|$ and $\mathbf{1}$, are irreducible. As explained in Section 6C3, such representations have a 2-dimensional space of I_{C_0}-fixed vectors if $\chi|_{N(O_E^\times)} = 1$ and a 0-dimensional space of I_{C_0}-fixed vectors otherwise.
- The representations $I_{|\cdot|}$ and $I_{\mathbf{1}}$ are reducible. In both cases, there is one trivial subquotient and another Steinberg subquotient. Both subquotients, the trivial representation and the Steinberg, have a 1-dimensional space of I_{C_0}-invariants.

The result is simply the aggregate of all of these possibilities. □

6C5. *Isolating* **1** *and* St *using the Euler–Poincaré test function.* In his work on Tamagawa numbers, Kottwitz made use of a test function which almost isolates the Steinberg representation.

Let C be a closed chamber of the building of $H = \boldsymbol{H}(F)$ for a semisimple $\boldsymbol{H}$ over F. For a compact open subgroup $J \subset H$, let dg_J denote the Haar measure of H assigning J measure 1. Let

$$\mathrm{EP} := \sum_{d=0}^{\operatorname{rank}\boldsymbol{H}} \sum_{\substack{\text{stabilizers of dim } d \\ \text{facets of } C}} (-1)^d \mathbf{1}_J\, dg_J.$$

Theorem 6.13 [Kottwitz 1986b]. *For an irreducible unitary representation π of H,*

$$\operatorname{tr}\pi(\mathrm{EP}) = \chi(H^\bullet(\pi)) = \begin{cases} 1 & \text{if } \pi = \mathbf{1}, \\ (-1)^{\operatorname{rank}\boldsymbol{H}} & \text{if } \pi = \mathrm{St}, \\ 0 & \text{otherwise.} \end{cases}$$

Corollary 6.14. *In the case of $\boldsymbol{H} = \mathrm{PGL}_2$, the formula from Theorem 6.13 holds for any irreducible admissible representation.*

Proof. Once again, we invoke the classification of irreducible admissible representations of $\mathrm{PGL}_2(F)$. Any nonunitary irreducible admissible representation must be an irreducible principal series representation of the form $\pi_s = I_{|\cdot|^s\chi_0}$. But

$$s \mapsto \operatorname{tr} \pi_s(\mathrm{EP})$$

is a continuous, integer-valued function of s and so must be constant and equal to $\operatorname{tr} \pi_0(\mathrm{EP}) = 0$. □

We are finally able to write down an indicator test function for E-potentially unramified representations.

Theorem 6.15. *The test function $m_{E,\mathrm{ur}} = \frac{1}{2}[\mathrm{EP} + 1_{C_0}\, dj]$ satisfies*

$$\operatorname{tr} \pi(m_{E,\mathrm{ur}}) = \begin{cases} 1 & \text{if } \pi \text{ is } E\text{-potentially unramified}, \\ 0 & \text{otherwise}. \end{cases}$$

Proof. This follows immediately from Proposition 6.12 and Corollary 6.14. □

6D. ***Definition of tame parahoric level structure and globally matching test functions.*** We now extend the definition of parahoric level structure to include places v of F for which E_v/F_v is tamely ramified.

Definition 6.16. Let E/F be everywhere tamely ramified. Also, assume that the set of places v where E_v/F_v is ramified is disjoint from the set of places where D_{F_v} is ramified. Let $\mathcal{U}_v \subset \boldsymbol{G}(E_v)$ be a compact open subgroup. We call $\mathcal{U}_v$ *tamely parahoric at* v if

- $\mathcal{U}_v$ is parahoric at v if E_v/F_v is split or unramified, and
- $\mathcal{U}_v = \mathrm{PGL}_2(O_{E_v})$ if E_v/F_v is tamely ramified.

We call a level structure $\mathcal{U} = \prod \mathcal{U}_v \subset \boldsymbol{G}(\mathbb{A}_E^{\mathrm{fin}})$ (*globally*) *tamely parahoric* if $\mathcal{U}_v$ is tamely parahoric at v for all v.

We now consolidate all of the preceding results of Section 6 to provide a class of examples of globally matching test functions.

Theorem 6.17. *Let E/F be everywhere tamely ramified, with $\Sigma = \{v_1, \ldots, v_n\}$ the places of F which ramify in E. Let $\mathcal{U} \subset \boldsymbol{G}(\mathbb{A}_E^{\mathrm{fin}})$ be a globally tamely parahoric level structure. Define $\mathcal{U}^\Sigma = \prod_{v \notin \Sigma} \mathcal{U}_v$, and let U^Σ denote a matching parahoric level structure outside Σ. For $v \in \Sigma$, let*

$$m_{E_v,\mathrm{ur}} = \frac{1}{2}\mathbf{1}_{K_v} dk_v + \frac{1}{2}\mathbf{1}_{K_v'} dk_v' - \frac{1}{2}\mathbf{1}_{I_v} di_v + \frac{1}{2}\mathbf{1}_{I_{C_{0,v}}} dc_0 := \sum_{i=1}^{4} c_{v,i}\, du_{v,i},$$

where K_v and K_v' are the stabilizers of two vertices in the tree for $\boldsymbol{G}(F_v) \cong \mathrm{PGL}_2(F_v)$; I_v is the pointwise stabilizer of the edge between them; $I_{C_{0,v}}$ is the "preimage in I_v of the p-th powers of the diagonal torus mod v" (cf. Corollary 6.10); *and dk denotes the volume-1 Haar measure for any compact group K. Then the test functions*

$$\mathbf{1}_{\mathcal{U}}\, du \leftrightarrow \sum c_{v_1,i_1} \cdots c_{v_n,i_n} \mathbf{1}_{\prod_{j=1}^n U_{v_j,i_j} \times U^\Sigma} \prod_{j=1}^n du_{v_j,i_j} \times du^\Sigma$$

trace-match (see Definition 4.13).

Proof. Theorem 6.15 shows that $m_{E_v,\mathrm{ur}}$ trace-matches $\mathbf{1}_{\mathcal{U}_v}\, d\tilde{u}_v$ for each place $v \in \Sigma$. For $v \notin \Sigma$, let U_v be associated to the parahoric level structure $\mathcal{U}_v$. Theorem 5.4 shows that $\mathbf{1}_{U_v}\, du_v$ trace-matches $\mathbf{1}_{\mathcal{U}_v}\, d\tilde{u}_v$. Therefore,

$$\mathbf{1}_{\mathcal{U}}\, d\tilde{u} \leftrightarrow \prod_{v \in \Sigma} m_{E_v,\mathrm{ur}} \times \mathbf{1}_{U^\Sigma}\, du^\Sigma \tag{20}$$

are matching test functions. The result follows after expanding the right-hand side of (20). □

7. A numerical form of base change functoriality for torsion

In this section, we'll exhibit examples of F-acyclic local systems of O_F-modules on locally symmetric spaces associated to $\boldsymbol{G}$ for which the Cheeger–Müller theorems of [Lipnowski 2014, §1.7, §4] can be applied. In conjunction with the trace formula comparison proven in Section 4D, this will yield a numerical form of torsion base change functoriality.

In Section 7A, we will describe a certain class of F-acyclic local systems of O_F-modules over locally symmetric spaces associated to $\boldsymbol{G}$. In Section 7B, we will prove the main comparison theorem of this paper, concerning a version of "numerical functoriality".

7A. ***A class of local systems.*** We recall the construction of some local systems described in [Calegari and Venkatesh 2012, §10.1].

For any quaternion algebra Q over F, we let $[Q]_m$ denote the F-vector space $[Q]_m = \mathrm{Sym}^m Q^0 / \Delta \,\mathrm{Sym}^{m-2} Q^0$, where Q^0 denotes the trace zero elements of Q and Δ denotes any invariant element of $\mathrm{Sym}^2 Q^0$. The F-vector space $[Q]_m$ affords an F-linear representation of $Q^\times / F^\times$, which acts by conjugation on Q and thus on the symmetric powers of Q^0.

Let $V_{a,b} = [D]_a \otimes [\bar{D}]_b$, where $\bar{D}$ denotes the quaternion algebra $D \otimes_\sigma F$, with σ denoting the nontrivial automorphism of F. We note that $[\bar{D}]_b = [\overline{D}]_b$.

Consider the representation $\rho_{a,b} : \boldsymbol{G} \to \mathrm{GL}(V_{a,b})$ given by conjugation action. By the second construction outlined in Section 4C, there is a matching representation $\tilde{\rho}_{a,b} : R_{E/F}\boldsymbol{G} \rtimes \Gamma_{E/F} \to R_{E/F}\,\mathrm{GL}(V_{a,b})$.

Suppose that $U \subset \boldsymbol{G}(\mathbb{A}_F^{\mathrm{fin}})$ is compact open and $K \subset \boldsymbol{G}(F_{\mathbb{R}})$ is a maximal compact subgroup. Suppose that $\mathcal{U} \subset \boldsymbol{G}(\mathbb{A}_E^{\mathrm{fin}})$ is compact open and $\mathcal{K} \subset \boldsymbol{G}(E_{\mathbb{R}})$ is maximal compact, with both $\mathcal{U}$ and $\mathcal{K}$ Galois-stable. Fix an O_F-lattice $\mathcal{O} \subset \rho_{a,b}$ and an O_E-lattice $\widetilde{\mathcal{O}} \subset \tilde{\rho}_{a,b}$. Suppose that U stabilizes $\mathcal{O}$ and $\mathcal{U}$ stabilizes $\widetilde{\mathcal{O}}$. By the construction of Section 2B, the matching representations $\rho_{a,b}$ and $\tilde{\rho}_{a,b}$ together with these data give rise to matching local systems

$$L_{a,b} \to M_U = \boldsymbol{G}(F)\backslash \boldsymbol{G}(\mathbb{A}_F)/KU, \quad \mathcal{L}_{a,b} \to \mathcal{M}_{\mathcal{U}} = \boldsymbol{G}(E)\backslash \boldsymbol{G}(\mathbb{A}_E)/\mathcal{K}\mathcal{U}.$$

For each complex embedding $\iota : E \hookrightarrow \mathbb{C}$, we let

$$L_{a,b,\iota} = L_{a,b} \otimes_{\iota \circ i_F} \mathbb{C}, \quad \mathcal{L}_{a,b,\iota} = \mathcal{L}_{a,b} \otimes_{\iota} \mathbb{C},$$

be local systems of $\mathbb{C}$-vector spaces.

7A1. *Acyclicity.* We recall a theorem of Borel–Wallach, specialized to our setup:

Theorem 7.1 [Borel and Wallach 2000, §II, Proposition 6.12]. *Let $\mathcal{L} \to \mathcal{M}_{\mathcal{U}}$ be the local system of $\mathbb{C}$-vector spaces corresponding to a complex representation $\rho : \boldsymbol{G}(E_{\mathbb{R}}) = R_{E/F}\boldsymbol{G}(F_{\mathbb{R}}) \to \mathrm{GL}(V)$. Suppose that $d\rho : \mathrm{Lie}(\boldsymbol{G}(E_{\mathbb{R}})) \to \mathrm{End}(V)$ is not isomorphic to its twist by the Cartan involution of $\boldsymbol{G}(E_{\mathbb{R}})$ corresponding to $\mathcal{K}$. Then $\mathcal{L} \to \mathcal{M}_{\mathcal{U}}$ is acyclic. A similar statement holds for a local system of $\mathbb{C}$-vector spaces $L \to M_U$ corresponding to representations of $\boldsymbol{G}(F_{\mathbb{R}})$.*

Proof. See [Bergeron and Venkatesh 2013, §4.1], wherein the stronger statement that representations ρ as above give rise to "strongly acyclic families" is proven. □

Corollary 7.2. *The local systems $L_{a,b,\iota} \to M_U$, $\mathcal{L}_{a,b,\iota} \to \mathcal{M}_{\mathcal{U}}$ are acyclic provided that $a \neq b$.*

Corollary 7.3. *The O_E-module $H^\bullet(\mathcal{M}_U, \mathcal{L}_{a,b})$ and the O_F-module $H^\bullet(M_U, L_{a,b})$ are torsion for $a \neq b$.*

7B. ***Numerical comparison theorem.*** We can finally combine our trace formula comparisons with the Cheeger–Müller theorems of [Lipnowski 2014, §1.7] to obtain a numerical comparison of Reidemeister torsion.

Theorem 7.4. *Let F be an imaginary quadratic field. Let E/F be Galois and cyclic of odd prime degree p. Let $a \neq b$. Then there is an equality*

$$\log \mathrm{RT}_\sigma(\mathcal{M}_{\mathcal{U}}, \mathcal{L}_{a,b,\iota}) = p\Big(\sum c_{v_1,i_1} \cdots c_{v_n,i_n} \log \mathrm{RT}(M_{\prod_{j=1}^n U_{v_j,i_j} \times U^\Sigma}, L_{a,b,\iota})\Big), \quad (21)$$

where the constants $c_{v,k}$ and level structures are as in Theorem 6.17.

Proof. By Theorem 6.17, the test functions

$$\mathbf{1}_{\mathcal{U}}\, du \leftrightarrow \sum c_{v_1,i_1} \cdots c_{v_n,i_n} \mathbf{1}_{\prod_{j=1}^n U_{v_j,i_j} \times U^\Sigma} \prod_{j=1}^n du_{v_j,i_j} \times du_\Sigma$$

are matching. By Corollary 4.19, there is thus an equality

$$\log \tau_\sigma(\mathcal{M}_\mathcal{U}, \mathcal{L}_{a,b,\iota}) = p\Big(\sum c_{v_1,i_1} \cdots c_{v_n,i_n} \log \tau(M_{\prod_{j=1}^n U_{v_j,i_j} \times U^\Sigma}, L_{a,b,\iota})\Big).$$

By the assumption $a \neq b$, Corollary 7.2 applies and so all regulators vanish. Because $\mathcal{L}_{a,b,\iota}$, $L_{a,b,\iota}$ are unimodular, the twisted Bismut–Zhang theorem (see [Lipnowski 2014, Theorem 4.1]) and the untwisted Cheeger–Müller theorem of [Müller 1993] (see [Lipnowski 2014, §1.7]) apply and give

$$\log \mathrm{RT}_\sigma(\mathcal{M}_\mathcal{U}, \mathcal{L}_{a,b,\iota}) = p\Big(\sum c_{v_1,i_1} \cdots c_{v_n,i_n} \log \mathrm{RT}(M_{\prod_{j=1}^n U_{v_j,i_j} \times U^\Sigma}, L_{a,b,\iota})\Big). \quad \square$$

The equality (21) from Theorem 7.4 is unwound into a numerical comparison between torsion cohomology groups in [Lipnowski 2014, Lemma 1.21]. A palatable corollary is as follows:

Corollary 7.5. *Let F be an imaginary quadratic field. Let E/F be an everywhere unramified cyclic Galois extension of odd prime degree p. Let $\mathcal{U} \subset \boldsymbol{G}(\mathbb{A}_E^{\mathrm{fin}})$ be a parahoric level structure and let $U = \mathcal{U} \cap \boldsymbol{G}(\mathbb{A}_F^{\mathrm{fin}})$. Suppose $a \neq b$. Then*

$$\prod{}^*\left(\frac{|H^i(\mathcal{M}_\mathcal{U}, \mathcal{L}_{a,b}^0)^{\sigma-1}|}{|H^i(\mathcal{M}_\mathcal{U}, \mathcal{L}_{a,b}^0)^{P(\sigma)}|}\right) \sim_p \left(\prod{}^* |H^i(M_U, L_{a,b}^0)|\right)^p,$$

where $\sim_p$ denotes equality up to powers of p. In particular, if $\ell \neq p$ is a prime dividing $|H^i(M_U, L_{a,b}^0)|$ for exactly one i, then ℓ divides $|H^*(\mathcal{M}_\mathcal{U}, \mathcal{L}_{a,b}^0)|$.

Proof. Because E/F is everywhere unramified, the right-hand side of (21) has $\mathrm{RT}(M_U, L_{a,b,\iota})$ as its only summand. Summing (21) over all complex embeddings ι of E and applying [Lipnowski 2014, Lemma 1.21] yields the desired result. $\square$

Remark 7.6. Empirically, the integer $|H^2(M_U, L_{a,b}^0)|$ tends to be supported at large sporadic primes [Şengün 2011]. On the other hand, the integers $|H^i(M_U, L_{a,b}^0)|$ for $i \neq 2$ provably grow at most polynomially in $\mathrm{vol}(M_U)$ [Bergeron and Venkatesh 2013, §8.6]. Corollary 7.5 thus strongly suggests an underlying torsion base change phenomenon. See Section 1A for a more detailed discussion of torsion base change.

8. Asymptotic growth of analytic torsion and torsion cohomology

Let $\boldsymbol{G}$ be the adjoint group of the unit group of a quaternion algebra D over an imaginary quadratic field F. Let E/F be a cyclic Galois extension of odd prime degree p.

In this section, we'll prove a torsion cohomology growth theorem for the local systems $\mathcal{L}_{a,b}$ defined in Section 7A over a sequence of locally symmetric spaces for $R_{E/F}\boldsymbol{G}$. The trace formula comparison that we have proven in Section 4D can be combined with the results of [Bergeron and Venkatesh 2013] to estimate the

asymptotic growth of torsion in homology through a sequence $\mathcal{M}_{\mathcal{U}_N}$ of such spaces where $\mathcal{U}_N$ is a parahoric level structure (see Definition 6.16).

We will recall the definition of a strongly acyclic family used in [Bergeron and Venkatesh 2013] in Section 8A. In Section 8B, we will prove a growth theorem for twisted analytic torsion. In Section 8C, we will combine our growth theorem for twisted analytic torsion with the Bismut–Zhang theorem to prove a torsion cohomology growth theorem.

8A. ***Redux of strong acyclicity.*** Let $L \to M$ be a metrized local system over a compact Riemannian manifold M. Let $M_n \xrightarrow{\pi_n} M$ be a sequence of covers.

Definition 8.1 (strong acyclicity). The family $L_n = \pi_n^* L \to M_n$ is *strongly acyclic* if the spectra of the Laplace operators Δ_{i,L_n}, $0 \le i \le \dim M$, admit a uniform spectral gap. That is, there is some $\epsilon > 0$ such that $\lambda > \epsilon$ for any eigenvalue λ of any Laplace operator Δ_{i,L_n}.

Bergeron and Venkatesh [2013] crucially use this hypothesis in proving a "limit multiplicity formula for analytic torsion"; it enables them to uniformly control the long time asymptotics of an infinite family of heat kernels. The surprising fact is that strongly acyclic local systems over locally symmetric spaces are abundant.

Let $\boldsymbol{H}$ be a semisimple algebraic group over F. Let M be an associated locally symmetric space $\Gamma\backslash \boldsymbol{H}(F_{\mathbb{R}})/K$.

Let $\rho : \boldsymbol{H} \to \mathrm{GL}(V_\rho)$ be a representation over F. Any O_F-lattice inside V_ρ which is stable by Γ gives rise to a local system $L_\rho^0 \to M$. We will require the following strengthened version of Theorem 7.1.

Theorem 8.2 [Bergeron and Venkatesh 2013, Theorem 4.1]. *Suppose we have $d\rho : \mathrm{Lie}(\boldsymbol{H}(F_{\mathbb{R}})) \to \mathrm{End}(V) \ncong d\rho \circ \theta$. Then for any family of covers $M_n \to M$, the family $L_n = \pi_n^* L \to M_n$ is strongly acyclic.*

8A1. *Representations of* $\mathrm{PGL}_2(\mathbb{C})$ *and strong acyclicity.* Fix a complex embedding $\iota : E \hookrightarrow \mathbb{C}$. There is an isomorphism $\boldsymbol{G}(E_{\mathbb{R}}) \cong \mathrm{PGL}_2(\mathbb{C})^p$. Via this identification, σ acts by a cyclic shift.

The irreducible representations of $\mathrm{SL}_2(\mathbb{C})$ are enumerated as

$$\rho_{a,b} = V_a \otimes \overline{V_b},$$

where $V_m = \mathrm{Sym}^m(\mathbb{C}^2)$ and where the $\bar{\bullet}$ denotes conjugation of a complex structure. In order to factor through $\mathrm{SL}_2(\mathbb{C})/\{\pm 1\} = \mathrm{PGL}_2(\mathbb{C})$, we must have $a + b$ even.

Thus, the representations of $\mathrm{PGL}_2(\mathbb{C})^p$ isomorphic to their σ-twists are of the form $\tilde{\rho}_{a,b} := (V_a \otimes \overline{V_b})^{\boxtimes p}$. The representation $\tilde{\rho}_{a,b}$ matches the representation $\rho_{a,b} := V_a \otimes \overline{V_b}$ of $\boldsymbol{G}(F_{\mathbb{R}}) \cong \mathrm{PGL}_2(\mathbb{C})$ (see Section 4C).

Remark 8.3. The $\rho_{a,b}$ from above is a slight abuse of notation. After having fixed a complex embedding ι of E, these are the homomorphisms on $F \otimes_{\mathbb{Q}} \mathbb{R}$-valued points induced by $\rho_{a,b}$ of Section 7A.

As explained in [Bergeron and Venkatesh 2013], the representations $\rho_{a,b}$ are strongly acyclic if and only if $a \neq b$. They verify that twisting by the (standard) Cartan involution θ yields $\rho_{a,b}^{\theta} = \rho_{b,a} \ncong \rho_{a,b}$. By [Bergeron and Venkatesh 2013, Lemma 4.1], this implies that $\rho_{a,b}$ is strongly acyclic.

By the same token, for the Cartan involution θ of $\mathcal{K}$, we see that

$$\tilde{\rho}_{a,b}^{\theta} = \tilde{\rho}_{b,a} \ncong \tilde{\rho}_{a,b} \quad \text{for } a \neq b,$$

implying that the sequence of local systems $\mathcal{L}_{\tilde{\rho}_{a,b,\iota}} \to \mathcal{M}_{\mathcal{U}_N}$ defined in Section 7A is strongly acyclic. In particular, the rational cohomology of this entire family of local systems vanishes.

8B. *Growth of twisted analytic torsion.*

Theorem 8.4. *Assume that E/F is everywhere tamely ramified. Assume further that the set Σ of places where E/F is ramified is disjoint from the set of places where the quaternion algebra D is ramified. Fix a complex embedding $\iota : E \hookrightarrow \mathbb{C}$.*

Let $\mathcal{U}_N \subset \mathcal{U}_0$ denote a sequence of compact open subgroups of $\boldsymbol{G}(\mathbb{A}_E^{\mathrm{fin}})$ such that:

- *The injectivity radius of $\mathcal{M}_{\mathcal{U}_N}$ approaches ∞.*
- *The level structures $\mathcal{U}_N = \prod_v \mathcal{U}_{N,v}$ are globally* tamely parahoric.

Let $U_{N,v}$ be a level structure associated with $\mathcal{U}_{N,v}$ (see Definition 5.3) *for all places $v \notin \Sigma$ and let $U_{N,v}$ be an Iwahori subgroup of* $\mathrm{PGL}_2(F_v)$ *if $v \in \Sigma$. For the matching local systems $L_{a,b}$, $\mathcal{L}_{a,b}$ defined in Section 7A,*

$$\lim_{N\to\infty} \frac{\log \tau_\sigma(\mathcal{M}_{\mathcal{U}_N}, \mathcal{L}_{a,b,\iota})}{\mathrm{vol}(M_{U_N})} \to p \cdot (1/2)^n \cdot c_{a,b} \cdot \prod_{i=1}^{n} \left(2|\boldsymbol{B}(k_{F_v})| - 1 + \frac{1}{q_v}\right) \neq 0 \quad (22)$$

where $\boldsymbol{B}$ denotes the corresponding Borel subgroup of PGL_2/O_{F_v} *and $c_{a,b}$ is a nonzero constant, the L^2-torsion of* $(\mathrm{PGL}_2(\mathbb{C}), \rho_{a,b,\iota})$ (see [Bergeron and Venkatesh 2013, Theorem 4.5]).

Proof. Because the level structure $\mathcal{U}_N$ is globally tamely parahoric, Theorem 6.17 implies that $\mathbf{1}_{\mathcal{U}}\, du$ and $\mathbf{1}_{U^\Sigma}\, du^\Sigma \times \prod_{v\in\Sigma} m_{E_v,\mathrm{ur}}$ are matching test functions (see Proposition 6.12 and Theorem 6.15 for a definition of the test function $m_{E_v,\mathrm{ur}}$). Expand the latter measure as

$$\mathbf{1}_{U^\Sigma}\, du^\Sigma \times \prod_{v\in\Sigma} m_{E_v,\mathrm{ur}} = \sum c_{v_1,i_1} \cdots c_{v_n,i_n} \mathbf{1}_{\prod_{j=1}^n U_{v_j,i_j} \times U^\Sigma} \prod_{j=1}^{n} du_{v_j,i_j} \times du_\Sigma$$

as in Theorem 6.17. Our abstract matching corollary for analytic torsion (Corollary 4.19) proves that

$$\log \tau_\sigma(\mathcal{M}_{\mathcal{U}_N}, \mathcal{L}_{a,b,\iota}) = p \sum c_{v_1,i_1} \cdots c_{v_n,i_n} \log \tau(M_{i_1,\ldots,i_n}, L_{a,b,\iota}),$$

where

$$U_{i_1,\ldots,i_n} := \prod_{j=1}^{n} U_{v_j,i_j} \times U^\Sigma, \quad M_{i_1,\ldots,i_n} = \boldsymbol{G}(F)\backslash \boldsymbol{G}(\mathbb{A}_F)/KU_{i_1,\ldots,i_n}$$

(see Theorem 6.17 for further discussion of this notation). For each tuple $(i_1, \ldots, i_n)$, the family of local systems $\mathcal{L}_{a,b,\iota} \to M_{i_1,\ldots,i_n}$ is strongly acyclic, by the discussion of Section 8A1. Therefore, we may apply the "limit multiplicity theorem for torsion" from [Bergeron and Venkatesh 2013, Theorem 4.5]. Dividing by $\mathrm{vol}(M_{U_N})$ and taking the limit as $N \to \infty$, the result follows. □

8C. *Cohomology growth theorem.*

Theorem 8.5. *Enforce all the notation and assumptions of Section 8B. Let $\mathcal{U}_N \subset \mathcal{U}_0$ denote a sequence of compact open subgroups of $\boldsymbol{G}(\mathbb{A}_E^{\mathrm{fin}})$ such that*:

- *The injectivity radius of $\mathcal{M}_{\mathcal{U}_N}$ approaches ∞.*
- *The level structures $\mathcal{U}_N = \prod_v \mathcal{U}_{N,v}$ are globally* tamely parahoric.
- *The p-adic part of the cohomology of $\mathcal{L}^0_{a,b}$ is controlled as follows, for all i*:

$$\frac{\log |H^i(\mathcal{M}_{\mathcal{U}_N}, \mathcal{L}^0_{a,b})[p^\infty]|}{\mathrm{vol}(M_{U_N})} \to 0.$$

- *There is not too much mod p cohomology in $\mathcal{L}^0_{a,b}|_{\mathcal{M}^\sigma_{\mathcal{U}_N}}$, i.e.,*

$$\frac{\log |H^i(\mathcal{M}^\sigma_{\mathcal{U}_N}, \mathcal{L}^0_{a,b,\mathbb{F}_p})|}{\mathrm{vol}(M_{U_N})} \to 0.$$

Then it follows that, for $a \neq b$,

$$\frac{\sum^* \log |H^i(\mathcal{M}_{\mathcal{U}_N}, \mathcal{L}^0_{a,b})^{\sigma-1}_{\mathrm{tors}}| - \frac{1}{p-1} \log |H^i(\mathcal{M}_{\mathcal{U}_N}, \mathcal{L}^0_{a,b})^{P(\sigma)}_{\mathrm{tors}}|}{\mathrm{vol}(M_{U_N})} \to d_{a,b} \neq 0.$$

Proof. Fix a complex embedding $\iota : E \hookrightarrow \mathbb{C}$. By Theorem 8.4, there is a limiting identity

$$\lim_{N\to\infty} \frac{\log \tau_\sigma(\mathcal{M}_{\mathcal{U}_N}, \mathcal{L}_{a,b,\iota})}{\mathrm{vol}(M_{U_N})} \to p \cdot (1/2)^n \cdot c_{a,b} \cdot \prod_{i=1}^{n} \left(2|\boldsymbol{B}(k_{F_{v_i}})| - 1 + \frac{1}{q_{v_i}}\right) \neq 0. \quad (23)$$

Combining [Lipnowski 2014, Proposition 4.5] with the results of [Lipnowski 2014, §5], specifically [Lipnowski 2014, Example 5.6], we know that

$$\tau_\sigma(\mathcal{M}, \mathcal{L}_\iota) = \mathrm{RT}_\sigma(\mathcal{M}, \mathcal{L}_\iota);$$

we have abbreviated $\mathcal{M} := \mathcal{M}_{\mathcal{U}_N}$, $\mathcal{L} = \mathcal{L}_{a,b}$. Let $A^\bullet$ denote the Morse–Smale complex for $\mathcal{L}_\iota$ and a fixed invariant weakly gradient-like vector field X on $\mathcal{M}$ satisfying Morse–Smale transversality. As proven in [Lipnowski 2014, Lemma 1.21], there exist f, $f' \in E$ such that

$$\log \mathrm{RT}_\sigma(A^\bullet) = \log|\iota(f)| - \frac{1}{p-1}\log|\iota(f')| \tag{24}$$

where

$$\mathrm{Norm}_{E/\mathbb{Q}}(f) = \prod\nolimits^* |H^i(A^\bullet[\sigma - 1])|, \quad \mathrm{Norm}_{E/\mathbb{Q}}(f') = \prod\nolimits^* |H^i(A^\bullet[P(\sigma)])|.$$

This identity is true for all embeddings ι. Summing (24) over all the embeddings ι, we find that

$$\sum_\iota \log \tau_\sigma(\mathcal{M}, \mathcal{L}_\iota) = \sum\nolimits^* \log|H^i(A^\bullet[\sigma-1])| - \frac{1}{p-1}\sum\nolimits^* \log|H^i(A^\bullet[P(\sigma)])|. \tag{25}$$

By the estimate [Lipnowski 2014, $(26)_p$] combined with [Lipnowski 2014, Proposition 3.7] which relates naive twisted Reidemeister torsion and Reidemeister torsion, we obtain that the right-hand side of (25) is equal to

$$-\Big(\sum\nolimits^* \log|H^i(\mathcal{M}, \mathcal{L}^0)[p^{-1}]^{\sigma-1}| - \frac{1}{p-1}\sum\nolimits^* \log|H^i(\mathcal{M}, \mathcal{L}^0)[p^{-1}]^{P(\sigma)}|\Big)$$
$$+ O\big(\log|H^*(\mathcal{M}, \mathcal{L}^0)[p^\infty]| + \log|H^*(\mathcal{M}, \mathcal{L}^0_{\mathbb{F}_p})| + \log|H^*(\mathcal{M}^\sigma, \mathcal{L}^0_{\mathbb{F}_p})|\big).$$

The remainder big O term in the above equation is $o(\mathrm{vol}(M_{U_N}))$ by our assumption on the size of p-power torsion in the cohomology $H^*(\mathcal{M}_{\mathcal{U}_N}, \mathcal{L}_{a,b})$ and the mod p cohomology $H^*(\mathcal{M}^\sigma_{U_N}, \mathcal{L}_{a,b,\mathbb{F}_p})$. Dividing both sides of the above equation by $\mathrm{vol}(M_{U_N})$, applying the limiting identity of (23) separately for each embedding ι, and letting $N \to \infty$ yields the desired result. □

Remark 8.6. One expects the hypothesis

$$\frac{\log|H^*(\mathcal{M}^\sigma_{\mathcal{U}_N}, \mathcal{L}^0_{a,b,\mathbb{F}_p})|}{\mathrm{vol}(M_{U_N})} \to 0 \tag{26}$$

to hold. For example, Calegari and Emerton [2011, Conjecture 1.2] have conjectured (26) whenever the M_{U_N} vary through a p-adic analytic tower of hyperbolic 3-manifolds.

Corollary 8.7. *Assume that E/F is everywhere tamely ramified of* odd *prime degree p. Assume further that the places where E/F is ramified are disjoint from the places where the quaternion algebra D is ramified.*

Let $\mathcal{U}_N \subset \mathcal{U}_0$ denote a sequence of compact open subgroups of $\boldsymbol{G}(\mathbb{A}_E^{\mathrm{fin}})$ such that:

- *The injectivity radius of $\mathcal{M}_{\mathcal{U}_N}$ approaches ∞.*
- *The level structures $\mathcal{U}_N = \prod_v \mathcal{U}_{N,v}$ are globally* tamely parahoric.

Then it follows that

$$\limsup_N \frac{\log|H^*(\mathcal{M}_{\mathcal{U}_N}, \mathcal{L}^0_{a,b})_{\mathrm{tors}}|}{\mathrm{vol}(\mathcal{M}_{\mathcal{U}_N})^{\frac{1}{p}}} > 0 \quad \textit{for } a \neq b.$$

Proof. If the p-adic part of the cohomology of the sequence $(\mathcal{M}_{\mathcal{U}_N}, \mathcal{L}^0_{a,b})$ is large, i.e., if

$$\frac{\log|H^*(\mathcal{M}_{\mathcal{U}_N}, \mathcal{L}^0_{a,b})[p^\infty]|}{\mathrm{vol}(\mathcal{M}_{\mathcal{U}_N})^{\frac{1}{p}}} \not\to 0 \quad \text{or} \quad \frac{\log|H^*(\mathcal{M}_{\mathcal{U}_N}, \mathcal{L}^0_{a,b,\mathbb{F}_p})|}{\mathrm{vol}(\mathcal{M}_{\mathcal{U}_N})^{\frac{1}{p}}} \not\to 0,$$

then the conclusion follows vacuously.

If the mod p cohomology of $(\mathcal{M}^\sigma_{\mathcal{U}_N}, \mathcal{L}^0_{a,b,\mathbb{F}_p})$ is large, i.e., if

$$\frac{\log|H^*(\mathcal{M}^\sigma_{\mathcal{U}_N}, \mathcal{L}^0_{a,b,\mathbb{F}_p})|}{\mathrm{vol}(M_{U_N})} \not\to 0,$$

then the conclusion follows by Smith theory [Bredon 1972, § III]. Indeed [Bredon 1972, § III.4.1],

$$\dim_{\mathbb{F}_p} H^*(\mathcal{M}^\sigma_{\mathcal{U}_N}, \mathcal{L}^0_{a,b,\mathbb{F}_p}) \leq \dim_{\mathbb{F}_p} H^*(\mathcal{M}_{\mathcal{U}_N}, \mathcal{L}^0_{a,b,\mathbb{F}_p}). \tag{27}$$

Since $(\mathcal{M}_{U_N}, \mathcal{L}^0_{a,b})$ has no rational cohomology by Theorem 7.1, the result follows by the universal coefficient theorem.

Otherwise, all hypotheses of Theorem 8.5 are met and so its more refined conclusion holds.[2] □

8D. ***Comparison to p-adic methods.*** Let $\boldsymbol{H}$ be a smooth semisimple algebraic group over $\mathbb{Z}_{(p)}$. Let $\mathcal{U}_{n,p} = \ker(\boldsymbol{H}(\mathbb{Z}_p) \to \boldsymbol{H}(\mathbb{Z}_p/p^n\mathbb{Z}_p))$, let $\mathcal{U}^p \subset \boldsymbol{H}(\mathbb{A}^{\infty,p})$ be a fixed compact open subgroup, and let $\mathcal{K}_H \subset \boldsymbol{H}(\mathbb{R})$ denote a maximal compact subgroup. As a byproduct of their study of completed cohomology, Calegari and Emerton [2009] are able to prove nontrivial upper and lower bounds on cohomology growth for the p-adic analytic tower of manifolds $\mathcal{M}_{\mathcal{U}_n} = \boldsymbol{H}(\mathbb{Q})\backslash\boldsymbol{H}(\mathbb{A})/\mathcal{K}_H\mathcal{U}^p_n\mathcal{U}_{n,p}$. Using Poincaré duality for completed cohomology, they show

$$\dim_{\mathbb{F}_p} H^*(\mathcal{M}_{\mathcal{U}_n}, \mathbb{F}_p) \gg \mathrm{vol}(\mathcal{M}_{\mathcal{U}_n})^{1-\alpha}$$

[2]Theorem 8.5 proves that the size of a cohomology group is exponential in $\mathrm{vol}(M_{U_N})$. But note that $\mathrm{vol}(\mathcal{M}_{\mathcal{U}_N})^{1/p}$ and $\mathrm{vol}(M_{U_N})$ have the same order of magnitude.

where $\alpha = \dim(\boldsymbol{H}(\mathbb{R})/K_H)/\dim \boldsymbol{H}(\mathbb{R})$; Calegari and Emerton [2011] prove this for $\mathcal{M}_{\mathcal{U}_n}$ a tower of hyperbolic 3-manifolds and Calegari [2013] extends this to general $\boldsymbol{H}$. For any local system $\mathcal{L}$ arising from a representation of $\boldsymbol{H}$ defined over $\mathbb{Q}$ with $\mathcal{L}_{\mathbb{Q}}$ acyclic, they deduce that

$$\log|H^*(\mathcal{M}_{\mathcal{U}_n}, \mathcal{L})_{\text{tors}}| \geq \log|H^*(\mathcal{M}_{\mathcal{U}_n}, \mathcal{L})[p^\infty]| \gg \text{vol}(\mathcal{M}_{\mathcal{U}_n})^{1-\alpha} \tag{28}$$

as an immediate consequence. It is noteworthy that $\alpha = 1/2$ if $\boldsymbol{H}(\mathbb{R})$ is a complex Lie group and $1 - \alpha \geq 1/3$ for arbitrary $\boldsymbol{H}$.

Now let $\boldsymbol{H}$ be equal to $\boldsymbol{G}$, the adjoint group of the unit group of a quaternion algebra D over an imaginary quadratic field F (viewed as a $\mathbb{Q}$-group). Suppose D is split at the odd prime p. Let E/F be an everywhere tamely ramified cyclic Galois extension of degree p. Let $\mathcal{U}_n = \mathcal{U}_{n,p}\mathcal{U}^p \subset \boldsymbol{G}(\mathbb{A}_E^{\text{fin}})$ be any parahoric level structure with $\mathcal{U}_{n,p}$ the full level p^n congruence subgroup as above. Let $\mathcal{L} = \mathcal{L}^0_{a,b}$ with $a \neq b$. Corollary 8.7 yields $|H^*(\mathcal{M}_{\mathcal{U}_n}, \mathcal{L})_{\text{tors}}| \gg \text{vol}(\mathcal{M}_{\mathcal{U}_n})^{1/p}$ whereas (28) yields the strictly better lower bound $|H^*(\mathcal{M}_{\mathcal{U}_n}, \mathcal{L})_{\text{tors}}| \gg \text{vol}(\mathcal{M}_{\mathcal{U}_n})^{1/2}$. Nonetheless, the lower bounds obtained by p-adic methods do not subsume our main theorems on torsion cohomology.

The origin of the torsion cohomology $H^*(\mathcal{M}_{\mathcal{U}_n}, \mathcal{L})_{\text{tors}}$ detected by p-adic methods should be regarded as very distinct from the torsion cohomology detected by the methods of this paper.

Cohomology classes accounted for by (28) are an aggregate of mod p congruences between (mod p) automorphic representations of $\boldsymbol{G}_E$ of arbitrary level.

On the other hand, the cohomology classes accounted for by Theorem 8.5 and Corollary 8.7 conjecturally arise by base change transfer over $\mathbb{Z}$ (see Section 1 and [Calegari and Venkatesh 2012]). Theorem 7.4 proves a numerical incarnation of base change transfer over $\mathbb{Z}$.

Base change for torsion cohomology leads us to expect that torsion detected in Theorem 8.5 is supported at the same primes as torsion in the cohomology of locally symmetric spaces for $\boldsymbol{G}/F$; computations suggest that the latter primes are large and irregular [Şengün 2011]. On the other hand, torsion detected through (28) is supported at a single prime p and gives no information about the prime-to-p part of torsion cohomology.

Theorem 8.5 and Corollary 8.7 detect torsion cohomology growth for any growing family of manifolds $\mathcal{M}_{\mathcal{U}_n}$ defined by parahoric level structures $\mathcal{U}_n$, *including* "horizontally growing families". Suppose D is split outside of a finite set of places S. Let $\mathcal{U}_S$ be an arbitrary parahoric level structure inside S. For any place v outside S, let $\mathcal{U}_v^S \subset \prod_{v' \notin S} \text{PGL}_2(O_{E,v'})$ be the product group equal to $\text{PGL}_2(O_{E,v'})$ if $v' \neq v$ and the Iwahori subgroup at v. Let $\mathcal{U}_v = \mathcal{U}_S\mathcal{U}_v^S$. Note that (28) does not give any information concerning torsion cohomology growth for horizontally growing families of manifolds like $\{\mathcal{M}_{\mathcal{U}_v}\}_{v \notin S}$.

List of symbols

We compile a list of frequently used notation. The descriptions given are consistent with the most common usage of the symbols. The reader should be warned, however, that within a given chapter or section, the symbols might carry a slightly different meaning; such local changes of notation will be made clear as necessary.

Algebraic groups and representation theory notation.

- E/F denotes a cyclic Galois extension of number fields of odd prime degree p with Galois group $\Gamma_{E/F} = \langle \sigma \rangle$. The rings O_E, O_F denote the ring of integers of E and F respectively.
- For a field extension N/F, we let $\iota : N \hookrightarrow \mathbb{C}$ denote a complex embedding of N and the induced complex embedding of F.
- D denotes a quaternion algebra over F.
- $\boldsymbol{H}$ denotes a semisimple algebraic group over a number field F.
- $\boldsymbol{G}$ denotes the adjoint group of $\underline{D}^\times$.
- $\mathcal{U}$ denotes a compact open Galois-stable subgroup of $\boldsymbol{G}(\mathbb{A}_E^{\mathrm{fin}})$ or $\boldsymbol{H}(\mathbb{A}_E^{\mathrm{fin}})$ and $\mathcal{K}$ denotes a Galois-stable maximal compact subgroup of $\boldsymbol{G}(E_{\mathbb{R}})$ or $\boldsymbol{H}(E_{\mathbb{R}})$.
- U denotes a compact open subgroup of $\boldsymbol{G}(\mathbb{A}_F^{\mathrm{fin}})$ or $\boldsymbol{H}(\mathbb{A}_F^{\mathrm{fin}})$ and K denotes a maximal compact subgroup of $\boldsymbol{G}(F_{\mathbb{R}})$ or $\boldsymbol{H}(F_{\mathbb{R}})$.
- $M_U := \boldsymbol{G}(F)\backslash\boldsymbol{G}(\mathbb{A}_F)/KU$ or $M_U := \boldsymbol{H}(F)\backslash\boldsymbol{H}(\mathbb{A}_F)/KU$.
- $\mathcal{M}_{\mathcal{U}} := \boldsymbol{G}(E)\backslash\boldsymbol{G}(\mathbb{A}_E)/\mathcal{K}\mathcal{U}$ or $\mathcal{M}_{\mathcal{U}} := \boldsymbol{H}(E)\backslash\boldsymbol{H}(\mathbb{A}_E)/\mathcal{K}\mathcal{U}$.
- $\tilde{\rho}$ is a finite dimensional representation of $R_{E/F}\boldsymbol{G}$ or $R_{E/F}\boldsymbol{H}$ and ρ is a finite dimensional representation of $\boldsymbol{G}$ or $\boldsymbol{H}$.
- L_ρ^0 and $L_\rho = L_\rho^0 \otimes_{O_N} N$ respectively denote the local system of O_N-modules and N-vector spaces associated to a rational representation ρ in the manner of Section 2B. $\mathcal{L}_{\tilde{\rho}}^0$ and $\mathcal{L}_{\tilde{\rho}}$ denote their equivariant counterparts.
- $\tilde{\pi}$ denotes a representation of $\boldsymbol{G}(\mathbb{A}_E) \rtimes \Gamma_{E/F}$ or $\boldsymbol{H}(\mathbb{A}_E) \rtimes \Gamma_{E/F}$ and π denotes a representation of $\boldsymbol{G}(\mathbb{A}_F)$ or $\boldsymbol{H}(\mathbb{A}_F)$.
- r denotes the regular representation of $\boldsymbol{G}(\mathbb{A}_F)$ on $L^2(\boldsymbol{G}(F)\backslash\boldsymbol{G}(\mathbb{A}_F))$ and $\mathcal{R}$ denotes the regular representation of $\boldsymbol{G}(\mathbb{A}_E) \rtimes \Gamma_{E/F}$ on $L^2(\boldsymbol{G}(E)\backslash\boldsymbol{G}(\mathbb{A}_E))$.
- For any representation (π, W_π) of $\boldsymbol{G}(\mathbb{A}_F)$ and any compactly supported smooth measure $f\,dg$ on $\boldsymbol{G}(\mathbb{A}_F)$, we let $\pi(f\,dg)$ denote the convolution operator

$$\int_{\boldsymbol{G}(\mathbb{A}_F)} f(g)\pi(g)\,dg \circlearrowleft W_\pi,$$

  and similarly for representations $\tilde{\pi}$ of $\boldsymbol{G}(\mathbb{A}_E)$.

- For finite dimensional complex representations $\tilde{\rho}$ and ρ of $\boldsymbol{G}(F_{\mathbb{R}})$ and $\boldsymbol{G}(E_{\mathbb{R}})$ respectively, we define

$$\mathcal{W} := L^2(\boldsymbol{G}(E)\backslash\boldsymbol{G}(\mathbb{A}_E)), \quad \mathcal{W}_{\tilde{\rho}} := L^2(\boldsymbol{G}(E)\backslash\boldsymbol{G}(\mathbb{A}_E)) \otimes \tilde{\rho},$$
$$W := L^2(\boldsymbol{G}(F)\backslash\boldsymbol{G}(\mathbb{A}_F)), \quad W_{\rho} := L^2(\boldsymbol{G}(F)\backslash\boldsymbol{G}(\mathbb{A}_F)) \otimes \rho.$$

- For a representation π of a group H and a representation V of H, we let $V[\pi]$ denote the π-isotypic subspace of H, i.e., the image of the canonical evaluation map $\mathrm{Hom}_H(\pi, V) \otimes \pi \to V$.
- For a semisimple group $\boldsymbol{H}/\mathbb{R}$ and a maximal compact subgroup $K \subset \boldsymbol{H}(\mathbb{R})$, we let θ denote the Cartan involution of $\boldsymbol{G}$ associated to K; the fixed point set of θ acting on $\boldsymbol{G}(\mathbb{R})$ equals K.
- If F is a local field with ring of integers O_F and maximal ideal $\mathfrak{m}_F$, we let k_F denote the residue field $O_F/\mathfrak{m}_F$.
- For any finite dimensional representation A of $\langle\sigma\rangle$, we let $\langle A\rangle$ denote $\mathrm{tr}\{\sigma|A\}$.
- Let V and W be finite dimensional representations of groups A, B. By $V \boxtimes W$ we mean the external tensor product representation on $V \otimes W$:

$$(a, b) \cdot (v \otimes w) = av \otimes bw.$$

  If $A = B$, we use $V \otimes W$ to denote the internal tensor product representation on the vector space $V \otimes W$:

$$a \cdot (v \otimes w) = av \otimes aw.$$

Reidemeister torsion notation.

- $\sum^*$ and $\prod^*$ respectively denote alternating sum and alternating product.
- $L \to M$ denotes a local system of projective O_F, F, $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{R}$, or $\mathbb{C}$-modules, depending on the context. $\mathcal{L} \to \mathcal{M}$ denotes a local system equivariant for the action of a finite group Γ, usually $\Gamma = \langle\sigma\rangle$ with $\sigma^p = 1$.
- $\mathrm{RT}(X, L)$ denotes the Reidemeister torsion of the Morse–Smale complex $\mathrm{MS}(X, L)$ for a vector field X, satisfying Morse–Smale transversality, and a local system $L \to M$, provided the Morse function f and the implicit volume forms are understood [Bismut and Zhang 1992]. $\mathrm{RT}_{\sigma}(\mathcal{X}, \mathcal{L})$ denotes the twisted Reidemeister torsion of the Morse–Smale complex whenever $\mathcal{L} \to \mathcal{M}$ is a $\langle\sigma\rangle$-equivariant local system. We often suppress the X, $\mathcal{X}$ and denote these by $\mathrm{RT}(M, L)$ and $\mathrm{RT}_{\sigma}(\mathcal{M}, \mathcal{L})$.
- For an R-module A which is acted on R-linearly by $\langle\sigma\rangle$, we let $A^{\sigma-1}$ be the set $\{a \in A : (\sigma - 1)\cdot a = 0\}$ and let $A^{P(\sigma)}$ be the set $\{a \in A : P(\sigma)\cdot a = 0\}$ where $P(\sigma)$ denotes the p-cyclotomic polynomial $P(x) = x^{p-1} + x^{p-2} + \cdots + 1$. Sometimes we denote these by $A[\sigma - 1]$ and $A[P(\sigma)]$ as well.

- For an R-module A which is acted on R-linearly by $\langle\sigma\rangle$, we define A' to be the set $A/(A[\sigma-1]\oplus A[P(\sigma)])$. Similarly, if $A^\bullet$ is a complex of R-modules acted on R-linearly by $\langle\sigma\rangle$, we define $A'^\bullet := A^\bullet/(A^\bullet[\sigma-1]\oplus A^\bullet[P(\sigma)])$.

Acknowledgements

This paper is an outgrowth of the author's PhD thesis. It owes its existence to the inspirational work of Bergeron–Venkatesh [2013] and Calegari–Venkatesh [2012].

The author owes thanks to many people: to Jayce Getz, Les Saper, and Mark Stern for their helpful comments on drafts of this paper; to Nicolas Bergeron for many stimulating discussions on torsion growth and twisted endoscopy; to the anonymous referee whose thoughtful feedback greatly improved this paper.

Last but not least, the author would like to express his deep gratitude to his advisor, Akshay Venkatesh, for sharing so many of his ideas and for providing constant encouragement and support during the preparation of this work.

References

[Arthur and Clozel 1989] J. Arthur and L. Clozel, *Simple algebras, base change, and the advanced theory of the trace formula*, Annals of Mathematics Studies **120**, Princeton University Press, 1989. MR 90m:22041 Zbl 0682.10022

[Bergeron and Venkatesh 2013] N. Bergeron and A. Venkatesh, "The asymptotic growth of torsion homology for arithmetic groups", *J. Inst. Math. Jussieu* **12**:2 (2013), 391–447. MR 3028790 Zbl 1266.22013

[Bismut and Zhang 1992] J.-M. Bismut and W. Zhang, *An extension of a theorem by Cheeger and Müller*, Astérisque **205**, Société Mathématique de France, Paris, 1992. MR 93j:58138 Zbl 0781.58039

[Bismut and Zhang 1994] J.-M. Bismut and W. Zhang, "Milnor and Ray–Singer metrics on the equivariant determinant of a flat vector bundle", *Geom. Funct. Anal.* **4**:2 (1994), 136–212. MR 96f:58179 Zbl 0830.58030

[Borel and Wallach 2000] A. Borel and N. Wallach, *Continuous cohomology, discrete subgroups, and representations of reductive groups*, 2nd ed., Mathematical Surveys and Monographs **67**, American Mathematical Society, Providence, RI, 2000. MR 2000j:22015 Zbl 0980.22015

[Bredon 1972] G. E. Bredon, *Introduction to compact transformation groups*, Pure and Applied Mathematics **46**, Academic Press, New York-London, 1972. MR 54 #1265 Zbl 0246.57017

[Bushnell and Henniart 2006] C. J. Bushnell and G. Henniart, *The local Langlands conjecture for* GL(2), Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences] **335**, Springer, Berlin, 2006. MR 2007m:22013 Zbl 1100.11041

[Buzzard and Gee 2015] K. Buzzard and T. Gee, "The conjectural connections between automorphic representations and Galois representations", preprint, 2015. arXiv 1009.0785

[Calegari 2013] F. Calegari, "Torsion in the cohomology of co-compact arithmetic lattices", blog entry, 2013, available at http://galoisrepresentations.wordpress.com/2013/02/06/torsion-in-the-cohomology. Published online February 6, 2013.

[Calegari and Emerton 2009] F. Calegari and M. Emerton, "Bounds for multiplicities of unitary representations of cohomological type in spaces of cusp forms", *Ann. of Math.* (2) **170**:3 (2009), 1437–1446. MR 2011c:22032 Zbl 1195.22015

[Calegari and Emerton 2011] F. Calegari and M. Emerton, "Mod-p cohomology growth in p-adic analytic towers of 3-manifolds", *Groups Geom. Dyn.* **5**:2 (2011), 355–366. MR 2012b:22010 Zbl 1242.57014

[Calegari and Venkatesh 2012] F. Calegari and A. Venkatesh, "A torsion Jacquet–Langlands correspondence", preprint, 2012. arXiv 1212.3847

[Cheeger 1979] J. Cheeger, "Analytic torsion and the heat equation", *Ann. of Math.* (2) **109**:2 (1979), 259–322. MR 80j:58065a Zbl 0412.58026

[Fung 2002] M. G. G. Fung, "Twisted torsion on compact hyperbolic spaces: a representation-theoretic approach", *Asian J. Math.* **6**:1 (2002), 169–193. MR 2003g:58050 Zbl 1018.58023

[Gelbart and Jacquet 1979] S. Gelbart and H. Jacquet, "Forms of GL(2) from the analytic point of view", pp. 213–251 in *Automorphic forms, representations and L-functions, Part 1* (Oregon State University, Corvallis, OR, 1977), edited by A. Borel and W. Casselman, Proc. Sympos. Pure Math. **XXXIII**, American Mathematical Society, Providence, RI, 1979. MR 81e:10024 Zbl 0409.22013

[Kottwitz 1982] R. E. Kottwitz, "Rational conjugacy classes in reductive groups", *Duke Math. J.* **49**:4 (1982), 785–806. MR 84k:20020 Zbl 0506.20017

[Kottwitz 1986a] R. E. Kottwitz, "Base change for unit elements of Hecke algebras", *Compositio Math.* **60**:2 (1986), 237–250. MR 88e:11039

[Kottwitz 1986b] R. E. Kottwitz, "Stable trace formula: elliptic singular terms", *Math. Ann.* **275**:3 (1986), 365–399. MR 88d:22027 Zbl 0577.10028

[Labesse and Waldspurger 2013] J.-P. Labesse and J.-L. Waldspurger, *La formule des traces tordue d'après le Friday Morning Seminar*, CRM Monograph Series **31**, American Mathematical Society, Providence, RI, 2013. MR 3026269 Zbl 1272.11070

[Langlands 1980] R. P. Langlands, *Base change for* GL(2), Annals of Mathematics Studies **96**, Princeton University Press, University of Tokyo Press, 1980. MR 82a:10032 Zbl 0444.22007

[Lipnowski 2014] M. Lipnowski, "The equivariant Cheeger–Müller theorem on locally symmetric spaces", *J. Inst. Math. Jussieu* (online publication October 2014), 1–38.

[Lück 1993] W. Lück, "Analytic and topological torsion for manifolds with boundary and symmetry", *J. Differential Geom.* **37**:2 (1993), 263–322. MR 94e:57054 Zbl 0792.53025

[Müller 1978] W. Müller, "Analytic torsion and R-torsion of Riemannian manifolds", *Adv. in Math.* **28**:3 (1978), 233–305. MR 80j:58065b Zbl 0395.57011

[Müller 1993] W. Müller, "Analytic torsion and R-torsion for unimodular representations", *J. Amer. Math. Soc.* **6**:3 (1993), 721–753. MR 93m:58119 Zbl 0789.58071

[Ray and Singer 1971] D. B. Ray and I. M. Singer, "R-torsion and the Laplacian on Riemannian manifolds", *Advances in Math.* **7** (1971), 145–210. MR 45 #4447 Zbl 0239.58014

[Şengün 2011] M. H. Şengün, "On the integral cohomology of Bianchi groups", *Exp. Math.* **20**:4 (2011), 487–505. MR 2859903 Zbl 1269.22007

[Speh 1994] B. Speh, "Analytic torsion and automorphic forms", pp. 147–156 in *Noncompact Lie groups and some of their applications* (San Antonio, TX, 1993), edited by E. A. Tanner and R. Wilson, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci. **429**, Kluwer Acad. Publ., Dordrecht, 1994. MR 96f:58183 Zbl 0845.57028

Communicated by Philippe Michel
Received 2014-05-13 Revised 2015-07-21 Accepted 2015-10-06

malipnow@math.duke.edu *Mathematics Department, Duke University, Duke University, Box 90320, Durham, NC 27708-0320, United States*

ALGEBRA AND NUMBER THEORY 9:10 (2015)
dx.doi.org/10.2140/ant.2015.9.2241

Induction parabolique et (φ, Γ)-modules

Christophe Breuil

Soit L une extension finie de $\mathbb{Q}_p$ et B un sous-groupe de Borel d'un groupe réductif déployé connexe G sur L de centre connexe. On définit un foncteur contravariant et exact à droite de la catégorie des représentations lisses de $B(L)$ sur $\mathbb{Z}/p^m\mathbb{Z}$ vers la catégorie des limites projectives de (φ, Γ)-modules étales (pour $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$) sur $\mathbb{Z}/p^m\mathbb{Z}$. On montre que ce foncteur est insensible à l'induction parabolique et que, restreint aux représentations de longueur finie dont les constituants sont des sous-quotients de séries principales, il est exact et donne de "vrais" (φ, Γ)-modules. Par passage à la limite projective, on en déduit que, convenablement normalisé, il envoie la $G(\mathbb{Q}_p)$-représentation $\Pi(\rho)^{\mathrm{ord}}$ de Breuil et Herzig (*Duke Math. J.* **164**:7 (2015), 1271–1352) vers le (φ, Γ)-module de la représentation $(L^{\otimes}|_{\widehat{B}_{C_\rho}})^{\mathrm{ord}} \circ \rho$ de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, reliant ainsi les deux constructions de loc. cit.

Let L be a finite extension of $\mathbb{Q}_p$ and B a Borel subgroup of a split reductive connected algebraic group G over L with a connected center. We define a right exact contravariant functor from the category of smooth representations of $B(L)$ over $\mathbb{Z}/p^m\mathbb{Z}$ to the category of projective limits of étale (φ, Γ)-modules (for $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$) over $\mathbb{Z}/p^m\mathbb{Z}$. We show that this functor is insensitive to parabolic induction and that, when restricted to finite length representations with all constituents being subquotients of principal series, it is exact and yields "genuine" (φ, Γ)-modules. By a projective limit process, we deduce that, conveniently normalized, it sends the $G(\mathbb{Q}_p)$-representation $\Pi(\rho)^{\mathrm{ord}}$ of Breuil and Herzig (*Duke Math. J.* **164**:7 (2015), 1271–1352) to the (φ, Γ)-module of the representation $(L^{\otimes}|_{\widehat{B}_{C_\rho}})^{\mathrm{ord}} \circ \rho$ of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, thus connecting the two constructions of loc. cit.

Je remercie pour leur soutien le CNRS, l'université Paris-Sud et le projet ThéHopaD ANR-2011-BS01-005. Je remercie Benjamin Schraen et Stefano Morra pour m'avoir informé de leurs travaux en cours [Schraen 2012–14; Morra et Schraen ≥ 2015] qui, avec [Schraen 2015], ont joué un rôle très important dans la gestation de cet article. Le travail en collaboration avec Florian Herzig [Breuil et Herzig 2015], ainsi que les dévissages astucieux de Julien Hauseux [2014], ont aussi eu une influence décisive.

MSC2010 : primary 11S20; secondary 20G25, 20G05.

Mots-clefs : p-adic Langlands, parabolic induction, (phi, Gamma)-modules.

1. Introduction

Soit p un nombre premier, L une extension finie de $\mathbb{Q}_p$ et B un sous-groupe de Borel d'un groupe algébrique réductif déployé connexe G sur L de centre connexe. L'objectif de cet article est d'une part de construire un foncteur de la catégorie des représentations lisses de $B(L)$ sur des $\mathcal{O}_E/(\varpi_E^m)$-modules (où E est une extension finie quelconque de $\mathbb{Q}_p$ d'anneau d'entiers $\mathcal{O}_E$, $\varpi_E \in \mathcal{O}_E$ une uniformisante et $m \geq 1$ un entier fixé) vers les pro-(φ, Γ)-modules étales sur $\mathcal{O}_E/(\varpi_E^m)$ (= les limites projectives de (φ, Γ)-modules étales usuels pour $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ à coefficients dans $\mathcal{O}_E/(\varpi_E^m)$), d'autre part de montrer que ce foncteur, convenablement tordu et après un passage à la limite projective, envoie la $G(\mathbb{Q}_p)$-représentation $\Pi(\rho)^{\mathrm{ord}}$ de [Breuil et Herzig 2015, §3.4] (pour ρ une représentation de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ sur E "générique ordinaire" comme dans [loc. cit.]) vers le (φ, Γ)-module du dual de la représentation $(L^{\otimes}|_{\widehat{B}_{C_\rho}})^{\mathrm{ord}} \circ \rho$ de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ ([Breuil et Herzig 2015, §2.5]), réalisant ainsi l'un des espoirs de [Breuil et Herzig 2015].

Rappelons brièvement l'histoire, encore courte, du sujet. Il a été très tôt remarqué (voir, e.g., [Breuil 2003]) que la correspondance de Langlands modulo p pour $\mathrm{GL}_2(\mathbb{Q}_p)$ devait attacher aux représentations réductibles de dimension 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ des représentations lisses de $\mathrm{GL}_2(\mathbb{Q}_p)$ *également réductibles* et génériquement de longueur 2 (en fait des extensions - éventuellement scindées - entre deux séries principales), montrant ainsi une différence fondamentale d'avec la correspondance locale classique. Ce phénomène a été expliqué par Colmez qui a construit dans [Colmez 2010] un *foncteur* exact de la catégorie des représentations lisses de longueur finie de $\mathrm{GL}_2(\mathbb{Q}_p)$ sur des $\mathcal{O}_E/(\varpi_E^m)$-modules (la définition ne nécessite en fait que l'action du Borel $B(\mathbb{Q}_p)$) vers la catégorie des (φ, Γ)-modules étales sur $\mathcal{O}_E/(\varpi_E^m)$, qui elle-même par un résultat de Fontaine [1990] est équivalente à la catégorie des représentations de longueur finie de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ sur des $\mathcal{O}_E/(\varpi_E^m)$-modules. Ce foncteur exact envoie une série principale de $\mathrm{GL}_2(\mathbb{Q}_p)$ vers

un caractère de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, et donc une extension entre deux séries principales vers une représentation réductible de dimension 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. Un peu plus tard, Schneider et Vignéras [2011] ont proposé un δ-foncteur étendant les constructions de [Colmez 2010] à un groupe algébrique réductif déployé connexe G comme au début, mais à valeurs dans des catégories de (φ, Γ)-modules à plusieurs variables. Malgré quelques résultats (voir, e.g., [Zábrádi 2011; Ollivier 2014]), le δ-foncteur de Schneider et Vignéras reste à ce jour plutôt mystérieux.

Dans [Breuil et Herzig 2015], les auteurs ont associé à une représentation modulo p (resp. p-adique) suffisamment générique ρ de dimension n de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ à valeurs dans le Borel une représentation modulo p (resp. continue unitaire p-adique) de longueur finie $\Pi(\rho)^{\mathrm{ord}}$ de $\mathrm{GL}_n(\mathbb{Q}_p)$ dont les constituants sont tous des séries principales (en fait la construction de $\Pi(\rho)^{\mathrm{ord}}$ est valable avec un groupe réductif déployé connexe de centre connexe et de dual de centre connexe). La bonne représentation $\Pi(\rho)$ de $\mathrm{GL}_n(\mathbb{Q}_p)$ associée à ρ par une hypothétique correspondance locale modulo p (resp. p-adique) n'est pas connue si $n > 2$, mais $\Pi(\rho)^{\mathrm{ord}}$ devrait être sa plus grande sous-représentation formée de séries principales. On sait par exemple dans de nombreux cas que $\Pi(\rho)^{\mathrm{ord}}$ apparaît dans des espaces de formes automorphes modulo p (resp. p-adiques), cf. [Breuil et Herzig 2015, §4] ou [Bergdall et Chojecki 2014]. Un point fondamental est que la construction de $\Pi(\rho)^{\mathrm{ord}}$ semble fonctoriellement reliée plutôt à une sous-représentation explicite de la représentation galoisienne $\otimes_{i=1}^{n-1} \bigwedge^i \rho$ qu'à la représentation ρ elle-même (si $n > 2$). Une question ouverte posée dans [Breuil et Herzig 2015, §3.5] est de savoir s'il existe un foncteur exact généralisant le foncteur défini par Colmez pour $\mathrm{GL}_2(\mathbb{Q}_p)$ et qui envoie $\Pi(\rho)^{\mathrm{ord}}$ sur le (φ, Γ)-module de cette sous-représentation (à torsion près par un caractère). Il n'est pas clair que le δ-foncteur de Schneider–Vignéras, au moins tel que, satisfasse cette condition.

Dans le présent article, on propose une nouvelle généralisation du foncteur de Colmez, dont la définition est relativement simple et naturelle, et qui envoie bien $\Pi(\rho)^{\mathrm{ord}}$ sur le (φ, Γ)-module de la sous-représentation voulue de $\otimes_{i=1}^{n-1} \bigwedge^i \rho$ (à twist près). En général ce foncteur est à valeurs dans les pro-(φ, Γ)-modules étales de Fontaine. Ses relations avec le δ-foncteur de Schneider–Vignéras ont commencé à être étudiées par Erdélyi et Zábrádi [2014].

Expliquons brièvement la définition du foncteur de cet article, qui combine des idées de Colmez [2010], Emerton [2008; 2010], Schneider–Vignéras [2011] et Schraen [2012–14; 2015]. Soit N le radical unipotent de B, on choisit d'abord un sous-groupe ouvert compact N_0 de $N(L)$ totalement décomposé (cf. § 3), un morphisme de groupes algébriques $\ell : N \to \mathbb{G}_{\mathrm{a}}$ qui se factorise par $\prod_{\alpha \in S} N_\alpha$ et qui est non nul sur chaque facteur N_α (où S désigne les racines simples de (G, B, T) et $N_\alpha \subseteq N$ le sous-groupe radiciel de la racine α) et des cocaractères fondamentaux $(\lambda_{\alpha^\vee})_{\alpha \in S} \in X^\vee(T)^S$ (qui existent car G est de centre connexe).

Soit $N_1 = \mathrm{Ker}(N_0 \xrightarrow{\ell} L \xrightarrow{\mathrm{Tr}_{L/\mathbb{Q}_p}} \mathbb{Q}_p)$ et $\xi = \sum_{\alpha\in S} \lambda_{\alpha^\vee} \in X^\vee(T)$. Si π est une représentation lisse de $B(L)$ sur un $\mathcal{O}_E/(\varpi_E^m)$-module, alors π^{N_1} est naturellement muni d'une structure de $\mathcal{O}_E/(\varpi_E^m)[\![N_0/N_1]\!] \cong \mathcal{O}_E/(\varpi_E^m)[\![X]\!]$-module, d'une action lisse de $\mathbb{Z}_p^\times$ via l'action de $\xi(\mathbb{Z}_p^\times)$ sur π (qui préserve π^{N_1}) et d'un endomorphisme $\mathcal{O}_E/(\varpi_E^m)[\![X]\!]$-semi-linéaire F donné par l'action de Hecke de $\xi(p)$ sur π^{N_1} à la manière de [Emerton 2010] (mais avec N_1 au lieu de N_0). Si $M \subseteq \pi^{N_1}$ est un sous-$\mathcal{O}_E/(\varpi_E^m)[\![X]\!][F]$-module de type fini qui est admissible comme $\mathcal{O}_E/(\varpi_E^m)[\![X]\!]$-module (i.e., tel que $\{m \in M,\ Xm = 0\}$ est un $\mathcal{O}_E/(\varpi_E^m)$-module de type fini) et stable par $\mathbb{Z}_p^\times$, alors la même preuve que dans [Colmez 2010] montre que $M^\vee[1/X] = \mathrm{Hom}_{\mathcal{O}_E/(\varpi_E^m)}(M, \mathcal{O}_E/(\varpi_E^m))[1/X]$ est naturellement muni d'une structure de (φ,Γ)-module étale sur $\mathcal{O}_E/(\varpi_E^m)$. On définit alors (voir § 3) :

$$D_\xi^\vee(\pi) \overset{\text{déf}}{=} \varprojlim_M \big(\mathrm{Hom}_{\mathcal{O}_E/(\varpi_E^m)}(M, \mathcal{O}_E/(\varpi_E^m))[1/X]\big)$$

la limite projective étant prise sur les sous-$\mathcal{O}_E/(\varpi_E^m)[\![X]\!][F]$-modules de type fini M de π^{N_1} admissibles comme $\mathcal{O}_E/(\varpi_E^m)[\![X]\!]$-modules et stables par $\mathbb{Z}_p^\times$.

On peut aussi définir $D_\xi^\vee(\pi)$ comme la limite projective des $\mathcal{O}_E/(\varpi_E^m)[\![X]\!][1/X]$-modules quotients de $\mathrm{Hom}_{\mathcal{O}_E/(\varpi_E^m)}(\pi^{N_1}, \mathcal{O}_E/(\varpi_E^m))[1/X]$ qui sont des (φ,Γ)-modules étales, voir le (iii) de la remarque 5.6.

Cette définition, assez simple et directe, a quelques inconvénients, par exemple j'ignore en général quand $D_\xi^\vee(\pi)$ est non nul ou quand c'est un "vrai" (φ,Γ)-module (étale). Par ailleurs, contrairement au cas de $\mathrm{GL}_2(\mathbb{Q}_p)$, il est impossible en général de retrouver π à partir de $D_\xi^\vee(\pi)$, comme le montre déjà le cas des séries principales (cf. Exemple 7.6). Mais elle a aussi des avantages car elle permet de montrer les résultats suivants :

(i) $D_\xi^\vee$ transforme une suite exacte $0 \to \pi' \to \pi \to \pi''$ de représentations lisses de $B(L)$ en une suite exacte $D_\xi^\vee(\pi'') \to D_\xi^\vee(\pi) \to D_\xi^\vee(\pi') \to 0$ (i.e., $D_\xi^\vee$ est contravariant exact à droite), cf. proposition 3.2 ;

(ii) $D_\xi^\vee$ est insensible aux inductions paraboliques, i.e., $D_\xi^\vee(\mathrm{Ind}_{P^-(L)}^{G(L)} \pi_P) \cong D_\xi^\vee(\pi_P)$ où P est un parabolique de G contenant B, P^- le parabolique opposé et π_P une représentation lisse du Levi $L_P(L)$, cf. Théorème 6.1 ;

(iii) $D_\xi^\vee$ est exact et donne de "vrais" (φ,Γ)-modules étales lorsque restreint à la catégorie abélienne des représentations de longueur finie de $G(L)$ dont les constituants sont des sous-quotients de séries principales, cf. corollaire 9.3.

(Et bien sûr $D_\xi^\vee$ ne dépend à isomorphisme près que de ξ, cf. § 4, et coïncide à normalisation près avec le foncteur défini par Colmez [2010] lorsque $G(L) = \mathrm{GL}_2(\mathbb{Q}_p)$, cf. proposition 3.2). Par un passage à la limite projective, la propriété (iii) permet d'étendre facilement $D_\xi^\vee$ à la catégorie abélienne des représentations continues unitaires topologiquement de longueur finie de $G(L)$ sur E dont les

constituants sont des sous-quotients de séries principales continues unitaires, cf. §9. Une motivation à l'origine de la définition de $D_\xi^\vee$ ci-dessus est de se débarrasser des constructions par "intersection" dont le comportement par suite exacte courte semble en général problématique, cf. par exemple [Schneider et Vignéras 2011, §2]. Une deuxième motivation provient des calculs de Schraen et Morra ([Morra et Schraen $\geq$ 2015; Schraen 2012–14], cf. la remarque 3.3). Une troisième motivation est la propriété (ii) ci-dessus, suggérée par les constructions de [Breuil et Herzig 2015]. En fait, les propriétés (ii) et (iii), combinées avec une compatibilité de $D_\xi^\vee$ au produit tensoriel (dont la preuve occupe le §5, cf. proposition 5.5) et un passage à la limite projective, permettent de répondre à une question importante de [Breuil et Herzig 2015, §3.5] qui avait motivé les constructions de [loc. cit.] (on renvoie au §9 pour plus de détails et pour un énoncé totalement précis) :

Théorème 1.1 (cf. corollaire 9.8). *Supposons que $L = \mathbb{Q}_p$ et que le dual $\widehat{G}$ de G a un centre connexe. Soit* :

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \widehat{B}(E)$$

une représentation continue générique au sens de [Breuil et Herzig 2015, §3.3] *où $\widehat{B}$ est le Borel dual de B et soit $\Pi(\rho)^{\mathrm{ord}}$ la représentation de $G(\mathbb{Q}_p)$ associée à ρ construite dans* [loc. cit] (*extension successive convenable de séries principales continues unitaires*). *Alors à torsion près on a un isomorphisme de (φ, Γ)-modules étales sur E* :

$$D_\xi^\vee(\Pi(\rho)^{\mathrm{ord}}) \cong (\varphi, \Gamma)\text{-module du dual de } \left((L^\otimes|_{\widehat{B}_{C_\rho}})^{\mathrm{ord}} \circ \rho\right)$$

où $L^\otimes$ est le produit tensoriel des représentations algébriques fondamentales de G sur E, $\widehat{B}_{C_\rho}$ le plus petit sous-groupe fermé de $\widehat{B}$ contenant l'image de ρ et $(L^\otimes|_{\widehat{B}_{C_\rho}})^{\mathrm{ord}}$ la "partie ordinaire" de $L^\otimes|_{\widehat{B}_{C_\rho}}$ (cf. [Breuil et Herzig 2015, §2.3]).

La même preuve (en plus simple) donne également une version en caractéristique p de ce théorème.

Bien entendu, on ne peut guère espérer faire de progrès substantiels sur $D_\xi^\vee$ sans avancer dans la compréhension des supersingulières de $G(L)$ sur $\mathcal{O}_E/(\varpi_E)$ lorsque $G(L) \neq \mathrm{GL}_2(\mathbb{Q}_p)$, comme le montre par exemple la propriété (ii) précédente combinée avec le résultat principal de [Abe 2013; Herzig 2011] (cf. aussi la remarque 8.7 et [Morra et Schraen $\geq$ 2015]). On peut par contre poser plusieurs questions naturelles sur le foncteur $D_\xi^\vee$, voir la remarque 3.3 pour deux d'entre elles. Je mentionnerai ici juste le sentiment suivant : l'exactitude de $D_\xi^\vee$ en restriction à la sous-catégorie des représentations de $G(L)$ dont les constituants sont des sous-quotients de séries principales (propriété (iii) ci-dessus, cf. aussi corollaire 9.2) suggère que cela pourrait être vrai plus généralement.

Voici les principales notations de l'article. Dans tout le texte, L (le corps de base) et E (le corps des coefficients) sont deux extensions finies quelconques de $\mathbb{Q}_p$. On note $\mathcal{O}_L$, $\mathcal{O}_E$ leurs anneaux d'entiers respectifs, $\varpi_E \in \mathcal{O}_E$ une uniformisante de $\mathcal{O}_E$ et $k_E = \mathcal{O}_E/(\varpi_E)$ son corps résiduel. On normalise l'application de réciprocité de la théorie du corps de classes local de sorte que les Frobenius géométriques s'envoient sur les uniformisantes. On désigne par ε le caractère cyclotomique p-adique.

Si $A = \mathcal{O}_E/(\varpi_E^m)$ (pour un entier $m \geq 1$) et H est un groupe analytique p-adique compact, on note $A[\![H]\!]$ l'algèbre d'Iwasawa de H à coefficients dans A. Si M est un A-module, on note $M^\vee \overset{\text{déf}}{=} \mathrm{Hom}_A(M, A)$ le dual algébrique. Si π est une représentation lisse d'un groupe analytique p-adique sur un A-module, on commet souvent (toujours) l'abus de notation d'identifier π et son A-module sous-jacent.

On munit $A[\![X]\!][1/X]$ d'une action A-linéaire de $\mathbb{Z}_p^\times$ par $a(S(X)) \overset{\text{déf}}{=} S((1+X)^a - 1)$ et d'un endomorphisme de Frobenius A-linéaire φ par $\varphi(S(X)) \overset{\text{déf}}{=} S((1+X)^p - 1)$ qui commute à $\mathbb{Z}_p^\times$ ($a \in \mathbb{Z}_p^\times$, $S(X) \in A[\![X]\!][1/X]$). Ces actions respectent le sous-anneau $A[\![X]\!]$. On appelle (φ, Γ)-module de longueur finie un $A[\![X]\!][1/X]$-module de longueur finie D muni d'un endomorphisme $\varphi : D \to D$ tel que $\varphi(S(X)v) = \varphi(S(X))\varphi(v)$ et d'une action continue de $\Gamma \xrightarrow{\sim} \mathbb{Z}_p^\times$ (pour la topologie X-adique sur D) commutant à φ telle que $a(S(X)v) = a(S(X))a(v)$ ($S(X) \in A[\![X]\!][1/X]$, $v \in D$, $a \in \mathbb{Z}_p^\times$). On dit qu'un (φ, Γ)-module de longueur finie D est étale si l'image de φ engendre D comme $A[\![X]\!][1/X]$-module, ou de manière équivalente si l'on a un isomorphisme $\mathrm{Id} \otimes \varphi : A[\![X]\!][1/X] \otimes_{\varphi, A[\![X]\!][1/X]} D \xrightarrow{\sim} D$. La catégorie des (φ, Γ)-modules de longueur finie étales est abélienne et équivalente à la catégorie des représentations continues de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ sur un A-module de longueur finie [Fontaine 1990]. On la note $\Phi\Gamma_A^{\text{ét}}$.

2. Les $A[\![X]\!][F]$-modules de torsion sur $A[\![X]\!]$

On donne quelques définitions et résultats préliminaires sur les $A[\![X]\!][F]$-modules qui sont de torsion sur $A[\![X]\!]$.

On fixe un entier $m \geq 1$ et on pose $A \overset{\text{déf}}{=} \mathcal{O}_E/(\varpi_E^m)$. On note $A[\![X]\!][F]$ l'algèbre non commutative des polynômes en F à coefficients dans les séries formelles $A[\![X]\!]$ avec $FX = ((1+X)^p - 1)F$. Rappelons qu'un $A[\![X]\!]$-module M est de torsion si tout sous-$A[\![X]\!]$-module de type fini est de type fini sur A et qu'un $A[\![X]\!]$-module de torsion est admissible si $M[X] \overset{\text{déf}}{=} \{m \in M,\ Xm = 0\}$ est de type fini sur A (de manière équivalente $M[X^n] \overset{\text{déf}}{=} \{m \in M,\ X^n m = 0\}$ est de type fini sur A pour tout entier $n > 0$). De même un $A[F]$-module est de torsion si tout sous-$A[F]$-module de type fini est de type fini sur A. Nous ne considérons dans cet article que des $A[\![X]\!][F]$-modules M qui sont de torsion comme $A[\![X]\!]$-modules (que l'on appelle $A[\![X]\!][F]$-modules de torsion sur $A[\![X]\!]$), et parmi eux ceux vérifiant en particulier

les conditions :

$$\begin{cases} M \text{ est de type fini comme } A[\![X]\!][F]\text{-module} \\ M \text{ est admissible comme } A[\![X]\!]\text{-module.} \end{cases} \tag{1}$$

Rappelons que, $A[\![X]\!][F]$ n'étant pas noethérien, un sous-$A[\![X]\!][F]$-module d'un $A[\![X]\!][F]$-module de type fini n'est pas de type fini en général.

Lemme 2.1. (i) *Si M est un $A[\![X]\!][F]$-module de torsion sur $A[\![X]\!]$ vérifiant les conditions* (1), *alors tout $A[\![X]\!][F]$-module sous-quotient de M vérifie* (1).

(ii) *Si N est un $A[\![X]\!][F]$-module de torsion sur $A[\![X]\!]$ et $M, M' \subseteq N$ sont deux sous-$A[\![X]\!][F]$-modules vérifiant* (1), *alors $M + M'$ vérifie aussi* (1).

Démonstration. Le (ii) découle du (i) et du fait que $M \oplus M'$ vérifie (1). Le (i) découle de [Emerton 2008, Proposition 3.3] après un dévissage pour se ramener à $A = k_E$. □

Définition 2.2. On dit qu'un $A[\![X]\!][F]$-module de torsion sur $A[\![X]\!]$ satisfait la propriété Ad (pour Admissible) si tout sous-$A[\![X]\!][F]$-module de type fini est admissible comme $A[\![X]\!]$-module.

Lemme 2.3. *Soit N un $A[\![X]\!][F]$-module de torsion sur $A[\![X]\!]$ qui satisfait la propriété Ad.*

(i) *Tout $A[\![X]\!][F]$-module sous-quotient de N satisfait la propriété Ad.*

(ii) *Le $A[F]$-module N/XN est de torsion.*

Démonstration. (i) C'est clair pour un sous-$A[\![X]\!][F]$-module. Pour un $A[\![X]\!][F]$-module quotient $\overline{N}$ de N, il suffit de relever dans N des générateurs d'un sous-$A[\![X]\!][F]$-module de type fini de $\overline{N}$ et d'appliquer le (i) du lemme 2.1. Un sous-quotient étant un quotient d'un sous-objet, cela montre (i).

(ii) Soit $v \in N/XN$, il faut montrer que le sous-$A[F]$-module $A[F]v$ de N/XN engendré par v est de type fini sur A. Par un dévissage facile (notons que tout sous-$A[F]$-module de $A[F]v$ est de type fini sur $A[F]$), on peut supposer $A = k_E$. Soit $\hat{v} \in N$ qui relève v, alors le $k_E[\![X]\!][F]$-sous-module $k_E[\![X]\!][F]\hat{v}$ de N engendré par $\hat{v}$ est admissible comme $k_E[\![X]\!]$-module par hypothèse. Par [Emerton 2008, Proposition 3.5], le $k_E[F]$-module $k_E[\![X]\!][F]\hat{v}/Xk_E[\![X]\!][F]\hat{v}$ est de torsion. Comme on a une surjection $k_E[F]$-linéaire $k_E[\![X]\!][F]\hat{v}/Xk_E[\![X]\!][F]\hat{v} \twoheadrightarrow k_E[F]v$, il en est de même du $k_E[F]$-module $k_E[F]v$. □

Notons qu'un $A[\![X]\!][F]$-module de torsion sur $A[\![X]\!]$ qui est aussi de torsion sur $A[F]$ satisfait en particulier la propriété Ad (puisque tout sous-$A[\![X]\!][F]$-module de type fini est dans ce cas de type fini sur A).

Lemme 2.4. *Soit $0 \to M' \to M \to M''$ une suite exacte de $A[\![X]\!][F]$-modules de torsion sur $A[\![X]\!]$ tels que M est de type fini sur $A[\![X]\!][F]$ et M'' est admissible*

comme $A[\![X]\!]$-module. Supposons que M' satisfait la propriété Ad, alors M' est un $A[\![X]\!]$-module admissible et un $A[\![X]\!][F]$-module de type fini, et M est un $A[\![X]\!]$-module admissible.

Démonstration. Par le (i) du lemme 2.1 il suffit de montrer que M est un $A[\![X]\!]$-module admissible. Quitte à remplacer M'' par l'image de M (encore le (i) du lemme 2.1), on peut supposer que la suite est exacte à droite. Par un dévissage facile (utilisant le (i) du lemme 2.3) on se ramène au cas $A = k_E$. On a une suite exacte courte de $k_E[F]$-modules :

$$0 \to M'/(M' \cap XM) \to M/XM \to M''/XM'' \to 0.$$

Comme M'/XM' est un $k_E[F]$-module de torsion par le (ii) du lemme 2.3, il en est de même du quotient $M'/(M' \cap XM)$. Comme M'' est un $k_E[\![X]\!]$-module admissible, le $k_E[F]$-module M''/XM'' est de torsion par [Emerton 2008, Proposition 3.5]. On déduit alors de la suite exacte courte ci-dessus que M/XM est aussi un $k_E[F]$-module de torsion, et donc par [Emerton 2008, Proposition 3.5] que M est un $k_E[\![X]\!]$-module admissible. □

Lemme 2.5. *Soit $N' \to N \to N''$ une suite exacte de $A[\![X]\!][F]$-modules de torsion sur $A[\![X]\!]$.*

(*i*) *Si N' et N'' sont de torsion sur $A[F]$, alors il en est de même de N.*

(*ii*) *Si N' et N'' satisfont la propriété Ad, alors il en est de même de N.*

Démonstration. (i) est clair.

(ii) Par le (i) du lemme 2.3, on peut remplacer N' par son image dans N et donc supposer la suite exacte à gauche. Soit $M \subseteq N$ un sous $A[\![X]\!][F]$-module de type fini, M'' son image dans N'', qui est un $A[\![X]\!]$-module admissible car N'' satisfait Ad, et $M' \overset{\text{déf}}{=} M \cap N'$, qui satisfait Ad par le (i) du lemme 2.3. Alors la suite exacte $0 \to M' \to M \to M''$ vérifie les hypothèses du lemme 2.4 et donc M est un $A[\![X]\!]$-module admissible. □

Soit N un $A[\![X]\!][F]$-module de torsion sur $A[\![X]\!]$ muni d'une action A-linéaire lisse de $\mathbb{Z}_p^\times$ vérifiant ($a \in \mathbb{Z}_p^\times$, $S(X) \in A[\![X]\!]$, $n \geq 0$, $v \in N$) :

$$a(S(X)F^n(v)) = S((1+X)^a - 1)F^n(a(v)). \tag{2}$$

On note $\mathcal{M}(N)$ l'ensemble des sous-$A[\![X]\!][F]$-modules de N stables par $\mathbb{Z}_p^\times$ et vérifiant (1).

Lemme 2.6. *Si $M \in \mathcal{M}(N)$ alors $M^\vee[1/X] = \mathrm{Hom}_A(M, A)[1/X]$ est naturellement muni d'une structure d'objet de $\Phi\Gamma_A^{\text{ét}}$.*

Démonstration. Cette preuve est déjà dans [Colmez 2010] ou [Emerton 2008]. On munit $M^\vee$ d'une structure de $A[\![X]\!]$-module (à gauche) par $(S(X)f)(m) \overset{\text{déf}}{=}$

$f(S(X)m)$, d'une action de $\mathbb{Z}_p^\times$ par $(x(f))(m) \overset{\text{déf}}{=} f(x^{-1}(m))$ et d'un endomorphisme F par $F(f)(m) \overset{\text{déf}}{=} f(F(m))$ où $S(X) \in A[\![X]\!]$, $x \in \mathbb{Z}_p^\times$, $f \in M^\vee$ et $m \in M$. Noter que $M^\vee$ est un $A[\![X]\!]$-module de type fini puisque M est admissible comme $A[\![X]\!]$-module. Il faut munir $M^\vee[1/X]$ d'un Frobenius semi-linéaire φ. Soit C le conoyau de $A[\![X]\!] \otimes_{\varphi, A[\![X]\!]} M \xrightarrow{\mathrm{Id}\otimes F} M$, c'est un $A[\![X]\!]$-module de type fini (car M est un $A[\![X]\!][F]$-module de type fini) et de torsion, donc de longueur finie. On a donc $C^\vee[1/X] = 0$ d'où on déduit une injection $A[\![X]\!][1/X]$-linéaire, donc un isomorphisme, entre $A[\![X]\!][1/X]$-modules de (même) longueur finie :

$$M^\vee[1/X] \xrightarrow{\sim} (A[\![X]\!] \otimes_{\varphi, A[\![X]\!]} M)^\vee[1/X] \cong A[\![X]\!] \otimes_{\varphi, A[\![X]\!]} M^\vee[1/X] \qquad (3)$$

dont l'inverse est par définition l'application $\mathrm{Id}\otimes\varphi$ (le deuxième isomorphisme provient de l'isomorphisme $A[\![X]\!]$-linéaire $(A[\![X]\!] \otimes_{\varphi, A[\![X]\!]} M)^\vee \cong A[\![X]\!] \otimes_{\varphi, A[\![X]\!]} M^\vee$ donné par $f \mapsto \sum_{i=0}^{p-1} (1+X)^{p-1-i} \otimes f_i$ où $f_i \in M^\vee$ est défini par $f_i(v) \overset{\text{déf}}{=} f((1+X)^i \otimes v)$ pour $v \in M$). On laisse le lecteur vérifier que le $A[\![X]\!][1/X]$-module $M^\vee[1/X]$ muni de l'action induite de $\mathbb{Z}_p^\times$ et de φ est bien un (φ,Γ)-module, nécessairement étale par (3). □

Rappelons que $A[\![X]\!][1/X]$ est un anneau artinien, donc pseudo-compact lorsqu'on le munit de la topologie discrète, et qu'un $A[\![X]\!][1/X]$-module pseudo-compact est un $A[\![X]\!][1/X]$-module topologique isomorphe à une limite projective $\varprojlim_{i\in I} D_i$ de $A[\![X]\!][1/X]$-modules D_i de longueur finie (ou de manière équivalente de type fini) avec la topologie de la limite projective (et la topologie discrète sur chaque D_i) pour un ensemble d'indices I préordonné filtrant quelconque. En prenant comme morphismes les applications $A[\![X]\!][1/X]$-linéaires continues, on obtient une catégorie abélienne (voir, e.g., [Gabriel 1962, §IV.3]).

Appelons (φ,Γ)-*module pseudo-compact étale* tout $A[\![X]\!][1/X]$-module topologique D muni d'actions de $\mathbb{Z}_p^\times$ et φ tel que D est topologiquement isomorphe à une limite projective $\varprojlim_{i\in I} D_i$ comme ci-dessus où les $D_i \to D_j$ sont des morphismes dans la catégorie $\Phi\Gamma_A^{\text{ét}}$ et où l'isomorphisme est compatible aux actions de $\mathbb{Z}_p^\times$ et φ (les actions sur $\varprojlim D_i$ étant induites par celles sur chaque D_i). Le $A[\![X]\!][1/X]$-module sous-jacent à un (φ,Γ)-module pseudo-compact étale est donc en particulier pseudo-compact. En prenant comme morphismes les applications $A[\![X]\!][1/X]$-linéaires continues qui commutent à $\mathbb{Z}_p^\times$ et φ, on obtient une catégorie abélienne $\widehat{\Phi\Gamma_A^{\text{ét}}}$ avec limites projectives exactes (la preuve est comme celle de [Gabriel 1962, §IV.3, théorème 3]).

Notons Mod_A la catégorie des $A[\![X]\!][F]$-modules de torsion sur $A[\![X]\!]$ qui sont munis d'une action A-linéaire lisse de $\mathbb{Z}_p^\times$ comme en (2) (les flèches étant les applications $A[\![X]\!][F]$-linéaires commutant à $\mathbb{Z}_p^\times$). C'est une catégorie abélienne

de manière évidente. Si N est un objet de Mod_A, on pose :

$$D^\vee(N) \overset{\text{déf}}{=} \varprojlim_{M\in\mathcal{M}(N)} (M^\vee[1/X]). \tag{4}$$

En particulier $D^\vee(M) = M^\vee[1/X] \in \Phi\Gamma_A^{\text{ét}}$ si M est un objet de Mod_A dont le $A[\![X]\!][F]$-module sous-jacent vérifie (1). La proposition suivante rassemble les propriétés de $D^\vee$.

Proposition 2.7. (i) *Pour tout N dans Mod_A, $D^\vee(N)$ est un objet de $\widehat{\Phi\Gamma}_A^{\text{ét}}$ et $N \mapsto D^\vee(N)$ induit un foncteur contravariant de la catégorie Mod_A vers la catégorie $\widehat{\Phi\Gamma}_A^{\text{ét}}$.*

(ii) *Si $0 \to N' \to N \to N''$ est une suite exacte dans Mod_A alors $D^\vee(N'') \to D^\vee(N) \to D^\vee(N') \to 0$ est une suite exacte dans $\widehat{\Phi\Gamma}_A^{\text{ét}}$.*

(iii) *Si N est un objet de Mod_A de torsion comme $A[F]$-module, alors $D^\vee(N) = 0$.*

(iv) *Si $0 \to N' \to N \to N'' \to N'''$ est une suite exacte dans Mod_A, si le $A[\![X]\!][F]$-module N' satisfait la propriété Ad et si N''' est de torsion sur $A[F]$, alors $0 \to D^\vee(N'') \to D^\vee(N) \to D^\vee(N') \to 0$ est une suite exacte dans $\widehat{\Phi\Gamma}_A^{\text{ét}}$.*

Démonstration. (i) La première assertion du (i) découle du (ii) du lemme 2.1, qui montre que l'ensemble $\mathcal{M}(N)$ préordonné par l'inclusion est filtrant, et du lemme 2.6. Un morphisme $f : N' \to N$ dans Mod_A induit une application $\mathcal{M}(N') \to \mathcal{M}(N)$, $M' \mapsto f(M')$ par le (i) du lemme 2.1. En particulier on a une inclusion $\{f(M'),\ M' \in \mathcal{M}(N')\} \subseteq \mathcal{M}(N)$. De plus le morphisme $M' \to f(M')$ dans Mod_A induit par fonctorialité de $(\cdot)^\vee[1/X]$ un morphisme $D^\vee(f(M')) \to D^\vee(M')$ dans $\Phi\Gamma_A^{\text{ét}}$. On en déduit des morphismes dans $\widehat{\Phi\Gamma}_A^{\text{ét}}$ dont le premier est surjectif :

$$\varprojlim_{M\in\mathcal{M}(N)} D^\vee(M) \twoheadrightarrow \varprojlim_{M'\in\mathcal{M}(N')} D^\vee(f(M')) \longrightarrow \varprojlim_{M'\in\mathcal{M}(N')} D^\vee(M') \tag{5}$$

d'où la fonctorialité de $D^\vee$.

(ii) En remplaçant N'' par l'image de N, il suffit de traiter le cas où l'application $N \to N''$ est surjective. Si $M \in \mathcal{M}(N)$, on a $M \cap N' \in \mathcal{M}(N')$ par le (i) du lemme 2.1 et tous les éléments de $\mathcal{M}(N')$ sont de cette forme (car $\mathcal{M}(N') \subseteq \mathcal{M}(N)$). On en déduit :

$$D^\vee(N') \cong \varprojlim_{M\in\mathcal{M}(N)} D^\vee(M \cap N'). \tag{6}$$

Soit f la surjection $N \twoheadrightarrow N''$, pour tout $M \in \mathcal{M}(N)$ on a en particulier une suite exacte dans Mod_A :

$$0 \to M \cap N' \to M \to f(M) \to 0$$

d'où on déduit une suite exacte dans $\Phi\Gamma_A^{\text{ét}}$:

$$0 \to D^\vee(f(M)) \to D^\vee(M) \to D^\vee(M \cap N') \to 0.$$

puisque dans ce cas $D^\vee(\cdot)=\mathrm{Hom}_A(\cdot,A)[1/X]$ est un foncteur exact (rappelons que $A=\mathcal{O}_E/(\varpi_E^m)$). Par exactitude des limites projectives dans $\widehat{\Phi\Gamma}_A^{\text{ét}}$, on obtient encore une suite exacte dans $\widehat{\Phi\Gamma}_A^{\text{ét}}$:

$$0\to \varprojlim_{M\in\mathcal{M}(N)} D^\vee(f(M)) \longrightarrow \varprojlim_{M\in\mathcal{M}(N)} D^\vee(M) \longrightarrow \varprojlim_{M\in\mathcal{M}(N)} D^\vee(M\cap N')\to 0$$

d'où on déduit une suite exacte $D^\vee(N'')\to D^\vee(N)\to D^\vee(N')\to 0$ dans $\widehat{\Phi\Gamma}_A^{\text{ét}}$ par (6) et la surjectivité de la première flèche en (5) appliquée à $f:N\to N''$.

(iii) Tout M dans $\mathcal{M}(N)$ est alors un A-module de type fini, d'où $M^\vee[1/X]=0$ et donc $D^\vee(N)=\varprojlim D^\vee(M)=0$.

(iv) Soit f le morphisme $N\to N''$, on a deux suites exactes $0\to N'\to N\to f(N)\to 0$ et $0\to f(N)\to N''\to N'''$ dans Mod_A. Par (ii) appliqué à $0\to f(N)\to N''\to N'''$ et (iii), on en déduit un isomorphisme $D^\vee(N'')\xrightarrow{\sim} D^\vee(f(N))$ dans $\widehat{\Phi\Gamma}_A^{\text{ét}}$. Il suffit donc de montrer l'énoncé (iv) en supposant $N'''=0$, i.e., en supposant f surjectif. En procédant comme dans la preuve du (ii), on a une injection :

$$\varprojlim_{M\in\mathcal{M}(N)} D^\vee(f(M)) \hookrightarrow \varprojlim_{M\in\mathcal{M}(N)} D^\vee(M)=D^\vee(N). \tag{7}$$

Soit $M\in\mathcal{M}(N'')$ et $\widehat{M}\subseteq N$ un sous-$A[\![X]\!][F]$-module de type fini stable par $\mathbb{Z}_p^\times$ relevant M (il en existe car f est surjectif, M est de type fini sur $A[\![X]\!][F]$ et l'action de $\mathbb{Z}_p^\times$ est lisse). On a une suite exacte $0\to\widehat{M}\cap N'\to\widehat{M}\to M\to 0$ où M est admissible comme $A[\![X]\!]$-module (par définition) et où $\widehat{M}\cap N'$ satisfait Ad (car N' satisfait Ad). Par le lemme 2.4, $\widehat{M}$ est admissible comme $A[\![X]\!]$-module, donc est dans $\mathcal{M}(N)$. Ainsi l'application $\mathcal{M}(N)\to\mathcal{M}(N'')$ induite par f est surjective ce qui implique $\{f(M),\ M\in\mathcal{M}(N)\}=\mathcal{M}(N'')$ et donc un isomorphisme dans $\widehat{\Phi\Gamma}_A^{\text{ét}}$:

$$D^\vee(N'')=\varprojlim_{M\in\mathcal{M}(N'')} D^\vee(M)\xrightarrow{\sim}\varprojlim_{M\in\mathcal{M}(N)} D^\vee(f(M)). \tag{8}$$

En combinant (7) et (8), on voit que la flèche $D^\vee(N'')\to D^\vee(N)$ est injective, ce qui par (ii) achève la preuve. □

Si $N'\to N\to N''\to N'''$ est une suite exacte dans Mod_A et si N' et N''' sont de torsion sur $A[F]$, on déduit aussi du (iii) et du (iv) de la proposition 2.7 un isomorphisme $D^\vee(N'')\xrightarrow{\sim} D^\vee(N)$ dans $\widehat{\Phi\Gamma}_A^{\text{ét}}$.

3. Un foncteur vers les (pro-)(φ,Γ)-modules

On définit un foncteur contravariant de la catégorie des représentations lisses du Borel vers la catégorie $\widehat{\Phi\Gamma}_A^{\text{ét}}$.

On conserve les notations du § 2. On fixe pour toute la suite (G, B, T) où G est un groupe algébrique réductif connexe déployé sur L, $B \subset G$ est un sous-groupe de Borel (défini sur L) et $T \subset B$ un tore maximal (déployé sur L). On note N le radical unipotent de B. On note $X(T) \overset{\text{déf}}{=} \mathrm{Hom}_{\mathrm{gr}}(T, \mathbb{G}_{\mathrm{m}})$ le groupe des caractères algébriques de T, $X^\vee(T) \overset{\text{déf}}{=} \mathrm{Hom}_{\mathrm{gr}}(\mathbb{G}_{\mathrm{m}}, T) \cong \mathrm{Hom}_{\mathbb{Z}}(X(T), \mathbb{Z})$ le groupe des cocaractères, $(X(T), R, X^\vee(T), R^\vee)$ la donnée radicielle de (G, T), $R^+ \subset X(T)$ les racines positives relativement à B, $S \subset R^+$ les racines simples et $R^{\vee +}$, $S^\vee$ les coracines correspondantes. Pour $\alpha \in R^+$, on note $N_\alpha \subseteq N$ le sous-groupe radiciel (commutatif) associé et, pour $\alpha \in S$, on fixe un isomorphisme $\iota_\alpha : N_\alpha \xrightarrow{\sim} \mathbb{G}_{\mathrm{a}}$ de groupes algébriques sur L tel que (cf. [Jantzen 2003, §II.1.2]) :

$$\iota_\alpha(t n_\alpha t^{-1}) = \alpha(t)\iota_\alpha(n_\alpha) \quad \forall\, t \in T, \quad \forall\, n_\alpha \in N_\alpha. \tag{9}$$

L'application produit donne un isomorphisme de variétés algébriques sur L (pour un ordre quelconque des α) $\prod_{\alpha \in R^+} N_\alpha \xrightarrow{\sim} N$. L'isomorphisme inverse composé avec la projection sur $\prod_{\alpha \in S} N_\alpha$, vu comme groupe produit commutatif, induit une surjection $N \twoheadrightarrow \prod_{\alpha \in S} N_\alpha$ de groupes algébriques sur L. Comme dans [Schneider et Vignéras 2011, §5] on note ℓ la composée :

$$N \twoheadrightarrow \prod_{\alpha \in S} N_\alpha \xrightarrow{\sum_{\alpha \in S} \iota_\alpha} \mathbb{G}_{\mathrm{a}},$$

qui est un morphisme de groupes algébriques sur L.

On suppose désormais que le centre Z_G de G est connexe. Par [Breuil et Herzig 2015, Proposition 2.1.1] (par exemple), il existe un cocaractère $\xi \in X^\vee(T)$ tel que $\alpha \circ \xi = \mathrm{Id}_{\mathbb{G}_{\mathrm{m}}}$ pour toute racine simple α (prendre $\xi = \sum_{\alpha^\vee \in S^\vee} \lambda_{\alpha^\vee}$ où les $\lambda_{\alpha^\vee}$ sont des cocaractères fondamentaux). Un tel cocaractère n'est pas unique mais tout autre est de la forme $\xi + \zeta$ (en notation additive) où $\zeta \in X^\vee(Z_G) \subseteq X^\vee(T)$. *On fixe un tel cocaractère ξ dans la suite.* Si $n = \prod_{\alpha \in R^+} n_\alpha \in N$ et $x \in \mathbb{G}_{\mathrm{m}}$, on a :

$$\begin{aligned} \ell\big(\xi(x) n \xi(x^{-1})\big) &= \ell\Big(\prod_{\alpha \in R^+} \xi(x) n_\alpha \xi(x^{-1})\Big) \\ &= \sum_{\alpha \in S} \iota_\alpha\big(\xi(x) n_\alpha \xi(x^{-1})\big) = \sum_{\alpha \in S} \alpha(\xi(x))\iota_\alpha(n_\alpha) = x\ell(n). \end{aligned} \tag{10}$$

On fixe un sous-groupe ouvert compact $N_0 \subset N(L)$ que l'on suppose *totalement décomposé* comme dans [Schneider et Vignéras 2011], c'est-à-dire tel que $\prod_{\alpha \in R^+} N_\alpha \xrightarrow{\sim} N$ induit une bijection $\prod_{\alpha \in R^+} N_\alpha(L) \cap N_0 \xrightarrow{\sim} N_0$ pour tout ordre sur les $\alpha \in R^+$. Le morphisme ℓ induit un morphisme de groupes encore noté $\ell : N_0 \to L$ et on définit :

$$N_1 \overset{\text{déf}}{=} \mathrm{Ker}(N_0 \xrightarrow{\ell} L \xrightarrow{\mathrm{Tr}_{L/\mathbb{Q}_p}} \mathbb{Q}_p) \tag{11}$$

qui est un sous-groupe compact distingué de N_0. Lorsque $N \neq 0$, i.e., lorsque $G \neq T$, le groupe N_0/N_1 s'identifie à un sous-$\mathbb{Z}_p$-module (libre de rang 1) de $\mathbb{Q}_p$, et donc est isomorphe à $\mathbb{Z}_p$.

Lemme 3.1. *On a* :

$$\xi(\mathbb{Z}_p\backslash\{0\}) \subseteq \{t \in T(L),\ tN_0t^{-1} \subseteq N_0\}$$

et :

$$\xi(\mathbb{Z}_p\backslash\{0\}) \subseteq \{t \in T(L),\ tN_1t^{-1} \subseteq N_1\}.$$

Démonstration. La première inclusion découle de (9), de l'égalité $\alpha(\xi(x)) = x$ et du fait que N_0 est totalement décomposé. La deuxième découle de la première, de (10) et du fait que la trace est $\mathbb{Z}_p$-linéaire. □

Soit π une représentation lisse de $B(L)$ sur un A-module. De manière analogue à [Emerton 2010, Definition 3.1.3], on munit le $A[\![N_0/N_1]\!]$-module π^{N_1} d'une action (de Hecke) A-linéaire du monoïde $\mathbb{Z}_p\backslash\{0\}$ comme suit :

$$x \cdot_\xi v \overset{\text{déf}}{=} \sum_{n_1 \in N_1/\xi(x)N_1\xi(x^{-1})} n_1\xi(x)v \quad \in \pi^{N_1}, \tag{12}$$

l'indice ξ rappelant que cela dépend du choix du cocaractère ξ (notons que cela a bien un sens par le lemme 3.1). Cette action est $A[\![N_0/N_1]\!]$-semi-linéaire car on vérifie que l'on a :

$$x \cdot_\xi \left(\sum_i a_i[n_i]\right)v = \left(\sum_i a_i[\xi(x)n_i\xi(x^{-1})]\right)(x \cdot_\xi v)$$

pour $x \in \mathbb{Z}_p\backslash\{0\}$, $\sum_i a_i[n_i] \in A[\![N_0/N_1]\!]$ et $v \in \pi^{N_1}$. Si $x \in \mathbb{Z}_p^\times$, (12) donne simplement $x \cdot_\xi v = \xi(x)v$.

On fixe un isomorphisme $N_0/N_1 \cong \mathbb{Z}_p$ lorsque $G \neq T$. En envoyant F sur l'endomorphisme (12) pour $x = p \in \mathbb{Z}_p\backslash\{0\}$, en faisant agir $A[\![X]\!]$ via $A[\![X]\!]/(X)$ si $G = T$, via l'isomorphisme $A[\![X]\!] \cong A[\![\mathbb{Z}_p]\!] \cong A[\![N_0/N_1]\!]$ envoyant X sur $[1]-1$ si $G \neq T$, et en faisant agir $\mathbb{Z}_p^\times$ via (12), on vérifie avec (10) que l'on munit π^{N_1} d'une structure de $A[\![X]\!][F]$-module avec action lisse de $\mathbb{Z}_p^\times$ qui en fait un objet de la catégorie Mod_A (cf. § 2, cette structure dépend donc du choix de ξ). On dispose donc de l'ensemble $\mathcal{M}(\pi^{N_1})$ des sous-$A[\![X]\!][F]$-modules M de π^{N_1} stables par $\mathbb{Z}_p^\times$ et vérifiant (1). Lorsque $G = T$ (ou de manière équivalente $B = T$), X agit par 0, et $\mathcal{M}(\pi^{N_1}) = \mathcal{M}(\pi)$ est l'ensemble des sous-A-modules de type fini de π stables par l'action de $\xi(\mathbb{Q}_p^\times)$, ou de manière équivalente de $\xi(\mathbb{Z}_p\backslash\{0\})$. Lorsque $G \neq T$, l'ensemble $\mathcal{M}(\pi^{N_1})$ est mystérieux en général (par exemple on ignore s'il est non vide), voir la remarque 3.3.

Supposons d'abord $G \neq T$. Si $M \in \mathcal{M}(\pi^{N_1})$, rappelons que $D^\vee(M) = M^\vee[1/X]$ muni de sa structure d'objet de $\Phi\Gamma_A^{\text{ét}}$ (lemme 2.6).

Supposons ensuite $G = T$. Si $M \in \mathcal{M}(\pi^{N_1}) = \mathcal{M}(\pi)$, l'action de $\mathbb{Q}_p^\times$ via ξ sur M se factorise par un quotient fini (car M est de cardinal fini) et en particulier s'étend par continuité via la réciprocité locale en une action continue de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. On note $D^\vee(M)$ le (φ, Γ)-module de la représentation *duale* de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ (via le foncteur covariant de [Fontaine 1990, théorème A.3.4.3]), c'est-à-dire par le lemme 7.5 ci-dessous $D^\vee(M) = A[\![X]\!][1/X] \otimes_A M^\vee$ où l'action de $\Gamma \cong \mathbb{Z}_p^\times$ est l'unique action $A[\![X]\!][1/X]$-semi-linéaire telle que $x(f)(m) = f(\xi(x^{-1})(m))$ et φ est l'unique endomorphisme $A[\![X]\!][1/X]$-semi-linéaire tel que $\varphi(f)(m) = f(\xi(p^{-1})(m))$ avec $f \in M^\vee$, $x \in \mathbb{Z}_p^\times$ et $m \in M$. Notons que dans ce cas $D^\vee(M)$ *n'*est *pas* $M^\vee[1/X]$ (qui est nul).

Pour toute représentation lisse π de $B(L)$ sur un A-module, on pose :

$$D_\xi^\vee(\pi) \overset{\text{déf}}{=} \varprojlim_{M \in \mathcal{M}(\pi^{N_1})} D^\vee(M) \;\cong\; \varprojlim_{M \in \mathcal{M}(\pi^{N_1})} (M^\vee[1/X]), \tag{13}$$

autrement dit $D_\xi^\vee(\pi) = D^\vee(\pi^{N_1})$ si $G \neq T$ avec les notations de (4).

Proposition 3.2. (i) *Pour tout π, $D_\xi^\vee(\pi)$ est un objet de $\widehat{\Phi\Gamma}_A^{\text{ét}}$ et $\pi \mapsto D_\xi^\vee(\pi)$ induit un foncteur contravariant de la catégorie des représentations lisses de $B(L)$ sur A vers la catégorie $\widehat{\Phi\Gamma}_A^{\text{ét}}$.*

(ii) *Si $0 \to \pi' \to \pi \to \pi''$ est une suite exacte de représentations lisses de $B(L)$ sur A, alors $D_\xi^\vee(\pi'') \to D_\xi^\vee(\pi) \to D_\xi^\vee(\pi') \to 0$ est une suite exacte dans $\widehat{\Phi\Gamma}_A^{\text{ét}}$.*

(iii) *Lorsque $G(L) = \mathrm{GL}_2(\mathbb{Q}_p)$ et π est la restriction à $B(\mathbb{Q}_p)$ d'une représentation de longueur finie de $\mathrm{GL}_2(\mathbb{Q}_p)$ sur A, le foncteur $D_\xi^\vee$ coïncide (à torsion près) avec le foncteur défini dans [Colmez 2010].*

Démonstration. (i) Clair par le (i) de la proposition 2.7.

(ii) Cela découle du (ii) de la proposition 2.7 appliqué à la suite exacte dans Mod_A : $0 \to \pi'^{N_1} \to \pi^{N_1} \to \pi''^{N_1}$.

(iii) Nous utilisons certains résultats de [Emerton 2008] qui ne sont écrits là que pour $A = \mathcal{O}_E/(\varpi_E)$ mais dont les preuves s'étendent directement à $A = \mathcal{O}_E/(\varpi_E^n)$ (voir aussi [Colmez 2010; Berger et Vienney 2014]). Lorsque π est la restriction à $B(\mathbb{Q}_p)$ d'une représentation admissible de $\mathrm{GL}_2(\mathbb{Q}_p)$ sur A, alors π satisfait la propriété Ad (définition 2.2). En effet, un sous-$A[\![X]\!][F]$-module de type fini de π est toujours contenu dans un des modules de type fini $M(V, V_0)$ de [Emerton 2008, Definition 4.1] qui est admissible par [loc. cit., Theorem 4.7]. Par ailleurs si $M \in \mathcal{M}(\pi)$ contient un sous-A-module de type fini stable par $\mathrm{GL}_2(\mathbb{Z}_p)\mathbb{Q}_p^\times$ qui engendre π sous $\mathrm{GL}_2(\mathbb{Q}_p)$, alors le (φ, Γ)-module $D^\vee(M)$ ne dépend plus de M (voir [loc. cit., preuve de la Prop. 4.4 et Rem. 4.8]). Lorsque π est de longueur finie comme représentation de $\mathrm{GL}_2(\mathbb{Q}_p)$, donc en particulier de type fini et admissible,

ceci est toujours vérifié pour un sous-$A[\![X]\!][F]$-module de type fini de π stable par $\mathbb{Z}_p^\times$ assez grand. On en déduit $D_\xi^\vee(\pi) = D^\vee(M) \in \Phi\Gamma_A^{\text{ét}}$, d'où le résultat. □

Remarque 3.3. Comme rien, ou presque, n'est connu sur $\mathcal{M}(\pi^{N_1})$ en dehors du cas $\mathrm{GL}_2(\mathbb{Q}_p)$, j'ignore en général si $D_\xi^\vee(\pi)$ est non nul ou s'il est de longueur finie (i.e., dans $\Phi\Gamma_A^{\text{ét}}$). Notons que Schraen montre dans [Schraen 2012–14], par un calcul explicite faisant intervenir certains des diagrammes de [Breuil et Paškūnas 2012, §13], que, au moins lorsque L est l'extension quadratique non ramifiée de $\mathbb{Q}_p$, alors $D_\xi^\vee(\pi)$ est non nul pour les représentations supersingulières de $\mathrm{GL}_2(L)$ sur k_E qui apparaissent dans [Breuil et Paškūnas 2012, Theorem 19.10]. Ces calculs sont étendus par Morra et Schraen dans [Morra et Schraen ≥ 2015] à des cas où L est non ramifiée de degré 3. Rappelons les deux questions naturelles qui se posent sur $\mathcal{M}(\pi^{N_1})$ lorsque, disons, π est une représentation lisse admissible de $G(L)$ sur A de longueur finie (comme représentation de $G(L)$) :

(1) Est-ce que $\mathcal{M}(\pi^{N_1})$ coïncide avec l'ensemble des sous-$A[\![X]\!][F]$-modules de type fini de π^{N_1} stables par $\mathbb{Z}_p^\times$ (de manière équivalente puisque l'action de $\mathbb{Z}_p^\times$ est lisse : est-ce que le $A[\![X]\!][F]$-module π^{N_1} satisfait la propriété Ad) ?

(2) Est-ce que $D_\xi^\vee(\pi) \in \Phi\Gamma_A^{\text{ét}}$ (de manière équivalente puisque les objets de $\Phi\Gamma_A^{\text{ét}}$ sont de longueur finie : est-ce que $D^\vee(M)$ se "stabilise" pour $M \in \mathcal{M}(\pi^{N_1})$ assez grand) ?

Pour π représentation lisse de $B(L)$ sur A, on peut par ailleurs aussi considérer les groupes de cohomologie continue $H^i(N_1, \pi)$ pour $i \geq 1$. Ils sont nuls si $G = T$ (puisque N_1 est nul), mais si $G \neq T$ ils sont naturellement munis d'une structure d'objet de Mod_A via l'isomorphisme $A[\![X]\!] \cong A[\![N_0/N_1]\!]$ où l'action de N_0 (qui se factorise par N_0/N_1) est induite par l'application $\phi \to n_0(\phi)$ envoyant une cochaîne continue $\phi : N_1^i \to \pi$ sur la cochaîne $n_0(\phi)(\cdot) \overset{\text{déf}}{=} n_0(\phi(n_0^{-1} \cdot n_0))$ et où l'action de $\xi(x)$ pour $x \in \mathbb{Z}_p \backslash \{0\}$ (donnant l'action de $F = \xi(p)$ et de $\mathbb{Z}_p^\times$) est la composée :

$$H^i(N_1, \pi) \xrightarrow{\xi(x)} H^i(\xi(x) N_1 \xi(x^{-1}), \pi) \longrightarrow H^i(N_1, \pi) \tag{14}$$

la première flèche étant induite par l'action de $\xi(x)$ sur π et la deuxième étant la corestriction de $\xi(x) N_1 \xi(x^{-1})$ à N_1 (voir, e.g., [Hauseux 2014, §3.1], noter que cette deuxième flèche est l'identité si $x \in \mathbb{Z}_p^\times$). On dispose donc pour tout $i \geq 1$ de foncteurs contravariants $\pi \longmapsto D^\vee(H^i(N_1, \pi))$ de la catégorie des représentations lisses de $B(L)$ sur A vers la catégorie $\widehat{\Phi\Gamma}_A^{\text{ét}}$.

Remarque 3.4. La catégorie des représentations lisses de $B(L)$ sur A ayant assez d'injectifs, on peut aussi considérer les foncteurs dérivés $R^i D_\xi^\vee$ du foncteur contravariant exact à droite $D_\xi^\vee$. La question du lien éventuel entre les foncteurs $D^\vee(H^i(N_1, \pi))$ et $R^i D_\xi^\vee$ n'est pas abordée dans cet article.

Lorsque π est une représentation lisse de $G(L)$ sur A, on commet dans la suite l'abus de notation $D_\xi^\vee(\pi) = D_\xi^\vee(\pi|_{B(L)})$.

4. Indépendance des choix

On montre que le foncteur $D_\xi^\vee$ dépend seulement du choix de ξ.

On conserve les notations des sections précédentes.

Si $G = T$, il n'y a que le choix de ξ qui intervient, on suppose donc $G \neq T$.

Soit π une représentation lisse de $B(L)$ sur A. Nous allons montrer que $D_\xi^\vee(\pi)$ en tant qu'objet de $\widehat{\Phi\Gamma}_A^{\text{ét}}$ ne dépend pas des choix des $(\iota_\alpha)_{\alpha\in S}$ satisfaisant (9), du sous-groupe ouvert compact $N_0 \subseteq N(L)$ totalement décomposé et de l'isomorphisme $N_0/N_1 \cong \mathbb{Z}_p$, et ce de manière fonctorielle en π. Rappelons que $(\iota_\alpha)_{\alpha\in S}$ et N_0 déterminent N_1 par (11).

Notons déjà que, à $(\iota_\alpha)_{\alpha\in S}$ et N_0 fixés, comme tout automorphisme de $\mathbb{Z}_p$-module de $\mathbb{Z}_p$ est de la forme $x \mapsto ax$ pour $a \in \mathbb{Z}_p^\times$, c'est un exercice trivial (laissé au lecteur) que l'objet π^{N_1} de Mod_A, et donc *a fortiori* $D_\xi^\vee(\pi)$, ne dépendent pas de l'isomorphisme choisi $N_0/N_1 \cong \mathbb{Z}_p$. On ne se préoccupe donc plus du choix d'un tel isomorphisme dans la suite.

Fixons $(\iota_\alpha)_{\alpha\in S}$ et soit N_0, N_0' deux sous-groupes ouverts compacts de $N(L)$ totalement décomposés. Notons $s : N_0 \twoheadrightarrow \mathbb{Z}_p$ la surjection induite par l'isomorphisme fixé $N_0/N_1 \cong \mathbb{Z}_p$. Quitte à remplacer N_0' par $N_0 \cap N_0'$ (encore totalement décomposé), on peut supposer $N_0' \subseteq N_0$. On note m l'entier ≥ 0 tel que $s(N_0') = p^m\mathbb{Z}_p$. On a $N_0' \subseteq N_0'' \subseteq N_0$ où $N_0'' \overset{\text{déf}}{=} s^{-1}(p^m\mathbb{Z}_p)$ et il suffit de passer de N_0 à N_0'', puis de N_0'' à N_0'. Autrement dit, en remarquant que $N_1 = \mathrm{Ker}(s : N_0'' \twoheadrightarrow p^m\mathbb{Z}_p)$ et en posant $N_1' \overset{\text{déf}}{=} \mathrm{Ker}(s : N_0' \twoheadrightarrow p^m\mathbb{Z}_p)$, il suffit de traiter les deux cas suivants : le cas $N_1' = N_1$ (mais $m \geq 0$), le cas $m = 0$ (mais $N_1' \subseteq N_1$).

Commençons par le cas $m = 0$.

Lemme 4.1. *L'application* :

$$j_{N_1',N_1} : \pi^{N_1'} \to \pi^{N_1}, \quad v \mapsto \sum_{n_1 \in N_1/N_1'} n_1 v \tag{15}$$

est un morphisme dans Mod_A.

Démonstration. Comme l'inclusion $N_0' \subseteq N_0$ induit $N_0'/N_1' \xrightarrow{\sim} N_0/N_1$ (car $m = 0$), il suffit de vérifier la commutation de j_{N_1',N_1} à l'action de N_0' pour avoir sa commutation à l'action de $A[\![X]\!]$. Cette commutation est claire car, si $(n_{1,i})_{i\in I}$ est un système de représentants de N_1/N_1' dans N_1, alors $({n_0'}^{-1} n_{1,i} n_0')_{i\in I}$ en est un autre pour tout $n_0' \in N_0'$ puisque N_1' est distingué dans N_0'. La commutativité à l'action de $\xi(\mathbb{Z}_p^\times)$ est aussi claire puisque $(\xi(x)^{-1} n_{1,i} \xi(x))_{i\in I}$ est un système de représentants de N_1/N_1' dans N_1 pour tout $x \in \mathbb{Z}_p^\times$. Rappelons que, si $G'' \subseteq G' \subseteq G$ sont trois groupes et si $(g_{i'}')_{i'\in I'}$, $(g_i)_{i\in I}$ sont des systèmes de représentants respectivement

dans G' et dans G de G'/G'' et de G/G', alors $(g_i g'_{i'})_{(i,i')\in I\times I'}$ est un système de représentants dans G de G/G''. En appliquant cela à $\xi(p)N'_1\xi(p^{-1}) \subseteq N'_1 \subseteq N_1$ et $\xi(p)N'_1\xi(p^{-1}) \subseteq \xi(p)N_1\xi(p^{-1}) \subseteq N_1$, on obtient :

$$(j_{N'_1,N_1} \circ F)(v) = (F \circ j_{N'_1,N_1})(v) = \sum_{n_1\in N_1/\xi(p)N'_1\xi(p^{-1})} n_1\xi(p)v,$$

qui donne la commutativité à l'action de F. □

Lemme 4.2. (i) *Soit* $M' \in \mathcal{M}(\pi^{N'_1})$ *et* $M \overset{\text{déf}}{=} j_{N'_1,N_1}(M') \in \mathcal{M}(\pi^{N_1})$ *son image par* $j_{N'_1,N_1}$. *Alors* $\mathrm{Ker}(M' \to M)$ *est un* $A[F]$*-module de torsion.*

(ii) *Soit* $M \in \mathcal{M}(\pi^{N_1})$, *alors il existe* $M' \in \mathcal{M}(\pi^{N'_1})$ *tel que l'on a une suite exacte dans* Mod_A :

$$0 \longrightarrow M'' \longrightarrow M' \xrightarrow{j_{N'_1,N_1}} M \longrightarrow M/M' \longrightarrow 0$$

avec M'' *et* M/M' *de torsion comme* $A[F]$*-modules.*

Démonstration. (i) Notons d'abord que M est dans $\mathcal{M}(\pi^{N_1})$ par le lemme 4.1 et le (i) du lemme 2.1. Soit $d \geq 0$ tel que $\xi(p^d)N_0\xi(p^{-d}) \subseteq N'_0$ (un tel entier d existe car $\xi(p^d)N_\alpha(L) \cap N_0\xi(p^{-d}) = \alpha(\xi(p^d))N_\alpha(L) \cap N_0 \subseteq p^d N_\alpha(L) \cap N_0$ pour tout $\alpha \in R^+$, en voyant $N_\alpha(L) \cap N_0$ comme $\mathbb{Z}_p$-module). On a donc $\xi(p^d)N'_1\xi(p^{-d}) \subseteq \xi(p^d)N_1\xi(p^{-d}) \subseteq N'_1$ d'où on déduit de manière similaire à la fin de la preuve du lemme 4.1 que l'endomorphisme de $\pi^{N'_1}$:

$$F^d = F \circ \cdots \circ F \ = \sum_{n'_1\in N'_1/\xi(p^d)N'_1\xi(p^{-d})} n'_1\xi(p^d)$$

se factorise comme suit :

$$\pi^{N'_1} \xrightarrow{j_{N'_1,N_1}} \pi^{N_1} \xrightarrow{\phi_{N'_1,N_1}} \pi^{N'_1}$$

où $\phi_{N'_1,N_1}$ envoie $v \in \pi^{N_1}$ sur $\sum_{n'_1\in N'_1/\xi(p^d)N_1\xi(p^{-d})} n'_1\xi(p^d)v \in \pi^{N'_1}$. En particulier $\mathrm{Ker}(j_{N'_1,N_1} : M' \to M) \subseteq \mathrm{Ker}(F^d : M' \to M')$ est un $A[F]$-module de torsion.

(ii) Comme dans la preuve du (i) mais en considérant cette fois $\xi(p^d)N_1\xi(p^{-d}) \subseteq N'_1 \subseteq N_1$ on en déduit que l'endomorphisme F^d de π^{N_1} se factorise par :

$$\pi^{N_1} \xrightarrow{\phi_{N'_1,N_1}} \pi^{N'_1} \xrightarrow{j_{N'_1,N_1}} \pi^{N_1}. \tag{16}$$

Noter que $\phi_{N'_1,N_1}$ commute à F (comme à la fin de la preuve du lemme 4.1, considérer $\xi(p^{d+1})N_1\xi(p^{-d-1}) \subseteq \xi(p^d)N_1\xi(p^{-d}) \subseteq N'_1$ et $\xi(p^{d+1})N_1\xi(p^{-d-1}) \subseteq \xi(p)N'_1\xi(p^{-1}) \subseteq N'_1$) et est φ^d-semi-linéaire (pour le Frobenius φ sur $A[\![X]\!]$). On en déduit que le sous-$A[\![X]\!]$-module M' de $\pi^{N'_1}$ engendré par $\phi_{N'_1,N_1}(M)$ est un $A[\![X]\!][F]$-module de type fini et que l'on a une surjection $A[\![X]\!]$-linéaire :

$$\mathrm{Id} \otimes \phi_{N'_1,N_1} : A[\![X]\!] \otimes_{\varphi^d, A[\![X]\!]} M \twoheadrightarrow M'.$$

Comme $A[\![X]\!]\otimes_{\varphi^d,A[\![X]\!]}M$ est un $A[\![X]\!]$-module admissible (car $(A[\![X]\!]\otimes_{\varphi^d,A[\![X]\!]}M)^\vee\cong A[\![X]\!]\otimes_{\varphi^d,A[\![X]\!]}M^\vee$), on en déduit que M' est admissible comme $A[\![X]\!]$-module, donc est dans $\mathcal{M}(\pi^{N_1'})$. On déduit aussi de la factorisation (16) et du fait que j_{N_1',N_1} est $A[\![X]\!]$-linéaire que l'on a $F^d(M)\subseteq j_{N_1',N_1}(M')\subseteq M$, et donc que $M/j_{N_1',N_1}(M')$ est annulé par F^d. Le fait que $M''=\mathrm{Ker}(j_{N_1',N_1}:M'\to M)$ est de $A[F]$-torsion résulte du (i). □

On déduit facilement du lemme 4.2 et du commentaire qui suit la proposition 2.7 que j_{N_1',N_1} induit un isomorphisme dans $\widehat{\Phi\Gamma}_A^{\text{ét}}$:

$$\varprojlim_{M\in\mathcal{M}(\pi^{N_1})} D^\vee(M)\xrightarrow{\sim}\varprojlim_{M'\in\mathcal{M}(\pi^{N_1'})} D^\vee(M')$$

qui est clairement fonctoriel en π.

Considérons maintenant le cas $N_1'=N_1$, qui implique $N_0'=s^{-1}(p^m\mathbb{Z}_p)$. On a une suite exacte par (10) :

$$\begin{array}{ccccccccc}
0 & \longrightarrow & N_1 & \longrightarrow & N_0' & \xrightarrow{s} & p^m\mathbb{Z}_p & \longrightarrow & 0\\
 & & \uparrow & & \uparrow & & \| & & \\
0 & \longrightarrow & \xi(p^m)N_1\xi(p^{-m}) & \longrightarrow & \xi(p^m)N_0\xi(p^{-m}) & \xrightarrow{s} & p^m\mathbb{Z}_p & \longrightarrow & 0
\end{array}$$

où les flèches verticales sont des inclusions. Par le cas $m=0$, on sait que N_0' et $\xi(p^m)N_0\xi(p^{-m})$ donnent le même foncteur $D_\xi^\vee$. On est donc ramené à comparer les foncteurs pour N_0 et $\xi(p^m)N_0\xi(p^{-m})$. Il suffit de vérifier que π^{N_1} et $\pi^{\xi(p^m)N_1\xi(p^{-m})}$ (ce dernier avec l'action induite de $\xi(p^m)N_0\xi(p^{-m})$) sont isomorphes de manière fonctorielle dans Mod_A. Le lecteur pourra vérifier que l'application :

$$\pi^{N_1}\to\pi^{\xi(p^m)N_1\xi(p^{-m})},\quad v\mapsto\xi(p^m)v$$

induit bien un tel isomorphisme.

Fixons maintenant N_0 et soit $(\iota_\alpha)_{\alpha\in S}$, $(\iota'_\alpha)_{\alpha\in S}$ satisfaisant (9). Soit ℓ, ℓ' comme au § 3 (avec des notations évidentes) et $N_1'\subset N_0$ le sous-groupe défini par (11) avec ℓ' au lieu de ℓ. Par le même argument que [Schneider et Vignéras 2011, §7, p. 27], il existe $t\in T(L)$ tel que $\ell'=\ell(t^{-1}\cdot t)$. Par ce que l'on a démontré ci-dessus, on obtient le même foncteur si l'on travaille avec N_0 et $(\iota'_\alpha)_{\alpha\in S}$ ou avec tN_0t^{-1} et $(\iota'_\alpha)_{\alpha\in S}$. Il suffit donc de montrer que les $D_\xi^\vee$ obtenus avec N_0 et $(\iota_\alpha)_{\alpha\in S}$ d'une part, tN_0t^{-1} et $(\iota'_\alpha)_{\alpha\in S}$ d'autre part sont les mêmes. Pour cela il suffit de montrer que π^{N_1} et $\pi^{tN_1t^{-1}}$ (ce dernier avec l'action induite de tN_0t^{-1}) sont isomorphes (de manière fonctorielle) dans Mod_A. Comme précédemment, l'application $(\pi^{N_1}\to\pi^{tN_1t^{-1}}$, $v\mapsto tv)$ induit un tel isomorphisme.

Remarque 4.3. Soit ξ' un autre choix de cocaractère, il existe $\zeta:\mathbb{G}_{\mathrm{m}}\to Z_G$ tel que $\xi'(x)=\zeta(x)\xi(x)$ pour $x\in L^\times$ (voir § 3). Lorsque $Z_G(L)$ agit sur π par un

caractère $\chi_\pi : Z_G(L) \to A^\times$ (ce qui est le cas dans la plupart des applications), on laisse le lecteur vérifier en utilisant le lemme 7.5 ci-dessous que $D_{\xi'}^\vee(\pi)$ est isomorphe à $D_\xi^\vee(\pi)$ tordu par le (φ, Γ)-module de l'inverse du caractère lisse :

$$\chi_\pi \circ \zeta : \mathbb{Q}_p^\times \to A^\times$$

(via la réciprocité locale).

5. Compatibilité au produit tensoriel

On montre une compatibilité au produit tensoriel du foncteur $D_\xi^\vee$.
On conserve les notations des §§2 et 3.

Lemme 5.1. *Soit M un $k_E[\![X]\!][F]$-module de torsion sur $k_E[\![X]\!]$. On suppose* :

(i) $M^\vee \cong k_E[\![X]\!]^d$ *pour $d > 0$ comme $k_E[\![X]\!]$-module* ;

(ii) *il existe une suite d'entiers positifs $(N_n)_{n>0}$ croissante et non bornée telle que, pour tout $n > 0$, il existe $v_n \in M[X^{N_n}] \backslash M[X^{N_n - 1}]$ avec $F(v_n) \in M[X^{N_n}]$.*

Alors il existe un sous-$k_E[\![X]\!]$-module admissible $M' \subseteq M$ tel que $M'^\vee \cong k_E[\![X]\!]$ et $F(m') = 0$ pour tout $m' \in M'$.

Démonstration. Par la dualité modules compacts - modules discrets [Gabriel 1962, §IV.4] l'hypothèse (i) est équivalente à :

$$M \cong \left(\varinjlim_n k_E[X]/(X^n)\right)^d \cong (k_E[\![X]\!][1/X]/k_E[\![X]\!])^d.$$

Pour tout $i > n$, on a $X^{N_i - N_n} v_i \in M[X^{N_n}] \backslash M[X^{N_n - 1}]$ et :

$$F(X^{N_i - N_n} v_i) = X^{p(N_i - N_n)} F(v_i) \in X^{p(N_i - N_n)} M[X^{N_i}] \subseteq M[X^{N_n}].$$

Comme $M[X^{N_n}]$ est un ensemble fini (car k_E est fini et M est admissible), quitte à remplacer v_n par l'un des $X^{N_i - N_n} v_i$ pour $i > n$ on peut supposer par un procédé diagonal que l'on a $v_n = X^{N_i - N_n} v_i$ pour tout $n > 0$ et tout $i > n$. Le sous-$k_E[\![X]\!]$-module M' de M engendré par les v_n pour $n > 0$ est alors clairement isomorphe à $\varinjlim_n k_E[X]/(X^{N_n}) \cong k_E[\![X]\!][1/X]/k_E[\![X]\!]$. Par ailleurs, comme pour tout $i > n$:

$$F(v_n) = F(X^{N_i - N_n} v_i) \in X^{(p-1)(N_i - N_n)} M[X^{N_n}],$$

on en déduit $F(v_n) = 0$ pour tout $n > 0$ puisque $(p-1)(N_i - N_n) \to +\infty$ quand $i \to +\infty$. Ceci achève la preuve. □

Lemme 5.2. *Soit M un $A[\![X]\!][F]$-module de torsion sur $A[\![X]\!]$. On suppose* :

(i) *M est admissible comme $A[\![X]\!]$-module* ;

(ii) *l'application* $\mathrm{Id} \otimes F : A[\![X]\!] \otimes_{\varphi, A[\![X]\!]} M \to M$ *induit un isomorphisme comme en* (3) *en dualisant puis en inversant X.*

Alors M est un $A[\![X]\!][F]$-module de type fini.

Démonstration. Soit $0 \to M' \to M \to M'' \to 0$ une suite exacte de $A[\![X]\!][F]$-modules de torsion sur $A[\![X]\!]$ avec M comme dans l'énoncé. En particulier M' et M'' sont aussi admissibles comme $A[\![X]\!]$-modules. Comme $\varphi : A[\![X]\!] \to A[\![X]\!]$ est plat et comme la localisation est exacte, les applications $\mathrm{Id} \otimes F$ induisent un diagramme commutatif de suites exactes courtes de $A[\![X]\!][1/X]$-modules :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M''^{\vee}[1/X] & \longrightarrow & M^{\vee}[1/X] & \longrightarrow & M'^{\vee}[1/X] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & (A[\![X]\!] \otimes_{\varphi, A[\![X]\!]} M'')^{\vee}\left[\tfrac{1}{X}\right] & \to & (A[\![X]\!] \otimes_{\varphi, A[\![X]\!]} M)^{\vee}\left[\tfrac{1}{X}\right] & \to & (A[\![X]\!] \otimes_{\varphi, A[\![X]\!]} M')^{\vee}\left[\tfrac{1}{X}\right] & \to & 0 \end{array}$$

où l'application verticale du milieu est un isomorphisme par hypothèse. On en déduit que l'application verticale de droite est surjective, donc est un isomorphisme puisque les deux $A[\![X]\!][1/X]$-modules sont de même longueur (finie). La flèche verticale de gauche est donc aussi un isomorphisme. Comme M est un $A[\![X]\!][F]$-module de type fini si et seulement si M' et M'' le sont, on voit que par dévissage on est ramené à montrer le lemme pour $A = k_E$, ce que l'on suppose désormais.

Comme M est admissible, on a :

$$M^{\vee} \cong k_E[\![X]\!]^d \oplus (M^{\vee})_{\mathrm{tors}}$$

où $d \geq 0$ et $(M^{\vee})_{\mathrm{tors}} \subseteq M^{\vee}$ est le sous-$k_E[\![X]\!]$-module de torsion de $M^{\vee}$ (de dimension finie sur k_E). Comme $(M^{\vee})_{\mathrm{tors}}$ est stable par F dans $M^{\vee}$ (utiliser $X^n F(f) = F(X^{pn} f)$ si $f \in M^{\vee}$) et vérifie $(M^{\vee})_{\mathrm{tors}}[1/X] = 0$, quitte à remplacer M par $\mathrm{Ker}(M \twoheadrightarrow ((M^{\vee})_{\mathrm{tors}})^{\vee})$ on peut supposer $M^{\vee} \cong k_E[\![X]\!]^d$ et $d > 0$. En particulier on a alors $M[X^n] \backslash M[X^{n-1}] \neq \varnothing$ pour tout $n > 0$.

Pour $n > 0$ soit $M_n \subseteq M$ le sous-$k_E[\![X]\!][F]$-module engendré par $M[X^n]$. Supposons d'abord que, pour tout $n > 0$, $M_n^{\vee}[1/X] = 0$. Alors $M_n^{\vee}$ est un $k_E[\![X]\!]$-module de type fini qui est de torsion, donc est de dimension finie sur k_E. Il en est de même pour M_n et il existe donc $R_n \geq n$ tel que $M_n \subseteq M[X^{R_n}]$. On en déduit l'existence d'une suite d'entiers positifs $(R_n)_{n>0}$ telle que $M_n \subseteq M[X^{R_n}]$ pour tout $n > 0$. Montrons l'existence de (N_1, v_1) tel que $1 \leq N_1$ et $v_1 \in M[X^{N_1}] \backslash M[X^{N_1 - 1}]$ avec $F(v_1) \in M[X^{N_1}]$. Soit $v \in M[X] \backslash \{0\} \subseteq M_1$, si $F(v) \in M[X]$ (dans M_1), on prend $N_1 \overset{\text{déf}}{=} 1$ et $v_1 \overset{\text{déf}}{=} v$. Sinon, on regarde $F(v) \in M_1$. On a $F(v) \in M[X^{S_1}] \backslash M[X^{S_1 - 1}]$ pour un entier S_1 tel que $2 \leq S_1 \leq R_1$. Si $F(F(v)) \in M[X^{S_1}]$, on prend $N_1 = S_1$ et $v_1 = F(v)$, sinon on recommence avec $F^2(v) \in M_1$. Comme $M_1 \subseteq M[X^{R_1}]$, on est certain que l'un des $F^i(v)$ va marcher. En recommençant ce procédé avec M_{N_1+1} au lieu de M_1, i.e., en partant de $v \in M[X^{N_1+1}] \backslash M[X^{N_1}] \subseteq M_{N_1+1}$, on trouve (N_2, v_2) tel que $N_1 < N_2$ et $v_2 \in M[X^{N_2}] \backslash M[X^{N_2 - 1}]$ avec $F(v_2) \in M[X^{N_2}]$. En continuant on obtient ainsi une suite $(N_n, v_n)_{n>0}$ comme dans le lemme 5.1. Par le lemme 5.1, il existe un sous-$k_E[\![X]\!]$-module M' de M tel que $M'^{\vee}[1/X] \neq 0$ et $F|_{M'} \equiv 0$ (en particulier M' est stable par F dans M). Considérons maintenant le diagramme

commutatif de $k_E[\![X]\!][1/X]$-espaces vectoriels de dimension finie :

$$\begin{array}{ccc} M^\vee[1/X] & \xrightarrow{(\mathrm{Id}\otimes F)^\vee} & (k_E[\![X]\!]\otimes_{\varphi,k_E[\![X]\!]} M)^\vee[1/X] \\ \downarrow & & \downarrow \\ M'^\vee[1/X] & \xrightarrow{(\mathrm{Id}\otimes F)^\vee} & (k_E[\![X]\!]\otimes_{\varphi,k_E[\![X]\!]} M')^\vee[1/X] \end{array}$$

Comme l'application horizontale du haut est un isomorphisme (par hypothèse) et comme les deux applications verticales sont surjectives (car duales d'injections tensorisées par $k_E[\![X]\!][1/X]$), l'application horizontale du bas est aussi surjective. Mais comme elle est en fait nulle (puisque $F|_{M'}\equiv 0$), on en déduit :

$$0=(k_E[\![X]\!]\otimes_{\varphi,k_E[\![X]\!]} M')^\vee[1/X]\cong k_E[\![X]\!]\otimes_{\varphi,k_E[\![X]\!]}(M'^\vee[1/X])$$

(cf. le deuxième isomorphisme en (3)), ce qui est une contradiction car $M'^\vee[1/X]$ ne s'annule pas.

Donc il existe $n>0$ tel que $M_n^\vee[1/X]\neq 0$. En dévissant comme au début de la preuve selon la suite exacte $0\to M_n\to M\to M/M_n\to 0$ et en remarquant que M_n est un $k_E[\![X]\!][F]$-module de type fini (puisque $M[X^n]$ est de dimension finie sur k_E), on voit qu'il suffit de montrer le lemme pour M/M_n (pour un $n>0$) au lieu de M. Comme $\dim_{k_E[\![X]\!][1/X]}((M/M_n)^\vee[1/X])<\dim_{k_E[\![X]\!][1/X]}(M^\vee[1/X])=d$, en faisant une récurrence descendante sur d, on est ainsi ramené à $d=0$, i.e., au cas $M^\vee\cong(M^\vee)_{\mathrm{tors}}$ que l'on a traité au début. □

Soit N et N' deux objets de Mod_A. On munit $N^\vee$ d'une structure de $A[\![X]\!][F]$-module avec action de $\mathbb{Z}_p^\times$ comme dans la démonstration du lemme 2.6. On note $\mathrm{Hom}_A^{\mathrm{cont}}(N^\vee,N')$ le A-module des homomorphismes continus A-linéaires de $N^\vee$ dans N' où $N^\vee$ est muni de la topologie profinie et N' de la topologie discrète. Tout $\mathcal{F}\in\mathrm{Hom}_A^{\mathrm{cont}}(N^\vee,N')$ se factorise donc par un quotient fini de $N^\vee$. On munit $\mathrm{Hom}_A^{\mathrm{cont}}(N^\vee,N')$ d'un endomorphisme F défini par $F(\mathcal{F})(f)\overset{\text{déf}}{=}F\big(\mathcal{F}(F(f))\big)$ et d'une action de $\mathbb{Z}_p^\times$ par $x(\mathcal{F})(f)\overset{\text{déf}}{=}x\big(\mathcal{F}(x^{-1}(f))\big)$ (où $\mathcal{F}\in\mathrm{Hom}_A^{\mathrm{cont}}(N^\vee,N')$, $f\in N^\vee$ et $x\in\mathbb{Z}_p^\times$). C'est aussi naturellement un $A[\![X]\!]\otimes_A A[\![X]\!]$ module via $(S'(X)\otimes S(X)\cdot\mathcal{F})(f)\overset{\text{déf}}{=}S'(X)\mathcal{F}(S(X)f)$.

Soit $Y\overset{\text{déf}}{=}(1+X)\otimes 1-1\otimes(1+X)=X\otimes 1-1\otimes X\in A[\![X]\!]\otimes_A A[\![X]\!]$, on a $F(Y)=Y\big(\sum_{i=0}^{p-1}(1+X)^{p-1-i}\otimes(1+X)^i\big)$ dans $A[\![X]\!]\otimes_A A[\![X]\!]$ et on voit que :

$$\begin{aligned}\mathrm{Hom}_A^{\mathrm{cont}}(N^\vee,N')[Y]&\overset{\text{déf}}{=}\{\mathcal{F}\in\mathrm{Hom}_A^{\mathrm{cont}}(N^\vee,N'),\ Y\mathcal{F}=0\}\\&=\{\mathcal{F}\in\mathrm{Hom}_A^{\mathrm{cont}}(N^\vee,N'),\ X\mathcal{F}(f)=\mathcal{F}(Xf)\ \forall\ f\in N^\vee\}\\&=\mathrm{Hom}_{A[\![X]\!]}^{\mathrm{cont}}(N^\vee,N')\end{aligned}$$

est un $A[\![X]\!]$-module de torsion (X^j agissant par $X^j \otimes 1$ ou $1 \otimes X^j$) stable par l'action de $\mathbb{Z}_p^\times$ et par :

$$\left(\sum_{i=0}^{p-1}(1+X)^{p-1-i} \otimes (1+X)^i\right)F \tag{17}$$

dans $\mathrm{Hom}_A^{\mathrm{cont}}(N^\vee, N')$ (il s'agit du sous-A-module de $\mathrm{Hom}_A^{\mathrm{cont}}(N^\vee, N')$ des homomorphismes $A[\![X]\!]$-linéaires). En *définissant* l'action de F sur $\mathrm{Hom}_{A[\![X]\!]}^{\mathrm{cont}}(N^\vee, N')$ par (17), on obtient un objet de Mod_A.

Lemme 5.3. *Soit M et M' deux objets de* Mod_A *dont les $A[\![X]\!]$-modules sous-jacents sont admissibles. Le dual de l'application* :

$$\mathrm{Id} \otimes F : A[\![X]\!] \otimes_{\varphi, A[\![X]\!]} \mathrm{Hom}_{A[\![X]\!]}^{\mathrm{cont}}(M^\vee, M') \to \mathrm{Hom}_{A[\![X]\!]}^{\mathrm{cont}}(M^\vee, M')$$

s'identifie à l'application $(\mathrm{Id} \otimes F_M)^\vee \otimes (\mathrm{Id} \otimes F_{M'})^\vee$ (*avec des notations évidentes*) :

$$\begin{aligned} M^\vee \otimes_{A[\![X]\!]} M'^\vee &\to (A[\![X]\!] \otimes_{\varphi, A[\![X]\!]} M)^\vee \otimes_{A[\![X]\!]} (A[\![X]\!] \otimes_{\varphi, A[\![X]\!]} M')^\vee \\ &\cong (A[\![X]\!] \otimes_{\varphi, A[\![X]\!]} M^\vee) \otimes_{A[\![X]\!]} (A[\![X]\!] \otimes_{\varphi, A[\![X]\!]} M'^\vee) \\ &\cong A[\![X]\!] \otimes_{\varphi, A[\![X]\!]} (M^\vee \otimes_{A[\![X]\!]} M'^\vee). \end{aligned}$$

Démonstration. Notons d'abord que $\mathrm{Hom}_{A[\![X]\!]}^{\mathrm{cont}}(M^\vee, M') = \mathrm{Hom}_{A[\![X]\!]}(M^\vee, M')$ (car $M^\vee$ est de type fini sur $A[\![X]\!]$) et que le $A[\![X]\!]$-module $\mathrm{Hom}_{A[\![X]\!]}(M^\vee, M')$ est admissible (car $\mathrm{Hom}_{A[\![X]\!]}(M^\vee, M')[X] = \mathrm{Hom}_A(M^\vee/(X), M'[X])$ est de type fini sur A puisque $M^\vee/(X)$ et $M'[X]$ le sont). Considérons l'application entre $A[\![X]\!]$-modules de type fini :

$$\begin{aligned} M^\vee \otimes_{A[\![X]\!]} M'^\vee &\longrightarrow \mathrm{Hom}_A\big(\mathrm{Hom}_{A[\![X]\!]}(M^\vee, M'), A\big) \\ f \otimes f' &\longmapsto \big(\mathcal{F} \mapsto f'(\mathcal{F}(f))\big) \end{aligned} \tag{18}$$

($f \in M^\vee$, $f' \in M'^\vee$, $\mathcal{F} \in \mathrm{Hom}_{A[\![X]\!]}(M^\vee, M')$). Elle est bien définie et $A[\![X]\!]$-linéaire car $(S(X)f')(\mathcal{F}(f)) = f'(S(X)\mathcal{F}(f)) = f'(\mathcal{F}(S(X)f))$ ($S(X) \in A[\![X]\!]$). Il est facile de vérifier qu'elle est de plus $\mathbb{Z}_p^\times$-invariante. Montrons qu'il s'agit d'un isomorphisme. Par dualité, il suffit de montrer que l'application $A[\![X]\!]$-linéaire induite sur les $A[\![X]\!]$-modules admissibles de torsion :

$$\begin{aligned} \mathrm{Hom}_{A[\![X]\!]}(M^\vee, M') &\to \mathrm{Hom}_A^{\mathrm{cont}}(M^\vee \otimes_{A[\![X]\!]} M'^\vee, A) \\ \mathcal{F} &\mapsto \big(f \otimes f' \mapsto f'(\mathcal{F}(f))\big) \end{aligned} \tag{19}$$

est un isomorphisme. Comme on a des isomorphismes de $A[\![X]\!]$-modules :

$$\begin{aligned} \mathrm{Hom}_{A[\![X]\!]}(M^\vee, M') &\cong \varinjlim_n \mathrm{Hom}_{A[\![X]\!]}\big(M^\vee/(X^n), M'[X^n]\big) \\ \mathrm{Hom}_A^{\mathrm{cont}}(M^\vee \otimes_{A[\![X]\!]} M'^\vee, A) &\cong \varinjlim_n \mathrm{Hom}_A\big(M^\vee/(X^n) \otimes_{A[\![X]\!]} M'^\vee/(X^n), A\big), \end{aligned}$$

il suffit de montrer l'analogue de (19) en remplaçant M (resp. M') par $M[X^n]$ (resp. $M'[X^n]$), i.e., il suffit de le démontrer avec M et M' des $A[\![X]\!]$-modules de torsion de type fini (donc finis). Changeant de notations, il suffit donc de montrer que :

$$\begin{aligned}\mathrm{Hom}_{A[\![X]\!]}(M, {M'}^\vee) &\to \mathrm{Hom}_A(M\otimes_{A[\![X]\!]} M', A)\\ \mathcal{F} &\mapsto \big(m\otimes m'\mapsto \mathcal{F}(m)(m')\big)\end{aligned} \tag{20}$$

est un isomorphisme, ce qui est clair car l'application réciproque est donnée par :

$$\mathcal{G}\in \mathrm{Hom}_A(M\otimes_{A[\![X]\!]} M', A)\longmapsto \big(m\mapsto (m'\mapsto \mathcal{G}(m\otimes m'))\big).$$

Reste enfin à montrer que le diagramme :

$$\begin{array}{ccc} M^\vee\otimes_{A[\![X]\!]} {M'}^\vee & \xrightarrow{(18)} & \mathrm{Hom}_A\big(\mathrm{Hom}^{\mathrm{cont}}_{A[\![X]\!]}(M^\vee, M'), A\big)\\ \downarrow & & \downarrow\\ A[\![X]\!]\otimes_{\varphi, A[\![X]\!]}(M^\vee\otimes_{A[\![X]\!]} {M'}^\vee) & \xrightarrow{\mathrm{Id}\otimes(18)} & A[\![X]\!]\otimes_{\varphi, A[\![X]\!]}\mathrm{Hom}_A\big(\mathrm{Hom}^{\mathrm{cont}}_{A[\![X]\!]}(M^\vee, M'), A\big)\end{array} \tag{21}$$

est commutatif où les deux applications verticales sont les duales de $\mathrm{Id}\otimes F$. Si N est un objet quelconque de Mod_A, l'application :

$$(\mathrm{Id}\otimes F)^\vee : N^\vee \to \big(A[\![X]\!]\otimes_{\varphi, A[\![X]\!]} N\big)^\vee \cong A[\![X]\!]\otimes_{\varphi, A[\![X]\!]} N^\vee$$

est donnée par :

$$f\mapsto \sum_{i=0}^{p-1}(1+X)^{p-1-i}\otimes f_i \tag{22}$$

où $f\in N^\vee$ et $f_i\in N^\vee$ est défini par $f_i(n)\overset{\text{déf}}{=} f((1+X)^i F(n))$ pour $n\in N$. La commutation de (21) est alors un calcul un petit peu laborieux mais sans difficulté et laissé au lecteur. □

Proposition 5.4. *Soit M et M' deux objets de* Mod_A *dont les $A[\![X]\!][F]$-modules sous-jacents vérifient* (1). *Alors* $\mathrm{Hom}^{\mathrm{cont}}_{A[\![X]\!]}(M^\vee, M')$ *vérifie aussi* (1).

Démonstration. On a vu dans la preuve du lemme 5.3 que le $A[\![X]\!]$-module $\mathrm{Hom}^{\mathrm{cont}}_{A[\![X]\!]}(M^\vee, M') = \mathrm{Hom}_{A[\![X]\!]}(M^\vee, M')$ est admissible. Il faut montrer qu'il est de type fini sur $A[\![X]\!][F]$. L'application :

$$\begin{aligned}&(\mathrm{Id}\otimes F_M)^\vee\otimes(\mathrm{Id}\otimes F_{M'})^\vee :\\ &\quad M^\vee\otimes_{A[\![X]\!]} {M'}^\vee \longrightarrow (A[\![X]\!]\otimes_{\varphi, A[\![X]\!]} M)^\vee\otimes_{A[\![X]\!]}(A[\![X]\!]\otimes_{\varphi, A[\![X]\!]} M')^\vee\\ &\qquad\qquad\cong A[\![X]\!]\otimes_{\varphi, A[\![X]\!]}(M^\vee\otimes_{A[\![X]\!]} {M'}^\vee)\end{aligned}$$

est un isomorphisme $A[\![X]\!][1/X]$-linéaire lorsque l'on inverse X car tel est le cas de $(\mathrm{Id}\otimes F_M)^\vee$ et $(\mathrm{Id}\otimes F_{M'})^\vee$ (puisque M, M' vérifient (1), cf. (3)). Le lemme 5.2

(que l'on peut appliquer à $\mathrm{Hom}_{A[\![X]\!]}(M^\vee, M')$ par le lemme 5.3) implique alors que $\mathrm{Hom}_{A[\![X]\!]}(M^\vee, M')$ est de type fini sur $A[\![X]\!][F]$. □

La catégorie $\widehat{\Phi\Gamma}_A^{\text{ét}}$ est munie d'un produit tensoriel naturel comme suit : si $D = \varprojlim_{i\in I} D_i$ et $D' = \varprojlim_{i'\in I'} D'_{i'}$ sont dans $\widehat{\Phi\Gamma}_A^{\text{ét}}$, on pose :

$$D\widehat{\otimes}D' \overset{\text{déf}}{=} \varprojlim_{(i,i')\in I\times I'} (D_i \otimes_{A[\![X]\!][1/X]} D'_{i'}) \in \widehat{\Phi\Gamma}_A^{\text{ét}} \tag{23}$$

où $D_i \otimes_{A[\![X]\!][1/X]} D'_{i'}$ est le produit tensoriel dans $\Phi\Gamma_A^{\text{ét}}$ (on vérifie que cela est indépendant des D_i, $D'_{i'}$ tels que $D = \varprojlim D_i$ et $D' = \varprojlim D'_{i'}$). Notons que $D\widehat{\otimes}D' = D \otimes_{A[\![X]\!][1/X]} D'$ si $D, D' \in \Phi\Gamma_A^{\text{ét}}$.

Nous montrons maintenant le résultat principal de cette section. Notons d'abord que, comme le foncteur $D_\xi^\vee$ du § 3 ne dépend que du choix de ξ, quitte à modifier ι_α et N_0 il n'est pas difficile de voir que l'on peut de plus supposer que ι_α induit des isomorphismes pour $\alpha \in S$:

$$N_\alpha(L) \cap N_0 \xrightarrow{\sim} \mathcal{O}_L \subset L = \mathbb{G}_{\mathrm{a}}(L). \tag{24}$$

On supposera toujours dans la suite que N_0 vérifie (24). De plus, on fixe une fois pour toute un isomorphisme de $\mathbb{Z}_p$-modules $\psi : \mathrm{Tr}_{L/\mathbb{Q}_p}(\mathcal{O}_L) \xrightarrow{\sim} \mathbb{Z}_p$, ce qui fixe donc un isomorphisme (si $G \neq T$) :

$$N_0/N_1 \xrightarrow[\mathrm{Tr}_{L/\mathbb{Q}_p}\circ\,\ell]{\sim} \mathrm{Tr}_{L/\mathbb{Q}_p}(\mathcal{O}_L) \xrightarrow[\psi]{\sim} \mathbb{Z}_p.$$

Soit G' un autre groupe algébrique réductif connexe déployé sur L de centre connexe, $B' \subseteq G'$ un sous-groupe de Borel et $T' \subseteq B'$ un tore maximal déployé dans B'. Comme pour (G, B, T) on fixe $(\iota_{\alpha'})_{\alpha'\in S'}$ (où S' désigne les racines simples associées à (G', B', T')), $\xi' \in X^\vee(T')$ et N'_0 totalement décomposé vérifiant (24). On définit N'_1 par (11) et, comme ci-dessus, l'isomorphisme ψ induit un isomorphisme de $\mathbb{Z}_p$-modules $N'_0/N'_1 \cong \mathbb{Z}_p$ si $G' \neq T'$. On considère $(G\times G', B\times B', T\times T')$ avec les choix $((\iota_\alpha)_{\alpha\in S}, (\iota_{\alpha'})_{\alpha'\in S'})$, $\xi \oplus \xi' \in X^\vee(T\times T')$ et $N_0 \times N'_0$ (qui est totalement décomposé et vérifie (24)) et on note :

$$N''_1 \overset{\text{déf}}{=} \mathrm{Ker}\big(N_0 \times N'_0 \xrightarrow{\sum\iota_\alpha+\sum\iota_{\alpha'}} \mathcal{O}_L \xrightarrow{\mathrm{Tr}_{L/\mathbb{Q}_p}} \mathrm{Tr}_{L/\mathbb{Q}_p}(\mathcal{O}_L) \xrightarrow{\psi} \mathbb{Z}_p\big). \tag{25}$$

Pour toute représentation lisse de $B(L)\times B'(L)$ sur A on dispose donc de $D^\vee_{\xi\oplus\xi'}(\cdot) \in \widehat{\Phi\Gamma}_A^{\text{ét}}$.

Proposition 5.5. *Soit π et π' des représentations lisses respectivement de $B(L)$ et $B'(L)$ sur des A-modules libres. On suppose que les $A[\![X]\!][F]$-modules π^{N_1} et ${\pi'}^{N'_1}$ satisfont la propriété Ad de la définition 2.2. Alors on a un isomorphisme dans $\widehat{\Phi\Gamma}_A^{\text{ét}}$:*

$$D^\vee_{\xi\oplus\xi'}(\pi \otimes_A \pi') \cong D^\vee_\xi(\pi)\widehat{\otimes}D^\vee_{\xi'}(\pi'). \tag{26}$$

Démonstration. Notons $\mathrm{Hom}_A^{\mathrm{cont}}(\pi^\vee,\pi')$ le A-module des homomorphismes A-linéaires continus de $\pi^\vee$ dans π' où $\pi^\vee$ est muni de la topologie profinie et π' de la topologie discrète. En écrivant $\pi=\varinjlim_n V_n$ et $\pi'=\varinjlim_{n'} V'_{n'}$, où V_n et $V'_{n'}$ sont des sous-A-modules *libres* de type fini quelconques de (l'espace sous-jacent à) respectivement π et π', on a :

$$\mathrm{Hom}_A^{\mathrm{cont}}(\pi^\vee,\pi')=\varprojlim_n \mathrm{Hom}_A(V_n^\vee,\pi')=\varprojlim_{n,n'}\mathrm{Hom}_A(V_n^\vee,V'_{n'}). \tag{27}$$

L'application $\pi\otimes_A\pi'\to\mathrm{Hom}_A^{\mathrm{cont}}(\pi^\vee,\pi')$, $v\otimes v'\mapsto(f\mapsto f(v)v')$ est un isomorphisme, car par (27) et $\pi\otimes_A\pi'=\varinjlim_{n,n'}V_n\otimes_A V_{n'}$ il suffit de le vérifier avec les A-modules libres de type fini V_n et $V_{n'}$ au lieu de π et π' où c'est évident.

Supposons d'abord $G\neq T$ et $G'\neq T'$. On déduit de ce qui précède un isomorphisme :

$$\begin{aligned}(\pi\otimes_A\pi')^{N_1\times N'_1}\xrightarrow{\sim}\mathrm{Hom}_A^{\mathrm{cont}}(\pi^\vee,\pi')^{N_1\times N'_1}&\cong\mathrm{Hom}_A^{\mathrm{cont}}(\pi^\vee,\pi'^{N'_1})^{N_1}\\&\cong\mathrm{Hom}_A^{\mathrm{cont}}\big((\pi^{N_1})^\vee,\pi'^{N'_1}\big).\end{aligned}\tag{28}$$

(Le dernier isomorphisme se montre en écrivant $\pi=\varinjlim_n W_n$ où la limite inductive est prise sur des sous-A-modules de type finis W_n de π stables par N_1 et en utilisant que les coinvariants $(W_n^\vee)_{N_1}$ de $W_n^\vee$ pour l'action de N_1 sont isomorphes à $(W_n^{N_1})^\vee$, ce qui découle en dualisant puis en remplaçant W_n par son dual du fait que, si V est une représentation lisse de N_1 sur un A-module de type fini, on a $(V^\vee)^{N_1}=(V_{N_1})^\vee$.) Il n'est pas difficile de vérifier que l'action de $N_0\times N'_0$ sur $(\pi\otimes_A\pi')^{N_1\times N'_1}$ induit la structure de $A[\![N_0/N_1]\!]\otimes_A A[\![N'_0/N'_1]\!]\cong A[\![N'_0/N'_1]\!]\otimes_A A[\![N_0/N_1]\!]\cong A[\![X]\!]\otimes_A A[\![X]\!]$-module définie ci-dessus sur $\mathrm{Hom}_A^{\mathrm{cont}}\big((\pi^{N_1})^\vee,\pi'^{N'_1}\big)$ (rappelons que π^{N_1} et $\pi'^{N'_1}$ sont dans Mod_A) et que, par (25), cela induit un isomorphisme de $A[\![X]\!]$-modules :

$$(\pi\otimes_A\pi')^{N''_1}\xrightarrow{\sim}\mathrm{Hom}_A^{\mathrm{cont}}\big((\pi^{N_1})^\vee,\pi'^{N'_1}\big)[Y]\cong\mathrm{Hom}_{A[\![X]\!]}^{\mathrm{cont}}\big((\pi^{N_1})^\vee,\pi'^{N'_1}\big)\tag{29}$$

qui commute aux actions de $\mathbb{Z}_p^\times$ et de F (avec l'action (17) de F à droite). Soit $H\subseteq\mathrm{Hom}_{A[\![X]\!]}^{\mathrm{cont}}((\pi^{N_1})^\vee,\pi'^{N'_1})$ un sous-$A[\![X]\!][F]$-module de type fini et $\mathcal{F}_1,\dots,\mathcal{F}_d$ des générateurs de H sur $A[\![X]\!][F]$. Par continuité chaque $\mathcal{F}_i:(\pi^{N_1})^\vee\to\pi'^{N'_1}$ se factorise par un quotient $M_i^\vee$ de $(\pi^{N_1})^\vee$ où $M_i\subseteq\pi^{N_1}$ est un sous-A-module de type fini que l'on peut prendre stable par $\mathbb{Z}_p^\times$, et est à valeurs dans un sous-A-module de type fini M'_i (stable par $\mathbb{Z}_p^\times$) de $\pi'^{N'_1}$. Soit M (resp. M') le sous-$A[\![X]\!][F]$-module de π^{N_1} (resp. $\pi'^{N'_1}$) engendré par $\sum_{i=1}^d M_i$ (resp. $\sum_{i=1}^d M'_i$), alors M et M' sont des $A[\![X]\!][F]$-modules de type fini (stables par $\mathbb{Z}_p^\times$) et donc des $A[\![X]\!]$-modules admissibles puisque π^{N_1} et $\pi'^{N'_1}$ satisfont la propriété Ad. De plus, par construction on a :

$$\mathcal{F}_i\in\mathrm{Hom}_{A[\![X]\!]}^{\mathrm{cont}}(M^\vee,M')=\mathrm{Hom}_{A[\![X]\!]}(M^\vee,M')$$

pour tout i et donc $H = \sum_{i=1}^{d} A[\![X]\!][F]\mathcal{F}_i \subseteq \mathrm{Hom}_{A[\![X]\!]}(M^\vee, M')$. Comme par la proposition 5.4 et (29), on a :

$$\mathrm{Hom}_{A[\![X]\!]}(M^\vee, M') \in \mathcal{M}\big(\mathrm{Hom}^{\mathrm{cont}}_{A[\![X]\!]}((\pi^{N_1})^\vee, \pi'^{N_1'})\big) = \mathcal{M}((\pi \otimes_A \pi')^{N_1''}),$$

on en déduit que H est un $A[\![X]\!]$-module admissible et que les $A[\![X]\!][F]$-modules $\mathrm{Hom}_{A[\![X]\!]}(M^\vee, M')$ pour (M, M') parcourant $\mathcal{M}(\pi^{N_1}) \times \mathcal{M}(\pi'^{N_1'})$ forment un système cofinal dans $\mathcal{M}((\pi \otimes_A \pi')^{N_1''})$. Cela implique :

$$\begin{aligned} D^\vee((\pi \otimes_A \pi')^{N_1''}) &\cong \varprojlim_{(M,M')} D^\vee\big(\mathrm{Hom}_{A[\![X]\!]}(M^\vee, M')\big) \\ &\cong \varprojlim_{(M,M')} \big(M^\vee[1/X] \otimes_{A[\![X]\!][1/X]} M'^\vee[1/X]\big) \\ &\cong D^\vee(\pi^{N_1}) \widehat{\otimes} D^\vee(\pi'^{N_1'}), \end{aligned}$$

où la limite projective est prise sur $(M, M') \in \mathcal{M}(\pi^{N_1}) \times \mathcal{M}(\pi'^{N_1'})$ et où le deuxième isomorphisme résulte du lemme 5.3. Cela donne l'isomorphisme de l'énoncé lorsque $G \neq T$, $G' \neq T'$.

Traitons le cas $G = T$ et $G' \neq T'$ et notons que $\pi^{N_1} = \pi$ est un $A[F]$-module de torsion puisqu'il satisfait la propriété Ad. Pour $(M, M') \in \mathcal{M}(\pi) \times \mathcal{M}(\pi'^{N_1})$ on a $\mathrm{Hom}^{\mathrm{cont}}_A(M^\vee, M') = \mathrm{Hom}_A(M^\vee, M')$ et un isomorphisme $A[\![X]\!]$-linéaire analogue à (18) :

$$(A[\![X]\!] \otimes_A M^\vee) \otimes_{A[\![X]\!]} M'^\vee \cong M^\vee \otimes_A M'^\vee \xrightarrow{\sim} \mathrm{Hom}_A(\mathrm{Hom}_A(M^\vee, M'), A).$$

Par une preuve analogue (en plus simple) à celle du cas $G \neq T$, $G' \neq T'$, on obtient que les $\mathrm{Hom}_A(M^\vee, M')$ pour $(M, M') \in \mathcal{M}(\pi) \times \mathcal{M}(\pi'^{N_1})$ forment un système cofinal dans $\mathcal{M}(\mathrm{Hom}^{\mathrm{cont}}_A(\pi^\vee, \pi'^{N_1'})) = \mathcal{M}(\pi \otimes_A \pi'^{N_1})$ et que $D^\vee(\mathrm{Hom}_A(M^\vee, M')) \cong D^\vee(M) \otimes_{A[\![X]\!][1/X]} D^\vee(M')$. On conclut comme dans le cas $G \neq T$, $G' \neq T'$. Enfin, le cas $G = T$, $G' = T'$ est encore plus simple et laissé au lecteur. □

Remarque 5.6. (i) La preuve de la proposition 5.5 donne aussi que le $A[\![X]\!][F]$-module $(\pi \otimes_A \pi')^{N_1''} \cong \mathrm{Hom}^{\mathrm{cont}}_{A[\![X]\!]}((\pi^{N_1})^\vee, \pi'^{N_1'})$ satisfait la propriété Ad. Par une récurrence immédiate, on en déduit pour tout entier $n > 0$ un isomorphisme (avec des notations évidentes) $D^\vee_{\xi_1 \oplus \cdots \oplus \xi_n}(\pi_1 \otimes_A \cdots \otimes_A \pi_n) \cong D^\vee_{\xi_1}(\pi_1) \widehat{\otimes} \cdots \widehat{\otimes} D^\vee_{\xi_n}(\pi_n)$ lorsque tous les π_i vérifient les hypothèses de la proposition 5.5.

(ii) L'énoncé de la proposition 5.5 est peut-être valable sans supposer que π^{N_1} et $\pi'^{N_1'}$ satisfont la propriété Ad ou que les espaces sous-jacents à π et π' sont libres sur A. Par exemple, on peut montrer que, lorsque $A = k_E$, l'isomorphisme (26) est vrai pour *toutes* représentations lisses π, π' de $B(L)$ et $B'(L)$ sur k_E sans hypothèse supplémentaire. Mais n'ayant qu'une preuve assez laborieuse de ce dernier résultat (pour $A = k_E$), et n'ayant de toute façon pas à appliquer (26) ici en dehors des

conditions de la proposition 5.5 (cf. §9), j'ai finalement opté pour l'énoncé *a minima* ci-dessus.

(iii) Soit N dans Mod_A et munissons $N^\vee = \mathrm{Hom}_A(N, A)$ de sa structure de $A[\![X]\!][F]$-module avec action de $\mathbb{Z}_p^\times$ comme ci-dessus. Alors tout quotient D de $N^\vee[1/X]$ de type fini comme $A[\![X]\!][1/X]$-module, stable par $\mathbb{Z}_p^\times$ et tel que $(\mathrm{Id}\otimes F)^\vee : N^\vee[1/X] \to A[\![X]\!]\otimes_{\varphi, A[\![X]\!]} N^\vee[1/X]$ induit un isomorphisme $D \xrightarrow{\sim} A[\![X]\!]\otimes_{\varphi, A[\![X]\!]} D$ est de la forme $M^\vee[1/X]$ pour un $M \in \mathcal{M}(N)$. En effet, il suffit de considérer l'image du $A[\![X]\!]$-module compact $N^\vee$ dans le $A[\![X]\!][1/X]$-module de type fini D, d'utiliser la dualité modules compacts - modules discrets [Gabriel 1962, §IV.4] et d'appliquer le lemme 5.2 au dual M de cette image. Comme réciproquement tout $M \in \mathcal{M}(N)$ donne un tel quotient $D = M^\vee[1/X]$ (lemme 2.6), on obtient que $D^\vee(N)$ s'identifie à la limite projective des quotients de $N^\vee[1/X]$ qui sont dans $\Phi\Gamma_A^{\text{ét}}$. En appliquant cela à $N = \pi^{N_1}$ pour π représentation lisse de $B(L)$ sur A (et $G \neq T$), on voit que $D_\xi^\vee(\pi)$ s'identifie à la limite projective des $A[\![X]\!][1/X]$-modules quotients de $(\pi^{N_1})^\vee[1/X]$ qui sont dans $\Phi\Gamma_A^{\text{ét}}$. On a une identification analogue lorsque $G = T$ en remplaçant $(\pi^{N_1})^\vee[1/X]$ par $\pi^\vee \otimes_A A[\![X]\!][1/X]$ que l'on laisse au lecteur.

(iv) On peut donner une variante comme suit de la preuve du lemme 5.2 (je remercie un rapporteur anonyme pour cette remarque). Via le même argument qu'au début du (iii) ci-dessus et une récurrence comme au début de la preuve du lemme 5.2, on peut supposer que $M^\vee[1/X]$ est un φ-module (étale) irréductible sur $k_E[\![X]\!][1/X]$ (on utilise que la catégorie des φ-modules étales de dimension finie est abélienne, noter qu'il n'y a pas de Γ ici). Dès lors (avec les notations de la preuve du lemme 5.2) : soit $M = M_n$ pour un $n > 0$, et c'est fini puisque M_n est de type fini sur $k_E[\![X]\!][F]$, soit $M_n^\vee[1/X] = 0$ pour tout $n > 0$ par irréductibilité de M, ce qui conduit à l'existence de M' et une contradiction.

(v) La construction de $D_\xi^\vee(\pi)$ donnée en (iii) ci-dessus peut aussi s'interpréter comme une propriété universelle de $D_\xi^\vee(\pi)$. Nous renvoyons pour cela le lecteur à l'article récent d'Erdélyi et Zábrádi [2014] où les auteurs utilisent [Zábrádi 2011] pour généraliser cette interprétation de $D_\xi^\vee(\pi)$ et faire le lien avec le foncteur construit dans [Schneider et Vignéras 2011].

6. Le cas des induites paraboliques I

Dans cette section et la suivante on calcule le $D_\xi^\vee$ d'une induite parabolique en fonction du $D_\xi^\vee$ de la représentation induisante du Levi.

On conserve les notations du § 3, en particulier on fixe des isomorphismes $\iota_\alpha : N_\alpha \xrightarrow{\sim} \mathbb{G}_{\mathrm{a}}$ pour $\alpha \in S$ vérifiant (9), un sous-groupe ouvert compact $N_0 \subset N(L)$ totalement décomposé et vérifiant (24), un isomorphisme de $\mathbb{Z}_p$-modules

$\psi : \mathrm{Tr}_{L/\mathbb{Q}_p}(\mathcal{O}_L) \xrightarrow{\sim} \mathbb{Z}_p$ (ce qui détermine un isomorphisme $N_0/N_1 \cong \mathbb{Z}_p$ lorsque $G \neq T$) et un cocaractère $\xi \in X^\vee(T)$ tel que $\alpha \circ \xi = \mathrm{Id}_{\mathbb{G}_\mathrm{m}}$ pour $\alpha \in S$.

Soit $P \subseteq G$ un sous-groupe parabolique contenant B, L_P son sous-groupe de Levi, N_P son radical unipotent, P^- le parabolique opposé à P et N_{P^-} le radical unipotent de P^-. Le groupe L_P est réductif connexe déployé et on fixe $B \cap L_P$ comme sous-groupe de Borel de L_P, dont le radical unipotent est $N_{L_P} = N \cap L_P$. On note R_P les racines de (L_P, T), $R_P^+ \subseteq R_P$ les racines positives relativement à $B \cap L_P$ et $S_P \subseteq R_P^+$ les racines simples. Comme Z_G est connexe par hypothèse, ou de manière équivalente le $\mathbb{Z}$-module $X(T)/(\oplus_{\alpha\in S}\mathbb{Z}\alpha)$ est sans torsion, on a que le centre Z_{L_P} de L_P est aussi connexe (car $X(T)/(\oplus_{\alpha\in S_P}\mathbb{Z}\alpha)$ est aussi sans torsion puisque $X(T)/(\oplus_{\alpha\in S}\mathbb{Z}\alpha)$ est sans torsion et $\oplus_{\alpha\in S_P}\mathbb{Z}\alpha$ est facteur direct de $\oplus_{\alpha\in S}\mathbb{Z}\alpha$).

Pour pouvoir appliquer à $(L_P, B\cap L_P, T)$ les constructions et résultats du §3 on doit fixer des choix pour le groupe réductif L_P. On le fait de manière compatible à ceux pour G comme suit. On garde le même $\xi \in X^\vee(T)$ et les mêmes ι_α (pour $\alpha \in S_P$) et on note ℓ_P la composée :

$$N_{L_P} \twoheadrightarrow \prod_{\alpha\in S_P} N_\alpha \xrightarrow{\sum_{\alpha\in S_P}\iota_\alpha} \mathbb{G}_\mathrm{a}.$$

On a donc un diagramme commutatif :

$$\begin{array}{ccc} N_{L_P} & \hookrightarrow & N \\ {\scriptstyle \ell_P}\downarrow & & \downarrow{\scriptstyle \ell} \\ \mathbb{G}_\mathrm{a} & = & \mathbb{G}_\mathrm{a} \end{array} \tag{30}$$

On pose $N_{L_P,0} \overset{\text{déf}}{=} N_{L_P}(L) \cap N_0 = \prod_{\alpha\in R_P^+} N_\alpha(L) \cap N_0$ de sorte que :

$$N_{L_P,1} \overset{\text{déf}}{=} \mathrm{Ker}(N_{L_P,0} \xrightarrow{\ell_P} L \xrightarrow{\mathrm{Tr}_{L/\mathbb{Q}_p}} \mathbb{Q}_p)$$

vérifie $N_{L_P,1} = N_{L_P}(L) \cap N_1 = N_{L_P,0} \cap N_1$ par (30). Lorsque $P \neq B$, l'hypothèse (24) implique que l'on a des suites exactes courtes :

$$0 \to N_{L_P,1} \to N_{L_P,0} \to \mathrm{Tr}_{L/\mathbb{Q}_p}(\mathcal{O}_L) \to 0, \quad 0 \to N_1 \to N_0 \to \mathrm{Tr}_{L/\mathbb{Q}_p}(\mathcal{O}_L) \to 0$$

d'où il suit que l'injection $N_{L_P,0} \subseteq N_0$ induit un isomorphisme (pour $P \neq B$) :

$$N_{L_P,0}/N_{L_P,1} \xrightarrow{\sim} N_0/N_1. \tag{31}$$

Toujours lorsque $P \neq B$, l'isomorphisme ψ induit $N_{L_P,0}/N_{L_P,1} \cong \mathbb{Z}_p$ qui coïncide avec (31) composé avec $N_0/N_1 \cong \mathbb{Z}_p$.

L'objectif de cette section et la suivante est de démontrer le théorème suivant.

Théorème 6.1. *Soit π_P une représentation lisse de $L_P(L)$ sur A, que l'on voit par inflation comme représentation lisse de $P^-(L)$. On a un isomorphisme fonctoriel en π_P dans la catégorie $\widehat{\Phi\Gamma}_A^{\text{ét}}$:*

$$D_\xi^\vee(\mathrm{Ind}_{P^-(L)}^{G(L)}\pi_P) \cong D_\xi^\vee(\pi_P).$$

On suppose $G \neq T$ dans la suite sinon il n'y a rien à montrer. On note $W \cong N_G(T)/T$ et $W_P \cong N_{L_P}(T)/T$ les groupes de Weyl respectifs de G et L_P, et $w_0 \in W$ l'élément de longueur maximale. On a $W_P \subseteq W$ et l'ensemble :

$$K_P \overset{\text{déf}}{=} \{w \in W,\ w^{-1}(R_P^+) \subseteq R^+\}$$

est un système de représentants (dits de Kostant) des classes à gauche $W_P\backslash W$. En utilisant que $\{ww_0,\ w \in K_P\}$ est encore un système de représentants de $W_P\backslash W$, on déduit de la décomposition de Bruhat généralisée [Digne et Michel 1991, Lemma 5.5] que l'on a une décomposition :

$$G = \coprod_{w\in K_P} P^- wB = \coprod_{w\in K_P} P^- wN. \tag{32}$$

En procédant comme dans [Emerton 2010, §4.3] ou [Vignéras 2008] ou encore [Hauseux 2014, §2.1], rappelons que la représentation $\mathrm{Ind}_{P^-(L)}^{G(L)}\pi_P$ admet une filtration croissante par des sous-$B(L)$-représentations dont les gradués sont contenus dans :

$$\mathcal{C}_w(\pi_P) \overset{\text{déf}}{=} \text{c-Ind}_{P^-(L)}^{P^-(L)wN(L)}\pi_P$$

pour $w \in K_P$ où c-Ind signifie les fonctions (localement constantes) à support compact modulo $P^-(L)$ et où l'action de $B(L)$ sur $\mathcal{C}_w(\pi_P)$ est la translation à droite sur les fonctions. De plus $\mathcal{C}_1(\pi_P)$ est le premier cran (ou premier gradué) de la filtration. En fait, au moins lorsque $P = B$, les gradués sont tous exactement les $\mathcal{C}_w(\pi_P)$, cf. par exemple [Hauseux 2014, §2.1] (nous n'aurons pas besoin de ce résultat pour $P \neq B$). Par exactitude à droite du foncteur contravariant $D_\xi^\vee$ (cf. (ii) de la proposition 3.2) et un dévissage évident, on voit qu'il suffit de démontrer les deux propositions suivantes.

Proposition 6.2. *On a $D_\xi^\vee(\mathcal{C}_w(\pi_P)) = 0$ pour tout $w \in K_P\backslash\{1\}$.*

Proposition 6.3. *On a un isomorphisme fonctoriel en π_P dans la catégorie $\widehat{\Phi\Gamma}_A^{\text{ét}}$:*

$$D_\xi^\vee(\mathcal{C}_1(\pi_P)) \cong D_\xi^\vee(\pi_P).$$

Pour $w \in K_P$ soit π_P^w la représentation de $w^{-1}P^-(L)w$ dont l'espace sous-jacent est le même que π_P et telle que $w^{-1}p^-w \in w^{-1}P^-(L)w$ agit par $\pi_P(p^-)$. On a un isomorphisme $B(L)$-équivariant :

$$\mathcal{C}_w(\pi_P) \xrightarrow{\sim} \text{c-Ind}_{w^{-1}P^-(L)w\cap N(L)}^{N(L)}\pi_P^w, \quad f \mapsto (n \mapsto f(wn)) \tag{33}$$

où l'action de $N(L)$ est la translation à droite sur les fonctions et où l'action de $T(L)$ est donnée par :

$$(th)(n) = \pi_P^w(t)(h(t^{-1}nt)) \tag{34}$$

si $t \in T(L)$, $n \in N(L)$ et $h \in \text{c-Ind}_{w^{-1}P^-(L)w\cap N(L)}^{N(L)} \pi_P^w$ (noter que $T(L)$ est contenu dans $w^{-1}P^-(L)w$).

Le reste de cette section est consacré à la démonstration de la proposition 6.2.

Lemme 6.4. *Notons R^- (resp. R_P^-) les racines négatives de (G,T) (resp. (L_P,T)) relativement à B (resp. $B\cap L_P$). Soit $w \in K_P\backslash\{1\}$, alors on a $w^{-1}(R^-\backslash R_P^-)\cap S \neq \varnothing$.*

Démonstration. Comme $w \neq 1$, on a $R^- \cap w(R^+) \neq \varnothing$ et donc $R^- \cap w(S) \neq \varnothing$ (puisqu'une racine de $w(R^+)$ est somme à coefficients positifs de racines de $w(S)$). Comme $w \in K_P$, on a $w^{-1}(R_P^-) \subseteq R^-$, donc $w^{-1}(R_P^-) \cap S = \varnothing$ c'est-à-dire $R_P^- \cap w(S) = \varnothing$. On en déduit $(R^-\backslash R_P^-) \cap w(S) \neq \varnothing$, d'où le résultat. □

Le lemme suivant s'inspire de [Schneider et Vignéras 2011, Proposition 12.2].

Lemme 6.5. *Soit $w \in K_P\backslash\{1\}$, alors $(w^{-1}N_{P^-}(L)w \cap N_0)\backslash N_0/N_1 = \{1\}$.*

Démonstration. Par le lemme 6.4, il existe $\alpha \in S$ tel que $N_\alpha \subseteq w^{-1}N_{P^-}w$, donc $N_\alpha(L)\cap N_0 \subseteq w^{-1}N_{P^-}(L)w\cap N_0$ et il suffit de montrer $(N_\alpha(L)\cap N_0)\backslash N_0/N_1 = \{1\}$. Soit $N_2 \overset{\text{déf}}{=} \text{Ker}(N_0 \overset{\ell}{\to} \mathcal{O}_L)$, on a $N_2 \subseteq N_1$ et il suffit de montrer que :

$$(N_\alpha(L) \cap N_0)\backslash N_0/N_2 = \{1\}.$$

Comme $\ell : N_0/N_2 \xrightarrow{\sim} \mathcal{O}_L$ par (24), il suffit de montrer $\ell(N_\alpha(L) \cap N_0)\backslash\mathcal{O}_L = \{0\}$. Mais c'est clair puisque $\ell(N_\alpha(L) \cap N_0) = \iota_\alpha(N_\alpha(L) \cap N_0) = \mathcal{O}_L$ (encore) par (24). □

Pour tout $w \in K_P$ on munit $\mathcal{C}_w(\pi_P)^{N_1} \cong \left(\text{c-Ind}_{w^{-1}P^-(L)w\cap N(L)}^{N(L)} \pi_P^w\right)^{N_1}$ de sa structure d'objet de Mod_A définie au § 3.

Lemme 6.6. (i) *Soit $M \subseteq \left(\text{c-Ind}_{w^{-1}P^-(L)w\cap N(L)}^{N(L)} \pi_P^w\right)^{N_1}$ un sous-$A[\![X]\!][F]$-module de type fini. Alors il existe un entier $n \geq 0$ tel que $F^n(M) \subseteq \left(\text{Ind}_{w^{-1}P^-(L)w\cap N_0}^{N_0} \pi_P^w\right)^{N_1}$.*

(ii) *Le sous-$A[\![X]\!]$-module $\left(\text{Ind}_{w^{-1}P^-(L)w\cap N_0}^{N_0} \pi_P^w\right)^{N_1}$ de $\left(\text{c-Ind}_{w^{-1}P^-(L)w\cap N(L)}^{N(L)} \pi_P^w\right)^{N_1}$ est un sous-objet dans* Mod_A.

Démonstration. (i) Par [Hauseux 2014, lemme 3.1.3] on a :

$$N(L) = \bigcup_{n\geq 0} \xi(p^{-n})N_0\xi(p^n)$$

et par (34) on a :

$$\xi(p)(\text{Ind}_{w^{-1}P^-(L)w\cap\xi(p^{-n})N_0\xi(p^n)}^{\xi(p^{-n})N_0\xi(p^n)} \pi_P^w) \subseteq \text{Ind}_{w^{-1}P^-(L)w\cap\xi(p^{-n+1})N_0\xi(p^{n-1})}^{\xi(p^{-n+1})N_0\xi(p^{n-1})} \pi_P^w.$$

Soit $n \geq 0$ et $M_n \overset{\text{déf}}{=} (\mathrm{Ind}_{w^{-1}P^-(L)w\cap\xi(p^{-n})N_0\xi(p^n)}^{\xi(p^{-n})N_0\xi(p^n)} \pi_P^w)^{N_1}$, on en déduit avec (12) (et $N_0 \subseteq \xi(p^{-n})N_0\xi(p^n)$) que les M_n sont des sous-$A[\![X]\!][F]$-modules croissants (quand n grandit) du $A[\![X]\!][F]$-module $(\text{c-Ind}_{w^{-1}P^-(L)w\cap N(L)}^{N(L)} \pi_P^w)^{N_1}$, que $F(M_n) \subseteq M_{n-1}$ si $n > 0$, et que :

$$(\text{c-Ind}_{w^{-1}P^-(L)w\cap N(L)}^{N(L)} \pi_P^w)^{N_1} = \bigcup_{n\geq 0} M_n.$$

Si $M \subseteq (\text{c-Ind}_{w^{-1}P^-(L)w\cap N(L)}^{N(L)} \pi_P^w)^{N_1}$ est de type fini sur $A[\![X]\!][F]$, il existe donc un entier $n \geq 0$ tel que $M \subseteq M_n$ d'où on déduit $F^n(M) \subseteq F^n(M_n) \subseteq M_0$.

(ii) Par le preuve du (i), $M_0 = (\mathrm{Ind}_{w^{-1}P^-(L)w\cap N_0}^{N_0} \pi_P^w)^{N_1}$ est stable par F dans $(\text{c-Ind}_{w^{-1}P^-(L)w\cap N(L)}^{N(L)} \pi_P^w)^{N_1}$. Comme M_0 est clairement stable par $\mathbb{Z}_p^\times$ (cf. (34)), c'est donc un sous-objet dans Mod_A. □

Proposition 6.7. *Pour tout $w \in K_P$, on a un isomorphisme dans $\widehat{\Phi\Gamma}_A^{\text{ét}}$:*

$$D_\xi^\vee(\text{c-Ind}_{w^{-1}P^-(L)w\cap N(L)}^{N(L)} \pi_P^w) \xrightarrow{\sim} D^\vee\big((\mathrm{Ind}_{w^{-1}P^-(L)w\cap N_0}^{N_0} \pi_P^w)^{N_1}\big).$$

Démonstration. Le (i) du lemme 6.6 montre que :

$$\mathcal{C}_w(\pi_P)^{N_1}/(\mathrm{Ind}_{w^{-1}P^-(L)w\cap N_0}^{N_0} \pi_P^w)^{N_1}$$

est un $A[F]$-module de torsion. Le résultat découle donc de la proposition 2.7. □

On démontre maintenant la proposition 6.2. Par la proposition 6.7, il suffit de montrer que tout sous-$A[\![X]\!][F]$-module M de $(\mathrm{Ind}_{w^{-1}P^-(L)w\cap N_0}^{N_0} \pi_P^w)^{N_1}$ vérifiant les conditions (1) est tel que $M^\vee[1/X] = 0$ si $w \neq 1$. Comme $w^{-1}N_{P^-}(L)w$ agit trivialement sur π_P^w, on a une injection N_0-équivariante (qui n'est pas un isomorphisme si $P \neq B$) :

$$\mathrm{Ind}_{w^{-1}P^-(L)w\cap N_0}^{N_0} \pi_P^w \hookrightarrow \mathcal{C}\big((w^{-1}N_{P^-}(L)w \cap N_0)\backslash N_0, \pi_P^w\big) \tag{35}$$

où le terme de droite désigne le A-module des fonctions localement constantes avec action de N_0 par translation à droite (et triviale sur π_P^w). Cette injection en induit une de $A[\![X]\!]$-modules :

$$\begin{aligned}(\mathrm{Ind}_{w^{-1}P^-(L)w\cap N_0}^{N_0} \pi_P^w)^{N_1} &\hookrightarrow \mathcal{C}\big((w^{-1}N_{P^-}(L)w \cap N_0)\backslash N_0, \pi_P^w\big)^{N_1} \\ &\cong \mathcal{C}\big((w^{-1}N_{P^-}(L)w \cap N_0)\backslash N_0/N_1, \pi_P^w\big).\end{aligned}$$

Or, si $w \neq 1$, le lemme 6.5 implique que X agit par 0 sur ce dernier terme, donc aussi sur $(\mathrm{Ind}_{w^{-1}P^-(L)w\cap N_0}^{N_0} \pi_P^w)^{N_1}$, donc *a fortiori* sur tout $M \subseteq (\mathrm{Ind}_{w^{-1}P^-(L)w\cap N_0}^{N_0} \pi_P^w)^{N_1}$ vérifiant (1), donc enfin sur $M^\vee$ (cf. la preuve du lemme 2.6). On en déduit $M^\vee[1/X] = 0$ ce qui achève la preuve.

Lorsque $P = B$, on peut préciser la proposition 6.2.

Proposition 6.8. *Supposons $P = B$ et π_B localement admissible (comme représentation de $T(L)$), alors $\mathcal{C}_w(\pi_B)^{N_1}$ est un $A[F]$-module de torsion pour tout $w \in W\backslash\{1\}$ (en particulier on retrouve $D_\xi^\vee(\mathcal{C}_w(\pi_B)) = 0$ par le (iii) de la proposition 2.7).*

La preuve est le cas particulier $i = 0$ du (ii) du théorème 8.1 ci-après, auquel on renvoie le lecteur.

Remarque 6.9. Il est possible que, pour $P \neq B$ et π_P localement admissible (comme représentation de $L_P(L)$), le $A[F]$-module $\mathcal{C}_w(\pi_P)^{N_1}$ soit en fait encore de torsion pour $w \in K_P\backslash\{1\}$ (voir aussi à ce propos la remarque 8.7).

7. Le cas des induites paraboliques II

On démontre la proposition 6.3, ce qui achève la preuve du théorème 6.1.

On conserve les notations des sections précédentes et on suppose $P \neq G$ sinon il n'y a rien à montrer. On pose $N_{P,0} \overset{\text{déf}}{=} N_P(L) \cap N_0 = \prod_{\alpha \in R^+\backslash R_P^+} (N_\alpha(L) \cap N_0)$ et $N_{P,1} \overset{\text{déf}}{=} N_P(L) \cap N_1 = N_{P,0} \cap N_1$. Comme N_0 est totalement décomposé, on a un produit semi-direct $N_0 = N_{L_P,0} N_{P,0}$ (avec $N_{P,0}$ distingué). Comme $(R^+\backslash R_P^+) \cap S \neq \varnothing$ (car $P \neq G$), on a par (24) une suite exacte courte :

$$0 \to N_{P,1} \to N_{P,0} \to \mathrm{Tr}_{L/\mathbb{Q}_p}(\mathcal{O}_L) \to 0$$

d'où on déduit que l'inclusion $N_{P,0} \subseteq N_0$ induit un isomorphisme $N_{P,0}/N_{P,1} \xrightarrow{\sim} N_0/N_1$. Notons que $N_{L_P,1} N_{P,1} \subsetneq N_1$ si $P \neq B$ et que $t N_{P,1} t^{-1} \subseteq N_{P,1}$, $t N_{L_P,1} t^{-1} \subseteq N_{L_P,1}$ (puisque $t N_P(L) t^{-1} = N_P(L)$, $t N_{L_P}(L) t^{-1} = N_{L_P}(L)$ et $t N_1 t^{-1} \subseteq N_1$) pour tout $t \in \xi(\mathbb{Z}_p\backslash\{0\})$.

Lemme 7.1. *Les inclusions $N_{L_P,0} \subseteq N_{L_P,0} N_{P,0}$ et $N_{P,0} \subseteq N_{L_P,0} N_{P,0}$ induisent un isomorphisme de groupes abéliens* :

$$N_{L_P,0}/N_{L_P,1} \times N_{P,0}/N_{P,1} \xrightarrow{\sim} N_0/(N_{L_P,1} N_{P,1}).$$

Démonstration. Par définition de $N_{L_P,1}$ et de $N_{P,1}$, on a :

$$\prod_{\alpha \in R_P^+\backslash S_P} (N_\alpha(L) \cap N_0) \subset N_{L_P,1} \quad \text{et} \quad \prod_{\alpha \in (R^+\backslash R_P^+)\backslash(S\backslash S_P)} (N_\alpha(L) \cap N_0) \subset N_{P,1}$$

qui entraîne $\prod_{\alpha \in R^+\backslash S} N_\alpha(L) \cap N_0 \subset N_{L_P,1} N_{P,1}$. On a par ailleurs un isomorphisme de groupes abéliens (rappelons que N_0 est totalement décomposé) :

$$N_0 \Big/ \Big(\prod_{\alpha \in R^+\backslash S} (N_\alpha(L) \cap N_0) \Big) \cong \prod_{\alpha \in S} (N_\alpha(L) \cap N_0) = \prod_{\alpha \in S_P} (N_\alpha(L) \cap N_0) \prod_{\alpha \in S\backslash S_P} (N_\alpha(L) \cap N_0). \quad (36)$$

De plus l'image de $N_{L_P,1}$ (resp. de $N_{P,1}$) dans le quotient (36) est clairement :

$$\mathrm{Ker}_{S_P} \overset{\text{déf}}{=} \mathrm{Ker}\Bigg(\prod_{\alpha \in S_P} (N_\alpha(L) \cap N_0) \xrightarrow{\sum_{\alpha \in S_P} \iota_\alpha} \mathcal{O}_L \xrightarrow{\psi \circ \mathrm{Tr}_{L/\mathbb{Q}_p}} \mathbb{Z}_p \Bigg)$$

(resp. avec partout $S \backslash S_P$ au lieu de S_P) de sorte que l'on a un isomorphisme de groupes abéliens :

$$(N_{L_P,1} N_{P,1}) \Big/ \Bigg(\prod_{\alpha \in R^+ \backslash S} (N_\alpha(L) \cap N_0) \Bigg) \xrightarrow{\sim} \mathrm{Ker}_{S_P} \times \mathrm{Ker}_{S \backslash S_P} . \tag{37}$$

En utilisant les isomorphismes :

$$N_{L_P,0}/N_{L_P,1} \xrightarrow{\sim} \Bigg(\prod_{\alpha \in S_P} (N_\alpha(L) \cap N_0) \Bigg) \Big/ \mathrm{Ker}_{S_P}$$

$$N_{P,0}/N_{P,1} \xrightarrow{\sim} \Bigg(\prod_{\alpha \in S \backslash S_P} (N_\alpha(L) \cap N_0) \Bigg) \Big/ \mathrm{Ker}_{S \backslash S_P}$$

on en déduit le résultat en faisant le quotient de (36) par (37). □

Via les isomorphismes $N_0/N_1 \cong \mathbb{Z}_p$, $N_{L_P,0}/N_{L_P,1} \xrightarrow{\sim} N_0/N_1 \cong \mathbb{Z}_p$ (si $P \neq B$) et $N_{P,0}/N_{P,1} \xrightarrow{\sim} N_0/N_1 \cong \mathbb{Z}_p$, on voit que la suite exacte courte de groupes abéliens $0 \to N_1/(N_{L_P,1} N_{P,1}) \to N_0/(N_{L_P,1} N_{P,1}) \to N_0/N_1 \to 0$ s'identifie à $0 \to 0 \to \mathbb{Z}_p \to \mathbb{Z}_p \to 0$ si $P = B$ et via le lemme 7.1 à :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}_p & \longrightarrow & \mathbb{Z}_p \times \mathbb{Z}_p & \longrightarrow & \mathbb{Z}_p & \longrightarrow & 0 \\ & & x & \longmapsto & (x, -x) & & & & \\ & & & & (z, y) & \longmapsto & z + y & & \end{array} \tag{38}$$

si $P \neq B$.

Rappelons que, par (33) et la proposition 6.7, on a :

$$D_\xi^\vee(\mathcal{C}_1(\pi_P)) = D_\xi^\vee(\text{c-Ind}_{P^-(L) \cap N(L)}^{N(L)} \pi_P) \xrightarrow{\sim} D^\vee((\mathrm{Ind}_{P^-(L) \cap N_0}^{N_0} \pi_P)^{N_1}). \tag{39}$$

La restriction à $N_{P,0}$ induit un isomorphisme :

$$\mathrm{Ind}_{P^-(L) \cap N_0}^{N_0} \pi_P \xrightarrow{\sim} \mathcal{C}(N_{P,0}, \pi_P) \cong \mathcal{C}(N_{P,0}, A) \otimes_A \pi_P \tag{40}$$

où le terme de droite désigne les fonctions localement constantes à valeurs dans π_P ou A, où l'action de $N_{P,0}$ est par translation à droite sur les fonctions (et triviale sur π_P), et où l'action de $N_{L_P,0}$ est donnée par :

$$(n_{L_P,0} h)(n_{P,0}) = \pi_P(n_{L_P,0}) \big(h(n_{L_P,0}^{-1} n_{P,0} n_{L_P,0}) \big) \tag{41}$$

si $n_{L_P,0} \in N_{L_P,0}$, $n_{P,0} \in N_{P,0}$ et $h \in \mathcal{C}(N_{P,0}, \pi_P)$.

Lemme 7.2. *On a un isomorphisme de $A[\![N_0/(N_{L_P,1}N_{P,1})]\!]$-modules* :

$$(\mathrm{Ind}_{P^-(L)\cap N_0}^{N_0}\pi_P)^{N_{L_P,1}N_{P,1}} \cong \mathcal{C}(N_{P,0}/N_{P,1}, \pi_P^{N_{L_P,1}}) \cong \mathcal{C}(N_{P,0}/N_{P,1}, A)\otimes_A \pi_P^{N_{L_P,1}}$$

où la structure de $A[\![N_0/(N_{L_P,1}N_{P,1})]\!]$-modules à droite est la structure évidente de $A[\![N_{P,0}/N_{P,1}]\!]\widehat{\otimes}_A A[\![N_{L_P,0}/N_{L_P,1}]\!]$-modules via l'isomorphisme du lemme 7.1.

Démonstration. Comme $N_{P,0}$ (et donc $N_{P,1}$) agit trivialement sur π_P, on a :

$$(\text{c-Ind}_{P^-(L)\cap N_0}^{N_0}\pi_P)^{N_{P,1}} \cong \mathcal{C}(N_{P,0}/N_{P,1}, \pi_P)$$

par (40). Par le lemme 7.1, l'action par conjugaison (41) de $N_{L_P,0}$ (et donc de $N_{L_P,1}$) sur $N_{P,0}$ devient triviale dans le quotient abélien $N_{P,0}/N_{P,1}$. On en déduit facilement le lemme. □

Supposons dans un premier temps $P \neq B$. Le groupe $N_{L_P,0}/N_{L_P,1} \cong \mathbb{Z}_p$ agit naturellement sur $\pi_P^{N_{L_P,1}}$ et via l'isomorphisme $N_{P,0}/N_{P,1} \cong \mathbb{Z}_p$ précédent, on a une injection :

$$\eta : \pi_P^{N_{L_P,1}} \hookrightarrow \mathcal{C}(N_{P,0}/N_{P,1}, \pi_P^{N_{L_P,1}}), \quad v \longmapsto (x \mapsto x(v)) = \eta(v)$$

où $x \in N_{P,0}/N_{P,1}$ et $v \in \pi_P^{N_{L_P,1}}$. Rappelons que $\pi_P^{N_{L_P,1}}$ et :

$$\mathcal{C}(N_{P,0}/N_{P,1}, \pi_P^{N_{L_P,1}})^{N_1} \overset{\text{lemme 7.2}}{\cong} (\mathcal{C}(N_{P,0}, \pi_P)^{N_{L_P,1}N_{P,1}})^{N_1} \cong \mathcal{C}(N_{P,0}, \pi_P)^{N_1}$$

sont munis d'une structure d'objets de Mod_A (pour les groupes réductifs respectifs L_P et G, cf. §3 et (ii) du lemme 6.6).

Lemme 7.3. *L'injection η induit un isomorphisme dans* Mod_A :

$$\pi_P^{N_{L_P,1}} \xrightarrow{\sim} \mathcal{C}(N_{P,0}/N_{P,1}, \pi_P^{N_{L_P,1}})^{N_1}.$$

Démonstration. Il faut montrer que η induit un isomorphisme de $A[\![X]\!][F]$-modules qui commute aux actions de $\mathbb{Z}_p^\times$. Posons $N_1' \overset{\text{déf}}{=} N_{L_P,1}N_{P,1}$, un sous-groupe distingué de N_1 (cf. lemme 7.1). Par le lemme 7.1 et le lemme 7.2, on voit que l'action de $N_0/N_1' \cong N_{L_P,0}/N_{L_P,1} \times N_{P,0}/N_{P,1} \cong \mathbb{Z}_p \times \mathbb{Z}_p$ sur $\mathcal{C}(N_{P,0}/N_{P,1}, \pi_P^{N_{L_P,1}}) \cong \mathcal{C}(\mathbb{Z}_p, \pi_P^{N_{L_P,1}})$ est donnée par :

$$((z, y)(f))(x) = z(f(x + y)). \tag{42}$$

Par la suite exacte (38) et par (42), un élément $f \in \mathcal{C}(N_{P,0}/N_{P,1}, \pi_P^{N_{L_P,1}})$ est invariant sous N_1, ou de manière équivalente sous $N_1/N_1' \cong \mathbb{Z}_p$, s'il vérifie $y(f(x-y)) = f(x)$ pour tout $x \in \mathbb{Z}_p$ et tout $y \in \mathbb{Z}_p$. En posant $v \overset{\text{déf}}{=} f(0) \in \pi_P^{N_{L_P,1}}$ et en faisant $y = x$, on obtient $f(x) = x(v)$, ce qui montre la surjectivité de η.

Si $x_0 \in N_0/N_1 \cong \mathbb{Z}_p$ et $f = \eta(v) \in \mathcal{C}(N_{P,0}/N_{P,1}, \pi_P^{N_{L_P,1}})^{N_1}$, on a (via (38)) :

$$(x_0(f))(x) = \big((0, x_0)(f)\big)(x) = f(x + x_0) = (x + x_0)(v) = x(x_0(v)) = \eta(x_0(v))(x)$$

ce qui montre la compatibilité à l'action de $A[\![X]\!]$.

On montre la compatibilité à l'action de F, laissant celle à l'action de $\mathbb{Z}_p^\times$, analogue en plus facile, au lecteur. Comme $\xi(p)N_1'\xi(p)^{-1}\subseteq N_1'$, on peut définir pour tout $f\in\mathcal{C}(N_{P,0},\pi_P)^{N_1'}$:

$$\xi(p)\cdot_{N_1'} f \overset{\text{déf}}{=} \sum_{n_1'\in N_1'/\xi(p)N_1'\xi(p)^{-1}} n_1'\xi(p)f \ \in \mathcal{C}(N_{P,0},\pi_P)^{N_1'}.$$

Via $\mathcal{C}(N_{P,0},\pi_P)^{N_1'}\cong\mathcal{C}(\mathbb{Z}_p,\pi_P^{N_{L_P,1}})$ (lemme 7.2), un petit calcul montre que cette action est explicitement donnée par :

$$(\xi(p)\cdot_{N_1'} f)(x) \ = \sum_{n_{L_P,1}\in N_{L_P,1}/\xi(p)N_{L_P,1}\xi(p)^{-1}} n_{L_P,1}\xi(p)(f(x/p)) \tag{43}$$

où $f(x/p)=0$ si $x\in\mathbb{Z}_p\backslash p\mathbb{Z}_p$. Par ailleurs, pour tout $f\in\mathcal{C}(N_{P,0},\pi_P)^{N_1}$ on a l'égalité suivante dans $\mathcal{C}(N_{P,0},\pi_P)^{N_1}$:

$$\sum_{n_1\in N_1/\xi(p)N_1\xi(p)^{-1}} n_1\xi(p)f \ = \sum_{\bar{n}_1\in(N_1/N_1')/\xi(p)(N_1/N_1')\xi(p)^{-1}} \bar{n}_1(\xi(p)\cdot_{N_1'} f). \tag{44}$$

(On laisse cette vérification facile au lecteur ; considérer la chaîne d'inclusions $\xi(p)N_1\xi(p)^{-1}\subseteq N_1'(\xi(p)N_1\xi(p)^{-1})\subseteq N_1$ comme dans la preuve du lemme 4.1 où $N_1'(\xi(p)N_1\xi(p)^{-1})$ est le sous-groupe de N_1 engendré par N_1' et $\xi(p)N_1\xi(p)^{-1}$, et remarquer que $N_1'\cap\xi(p)N_1\xi(p)^{-1}=\xi(p)N_1'\xi(p)^{-1}$.) En combinant (43), (44) et (42) (appliqué avec $(z,y)=(i,-i)\in N_1/N_1'\subseteq N_0/N_1'$), on voit que l'action de F sur $f=\eta(v)\in\mathcal{C}(N_{P,0},\pi_P)^{N_1}\cong\mathcal{C}(\mathbb{Z}_p,\pi_P^{N_{L_P,1}})^{N_1/N_1'}$ est explicitement donnée par :

$$F(\eta(v))(x)=\sum_{i=0}^{p-1} i\Bigg(\sum_{n_{L_P,1}\in N_{L_P,1}/\xi(p)N_{L_P,1}\xi(p)^{-1}} n_{L_P,1}\xi(p)\Big(\frac{x-i}{p}(v)\Big)\Bigg) \tag{45}$$

où $((x-i)/p)(v)=0$ si x n'est pas congru à i modulo p. En notant $i_x\in\{0,\dots,p-1\}$ l'unique entier congru à $x\in\mathbb{Z}_p$ modulo p et $n_x\in\xi(p)N_{L_P,0}\xi(p)^{-1}\subseteq N_{L_P,0}$ un relevé de $x-i_x\in p\mathbb{Z}_p$ via $\xi(p)N_{L_P,0}\xi(p)^{-1}/\xi(p)N_{L_P,1}\xi(p)^{-1}\xrightarrow{\sim}p\mathbb{Z}_p$, (45) se récrit :

$$F(\eta(v))(x)=i_x\Bigg(\sum_{N_{L_P,1}/\xi(p)N_{L_P,1}\xi(p)^{-1}} n_{L_P,1}n_x\xi(p)(v)\Bigg)$$

ou encore :

$$F(\eta(v))(x)=x\Bigg(\sum_{N_{L_P,1}/\xi(p)N_{L_P,1}\xi(p)^{-1}} n_x^{-1}n_{L_P,1}n_x\xi(p)(v)\Bigg). \tag{46}$$

Comme $N_{L_P,1}$ est distingué dans $N_{L_P,0}$ et $\xi(p)N_{L_P,1}\xi(p)^{-1}$ est distingué dans $\xi(p)N_{L_P,0}\xi(p)^{-1}$, l'ensemble $\{n_x^{-1}n_{L_P,1}n_x\}$ dans la somme ci-dessus est encore

un système de représentants de $N_{L_P,1}/\xi(p)N_{L_P,1}\xi(p)^{-1}$ dans $N_{L_P,1}$ pour chaque $x \in \mathbb{Z}_p$. On en déduit que (46) se récrit :

$$F(\eta(v))(x) = x\Bigg(\sum_{N_{L_P,1}/\xi(p)N_{L_P,1}\xi(p)^{-1}} n_{L_P,1}\xi(p)(v)\Bigg) = x(F(v))$$

pour l'action de F sur $\pi_P^{N_{L_P,1}}$ à droite. Cela montre $F(\eta(v)) = \eta(F(v))$. □

Par le lemme 7.3, on a donc $D^\vee\big(\mathcal{C}(N_{P,0}, \pi_P)^{N_1}\big) \xrightarrow{\sim} D_\xi^\vee(\pi_P)$ ce qui, avec (40) et (39), montre la proposition 6.3 lorsque $P \neq B$ (tous les isomorphismes étant par ailleurs clairement fonctoriels en π_P).

On suppose maintenant $P = B$. Par le lemme 7.2 on a un isomorphisme de $A[\![X]\!]$-modules $\mathcal{C}(N_0, \pi_B)^{N_1} \cong \mathcal{C}(\mathbb{Z}_p, A) \otimes_A \pi_B$. En munissant le terme de droite d'une action de $\mathbb{Z}_p\backslash\{0\}$ donnée par l'action de $\xi(\mathbb{Z}_p\backslash\{0\}) \subseteq T(L)$ sur π_B et par $f \mapsto (x \mapsto f(x/a))$ sur $\mathcal{C}(\mathbb{Z}_p, A)$ où $a \in \mathbb{Z}_p\backslash\{0\}$ et $f(x/a) = 0$ si $x/a \in \mathbb{Q}_p\backslash\mathbb{Z}_p$, on vérifie facilement qu'il s'agit d'un isomorphisme dans Mod_A (cf. (43) avec $N_1' = N_1$ et $N_{L_P,1} = \{1\}$).

Lemme 7.4. (i) *Si $M_B \subseteq \pi_B$ est un sous-A-module de type fini stable par $\xi(\mathbb{Z}_p\backslash\{0\})$ alors $\mathcal{C}(\mathbb{Z}_p, A) \otimes_A M_B$ est un sous-$A[\![X]\!][F]$-module de $\mathcal{C}(N_0, \pi_B)^{N_1} \cong \mathcal{C}(\mathbb{Z}_p, A) \otimes_A \pi_B$ stable par $\mathbb{Z}_p^\times$ qui vérifie les conditions* (1).

(i) *Tout sous-$A[\![X]\!][F]$-module de $\mathcal{C}(N_0, \pi_B)^{N_1}$ stable par $\mathbb{Z}_p^\times$ qui vérifie* (1) *est contenu dans $\mathcal{C}(\mathbb{Z}_p, A) \otimes_A M_B$ pour $M_B \subseteq \pi_B$ un sous-A-module de type fini stable par $\xi(\mathbb{Z}_p\backslash\{0\})$.*

Démonstration. (i) On a :

$$\mathrm{Hom}_A(\mathcal{C}(\mathbb{Z}_p, A) \otimes_A M_B, A) \cong A[\![X]\!] \otimes_A M_B^\vee$$

qui montre que $\mathcal{C}(\mathbb{Z}_p, A) \otimes_A M_B$ est un $A[\![X]\!]$-module admissible puisque $M_B^\vee$ est de type fini sur A. Montrons qu'il est de type fini sur $A[\![X]\!][F]$. Par dévissage ($\mathcal{C}(\mathbb{Z}_p, A)$ est plat sur A), on se ramène au cas $A = k_E$. Comme $k_E'[\![X]\!][F] \cong k_E' \otimes_{k_E} (k_E[\![X]\!][F])$ est de type fini sur $k_E[\![X]\!][F]$ pour toute extension finie k_E' de k_E, on peut quitte à étendre les scalaires supposer que $M_B|_{\xi(\mathbb{Q}_p^\times)}$ est une extension successive de caractères lisses de $\xi(\mathbb{Q}_p^\times)$ (à valeurs dans $k_E^\times$). Par dévissage encore, on est donc ramené au cas $\dim_{k_E} M_B = 1$ et, quitte à twister l'action de $\xi(\mathbb{Z}_p\backslash\{0\})$ sur $\mathcal{C}(\mathbb{Z}_p, k_E) \otimes_{k_E} M_B$, on peut même supposer que $M_B|_{\xi(\mathbb{Q}_p^\times)}$ est le caractère trivial. On est finalement ramené à $\mathcal{C}(\mathbb{Z}_p, k_E)$ qui est bien de type fini sur $k_E[\![X]\!][F]$, engendré par exemple par la fonction $\mathbf{1}_{\mathbb{Z}_p}$.

(ii) Soit $M \subseteq \mathcal{C}(\mathbb{Z}_p, A) \otimes_A \pi_B$ stable par $\mathbb{Z}_p^\times$ et qui vérifie (1). En prenant $\mathrm{Hom}_A(\cdot, A)$, on a une surjection de $A[\![X]\!][F]$-modules $A[\![X]\!]\widehat{\otimes}_A \pi_B^\vee \twoheadrightarrow M^\vee$ compatible à $\mathbb{Z}_p^\times$ où $M^\vee$ est un $A[\![X]\!]$-module de type fini, d'où une surjection de A-modules $\pi_B^\vee \twoheadrightarrow M^\vee/XM^\vee$ qui commute à F et $\mathbb{Z}_p^\times$. Comme $F = \xi(p)$ est ici bijectif sur π_B,

donc sur $\pi_B^\vee$, il est surjectif (et A-linéaire) sur le A-module de type fini $M^\vee/XM^\vee$, donc aussi bijectif. Par un argument classique (parfois appelé "Dwork's trick"), on en déduit une section $A[F]$-linéaire canonique $s : M^\vee/XM^\vee \hookrightarrow M^\vee$ de la surjection $M^\vee \twoheadrightarrow M^\vee/XM^\vee$ qui commute avec la section évidente $\pi_B^\vee \hookrightarrow A[\![X]\!]\widehat{\otimes}_A\pi_B^\vee$ et avec l'action de $\mathbb{Z}_p^\times$. Autrement dit la surjection $A[\![X]\!]\widehat{\otimes}_A\pi_B^\vee \twoheadrightarrow M^\vee$ se factorise comme suit :

$$A[\![X]\!]\widehat{\otimes}_A\pi_B^\vee \twoheadrightarrow A[\![X]\!]\otimes_A M^\vee/XM^\vee \xrightarrow{\mathrm{Id}\otimes s} M^\vee.$$

Et on voit que $M_B \overset{\text{déf}}{=} \mathrm{Hom}_A(M^\vee/XM^\vee, A)$ convient. □

Le lemme suivant est un exercice simple sur les (φ,Γ)-modules que l'on laisse au lecteur.

Lemme 7.5. *Soit M un A-module de type fini muni d'une action A-linéaire lisse de $\mathbb{Q}_p^\times$, $V(M)$ la représentation de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ sur A associée par la réciprocité locale et $D(M)$ le (φ,Γ)-module associé à $V(M)$ par le foncteur covariant de [Fontaine 1990, théorème A.3.4.3]. On a $D(M)\cong A[\![X]\!][1/X]\otimes_A M$ où l'action de $\Gamma\cong\mathbb{Z}_p^\times$ est l'unique action $A[\![X]\!][1/X]$-semi-linéaire donnée par l'action de $\mathbb{Z}_p^\times$ sur M et où l'action de φ est l'unique action semi-linéaire donnée par l'action de p sur M.*

Par le lemme 7.4, on obtient un isomorphisme dans $\widehat{\Phi\Gamma}_A^{\text{ét}}$:

$$D^\vee(\mathcal{C}(N_0,\pi_B)^{N_1}) \cong \varprojlim_{M_B}(A[\![X]\!][1/X]\otimes_A M_B^\vee) \tag{47}$$

où la limite projective est prise sur les éléments M_B de $\mathcal{M}(\pi_B)$ et où l'action de φ et de $\mathbb{Z}_p^\times$ (ou de manière équivalente de $\mathbb{Q}_p^\times$) sur $M_B^\vee$ est donnée par $(\varphi(f))(m) = f(\xi(p)^{-1}(m))$ et $(x(f))(m) = f(\xi(x)^{-1}(m))$, $x\in\mathbb{Z}_p^\times$. Par le lemme 7.5 appliqué à $M_B^\vee$ et le fait que le foncteur (φ,Γ)-module commute à la dualité, on a $A[\![X]\!][1/X]\otimes_A M_B^\vee \cong D^\vee(M_B)$ pour $M_B\in\mathcal{M}(\pi_B)$ (cf. § 3), d'où on déduit $D^\vee(\mathcal{C}(N_0,\pi_B)^{N_1}) \cong D_\xi^\vee(\pi_B)$ par (47). Par (40) et (39), on en déduit la proposition 6.3 lorsque $P = B$ (la fonctorialité étant là aussi claire).

Exemple 7.6. Soit $\chi : T(L)\to A^\times$ un caractère lisse, alors $D_\xi^\vee(\mathrm{Ind}_{B^-(L)}^{G(L)}\chi)$ est le (φ,Γ)-module du dual du caractère de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ sur A donné (via la réciprocité locale) par $\mathbb{Q}_p^\times\to A^\times$, $x\mapsto\chi(\xi(x))$.

Proposition 7.7. *Supposons π_B localement admissible* (*comme représentation de $T(L)$*), *alors le $A[\![X]\!][F]$-module $\mathcal{C}_1(\pi_B)^{N_1}$ satisfait la propriété Ad* (définition 2.2).

Démonstration. En procédant comme dans la preuve de la proposition 6.7, par le (ii) du lemme 2.5 il suffit de montrer le résultat pour le sous-$A[\![X]\!][F]$-module $\mathcal{C}(N_0,\pi_B)^{N_1}\cong\mathcal{C}(\mathbb{Z}_p,A)\otimes_A\pi_B$. Comme π_B est un $A[F]$-module de torsion (car π_B est localement admissible), tout sous-$A[\![X]\!][F]$-module de type fini de $\mathcal{C}(\mathbb{Z}_p,A)\otimes_A$

π_B est contenu dans $\mathcal{C}(\mathbb{Z}_p, A) \otimes_A M_B$ où $M_B \subseteq \pi_B$ est un sous-A-module de type fini stable par F. On en déduit le résultat par le (i) du lemme 7.4 et le (i) du lemme 2.1. □

8. Le cas des $H^i(N_1, \mathcal{C}_w(\pi_B))$ pour $i \geq 1$

On montre que les $A[F]$-modules $H^i(N_1, \mathcal{C}_w(\pi_B))$ (cf. fin du § 3) sont très souvent de torsion.

On garde les notations des sections précédentes.

Théorème 8.1. *Soit π_B une représentation lisse de $T(L)$ sur A.*

(i) *Le $A[F]$-module $H^i(N_1, \mathcal{C}_1(\pi_B))$ est de torsion pour tout $i \geq 1$.*

(ii) *Si π_B est de plus localement admissible (comme représentation de $T(L)$), le $A[F]$-module $H^i(N_1, \mathcal{C}_w(\pi_B))$ est de torsion pour tout $i \geq 0$ et tout $w \in W\backslash\{1\}$.*

Le théorème 8.1 va résulter de la combinaison de quatre propositions énoncées (et démontrées) ci-dessous.

Pour tout $w \in W$, posons $\mathcal{C}_{w,0}(\pi_B) \overset{\text{déf}}{=} \mathcal{C}((w^{-1}N^-(L)w \cap N_0)\backslash N_0, \pi_B^w)$ (notons que (35) est un isomorphisme lorsque $P = B$). C'est un sous-A-module de $\mathcal{C}_w(\pi_B)$ stable par l'action de N_0 et de $\xi(\mathbb{Z}_p\backslash\{0\})$ (pour cette dernière cela découle de (34), voir la preuve du (i) du lemme 6.6). En particulier on peut définir pour tout $i \geq 0$ et tout $w \in W$ des objets de Mod_A, $H^i(N_1, \mathcal{C}_{w,0}(\pi_B))$ et $H^i(N_1, \mathcal{C}_w(\pi_B)/\mathcal{C}_{w,0}(\pi_B))$, comme à la fin du § 3.

Proposition 8.2. *Si les assertions (i) et (ii) du théorème 8.1 sont vraies avec $\mathcal{C}_{1,0}(\pi_B)$ et $\mathcal{C}_{w,0}(\pi_B)$ au lieu de $\mathcal{C}_1(\pi_B)$ et $\mathcal{C}_w(\pi_B)$, alors le théorème 8.1 est vrai.*

Démonstration. La suite exacte courte :

$$0 \to \mathcal{C}_{w,0}(\pi_B) \to \mathcal{C}_w(\pi_B) \to \mathcal{C}_w(\chi)/\mathcal{C}_{w,0}(\pi_B) \to 0$$

donne des suites exactes dans Mod_A pour tout $i \geq 1$:

$$H^{i-1}(N_1, \mathcal{C}_w(\pi_B)/\mathcal{C}_{w,0}(\pi_B)) \to H^i(N_1, \mathcal{C}_{w,0}(\pi_B)) \to H^i(N_1, \mathcal{C}_w(\pi_B)) \to H^i(N_1, \mathcal{C}_w(\pi_B)/\mathcal{C}_{w,0}(\pi_B)). \quad (48)$$

La même preuve que celle de [Hauseux 2014, lemme 3.3.1] (voir aussi celle du (i) du lemme 6.6) montre que $\xi(p)$ est localement nilpotent sur $\mathcal{C}_w(\pi_B)/\mathcal{C}_{w,0}(\pi_B)$ pour tout $w \in W$, et donc F est localement nilpotent sur $H^i(N_1, \mathcal{C}_w(\chi)/\mathcal{C}_{w,0}(\pi_B))$ pour tout $i \geq 0$ et tout $w \in W$ (cf. (14)). En particulier $H^i(N_1, \mathcal{C}_w(\pi_B)/\mathcal{C}_{w,0}(\pi_B))$ est toujours de $A[F]$-torsion. Par le (i) du lemme 2.5 et (48), cela montre la proposition. □

Proposition 8.3. *Le $A[F]$-module $H^i(N_1, \mathcal{C}_{1,0}(\pi_B))$ est nul pour tout $i \geq 1$.*

Démonstration. Comme $N_0/N_1 \cong \mathbb{Z}_p$ est de dimension 1, on a pour tout $i \geq 1$ une suite exacte courte déduite de la suite spectrale de Hochschild–Serre (cf. [Hauseux 2014, §3.2(12)]) :

$$0 \to H^1\big(\mathbb{Z}_p, H^{i-1}(N_1, \mathcal{C}_{1,0}(\pi_B))\big) \to H^i(N_0, \mathcal{C}_{1,0}(\pi_B)) \to H^0\big(\mathbb{Z}_p, H^i(N_1, \mathcal{C}_{1,0}(\pi_B))\big) \to 0. \quad (49)$$

Comme $\mathcal{C}_{1,0}(\pi_B) = \mathcal{C}(N_0, \pi_B)$ est une représentation injective de N_0 (agissant par translation à droite sur les fonctions), on a $H^i(N_0, \mathcal{C}_{1,0}(\pi_B)) = 0$ pour $i \geq 1$. Par (49) on en déduit $H^0\big(\mathbb{Z}_p, H^i(N_1, \mathcal{C}_{1,0}(\pi_B))\big) = 0$. Comme $\mathbb{Z}_p$ est un pro-p-groupe, un A-module non nul avec une action lisse de $\mathbb{Z}_p$ a toujours des vecteurs non nuls invariants sous $\mathbb{Z}_p$, d'où $H^i(N_1, \mathcal{C}_{1,0}(\pi_B)) = 0$ pour $i \geq 1$. □

Par la proposition 8.2, cela montre le (i) du théorème 8.1.

On fixe dans la suite $w \neq 1$. On va montrer le (ii) du théorème 8.1 pour $\mathcal{C}_{w,0}(\pi_B)$. Par un dévissage sur A évident et le (i) du lemme 2.5, on peut supposer $A = k_E$. Comme π_B est une représentation lisse localement admissible du groupe commutatif $T(L)$ sur k_E, on peut l'écrire comme limite inductive $\pi_B = \varinjlim_\iota \pi_{B,\iota}$ de représentations $\pi_{B,\iota}$ de $T(L)$ de dimension finie sur k_E. Comme N_0 est compact, toute fonction de $\mathcal{C}_{w,0}(\pi_B)$ est à valeurs dans une sous-représentation $\pi_{B,\iota}^w$ de π_B^w de dimension finie sur k_E, de sorte que l'on a $\mathcal{C}_{w,0}(\pi_B) = \varinjlim_\iota \mathcal{C}_{w,0}(\pi_{B,\iota})$ (avec des notations évidentes). Comme la cohomologie (continue) commute aux limites inductives, on voit qu'il suffit de traiter le cas où π_B est de dimension finie sur k_E, ce que l'on suppose dans la suite. On va en fait montrer que $H^i(N_1, \mathcal{C}_{w,0}(\pi_B))$ est alors aussi de dimension finie sur k_E pour tout $i \geq 0$, ce qui implique qu'il est *a fortiori* de torsion comme $k_E[F]$-module.

On note $N^S \overset{\text{déf}}{=} \prod_{\alpha \in R^+ \setminus S} N_\alpha$: c'est un sous-groupe algébrique fermé normal de N de quotient abélien isomorphe à $\prod_{\alpha \in S} N_\alpha$. De plus, on a $N^S(L) \cap N_0 \subseteq N_1 \subseteq N_0$. Soit $R_w^+ \overset{\text{déf}}{=} R^+ \cap w^{-1}(R^+)$, comme N_0 est totalement décomposé, on a :

$$\prod_{\alpha \in R_w^+} (N_\alpha(L) \cap N_0) \cong w^{-1}N(L)w \cap N_0 \xrightarrow{\sim} (w^{-1}N^-(L)w \cap N_0)\backslash N_0. \quad (50)$$

Proposition 8.4. *Il existe une suite* $0 = N_0^S \subseteq N_1^S \subseteq N_2^S \subseteq \cdots \subseteq N_m^S = N^S$ *de sous-groupes algébriques fermés de* N^S *vérifiant les conditions suivantes* :

(i) N_j^S *est un sous-groupe normal de* N *pour tout* $j \in \{0, \ldots, m\}$;

(ii) *pour tout* $j \in \{1, \ldots, m\}$, *ou bien l'action de* $(N_j^S(L) \cap N_0)/(N_{j-1}^S(L) \cap N_0)$ *sur* $\mathcal{C}_{w,0}(\pi_B)^{N_{j-1}^S(L) \cap N_0}$ *est triviale, ou bien* $\mathcal{C}_{w,0}(\pi_B)^{N_{j-1}^S(L) \cap N_0}$ *est une représentation injective lisse de* $(N_j^S(L) \cap N_0)/(N_{j-1}^S(L) \cap N_0)$ *sur* k_E.

Démonstration. Si N^S est trivial (i.e., si $R^+ = S$), il n'y a rien à montrer. On suppose donc N^S non trivial dans la suite.

Construisons d'abord N_1^S. Soit $\alpha_1 \in R^+\backslash S$ une racine de hauteur maximale dans R^+ (cf. par exemple [Breuil et Herzig 2015, Remark 2.5.3]), alors N_{α_1} est un sous-groupe algébrique de N^S normal dans N par [Digne et Michel 1991, Theorem 0.31(iv)] (en fait N_{α_1} commute même à tout élément de N par [loc. cit.]).

Supposons $w(\alpha_1) \in R^-$, i.e., $\alpha_1 \notin R_w^+$ ou de manière équivalente :

$$N_{\alpha_1} \subseteq w^{-1}N^-w \cap N,$$

alors pour tout $n_0 \in N_0$ et $n_{\alpha_1} \in N_{\alpha_1}(L) \cap N_0$ on a dans $(w^{-1}N^-(L)w \cap N_0)\backslash N_0$:

$$\begin{aligned}(w^{-1}N^-(L)w \cap N_0)n_0n_{\alpha_1} &= (w^{-1}N^-(L)w \cap N_0)n_0n_{\alpha_1}n_0^{-1}n_0\\ &= (w^{-1}N^-(L)w \cap N_0)n_0\end{aligned}$$

puisque $n_0n_{\alpha_1}n_0^{-1} \in N_{\alpha_1}(L) \cap N_0$ et $N_{\alpha_1}(L) \cap N_0 \subseteq w^{-1}N^-(L)w \cap N_0$. Donc l'action de $N_{\alpha_1}(L) \cap N_0$ sur $\mathcal{C}_{w,0}(\pi_B)$ est triviale.

Supposons $w(\alpha_1) \in R^+$, i.e., $\alpha_1 \in R_w^+$ ou de manière équivalente $N_{\alpha_1} \subseteq w^{-1}Nw \cap N$. En utilisant (50), on voit que l'on a un isomorphisme compatible à l'action de $N_{\alpha_1}(L) \cap N_0$:

$$\mathcal{C}_{w,0}(\pi_B)|_{N_{\alpha_1}(L)\cap N_0} \cong \bigotimes_{\alpha\in R_w^+} \mathcal{C}(N_\alpha(L) \cap N_0, \pi_B^w)$$

(le produit tensoriel étant sur k_E) où l'action de $N_{\alpha_1}(L) \cap N_0$ est triviale sur $\mathcal{C}(N_\alpha(L) \cap N_0, \pi_B^w)$ si $\alpha \neq \alpha_1$ et est la translation à droite sur $\mathcal{C}(N_{\alpha_1}(L) \cap N_0, \pi_B^w)$ (π_B^w ne jouant aucun rôle). Comme $\mathcal{C}(N_{\alpha_1}(L) \cap N_0, \pi_B^w)$ est une représentation injective de $N_{\alpha_1}(L) \cap N_0$ sur k_E, on voit que $\mathcal{C}_{w,0}(\pi_B)|_{N_{\alpha_1}(L)\cap N_0}$ est une somme directe de représentations injectives de $N_{\alpha_1}(L) \cap N_0$ sur k_E, donc est injective.

On peut poser $N_1^S \overset{\text{déf}}{=} N_{\alpha_1}$. Si $N_1^S = N^S$, c'est fini. Sinon, en remplaçant N par N/N_1^S, N^S par N^S/N_1^S, R^+ par $R^+\backslash\{\alpha_1\}$, R_w^+ par $R_w^+\backslash\{\alpha_1\}$ (qui peut être égal à R_w^+ selon les cas) et $\mathcal{C}_{w,0}(\pi_B)$ par :

$$\begin{aligned}\mathcal{C}_{w,0}(\pi_B)^{N_1^S(L)\cap N_0} &\cong \mathcal{C}\big((w^{-1}N^-(L)w \cap N_0)\backslash N_0/(N_{\alpha_1}(L) \cap N_0), \pi_B^w\big)\\ &\cong \mathcal{C}\big(\big((w^{-1}N^-(L)wN_{\alpha_1}(L)) \cap N_0\big)\backslash N_0, \pi_B^w\big)\\ &\cong \bigotimes_{\alpha\in R_w^+\backslash\{\alpha_1\}} \mathcal{C}(N_\alpha(L) \cap N_0, \pi_B^w),\end{aligned}$$

le même argument donne $\alpha_2 \in (R^+\backslash\{\alpha_1\})\backslash S$ (de hauteur maximale dans $R^+\backslash\{\alpha_1\}$) tel que N_{α_2} est un sous-groupe algébrique de N^S/N_1^S normal dans N/N_1^S, et tel que l'action de $N_{\alpha_2}(L) \cap N_0$ sur $\mathcal{C}_{w,0}(\pi_B)^{N_1^S(L)\cap N_0}$ par translation à droite est soit triviale soit "injective" selon que $w(\alpha_2) \in R^-$ ou $w(\alpha_2) \in R^+$. On pose alors $N_2^S \overset{\text{déf}}{=} N_1^SN_{\alpha_2} = N_{\alpha_2}N_1^S \subseteq N^S$, qui est bien normal dans N. On poursuit par une récurrence évidente, qui s'arrête lorsque $N_i^S = N^S$. □

Par le (i) de la proposition 8.4, $N_{j,0}^S \overset{\text{déf}}{=} N_j^S(L)\cap N_0$ est en particulier un sous-groupe normal de N_1 pour tout $j\in\{0,\dots,m\}$.

Proposition 8.5. *Pour tout $i\geq 0$ et tout $j\in\{0,\dots,m\}$, le k_E-espace vectoriel $H^i\big(N_1/N_{j,0}^S, \mathcal{C}_{w,0}(\pi_B)^{N_{j,0}^S}\big)$ est de dimension finie* (rappelons que $\dim_{k_E}\pi_B<+\infty$).

Démonstration. On fait une récurrence descendante sur j.

Supposons d'abord $j=m$. Alors $N_0/N_{m,0}^S = N_0/(N^S(L)\cap N_0)$ est le groupe abélien $\prod_{\alpha\in S}(N_\alpha(L)\cap N_0)$ et

$$\mathcal{C}_{w,0}(\pi_B)^{N^S(L)\cap N_0} = \mathcal{C}\Big(\prod_{\alpha\in S_w}(N_\alpha(L)\cap N_0),\pi_B^w\Big)$$

où $S_w \overset{\text{déf}}{=} S\cap R_w^+$. Comme $w\neq 1$, il existe $\beta\in S\backslash S_w$. On fixe un tel β et on définit une injection (d'ensembles) :

$$j_{w,\beta}:\prod_{\alpha\in S_w}(N_\alpha(L)\cap N_0)\hookrightarrow N_1,\quad n\mapsto \iota_\beta^{-1}(-\ell(n))n$$

où $\iota_\beta^{-1}(-\ell(n))$ est l'unique élément de $N_\beta(L)\cap N_0$ dont l'image par ι_β est $-\ell(n)\in\mathcal{O}_L$ (cf. (24), on a bien alors $\iota_\beta^{-1}(-\ell(n))n\in N_1$). Composée avec la projection $N_1\twoheadrightarrow N_1/(N^S(L)\cap N_0)$, $j_{w,\beta}$ induit une injection de groupes abéliens (en fait de $\mathbb{Z}_p$-modules libres de type fini) :

$$\overline{j_{w,\beta}}:\prod_{\alpha\in S_w}(N_\alpha(L)\cap N_0)\hookrightarrow N_1/(N^S(L)\cap N_0)$$

dont le conoyau est sans torsion (regarder le conoyau dans $N_0/(N^S(L)\cap N_0)\cong\prod_{\alpha\in S}(N_\alpha(L)\cap N_0)$). Notons $N_{1,w,\beta}$ un facteur direct de $\prod_{\alpha\in S_w}(N_\alpha(L)\cap N_0)$ dans $N_1/(N^S(L)\cap N_1)$ via l'injection $\overline{j_{w,\beta}}$ ($N_{1,w,\beta}$ est donc isomorphe à une somme de copies de $\mathbb{Z}_p$). Par la suite spectrale de Hochschild–Serre, il suffit de montrer que le k_E-espace vectoriel :

$$H^{i_1}\Big(N_{1,w,\beta},\ H^{i_2}\Big(\prod_{\alpha\in S_w}(N_\alpha(L)\cap N_0),\mathcal{C}\Big(\prod_{\alpha\in S_w}(N_\alpha(L)\cap N_0),\pi_B^w\Big)\Big)\Big)$$

est de dimension finie sur k_E pour tout couple d'entiers (i_1,i_2). Comme il est nul si $i_2>0$ (par injectivité de $\mathcal{C}\big(\prod_{\alpha\in S_w}(N_\alpha(L)\cap N_0),\pi_B^w\big)$), on peut supposer $i_2=0$ auquel cas il reste $H^{i_1}(N_{1,w,\beta},\pi_B^w)$ qui est de dimension finie car $N_{1,w,\beta}$ est un pro-p-groupe analytique compact et sans torsion et π_B^w est de dimension finie, cf. par exemple [Serre 1994, §I.4.5].

Supposons maintenant $H^i\big(N_1/N_{j+1,0}^S,\mathcal{C}_{w,0}(\pi_B)^{N_{j+1,0}^S}\big)$ de dimension finie pour un $j\in\{0,\dots,m-1\}$ et tout entier $i\geq 0$, et montrons que $H^i\big(N_1/N_{j,0}^S,\mathcal{C}_{w,0}(\pi_B)^{N_{j,0}^S}\big)$

est de dimension finie pour tout entier $i \geq 0$. Par la suite spectrale de Hochschild–Serre appliquée à :

$$1 \to N^S_{j+1,0}/N^S_{j,0} \to N_1/N^S_{j,0} \to N_1/N^S_{j+1,0} \to 1,$$

il suffit de montrer que le k_E-espace vectoriel :

$$H^{i_1}\big(N_1/N^S_{j+1,0}, H^{i_2}\big(N^S_{j+1,0}/N^S_{j,0}, \mathcal{C}_{w,0}(\pi_B)^{N^S_{j,0}}\big)\big)$$

est de dimension finie sur k_E pour tout couple d'entiers (i_1, i_2). Supposons d'abord que $\mathcal{C}_{w,0}(\pi_B)^{N^S_{j,0}}$ est une représentation injective de $N^S_{j+1,0}/N^S_{j,0}$ (cf. le (ii) de la proposition 8.4), alors comme dans le cas précédent seul reste à considérer $H^{i_1}\big(N_1/N^S_{j+1,0}, \mathcal{C}_{w,0}(\pi_B)^{N^S_{j+1,0}}\big)$ (les autres cas étant nuls), qui est de dimension finie par hypothèse de récurrence. Supposons maintenant que $N^S_{j+1,0}/N^S_{j,0}$ agit trivialement sur $\mathcal{C}_{w,0}(\pi_B)^{N^S_{j,0}}$. Alors on a un isomorphisme compatible à l'action de $N_1/N^S_{j+1,0}$:

$$H^{i_2}\big(N^S_{j+1,0}/N^S_{j,0}, \mathcal{C}_{w,0}(\pi_B)^{N^S_{j,0}}\big) \cong \mathcal{C}_{w,0}(\pi_B)^{N^S_{j,0}} \otimes_{k_E} H^{i_2}(N^S_{j+1,0}/N^S_{j,0}, k_E) \quad (51)$$

pour l'action usuelle de $N_1/N^S_{j+1,0}$ sur :

$$\mathcal{C}_{w,0}(\pi_B)^{N^S_{j,0}} \cong \mathcal{C}_{w,0}(\pi_B)^{N^S_{j+1,0}}$$

(provenant de l'action par translation à droite) et l'action naturelle de $N_1/N^S_{j+1,0}$ sur $H^{i_2}(N^S_{j+1,0}/N^S_{j,0}, k_E)$ obtenue en voyant k_E comme représentation triviale de $N_1/N^S_{j,0}$. Comme $N^S_{j+1,0}/N^S_{j,0}$ est un pro-p-groupe analytique compact et sans torsion, $H^{i_2}(N^S_{j+1,0}/N^S_{j,0}, k_E)$ est de dimension finie sur k_E ([Serre 1994, §I.4.5]), et comme $N_1/N^S_{j+1,0}$ est pro-p-groupe, on voit que $H^{i_2}(N^S_{j+1,0}/N^S_{j,0}, k_E)$ est une extension successive finie de représentations triviales de $N_1/N^S_{j+1,0}$ sur k_E. Ainsi la représentation (51) de $N_1/N^S_{j+1,0}$ est une extension successive finie de $\mathcal{C}_{w,0}(\pi_B)^{N^S_{j+1,0}}$. Par les suites exactes longues de cohomologie des groupes usuelles et un dévissage évident, il suffit donc de savoir que $H^{i_1}\big(N_1/N^S_{j+1,0}, \mathcal{C}_{w,0}(\pi_B)^{N^S_{j+1,0}}\big)$ est de dimension finie sur k_E pour tout $i_1 \geq 0$, ce qui est de nouveau l'hypothèse de récurrence. □

Par la proposition 8.2, le (ii) du théorème 8.1 découle du cas $j = 0$ de la proposition 8.5, ce qui achève la preuve du théorème 8.1.

On a le corollaire suivant immédiat par le (iii) de la proposition 2.7.

Corollaire 8.6. *Soit π_B une représentation lisse de $T(L)$ sur A.*

(i) *On a $D^\vee\big(H^i(N_1, \mathcal{C}_1(\pi_B))\big) = 0$ pour tout $i \geq 1$.*

(ii) *Si π_B est de plus localement admissible (comme représentation de $T(L)$), on a $D^\vee\big(H^i(N_1, \mathcal{C}_w(\pi_B))\big) = 0$ pour tout $i \geq 0$ et tout $w \in W\backslash\{1\}$.*

Remarque 8.7. Des calculs ainsi que la remarque 6.9 suggèrent que le théorème 8.1 et le corollaire 8.6 devraient se généraliser comme suit à tout sous-groupe parabolique $P \subseteq G$ contenant B comme au § 3 : soit π_P une représentation lisse de $L_P(L)$ sur A, alors on devrait avoir un isomorphisme dans la catégorie $\widehat{\Phi\Gamma}_A^{\text{ét}}$ pour tout $i \geq 1$:

$$D^\vee\big(H^i(N_1, \mathcal{C}_1(\pi_P))\big) \overset{?}{\cong} D^\vee(H^i(N_{L_P,1}, \pi_P)),$$

et si π_P est de plus localement admissible (comme représentation de $L_P(L)$), alors on devrait avoir que le $A[F]$-module $H^i(N_1, \mathcal{C}_w(\pi_P))$ est de torsion pour tout $i \geq 0$ et tout $w \in K_P\backslash\{1\}$, et donc dans ce cas $D^\vee\big(H^i(N_1, \mathcal{C}_w(\pi_P))\big) \overset{?}{=} 0$.

9. Quelques conséquences

On explicite quelques conséquences des résultats précédents, en particulier on en déduit la réponse à une question posée dans [Breuil et Herzig 2015].

On garde les notations des sections précédentes. On note SP_A la catégorie abélienne des représentations lisses de $G(L)$ sur A de longueur finie dont les constituants irréductibles sont des sous-quotients de séries principales.

Corollaire 9.1. *Soit π un objet de SP_A.*

(i) *Le $A[\![X]\!][F]$-module π^{N_1} satisfait la propriété Ad de la définition 2.2.*

(ii) *Le $A[F]$-module $H^i(N_1, \pi)$ est de torsion pour $i \geq 1$.*

(iii) *On a $D_\xi^\vee(\pi) \in \Phi\Gamma_A^{\text{ét}}$ (et pas seulement $\widehat{\Phi\Gamma}_A^{\text{ét}}$).*

Démonstration. (i) Noter que $\pi|_{B(L)}$ est encore de longueur finie comme représentation de $B(L)$ par [Vignéras 2008, théorème 5]. Par le (ii) du lemme 2.5 et un dévissage, on se ramène à $A = k_E$. Si π_B est un caractère lisse de $T(L)$ sur k_E, rappelons que la $B(L)$-représentation $(\mathrm{Ind}_{B^-(L)}^{G(L)}\pi_B)|_{B(L)}$ est de longueur finie et que ses constituants sont exactement les $B(L)$-représentations $\mathcal{C}_w(\pi_B)$ du § 6 pour $w \in W$, cf. [Vignéras 2008, théorème 5]. Par le (ii) du lemme 2.5 et un dévissage sur les constituants de $\pi|_{B(L)}$, on se ramène ainsi à une $B(L)$-représentation $\mathcal{C}_w(\pi_B)$. Cela découle alors de la proposition 6.8 et de la proposition 7.7.

(ii) Par le (i) du lemme 2.5 et un dévissage comme au (i), il suffit de démontrer l'énoncé pour $A = k_E$ et $\mathcal{C}_w(\pi_B)$ comme au (i), ce qui suit du théorème 8.1.

(iii) Là encore, par le (ii) de la proposition 2.7 et un dévissage, on se ramène à $\mathcal{C}_w(\pi_B)$ comme au (i). Si $w \neq 1$, c'est clair par la proposition 6.8. Si $w = 1$, cela résulte de (39) et (47) (cf. Exemple 7.6). □

Corollaire 9.2. *Soit $0 \to \pi' \to \pi \to \pi'' \to 0$ une suite exacte courte de représentations lisses de $G(L)$ sur A telle que π' est dans SP_A. Alors on a une suite exacte courte $0 \to D_\xi^\vee(\pi'') \to D_\xi^\vee(\pi) \to D_\xi^\vee(\pi') \to 0$ dans $\widehat{\Phi\Gamma}_A^{\text{ét}}$.*

Démonstration. On a une suite exacte dans Mod_A :

$$0 \longrightarrow \pi'^{N_1} \longrightarrow \pi^{N_1} \longrightarrow \pi''^{N_1} \longrightarrow H^1(N_1, \pi').$$

Le $A[\![X]\!][F]$-module π'^{N_1} satisfait la propriété Ad par le (i) du corollaire 9.1 et $H^1(N_1, \pi')$ est un $A[F]$-module de torsion par le (ii) du corollaire 9.1. Par le (iv) de la proposition 2.7, on en déduit le résultat. □

Corollaire 9.3. *En restriction à la catégorie* SP_A, *le foncteur* $D_\xi^\vee$ *est exact et à valeurs dans* $\Phi\Gamma_A^{\text{ét}}$.

Démonstration. La première partie résulte du corollaire 9.2 et la deuxième est le (iii) du corollaire 9.1. □

Remarque 9.4. La preuve du corollaire 9.3 reste la même en remplaçant SP_A par la catégorie abélienne C_A formée des représentations de $G(L)$ de longueur finie sur A dont les constituants irréductibles π vérifient les 3 conditions : (1) π^{N_1} satisfait Ad, (2) $H^1(N_1, \pi)$ est un $A[F]$-module de torsion, (3) $D_\xi^\vee(\pi) \in \Phi\Gamma_A^{\text{ét}}$. Il est vraisemblable que C_A contienne *strictement* SP_A au moins pour $L = \mathbb{Q}_p$. Par exemple on peut s'attendre à ce que les induites paraboliques irréductibles (sur k_E donc) ne faisant intervenir que des représentations (irréductibles) de $\mathrm{GL}_2(\mathbb{Q}_p)$ ou des caractères de $\mathbb{Q}_p^\times$ dans la représentation du Levi [Abe 2013; Herzig 2011] vérifient (1) et (2) (elles vérifient (3) par le théorème 6.1, la proposition 5.5 et les résultats pour $\mathrm{GL}_2(\mathbb{Q}_p)$ [Colmez 2010; Emerton 2008; Berger et Vienney 2014; Colmez et al. 2014]).

Considérons maintenant la catégorie abélienne SP_E des représentations continues unitaires de $G(L)$ sur E topologiquement de longueur finie dont les constituants (topologiquement) irréductibles sont des sous-quotients de séries principales continues unitaires sur E. Alors le foncteur $D_\xi^\vee$ s'étend en un foncteur contravariant et exact de SP_E dans la catégorie $\Phi\Gamma_E^{\text{ét}}$ des (φ, Γ)-module étales usuels sur E en posant si Π est dans SP_E :

$$D_\xi^\vee(\Pi) \overset{\text{déf}}{=} E \otimes_{\mathcal{O}_E} \varprojlim_m D_\xi^\vee(\Pi^0/(\varpi_E^m))$$

où Π^0 est une boule unité (quelconque) de Π stable par $G(L)$ et où les flèches de transition (surjectives) $D_\xi^\vee(\Pi^0/(\varpi_E^m)) \twoheadrightarrow D_\xi^\vee(\Pi^0/(\varpi_E^{m-1}))$ proviennent de :

$$\Pi^0/(\varpi_E^{m-1}) \xhookrightarrow{\varpi_E} \Pi^0/(\varpi_E^m).$$

En utilisant les propriétés d'exactitude de $D_\xi^\vee$, on vérifie facilement que $D_\xi^\vee(\Pi)$ ne dépend pas du choix de Π^0. Ces mêmes propriétés d'exactitude montrent que $D_\xi^\vee(\Pi^0/(\varpi_E^m))$ est libre de rang fini (indépendant de m) sur $\mathcal{O}_E/(\varpi_E)^m[\![X]\!][1/X]$ pour tout m.

Soit G' un autre groupe algébrique réductif connexe déployé sur L de centre connexe et soit $D^\vee_{\xi'}$, $D^\vee_{\xi\oplus\xi'}$ comme au §5. On définit les catégories SP'_E (resp. SP''_E) comme SP_E mais avec le groupe G' (resp. $G\times G'$) au lieu de G, auxquelles on étend $D^\vee_{\xi'}$ (resp. $D^\vee_{\xi\oplus\xi'}$) comme ci-dessus. Si $(\Pi,\Pi')\in \mathrm{SP}_E\times\mathrm{SP}'_E$, notons que $\Pi\widehat{\otimes}_E\Pi'$ est aussi un objet de SP''_E (cela se déduit aisément du fait que le produit tensoriel complété de deux séries principales continues unitaires de $G(L)$ et $G'(L)$ est une série principale continue unitaire de $G(L)\times G'(L)$), de sorte que $D^\vee_{\xi\oplus\xi'}(\Pi\widehat{\otimes}_E\Pi')$ est bien défini dans $\Phi\Gamma^{\text{ét}}_E$. On note de manière analogue à [Fontaine 1990, §A.2.2.1] :

$$\mathcal{E}\overset{\text{déf}}{=}E\otimes_{\mathcal{O}_E}\big(\varprojlim_m \mathcal{O}_E/(\varpi_E)^m[\![X]\!][1/X]\big)\cong E\otimes_{\mathcal{O}_E}\big(\mathcal{O}_E[\![X]\!][1/X]\big)\widehat{\ }$$

muni des actions de $\mathbb{Z}_p^\times$ et φ induites par celles sur $\mathcal{O}_E/(\varpi_E)^m[\![X]\!][1/X]$ pour tout m.

Corollaire 9.5. *Avec les notations précédentes, on a un isomorphisme dans* $\Phi\Gamma^{\text{ét}}_E$:

$$D^\vee_{\xi\oplus\xi'}(\Pi\widehat{\otimes}_E\Pi')\cong D^\vee_\xi(\Pi)\otimes_{\mathcal{E}} D^\vee_{\xi'}(\Pi').$$

Démonstration. Soit Π^0 (resp. Π'^0) une boule unité de Π (resp. Π') stable par $G(L)$ (resp. $G'(L)$), alors $\Pi^0\widehat{\otimes}_{\mathcal{O}_E}\Pi'^0$ est une boule unité de $\Pi\widehat{\otimes}_E\Pi'$ stable par $G(L)\otimes G'(L)$ et par définition :

$$D^\vee_{\xi\oplus\xi'}(\Pi\widehat{\otimes}_E\Pi')=E\otimes_{\mathcal{O}_E}\varprojlim_m D^\vee_{\xi\oplus\xi'}\big(\Pi^0/(\varpi_E^m)\otimes_{\mathcal{O}_E}\Pi'^0/(\varpi_E^m)\big).$$

Comme on a :

$$D^\vee_\xi(\pi)\otimes_{\mathcal{E}} D^\vee_{\xi'}(\pi')\cong E\otimes_{\mathcal{O}_E}\varprojlim_m\big(D^\vee_\xi(\Pi^0/(\varpi_E^m))\otimes_{\mathcal{O}_E[\![X]\!][1/X]} D^\vee_{\xi'}(\Pi'^0/(\varpi_E^m))\big),$$

il suffit de montrer que pour tout m :

$$D^\vee_{\xi\oplus\xi'}\big(\Pi^0/(\varpi_E^m)\otimes_{\mathcal{O}_E}\Pi'^0/(\varpi_E^m)\big)\cong D^\vee_\xi(\Pi^0/(\varpi_E^m))\otimes_{\mathcal{O}_E[\![X]\!][1/X]} D^\vee_{\xi'}(\Pi'^0/(\varpi_E^m))$$

ce qui découle de la proposition 5.5, que l'on peut appliquer grâce au (i) du corollaire 9.1 (notons que les $\mathcal{O}_E/(\varpi_E)^m$-modules sous-jacents à $\Pi^0/(\varpi_E^m)$ et $\Pi'^0/(\varpi_E^m)$ sont bien libres, une base s'obtenant en relevant une base quelconque de $\Pi^0/(\varpi_E)$ et $\Pi'^0/(\varpi_E)$). □

Remarque 9.6. Par le (i) de la remarque 5.6, la même preuve donne une version du corollaire 9.5 avec un nombre fini quelconque de représentations.

On a aussi une version p-adique du théorème 6.1 dont la preuve, sans difficulté, est laissée au lecteur.

Corollaire 9.7. *Soit π_P une représentation continue unitaire de $L_P(L)$ sur E topologiquement de longueur finie dont les constituants irréductibles sont des sous-quotients de séries principales continues unitaires de $L_P(L)$, et soit* $(\mathrm{Ind}_{P^-(L)}^{G(L)}\pi_P)^{\mathcal{C}^0}$

l'induite parabolique continue unitaire de π_P. On a un isomorphisme dans $\Phi\Gamma_E^{\text{ét}}$ fonctoriel en π_P :

$$D_\xi^\vee((\mathrm{Ind}_{P^-(L)}^{G(L)}\pi_P)^{\mathcal{C}^0}) \cong D_\xi^\vee(\pi_P).$$

(Notons que, par induction "par étages", la représentation $(\mathrm{Ind}_{P^-(L)}^{G(L)}\pi_P)^{\mathcal{C}^0}$ est bien dans la catégorie SP_E.)

Nous pouvons maintenant répondre de manière significative (et positive) à une question formulée dans [Breuil et Herzig 2015, §3.5]. Nous devons rappeler pour cela plusieurs notations, définitions et constructions de [loc. cit.]. On suppose désormais $L = \mathbb{Q}_p$ (comme dans [loc. cit.]).

On note (G, B, T), $(X(T), R, X^\vee(T), R^\vee)$, etc. comme au début du § 3. On suppose G de centre connexe, on fixe des cocaractères fondamentaux $\lambda_{\alpha^\vee} : \mathbb{G}_{\mathrm{m}} \to T$ pour $\alpha \in S$ et on pose $\xi \overset{\text{déf}}{=} \sum_{\alpha\in S}\lambda_{\alpha^\vee} \in X^\vee(T)$ comme au § 3. La donnée radicielle duale $(X^\vee(T), R^\vee, X(T), R)$ est associée à $(\widehat{G}, \widehat{B}, \widehat{T})$ où $\widehat{G}$ est le groupe réductif déployé sur $\mathbb{Q}_p$ dual de G, $\widehat{B}$ le Borel associé à $(R^\vee)^+$ et $\widehat{T} \subseteq \widehat{B}$ le tore maximal (tel que $X(\widehat{T}) \cong X^\vee(T)$). On note $\widehat{N}$ le radical unipotent de $\widehat{B}$ et $\widehat{N}_\alpha \subseteq \widehat{N}$ le sous-groupe radiciel associé à $\alpha \in (R^\vee)^+$. On suppose que $\widehat{G}$ est *aussi* de centre connexe, en particulier il existe un caractère $\theta \in X(T)$ tel que $\theta \circ \alpha^\vee = \mathrm{Id}_{\mathbb{G}_{\mathrm{m}}}$ pour tout $\alpha \in S$ [Breuil et Herzig 2015, Proposition 2.1.1]. On rappelle qu'à tout sous-ensemble $C \subseteq (R^\vee)^+$ clos (i.e., tel que $\alpha,\ \beta \in C$ et $\alpha+\beta \in (R^\vee)^+ \Rightarrow \alpha+\beta \in C$) est associé un sous-groupe algébrique fermé $\widehat{B}_C$ de $\widehat{B}$ (resp. $\widehat{G}_C$ de $\widehat{G}$) sur $\mathbb{Q}_p$ engendré par $\widehat{T}$ et les $\widehat{N}_\alpha$ (resp. $\widehat{T}$ et les $\widehat{N}_\alpha$, $\widehat{N}_{-\alpha}$) pour $\alpha \in C$. De plus tout sous-groupe algébrique fermé de $\widehat{B}$ contenant $\widehat{T}$ est de la forme $\widehat{B}_C$.

Soit $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \widehat{B}(E) \subseteq \widehat{G}(E)$ un homomorphisme continu et :

$$\widehat{\chi}_\rho : \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \xrightarrow{\rho} \widehat{B}(E) \twoheadrightarrow \widehat{T}(E).$$

On suppose $\alpha^\vee \circ \widehat{\chi}_\rho \notin \{1, \varepsilon^{\pm 1}\}$ pour tout $\alpha \in R^+$, i.e., ρ est générique au sens de [loc. cit., Definition 3.3.1]. On note $C_\rho \subseteq (R^\vee)^+$ le plus petit sous-ensemble clos tel que ρ est à valeurs dans $\widehat{B}_{C_\rho}(E) \subseteq \widehat{B}(E)$. Quitte à remplacer ρ par un conjugué dans $\widehat{B}(E)$, on suppose de plus C_ρ minimal parmi tous les conjugués de ρ dans $\widehat{B}(E)$ (cf. [Breuil et Herzig 2015, §3.2]). On pose :

$$W_{C_\rho} \overset{\text{déf}}{=} \{w \in W,\ w^{-1}(C_\rho) \subseteq (R^\vee)^+\}.$$

Si $w \in W_{C_\rho}$ et $I \subseteq w(S^\vee) \cap C_\rho$ est un sous-ensemble de racines deux à deux orthogonales, alors I et $C_\rho \backslash I$ sont des sous-ensembles clos de $(R^\vee)^+$ [loc. cit., Lemma 2.3.7] et $\widehat{B}_{C_\rho}$ est un produit semi-direct $\widehat{N}_{C_\rho\backslash I} \rtimes \widehat{B}_I$ où :

$$\widehat{N}_{C_\rho\backslash I} \cong \prod_{\alpha\in C_\rho\backslash I} \widehat{N}_\alpha$$

est le radical unipotent de $\widehat{B}_{C_\rho\backslash I}$. De plus $\widehat{B}_I$ est isomorphe à $\widehat{T}_I \times (\prod_{\alpha\in I}\widehat{B}_\alpha)$ où $\widehat{T}_I \subseteq \widehat{T}$ est un sous-tore central dans $\widehat{B}_I$ tel que $\widehat{T} \cong \widehat{T}_I \times (\prod_{\alpha\in I}\widehat{T}_\alpha)$, $\widehat{T}_\alpha$ (resp. $\widehat{B}_\alpha$) étant un tore déployé (resp. un sous-groupe de Borel contenant $\widehat{T}_\alpha$) de la copie de GL_2 dans $\widehat{G}$ correspondant à la racine α, cf. [loc. cit., §2.3]. Soit $w \in W_{C_\rho}$ et $\alpha \in w(S^\vee)\cap C_\rho$, en utilisant la minimalité de C_ρ, on voit que la représentation :

$$\rho_\alpha : \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \xrightarrow{\rho} \widehat{B}_{C_\rho}(E) \twoheadrightarrow \widehat{B}_\alpha(E)$$

est non scindée (i.e., n'est pas à valeurs dans $\widehat{T}_\alpha(E)$ à conjugaison près dans $\widehat{B}_\alpha(E)$) et est générique.

On note $L^\otimes \overset{\text{déf}}{=} \otimes_{\alpha\in S} L(\lambda_{\alpha^\vee})$ (une représentation algébrique de $\widehat{G}$ sur E) où $L(\lambda_{\alpha^\vee})$ est la représentation algébrique de $\widehat{G}$ sur E de plus haut poids (dominant) $\lambda_{\alpha^\vee}$ relativement à $\widehat{B}$ (cf. [loc. cit., §2.1], on utilise ici $X^\vee(T) \cong X(\widehat{T})$). On note $(L^\otimes|_{\widehat{B}_{C_\rho}})^{\mathrm{ord}}$ la plus grande sous-représentation algébrique de $L^\otimes|_{\widehat{B}_{C_\rho}}$ dont les poids (dans $X(\widehat{T})$) sont dans $\{w(\xi),\, w\in W\}$ en voyant ξ dans $X(\widehat{T})$. Pour suivre les notations de [loc. cit., §2], on écrit plutôt α au lieu de $\alpha^\vee$, par exemple $L^\otimes = \otimes_{\alpha\in S^\vee} L(\lambda_\alpha)$. Si $w \in W_{C_\rho}$ et $I \subseteq w(S^\vee)\cap C_\rho$ est un sous-ensemble de racines deux à deux orthogonales, on considère la représentation algébrique de $\widehat{B}_I \cong \widehat{T}_I \times \big(\prod_{\alpha\in I}\widehat{B}_\alpha\big)$ sur E :

$$L_I \overset{\text{déf}}{=} w(\xi)|_{\widehat{T}_I} \otimes_E \left(\bigotimes_{\alpha\in I} L_\alpha\right)$$

où L_α est la restriction à $\widehat{B}_\alpha$ de la représentation algébrique de GL_2 sur E de plus haut poids $w(\xi)|_{\widehat{T}_\alpha}$ relativement à $\widehat{B}_\alpha$. En fait L_α a dimension 2 et est l'unique extension non scindée du poids $s_\alpha(w(\xi)|_{\widehat{T}_\alpha})$ par le poids $w(\xi)|_{\widehat{T}_\alpha}$ où $s_\alpha \in W$ est la permutation associée à α (voir [loc. cit., §2.3]). On voit L_I comme représentation algébrique de $\widehat{B}_{C_\rho}$ via $\widehat{B}_{C_\rho} \twoheadrightarrow \widehat{B}_I$. Si $I \subseteq I'$, on a une unique injection $L_I \hookrightarrow L_{I'}$ ce qui permet de définir (à isomorphisme près) la représentation algébrique $L_{C_\rho,w} \overset{\text{déf}}{=} \varinjlim L_I$ de $\widehat{B}_{C_\rho}$ sur E où la limite inductive est prise sur les sous-ensembles I de $w(S^\vee)\cap C_\rho$ de racines deux à deux orthogonales. Alors on a un isomorphisme de représentations algébriques de $\widehat{B}_{C_\rho}$ sur E ([Breuil et Herzig 2015, Theorem 2.4.1]) :

$$\oplus_{w\in W_{C_\rho}} L_{C_\rho,w} \cong (L^\otimes|_{\widehat{B}_{C_\rho}})^{\mathrm{ord}}.$$

Si l'on note $\widehat{\chi}_{\rho_I}$ l'image de $\widehat{\chi}_\rho$ via la surjection $\widehat{T}(E) \twoheadrightarrow \widehat{T}_I(E)$, on dispose aussi de la représentation de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ sur E :

$$L_I \circ \rho \cong (w(\xi)|_{\widehat{T}_I} \circ \widehat{\chi}_{\rho_I}) \otimes_E \left(\bigotimes_{\alpha\in I} L_\alpha \circ \rho_\alpha\right). \tag{52}$$

À ρ comme ci-dessus est par ailleurs associée dans [loc. cit., §3.3] une représentation dans SP_E notée $\Pi(\rho)^{\mathrm{ord}}$ dont on rappelle la définition. C'est une somme directe $\Pi(\rho)^{\mathrm{ord}} = \oplus_{w\in W_{C_\rho}} \Pi(\rho)_{C_\rho,w}$ où $\Pi(\rho)_{C_\rho,w}$ est défini comme suit.

Soit $w \in W_{C_\rho}$ et $J \subseteq S$ un sous-ensemble de racines simples deux à deux orthogonales tel que $w(J) \subseteq C_\rho^\vee$ où $C_\rho^\vee \overset{\text{déf}}{=} \{\alpha^\vee,\ \alpha \in C_\rho\} \subseteq R^+$. Dans ce cas G_J est le sous-groupe de Levi du parabolique $B^- G_J$ de G et est isomorphe à $T_J \times \mathrm{GL}_2^J$ où $T_J \subseteq T$ est un sous-tore central dans G_J tel que $T \cong T_J \times (\prod_{\alpha\in J} T_\alpha)$, T_α étant un tore déployé de la copie de GL_2 dans G correspondant à la racine α, cf. [loc. cit., Lemma 3.1.4]. On choisit cette décomposition de telle sorte que $\widehat{T}_{w(J)^\vee}$ (cf. ci-dessus) (resp. $\widehat{T}_{w(\alpha)^\vee}$, $\alpha \in J$) soit le dual de $wT_J w^{-1} \subseteq wTw^{-1} \cong T$ (resp. de $wT_\alpha w^{-1}$) où $w(J)^\vee \overset{\text{déf}}{=} \{w(\alpha)^\vee,\ \alpha \in J\} \subseteq w(S^\vee) \cap C_\rho$. Notons que $B \cap G_J = T_J \times (\prod_{\alpha\in J} B_\alpha)$ où $B_\alpha \subset \mathrm{GL}_2$ est un sous-groupe de Borel contenant T_α. Si $\alpha \in J$ et $\chi_\alpha : T_\alpha(\mathbb{Q}_p) \to \mathcal{O}_E^\times \subset E^\times$ est un caractère continu unitaire, on pose avec les notations de [loc. cit., §3.1] (série principale continue unitaire) :

$$\Pi_\alpha(\chi_\alpha) \overset{\text{déf}}{=} \big(\mathrm{Ind}_{B_\alpha^-(\mathbb{Q}_p)}^{\mathrm{GL}_2(\mathbb{Q}_p)}(\chi_\alpha \cdot (\varepsilon^{-1}\circ\theta)|_{T_\alpha(\mathbb{Q}_p)})\big)^{\mathcal{C}^0}.$$

Soit $\chi_\rho : T(\mathbb{Q}_p) \to \mathcal{O}_E^\times \subset E^\times$ le caractère continu (unitaire) correspondant à $\widehat{\chi}_\rho$ par la correspondance de Langlands pour les tores (cf. par exemple [loc. cit., (10)]). Pour $\alpha \in S$ on note $\mathcal{E}_\alpha$ l'unique extension non scindée de $\Pi_\alpha\big(s_\alpha(w^{-1}(\chi_\rho)|_{T_\alpha(\mathbb{Q}_p)})\big)$ par $\Pi_\alpha(w^{-1}(\chi_\rho)|_{T_\alpha(\mathbb{Q}_p)})$ (cf. [loc. cit., Appendix B] pour des références) et on considère l'induite parabolique continue :

$$\Pi(\rho)_J \overset{\text{déf}}{=} \big(\mathrm{Ind}_{B^-(\mathbb{Q}_p)G_J(\mathbb{Q}_p)}^{G(\mathbb{Q}_p)}\big((w^{-1}(\chi_\rho)\cdot(\varepsilon^{-1}\circ\theta))|_{T_J(\mathbb{Q}_p)} \otimes_E (\otimes_{\alpha\in J}\mathcal{E}_\alpha)\big)\big)^{\mathcal{C}^0}.$$

Pour $J \subseteq J'$ comme ci-dessus, on a une unique injection $G(\mathbb{Q}_p)$-équivariante $\Pi(\rho)_J \hookrightarrow \Pi(\rho)_{J'}$ à scalaire près [loc. cit., §3.3] et on pose $\Pi(\rho)_{C_\rho,w} \overset{\text{déf}}{=} \varinjlim \Pi(\rho)_J$ où la limite inductive est prise sur les sous-ensembles J de $S \cap w^{-1}(C_\rho^\vee)$ de racines deux à deux orthogonales. Il est clair que $\Pi(\rho)_{C_\rho,w}$ est dans SP_E (en fait $\Pi(\rho)_{C_\rho,w}$ admet une suite de composition formée de séries principales "complètes", cf. [loc. cit., §3.3]).

Dans [Breuil et Herzig 2015, §3.5], on demande s'il existe un foncteur covariant noté F de la catégorie des représentations continues unitaires admissibles (topologiquement) de longueur finie de $G(\mathbb{Q}_p)$ sur E dans la catégorie Rep_E des représentations continues de dimension finie de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ sur E vérifiant les trois propriétés suivantes :

(i) pour tout caractère continu unitaire $\chi : T(\mathbb{Q}_p) \to \mathcal{O}_E^\times \subset E^\times$ on a :

$$F\big((\mathrm{Ind}_{B^-(\mathbb{Q}_p)}^{G(\mathbb{Q}_p)}\chi\cdot(\varepsilon^{-1}\circ\theta))^{\mathcal{C}^0}\big) = \xi\circ\widehat{\chi},$$

où $\widehat{\chi} : \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \widehat{T}(E)$ correspond à χ par la correspondance de Langlands pour les tores et où on voit ξ dans $X(\widehat{T})$;

(ii) F est exact lorsque restreint à la catégorie SP_E ;

(iii) $F(\Pi(\rho)^{\mathrm{ord}}) = (L^\otimes|_{\widehat{B}_{C_\rho}})^{\mathrm{ord}} \circ \rho$.

Alternativement (i) est équivalent via la réciprocité locale à :

$$F\big((\mathrm{Ind}_{B^-(\mathbb{Q}_p)}^{G(\mathbb{Q}_p)}\chi\cdot(\varepsilon^{-1}\circ\theta))^{C^0}\big)=\big(x\mapsto\chi(\xi(x))\big)$$

où $x\in\mathbb{Q}_p^\times$. Notons que la définition de $\Pi(\rho)^{\mathrm{ord}}$ ne dépend pas de ξ, mais comme celle de $L^\otimes$ en dépend (via les $\lambda_{\alpha^\vee}$), on s'attend par (i) et (iii) à ce que ξ intervienne aussi dans le définition d'un tel foncteur F.

Notons $V^\vee$ le foncteur contravariant de $\Phi\Gamma_E^{ét}$ dans la catégorie Rep_E défini comme le *dual* du foncteur covariant $\boldsymbol{V}_{\mathcal{E}}$ de [Fontaine 1990, §A.3.4.4(c)]. Soit $\delta:\mathbb{Q}_p^\times\to\mathcal{O}_E^\times\subset E^\times,\ x\mapsto\varepsilon^{-1}\big(\theta(\xi(x))\big)=\delta(x)$ que l'on voit comme caractère de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ (une puissance de ε donc). Le corollaire suivant montre que, au moins lorsque l'on se restreint à la catégorie SP_E (qui suffit pour exprimer les propriétés (i) à (iii) ci-dessus), un tel foncteur F existe bien.

Corollaire 9.8. *Le foncteur* $F\overset{\text{déf}}{=}(V^\vee\circ D_\xi^\vee)\otimes\delta^{-1}$ *de la catégorie* SP_E *dans la catégorie* Rep_E *satisfait les propriétés* (*i*), (*ii*) *et* (*iii*) *ci-dessus.*

Démonstration. La propriété (i) découle du corollaire 9.7 et des définitions (cf. Exemple 7.6). La propriété (ii) suit du corollaire 9.3 (cf. la discussion qui suit la remarque 9.4). Montrons la propriété (iii). Soit $w\in W_{C_\rho}$ et $J\subseteq S\cap w^{-1}(C_\rho^\vee)$ un sous-ensemble de racines deux à deux orthogonales. Par le corollaire 9.7 appliqué avec $L=\mathbb{Q}_p$, $P=BG_J$ et :

$$\pi_P\overset{\text{déf}}{=}(w^{-1}(\chi_\rho)\cdot(\varepsilon^{-1}\circ\theta))|_{T_J(\mathbb{Q}_p)}\otimes_E(\otimes_{\alpha\in J}\mathcal{E}_\alpha),$$

et par le corollaire 9.5 (avec la remarque 9.6), on a dans $\Phi\Gamma_E^{\text{ét}}$:

$$D_\xi^\vee(\Pi(\rho)_J)=D_{\xi_J}^\vee\big((w^{-1}(\chi_\rho)\cdot(\varepsilon^{-1}\circ\theta))|_{T_J(\mathbb{Q}_p)}\big)\otimes_{\mathcal{E}}(\otimes_{\alpha\in J}D_{\xi_\alpha}^\vee(\mathcal{E}_\alpha))\qquad(53)$$

où ξ_J (resp. ξ_α) est la composée $\mathbb{G}_{\mathrm{m}}\xrightarrow{\xi}T\twoheadrightarrow T_J$ (resp. $\mathbb{G}_{\mathrm{m}}\xrightarrow{\xi}T\twoheadrightarrow T_\alpha$). Par définition de $D_{\xi_J}^\vee$ (cf. § 3 et le lemme 7.5), on a (en voyant $T_J(\mathbb{Q}_p)$ comme facteur direct de $T(\mathbb{Q}_p)$ et via la réciprocité locale) :

$$\begin{aligned}V^\vee\big(D_{\xi_J}^\vee\big((w^{-1}(\chi_\rho)\cdot(\varepsilon^{-1}\circ\theta))|_{T_J(\mathbb{Q}_p)}\big)\big)&=\big(x\mapsto(w^{-1}(\chi_\rho)\cdot(\varepsilon^{-1}\circ\theta))(\xi_J(x))\big)\\&=\big(x\mapsto w^{-1}(\chi_\rho)(\xi_J(x))\big)\otimes\delta_J\end{aligned}$$

où $x\in\mathbb{Q}_p^\times$ et δ_J est le caractère de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ induit par $x\mapsto\varepsilon^{-1}\big(\theta(\xi_J(x))\big)$. Mais le caractère de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ induit par $x\mapsto w^{-1}(\chi_\rho)(\xi_J(x))$ est exactement le caractère $w(\xi)|_{\widehat{T}_{w(J)^\vee}}\circ\widehat{\chi}_{\rho_{w(J)^\vee}}$ (en suivant les définitions et en voyant maintenant ξ dans $X(\widehat{T})$). De même, si $\alpha\in J$ et si δ_α est le caractère de $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ induit par $x\mapsto\varepsilon^{-1}\big(\theta(\xi_\alpha(x))\big)$ (en voyant $T_\alpha(\mathbb{Q}_p)$ comme facteur direct de $T(\mathbb{Q}_p)$), on a :

$$V^\vee(D_{\xi_\alpha}^\vee(\mathcal{E}_\alpha))\cong(L_{w(\alpha)^\vee}\circ\rho_{w(\alpha)^\vee})\otimes\delta_\alpha$$

car, par généricité de $\rho_{w(\alpha)^\vee}$, par [Colmez 2010] (voir aussi [Colmez et al. 2014]) avec le (iii) de la proposition 3.2 (et un passage à la limite projective évident) et

par la propriété (i), $V^\vee(D^\vee_{\xi_\alpha}(\mathcal{E}_\alpha))\otimes\delta_\alpha^{-1}$ est l'*unique* extension non scindée de :

$$\begin{aligned}\big(x\mapsto s_\alpha w^{-1}(\chi_\rho)(\xi_\alpha(x))\big) &= (ws_\alpha(\xi))|_{\widehat{T}_{w(\alpha)^\vee}}\circ\widehat{\chi}_{\rho_{w(\alpha)^\vee}}\\ &= s_{w(\alpha)^\vee}(w(\xi)|_{\widehat{T}_{w(\alpha)^\vee}})\circ\widehat{\chi}_{\rho_{w(\alpha)^\vee}}\end{aligned}$$

par $\big(x\mapsto w^{-1}(\chi_\rho)(\xi_\alpha(x))\big)=w(\xi)|_{\widehat{T}_{w(\alpha)^\vee}}\circ\widehat{\chi}_{\rho_{w(\alpha)^\vee}}$. Comme $V^\vee$ commute aux produits tensoriels, on en déduit avec (52), (53) et l'égalité $\delta_J\prod_{\alpha\in J}\delta_\alpha=\delta$ que $F(\Pi(\rho)_J)=L_{w(J)^\vee}\circ\rho$. Par passage à la limite inductive sur J et exactitude de F, on obtient facilement $F(\Pi(\rho)_{C_\rho,w})=L_{C_\rho,w}\circ\rho$ d'où la propriété (iii) en sommant sur $w\in W_{C_\rho}$. □

Remarque 9.9. Par une preuve totalement analogue (dont on laisse les détails au lecteur intéressé), lorsque p est un bon premier pour $\widehat{G}$ au sens de [Breuil et Herzig 2015, Definition 2.5.1], on montre une version sur k_E du corollaire 9.8 (comme espéré à la fin de [Breuil et Herzig 2015, §3.5]).

Bibliographie

[Abe 2013] N. Abe, "On a classification of irreducible admissible modulo p representations of a p-adic split reductive group", *Compos. Math.* **149**:12 (2013), 2139–2168. MR 3143708 Zbl 06250165

[Bergdall et Chojecki 2014] J. Bergdall et P. Chojecki, "Ordinary representations and companion points for $U(3)$ in the indecomposable case", prépublication, 2014, Voir http://arxiv.org/abs/1405.3026. arXiv 1405.3026

[Berger et Vienney 2014] L. Berger et M. Vienney, "Irreducible modular representations of the Borel subgroup of $\mathrm{GL}_2(\mathbb{Q}_p)$", pp. 32–51 dans *Automorphic Forms and Galois Representations*, vol. 1, édité par F. Diamond et al., London Math. Soc. Lecture Note Series **414**, Cambridge University Press, 2014.

[Breuil 2003] C. Breuil, "Sur quelques représentations modulaires et p-adiques de $\mathrm{GL}_2(\mathbb{Q}_p)$: I", *Compositio Math.* **138**:2 (2003), 165–188. MR 2004k:11062 Zbl 1044.11041

[Breuil et Herzig 2015] C. Breuil et F. Herzig, "Ordinary representations of $G(\mathbb{Q}_p)$ and fundamental algebraic representations", *Duke Math. J.* **164**:7 (2015), 1271–1352. MR 3347316 Zbl 06455742

[Breuil et Paškūnas 2012] C. Breuil et V. Paškūnas, *Towards a modulo p Langlands correspondence for* GL_2, vol. 216, Mem. Amer. Math. Soc. **1016**, 2012. MR 2931521 Zbl 1245.22010

[Colmez 2010] P. Colmez, "Représentations de $\mathrm{GL}_2(\mathbb{Q}_p)$ et (ϕ,Γ)-modules", pp. 281–509 dans *Représentations p-adiques de groupes p-adiques II : Représentations de* $\mathrm{GL}_2(\mathbb{Q}_p)$ *et* (ϕ,Γ)*-modules*, édité par L. Berger et al., Astérisque **330**, 2010. MR 2011j:11224 Zbl 1218.11107

[Colmez et al. 2014] P. Colmez, G. Dospinescu et V. Paškūnas, "The p-adic local Langlands correspondence for $\mathrm{GL}_2(\mathbb{Q}_p)$", *Camb. J. Math.* **2**:1 (2014), 1–47. MR 3272011 Zbl 1312.11090

[Digne et Michel 1991] F. Digne et J. Michel, *Representations of finite groups of Lie type*, London Mathematical Society Student Texts **21**, Cambridge University Press, 1991. MR 92g:20063 Zbl 0815.20014

[Emerton 2008] M. Emerton, "On a class of coherent rings, with applications to the smooth representation theory of $\mathrm{GL}_2(\mathbb{Q}_p)$ in characteristic p", prépublication, 2008, Voir http://wvii-w.claymath.org/sites/default/files/emerton.pdf.

[Emerton 2010] M. Emerton, "Ordinary parts of admissible representations of p-adic reductive groups I. Definition and first properties", pp. 355–402 dans *p-adic representations of p-adic groups III : Global and geometrical methods*, Astérisque **331**, 2010. MR 2011k:22013 Zbl 1205.22013

[Erdélyi et Zábrádi 2014] M. Erdélyi et G. Zábrádi, "Links between generalized Montréal-functors", prépublication, 2014. arXiv 1412.5778

[Fontaine 1990] J.-M. Fontaine, "Représentations p-adiques des corps locaux ($1^{\text{ère}}$ partie)", pp. 249–309 dans *The Grothendieck Festschrift*, vol. II, édité par P. Cartier et al., Progr. Math. **87**, Birkhäuser, Boston, 1990. MR 92i:11125 Zbl 0743.11066

[Gabriel 1962] P. Gabriel, "Des catégories abéliennes", *Bull. Soc. Math. France* **90** (1962), 323–448. MR 38 #1144 Zbl 0201.35602

[Hauseux 2014] J. Hauseux, "Extensions entre séries principales p-adiques et modulo p de $G(F)$", *J. Inst. Math. Jussieu* (publié en ligne août 2014).

[Herzig 2011] F. Herzig, "The classification of irreducible admissible mod p representations of a p-adic GL_n", *Invent. Math.* **186**:2 (2011), 373–434. MR 2845621 Zbl 1235.22030

[Jantzen 2003] J. C. Jantzen, *Representations of algebraic groups*, 2-nd éd., Mathematical Surveys and Monographs **107**, Amer. Math. Soc., Providence, RI, 2003. MR 2004h:20061 Zbl 1034.20041

[Morra et Schraen $\geq$ 2015] S. Morra et B. Schraen, "Structure partielle de certaines représentations supersingulières de GL_2", en préparation.

[Ollivier 2014] R. Ollivier, "Resolutions for principal series representations of p-adic GL_n", *Münster J. Math.* **7** (2014), 225–240. MR 3271245 Zbl 1316.22015

[Schneider et Vignéras 2011] P. Schneider et M.-F. Vigneras, "A functor from smooth o-torsion representations to (ϕ, Γ)-modules", pp. 525–601 dans *On certain L-functions*, édité par J. Arthur et al., Clay Math. Proc. **13**, Amer. Math. Soc., Providence, RI, 2011. MR 2012e:11194 Zbl 1278.11061

[Schraen 2012–14] B. Schraen, communications personnelles, novembre 2012 et mars 2014.

[Schraen 2015] B. Schraen, "Sur la présentation des représentations supersingulières de $\mathrm{GL}_2(F)$", *J. Reine Angew. Math.* **704** (2015), 187–208. MR 3365778 Zbl 06455996

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

[Vignéras 2008] M.-F. Vignéras, "Série principale modulo p de groupes réductifs p-adiques", *Geom. Funct. Anal.* **17**:6 (2008), 2090–2112. MR 2009a:22015 Zbl 05275302

[Zábrádi 2011] G. Zábrádi, "Exactness of the reduction on étale modules", *J. Algebra* **331** (2011), 400–415. MR 2012c:11253 Zbl 1227.22022

Communicated by Brian Conrad
Received 2014-09-06 Revised 2015-06-12 Accepted 2015-08-08

christophe.breuil@math.u-psud.fr *C.N.R.S. et Université Paris-Sud, Bâtiment 425, 91405 Orsay Orsay, France*

ALGEBRA AND NUMBER THEORY 9:10 (2015)
dx.doi.org/10.2140/ant.2015.9.2293

msp

On the normalized arithmetic Hilbert function

Mounir Hajli

Let $X \subset \mathbb{P}^N_{\overline{\mathbb{Q}}}$ be a subvariety of dimension n, and let $\mathcal{H}_{\mathrm{norm}}(X;\ \cdot\ )$ be the normalized arithmetic Hilbert function of X introduced by Philippon and Sombra. We show that this function admits the asymptotic expansion

$$\mathcal{H}_{\mathrm{norm}}(X; D) = \frac{\hat{h}(X)}{(n+1)!} D^{n+1} + o(D^{n+1}), \quad \forall D \gg 1,$$

where $\hat{h}(X)$ is the normalized height of X. This gives a positive answer to a question raised by Philippon and Sombra.

1. Introduction

In [Philippon and Sombra 2008], the authors introduce an arithmetic Hilbert function defined for any subvariety in $\mathbb{P}^N$, the projective space of dimension N over $\overline{\mathbb{Q}}$. This function measures the binary complexity of the subvariety. In the case of toric subvarieties, a result of Philippon and Sombra shows that the asymptotic behavior of the associated normalized arithmetic Hilbert function is related to the normalized height of the subvariety considered; see [Philippon and Sombra 2008, Proposition 0.4]. This result is an important step toward the proof of the main theorem of the same paper, which is an explicit formula for the normalized height of projective translated toric varieties; see [Philippon and Sombra 2008, Théorème 0.1].

In [Philippon and Sombra 2008, Question 2.2], the authors ask if the normalized arithmetic Hilbert function admits an asymptotic expansion similar to the toric case. More precisely, given X a subvariety of dimension n in $\mathbb{P}^N$, the projective space of dimension N over $\overline{\mathbb{Q}}$, can we find a real $c(X) \geq 0$ such that

$$\mathcal{H}_{\mathrm{norm}}(X; D) = \frac{c(X)}{(n+1)!} D^{n+1} + o(D^{n+1})?$$

If so, do we have $c(X) = \hat{h}(X)$, where $\hat{h}(X)$ is the normalized height of X?

In this article, we give an affirmative answer to this question.

MSC2010: primary 14G40; secondary 11G50, 11G35.
Keywords: arithmetic Hilbert function, height.

Theorem 1.1. *Let $X \subset \mathbb{P}^N$ be a subvariety of dimension n in $\mathbb{P}^N$. Then the normalized arithmetic Hilbert function associated to X admits the asymptotic expansion*

$$\mathcal{H}_{\mathrm{norm}}(X; D) = \frac{\hat{h}(X)}{(n+1)!} D^{n+1} + o(D^{n+1}), \quad \forall D \gg 1.$$

The notion of normalized height plays an important role in the diophantine approximation on tori, particularly in Bogomolov's and generalized Lehmer's problems; see [David and Philippon 1999; Amoroso and David 2003]. A result of Zhang [1992] shows that a subvariety X with a vanishing normalized height is necessarily a union of toric subvarieties.

Gillet and Soulé [1992] proved an arithmetic Hilbert–Samuel formula as a consequence of the arithmetic Riemann–Roch theorem. Roughly speaking, this formula describes the asymptotic behavior of the arithmetic degree of a hermitian module defined by the global sections of the tensorial power of a positive hermitian line bundle on an arithmetic variety. Moreover, the leading term is given by the arithmetic degree of the hermitian line bundle. Later Abbès and Bouche [1995] gave a new proof for this result without using the arithmetic Riemann–Roch theorem. Randriambololona [2006] extended the result Gillet and Soulé to the case of coherent sheaf provided as a subquotient of a metrized vector bundle on an arithmetic variety.

Notation. Let $\mathbb{Q}$ be the field of rational numbers, $\mathbb{Z}$ the ring of integers, K a number field and $\mathcal{O}_K$ its ring of integers. For N and D two integers in $\mathbb{N}$ we define $\mathbb{N}_D^{N+1} := \{a \in \mathbb{N}^{N+1} : a_0 + \cdots + a_N = D\}$, and we let $\mathbb{C}[x_0, \ldots, x_N]_D$ (resp. $K[x_0, \ldots, x_N]_D$) denote the complex vector space (resp. K-vector space) of homogeneous polynomials of degree D in $\mathbb{C}[x_0, \ldots, x_N]$ (resp. in $K[x_0, \ldots, x_N]$).

For any prime number p we denote by $|\cdot|_p$ the p-adic absolute value on $\mathbb{Q}$ such that $|p|_p = p^{-1}$ and by $|\cdot|_\infty$, or simply $|\cdot|$, the standard absolute value. Let $M_{\mathbb{Q}}$ be the set of these absolute values. We denote by M_K the set of absolute values of K extending the absolute values of $M_{\mathbb{Q}}$, and by M_K^∞ the subset in M_K of archimedean absolute values.

We denote by $\mathbb{P}^N$ the projective space over $\overline{\mathbb{Q}}$ of dimension N. A variety is assumed reduced and irreducible.

2. The proof of Theorem 1.1

We keep the same notation as in [Philippon and Sombra 2008]. Let ω be the Fubini–Study form on $\mathbb{P}^N(\mathbb{C})$. For any $k \in \mathbb{N}_{\geq 1} \cup \{\infty\}$, we denote by h_k the hermitian metric on $\mathcal{O}(1)$ given by

$$h_k(\cdot, \cdot) = \frac{|\cdot|^2}{(|x_0|^{2k} + \cdots + |x_N|^{2k})^{1/2k}} \quad \text{and} \quad h_\infty(\cdot, \cdot) = \frac{|\cdot|^2}{\max(|x_0|, \ldots, |x_N|)^2},$$

and we let $\overline{\mathcal{O}(1)}_k := (\mathcal{O}(1), h_k)$ and $\omega_k := c_1(\mathcal{O}(1), h_k)$ for any $k \in \mathbb{N} \cup \{\infty\}$. Note that $\omega_k = (1/k)[k]^*\omega$, where $[k] : \mathbb{P}^N(\mathbb{C}) \to \mathbb{P}^N(\mathbb{C}),\ [x_0 : \cdots : x_N] \mapsto [x_0^k : \cdots : x_N^k]$. Observe that the sequence $(\omega_k)_{k \in \mathbb{N}_{\geq 1}}$ converges weakly to the current ω_∞. We consider the normalized volume form

$$\Omega_k := \omega_k^{\wedge N}, \quad \forall k \in \mathbb{N}_{\geq 1} \cup \{\infty\}.$$

For any $k \in \mathbb{N}_{\geq 1} \cup \{\infty\}$, the metrics of $\overline{\mathcal{O}(1)}_k$ and Ω_k define a scalar product $\mathbb{C}[x_0, \ldots, x_N]_D$ denoted by $\langle \cdot, \cdot \rangle_k$ and given by

$$\langle f, g \rangle_k := \int_{\mathbb{P}^N(\mathbb{C})} h_k^{\otimes D}(f, g)\Omega_k, \tag{1}$$

for any $f = \sum_a f_a x^a,\ g = \sum_a g_a x^a$ in $\mathbb{C}[x_0, \ldots, x_N]_D$ with $f_a, g_a \in \mathbb{C}$. We denote by $\| \cdot \|_k$ the associated norm for any $k \in \mathbb{N}_{\geq 1} \cup \{\infty\}$. Note that $\langle f, g \rangle_\infty = \sum_a f_a \bar{g}_a$ and $\|x^a\|_\infty = 1$ for any $a \in \mathbb{N}_D^{N+1}$ and $D \in \mathbb{N}$.

Let $X \subset \mathbb{P}^N$ be a subvariety defined over a number field K. Define an embedding $\sigma_v : K \to \mathbb{C}$, where $v \in M_K^\infty$. For any $p_1, \ldots, p_l \in K[x_0, \ldots, x_N]_D$, we set

$$\|p_1 \wedge \cdots \wedge p_l\|_{k,v} := \|\sigma_v(p_1) \wedge \cdots \wedge \sigma_v(p_l)\|_k, \quad \forall k \in \mathbb{N} \cup \{\infty\}.$$

Define $\mathcal{O}(D) := \mathcal{O}(1)^{\otimes D}$. We let $M := \Gamma(\Sigma, \mathcal{O}(D)_{|\Sigma})$ be the $\mathcal{O}_K$-module of global sections of $\mathcal{O}(D)_{|\Sigma}$, where Σ is the Zariski closure of X in $\mathbb{P}^N_{\mathcal{O}_K}$. For any $v \in M_K^\infty$, we set $\Gamma(\Sigma, \mathcal{O}(D)_{|\Sigma})_{\sigma_v} := \Gamma(\Sigma, \mathcal{O}(D)_{|\Sigma}) \otimes_{\sigma_v} \mathbb{C}$. We consider the following restriction map:

$$\pi : \Gamma(\mathbb{P}^N_{\mathcal{O}_K}, \mathcal{O}(D))_{\sigma_v} \to \Gamma(\Sigma, \mathcal{O}(D)_{|\Sigma})_{\sigma_v} \to 0.$$

The space $\Gamma(\mathbb{P}^N_{\mathcal{O}_K}, \mathcal{O}(D))_{\sigma_v}$ is identified canonically to $K_\sigma[x_0, \ldots, x_N]_D$. For any $k \in \mathbb{N}_{\geq 1} \cup \{\infty\}$, this space can be endowed by the scalar product induced by Ω_k and h_k and denoted by $\langle \cdot, \cdot \rangle_{k,v}$, where

$$\langle f, g \rangle_{k,v} = \langle \sigma_v(f), \sigma_v(g) \rangle_k$$

for any $f, g \in \Gamma(\mathbb{P}^N_{\mathcal{O}_K}, \mathcal{O}(D))_{\sigma_v}$. Since $\mathcal{O}(1)$ is ample, there exists a $D_0 \in \mathbb{N}$ such that, for any $D \geq D_0$, the restriction map is surjective. Let $D \geq D_0$. For any $k \in \mathbb{N} \cup \{\infty\}$, we denote by $\| \cdot \|_{k,v,\mathrm{quot}}$ the quotient norm induced by π and $\| \cdot \|_{k,v}$. Following [Philippon and Sombra 2008, p. 348], we endow $\Gamma(\Sigma, \mathcal{O}(D)_{|\Sigma})_{\sigma_v}$ with $\| \cdot \|_{k,v,\mathrm{quot}}$, for any $k \in \mathbb{N}_{\geq 1} \cup \{\infty\}$. By this construction, M can be equipped with a structure of a hermitian $\mathcal{O}_K$-module, denoted by $\bar{M}_k$. If $f_1, \ldots, f_s \in M$, is a K-basis for $M \otimes_{\mathcal{O}_K} K$, then

$$\begin{aligned}\widehat{\deg}(\bar{M}_k) &= \widehat{\deg}(\overline{\Gamma(\Sigma, \mathcal{O}(D)_{|\Sigma})}_k) \\ &:= \frac{1}{[K : \mathbb{Q}]}\left(\log \mathrm{Card}\big(\textstyle\bigwedge^s M/(f_1 \wedge \cdots \wedge f_s)\big) - \sum_{v : K \to \mathbb{C}} \log \|f_1 \wedge \cdots f_s\|_{k,v}\right).\end{aligned}$$

The normalized arithmetic Hilbert function. Let $X \subset \mathbb{P}^N$ be a subvariety defined over a number field K and let $I := I(X) \subset K[x_0, \dots, x_N]$ be its ideal of definition. We set

$$\mathcal{H}_{\text{geom}}(X; D) := \dim_K \big(K[x_0, \dots, x_N]/I\big)_D = \binom{D+N}{N} - \dim_K(I_D).$$

The function $\mathcal{H}_{\text{geom}}(X; \cdot)$ is known as *the classical geometric Hilbert function*. Philippon and Sombra [2008] introduced an arithmetic analogue of this function. Define $m := \mathcal{H}_{\text{geom}}(X; D)$, $l := \dim_K(I_D)$ and let

$$\bigwedge^l K[x_0, \dots, x_N]_D$$

be the l-th exterior power product of $K[x_0, \dots, x_N]_D$. For $f \in \bigwedge^l K[x_0, \dots, x_N]_D$ and $v \in M_K$ we denote by $|f|_v$ the sup-norm of the coefficients of f at the place v, with respect to the standard basis of $\bigwedge^l K[x_0, \dots, x_N]_D$.

Definition 2.1 [Philippon and Sombra 2008, Définition 2.1]. Let $p_1, \dots, p_l$ be a K-basis of I_D. We set

$$\mathcal{H}_{\text{norm}}(X; D) = \sum_{v \in M_K} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log |p_1 \wedge \cdots \wedge p_m|_v.$$

By the product formula, this definition does not depend on the choice of the basis; also it is invariant under finite extensions of K. We call $\mathcal{H}_{\text{norm}}(X; \cdot)$ the normalized arithmetic Hilbert function of X.

Following Philippon and Sombra, this arithmetic Hilbert function measures, for any $D \in \mathbb{N}$, the binary complexity of the K-vector space of forms of degree D in $K[x_0, \dots, x_N]$ modulo I. As pointed out by Philippon and Sombra [2008, Proposition 0.4], when X is a toric variety, the asymptotic behavior of its associated normalized arithmetic Hilbert function is related to $\hat{h}(X)$, the normalized height of X. The authors ask the following question:

Given X a subvariety in $\mathbb{P}^N$ of dimension n, can we find a real $c(X) \geq 0$ such that

$$\mathcal{H}_{\text{norm}}(X; D) = \frac{c(X)}{(n+1)!} D^{n+1} + o(D^{n+1})?$$

If so, do we have $c(X) = \hat{h}(X)$?

We recall the following proposition, which gives a dual formulation for $\mathcal{H}_{\text{norm}}$.

Proposition 2.2. *Let $q_1, \dots, q_m \in K[x_0, \dots, x_N]_D^\vee$ be a K-basis of* $\text{Ann}(I_D)$. *Then*

$$\mathcal{H}_{\text{norm}}(X; D) = \sum_{v \in M_K} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log |q_1 \wedge \cdots \wedge q_m|_v.$$

Proof. See [Philippon and Sombra 2008, Proposition 2.3]. □

For any $k \in \mathbb{N}_{\geq 1} \cup \{\infty\}$, we consider the arithmetic function

$$\begin{aligned}\mathcal{H}_{\mathrm{arith}}(X; D, k) &:= \sum_{v \in M_K^\infty} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log \|p_1 \wedge \cdots \wedge p_l\|_{k,v} \\ &\quad + \sum_{v \in M_K \setminus M_K^\infty} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log |p_1 \wedge \cdots \wedge p_l|_v + \tfrac{1}{2} \log(\gamma(N, D, k)), \quad (2)\end{aligned}$$

where $p_1, \ldots, p_l$ is a K-basis of I_D and

$$\gamma(N; D, k) := \prod_{a \in \mathbb{N}_D^{N+1}} \langle a, a \rangle_k^{-1}. \quad (3)$$

For $k = 1$, notice that $\mathcal{H}_{\mathrm{arith}}(X; \cdot, 1)$ corresponds, up to a constant, to the arithmetic function $\mathcal{H}_{\mathrm{arith}}(X; \cdot)$ considered in [Philippon and Sombra 2008, p. 346].

Similarly to $\mathcal{H}_{\mathrm{norm}}$, the function $\mathcal{H}_{\mathrm{arith}}$ admits a dual formulation. The scalar product $\langle \cdot, \cdot \rangle_k$ induces the following linear isomorphism:

$$\eta_k : \mathbb{C}[x_0, \ldots, x_N] \to \mathbb{C}[x_0, \ldots, x_N]^\vee, \quad f \mapsto \langle \cdot, f \rangle_k.$$

Thus $\mathbb{C}[x_0, \ldots, x_N]^\vee$ can be endowed with the dual scalar product, given by

$$\langle \eta_k(f), \eta_k(g) \rangle_k := \langle f, g \rangle_k, \quad \forall f, g \in \mathbb{C}[x_0, \ldots, x_N]_D.$$

We can check easily that, for any $k \in \mathbb{N} \cup \{\infty\}$, we have

$$\|\theta\|_k' := \sup_{g \in \mathbb{C}[x_0, \ldots, x_N] \setminus \{0\}} \frac{|\theta(g)|}{\|g\|_k} = \|f\|_k,$$

where $f \in \mathbb{C}[x_0, \ldots, x_N]$ is such that $\theta = \eta_k(f)$. Then $\|\theta\|_k'^2 = \langle \theta, \theta \rangle_k$ for any $\theta \in \mathbb{C}[x_0, \ldots, x_N]^\vee$. It follows that

$$\langle \theta, \zeta \rangle_k = \sum_b \langle x^b, x^b \rangle_k^{-1} \theta_b \bar{\zeta}_b. \quad (4)$$

This product extends to $\wedge^m(\mathbb{C}[x_0, \ldots, x_N]_D^\vee)$ as follows:

$$\langle \theta_1 \wedge \cdots \wedge \theta_m, \zeta_1 \wedge \cdots \wedge \zeta_m \rangle_k := \det(\langle \theta_i, \zeta_j \rangle_k)_{1 \leq i,j \leq m}.$$

Proposition 2.3. *Let $q_1, \ldots, q_m \in K[x_0, \ldots, x_N]_D^\vee$ be a K-basis of* $\mathrm{Ann}(I_D)$. *Then*

$$\begin{aligned}&\mathcal{H}_{\mathrm{arith}}(X; D, k) \\ &= \sum_{v \in M_K^\infty} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log \|q_1 \wedge \cdots \wedge q_m\|_{k,v}^\vee + \sum_{v \in M_K \setminus M_K^\infty} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log |q_1 \wedge \cdots \wedge q_m|_v.\end{aligned}$$

Proof. The proof is similar to [Philippon and Sombra 2008, Proposition 2.5]. □

Lemma 2.4. *There exists a D_1 such that, for any $D \geq D_1$ and any $k \in \mathbb{N}$, we have*

$$\mathcal{H}_{\mathrm{arith}}(X; D, k) = \widehat{\deg}(\overline{\Gamma(\Sigma, \mathcal{O}(D)_{|\Sigma})}_k) - \tfrac{1}{2}\mathcal{H}_{\mathrm{geom}}(X; D)\log\binom{D+N}{N}.$$

Proof. The proof is similar to [Philippon and Sombra 2008, Lemme 2.6]. Let $\mathcal{I}$ be the ideal sheaf of Σ and let $\Gamma(\mathbb{P}^N_{\mathcal{O}_K}, \mathcal{I}\mathcal{O}(D))$ be the $\mathcal{O}_K$-module of global sections of $\mathcal{I}\mathcal{O}(D)$, endowed with the scalar products induced by the scalar product $\langle \cdot, \cdot \rangle_k$. We claim that there exists an integer D_1, which does not depend on k, such that, for any $D \geq D_1$, we have

$$\widehat{\deg}(\overline{\Gamma(\Sigma, \mathcal{O}(D)_{|\Sigma})}_k) = \widehat{\deg}(\overline{\Gamma(\mathbb{P}^N_{\mathcal{O}_K}, \mathcal{O}(D))}_k) - \widehat{\deg}(\overline{\Gamma(\mathbb{P}^N_{\mathcal{O}_K}, \mathcal{I}\mathcal{O}(D))}_k).$$

Indeed, we can find a $D_1 \in \mathbb{N}$ such that, for all $D \geq D_1$, the following sequence is exact:

$$0 \to \Gamma(\mathbb{P}^N_{\mathcal{O}_K}, \mathcal{I}\mathcal{O}(D)_{|\Sigma}) \to \Gamma(\mathbb{P}^N_{\mathcal{O}_K}, \mathcal{O}(D)) \to \Gamma(\Sigma, \mathcal{O}(D)_{|\Sigma}) \to 0.$$

Then by [Randriambololona 2001, Lemme 2.3.6], the sequence of hermitian $\mathcal{O}_K$-modules

$$0 \to \overline{\Gamma(\mathbb{P}^N_{\mathcal{O}_K}, \mathcal{I}\mathcal{O}(D)_{|\Sigma})}_k \to \overline{\Gamma(\mathbb{P}^N_{\mathcal{O}_K}, \mathcal{O}(D))}_k \to \overline{\Gamma(\Sigma, \mathcal{O}(D)_{|\Sigma})}_k \to 0$$

is exact, where the metrics of $\overline{\Gamma(\mathbb{P}^N_{\mathcal{O}_K}, \mathcal{I}\mathcal{O}(D)_{|\Sigma})}_k$ and $\overline{\Gamma(\Sigma, \mathcal{O}(D)_{|\Sigma})}_k$ are induced by the metric of $\overline{\Gamma(\mathbb{P}^N_{\mathcal{O}_K}, \mathcal{O}(D))}_k$.

We have

$$\widehat{\deg}(\overline{\Gamma(\mathbb{P}^N_{\mathcal{O}_K}, \mathcal{O}(D))}_k) = \tfrac{1}{2}\log(\gamma(N; D, k)) + \tfrac{1}{2}\binom{D+N}{N}\log\binom{N+D}{N}. \quad (5)$$

As in the proof of [Philippon and Sombra 2008, Lemme 2.6], and keeping the same notation, we have

$$\begin{aligned}
&\widehat{\deg}(\overline{\Gamma(\Sigma, \mathcal{O}(D)_{|\Sigma})}_k) \\
&\quad = \tfrac{1}{2}\log(\gamma(N; D, k)) + \tfrac{1}{2}\mathcal{H}_{\mathrm{geom}}(X; D)\log\binom{N+D}{N} \\
&\qquad + \sum_{v \in M_K^\infty} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log \|p_1 \wedge \cdots \wedge p_l\|^\vee_{k,v} \\
&\qquad\qquad - \frac{1}{[K : \mathbb{Q}]} \log \mathrm{Card}\big(\textstyle\bigwedge^l (I_{\mathcal{O}_K})/(p_1 \wedge \cdots \wedge p_l)\big). \quad (6)
\end{aligned}$$

The last term in (6) does not depend on the metric. It is computed in [Philippon and Sombra 2008, p. 349]; we have

$$\frac{1}{[K:\mathbb{Q}]}\log \mathrm{Card}\big(\textstyle\bigwedge^{l}(I_{\mathcal{O}_K})/(p_1\wedge\cdots\wedge p_l)\big) = -\sum_{v\in M_K\setminus M_K^{\infty}}\frac{[K_v:\mathbb{Q}_v]}{[K:\mathbb{Q}]}\log|p_1\wedge\cdots\wedge p_l|_v. \quad \square$$

By [Randriambololona 2006, Théorème A], we have

$$\widehat{\deg}(\overline{\Gamma(\Sigma,\mathcal{O}(D)_{|\Sigma})}_k) = \frac{h_{\overline{\mathcal{O}(1)}_k}(X)}{(n+1)!}D^{n+1}+o(D^{n+1}),\quad \forall D\gg 1, \tag{7}$$

where $h_{\overline{\mathcal{O}(1)}_k}(X)$ denotes the height of the Zariski closure of X in $\mathbb{P}^N_{\mathcal{O}_K}$ with respect to $\overline{\mathcal{O}(1)}_k$. Since $\frac{1}{2}\mathcal{H}_{\mathrm{geom}}(X;D)\log\binom{D+N}{N}=o(D^{n+1})$ for $D\gg 1$, by Lemma 2.4, we get

$$\mathcal{H}_{\mathrm{arith}}(X;D,k) = \frac{h_{\overline{\mathcal{O}(1)}_k}(X)}{(n+1)!}D^{n+1}+o(D^{n+1}),\quad \forall D\gg 1. \tag{8}$$

Let $q_1,\dots,q_m\in K[x_0,\dots,x_N]^{\vee}$ be a K-basis of $\mathrm{Ann}(I_D)$. For any finite subset M in $\mathbb{N}_D^{N+1}$ of cardinal m, we set $q_M:=(q_{jb})_{1\le j\le m,b\in M}\in K^{m\times m}$ where the q_{jb} are such that $q_j=\sum_{b\in\mathbb{N}_D^{N+1}}q_{jb}(x^b)^{\vee}$. For any $v\in M_K^{\infty}$, we have

$$\begin{aligned}|q_1\wedge\cdots\wedge q_m|_v &= \max\{|\det(q_M)|_v : M\subset\mathbb{N}_D^{N+1},\ \mathrm{Card}(M)=m\}\\ &\le \Bigg(\sum_{M;\mathrm{Card}(M)=m}\Bigg(\prod_{b\in M}\langle b,b\rangle_{v,k}^{-1}\Bigg)|\det(q_M)|_v^2\Bigg)^{1/2}.\end{aligned} \tag{9}$$

(We use the inequality $\langle x^a,x^a\rangle_k=\int_{\mathbb{P}^N(\mathbb{C})}h_{\overline{\mathcal{O}(D)}_k}(x^a,x^a)\Omega_k\le 1$ for any $a\in\mathbb{N}_D^{N+1}$, which follows from $h_{\overline{\mathcal{O}(D)}_k}(x^a,x^a)\le h_{\overline{\mathcal{O}(D)}_\infty}(x^a,x^a)\le 1$ on $\mathbb{P}^N(\mathbb{C})$ and the facts that $\Omega_k>0$ on $\mathbb{P}^N(\mathbb{C})$ and $\int_{\mathbb{P}^N(\mathbb{C})}\Omega_k=1$.)

Then

$$|q_1\wedge\cdots\wedge q_m|_v\le\|q_1\wedge\cdots\wedge q_m\|_{k,v}^{\vee},\quad \forall k\in\mathbb{N}. \tag{10}$$

By Propositions 2.2 and 2.3, we get

$$\mathcal{H}_{\mathrm{norm}}(X;D)\le\mathcal{H}_{\mathrm{arith}}(X;D,k),\quad \forall k\in\mathbb{N}. \tag{11}$$

By (8), the previous inequality gives

$$\limsup_{D\to\infty}\frac{(n+1)!}{D^{n+1}}\mathcal{H}_{\mathrm{norm}}(X;D)\le h_{\overline{\mathcal{O}(1)}_k}(X),\quad \forall k\in\mathbb{N}. \tag{12}$$

We know that $(h_k)_{k\in\mathbb{N}}$ converges uniformly to h_∞ on $\mathbb{P}^N(\mathbb{C})$. Fix $0<\varepsilon<1$. Then there exists a $k_0\in\mathbb{N}$ such that, for any $k\geq k_0$, we have

$$(1-\varepsilon)^{2D}\leq\frac{(\max(|x_0|_v,\dots,|x_N|_v))^{2D}}{(|x_0|_v^{2k}+\cdots+|x_N|_v^{2k})^{D/k}}\leq(1+\varepsilon)^{2D},\quad\forall x\in\mathbb{P}^N(\mathbb{C}),\ \forall D\in\mathbb{N}.$$

Thus, for any $k\geq k_0$, $D\in\mathbb{N}_{\geq 1}$ and $a\in\mathbb{N}_D^{N+1}$, we get

$$\langle x^a,x^a\rangle_k\geq(1-\varepsilon)^{2D}\int_{\mathbb{P}^N(\mathbb{C})}h_\infty^{\otimes D}(x^a,x^a)\omega_k^N. \tag{13}$$

We have

$$\begin{aligned}
&\int_{\mathbb{P}^N(\mathbb{C})}h_\infty^{\otimes D}(x^a,x^a)\omega_k^N\\
&\qquad=\int_{\mathbb{C}^N}\frac{|z^{2a}|}{\max(1,|z_1|,\dots,|z_N|)^{2D}}\frac{k^N\prod_{i=1}^N|z_i|^{2(k-1)}\prod_{i=1}^N dz_i\wedge d\bar{z}_i}{\left(1+\sum_{i=1}^N|z_i^{2k}|\right)^{N+1}}\\
&\qquad=2^N\int_{(\mathbb{R}^+)^N}\frac{k^N r^{a+k-1}}{\max(1,r_1,\dots,r_N)^{2D}}\frac{\prod_{i=1}^N dr_i}{\left(1+\sum_{i=1}^N r_i^k\right)^{N+1}}\\
&\qquad=2^N\int_{(\mathbb{R}^+)^N}\frac{r^{a/k}}{\max_i(1,r_1,\dots,r_N)^{D/k}}\frac{\prod_{i=1}^N dr_i}{\left(1+\sum_{i=1}^N r_i^k\right)^{N+1}}\\
&\qquad=2^N\sum_{j=0}^N\int_{E_j}\frac{r^{a/k}}{\max_i(1,r_1,\dots,r_N)^{D/k}}\frac{\prod_{i=1}^N dr_i}{\left(1+\sum_{i=1}^N r_i\right)^{N+1}},
\end{aligned}$$

where $E_j:=\{x\in(\mathbb{R}^+)^N:x_j\geq 1,\ x_l\leq x_j \text{ for } l=1,\dots,N\}$ for $j=1,\dots,N$ and $E:=\{x\in(\mathbb{R}^+)^N:x_l\leq 1,\ \text{for } l=1,\dots,N\}$. Using the function

$$(\mathbb{R}^{*+})^N\to(\mathbb{R}^{*+})^N,\quad x=(x_1,\dots,x_N)\mapsto\left(\frac{x_1}{x_j},\dots,\frac{x_{j-1}}{x_j},\frac{1}{x_j},\dots,\frac{x_n}{x_j}\right),$$

for $j=1,\dots,N$, we can show that there exists a $b^{(j)}=(b_1^{(j)},\dots,b_N^{(j)})\in\mathbb{N}^N$ such that

$$\int_{E_j}\frac{r^{a/k}}{\max_i(1,r_1,\dots,r_N)^{D/k}}\frac{\prod_{i=1}^N dr_i}{\left(1+\sum_{i=1}^N r_i\right)^{N+1}}=\int_E r^{b^{(j)}/k}\frac{\prod_{i=1}^N dr_i}{\left(1+\sum_{i=1}^N r_i\right)^{N+1}}. \tag{14}$$

We set $b^{(0)}:=a$. Then

$$\int_{\mathbb{P}^N(\mathbb{C})}h_\infty^D(x^a,x^a)\omega_k^N=2^N\sum_{j=0}^N\int_E r^{b^{(j)}/k}\frac{\prod_{i=1}^N dr_i}{\left(1+\sum_{i=1}^N r_i\right)^{N+1}}. \tag{15}$$

Let $0<\delta<1$, and set $E_\delta := \{x \in E : x_l \geq \delta \text{ for } l = 1, \ldots, N\}$. From (13) and (15), we obtain

$$\langle x^a, x^a\rangle_k \geq (1-\varepsilon)^{2D} 2^N \sum_{j=0}^{N} \int_{E_\delta} r^{b^{(j)}/k} \frac{\prod_{i=1}^N dr_i}{\left(1+\sum_{i=1}^N r_i\right)^{N+1}} \geq (1-\varepsilon)^{2D} 2^N (N+1)\delta^{D/k}\mu_\delta,$$

where $\mu_\delta := \int_{E_\delta} \prod_{i=1}^N dr_i / \left(1+\sum_{i=1}^N r_i\right)^{N+1}$.

Thus,

$$\langle x^a, x^a\rangle_k^{-1} \leq (1-\varepsilon)^{-2D}\delta^{-D/k}{\mu_\delta}^{-1}, \quad \forall k \geq k_0,\ \forall D \in \mathbb{N}_{\geq 1},\ \forall a \in \mathbb{N}_D^{N+1}. \quad (16)$$

Then, for any $k \geq k_0$ and $D \geq D_1$,

$$\begin{aligned}
\|q_1 \wedge \cdots \wedge q_m\|_{k,v}^{\vee} &\leq \left(\sum_{M;\mathrm{Card}(M)=m} \left(\prod_{b\in M} \langle b, b\rangle_{v,k}^{-1}\right)\right)^{1/2} |q_1 \wedge \cdots \wedge q_m|_v \\
&\leq \mathrm{Card}\{M \subset \mathbb{N}_D^{N+1} : \mathrm{Card}(M) = m\}^{1/2} \\
&\qquad \times (1-\varepsilon)^{-mD}\delta^{-mD/k}\mu_\delta^{-m}|q_1 \wedge \cdots \wedge q_m|_v \\
&\leq \mathrm{Card}(\mathbb{N}_D^{N+1})(1-\varepsilon)^{-mD}\delta^{-mD/k}\mu_\delta^{-m}|q_1 \wedge \cdots \wedge q_m|_v \\
&= \binom{N+D}{N}^{1/2}(1-\varepsilon)^{-mD}\delta^{-mD/k}\mu_\delta^{-m}|q_1 \wedge \cdots \wedge q_m|_v, \quad (17)
\end{aligned}$$

where the second line follows by (16).

Therefore,

$$\begin{aligned}
&\mathcal{H}_{\mathrm{arith}}(X; D, k) \\
&\qquad \leq \mathcal{H}_{\mathrm{norm}}(X; D) + \tfrac{1}{2}\log\binom{N+D}{N} - D\mathcal{H}_{\mathrm{geom}}(X; D)\log(1-\varepsilon) \\
&\qquad\qquad - \frac{D\mathcal{H}_{\mathrm{geom}}(X; D)}{k}\log\delta - \mathcal{H}_{\mathrm{geom}}(X; D)\log\mu_\delta. \quad (18)
\end{aligned}$$

By (8), we obtain that

$$h_{\overline{\mathcal{O}(1)}_k}(X) \leq \liminf_{D\to\infty} \frac{(n+1)!}{D^{n+1}}\mathcal{H}_{\mathrm{norm}}(X; D) + O(\varepsilon) + \frac{\log\delta}{k}O(1), \quad \forall k \geq k_0. \quad (19)$$

Gathering (12) and (19), we conclude that, for any $0<\varepsilon<1$, there exists a $k_0 \in \mathbb{N}$ such that

$$\begin{aligned}
&\limsup_{D\to\infty} \frac{(n+1)!}{D^{n+1}}\mathcal{H}_{\mathrm{norm}}(X; D) \leq h_{\overline{\mathcal{O}(1)}_k}(X) \\
&\qquad \leq \liminf_{D\to\infty} \frac{(n+1)!}{D^{n+1}}\mathcal{H}_{\mathrm{norm}}(X; D) + O(\varepsilon) + \frac{\log\delta}{k}O(1), \quad \forall k \geq k_0. \quad (20)
\end{aligned}$$

Since $\lim_{k\to\infty} h_{\overline{\mathcal{O}(1)}_k}(X) = h_{\overline{\mathcal{O}(1)}_\infty}(X)$ (see for instance [Zhang 1995]) and since $h_{\overline{\mathcal{O}(1)}_\infty}(X) = \hat{h}(X)$ (see [Philippon and Sombra 2008, p. 342]), we get

$$\liminf_{D\to\infty} \frac{(n+1)!}{D^{n+1}} \mathcal{H}_{\mathrm{norm}}(X; D) = \limsup_{D\to\infty} \frac{(n+1)!}{D^{n+1}} \mathcal{H}_{\mathrm{norm}}(X; D) = \hat{h}(X). \tag{21}$$

Thus, we have proved Theorem 1.1. □

Acknowledgements

I am very grateful to Martín Sombra for his helpful conversations and encouragement during the preparation of this paper. I would like to thank Vincent Maillot for his useful discussions.

References

[Abbes and Bouche 1995] A. Abbes and T. Bouche, "Théorème de Hilbert–Samuel 'arithmétique"', *Ann. Inst. Fourier* (*Grenoble*) **45**:2 (1995), 375–401. MR 96e:14024 Zbl 0818.14011

[Amoroso and David 2003] F. Amoroso and S. David, "Minoration de la hauteur normalisée dans un tore", *J. Inst. Math. Jussieu* **2**:3 (2003), 335–381. MR 2004m:11101 Zbl 1041.11048

[David and Philippon 1999] S. David and P. Philippon, "Minorations des hauteurs normalisées des sous-variétés des tores", *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* (4) **28**:3 (1999), 489–543. MR 2001a:11109 Zbl 1002.11055

[Gillet and Soulé 1992] H. Gillet and C. Soulé, "An arithmetic Riemann–Roch theorem", *Invent. Math.* **110**:3 (1992), 473–543. MR 94f:14019 Zbl 0777.14008

[Philippon and Sombra 2008] P. Philippon and M. Sombra, "Hauteur normalisée des variétés toriques projectives", *J. Inst. Math. Jussieu* **7**:2 (2008), 327–373. MR 2010a:11125 Zbl 1147.11033

[Randriambololona 2001] H. Randriambololona, *Hauteurs pour les sous-schémas et exemples d'utilisation de méthodes arakeloviennes en théorie de l'approximation diophantienne*, Ph.D. thesis, Université Paris-Sud, 2001, available at http://www.infres.enst.fr/ randriam/maths/these.pdf.

[Randriambololona 2006] H. Randriambololona, "Métriques de sous-quotient et théorème de Hilbert–Samuel arithmétique pour les faisceaux cohérents", *J. Reine Angew. Math.* **590** (2006), 67–88. MR 2007d:14053 Zbl 1097.14020

[Zhang 1992] S. Zhang, "Positive line bundles on arithmetic surfaces", *Ann. of Math.* (2) **136**:3 (1992), 569–587. MR 93j:14024 Zbl 0788.14017

[Zhang 1995] S. Zhang, "Small points and adelic metrics", *J. Algebraic Geom.* **4**:2 (1995), 281–300. MR 96e:14025 Zbl 0861.14019

Communicated by Joseph Silverman
Received 2014-11-19 Revised 2015-09-10 Accepted 2015-10-15

hajli@math.sinica.edu.tw *Institute of Mathematics, Academia Sinica, 6F, Astronomy-Mathematics Building, No. 1, Sec. 4, Roosevelt Road, Taipei 10617, Taiwan*

ALGEBRA AND NUMBER THEORY 9:10 (2015)
dx.doi.org/10.2140/ant.2015.9.2303

msp

The abelian monoid of fusion-stable finite sets is free

Sune Precht Reeh

We show that the abelian monoid of isomorphism classes of G-stable finite S-sets is free for a finite group G with Sylow p-subgroup S; here a finite S-set is called G-stable if it has isomorphic restrictions to G-conjugate subgroups of S. These G-stable S-sets are of interest, e.g., in homotopy theory. We prove freeness by constructing an explicit (but somewhat nonobvious) basis, whose elements are in one-to-one correspondence with the G-conjugacy classes of subgroups in S. As a central tool of independent interest, we give a detailed description of the embedding of the Burnside ring for a saturated fusion system into its associated ghost ring.

1. Introduction

Finite G-sets, where G is a finite group, appear again and again throughout mathematics, e.g., in homotopy theory. In certain instances we are however interested, not in the G-sets themselves, but instead in the shadows cast by G-sets when we restrict the actions to a Sylow p-subgroup S of G. When a finite set X has an action of S that "looks like" it comes from a G-action, we say that the S-set X is G-stable (see below). G-stable S-sets occur for instance in homotopy theory when describing maps between classifying spaces. The isomorphism classes of these G-stable S-sets together form an abelian monoid with disjoint union as the addition. In this paper we construct a basis for the abelian monoid of G-stable sets when G is a finite group with Sylow p-subgroup S. Theorem A$'$ states that this abelian monoid is free, and that the basis elements are in one-to-one correspondence with the G-conjugacy classes of subgroups in S. Theorem A$'$ is a special case of the more general Theorem A formulated for a saturated fusion systems $\mathcal{F}$ over S. As a main tool for proving Theorem A we describe the Burnside ring of a saturated fusion system $\mathcal{F}$, and its embedding into the associated ghost ring (Theorem B).

Supported by the Danish National Research Foundation through the Centre for Symmetry and Deformation (DNRF92), and by The Danish Council for Independent Research's Sapere Aude programme (DFF — 4002-00224).

MSC2010: primary 20D20; secondary 20J15, 19A22.

Keywords: Fusion systems, Burnside rings, finite groups.

In more detail, let us consider a finite group G acting on a finite set X. We can restrict the action to a Sylow p-subgroup S of G. The resulting S-set has the property that it stays the same (up to S-isomorphism) whenever we change the action via a conjugation map from G. More precisely, if $P \leq S$ is a subgroup and $\varphi\colon P \to S$ is a homomorphism given by conjugation with some element of G, we can turn X into a P-set by using φ to define the action $p.x := \varphi(p)x$. We denote the resulting P-set by ${}_{P,\varphi}X$. In particular when $\mathrm{incl}\colon P \to S$ is the inclusion map, ${}_{P,\mathrm{incl}}X$ has the usual restricted action from S to P. When a finite S-set X is the restriction of a G-set, then X has the property

$$\begin{aligned}&{}_{P,\varphi}X \textit{ is isomorphic to } {}_{P,\mathrm{incl}}X \textit{ as } P\textit{-sets, for all } P \leq S \textit{ and homomorphisms}\\ &\varphi\colon P \to S \textit{ induced by } G\textit{-conjugation.}\end{aligned} \tag{1-1}$$

Any S-set with property (1-1) is called *G-stable*. Whenever we restrict a G-set to S, the resulting S-set is G-stable; however there are G-stable S-sets whose S-actions do not extend to actions of G.

The isomorphism classes of finite S-sets form a semiring $A_+(S)$ with disjoint union as addition and cartesian product as multiplication. The collection of G-stable S-sets is closed under addition and multiplication, hence G-stable sets form a subsemiring.

Theorem A′. *Let G be a finite group with Sylow p-group S. Every G-stable S-set splits uniquely, up to S-isomorphism, as a disjoint union of irreducible G-stable sets, and there is a one-to-one correspondence between the irreducible G-stable sets and G-conjugacy classes of subgroups in S.*

Hence the semiring of G-stable S-sets is additively a free commutative monoid with rank equal to the number of G-conjugacy classes of subgroups in S.

As part of the proof we give an explicit construction of the irreducible G-stable sets (see Proposition 4.8).

It is a well-known fact that any finite S-set splits uniquely into orbits (i.e., transitive S-sets), and the isomorphism type of a transitive set S/P depends only on the subgroup P up to S-conjugation. Theorem A′ states that this fact generalizes nicely to G-stable S-sets, which turns out to be less obvious than it might first appear.

If we consider G-sets and restrict their actions to S, then two nonisomorphic G-sets might very well become isomorphic as S-sets. Therefore even though finite G-sets decompose uniquely into orbits, we have no guarantee that this decomposition remains unique when we restrict the actions to the Sylow subgroup S. In fact, uniqueness of decompositions fails in general when we consider restrictions of G-sets to S, as demonstrated in Example 4.3 for the symmetric group Σ_5 and a Sylow 2-subgroup. It is therefore perhaps a surprise that if we consider *all* G-stable

S-sets, and not just the restrictions of actual G-sets, we are again able to write stable sets as a disjoint union of irreducibles in a unique way.

It is also worth noting that the analogue of Theorem A′ is false if we consider representations instead of sets: the submonoid of G-stable S-representations is not a free submonoid of the free monoid of complex S-representations when $G = \mathrm{PGL}_3(\mathbb{F}_3)$ and $p = 2$. We explain this counterexample in the Appendix, in particular in Example A.2.

The proof of Theorem A′ relies only on the way G acts on the subgroups of S by conjugation. We therefore state and prove the theorem in general for abstract saturated fusion systems, which abstractly model the conjugacy relations within a p-group induced by an ambient group (see Definitions 2.1 and 2.2).

If $\mathcal{F}$ is a fusion system over a p-group S, we say that an S-set X is *$\mathcal{F}$-stable* if it satisfies

$$\begin{aligned}&{}_{P,\varphi}X \text{ is isomorphic to } {}_{P,\mathrm{incl}}X \text{ as } P\text{-sets, for all } P \le S \text{ and homomorphisms}\\ &\varphi\colon P \to S \text{ in } \mathcal{F}.\end{aligned} \tag{1-2}$$

The $\mathcal{F}$-stable S-sets form a semiring $A_+(\mathcal{F})$ since the disjoint union and cartesian product of $\mathcal{F}$-stable sets is again $\mathcal{F}$-stable. Theorem A′ then generalizes to Theorem A below, which we prove instead.

Theorem A. *Let $\mathcal{F}$ be a saturated fusion system over a p-group S. Every $\mathcal{F}$-stable S-set splits uniquely, up to S-isomorphism, as a disjoint union of irreducible $\mathcal{F}$-stable sets, and there is a one-to-one correspondence between the irreducible $\mathcal{F}$-stable sets and conjugacy/isomorphism classes of subgroups in the fusion system $\mathcal{F}$.*

Hence the semiring $A_+(\mathcal{F})$ of $\mathcal{F}$-stable S-sets is additively a free commutative monoid with rank equal to the number of conjugacy classes of subgroups in $\mathcal{F}$.

One application of Theorem A is in homotopy theory, where classifying spaces for groups and maps between them play an important role. For finite groups G, H, or in general discrete groups, the homotopy classes of unbased maps $[BG, BH]$ is in bijection with $\mathrm{Rep}(G, H) = H\backslash\mathrm{Hom}(G, H)$, where H acts on $\mathrm{Hom}(G, H)$ by postconjugation. Hence $[BG, B\Sigma_n]$ corresponds to the different ways G can act on a set with n elements up to G-isomorphism. This implies that for a finite group G we have $[BG, \coprod_n B\Sigma_n] \cong A_+(G)$ as monoids.

However in homotopy theory one is often only interested in studying classifying spaces, and maps between them, one prime at a time via the Bousfield–Kan p-completion functor $(-)^\wedge_p$ [1972, Sections I.1, VI.6 and VII.5]. In this context, when S is a p-group, a formula of Mislin [1990, Formula 4] says that S satisfies

$$[BS, \coprod_n (B\Sigma_n)^\wedge_p] \simeq A_+(S)$$

as monoids. (See also [Dwyer and Zabrodsky 1987; Lannes 1995; Miller 1987; Carlsson 1991] which Mislin's work builds upon.) For a general finite group G, the monoid $[BG, \coprod_n (B\Sigma_n)^\wedge_p]$ is highly interesting but still mysterious. Restriction along the inclusion $\iota\colon S \to G$ of a Sylow p-subgroup induces a map

$$\iota^*\colon [BG, \coprod_n (B\Sigma_n)^\wedge_p] \to [BS, \coprod_n (B\Sigma_n)^\wedge_p] \simeq A_+(S),$$

and the image must necessarily be contained in the collection of G-stable sets $A_+(\mathcal{F}_S(G))$, where $\mathcal{F}_S(G)$ is the fusion system over S generated by G.

The map $\iota^*\colon [BG, \coprod_n (B\Sigma_n)^\wedge_p] \to A_+(\mathcal{F}_S(G))$ is an isomorphism in the cases where both the left-hand side and the right-hand side have been calculated, though both injectivity and surjectivity is currently unknown in general. In any case, Theorem A shows that the algebraic approximation $A_+(\mathcal{F}_S(G))$ has a very regular structure for any finite group G, and hence provides information in understanding the monoid on the left-hand side.

An important tool in proving Theorem A is *the Burnside ring of* $\mathcal{F}$, denoted by $A(\mathcal{F})$. We can either define $A(\mathcal{F})$ as the Grothendieck group of the semiring $A_+(\mathcal{F})$ of $\mathcal{F}$-stable sets, or we can define $A(\mathcal{F})$ as the subring of $A(S)$ consisting of all $\mathcal{F}$-stable elements, where the $\mathcal{F}$-stable elements satisfy a property similar to (1-2). Thanks to Proposition 4.4 we know that these two definitions coincide for saturated fusion systems.

We note that there is an earlier definition by Diaz and Libman [2009a] of a Burnside ring for $\mathcal{F}$, only involving the so-called $\mathcal{F}$-centric subgroups of S, while the Burnside ring defined here concerns *all* subgroups of S in relation to the fusion system $\mathcal{F}$. More precisely, after p-localization the Diaz-Libman *centric* Burnside ring for $\mathcal{F}$ is the quotient of the Burnside ring $A(\mathcal{F})$ defined here by the noncentric part of $A(\mathcal{F})$, as described in [Díaz and Libman 2009b, Theorem A] and even further in [Reeh 2016, Proposition 4.8].

The Burnside ring of $\mathcal{F}$ inherits the homomorphism of marks Φ from $A(S)$ by restriction, embedding $A(\mathcal{F})$ into a product of a suitable number of copies of $\mathbb{Z}$. As a main step in proving Theorem A, we show that this mark homomorphism has properties analogous the mark homomorphism for groups:

Theorem B. *Let $\mathcal{F}$ be a saturated fusion system over a p-group S, and let $A(\mathcal{F})$ be the Burnside ring of $\mathcal{F}$, i.e., the subring consisting of the $\mathcal{F}$-stable elements in the Burnside ring of S. Then there is a ring homomorphism Φ and a group homomorphism Ψ that fit together in the following short exact-sequence of groups*:

$$0 \longrightarrow A(\mathcal{F}) \xrightarrow{\Phi} \prod_{\substack{\text{conj. classes of}\\ \text{subgroups in } \mathcal{F}}} \mathbb{Z} \xrightarrow{\Psi} \prod_{\substack{[P]_\mathcal{F} \text{ conj. class of}\\ \text{subgroups in } \mathcal{F}}} \mathbb{Z}/|W_S P|\mathbb{Z} \longrightarrow 0,$$

where $P \leq S$ is a fully $\mathcal{F}$-normalized representative of $[P]_\mathcal{F}$, and $W_S P := N_S P / P$.

The map Φ comes from restricting the mark homomorphism of $A(S)$, and Ψ is given by the $[P]_{\mathcal{F}}$-coordinate functions

$$\Psi_P(f) := \sum_{\bar{s}\in W_S P} f_{\langle s\rangle P} \pmod{|W_S P|}$$

when P is a fully normalized representative of the conjugacy class $[P]_{\mathcal{F}}$ of subgroups in $\mathcal{F}$. Here $\Psi_P = \Psi_{P'}$ if $P \sim_{\mathcal{F}} P'$ are both fully normalized.

Theorem B generalizes previous results by Burnside, Dress and others (see [Dress 1986], [tom Dieck 1979, Section 1] or [Yoshida 1990]) concerning the mark homomorphism and congruence relations for Burnside rings of finite groups, and such congruence relations can for instance be used, in [Reeh 2016, Corollary 6.6], for determining idempotents in $A(\mathcal{F})_{(p)}$. As with Theorem A, Theorem B is interesting from the viewpoint of homotopy theory: Grodal has recently announced [2011; $\geq$ 2015] that the map on Grothendieck groups

$$\mathrm{Gr}([BG, \coprod_n (B\Sigma_n)^\wedge_p]) \to A(\mathcal{F}_S(G))$$

is an isomorphism, so Theorem B also provides information about a homotopical object via this map.

2. Fusion systems

The next few pages contain a very short introduction to fusion systems. The aim is to introduce the terminology from the theory of fusion systems that will be used in the paper, and to establish the relevant notation. For a proper introduction to fusion systems see for instance Part I of "*Fusion systems in algebra and topology*" by Aschbacher, Kessar and Oliver [2011].

Definition 2.1. A *fusion system* $\mathcal{F}$ over a p-group S, is a category where the objects are the subgroups of S, and for all $P, Q \leq S$ the morphisms must satisfy:

(i) Every morphism $\varphi \in \mathrm{Mor}_{\mathcal{F}}(P, Q)$ is an injective group homomorphism, and the composition of morphisms in $\mathcal{F}$ is just composition of group homomorphisms.

(ii) $\mathrm{Hom}_S(P, Q) \subseteq \mathrm{Mor}_{\mathcal{F}}(P, Q)$, where

$$\mathrm{Hom}_S(P, Q) = \{c_s \mid s \in N_S(P, Q)\}$$

is the set of group homomorphisms $P \to Q$ induced by S-conjugation.

(iii) For every morphism $\varphi \in \mathrm{Mor}_{\mathcal{F}}(P, Q)$, the group isomorphisms $\varphi\colon P \to \varphi P$ and $\varphi^{-1}\colon \varphi P \to P$ are elements of $\mathrm{Mor}_{\mathcal{F}}(P, \varphi P)$ and $\mathrm{Mor}_{\mathcal{F}}(\varphi P, P)$, respectively.

We also write $\mathrm{Hom}_{\mathcal{F}}(P, Q)$ or just $\mathcal{F}(P, Q)$ for the morphism set $\mathrm{Mor}_{\mathcal{F}}(P, Q)$; the group $\mathcal{F}(P, P)$ of automorphisms is denoted by $\mathrm{Aut}_{\mathcal{F}}(P)$.

The canonical example of a fusion system comes from a finite group G with a given p-subgroup S. The fusion system of G over S, denoted $\mathcal{F}_S(G)$, is the fusion system over S where the morphisms from $P \leq S$ to $Q \leq S$ are the homomorphisms induced by G-conjugation:

$$\mathrm{Hom}_{\mathcal{F}_S(G)}(P, Q) := \mathrm{Hom}_G(P, Q) = \{c_g \mid g \in N_G(P, Q)\}.$$

A particular case is the fusion system $\mathcal{F}_S(S)$ consisting only of the homomorphisms induced by S-conjugation.

Let $\mathcal{F}$ be an abstract fusion system over S. We say that two subgroup $P, Q \leq S$ are *$\mathcal{F$-conjugate*, written $P \sim_{\mathcal{F}} Q$, if they are isomorphic in $\mathcal{F}$, i.e., there exists a group isomorphism $\varphi \in \mathcal{F}(P, Q)$. The relation of $\mathcal{F}$-conjugation is an equivalence relation, and the set of $\mathcal{F}$-conjugates to P is denoted by $[P]_{\mathcal{F}}$. The set of all $\mathcal{F}$-conjugacy classes of subgroups in S is denoted by $\mathrm{Cl}(\mathcal{F})$. Similarly, we write $P \sim_S Q$ if P and Q are S-conjugate, the S-conjugacy class of P is written $[P]_S$ or just $[P]$, and we write $\mathrm{Cl}(S)$ for the set of S-conjugacy classes of subgroups in S. Since all S-conjugation maps are in $\mathcal{F}$, any $\mathcal{F}$-conjugacy class $[P]_{\mathcal{F}}$ can be partitioned into disjoint S-conjugacy classes of subgroups $Q \in [P]_{\mathcal{F}}$.

We say that Q is $\mathcal{F}$- or S-*subconjugate* to P if Q is respectively $\mathcal{F}$- or S-conjugate to a subgroup of P, and we denote this by $Q \lesssim_{\mathcal{F}} P$ or $Q \lesssim_S P$, respectively. In the case where $\mathcal{F} = \mathcal{F}_S(G)$, we have $Q \lesssim_{\mathcal{F}} P$ if and only if Q is G-conjugate to a subgroup of P; the $\mathcal{F}$-conjugates of P are just those G-conjugates of P which are contained in S.

A subgroup $P \leq S$ is said to be *fully $\mathcal{F}$-normalized* if $|N_S P| \geq |N_S Q|$ for all $Q \in [P]_{\mathcal{F}}$; similarly P is *fully $\mathcal{F}$-centralized* if $|C_S P| \geq |C_S Q|$ for all $Q \in [P]_{\mathcal{F}}$.

Definition 2.2. A fusion system $\mathcal{F}$ over S is said to be *saturated* if the following properties are satisfied for all $P \leq S$:

(i) If P is fully $\mathcal{F}$-normalized, then P is fully $\mathcal{F}$-centralized, and $\mathrm{Aut}_S(P)$ is a Sylow p-subgroup of $\mathrm{Aut}_{\mathcal{F}}(P)$).

(ii) Every homomorphism $\varphi \in \mathcal{F}(P, S)$ where $\varphi(P)$ is fully $\mathcal{F}$-centralized, extends to a homomorphism $\varphi \in \mathcal{F}(N_\varphi, S)$ where

$$N_\varphi := \{x \in N_S(P) \mid \exists y \in S \colon \varphi \circ c_x = c_y \circ \varphi\}.$$

The saturated fusion systems form a class of particularly nice fusion systems, and the saturation axiom are a way to emulate the Sylow theorems for finite groups. In particular, whenever S is a Sylow p-subgroup of G, then the Sylow theorems imply that the induced fusion system $\mathcal{F}_S(G)$ is saturated (see for instance [Aschbacher et al. 2011, Theorem 2.3]).

In this paper, we shall rarely use the defining properties of saturated fusion systems directly. We shall instead mainly use the following lifting property that saturated fusion systems satisfy:

Lemma 2.3 [Roberts and Shpectorov 2009]. *Let $\mathcal{F}$ be saturated. Suppose that $P \leq S$ is fully normalized. Then for each $Q \in [P]_{\mathcal{F}}$ there exists a homomorphism $\varphi \in \mathcal{F}(N_S Q, N_S P)$ with $\varphi(Q) = P$.*

For the proof, see Lemma 4.5 of [Roberts and Shpectorov 2009] or Lemma 2.6(c) of [Aschbacher et al. 2011].

3. Burnside rings for groups

In this section we consider the Burnside ring of a finite group S, and the semiring of finite S-sets. We recall the structure of the Burnside ring $A(S)$ and how to describe the elements and operations of $A(S)$ in terms of fixed points and the homomorphism of marks. In this section S can be any finite group, but later we shall only need the case where S is a p-group.

We consider finite S-sets up to S-isomorphism, and let $A_+(S)$ denote the set of isomorphism classes. Given a finite S-set X, we denote the isomorphism class of X by $[X] \in A_+(S)$. Taking disjoint union as addition and cartesian product as multiplication gives a commutative semiring structure on $A_+(S)$. Additively, $A_+(S)$ is a free commutative monoid, where the basis consists of the (isomorphism classes of) transitive S sets, i.e., $[S/P]$ where P is a subgroup of S. Two transitive S-sets S/P and S/Q are isomorphic if and only if P is conjugate to Q in S.

To describe the multiplication of the semiring $A_+(S)$, it is enough to know the products of basis elements $[S/P]$ and $[S/Q]$. By taking the product $(S/P) \times (S/Q)$ and considering how it breaks into orbits, one reaches the following double coset formula for the multiplication in $A_+(S)$:

$$[S/P] \cdot [S/Q] = \sum_{s \in [P \backslash S/Q]} [S/(P \cap {}^s Q)], \tag{3-1}$$

where $[P \backslash S/Q]$ is a set of representative of the double cosets PsQ with $s \in S$.

The *Burnside ring of* S, denoted $A(S)$, is constructed as the Grothendieck group of $A_+(S)$, consisting of formal differences of finite S-sets. Additively, $A(S)$ is a free abelian group with the same basis as $A_+(S)$. For each element $X \in A(S)$ we define $c_P(X)$, with $P \leq S$, to be the coefficients when we write X as a linear combination of the basis elements $[S/P]$ in $A(S)$, i.e.,

$$X = \sum_{[P] \in \mathrm{Cl}(S)} c_P(X) \cdot [S/P],$$

where $\mathrm{Cl}(S)$ denotes the set of S-conjugacy classes of subgroup in S.

The resulting maps $c_P\colon A(S) \to \mathbb{Z}$ are group homomorphisms, but they are *not* ring homomorphisms. Note also that an element X is in $A_+(S)$, i.e., X is an S-set, if and only if $c_P(X) \geq 0$ for all $P \leq S$.

Instead of counting orbits, an alternative way of characterising an S-set is counting the fixed points for each subgroup $P \leq S$. For every $P \leq S$ and S-set X, we denote the number of fixed points by $\Phi_P(X) := |X^P|$, and this number only depends on P up to S-conjugation. Since we have

$$|(X \sqcup Y)^P| = |X^P| + |Y^P| \quad \text{and} \quad |(X \times Y)^P| = |X^P| \cdot |Y^P|$$

for all S-sets X and Y, the *fixed point map* $\Phi_P\colon A_+(S) \to \mathbb{Z}$ extends to a ring homomorphism $\Phi_P\colon A(S) \to \mathbb{Z}$. On the basis elements $[S/P]$, the number of fixed points is given by

$$\Phi_Q([S/P]) = |(S/P)^Q| = \frac{|N_S(Q, P)|}{|P|},$$

where $N_S(Q, P) = \{s \in S \mid {}^sQ \leq P\}$ is the transporter in S from Q to P. In particular, $\Phi_Q([S/P]) \neq 0$ if and only if $Q \lesssim_S P$ (Q is conjugate to a subgroup of P).

We have one fixed point homomorphism Φ_P per conjugacy class of subgroups in S, and we combine them into the *homomorphism of marks*

$$\Phi = \Phi^S\colon A(S) \xrightarrow{\prod_{[P]} \Phi_P} \prod_{[P] \in \mathrm{Cl}(S)} \mathbb{Z}.$$

This ring homomorphism maps $A(S)$ into the product ring $\widetilde{\Omega}(S) := \prod_{[P]\in \mathrm{Cl}(S)} \mathbb{Z}$ which is the so-called *ghost ring* for the Burnside ring $A(S)$.

Results by Burnside, Dress and others show that the mark homomorphism is injective, and that the *obstruction group* $\mathrm{Obs}(S) := \prod_{[P]\in \mathrm{Cl}(S)} (\mathbb{Z}/|W_S P|\mathbb{Z})$, where $W_S P := N_S P/P$, is the cokernel of Φ. These statements are combined in the following proposition, the proof of which can be found in [Dress 1986], [tom Dieck 1979, Chapter 1] and [Yoshida 1990, Lemma 2.1].

Proposition 3.1. *Let* $\Psi = \Psi^S\colon \widetilde{\Omega}(S) \to \mathrm{Obs}(S)$ *be given by the* $[P]$*-coordinate functions*

$$\Psi_P(\xi) := \sum_{\bar{s} \in W_S P} \xi_{\langle s \rangle P} \pmod{|W_S P|}.$$

Here $\xi_{\langle s \rangle P}$ *denotes the* $[\langle s \rangle P]$*-coordinate of an element* $\xi \in \widetilde{\Omega}(S) = \prod_{[P]\in \mathrm{Cl}(S)} \mathbb{Z}$.

The following sequence of abelian groups is then exact:

$$0 \longrightarrow A(S) \xrightarrow{\Phi} \widetilde{\Omega}(S) \xrightarrow{\Psi} \mathrm{Obs}(S) \longrightarrow 0.$$

Moreover, Φ *is a ring homomorphism, while* Ψ *is just a group homomorphism.*

The strength of this result is that it enables one to perform calculations for the Burnside ring $A(S)$ inside the much nicer product ring $\widetilde{\Omega}(S)$, where we identify each element $X \in A(S)$ with its fixed point vector $(\Phi_Q(X))_{[Q]\in \mathrm{Cl}(S)}$.

Corollary 3.2. *For a normal subgroup $P \leq S$, and an S-set X, we have*

$$\sum_{\bar{s}\in S/P} \Phi_{\langle s\rangle P}(X) \equiv 0 \pmod{|S/P|}.$$

Proof. Applying Proposition 3.1 with $W_S P = S/P$, gives $\Psi_P(\Phi(X)) = 0$ in $\mathbb{Z}/|P/S|\mathbb{Z}$. □

4. Stable sets for a fusion system

Let $\mathcal{F}$ be a fusion system over a p-group S. In this section we rephrase the property of $\mathcal{F}$-stability in terms of the fixed point homomorphisms, and show in Example 4.3 how Theorem A can fail for a group G if we only consider S-sets that are restrictions of G-sets, instead of considering all G-stable sets. We also consider two possible definitions for the Burnside ring of a fusion system — these agree if $\mathcal{F}$ is saturated. The proof of Theorem A begins in Section 4.1 in earnest.

A finite S-set X is said to be *$\mathcal{F}$-stable* if it satisfies (1-2):

> *${}_{P,\varphi}X$ is isomorphic to ${}_{P,\mathrm{incl}}X$ as P-sets, for all $P \leq S$ and homomorphisms $\varphi\colon P \to S$ in $\mathcal{F}$.*

In order to define $\mathcal{F}$-stability not just for S-sets, but for all elements of the Burnside ring, we extend ${}_{P,\varphi}X$ to all $X \in A(S)$. Given a homomorphism $\varphi \in \mathcal{F}(P, S)$ and an S-set X, the P-set ${}_{P,\varphi}X$ was defined as X with the action restricted along φ, that is $p.x := \varphi(p)x$ for $x \in X$ and $p \in P$. This construction then extends linearly to a ring homomorphism $r_\varphi\colon A(S) \to A(P)$, and we denote ${}_{P,\varphi}X := r_\varphi(X)$ for all $X \in A(S)$. In this way (1-2) makes sense for all $X \in A(S)$.

It is possible to state $\mathcal{F}$-stability purely in terms of fixed points and the homomorphism of marks for $A(S)$. The following lemma seems to be generally known, but not published anywhere, so we include it for the sake of completeness. A version of this lemma was included in the Ph.D. thesis of Gelvin [2010, Proposition 3.2.3], and previously the lemma has at least been implicitly used by Broto, Levi and Oliver [2003, Proof of Proposition 5.5]. A special case of the lemma, for bisets, was also proved by Ragnarsson and Stancu [2013, Lemma 4.8, parts (b) and (c)].

Lemma 4.1 [Gelvin 2010]. *The following are equivalent for all elements $X \in A(S)$:*

(i) ${}_{P,\varphi}X = {}_{P,\mathrm{incl}}X$ *in $A(P)$ for all $\varphi \in \mathcal{F}(P, S)$ and $P \leq S$.*

(ii) $\Phi_P(X) = \Phi_{\varphi P}(X)$ *for all $\varphi \in \mathcal{F}(P, S)$ and $P \leq S$.*

(iii) $\Phi_P(X) = \Phi_Q(X)$ *for all pairs $P, Q \leq S$ with $P \sim_{\mathcal{F}} Q$.*

We shall primarily use (ii) and (iii) to characterize $\mathcal{F}$-stability.

Proof. Let $\Phi^P\colon A(P) \to \widetilde{\Omega}(P)$ be the homomorphism of marks for $A(P)$, and note that $\Phi^P_R({}_{P,\mathrm{incl}}X) = \Phi_R(X)$ for all $R \leq P \leq S$.

By the definition of the P-action on ${}_{P,\varphi}X$, we have $({}_{P,\varphi}X)^R = X^{\varphi R}$ for any S-set X and all subgroups $R \leq P$. This generalizes to

$$\Phi^P_R({}_{P,\varphi}X) = \Phi_{\varphi R}(X)$$

for $X \in A(S)$.

Assume (i). Then we immediately get

$$\Phi_P(X) = \Phi^P_P({}_{P,\mathrm{incl}}X) = \Phi^P_P({}_{P,\varphi}X) = \Phi_{\varphi P}(X)$$

for all $P \leq S$ and $\varphi \in \mathcal{F}(P, S)$, which proves (i)⇒(ii).

Assume (ii). Let $P \leq S$ and $\varphi \in \mathcal{F}(P, S)$. By assumption, we have $\Phi_{\varphi R}(X) = \Phi_R(X)$ for all $R \leq P$, hence

$$\Phi^P_R({}_{P,\varphi}X) = \Phi_{\varphi R}(X) = \Phi_R(X) = \Phi^P_R({}_{P,\mathrm{incl}}X).$$

Since Φ^P is injective, we get ${}_{P,\varphi}X = {}_{P,\mathrm{incl}}X$; so (ii)⇒(i).

Finally, we have (ii)⇔(iii) because Q is $\mathcal{F}$-conjugate to P exactly when Q is the image of a map $\varphi \in \mathcal{F}(P, S)$ in the fusion system. □

Definition 4.2. We let $A_+(\mathcal{F}) \subseteq A_+(S)$ be the set of all the $\mathcal{F}$-stable sets, and by property (iii) the sums and products of stable elements are still stable, so $A_+(\mathcal{F})$ is a subsemiring of $A_+(S)$.

Suppose that $\mathcal{F} = \mathcal{F}_S(G)$ is the fusion system for a group with $S \in \mathrm{Syl}_p(G)$. Let $X \in A_+(G)$ be a G-set, and let ${}_{S,\mathrm{incl}}X$ be the same set with the action restricted to the Sylow p-subgroup S. If we let $P \leq S$ and $c_g \in \mathrm{Hom}_{\mathcal{F}_S(G)}(P, S)$ be given, then $x \mapsto gx$ is an isomorphism ${}_{P,\mathrm{incl}}X \cong {}_{P,c_g}X$ of P-sets. The restriction ${}_{S,\mathrm{incl}}X$ is therefore G-stable.

Restricting the group action from G to S therefore defines a homomorphism of semirings $A_+(G) \to A_+(\mathcal{F}_S(G))$, but as the following example shows, this map need not be injective or surjective.

Example 4.3. The symmetric group Σ_5 on 5 letters has Sylow 2-subgroups isomorphic to the dihedral group D_8 of order 8. We then consider D_8 as embedding in Σ_5 as one of the Sylow 2-subgroups. Let H, K be respectively Sylow 3- and 5-subgroups of Σ_5.

The transitive Σ_5-set $[\Sigma_5/H]$ contains 40 elements and all the stabilizers have odd order (they are conjugate to H). When we restrict the action to D_8, the stabilizers therefore become trivial so the D_8-action is free, hence $[\Sigma_5/H]$ restricts to the D_8-set $5 \cdot [D_8/1]$, that is 5 disjoint copies of the free orbit $[D_8/1]$. Similarly, the transitive Σ_5-set $[\Sigma_5/K]$ restricts to $3 \cdot [D_8/1]$.

These two restrictions of Σ_5-sets are not linearly independent as D_8-sets — the Σ_5-sets $3\cdot[\Sigma_5/H]$ and $5\cdot[\Sigma_5/K]$ both restrict to $15\cdot[D_8/1]$. If the restrictions of Σ_5-sets were to form a free abelian monoid, then the set $[D_8/1]$ would have to be the restriction of an Σ_5-set as well; since $[D_8/1]$ is irreducible as a D_8-set, it would have to be the restriction of an irreducible (hence transitive) Σ_5-set. However Σ_5 has no subgroup of index 8, hence there is no transitive Σ_5 with 8 elements.

This shows that the restrictions of Σ_5-sets to D_8 do not form a free abelian monoid, and we also see that $[D_8/1]$ is an example of an $\mathcal{F}_{D_8}(\Sigma_5)$-stable set ($\Phi_1([D_8/1])=8$ and $\Phi_Q([D_8/1])=0$ for $1\neq Q\leq D_8$) which cannot be given the structure of a Σ_5-set.

To define the Burnside ring of a fusion system $\mathcal{F}$, we have two possibilities. We can consider the semiring of all the $\mathcal{F}$-stable S-sets and take the Grothendieck group of this. Alternatively, we can first take the Grothendieck group for all S-sets to get the Burnside ring of S, and then afterwards we consider the subring herein consisting of all the $\mathcal{F}$-stable elements. The following proposition implies that the two definitions coincide for saturated fusion systems.

Proposition 4.4. *Let $\mathcal{F}$ be a fusion system over a p-group S, and consider the subsemiring $A_+(\mathcal{F})$ of $\mathcal{F}$-stable S-sets in the semiring $A_+(S)$ of finite S-sets.*

This inclusion induces a ring homomorphism from the Grothendieck group of $A_+(\mathcal{F})$ to the Burnside ring $A(S)$, which is injective.

If $\mathcal{F}$ is saturated, then the image of the homomorphism is the subring of $A(S)$ consisting of the $\mathcal{F}$-stable elements.

Proof. Let Gr be the Grothendieck group of $A_+(\mathcal{F})$, and let $I\colon \mathrm{Gr}\to A(S)$ be the induced group homomorphism coming from the inclusion $i\colon A_+(\mathcal{F})\hookrightarrow A_+(S)$.

An element of Gr is a formal difference $X-Y$ where X and Y are $\mathcal{F}$-stable sets. Assume now that $X-Y$ lies in $\ker I$. This means that $i(X)-i(Y)=0$ in $A(S)$; since $A_+(S)$ is a free commutative monoid, we conclude that $i(X)=i(Y)$ as S-sets. But i is just the inclusion map, so we must have $X=Y$ in $A_+(\mathcal{F})$ as well, and $X-Y=0$ in Gr. Hence $I\colon \mathrm{Gr}\to A(S)$ is injective.

It is clear that the difference of two $\mathcal{F}$-stable sets is still $\mathcal{F}$-stable, so $\operatorname{im} I$ lies in the subring of $\mathcal{F}$-stable elements. If $\mathcal{F}$ is saturated, then the converse holds, and all $\mathcal{F}$-stable elements of $A(S)$ can be written as a difference of $\mathcal{F}$-stable sets; however the proof of this must be postponed to Corollary 4.11 below. □

Definition 4.5. Let $\mathcal{F}$ be saturated. We define *the Burnside ring of $\mathcal{F}$*, denoted $A(\mathcal{F})$, to be the subring consisting of the $\mathcal{F}$-stable elements in $A(S)$.

Once we have proven Corollary 4.11, we will know that $A(\mathcal{F})$ is also the Grothendieck group of the semiring $A_+(\mathcal{F})$ of $\mathcal{F}$-stable sets.

4.1. ***Proving Theorems A and B.*** The proof of Theorem A falls into several parts. We begin by constructing some $\mathcal{F}$-stable sets α_P satisfying certain properties — this is the content of 4.6–4.8. We construct one α_P per $\mathcal{F}$-conjugacy class of subgroups, and these are the $\mathcal{F}$-stable sets which we will later show are the irreducible stable sets. A special case of the construction was originally used by Broto, Levi and Oliver [2003, Proposition 5.5] to show that every saturated fusion system has a characteristic biset.

In 4.9–4.11 we then proceed to show that the constructed α_P's are linearly independent, and that they generate the Burnside ring $A(\mathcal{F})$. When proving that the α_P's generate $A(\mathcal{F})$, the same proof also establishes Theorem B.

Finally, we use the fact that the α_P's form a basis for the Burnside ring, to argue that they form an additive basis already for the semiring $A_+(\mathcal{F})$, completing the proof of Theorem A itself.

As mentioned, we first construct an $\mathcal{F}$-stable set α_P for each $\mathcal{F}$-conjugacy class of subgroups. The idea when constructing α_P is that we start with the single orbit $[S/P]$ which we then stabilize: we run through the subgroups $Q \leq S$ in decreasing order and add orbits to the constructed S-set until it becomes $\mathcal{F}$-stable at the conjugacy class of Q in $\mathcal{F}$. The stabilization procedure is handled in the following technical Lemma 4.6, which is then applied in Proposition 4.8 to construct the α_P's.

Recall that $c_P(X)$ denotes the number of (S/P)-orbits in X, and $\Phi_P(X)$ denotes the number of P-fixed points.

Lemma 4.6. *Let $\mathcal{F}$ be a saturated fusion system over a p-group S, and let $\mathcal{H}$ be a collection of subgroups of S such that $\mathcal{H}$ is closed under taking $\mathcal{F}$-subconjugates, i.e., if $P \in \mathcal{H}$, then $Q \in \mathcal{H}$ for all $Q \lesssim_{\mathcal{F}} P$.*

Assume that $X \in A_+(S)$ is an S-set satisfying $\Phi_P(X) = \Phi_{P'}(X)$ for all pairs $P \sim_{\mathcal{F}} P'$, with $P, P' \notin \mathcal{H}$. Assume furthermore that $c_P(X) = 0$ for all $P \in \mathcal{H}$.

Then there exists an $\mathcal{F}$-stable set $X' \in A_+(\mathcal{F}) \subseteq A_+(S)$ satisfying $\Phi_P(X') = \Phi_P(X)$ and $c_P(X') = c_P(X)$ for all $P \notin \mathcal{H}$, and $c_P(X') = c_P(X)$ for all $P \leq S$ which are fully normalized in $\mathcal{F}$. In particular, for a $P \in \mathcal{H}$ which is fully normalized, we have $c_P(X') = 0$.

Proof. We proceed by induction on the size of the collection $\mathcal{H}$. If $\mathcal{H} = \varnothing$, then X is $\mathcal{F}$-stable by assumption, so $X' := X$ works.

Assume that $\mathcal{H} \neq \varnothing$, and let $P \in \mathcal{H}$ be maximal under $\mathcal{F}$-subconjugation as well as fully normalized.

Let $P' \sim_{\mathcal{F}} P$. Then there is a homomorphism $\varphi \in \mathcal{F}(N_S P', N_S P)$ with $\varphi(P') = P$ by Lemma 2.3 since $\mathcal{F}$ is saturated. The restriction of S-actions to $\varphi(N_S P')$ gives a ring homomorphism $A(S) \to A(\varphi(N_S P'))$ that preserves the fixed-point homomorphisms Φ_Q for $Q \leq \varphi(N_S P') \leq N_S P$.

If we consider the S-set X with the action restricted to $\varphi(N_S P')$, we can apply Corollary 3.2 for the normal subgroup $P = \varphi(P') \trianglelefteq \varphi(N_S P')$ to get

$$\sum_{\bar{s} \in \varphi(N_S P')/P} \Phi_{\langle s \rangle P}(X) \equiv 0 \pmod{|\varphi(N_S P')/P|}.$$

Similarly, we have $P' \trianglelefteq N_S P'$, with which Corollary 3.2 gives us

$$\sum_{\bar{s} \in N_S P'/P'} \Phi_{\langle s \rangle P'}(X) \equiv 0 \pmod{|N_S P'/P'|}.$$

Since P is maximal in $\mathcal{H}$, we have by assumption $\Phi_Q(X) = \Phi_{Q'}(X)$ for all $Q \sim_{\mathcal{F}} Q'$ where P is $\mathcal{F}$-conjugate to a *proper* subgroup of Q. Specifically, we have

$$\Phi_{\langle \varphi(s) \rangle P}(X) = \Phi_{\varphi(\langle s \rangle P')}(X) = \Phi_{\langle s \rangle P'}(X)$$

for all $s \in N_S P'$ with $s \notin P'$. It then follows that

$$\begin{aligned} \Phi_P(X) - \Phi_{P'}(X) &= \sum_{\bar{s} \in \varphi(N_S P')/P} \Phi_{\langle s \rangle P}(X) - \sum_{\bar{s} \in N_S P'/P'} \Phi_{\langle s \rangle P'}(X) \\ &\equiv 0 - 0 \pmod{|W_S P'|}. \end{aligned}$$

We can therefore define $\lambda_{P'} := (\Phi_P(X) - \Phi_{P'}(X))/|W_S P'| \in \mathbb{Z}$.

Using the $\lambda_{P'}$ as coefficients, we construct a new S-set

$$\widetilde{X} := \Big(X + \sum_{[P']_S \subseteq [P]_{\mathcal{F}}} \lambda_{P'} \cdot [S/P'] \Big) \in A(S).$$

Here $[P]_{\mathcal{F}}$ is the collection of subgroups that are $\mathcal{F}$-conjugate to P. The sum is then taken over one representative from each S-conjugacy class contained in $[P]_{\mathcal{F}}$.

A priori, the $\lambda_{P'}$ might be negative, and as a result $\widetilde{X}$ might not be an S-set. In the original construction of [Broto et al. 2003], this problem is circumvented by adding copies of

$$\sum_{[P']_S \subseteq [P]_{\mathcal{F}}} \frac{|N_S P|}{|N_S P'|} \cdot [S/P']$$

until all the coefficients are nonnegative.

It will however be shown in Lemma 4.7 below, under the assumption that $c_{P'}(X) = 0$ for $P' \sim_{\mathcal{F}} P$, that $\lambda_{P'}$ is always nonnegative, and $\lambda_{P'} = 0$ if P' is fully normalized. Hence $\widetilde{X}$ is already an S-set without further adjustments.

We clearly have $c_Q(\widetilde{X}) = c_Q(X)$ for all $Q \not\sim_{\mathcal{F}} P$, in particular for all $Q \notin \mathcal{H}$. Furthermore, if $P' \sim_{\mathcal{F}} P$ is fully normalized, then $c_{P'}(\widetilde{X}) = c_{P'}(X) + \lambda_{P'} = c_{P'}(X)$.

Because $\Phi_Q([S/P']) = 0$ unless $Q \lesssim_S P'$, we see that $\Phi_Q(\widetilde{X}) = \Phi_Q(X)$ for every $Q \notin \mathcal{H}$. Secondly, we calculate $\Phi_{P'}(\widetilde{X})$ for each $P' \sim_{\mathcal{F}} P$:

$$\begin{aligned}\Phi_{P'}(\widetilde{X}) &= \Phi_{P'}(X) + \sum_{[\widetilde{P}]_S \subseteq [P]_{\mathcal{F}}} \lambda_{\widetilde{P}} \cdot \Phi_{P'}([S/\widetilde{P}]) \\ &= \Phi_{P'}(X) + \lambda_{P'} \cdot \Phi_{P'}([S/P']) = \Phi_{P'}(X) + \lambda_{P'} |W_S P'| \\ &= \Phi_P(X),\end{aligned}$$

which is independent of the choice of $P' \sim_{\mathcal{F}} P$.

We define $\mathcal{H}' := \mathcal{H} \setminus [P]_{\mathcal{F}}$ as $\mathcal{H}$ with the $\mathcal{F}$-conjugates of P removed. Because P is maximal in $\mathcal{H}$, the subcollection $\mathcal{H}'$ again contains all $\mathcal{F}$-subconjugates of any $H \in \mathcal{H}'$.

By induction we can apply Lemma 4.6 to $\widetilde{X}$ and to the smaller collection $\mathcal{H}'$. We get an $X' \in A_+(\mathcal{F})$ with $\Phi_Q(X') = \Phi_Q(\widetilde{X})$ and $c_Q(X') = c_Q(\widetilde{X})$ for all $Q \notin \mathcal{H}'$, such that $c_Q(X') = 0$ if $Q \in \mathcal{H}'$ is fully normalized.

It follows that $\Phi_Q(X') = \Phi_Q(\widetilde{X}) = \Phi_Q(X)$ and $c_Q(X') = c_Q(\widetilde{X}) = c_Q(X)$ for all $Q \notin \mathcal{H}$, and we also have $c_Q(X') = 0$ if $Q \in \mathcal{H}$ is fully normalized. □

Lemma 4.7. *Let $\mathcal{F}$ be a saturated fusion system over a p-group S, and let $P \leq S$ be a fully normalized subgroup.*

Suppose that X is an S-set with $c_{P'}(X) = 0$ for all $P' \sim_{\mathcal{F}} P$, and suppose that X is already $\mathcal{F}$-stable for subgroups larger than P, i.e., $\left|X^R\right| = \left|X^{R'}\right|$ for all $R \sim_{\mathcal{F}} R'$, where P is $\mathcal{F}$-conjugate to a proper subgroup of R.

Then $\left|X^P\right| \geq \left|X^{P'}\right|$ for all $P' \sim_{\mathcal{F}} P$.

Proof. Let $Q \sim_{\mathcal{F}} P$ be given. Because P is fully normalized, there exists by Lemma 2.3 a homomorphism $\varphi\colon N_S Q \hookrightarrow N_S P$ in $\mathcal{F}$, with $\varphi(Q) = P$.

Let $A_1, \dots, A_k$ be the subgroups of $N_S Q$ that strictly contain Q, meaning that $Q < A_i \leq N_S Q$. We put $B_i := \varphi(A_i)$, and thus also have $P < B_i \leq N_S P$. We let $C_1, \dots, C_\ell$ be the subgroups of $N_S P$ strictly containing P which are not the image (under φ) of some A_i. Hence $B_1, \dots, B_k, C_1, \dots, C_\ell$ are all the different subgroups of $N_S P$ strictly containing P. We denote the set $\{1, \dots, k\}$ of indices by I, and also $J := \{1, \dots, \ell\}$.

Because $c_Q(X) = c_P(X) = 0$ by assumption, no orbit of X is isomorphic to S/Q, hence no element in X^Q has Q as a stabilizer. Let $x \in X^Q$ be any element, and let $K > Q$ be the stabilizer of x; so $x \in X^K \subseteq X^Q$. Since K is a p-group, there is some intermediate group L with $Q \lhd L \leq K$; hence $x \in X^L$ for some $Q < L \leq N_S Q$. We conclude that

$$X^Q = \bigcup_{i \in I} X^{A_i}.$$

With similar reasoning we also get

$$X^P = \bigcup_{i\in I} X^{B_i} \cup \bigcup_{j\in J} X^{C_j}.$$

The proof is then completed by showing

$$\left|X^P\right| = \left|\bigcup_{i\in I} X^{B_i} \cup \bigcup_{j\in J} X^{C_j}\right| \geq \left|\bigcup_{i\in I} X^{B_i}\right| \overset{(*)}{=} \left|\bigcup_{i\in I} X^{A_i}\right| = \left|X^Q\right|.$$

We only need to prove equality $(*)$.

Showing $(*)$ has only to do with fixed points for the subgroups A_i and B_i. Because $B_i = \varphi(A_i) \sim_{\mathcal{F}} A_i$ are subgroups that strictly contain P and Q, respectively, we have $|X^{B_i}| = |X^{A_i}|$ by assumption.

To get $(*)$ for the unions $\bigcup A_i$ and $\bigcup B_i$ we then have to apply the inclusion-exclusion principle:

$$\left|\bigcup_{i\in I} X^{B_i}\right| = \sum_{\varnothing\neq\Lambda\subseteq I} (-1)^{|\Lambda|+1}\left|\bigcap_{i\in\Lambda} X^{B_i}\right| = \sum_{\varnothing\neq\Lambda\subseteq I} (-1)^{|\Lambda|+1}\left|X^{\langle B_i\rangle_{i\in\Lambda}}\right|.$$

Here $\langle B_i\rangle_{i\in\Lambda} \leq N_S P$ is the subgroup generated by the elements of the B_i's with $i \in \Lambda \subseteq I$. Recalling that $B_i = \varphi(A_i)$ by definition, we have $\langle B_i\rangle_{i\in\Lambda} = \langle\varphi(A_i)\rangle_{i\in\Lambda} = \varphi(\langle A_i\rangle_{i\in\Lambda})$, and consequently,

$$\sum_{\varnothing\neq\Lambda\subseteq I} (-1)^{|\Lambda|+1}\left|X^{\langle B_i\rangle_{i\in\Lambda}}\right| = \sum_{\varnothing\neq\Lambda\subseteq I} (-1)^{|\Lambda|+1}\left|X^{\varphi(\langle A_i\rangle_{i\in\Lambda})}\right|.$$

Because $Q < A_i \leq N_S Q$, we also have $Q < \langle A_i\rangle_{i\in\Lambda} \leq N_S Q$; by assumption we therefore get $|X^{\varphi(\langle A_i\rangle_{i\in\Lambda})}| = |X^{\langle A_i\rangle_{i\in\Lambda}}|$ for all $\varnothing \neq \Lambda \subseteq I$. It then follows that

$$\sum_{\varnothing\neq\Lambda\subseteq I} (-1)^{|\Lambda|+1}\left|X^{\varphi(\langle A_i\rangle_{i\in\Lambda})}\right| = \sum_{\varnothing\neq\Lambda\subseteq I} (-1)^{|\Lambda|+1}\left|X^{\langle A_i\rangle_{i\in\Lambda}}\right| = \cdots = \left|\bigcup_{i\in I} X^{A_i}\right|,$$

where we use the inclusion-exclusion principle in reverse. We have thus shown the equality $\left|\bigcup_{i\in I} X^{B_i}\right| = \left|\bigcup_{i\in I} X^{A_i}\right|$ as required. □

Applying the technical Lemma 4.6, we can now construct the irreducible $\mathcal{F}$-stable sets α_P for $P \leq S$ as described in the following proposition. That the α_P's are in fact irreducible, or even that they are unique, will not be shown until the proof of Theorem A itself.

Proposition 4.8. *Let $\mathcal{F}$ be a saturated fusion system over a p-group S.*

For each $\mathcal{F}$-conjugacy class $[P]_{\mathcal{F}} \in \mathrm{Cl}(\mathcal{F})$ of subgroups, there is an $\mathcal{F}$-stable set $\alpha_P \in A_+(\mathcal{F})$ such that

(i) $\Phi_Q(\alpha_P) = 0$ *unless Q is $\mathcal{F}$-subconjugate to P.*

(ii) $c_{P'}(\alpha_P) = 1$ *and* $\Phi_{P'}(\alpha_P) = |W_S P'|$ *when P' is fully normalized and $P' \sim_{\mathcal{F}} P$.*

(iii) $c_Q(\alpha_P) = 0$ *when Q is fully normalized and $Q \not\sim_{\mathcal{F}} P$.*

Proof. Let $P \leq S$ be fully $\mathcal{F}$-normalized. We let $X \in A_+(S)$ be the S-set

$$X := \sum_{[P']_S \subseteq [P]_\mathcal{F}} \frac{|N_S P|}{|N_S P'|} \cdot [S/P'] \in A_+(S).$$

X then satisfies that $\Phi_Q(X) = 0$ unless $Q \lesssim_S P'$ for some $P' \sim_\mathcal{F} P$, in which case we have $Q \lesssim_\mathcal{F} P$. For all P', $P'' \in [P]_\mathcal{F}$ we have $\Phi_{P''}([S/P']) = 0$ unless $P'' \sim_S P'$; consequently,

$$\Phi_{P'}(X) = \frac{|N_S P|}{|N_S P'|} \cdot \Phi_{P'}([S/P']) = \frac{|N_S P|}{|N_S P'|} \cdot |W_S P'| = |W_S P|$$

which doesn't depend on $P' \sim_\mathcal{F} P$.

Let $\mathcal{H}$ be the collection of all Q which are $\mathcal{F}$-conjugate to a *proper* subgroup of P; then $\Phi_Q(X) = \Phi_{Q'}(X)$ for all pairs $Q \sim_\mathcal{F} Q'$ not in $\mathcal{H}$. Using Lemma 4.6 we get some $\alpha_P \in A_+(\mathcal{F})$ with the required properties. □

Properties (ii) and (iii) make it really simple to decompose a linear combination X of the α_P's. The coefficient of α_P in X is just the number of $[S/P]$-orbits in X as an S-set — when P is fully normalized. This is immediate since α_P contains exactly one copy of $[S/P]$, and no other α_Q contains $[S/P]$.

In particular we have:

Corollary 4.9. *The α_P's in Proposition 4.8 are linearly independent.*

In order to prove that the α_P's generate all $\mathcal{F}$-stable sets, we will first show that the α_P's generate all the $\mathcal{F}$-stable elements in the Burnside ring. As a tool for proving this, we define a ghost ring for the Burnside ring $A(\mathcal{F})$; as a consequence of how the proof proceeds, we end up showing an analogue of Proposition 3.1 for saturated fusion systems, describing how the Burnside ring $A(\mathcal{F})$ lies embedded in the ghost ring — this is the content of Theorem B.

Definition 4.10. We defined the ghost ring $\widetilde{\Omega}(S)$ for the Burnside ring of a group as the product ring $\prod_{[P]_S \in \mathrm{Cl}(S)} \mathbb{Z}$ where the coordinates correspond to the S-conjugacy classes of subgroups. For the ring $A(\mathcal{F})$, we now similarly define *the ghost ring* $\widetilde{\Omega}(\mathcal{F})$ as a product ring $\prod_{[P]_\mathcal{F} \in \mathrm{Cl}(\mathcal{F})} \mathbb{Z}$ with coordinates corresponding to the $\mathcal{F}$-conjugacy classes of subgroups.

The surjection of indexing sets $\mathrm{Cl}(S) \to \mathrm{Cl}(\mathcal{F})$ which sends an S-conjugacy class $[P]_S$ to its $\mathcal{F}$-conjugacy class $[P]_\mathcal{F}$, induces a homomorphism $\widetilde{\Omega}(\mathcal{F}) \hookrightarrow \widetilde{\Omega}(S)$ that embeds $\widetilde{\Omega}(\mathcal{F})$ as the subring of vectors which are constant on each $\mathcal{F}$-conjugacy class.

Since $A(\mathcal{F})$ is the subring of $\mathcal{F}$-stable elements in $A(S)$, we can restrict the mark homomorphism $\Phi^S \colon A(S) \to \widetilde{\Omega}(S)$ to the subring $A(\mathcal{F})$ and get an injective ring homomorphism $\Phi^\mathcal{F} \colon A(\mathcal{F}) \to \widetilde{\Omega}(\mathcal{F})$. This is the *homomorphism of marks* for $A(\mathcal{F})$.

To model the cokernel of $\Phi^{\mathcal{F}}$ we define $\mathrm{Obs}(\mathcal{F})$ as

$$\mathrm{Obs}(\mathcal{F}) := \prod_{\substack{[P]\in \mathrm{Cl}(\mathcal{F}) \\ P \text{ f.n.}}} (\mathbb{Z}/|W_S P|\mathbb{Z}),$$

where "f.n." is short for "fully normalized", so we take fully normalized representatives of the conjugacy classes in $\mathcal{F}$.

Theorem B. *Let $\mathcal{F}$ be a saturated fusion system over a p-group S, and let $A(\mathcal{F})$ be the Burnside ring of $\mathcal{F}$, i.e., the subring consisting of the $\mathcal{F}$-stable elements in the Burnside ring of S. We then have a short-exact sequence*

$$0 \longrightarrow A(\mathcal{F}) \xrightarrow{\Phi} \widetilde{\Omega}(\mathcal{F}) \xrightarrow{\Psi} \mathrm{Obs}(\mathcal{F}) \longrightarrow 0.$$

where $\Phi = \Phi^{\mathcal{F}}$ is the homomorphism of marks, and $\Psi = \Psi^{\mathcal{F}} \colon \widetilde{\Omega}(\mathcal{F}) \to \mathrm{Obs}(\mathcal{F})$ is a group homomorphism given by the $[P]$-coordinate functions

$$\Psi_P(\xi) := \sum_{\bar{s}\in W_S P} \xi_{\langle s\rangle P} \pmod{|W_S P|}$$

when $P \le S$ is a fully normalized representative of the conjugacy class $[P]$ in $\mathcal{F}$. Here $\Psi_P = \Psi_{P'}$ if $P \sim_{\mathcal{F}} P'$ are both fully normalized.

Proof. We choose some total order of the conjugacy classes $[P], [Q] \in \mathrm{Cl}(\mathcal{F})$ such that $|P| > |Q|$ implies $[P] < [Q]$, i.e., we take the subgroups in decreasing order. It holds in particular that $Q \lesssim_{\mathcal{F}} P$ implies $[P] \le [Q]$.

With respect to the ordering above, the group homomorphism Ψ is given by a lower triangular matrix with 1's in the diagonal, hence Ψ is surjective. The mark homomorphism $\Phi = \Phi^{\mathcal{F}}$ is the restriction of the injective ring homomorphism $\Phi^S \colon A(S) \to \widetilde{\Omega}(S)$, so Φ is injective.

We know from the group case, Proposition 3.1, that $\Psi^S \circ \Phi^S = 0$. By construction we have $(\Psi)_P = (\Psi^S)_P$ for the coordinate functions when P is fully normalized; and Φ is the restriction of Φ^S. We conclude that $\Psi \circ \Phi = 0$ as well. It remains to be shown that $\mathrm{im}\,\Phi$ is actually all of $\ker \Psi$.

Consider the subgroup $H := \mathrm{Span}\{\alpha_P \mid [P] \in \mathrm{Cl}(\mathcal{F})\}$ spanned by the α_P's in $A(\mathcal{F})$, and consider also the restriction $\Phi|_H$ of the mark homomorphism $\Phi \colon A(\mathcal{F}) \to \widetilde{\Omega}(\mathcal{F})$.

The map $\Phi|_H$ is described by a square matrix M in terms of the ordered bases of $H = \mathrm{Span}\{\alpha_P\text{'s}\}$ and $\widetilde{\Omega}(\mathcal{F})$. Because $M_{[Q],[P]} := \Phi_Q(\alpha_P)$ is zero unless $P \sim_{\mathcal{F}} Q$ or $|P| > |Q|$, we conclude that M is a lower triangular matrix. The diagonal entries of M are

$$M_{[P],[P]} = \Phi_P(\alpha_P) = |W_S P|,$$

when P is fully normalized.

All the diagonal entries are nonzero, so the cokernel of $\Phi|_H$ is finite of order

$$|\operatorname{coker}\Phi|_H| = \prod_{[P]\in \mathrm{Cl}(\mathcal{F})} M_{[P],[P]} = \prod_{\substack{[P]\in \mathrm{Cl}(\mathcal{F}) \\ P \text{ f.n.}}} |W_S P|.$$

Since $\Phi|_H$ is a restriction of Φ, it follows that $|\operatorname{coker}\Phi| \leq |\operatorname{coker}\Phi|_H|$. At the same time, $\Psi \circ \Phi = 0$ implies that $|\operatorname{coker}\Phi| \geq |\mathrm{Obs}(\mathcal{F})|$.

We do however have

$$|\mathrm{Obs}(\mathcal{F})| = \prod_{\substack{[P]\in \mathrm{Cl}(\mathcal{F}) \\ P \text{ f.n.}}} |W_S P| = |\operatorname{coker}\Phi|_H|.$$

The only possibility is that $\ker\Psi = \operatorname{im}\Phi = \operatorname{im}\Phi|_H$, completing the proof of Theorem B. □

From the last equality $\operatorname{im}\Phi = \operatorname{im}\Phi|_H$, and the fact that Φ is injective, it also follows that $A(\mathcal{F}) = H$ so the α_P's span all of $A(\mathcal{F})$. Combining this with Corollary 4.9 we get:

Corollary 4.11. *The α_P's form an additive basis for the Burnside ring $A(\mathcal{F})$.*

The corollary tells us that any element $X \in A(\mathcal{F})$ can be written uniquely as an integral linear combination of the α_P's. In particular, any $\mathcal{F}$-stable set can be written as a linear combination of α_P's, and if the coefficients are all nonnegative, then we have a linear combination in $A_+(\mathcal{F})$.

Theorem A. *Let $\mathcal{F}$ be a saturated fusion system over a p-group S. The sets α_P from Proposition 4.8 are all the irreducible $\mathcal{F}$-stable sets, and every $\mathcal{F}$-stable set splits uniquely, up to S-isomorphism, as a disjoint union of the α_P's.*

Hence the semiring $A_+(\mathcal{F})$ of $\mathcal{F}$-stable sets is additively a free commutative monoid with rank equal to the number of conjugacy classes of subgroups in $\mathcal{F}$.

Proof. Let $\alpha_P \in A_+(\mathcal{F})$ for each conjugacy class $[P] \in \mathrm{Cl}(\mathcal{F})$ be given as in Proposition 4.8. Let $X \in A_+(\mathcal{F})$ be any $\mathcal{F}$-stable S-set.

Since the α_P's form a basis for $A(\mathcal{F})$ by Corollary 4.11, we can write X uniquely as

$$X = \sum_{[P]\in \mathrm{Cl}(\mathcal{F})} \lambda_P \cdot \alpha_P$$

with $\lambda_P \in \mathbb{Z}$.

Suppose that P is fully normalized; then $c_P(\alpha_Q) = 1$ if $P \sim_{\mathcal{F}} Q$, and $c_P(\alpha_Q) = 0$ otherwise. As a consequence of this, we have

$$c_P(X) = \sum_{[Q]\in \mathrm{Cl}(\mathcal{F})} \lambda_Q \cdot c_P(\alpha_Q) = \lambda_P$$

whenever P is fully normalized.

Because X is an S-set, we see that $\lambda_P = c_P(X) \geq 0$. Hence the linear combination $X = \sum_{[P]\in \mathrm{Cl}(\mathcal{F})} \lambda_P \cdot \alpha_P$ has nonnegative coefficients, i.e., it is a linear combination in the semiring $A_+(\mathcal{F})$.

As a special case, if we have another element α'_P in $A(\mathcal{F})$ satisfying the properties of Proposition 4.8, then the fact that $\lambda_Q = c_Q(\alpha'_P)$ for all fully normalized $Q \leq S$, shows that $\lambda_P = 1$ and $\lambda_Q = 0$ for $Q \not\sim_{\mathcal{F}} P$. Thus the linear combination above simplifies to $\alpha'_P = \alpha_P$. Hence the α_P's are uniquely determined by the properties of Proposition 4.8. □

Appendix: The monoid of complex representations

For a saturated fusion system $\mathcal{F}$ over S, it makes sense to talk about $\mathcal{F}$-stability of S-representations instead of S-sets. In this appendix we show that the analogues of Theorems A and A′ fail for representations in general by giving an example where the abelian monoid of $\mathcal{F}$-stable complex representations is not free.

For a finite dimensional complex representation $\rho\colon S \to GL_n(\mathbb{C})$ of S, we can restrict ρ along any fusion map $\varphi \in \mathcal{F}(P, S)$ to form a representation ${}_{P,\varphi}\rho := \rho \circ \varphi$ of the subgroup $P \leq S$. Just as for finite S-sets, we compare each ${}_{P,\varphi}\rho$ to the usual restriction ${}_{P,\mathrm{incl}}\rho$ and say that ρ is $\mathcal{F}$-stable if

> *${}_{P,\varphi}\rho$ is isomorphic to ${}_{P,\mathrm{incl}}X$ as representations of P, for all $P \leq S$ and homomorphisms $\varphi\colon P \to S$ in $\mathcal{F}$.*

The isomorphism classes of $\mathcal{F}$-stable complex S-representations form an abelian monoid $R_+(\mathcal{F})$ with direct sum of representations as the addition. As we know, the isomorphism class of any complex representation is determined completely by the associated character. Our first order of business is therefore to determine which characters belong to $\mathcal{F}$-stable representations. We say that a character $\chi\colon S \to \mathbb{C}$ is $\mathcal{F}$-stable if it satisfies $\chi(s) = \chi(\varphi(s))$ for all elements $s \in S$ and maps $\varphi \in \mathcal{F}(\langle s\rangle, S)$, that is χ should be constant on each conjugacy class in $\mathcal{F}$ of elements in S.

Lemma A.1. *Let $\rho\colon S \to GL_n(\mathbb{C})$ be a representation, and let $\chi\colon S \to \mathbb{C}$ be the associated character. Then ρ is $\mathcal{F}$-stable if and only if χ is $\mathcal{F}$-stable.*

Proof. Consider a subgroup $P \leq S$ and a map $\varphi \in \mathcal{F}(P, S)$. Then the character associated to the restriction ${}_{P,\varphi}\rho = \rho \circ \varphi$ is equal to $\chi \circ \varphi$. The representation ${}_{P,\varphi}\rho$ is isomorphic to ${}_{P,\mathrm{incl}}\rho$ precisely when they have the same character on P, that is, whenever $\chi \circ \varphi = \chi|_P$, which on elements becomes $\chi(\varphi(s)) = \chi(s)$ for all $s \in P$.

We now immediately conclude that ρ is $\mathcal{F}$-stable if and only if $\chi(\varphi(s)) = \chi(s)$ for all $s \in P$, $P \leq S$ and $\varphi \in \mathcal{F}(P, S)$. By restricting each φ to the cyclic subgroup $\langle s\rangle \leq P$, it is enough to check that $\chi(\varphi(s)) = \chi(s)$ for all $s \in S$ and $\varphi \in \mathcal{F}(\langle s\rangle, S)$, i.e., that χ is $\mathcal{F}$-stable. □

Using Lemma A.1 to characterize the $\mathcal{F}$-stable representations, we will now study the example below and see that $R_+(\mathcal{F})$ is not a free abelian monoid for this particular choice of $\mathcal{F}$.

Example A.2. We consider the saturated fusion system $\mathcal{F} := \mathcal{F}_{\mathrm{SD}_{16}}(\mathrm{PGL}_3(\mathbb{F}_3))$ induced by the projective general linear group $\mathrm{PGL}_3(\mathbb{F}_3)$ on the semidihedral group of order 16, i.e., the group $\mathrm{SD}_{16} = \langle D, S \mid D^8 = S^2 = 1, SDS^{-1} = D^3 \rangle$. One possible inclusion of SD_{16} inside $\mathrm{PGL}_3(\mathbb{F}_3)$ has as matrix representatives:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 2 & 1 & 0 \end{pmatrix} \text{ represents } D, \text{ and } \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 2 \end{pmatrix} \text{ represents } S.$$

The group SD_{16} has 7 conjugacy classes of elements, and 7 irreducible characters. These are all listed in the character table below:

	1	D, D^3	D^5, D^7	D^2, D^6	D^4	S, D^2S, D^4S, D^6S	DS, D^3S, D^5S, D^7S
$\mathbf{1}$	1	1	1	1	1	1	1
χ_a	1	-1	-1	1	1	-1	1
χ_b	1	-1	-1	1	1	1	-1
χ_{ab}	1	1	1	1	1	-1	-1
χ_2	2	0	0	-2	2	0	0
χ_i	2	$i\sqrt{2}$	$-i\sqrt{2}$	0	-2	0	0
χ_{-i}	2	$-i\sqrt{2}$	$i\sqrt{2}$	0	-2	0	0

Inside $\mathcal{F}$, the class of D^4 becomes conjugate to the class of S, and the class of D^2 becomes conjugate to the class of DS. None of the other conjugacy classes in SD_{16} are fused in $\mathcal{F}$. The $\mathcal{F}$-stable characters are therefore precisely the characters where the 4-th value is equal to the 7-th value, and the 5-th is equal to the 6-th.

Note that $\mathbf{1}$ is the only irreducible character for SD_{16} that is $\mathcal{F}$-stable. Adding rows we see that the following four characters are also $\mathcal{F}$-stable: $\alpha := \chi_a + \chi_i$, $\beta := \chi_a + \chi_{-i}$, $\gamma := \chi_b + \chi_2 + \chi_i$ and $\delta := \chi_b + \chi_2 + \chi_{-i}$. Each of these four characters cannot be written as a sum of smaller $\mathcal{F}$-stable characters, so α, β, γ and δ correspond to representations that are irreducible in $R_+(\mathcal{F})$. At the same time, however, we have

$$\chi_a + \chi_b + \chi_2 + \chi_i + \chi_{-i} = \alpha + \delta = \beta + \gamma.$$

Hence $\chi_a + \chi_b + \chi_2 + \chi_i + \chi_{-i}$ corresponds to an element of $R_+(\mathcal{F})$ that can be written as a sum of two irreducible elements in two different ways. The abelian monoid $R_+(\mathcal{F})$ is therefore *not* free, so the analogue of Theorem A for complex representations is false.

Acknowledgements. The claim of Theorem A was initially suggested by Matthew Gelvin and formed by his previous interest in similar problems as well as my own work on my masters thesis and the first part of [Reeh 2016]. Matthew's claim became the subject of conversations at the University of Copenhagen, involving also Jesper Michael Møller, Bob Oliver, Kasper Andersen and Jesper Grodal. Due to a seeming lack of systematic structure in the irreducible stable sets, and the fact that the decompositions are only unique up to S-isomorphism, the claim was met with initial skepticism, but Kasper Andersen produced a large amount of computer evidence supporting the claim's validity (using Magma). I would like to thank them all. In particular it was Kasper Andersen's examples that gave me the idea for Lemma 4.7, which formed the missing link in the proof of Theorem A. I also thank my Ph.D. advisor Jesper Grodal for his helpful suggestions and feedback during the writing of this paper.

References

[Aschbacher et al. 2011] M. Aschbacher, R. Kessar, and B. Oliver, *Fusion systems in algebra and topology*, London Mathematical Society Lecture Note Series **391**, Cambridge University Press, 2011. MR 2012m:20015 Zbl 1255.20001

[Bousfield and Kan 1972] A. K. Bousfield and D. M. Kan, *Homotopy limits, completions and localizations*, vol. 304, Lecture Notes in Mathematics, Springer, Berlin, 1972. MR 51 #1825 Zbl 0259.55004

[Broto et al. 2003] C. Broto, R. Levi, and B. Oliver, "The homotopy theory of fusion systems", *J. Amer. Math. Soc.* **16**:4 (2003), 779–856. MR 2004k:55016 Zbl 1033.55010

[Carlsson 1991] G. Carlsson, "Equivariant stable homotopy and Sullivan's conjecture", *Invent. Math.* **103**:3 (1991), 497–525. MR 92g:55007 Zbl 0736.55008

[Díaz and Libman 2009a] A. Díaz and A. Libman, "The Burnside ring of fusion systems", *Adv. Math.* **222**:6 (2009), 1943–1963. MR 2011a:20039 Zbl 1188.19001

[Díaz and Libman 2009b] A. Díaz and A. Libman, "Segal's conjecture and the Burnside rings of fusion systems", *J. Lond. Math. Soc.* (2) **80**:3 (2009), 665–679. MR 2011d:55029 Zbl 1183.55003

[tom Dieck 1979] T. tom Dieck, *Transformation groups and representation theory*, Lecture Notes in Mathematics **766**, Springer, Berlin, 1979. MR 82c:57025 Zbl 0445.57023

[Dress 1986] A. W. M. Dress, "Congruence relations characterizing the representation ring of the symmetric group", *J. Algebra* **101**:2 (1986), 350–364. MR 87j:20019 Zbl 0592.20012

[Dwyer and Zabrodsky 1987] W. Dwyer and A. Zabrodsky, "Maps between classifying spaces", pp. 106–119 in *Algebraic topology, Barcelona, 1986*, edited by J. Aguadé and R. Kane, Lecture Notes in Math. **1298**, Springer, Berlin, 1987. MR 89b:55018 Zbl 0646.55007

[Gelvin 2010] M. J. K. Gelvin, *Fusion action systems*, Ph.D. thesis, Massachusetts Institute of Technology, 2010, Available at http://search.proquest.com/docview/847033297. MR 2814028

[Grodal 2011] J. Grodal, "Group actions on sets, at a prime p", pp. 2647–2648 in *Homotopy theory*, Oberwolfach Rep. **8**:3, European Mathematican Society, Zürich, 2011. MR 2978664

[Grodal $\geq$ 2015] J. Grodal, "The Burnside ring of the p-completed classifying space of a finite group", in preparation.

[Lannes 1995] J. Lannes, "Applications dont la source est un classifiant", pp. 566–573 in *Proceedings of the International Congress of Mathematicians, Vol. 1, 2* (Zürich, 1994), edited by S. D. Chatterji, Birkhäuser, Basel, 1995. MR 97h:55021 Zbl 0854.55014

[Miller 1987] H. Miller, "The Sullivan conjecture and homotopical representation theory", pp. 580–589 in *Proceedings of the International Congress of Mathematicians, Vol. 1, 2* (Berkeley, Calif., 1986), edited by A. M. Gleason, Amer. Math. Soc., Providence, RI, 1987. MR 89f:55016 Zbl 0678.55008

[Mislin 1990] G. Mislin, "On group homomorphisms inducing mod-p cohomology isomorphisms", *Comment. Math. Helv.* **65**:3 (1990), 454–461. MR 92a:20059 Zbl 0713.55009

[Ragnarsson and Stancu 2013] K. Ragnarsson and R. Stancu, "Saturated fusion systems as idempotents in the double Burnside ring", *Geom. Topol.* **17**:2 (2013), 839–904. MR 3070516 Zbl 1306.20011

[Reeh 2016] S. P. Reeh, "Transfer and characteristic idempotents for saturated fusion systems", *Adv. in Math.* **289** (2016), 161–211.

[Roberts and Shpectorov 2009] K. Roberts and S. Shpectorov, "On the definition of saturated fusion systems", *J. Group Theory* **12**:5 (2009), 679–687. MR 2010h:20047 Zbl 1234.20028

[Yoshida 1990] T. Yoshida, "On the unit groups of Burnside rings", *J. Math. Soc. Japan* **42**:1 (1990), 31–64. MR 90j:20027 Zbl 0694.20009

Communicated by David Benson
Received 2014-12-03 Revised 2015-08-31 Accepted 2015-10-08

reeh@mit.edu *Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139, United States*

ALGEBRA AND NUMBER THEORY 9:10 (2015)
dx.doi.org/10.2140/ant.2015.9.2325

msp

Polynomial values modulo primes on average and sharpness of the larger sieve

Xuancheng Shao

This paper is motivated by the following question in sieve theory. Given a subset $X \subset [N]$ and $\alpha \in \left(0, \frac{1}{2}\right)$. Suppose that $|X \pmod p| \leq (\alpha + o(1))p$ for every prime p. How large can X be? On the one hand, we have the bound $|X| \ll_\alpha N^\alpha$ from Gallagher's larger sieve. On the other hand, we prove, assuming the truth of an inverse sieve conjecture, that the bound above can be improved (for example, to $|X| \ll_\alpha N^{O(\alpha^{2014})}$ for small α). The result follows from studying the average size of $|X \pmod p|$ as p varies, when $X = f(\mathbb{Z}) \cap [N]$ is the value set of a polynomial $f(x) \in \mathbb{Z}[x]$.

1. Introduction

For a positive integer N, denote by $[N]$ the set $\{1, 2, \ldots, N\}$. The letter p is always used to denote a prime. The primary goal of this paper is to study upper bounds for the sizes of subsets $X \subset [N]$ occupying a small fraction of residue classes modulo many primes p. Gallagher's larger sieve [1971] provides such an upper bound.

Theorem 1.1 (larger sieve). *Let $X \subset [N]$ be a subset and $\mathcal{P}$ be a set of primes. We have*

$$|A| \leq \frac{\sum_{p\in\mathcal{P}} \log p}{\sum_{p\in\mathcal{P}} |X \pmod p|^{-1} \log p - \log N}$$

whenever the denominator is positive.

See [Croot and Elsholtz 2004] for some variants of it and references therein for applications. We are particularly interested in the situation when $|X \pmod p| \leq \alpha p$ for some fixed $\alpha \in (0, 1)$, and whether the bound provided by the larger sieve is best possible.

Corollary 1.2 (larger sieve, special case). *Let $X \subset [N]$ be a subset and $\alpha \in \left(0, \frac{1}{2}\right]$. If $|X \pmod p| \leq (\alpha + o(1))p$ for every prime p, then $|X| \ll N^{\alpha+o(1)}$.*

MSC2010: primary 11N35; secondary 11R45, 11R09.

Keywords: Gallagher's larger sieve, inverse sieve conjecture, value sets of polynomials over finite fields.

This is easily deduced from Theorem 1.1 by taking $\mathcal{P}$ to be the set of primes up to $N^{\alpha+o(1)}$. When $\alpha > \frac{1}{2}$, the statement still holds, but is beaten by the bound $|X| \ll_\alpha N^{1/2}$ following from the large sieve [Montgomery 1978]. When $\alpha \le \frac{1}{2}$, is the bound $|X| \ll N^{\alpha+o(1)}$ sharp? If X is the set of perfect squares up to N, then $|X| \sim N^{1/2}$ and X occupies $(p+1)/2$ residue classes (the quadratic residues) modulo any odd prime p. The question of whether this is the only type of sharp example is usually referred to as the inverse sieve conjecture, informally stated as follows.

Conjecture 1.3 (inverse sieve conjecture, rough form). *Let $X \subset [N]$ be a subset. If $|X \pmod p| \le 0.9p$ for every prime p, then either one of the following two statements holds*:

(1) *The cardinality of X is extremely small.*

(2) *The set X possesses algebraic structure.*

See Conjecture 4.1 below for one precise formulation of it. See also [Croot and Lev 2007; Helfgott and Venkatesh 2009; Walsh 2012; Green and Harper 2014] for more discussions and evidences towards it.

Now assume that $\alpha < \frac{1}{2}$ is fixed. Motivated by the inverse sieve conjecture, we consider the sizes of $X \pmod p$ when X is the value set of a polynomial. For a polynomial $f(x) \in \mathbb{Z}[x]$ of degree $d \ge 1$, denote by $f_p \in \mathbb{F}_p[x]$ the reduction of f modulo p. Let $\alpha_p(f) = p^{-1}|f_p(\mathbb{F}_p)|$, the relative size of the value set of $f \pmod p$. Define $\alpha(f)$ to be the average of $\alpha_p(f)$ as p varies:

$$\alpha(f) = \lim_{Q\to\infty} \frac{1}{\pi(Q)} \sum_{p\le Q} \alpha_p(f).$$

Note the trivial lower bounds $\alpha_p(f) \ge d^{-1}$ and $\alpha(f) \ge d^{-1}$.

Theorem 1.4 (polynomial values modulo primes on average). *Let $f \in \mathbb{Z}[x]$ be a polynomial of degree $d \ge 1$. Then*

$$\lim_{Q\to\infty} \frac{1}{\pi(Q)} \sum_{p\le Q} \alpha_p(f)^{-1} \le \tau(d), \tag{1-1}$$

where $\tau(d)$ is the number of positive divisors of d. Consequently, $\alpha(f) \ge \tau(d)^{-1}$.

Note that for $d \ge 3$ we always have $\tau(d) < d$. Hence, it is reasonable to conjecture that Corollary 1.2 is not sharp whenever α is smaller than (and bounded away from) $\frac{1}{2}$. See the last section in [Shao 2014] for a preliminary discussion on the simplest case $d = 3$.

Theorem 1.5 (inverse sieve conjecture implies improved larger sieve). *Assume the truth of Conjecture 4.1. Let $X \subset [N]$ be a subset and $\alpha \in (0, 1)$. Let $\epsilon \in (0, 1)$ be a parameter. If $|X \pmod p| \le (\alpha + o(1))p$ for every prime p, then $|X| \ll_{\alpha,\epsilon} N^{1/d}$, where d is the smallest positive integer with $\tau(d) \ge (1-\epsilon)\alpha^{-1}$.*

For example, when $\alpha = 0.49$, we obtain the upper bound $|X| \ll N^{1/4}$. On the other hand, since $\tau(d) \le d^{C/\log\log d}$ for some constant $C > 0$, we get $|X| \ll_\alpha N^{\alpha^{c\log\log\alpha^{-1}}}$ for some constant $c > 0$, a huge improvement upon Corollary 1.2 for small α (assuming the truth of the inverse sieve conjecture).

Remark 1.6. Instead of assuming that $|X \pmod p| \le (\alpha + o(1))p$ for every prime p, knowing this on average over p in an appropriate sense is sufficient for our proof to follow. In this paper, we will focus on the model case in which we assume the pointwise estimate.

In the remainder of this introduction we discuss further the quantities $\alpha_p(f)$ and $\alpha(f)$. Note that (1-1) becomes an equality when $f(x) = x^d$. Indeed, in this case we have $\alpha_p(f) \sim (p-1, d)^{-1}$, and thus the average of $\alpha_p(f)^{-1}$ is equal to

$$\frac{1}{\phi(d)} \sum_{a \in (\mathbb{Z}/d\mathbb{Z})^\times} (a-1, d) = \tau(d).$$

Note, however, that in this case the average of $\alpha_p(f)$ is equal to

$$\alpha(f) = \frac{1}{\phi(d)} \sum_{a \in (\mathbb{Z}/d\mathbb{Z})^\times} (a-1, d)^{-1},$$

which can be evaluated to $\phi(d)/d$ when d is squarefree (and is at least $(\phi(d)/d)^2$ for any d). Since $\phi(d)/d \gg (\log\log d)^{-1}$, the following construction provides polynomials f with smaller $\alpha(f)$.

Theorem 1.7 (polynomials with small value sets modulo primes). *Define a sequence of polynomials $\{f_n\}$ by*

$$f_1(x) = x^2, \quad f_{n+1}(x) = (f_n(x) + 1)^2.$$

Then $\alpha_p(f_n) = a_n$ provided that $p > 2f_{n-1}(0) + 2$ when $n > 1$, where the sequence $\{a_n\}$ is defined by

$$a_1 = \tfrac{1}{2}, \quad a_{n+1} = a_n - \tfrac{1}{2}a_n^2.$$

Moreover, we have $a_n \le 2n^{-1}$ for each n.

See Remark 2.5 below for the reasoning behind this construction of f_n. It is easy to see heuristically why one expects the relation $a_{n+1} = a_n - \frac{1}{2}a_n^2$. Indeed, if we model the value set of $f_n \pmod p$ as a random subset $S \subset \mathbb{F}_p$ with each element $s \in \mathbb{F}_p$ chosen in S with probability a_n independently at random, then for every quadratic residue r, the probability that r can be written as $(s+1)^2$ for some $s \in S$ is $2a_n - a_n^2$. Hence the expected size of the set $(S+1)^2$ is $(2a_n - a_n^2)p/2 + O(1)$, as desired.

Since $\deg f_n = 2^n$, we have $\alpha(f_n) \ll (\log(\deg f_n))^{-1}$. We do not know whether this is the best example or whether the bound for $\alpha(f)$ in Theorem 1.4 is sharp. See Section 6B for more discussion of this.

The investigation of $\alpha_p(f)$ for a fixed prime p has a long history (see [Birch and Swinnerton-Dyer 1959; Cohen 1970]), and explicit formulae for $\alpha_p(f)$ are known in terms of the proportion of fixed-point-free elements in a certain Galois group (see Lemma 5.1 and the remark following). Not surprisingly, the quantity $\alpha(f)$ can also be evaluated in terms of a certain Galois group, and this is recorded in Proposition 6.1. Due to a lack of understanding of the relevant Galois groups, our lower bound for $\alpha(f)$ is instead obtained by studying the number of solutions to $f(x) \equiv f(y) \pmod p$ on average as p varies (see Section 2), and it is for this reason that the average of $\alpha_p(f)^{-1}$ naturally shows up.

A related line of work is on classifying those polynomials $f \in \mathbb{F}_p[x]$ for which $\alpha_p(f)$ is close to the lower bound d^{-1} (for a fixed p). In particular, results in [Gomez-Calderon and Madden 1988] imply that $\alpha_p(f) \geq 2d^{-1} + o(1)$ whenever $p \not\equiv \pm 1 \pmod d$.

The rest of this paper is organized as follows. In Section 2 we state a general and quantitative version of Theorem 1.4 for polynomials over arbitrary number fields, and outline the proof strategy, with the details given in Section 3. In Section 4 we state a precise form of the inverse sieve conjecture and deduce Theorem 1.5. In Section 5, Theorem 1.7 is proved by computing relevant Galois groups. Finally, in Section 6, we make some further remarks concerning the larger sieve as well as the quantity $\alpha(f)$.

2. Statement of results and proof strategy

Notation. For a number field K, we denote by $\mathcal{O}_K$ its ring of integers and by Δ_K its (absolute) discriminant. For a prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$, we use $\kappa_\mathfrak{p}$ to denote the residue field $\mathcal{O}_K/\mathfrak{p}$ and $N(\mathfrak{p}) = |\kappa_\mathfrak{p}|$ to denote the norm of $\mathfrak{p}$. For a polynomial f with coefficients in $\mathcal{O}_K$, we use $f_\mathfrak{p}$ to denote its reduction modulo $\mathfrak{p}$.

As indicated in the introduction, we are mainly interested in studying the sizes of value sets of $f_\mathfrak{p}$ for one-variable polynomials f.

Definition 2.1. Let K be a number field, and let $f(x) \in \mathcal{O}_K[x]$ be a polynomial. For any prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$, define

$$\alpha_\mathfrak{p}(f) = N(\mathfrak{p})^{-1} |f_\mathfrak{p}(\kappa_\mathfrak{p})|.$$

This will be studied via the related quantity that measures the number of solutions of $g_\mathfrak{p} = 0$ for (multivariable) polynomials g.

Definition 2.2. Let K be a number field and let $g(\underline{X}) \in \mathcal{O}_K[\underline{X}]$ be a polynomial in n variables $\underline{X} = (X_1, \dots, X_n)$. For any prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$, define

$$m_\mathfrak{p}(g) = N(\mathfrak{p})^{-(n-1)} |\{\underline{X} \in \kappa_\mathfrak{p}^n : g_\mathfrak{p}(\underline{X}) = 0\}|.$$

To make our result quantitative, we also need a notion that measures the sizes of the coefficients of a polynomial.

Definition 2.3 (heights). Let K be a number field, and let $g(x) \in \mathbb{O}_K[\underline{X}]$ be a polynomial. We define its (absolute logarithmic) height $h(g)$ to be the sum

$$h(g) = \sum_v \max_a \log |a|_v, \tag{2-1}$$

where the sum is over all places v of K and the maximum is taken over all coefficients a of g.

Here $|a|_v$ is the normalized absolute value, so that it does not depend on the choice of the field K. For example, when $f \in \mathbb{Z}[x]$ is primitive, the height $h(f)$ is the logarithm of the (usual archimedean) absolute value of the largest coefficient of f. See [Hindry and Silverman 2000] for basic properties of the height function.

Theorem 2.4. *Let K be a number field and $f \in \mathbb{O}_K[x]$ be a polynomial of degree $d \geq 1$. Let $g \in \mathbb{O}_K[x, y]$ be the polynomial defined by $g(x, y) = f(x) - f(y)$. Let $s(g)$ be the number of irreducible factors of g in $K[x, y]$. Then for any $Q \geq 2$ we have*

$$\sum_{N(\mathfrak{p}) \leq Q} m_{\mathfrak{p}}(g) = s(g) \sum_{N(\mathfrak{p}) \leq Q} 1 + O\big(Q \exp(-c\sqrt{\log Q}) + h(g)\big)$$

for sufficiently small $c = c(K, d) > 0$.

Proof of Theorem 1.4 assuming Theorem 2.4. First, by an application of the Cauchy–Schwarz inequality, we have $\alpha_{\mathfrak{p}}(f) \geq m_{\mathfrak{p}}(g)^{-1}$. It thus suffices to show that

$$s(g) \leq \tau(d) \tag{2-2}$$

when $K = \mathbb{Q}$. This follows by considering the homogeneous part of degree d of $g(x, y) = f(x) - f(y)$. Indeed, since this homogeneous part is $a(x^d - y^d)$ for some $a \neq 0$, it factors into $\tau(d)$ irreducible factors over $\mathbb{Q}$ (which are cyclotomic polynomials), and thus $g(x, y)$ can be factored into at most $\tau(d)$ irreducible factors over $\mathbb{Q}$. □

Remark 2.5. The argument above motivates the choice of f_n in Theorem 1.7. Indeed, if a polynomial f is highly decomposable, in the sense that f is the composition of many polynomials (each of which has degree at least 2), then $g(x, y) = f(x) - f(y)$ will necessarily have many irreducible factors, which should lead to small values of $\alpha_p(f)$. In Proposition 5.3 we deduce another consequence of Theorem 2.4, that indecomposable polynomials have large values of α_p.

We will in fact prove the following more general result, of which Theorem 2.4 is a special case. Two polynomials g_1, g_2 are said to be equivalent if they are scalar multiples of each other. Recall also that $g \in K[\underline{X}]$ is said to be absolutely

(or geometrically) irreducible if it is irreducible and remains irreducible over the algebraic closure of K.

Theorem 2.6 (average number of solutions modulo primes). *Let K be a number field and $g(\underline{X}) \in \mathbb{O}_K[\underline{X}]$ be a polynomial in n variables of total degree $d \geq 1$. Let $s(g)$ be the number of nonequivalent irreducible factors of g in $K[\underline{X}]$. Let L be a Galois extension of K such that g factors into absolutely irreducible factors in $L[\underline{X}]$. Let $C = C(K, n, d) > 0$ be sufficiently large. If $Q \geq \exp(C(\log \Delta_L)^2)$, then*

$$\sum_{N(\mathfrak{p}) \leq Q} m_{\mathfrak{p}}(g) \log N(\mathfrak{p}) = s(g)Q - t(g)\frac{Q^{\beta_0}}{\beta_0} + O\big(Q \exp(-c\sqrt{\log Q}) + h(g) + \log \Delta_L\big) \quad (2\text{-}3)$$

for sufficiently small $c = c(K, n, d) > 0$, where $t(g) \in [0, s(g)]$, and the second term appears only if the Dedekind zeta function ζ_L has a Siegel zero $\beta_0 \in \big(\frac{1}{2}, 1\big)$. Consequently, for $Q \geq \exp(C(\log \Delta_L)^2)$ we have

$$\sum_{N(\mathfrak{p}) \leq Q} m_{\mathfrak{p}}(g) \leq s(g) \sum_{N(\mathfrak{p}) \leq Q} 1 + O\big(Q \exp(-c\sqrt{\log Q}) + h(g) + \log \Delta_L\big). \quad (2\text{-}4)$$

The bounds for the error terms stem from a quantitative version of the Chebotarev density theorem in [Lagarias and Odlyzko 1977]. Assuming the truth of the generalized Riemann hypothesis (GRH) for ζ_L, we can get a much better error term $O\big(Q^{1/2}(\log \Delta_L + [L : Q] \log Q)\big)$, and of course without the Siegel zero term. The unconditional error term, however, is already enough for our application.

Proof of Theorem 2.4 assuming Theorem 2.6. We show that $g(x, y) = f(x) - f(y)$ factors into absolutely irreducible factors over $L = K(\mu_d)$, where μ_d is the group of d-th roots of unity. Indeed, since the homogeneous part of degree d of $f(x) - f(y)$ is $a(x^d - y^d)$ for some nonzero $a \in K$, it factors over L into linear factors. Thus, there is a factorization

$$f(x) - f(y) = \prod_{i=1}^{r} g_i(x, y)$$

of $f(x) - f(y)$ into absolutely irreducible factors $g_1, g_2, \ldots, g_r$, such that the top-degree part of each g_i is defined over L. We claim that each g_i is defined over L as well. Suppose not. Without loss of generality, assume that some coefficient of g_1 does not lie in L. Let $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/L)$ be an automorphism that moves this coefficient. Let $\tau(g_1)$ be the polynomial obtained by applying τ to every coefficient of g_1. Then $\tau(g_1)$ is also a factor of $f(x) - f(y)$, and thus $\tau(g_1)$ is equivalent to g_i for some $1 \leq i \leq r$. By our choice of τ, $\tau(g_1)$ must be equivalent to g_i for some $i > 1$, and thus g_1 and g_i have equivalent top-degree parts. This contradicts the fact that $x^d - y^d$ has no repeated factors.

Now that the potential Siegel zero β_0 of ζ_L depends only on K and d, the Siegel zero term in (2-3) can be absorbed into the error term, and the conclusion follows easily from partial summation. □

Remark 2.7. In the argument above we used the fact that polynomials of the form $f(x) - f(y) \in K[x, y]$ factor into absolutely irreducible factors in $L[x, y]$, with $L = K(\mu_d)$. For a general polynomial $g(\underline{X}) \in K[\underline{X}]$ of height $h(g)$, it can be shown that one can take L with $[L : \mathbb{Q}] \leq C$ and $\Delta_L \leq C \exp(Ch(g))$ for some constant $C = C(K, n, d) > 0$. Thus the $\log \Delta_L$ factor in the error term can be removed, and the assumption on Q can be replaced by $Q \geq \exp(Ch(g)^2)$. We will, however, not need this relation between the size of L and the height $h(g)$.

Remark 2.8. The arguments used in proving Theorem 2.6 can be generalized to study the average behavior of $|V(\mathbb{F}_p)|$ as p varies, for any algebraic variety V defined over $\mathbb{Z}$. More precisely, let $m = \dim V$. Then the average of $p^{-m}|V(\mathbb{F}_p)|$ as p varies is equal to the number of irreducible components of V.

To finish this section, we sketch the proof of Theorem 2.6. By Lang–Weil, $m_{\mathfrak{p}}(g)$ is essentially the number of absolutely irreducible factors of $g_{\mathfrak{p}}$. Factor g into absolutely irreducible factors in $L[\underline{X}]$, and consider the natural action of the Galois group $G = \mathrm{Gal}(L/K)$ on these factors. For almost all primes $\mathfrak{P} \subset \mathbb{O}_L$, these absolutely irreducible factors remain absolutely irreducible modulo $\mathfrak{P}$, and thus $m_{\mathfrak{p}}(g)$ is essentially the number of these factors which are defined over $\kappa_{\mathfrak{p}}$. This is equal to the number of fixed points of the Frobenius element associated with $\mathfrak{P}$. By the Chebotarev density theorem, these Frobenius elements are equidistributed in G as $\mathfrak{P}$ varies. Hence the average of $m_{\mathfrak{p}}(g)$ is equal to the average number of fixed points of the G-action. By Burnside's lemma, this is equal to the number of G-orbits, which is exactly the number of irreducible factors $s(g)$ of g. In carrying out this procedure some additional effort is needed to keep track of the explicit dependence on the height of g.

3. Proof of Theorem 2.6

In this section we prove Theorem 2.6. The implied constants appearing in this section are always allowed to depend on K, n, d.

Factor (g) into principal prime ideals in $L[\underline{X}]$:

$$(g) = (g_1)^{e_1}(g_2)^{e_2} \cdots (g_r)^{e_r},$$

where $g_i \in L[\underline{X}]$ is absolutely irreducible, and g_i, g_j are not equivalent when $i \neq j$. Let G be the Galois group $\mathrm{Gal}(L/K)$. For any $1 \leq i \leq r$ and any $\xi \in G$, let $\xi(g_i)$ be the polynomial obtained by applying ξ to all coefficients of g_i. Since $\xi(g_i)$ is also a factor of g, $\xi(g_i)$ is equivalent to g_j for some $1 \leq j \leq r$. Hence ξ acts on

$\{(g_1), \dots, (g_r)\}$ by sending (g_i) to $(\xi(g_i))$. In this way we obtain a G-action on $\{(g_1), \dots, (g_r)\}$.

Lemma 3.1 (Galois descent). *Let E be any field and F be a Galois extension of E. Let $h \in F[\underline{X}]$ be a polynomial. The following two statements are equivalent*:

(1) *The ideal $(h) \subset F[\underline{X}]$ is fixed by every element of $G = \mathrm{Gal}(F/E)$.*

(2) *The ideal (h) is defined over E. In other words, there exists a scalar $\alpha \in F^\times$ such that $\alpha h \in E[\underline{X}]$.*

Proof. This is a standard result in the theory of Galois descent. For completeness, we give a proof here. Clearly (2) implies (1). Now assume that (1) holds, so that for each $\xi \in G$, we have $\xi(h) = c_\xi h$ for some $c_\xi \in F^\times$. The scalars $\{c_\xi : \xi \in G\}$ form a 1-cocycle $G \to F^\times$, and thus by Hilbert's Theorem 90 we have $c_\xi = \alpha/\xi(\alpha)$ for some $\alpha \in F^\times$. Now that $\xi(h) = \alpha h/\xi(\alpha)$, we conclude that $\xi(\alpha h) = \alpha h$ for each $\xi \in G$. Thus $\alpha h \in E[\underline{X}]$, as desired. □

Lemma 3.2. *Let the notation be as above. The number of orbits of the G-action on $\{(g_1), (g_2), \dots, (g_r)\}$ is equal to $s(g)$.*

Proof. Let $\mathcal{H} = \{h_1, h_2, \dots, h_s\}$ be the set of nonequivalent irreducible factors of g (well defined up to scalars in K), where $s = s(g)$. We construct a bijection between the set of orbits and $\mathcal{H}$.

Let $\mathbb{O} \subset \{(g_1), (g_2), \dots, (g_r)\}$ be a G-orbit, and let h be the product of those g_i with $(g_i) \in \mathbb{O}$. We claim that (h) is defined over K, and moreover (h) is a prime ideal in $K[\underline{X}]$ (hence $(h) = (h_j)$ for some $1 \le j \le s$). In fact, since any $\xi \in G$ permutes the factors in $\mathbb{O}$, the ideal (h) is fixed by ξ. By Lemma 3.1, the ideal (h) is defined over K. Now let $h' \in K[\underline{X}]$ be a factor of h (with positive degree), and let $\mathbb{O}' \subset \mathbb{O}$ be the set of those $(g_i) \in \mathbb{O}$ dividing h'. For any $(g_i) \in \mathbb{O}'$ and any $\xi \in G$, $\xi(g_i)$ is also a factor of h' and thus $(\xi(g_i)) \in \mathbb{O}'$. This shows that G preserves $\mathbb{O}'$, and thus $\mathbb{O}' = \mathbb{O}$ and $(h') = (h)$. Hence (h) is a prime ideal.

Conversely, let $h_j \in \mathcal{H}$ be an irreducible factor of g, and let $\mathbb{O}$ be the set of those (g_i) dividing h_j. We claim that $\mathbb{O}$ is a G-orbit, and moreover the product of those ideals in $\mathbb{O}$ is equal to (h_j). In fact, for any $\xi \in G$ and $(g_i) \in \mathbb{O}$, the polynomial $\xi(g_i)$ is also a factor of h_j. Hence G preserves $\mathbb{O}$. If $\mathbb{O}' \subset \mathbb{O}$ is a G-orbit, the argument above shows that the product of the ideals in $\mathbb{O}'$ is defined over K. Hence $\mathbb{O}' = \mathbb{O}$ by the irreducibility of h_j. Finally, the argument above also shows that the product of the ideals in $\mathbb{O}$ is defined over K, and is thus equal to (h_j). □

The following lemma shows that the heights of the factors g_i are controlled by the height of g. Note that the height $h(g_i)$ depends only on the ideal (g_i) since two equivalent polynomials have the same height.

Lemma 3.3 (Gelfond's inequality). *Let the notation be as above. Then $h(g_i) \le h(g) + C$ for some constant $C = C(K, n, d) > 0$.*

Proof. See Proposition B.7.3 in [Hindry and Silverman 2000]. □

Let $\mathfrak{p}$ be a prime in $\mathbb{O}_K$ and $\mathfrak{P}$ be a prime in $\mathbb{O}_L$ lying above $\mathfrak{p}$. For each $1 \le i \le r$, let $(g_i) \pmod{\mathfrak{P}}$ be the ideal in $\kappa_{\mathfrak{P}}[\underline{X}]$ obtained by reduction modulo $\mathfrak{P}$. The following lemma will be used to ensure that $(g_i) \pmod{\mathfrak{P}}$ remains absolutely irreducible for all but finitely many $\mathfrak{P}$.

Lemma 3.4 (Noether). *Let n, d be positive integers. There exist polynomials $\ell_1, \dots, \ell_m$ with integral coefficients depending only on n and d in variables $A_{i_1 \dots i_n}$ $(i_1 + \cdots + i_n \le d)$, such that the following statement holds. For any algebraically closed field $\bar{F}$, a polynomial $f \in \bar{F}[\underline{X}]$ in n variables of total degree at most d with*

$$f(x_1, \dots, x_n) = \sum_{i_1 + \cdots + i_n \le d} a_{i_1 \dots i_n} x_1^{i_1} \cdots x_n^{i_n}$$

is reducible over $\bar{F}$ or has total degree less than d if and only if $\ell_j((a_{i_1 \dots i_n})) = 0$ for each $1 \le j \le m$.

Proof. See Theorem 2A in [Schmidt 1976]. □

Lemma 3.5. *Let the notation be as above. There exists a positive integer $E \le C \exp(Ch(g))$, for some $C = C(K, n, d) > 0$, such that $(g_i) \pmod{\mathfrak{P}}$ is absolutely irreducible for each $1 \le i \le r$ whenever $\mathfrak{P} \nmid E$.*

Proof. It suffices to prove the statement for each individual i. Let $\ell_1, \dots, \ell_m$ be the polynomials in Lemma 3.4 corresponding to the degree of g_i. After normalizing we may assume that some coefficient of g_i is equal to 1. Thus $h(a) \le h(g_i)$ for every coefficient a of g_i, where $h(a)$ for $a \in L^\times$ is defined by

$$h(a) = \sum_v \max(\log |a|_v, 0).$$

Since g_i is absolutely irreducible, ℓ_j does not vanish at the coefficient vector of g_i for some $1 \le j \le m$; call this nonvanishing value $A \in L \setminus \{0\}$. Since all coefficients of g_i have heights bounded by $h(g_i)$, we have $h(A) = O(h(g_i) + 1) = O(h(g) + 1)$. Therefore, there exists a positive integer $E \le C \exp(Ch(g))$ such that $A \pmod{\mathfrak{P}}$ is nonzero whenever $\mathfrak{P} \nmid E$. For these $\mathfrak{P}$, the absolute irreducibility of $g_i \pmod{\mathfrak{P}}$ follows from another application of Lemma 3.4. □

Remark 3.6. The qualitative version of this statement is a special case of a general result in algebraic geometry: if R is a domain with fraction field F and S is a domain finitely generated over R such that the F-algebra $S_F = F \otimes_R S$ is absolutely irreducible over F, then there is a nonempty open subset $U \subset \operatorname{Spec}(R)$ such that the fiber algebra $S_u = k(u) \otimes_R S$ over $k(u)$, the residue field at u, is absolutely irreducible.

Let E be the positive integer from Lemma 3.5. After enlarging E if necessary (but still with $E \le C\exp(Ch(g))$), we may assume that $g_1 \pmod{\mathfrak{P}}, \dots, g_r \pmod{\mathfrak{P}}$ are pairwise inequivalent whenever $\mathfrak{P} \nmid E$.

Let $\mathfrak{p} \nmid E$ be a prime in $\mathbb{O}_K$ and $\mathfrak{P}$ be a prime in $\mathbb{O}_L$ lying above $\mathfrak{p}$. The decomposition group $G_{\mathfrak{P}} = \mathrm{Gal}(\kappa_{\mathfrak{P}}/\kappa_{\mathfrak{p}})$ acts on the factors $\{g_1 \pmod{\mathfrak{P}}, \dots, g_r \pmod{\mathfrak{P}}\}$ so that $\xi(g_i \pmod{\mathfrak{P}})$ is equivalent to $g_j \pmod{\mathfrak{P}}$ for any $\xi \in G_{\mathfrak{P}}$. Comparing this with the G-action on $\{g_1, \dots, g_r\}$ described at the beginning of this section, we see that they are compatible via the natural inclusion $G_{\mathfrak{P}} \hookrightarrow G$. In particular, both $G_{\mathfrak{P}}$ and G can be viewed as subgroups of the symmetric group on r elements.

For any conjugacy class $[\xi] \subset G$, let $s([\xi])$ be the number of fixed points of any element in $[\xi]$.

Lemma 3.7. *Let the notation be as above. If $\mathfrak{p} \nmid E$ and $\mathfrak{p}$ is unramified in L, then $m_{\mathfrak{p}}(g) = s([\sigma_{\mathfrak{p}}]) + O(N(\mathfrak{p})^{-1/2})$, where $[\sigma_{\mathfrak{p}}]$ is the Frobenius conjugacy class associated to $\mathfrak{p}$.*

Proof. Let $h \in \{g_1, \dots, g_r\}$. Note that $\sigma_{\mathfrak{P}}$ fixes (h) if and only if $\sigma_{\mathfrak{P}}$ fixes $(h_{\mathfrak{P}})$, and this happens if and only if $(h_{\mathfrak{P}})$ is defined over $\kappa_{\mathfrak{p}}$, by Lemma 3.1. Hence $s([\sigma_{\mathfrak{p}}])$ is exactly the number of nonequivalent absolutely irreducible factors of $g_{\mathfrak{p}}$ in $\kappa_{\mathfrak{p}}[\underline{X}]$.

Now let $h_1, \dots, h_s, h_{s+1}, \dots, h_t$ be the nonequivalent irreducible factors of $g_{\mathfrak{p}}$ in $\kappa_{\mathfrak{p}}[\underline{X}]$, where $h_1, \dots, h_s$ are absolutely irreducible, with $s = s([\sigma_{\mathfrak{p}}])$. Let $V(h_i)$ be the solution set $\{\underline{X} \in \kappa_{\mathfrak{p}}^n : h_i(\underline{X}) = 0\}$. Then

$$m_{\mathfrak{p}}(g) = N(\mathfrak{p})^{-(n-1)}\left(\sum_{i=1}^{t} |V(h_i)| + O\left(\sum_{i<j} |V(h_i) \cap V(h_j)|\right)\right). \tag{3-1}$$

For $i < j$, since h_i and h_j are nonequivalent, $V(h_i) \cap V(h_j)$ has dimension at most $n-2$. Thus by the Lang–Weil bound [1954] we have

$$|V(h_i) \cap V(h_j)| \ll N(\mathfrak{p})^{n-2}.$$

(In fact the weaker Schwarz–Zippel estimate is enough here). On the other hand, for $1 \le i \le s$, the Lang–Weil bound gives

$$|V(h_i)| = N(\mathfrak{p})^{n-1}(1 + O(N(\mathfrak{p})^{-1/2}))$$

since h_i is absolutely irreducible, and for $s < i \le t$ we have

$$|V(h_i)| = |V(h_i) \cap V(h_j)| \ll N(\mathfrak{p})^{n-2}$$

for some $s < j \le t$, with h_j a Galois conjugate of h_i. Combining these estimates together in (3-1) we obtain

$$m_{\mathfrak{p}}(g) = s + O(N(\mathfrak{p})^{-1/2}),$$

as desired. □

We are now ready to evaluate the quantity

$$M_f(Q) = \sum_{N(\mathfrak{p}) \le Q} m_{\mathfrak{p}}(g) \log N(\mathfrak{p}).$$

By Lemma 3.7, we have

$$M_f(Q) = \sum_{\substack{N(\mathfrak{p}) \le Q \\ \mathfrak{p} \text{ unramified in } L}} s([\sigma_{\mathfrak{p}}]) \log N(\mathfrak{p}) + O(Q^{1/2} \log Q + \log E + \log \Delta_L).$$

Since $E \le C \exp(Ch(g))$, we have $\log E = O(h(g) + 1)$. Hence

$$M_f(Q) = \sum_C s(C)\psi_C(Q) + O(Q^{1/2} \log Q + h(g) + \log \Delta_L),$$

where the sum is over all conjugacy classes C in G, and

$$\psi_C(Q) = \sum_{\substack{N(\mathfrak{p}) \le Q \\ \mathfrak{p} \text{ unramified in } L \\ [\sigma_{\mathfrak{p}}]^m = C}} \log N(\mathfrak{p}).$$

By (a quantitative version of) the Chebotarev density theorem [Lagarias and Odlyzko 1977], for $Q \ge \exp(C(\log \Delta_L)^2)$ we have

$$\psi_C(Q) = \frac{|C|}{|G|} Q - \frac{|C|}{|G|} \chi_0(C) \frac{Q^{\beta_0}}{\beta_0} + O\big(Q \exp(-c(\log Q)^{1/2})\big),$$

where the second term occurs only if the Dedekind zeta function ζ_L has a Siegel zero β_0, and χ_0 is the real character of a one-dimensional representation of G for which the associated L-function has β_0 as a zero. It follows that

$$M_f(Q) = Q \cdot \frac{1}{|G|} \sum_{\xi \in G} s(\xi) - \frac{Q^{\beta_0}}{\beta_0} \cdot \frac{1}{|G|} \sum_{\xi \in G} s(\xi)\chi_0(\xi) + O\big(Q \exp(-c(\log Q)^{1/2}) + h(g) + \log \Delta_L\big).$$

By Burnside's lemma and Lemma 3.2, we have

$$\frac{1}{|G|} \sum_{\xi \in G} s(\xi) = s(g). \tag{3-2}$$

The equality (2-3) follows by setting

$$t(g) = \frac{1}{|G|} \sum_{\xi \in G} s(\xi)\chi_0(\xi). \tag{3-3}$$

By a change of summation, we can write

$$t(g) = \frac{1}{|G|} \sum_{i=1}^{r} \sum_{\xi \in G_i} \chi_0(\xi),$$

where $G_i \subset G$ is the subgroup of elements fixing (g_i). Since χ_0 is a one-dimensional real character, the inner sum is either 0 or $|G_i|$, and in the latter case $\chi_0(\xi) = 1$ for all $\xi \in G_i$. Thus in the sum in (3-3) we may restrict to those ξ with $\chi_0(\xi) = 1$. Comparing this with (3-2), we obtain $t(g) \in [0, s(g)]$ as claimed.

Finally, the inequality (2-4) follows easily from (2-3) by dropping the Siegel zero term and partial summation.

4. Inverse sieve conjecture implies improved larger sieve

In this section we state a precise version of the inverse sieve conjecture and then prove Theorem 1.5. The implied constants here are always allowed to depend on α, ϵ.

Conjecture 4.1 (inverse sieve conjecture). *Let $X \subset [N]$ be a subset and let $\epsilon, \epsilon' > 0$ be real. Assume that for each parameter $Q \geq N^{\epsilon}$ we have*

$$\sum_{p \leq Q} \frac{|X \pmod p|}{p} \leq (1 - \epsilon')\pi(Q).$$

Then at least one of the following two situations happens:

(1) (*very small size*) $|X| \ll_{\epsilon, \epsilon'} N^{\epsilon}$.

(2) (*algebraic structure*) *There exists a polynomial $f(x) \in \mathbb{Q}[x]$ of degree $d \in [2, C]$ and height at most N^C such that $|X \cap f([N])| \geq C^{-1}|X|$, where $C = C(\epsilon, \epsilon')$ is a constant.*

Here, we say that a polynomial $f(x) \in \mathbb{Q}[x]$ has height at most H if $f(x) = A^{-1} f^*(x)$ for some positive integer $A \leq H$ and $f^* \in \mathbb{Z}[x]$ with all coefficients bounded by H in absolute value. This is slightly different from the notion of height used in the statement of Theorem 2.4, in that $h(f)$ is invariant under scalar multiplication but the notion here is not. Note that if a polynomial $f(x) \in \mathbb{Q}[x]$ has height at most H, then $h(f) \ll \log H$.

Remark 4.2. We make a few remarks explaining why some quantitative aspects of this conjecture are reasonable.

- The condition on X essentially says that X misses a positive proportion of residue classes modulo primes p on average, as soon as p exceeds a small positive power of N. With this assumption, we know from the large sieve that $|X| \ll N^{1/2}$ and from the larger sieve that $|X| \ll N^{\alpha + O(\epsilon)}$ if the upper bound $(1 - \epsilon')\pi(Q)$ is

replaced by $\alpha\pi(Q)$. Without the knowledge about $X \pmod p$ for $p \le N^\epsilon$, one can essentially add to X any N^ϵ extra elements without violating the assumption, but one should still expect to see algebraic structure apart from these extra elements.

- The conclusion $|X \cap f([N])| \ge C^{-1}|X|$ is equivalent to the seemingly weaker one $|X \cap f(\mathbb{Q})| \ge C^{-1}|X|$, after a suitable modification of the polynomial f which does not increase its height too much. To see that the interval $[N]$ can be replaced by $\mathbb{Z}$, note that the set $J = \{n \in \mathbb{Z} : 1 \le f(n) \le N\}$ is the union of at most d intervals and has size at most dN. Since $X \cap f(\mathbb{Z}) = X \cap f(J)$, there is an interval $I \subset J$ with $|X \cap f(I)| \ge d^{-1}|X \cap f(\mathbb{Z})|$, and we may assume that $I \subset [N]$ after a translation. To see that $f(\mathbb{Z})$ can be replaced by $f(\mathbb{Q})$, note that if $f(x) \in \mathbb{Z}$ for some $x \in \mathbb{Q}$ then the denominator of x must divide some positive integer B depending on the coefficient of f. Then $f(\mathbb{Q}) \cap \mathbb{Z} \subset f^*(\mathbb{Z}) \cap \mathbb{Z}$, where f^* is defined by $f^*(x) = f(x/B)$.
- The conclusion that $f(\mathbb{Z})$ captures a positive proportion of X cannot be replaced by the stronger one that $f(\mathbb{Z})$ captures almost all of X. Indeed, it is possible for X to be the union of $f(\mathbb{Z})$ for several distinct polynomials f.

If $|X \pmod p| \le \alpha p$ for small α, repeated applications of Conjecture 4.1 allow us to strengthen it by requiring the degree d to be fairly large.

Proposition 4.3 (inverse sieve conjecture in the larger sieve regime). *Assume the truth of Conjecture 4.1. Let $X \subset [N]$ be a subset. Let $\alpha \in (0, 1)$ and $\epsilon \in (0, \alpha)$ be real. Assume that $|X \pmod p| \le (\alpha + o(1))p$ for each prime p. Then at least one of the following two situations happens*:

(1) (*very small size*) $|X| \ll_\epsilon N^\epsilon$.

(2) (*algebraic structure*) *There exists a polynomial $f(x) \in \mathbb{Q}[x]$ of degree $d \in [2, C]$ and height at most N^C such that $|X \cap f(\mathbb{Z})| \ge C^{-1}|X|$, where $C = C(\epsilon)$ is a constant. Moreover, we may ensure that $\tau(d) \ge (1 - \epsilon)\alpha^{-1}$.*

Proof. Suppose that $|X| \gg N^\epsilon$. We will apply Conjecture 4.1 iteratively to construct a sequence of polynomials $f_1, f_2, \dots, f_k$ and a sequence of sets $X_0 = X, X_1, X_2, \dots, X_k$, with $k = O(1)$, such that the following conditions hold:

(1) $\deg f_i = d_i \in [2, C]$, and $\tau(d_1 d_2 \cdots d_k) \ge (1 - \epsilon)\alpha^{-1}$;

(2) the height of f_i is at most $N^{O(1)}$ for each $1 \le i \le k$;

(3) $X_i \subset [N]$ and $|X_i| \gg |X_{i-1}|$ for each $1 \le i \le k$;

(4) $f_i(X_i) \subset X_{i-1}$ for each $1 \le i \le k$.

Suppose first that these objects are constructed. Let $f = f_1 \circ f_2 \circ \cdots \circ f_k$. By property (1), the degree d of f is $O(1)$ and satisfies $\tau(d) \ge (1 - \epsilon)\alpha^{-1}$. By

property (2), the height of f is $N^{O(1)}$. By property (3), we have $|X_k| \gg |X|$. By property (4), we have $f(X_k) \subset X \cap f([N])$. Hence

$$|X \cap f([N])| \geq |f(X_k)| \gg |X_k| \gg |X|,$$

as desired.

It thus remains to construct $f_1, \ldots, f_k$ and $X_1, \ldots, X_k$. Suppose that f_j, X_j with $j < i$ are already chosen for some $i \geq 1$ satisfying the required properties (2)–(4) and $\deg f_j = d_j \in [2, C]$. We will construct f_i and X_i from these. Let $F = f_1 \circ \cdots \circ f_{i-1}$ if $i > 1$ and let F be the identity map if $i = 1$. Let D be the degree of F. We may assume that $\tau(D) < (1-\epsilon)\alpha^{-1}$, since we may stop the iteration otherwise. By property (4), we have $F(X_{i-1}) \subset X$.

Let $F = A^{-1}F^*$ with $A \leq N^C$ a positive integer and $F^* \in \mathbb{Z}[x]$ a polynomial whose coefficients are all bounded by N^C. Let $G \in \mathbb{Z}[x, y]$ be the polynomial defined by $G(x, y) = F^*(x) - F^*(y)$. Let $p \nmid A$ be a prime. For each $r \in \mathbb{Z}/p\mathbb{Z}$, let $\nu_p(r)$ be the number of $x \in \mathbb{Z}/p\mathbb{Z}$ with $F(x) \equiv r \pmod p$. Then

$$\begin{aligned} |X_{i-1} \pmod p| &\leq \sum_{r \in F(X_{i-1}) \pmod p} \nu_p(r) \\ &\leq |X \pmod p|^{1/2} \Big(\sum_r \nu_p(r)^2 \Big)^{1/2} \\ &\leq (\alpha + o(1))^{1/2} m_p(G)^{1/2} p, \end{aligned}$$

by Cauchy–Schwarz, the assumption that $|X \pmod p| \leq (\alpha + o(1))p$, and the definition of $m_p(G)$ in Definition 2.2. For any $Q \geq N^\epsilon$, we then have

$$\begin{aligned} \sum_{p \leq Q} \frac{|X_{i-1} \pmod p|}{p} &\leq (\alpha + o(1))^{1/2} \sum_{p \leq Q} m_p(G)^{1/2} + O(\log A) \\ &\leq (\alpha + o(1))^{1/2} \pi(Q)^{1/2} \Big(\sum_{p \leq Q} m_p(G) \Big)^{1/2} + O(\log N). \end{aligned}$$

Now apply Theorem 2.4 (and recall (2-2)) to obtain

$$\begin{aligned} &\sum_{p \leq Q} \frac{|X_{i-1} \pmod p|}{p} \\ &\qquad \leq [(\alpha + o(1))\tau(D)]^{1/2} \pi(Q) + O\big(Q \exp(-c(\log Q)^{1/2}) + Q^{1/2} \log N\big). \end{aligned}$$

Since $\tau(D) < (1-\epsilon)\alpha^{-1}$, the first term above is at most $(1 - \epsilon/2)\pi(Q)$, and thus X_{i-1} satisfies the hypotheses in Conjecture 4.1, with ϵ replaced by $\epsilon/3$ and N sufficiently large. Since $|X_{i-1}| \gg N^\epsilon$, we must be in the algebraic case. Let $f_i \in \mathbb{Q}[x]$ be a polynomial of degree $d_i \in [2, C]$ and height at most N^C such that $|X_{i-1} \cap f_i([N])| \gg |X_{i-1}|$, and let $X_i \subset [N]$ be chosen so that $f_i(X_i) \subset X_{i-1}$

and $|X_i| \gg |X_{i-1}|$. This completes the inductive construction. Finally, since the quantity $\tau(d_1 d_2 \cdots d_i)$ strictly increases with i, the process terminates after $O(1)$ iterations. □

Proof of Theorem 1.5. Apply Proposition 4.3 to conclude that either $|X|$ is very small and we are done, or else there exists a polynomial $f(x) \in \mathbb{Q}[x]$ of degree $d \in [2, C]$ and height at most N^C such that $|X \cap f([N])| \geq C^{-1}|X|$. Moreover, we have $\tau(d) \geq (1-\epsilon)\alpha^{-1}$. Hence

$$|X| \ll |X \cap f([N])| \leq |[N] \cap f([N])| \ll N^{1/d},$$

where the last inequality follows from a result of Walsh [2015], which removes the ϵ term from the exponent appearing in [Bombieri and Pila 1989; Heath-Brown 2002]. □

5. Polynomials with small value sets modulo primes

In this section we prove Theorem 1.7. First we state a result connecting the quantity $\alpha_p(f)$ to a Galois group. For a polynomial $f(x) \in \mathbb{F}_p[x]$ of degree d, denote by R_f the set of roots in $\overline{\mathbb{F}_p(t)}$ of the polynomial $f(x) - t$. Define

$$G_f = \mathrm{Gal}(\mathbb{F}_p(R_f)/\mathbb{F}_p(t)), \quad G_f^* = \mathrm{Gal}(\overline{\mathbb{F}}_p(R_f)/\overline{\mathbb{F}}_p(t)).$$

In other words, G_f and G_f^* are the Galois groups of the splitting field of $f(x) - t$ over $\mathbb{F}_p(t)$ and $\overline{\mathbb{F}}_p(t)$, respectively. It is easy to see that G_f^* is a normal subgroup of G_f with G_f/G_f^* cyclic. In fact, G_f/G_f^* is isomorphic to $\mathrm{Gal}(\mathbb{F}_p(R_f) \cap \overline{\mathbb{F}}_p/\mathbb{F}_p)$. For any subset $\Xi \subset G_f$, we use $\alpha(\Xi)$ to denote the proportion of elements in Ξ with at least one fixed point under the natural action on R_f.

Lemma 5.1 [Cohen 1970]. *Let $f(x) \in \mathbb{F}_p[x]$ be a polynomial of degree $d \geq 1$. Let σG_f^* be the coset which is the Frobenius generator of the cyclic quotient G_f/G_f^*, considered under its isomorphism with* $\mathrm{Gal}(\mathbb{F}_p(R_f) \cap \overline{\mathbb{F}}_p/\mathbb{F}_p)$. *Then*

$$\alpha_p(f) = \alpha(\sigma G_f^*) + O_d(p^{-1/2}).$$

In particular, if $G_f = G_f^*$ then

$$\alpha_p(f) = \alpha(G_f) + O_d(p^{-1/2}).$$

Remark 5.2. In [Cohen 1970] this is deduced from a function field version of the Chebotarev density theorem. The Galois groups G_f and G_f^* above can be interpreted in terms of finite étale Galois coverings of $\mathbb{P}^1(\mathbb{F}_p)$. In this way Lemma 5.1 becomes a 0-dimensional special case of Deligne's equidistribution theorem. See [Kowalski 2010] for an excellent survey on this topic. This function field version of the Chebotarev density theorem and related equidistribution results play an important

role in proving function field analogues of certain classical analytic number theory conjectures [Bank et al. 2015; Andrade et al. 2015; Entin 2014].

Proof of Theorem 1.7. Recall that the sequence of polynomials $\{f_n\}$ is defined by

$$f_1(x) = x^2, \quad f_{n+1}(x) = (f_n(x)+1)^2.$$

Write $G_n = G_{f_n}$, $G_n^* = G_{f_n}^*$, and $R_n = R_{f_n}$. Since any root $\alpha \in R_n$ satisfies either $f_{n-1}(\alpha) = -1+\sqrt{t}$ or $f_{n-1}(\alpha) = -1-\sqrt{t}$, we may decompose R_n as the union $R_n = R_n^+ \cup R_n^-$, with

$$R_n^\pm = \{\alpha \in R_n : f_{n-1}(\alpha) = -1 \pm \sqrt{t}\}.$$

Note that both $\mathrm{Gal}(\mathbb{F}_p(R_n^+)/\mathbb{F}_p(\sqrt{t})$ and $\mathrm{Gal}(\mathbb{F}_p(R_n^-)/\mathbb{F}_p(\sqrt{t}))$ are isomorphic to G_{n-1}, and similarly both $\mathrm{Gal}(\overline{\mathbb{F}}_p(R_n^+)/\overline{\mathbb{F}}_p(\sqrt{t})$ and $\mathrm{Gal}(\overline{\mathbb{F}}_p(R_n^-)/\overline{\mathbb{F}}_p(\sqrt{t}))$ are isomorphic to G_{n-1}^*.

Let H_n and H_n^* be the normal subgroup of G_n and G_n^* that fixes $\sqrt{t}$, so that $[G_n : H_n] = [G_n^* : H_n^*] = 2$. Since H_n preserves both R_n^+ and R_n^-, we get an embedding $\iota_n : H_n \hookrightarrow G_{n-1} \times G_{n-1}$ by setting the first and second components of $\iota_n(\xi)$ to be the images of ξ under the two quotient maps $H_n \to \mathrm{Gal}(\mathbb{F}_p(R_n^+)/\mathbb{F}_p(\sqrt{t}))$ and $H_n \to \mathrm{Gal}(\mathbb{F}_p(R_n^-)/\mathbb{F}_p(\sqrt{t}))$, respectively. Similarly, we also get an embedding $\iota_n^* : H_n^* \hookrightarrow G_{n-1}^* \times G_{n-1}^*$.

We show, by induction on n, that when $p > 2f_{n-1}(0)+2$, the embeddings ι_n and ι_n^* are in fact isomorphisms, and moreover $G_n = G_n^*$ for each n. The base case is clear. Now assume that $G_{n-1} = G_{n-1}^*$. To see that ι_n^* is surjective, by Lemma 15 in [Fried 1970] it suffices to verify that for each $\lambda \in \overline{\mathbb{F}}_p$, at most one of the two values $-1+\sqrt{\lambda}$ and $-1-\sqrt{\lambda}$ is a branch point of f_{n-1}. By definition, the set of branch points of f_{n-1} is

$$\{f_{n-1}(x) : x \in \overline{\mathbb{F}}_p,\ f_{n-1}'(x) = 0\}.$$

This is easily computed to be the set

$$\{f_1(0), f_2(0), \ldots, f_{n-1}(0)\} = \{0, 1, 4, 25, \ldots\}.$$

When $p > 2f_{n-1}(0)+2$, it is indeed the case that at most one of $-1+\sqrt{\lambda}$ and $-1-\sqrt{\lambda}$ can lie in this set for any λ. This shows that

$$H_n^* \cong G_{n-1}^* \times G_{n-1}^* \cong G_{n-1} \times G_{n-1}.$$

Moreover, since $H_n^* \subset H_n \subset G_{n-1} \times G_{n-1}$, we conclude that $H_n^* = H_n$, and thus $G_n^* = G_n$ as well. This completes the induction step.

With the structure of G_n in hand, it is now a simple matter to write down the recursive relation

$$\alpha_p(f_n) = \tfrac{1}{2}\big[1 - (1-\alpha_p(f_{n-1}))^2\big] = \alpha_p(f_{n-1}) - \tfrac{1}{2}\alpha_p(f_{n-1})^2,$$

provided that $p > 2f_{n-1}(0) + 2$. In fact, if $\xi \in G_n$ has a fixed point, then ξ must fix $\sqrt{t}$ and thus lie in H_n, and moreover at least one of the two components of $\iota_n(\xi)$ has a fixed point. Finally, the bound $a_n \le 2n^{-1}$ follows from a standard induction argument. □

We mentioned in Remark 2.5 the reasoning behind making f_n highly decomposable. To end this section, we show that decomposability is quite essential in order for α_p to be small. The proof uses Theorem 2.4 together with results in [Fried 1970] (similar arguments are also used in [Guralnick and Wan 1997]). We say that a polynomial f is indecomposable if it cannot be written as a composition of two polynomials of degree at least 2.

Proposition 5.3. *Let $f(x) \in \mathbb{Z}[x]$ be an indecomposable polynomial of degree $d \ge 1$. Then the average value of $\alpha_p(f)^{-1}$ as p varies is at most 2. Consequently, $\alpha(f) \ge \frac{1}{2}$.*

Proof. Let G be the Galois group of the splitting field of $f(x) - t$ over $\mathbb{Q}(t)$, viewed as a subgroup of the symmetric group S_d on d letters via its action on the d roots of $f(x) - t$. Since f is indecomposable, G is primitive [Fried 1970, Lemma 2]. Moreover, G contains a d-cycle [ibid., Lemma 3]. Hence either d is prime or G is doubly transitive [ibid., Lemma 7]. In either case, the conclusion follows from Theorem 2.4, since $\tau(d) = 2$ when d is prime and $(f(x) - f(y))/(x - y) \in \mathbb{Q}[x, y]$ is irreducible when G is doubly transitive [ibid., Lemma 14]. □

6. Further remarks

6A. ***More on the sharpness of Gallagher's larger sieve.*** Gallagher's larger sieve in its general form as stated in Theorem 1.1 has the optimal bound. Indeed, if we take $A \subset [N]$ to be any subset with cardinality Q and take $\mathcal{P}$ be the set of all primes between Q and N, the general form of the larger sieve gives the sharp bound $|A| \ll Q$, because the numerator is about N and the denominator is about N/Q. This shows that any potential improvement to Corollary 1.2 must incorporate the ill-distribution modulo many *small* primes.

Under the assumption of Corollary 1.2, one may go over the argument in the proof of the larger sieve to find out what happens if $|A|$ is close to N^α. Indeed, in the typical proof of Gallagher's larger sieve, one uses the upper and lower bounds

$$\frac{|X|^2}{\alpha} \log Q \le \sum_{x,x' \in X} \sum_{\substack{p \mid x - x' \\ p \le Q}} \log p \le |X|^2 \log N + |X| Q, \tag{6-1}$$

where Q is about N^α.

If the upper bound is (almost) sharp, then almost all of the nonzero differences $x - x'$ should be Q-smooth, meaning that they do not have prime divisors larger

than Q. For a random integer n, it is reasonable to expect that

$$\sum_{\substack{p\mid n\\ p\le Q}} \log p \approx \sum_{p\le Q} \frac{\log p}{p} \sim \log Q. \tag{6-2}$$

If this indeed holds for almost all differences $x - x'$, then one can take Q to be any small power of N and deduce from (6-1) that $|X| \ll N^{\epsilon}$.

Now consider the situation when X is the set of d-th powers up to N. Because of the factorization

$$a^d - b^d = \prod_{\ell\mid d} \Phi_\ell(a, b),$$

where Φ_ℓ is the cyclotomic polynomial of degree $\phi(\ell)$, we cannot expect (6-2) to be true for $n = a^d - b^d$. However, it is still reasonable to expect that each factor $\Phi_\ell(a, b)$ satisfies (6-2). If so, then we obtain an upper bound in (6-1) with $\log N$ there replaced by $\tau(d) \log Q$, which in turn implies that $\tau(d) \ge \alpha^{-1}$. This is consistent with the conclusion of Theorem 1.5.

On the other hand, making this heuristic rigorous could be extremely hard. For example, it is an open problem to obtain a bound better than $|X| \ll N^{1/2}$ for $X \subset [N]$ with all nonzero differences $x - x'$ $(x, x' \in X)$ N^{κ}-smooth, where $\kappa > 0$ is sufficiently small (see [Elsholtz and Harper 2015]).

There are versions of Gallagher's larger sieve over arbitrary number fields [Ellenberg et al. 2009; Zywina 2010]. One can ask similar questions about their sharpness in this general setting, and use Theorem 2.4 to formulate an improved larger sieve conjecture. We will not do so here since the case over $\mathbb{Z}$ is already quite interesting.

6B. ***Computing $\alpha(f)$ via Galois groups.*** The main result of this paper computes the average of $m_p(f)$ as p varies, as a consequence of the Chebotarev density theorem. It is natural to ask if one can compute $\alpha(f)$, the average of $\alpha_p(f)$ as p varies, directly, especially since we do have such a formula for each individual $\alpha_p(f)$ as in Lemma 5.1.

Proposition 6.1. *Let K be a number field and $f(x) \in \mathcal{O}_K[x]$ be a monic polynomial of degree d. Let $G = \mathrm{Gal}(K(R)/K(t))$, where R is the set of roots of $f(x) - t$. Let $\alpha(G)$ be the proportion of elements in G with at least one fixed point under the natural action on R. Then*

$$\lim_{Q\to\infty} \frac{1}{\pi(Q)} \sum_{N(\mathfrak{p})\le Q} \alpha_{\mathfrak{p}}(f) = \alpha(G).$$

In other words, $\alpha(f) = \alpha(G)$.

Remark 6.2. Unfortunately, we are unable to use this interpretation to obtain good lower bounds on $\alpha(f)$, but see [Guralnick and Wan 1997] for an example where

large values of $\alpha_p(f)$ are studied via Galois groups. On the other hand, we feel that any possible improvement to the bound $\alpha(f) \geq \tau(d)^{-1}$ is likely to come from studying the Galois group G.

Proof. Write $E = K(R)$. Let $G^* = \mathrm{Gal}(\overline{K}(R)/\overline{K}(t))$. Let $L = E \cap \overline{K}$ be the algebraic closure of K in E, so that $E = L(R)$ and $G^* = \mathrm{Gal}(E/L(t))$. By the primitive element theorem, there exists $\theta \in E$ such that $E = L(t, \theta)$. Suppose that θ satisfies the relation

$$h_m(t)\theta^m + \cdots + h_1(t)\theta + h_0(t) = 0,$$

where $m = [E : L(t)]$ and $h_m(t), \ldots, h_1(t), h_0(t)$ are relatively prime polynomials over L. Let $h \in L[t, y]$ be the two-variable polynomial defined by

$$h(t, y) = h_m(t)y^m + \cdots + h_1(t)y + h_0(t).$$

Clearly h is a minimal polynomial of θ, and thus h is irreducible. By the definition of L, the polynomial h is also absolutely irreducible.

Let $\mathfrak{p} \subset \mathbb{O}_K$ be a prime in K and $\mathfrak{P} \subset \mathbb{O}_L$ be a prime in L lying above $\mathfrak{p}$. By Lemma 3.5, $h_{\mathfrak{P}} \in \kappa_{\mathfrak{P}}[t, y]$ remains absolutely irreducible for all but finitely many $\mathfrak{P}$. Let $\theta_{\mathfrak{P}} \in \overline{\kappa_{\mathfrak{P}}(t)}$ be an element satisfying $h_{\mathfrak{P}}(t, \theta_{\mathfrak{P}}) = 0$, so that $E_{\mathfrak{P}} = \kappa_{\mathfrak{P}}(t, \theta_{\mathfrak{P}})$ is a degree-m field extension of $\kappa_{\mathfrak{P}}(t)$ with $E_{\mathfrak{P}} \cap \overline{\kappa_{\mathfrak{p}}} = \kappa_{\mathfrak{P}}$. Since $E/L(t)$ is Galois, all roots of $h(t, y)$ in $\overline{L(t)}$ lie in E. This implies that all roots of $h_{\mathfrak{P}}(t, y)$ in $\overline{\kappa_{\mathfrak{P}}(t)}$ lie in $E_{\mathfrak{P}}$ for all but finitely many $\mathfrak{P}$, and thus $E_{\mathfrak{P}}/\kappa_{\mathfrak{P}}(t)$ is also Galois. Note that there is a natural isomorphism $G^* = \mathrm{Gal}(E/L(t)) \cong \mathrm{Gal}(E_{\mathfrak{P}}/\kappa_{\mathfrak{P}}(t))$, since an element in either Galois group is determined by its image of θ or $\theta_{\mathfrak{P}}$.

Now we look at the polynomial $f(x) - t$. Since it factors into linear factors over E, its reduction $f_{\mathfrak{p}}(x) - t$ factors into linear factors over $E_{\mathfrak{P}}$ for all but finitely many $\mathfrak{P}$. By an abuse of notation, we will continue to write R for the set of roots of $f_{\mathfrak{p}}(x) - t$ in $\overline{\kappa_{\mathfrak{p}}(t)}$. Therefore the splitting fields $\kappa_{\mathfrak{P}}(R)$ and $\kappa_{\mathfrak{p}}(R)$ are contained in $E_{\mathfrak{P}}$. On the other hand, since $\theta \in K(R)$ and $L \subset K(R)$, we have $\theta_{\mathfrak{P}} \in \kappa_{\mathfrak{p}}(R)$ and $\kappa_{\mathfrak{P}} \subset \kappa_{\mathfrak{p}}(R)$ for all but finitely many $\mathfrak{P}$. This shows that $\kappa_{\mathfrak{p}}(R) = E_{\mathfrak{P}}$.

Let $\sigma_{\mathfrak{P}}G^*$ be the coset which is the inverse image of the Frobenius automorphism $\sigma_{\mathfrak{P}}$ under the quotient map

$$\mathrm{Gal}(E_{\mathfrak{P}}/\kappa_{\mathfrak{p}}(t)) \twoheadrightarrow \mathrm{Gal}(\kappa_{\mathfrak{P}}(t)/\kappa_{\mathfrak{p}}(t)) = \mathrm{Gal}(\kappa_{\mathfrak{P}}/\kappa_{\mathfrak{p}}),$$

which has kernel $\mathrm{Gal}(E_{\mathfrak{P}}/\kappa_{\mathfrak{P}}(t)) = G^*$. By Lemma 5.1, we have

$$\alpha_{\mathfrak{p}}(f) = \alpha(\sigma_{\mathfrak{P}}G^*) + O_d(N(\mathfrak{p})^{-1/2}).$$

Note that the quantity $\alpha(\sigma_{\mathfrak{P}}G^*)$ does not depend on the choice of $\mathfrak{P}$. Via the inclusion $\mathrm{Gal}(\kappa_{\mathfrak{P}}/\kappa_{\mathfrak{p}}) \hookrightarrow \mathrm{Gal}(L/K)$, we may view $\sigma_{\mathfrak{P}}$ as an element in $\mathrm{Gal}(L/K)$

and $\sigma_{\mathfrak{P}} G^*$ as a coset in G. By the Chebotarev density theorem, the cosets $\sigma_{\mathfrak{P}} G^*$ become equidistributed in G as $\mathfrak{p}$ varies. Therefore $\alpha(f) = \alpha(G)$ as desired. □

For a generic polynomial of degree d, the Galois group G in Proposition 6.1 is the full symmetric group S_d. Indeed, using the large sieve inequality, Gallagher [1973] obtained a precise bound on the number of exceptional polynomials (with coefficients bounded by a parameter) whose Galois group is not S_d. This bound has since been improved by Dietmann [2013]. By Proposition 6.1, this implies that

$$\alpha(f) = \alpha(S_d) = 1 - \frac{1}{2} + \frac{1}{6} - \frac{1}{24} + \cdots + \frac{(-1)^{d-1}}{d!}$$

for a typical f of degree d. Moreover, this quantity tends to $1 - e^{-1}$ as $d \to \infty$.

For $d \leq 4$, we have the following sharp lower bounds.

Proposition 6.3 (polynomials of small degree). *For a positive integer d, let α_d be the smallest possible value of $\alpha(f)$, where $f \in \mathbb{Q}[x]$ is a polynomial of degree d. Then $\alpha_2 = \frac{1}{2}$, $\alpha_3 = \frac{2}{3}$, and $\alpha_4 = \frac{3}{8}$.*

Proof. For $d = 2$ this is obvious. Suppose that $d \in \{3, 4\}$. Let G be the Galois group as in Proposition 6.1. We claim that $G \neq \mathbb{Z}/d\mathbb{Z}$, the cyclic group of order d. In fact, for $t \in \mathbb{Z}$ sufficiently large, the polynomial $f(x) = t$ has at least one real root and at least one nonreal root. Let $\alpha \in \mathbb{R}$ be a real root of $f(x) = t$. Then the splitting field of $f(x) - t$ contains properly the subfield $\mathbb{Q}(\alpha)$, and thus has degree larger than d over $\mathbb{Q}$. This shows that the Galois group of $f(x) - t$ is not $\mathbb{Z}/d\mathbb{Z}$ for all t sufficiently large. The fact that $G \neq \mathbb{Z}/d\mathbb{Z}$ then follows from Hilbert's irreducibility theorem. Now that $G \subset S_d$ is transitive and $G \neq \mathbb{Z}/d\mathbb{Z}$, the only possibilities are $G = S_3$ when $d = 3$ and $G \in \{S_4, A_4, D_4\}$ when $d = 4$. The conclusion follows by computing $\alpha(G)$ for these choices of G. □

Not surprisingly, the nature of α_d depends not only on the size of d, but also the arithmetic of d (see Proposition 5.3). In general, given a transitive subgroup $G \subset S_d$, we do not know how to tell whether G can be realized as a Galois group as in Proposition 6.1. This is reminiscent of the inverse Galois problem over $K(t)$, but here we require the polynomial to take the shape $f(x) - t$ for some $f(x) \in K[x]$. We refer the interested reader to the book [Serre 2008] and references therein for background and known results on the classical inverse Galois problem.

Acknowledgements

Thanks to Brian Conrad for help with proofs and many useful comments, to Kannan Soundararajan for helpful discussions, to Akshay Venkatesh for asking a question that led to this paper, and to the anonymous referee for helpful suggestions.

References

[Andrade et al. 2015] J. C. Andrade, L. Bary-Soroker, and Z. Rudnick, "Shifted convolution and the Titchmarsh divisor problem over $\mathbb{F}_q[t]$", *Philos. Trans. A* **373**:2040 (2015), 20140308, 18. MR 3338116

[Bank et al. 2015] E. Bank, L. Bary-Soroker, and L. Rosenzweig, "Prime polynomials in short intervals and in arithmetic progressions", *Duke Math. J.* **164**:2 (2015), 277–295. MR 3306556 Zbl 06416949

[Birch and Swinnerton-Dyer 1959] B. J. Birch and H. P. F. Swinnerton-Dyer, "Note on a problem of Chowla", *Acta Arith.* **5** (1959), 417–423. MR 22 #4675 Zbl 0091.04301

[Bombieri and Pila 1989] E. Bombieri and J. Pila, "The number of integral points on arcs and ovals", *Duke Math. J.* **59**:2 (1989), 337–357. MR 90j:11099 Zbl 0718.11048

[Cohen 1970] S. D. Cohen, "The distribution of polynomials over finite fields", *Acta Arith.* **17** (1970), 255–271. MR 43 #3234 Zbl 0209.36001

[Croot and Elsholtz 2004] E. S. Croot, III and C. Elsholtz, "On variants of the larger sieve", *Acta Math. Hungar.* **103**:3 (2004), 243–254. MR 2005c:11113 Zbl 1060.11056

[Croot and Lev 2007] E. S. Croot, III and V. F. Lev, "Open problems in additive combinatorics", pp. 207–233 in *Additive combinatorics*, CRM Proc. Lecture Notes **43**, Amer. Math. Soc., Providence, RI, 2007. MR 2009d:11038 Zbl 1183.11005

[Dietmann 2013] R. Dietmann, "Probabilistic Galois theory", *Bull. Lond. Math. Soc.* **45**:3 (2013), 453–462. MR 3065016 Zbl 06176870

[Ellenberg et al. 2009] J. S. Ellenberg, C. Elsholtz, C. Hall, and E. Kowalski, "Non-simple abelian varieties in a family: geometric and analytic approaches", *J. Lond. Math. Soc.* (2) **80**:1 (2009), 135–154. MR 2010f:11093 Zbl 1263.11064

[Elsholtz and Harper 2015] C. Elsholtz and A. J. Harper, "Additive decompositions of sets with restricted prime factors", *Trans. Amer. Math. Soc.* **367**:10 (2015), 7403–7427. MR 3378834 Zbl 06479361

[Entin 2014] A. Entin, "On the Bateman–Horn conjecture for polynomials over large finite fields", preprint, 2014. arXiv 1409.0846

[Fried 1970] M. Fried, "On a conjecture of Schur", *Michigan Math. J.* **17** (1970), 41–55. MR 41 #1688 Zbl 0169.37702

[Gallagher 1971] P. X. Gallagher, "A larger sieve", *Acta Arith.* **18** (1971), 77–81. MR 45 #214 Zbl 0231.10028

[Gallagher 1973] P. X. Gallagher, "The large sieve and probabilistic Galois theory", pp. 91–101 in *Analytic number theory* (St. Louis, MO, 1972), Proc. Sympos. Pure Math. **24**, Amer. Math. Soc., Providence, R.I., 1973. MR 48 #11020 Zbl 0279.10036

[Gomez-Calderon and Madden 1988] J. Gomez-Calderon and D. J. Madden, "Polynomials with small value set over finite fields", *J. Number Theory* **28**:2 (1988), 167–188. MR 89d:11111 Zbl 0634.12014

[Green and Harper 2014] B. Green and A. J. Harper, "Inverse questions for the large sieve", *Geom. Funct. Anal.* **24**:4 (2014), 1167–1203. MR 3248483 Zbl 1316.11085

[Guralnick and Wan 1997] R. Guralnick and D. Wan, "Bounds for fixed point free elements in a transitive group and applications to curves over finite fields", *Israel J. Math.* **101** (1997), 255–287. MR 98j:12002 Zbl 0910.11053

[Heath-Brown 2002] D. R. Heath-Brown, "The density of rational points on curves and surfaces", *Ann. of Math.* (2) **155**:2 (2002), 553–595. MR 2003d:11091 Zbl 1039.11044

[Helfgott and Venkatesh 2009] H. A. Helfgott and A. Venkatesh, "How small must ill-distributed sets be?", pp. 224–234 in *Analytic number theory*, Cambridge Univ. Press, 2009. MR 2010d:11087 Zbl 1217.11073

[Hindry and Silverman 2000] M. Hindry and J. H. Silverman, *Diophantine geometry*, Graduate Texts in Mathematics **201**, Springer, New York, 2000. MR 2001e:11058 Zbl 0948.11023

[Kowalski 2010] E. Kowalski, "Some aspects and applications of the Riemann hypothesis over finite fields", *Milan J. Math.* **78**:1 (2010), 179–220. MR 2011g:11229 Zbl 1271.11113

[Lagarias and Odlyzko 1977] J. C. Lagarias and A. M. Odlyzko, "Effective versions of the Chebotarev density theorem", pp. 409–464 in *Algebraic number fields: L-functions and Galois properties* (Durham, UK, 1975), edited by A. Fröhlich, Academic Press, London, 1977. MR 56 #5506 Zbl 0362.12011

[Lang and Weil 1954] S. Lang and A. Weil, "Number of points of varieties in finite fields", *Amer. J. Math.* **76** (1954), 819–827. MR 16,398d Zbl 0058.27202

[Montgomery 1978] H. L. Montgomery, "The analytic principle of the large sieve", *Bull. Amer. Math. Soc.* **84**:4 (1978), 547–567. MR 57 #5931 Zbl 0408.10033

[Schmidt 1976] W. M. Schmidt, *Equations over finite fields: an elementary approach*, Lecture Notes in Mathematics **536**, Springer, Berlin, 1976. MR 55 #2744 Zbl 0329.12001

[Serre 2008] J.-P. Serre, *Topics in Galois theory*, 2nd ed., Research Notes in Mathematics **1**, A K Peters, Wellesley, MA, 2008. MR 2008i:12010 Zbl 1128.12001

[Shao 2014] X. Shao, "On an inverse ternary Goldbach problem", preprint, 2014. To appear in *Amer. J. Math.* arXiv 1404.6022

[Walsh 2012] M. N. Walsh, "The inverse sieve problem in high dimensions", *Duke Math. J.* **161**:10 (2012), 2001–2022. MR 2954623 Zbl 06063227

[Walsh 2015] M. N. Walsh, "Bounded rational points on curves", *Int. Math. Res. Not.* **2015**:14 (2015), 5644–5658. MR 3384452

[Zywina 2010] D. Zywina, "Hilbert's irreducibility theorem and the larger sieve", preprint, 2010. arXiv 1011.6465

Communicated by Andrew Granville
Received 2014-12-17 Revised 2015-07-19 Accepted 2015-08-17

xuancheng.shao@maths.ox.ac.uk *Mathematical Institute, University of Oxford, Radcliffe Observatory Quarter, Woodstock Road, Oxford, OX2 6GG, United Kingdom*

ALGEBRA AND NUMBER THEORY 9:10 (2015)
dx.doi.org/10.2140/ant.2015.9.2347

msp

Bounds for Serre's open image theorem for elliptic curves over number fields

Davide Lombardo

For an elliptic curve E/K without potential complex multiplication we bound the index of the image of $\mathrm{Gal}(\overline{K}/K)$ in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, the representation being given by the action on the Tate modules of E at the various primes. The bound is explicit and only depends on $[K:\mathbb{Q}]$ and on the stable Faltings height of E. We also prove a result relating the structure of closed subgroups of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ to certain Lie algebras naturally attached to them.

1. Introduction

We are interested in studying Galois representations attached (via ℓ-adic Tate modules) to elliptic curves E defined over an arbitrary number field K and without complex multiplication, i.e., such that $\mathrm{End}_{\overline{K}}(E) = \mathbb{Z}$. Let us recall briefly the setting and fix some notation: the action of $\mathrm{Gal}(\overline{K}/K)$ on the torsion points of $E_{\overline{K}}$ gives rise to a family of representations (indexed by the rational primes ℓ)

$$\rho_\ell : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}(T_\ell(E)),$$

where $T_\ell(E)$ denotes the ℓ-adic Tate module of E. As $T_\ell(E)$ is a free module of rank 2 over $\mathbb{Z}_\ell$, it is convenient to fix bases and regard these representations as morphisms

$$\rho_\ell : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\mathbb{Z}_\ell),$$

and it is the image G_ℓ of these maps that we aim to study. It is also natural to encode all these representations in a single "adelic" map

$$\rho_\infty : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\widehat{\mathbb{Z}}),$$

whose components are the ρ_ℓ and whose image we denote G_∞. By a theorem of Serre [1972, §4, Théorème 3], G_∞ is open in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, and the purpose of the present study is to show that the adelic index $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G_\infty]$ is in fact bounded by an explicit function depending only on the stable Faltings height $h(E)$ of E and

MSC2010: primary 11G05; secondary 11F80, 14K15.
Keywords: Galois representations, elliptic curves, Lie algebras, open image theorem.

on the degree of K over $\mathbb{Q}$, generalizing and making completely explicit a result proved by Zywina [2011] in the special case $K = \mathbb{Q}$. More precisely we show:

Corollary 9.3. *Let E/K be an elliptic curve that does not admit complex multiplication. The inequality*

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_\infty(\mathrm{Gal}(\overline{K}/K))] < \gamma_1 \cdot [K : \mathbb{Q}]^{\gamma_2} \cdot \max\{1, h(E), \log[K : \mathbb{Q}]\}^{2\gamma_2}$$

holds, where $\gamma_1 = \exp(10^{21483})$ and $\gamma_2 = 2.4 \cdot 10^{10}$.

Remark 1.1. We actually prove a more precise result (Theorem 9.1), from which the present bound follows through elementary estimates. The large constants appearing in this theorem have a very strong dependence on those of Theorem 2.1; unpublished results that Éric Gaudron and Gaël Rémond have been kind enough to share with the author show that the statement can be improved to

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_\infty(\mathrm{Gal}(\overline{K}/K))] < \gamma_3 \cdot \left([K : \mathbb{Q}] \cdot \max\{1, h(E), \log[K : \mathbb{Q}]\}\right)^{\gamma_4}$$

with the much better constants $\gamma_3 = \exp(1.9 \cdot 10^{10})$ and $\gamma_4 = 12395$; see Remark 9.4.

As an easy corollary we also get:

Corollary 9.5. *Let E/K be an elliptic curve that does not admit complex multiplication. There exists a constant $\gamma(E/K)$ such that the inequality*

$$[K(x) : K] \geq \gamma(E/K) N(x)^2$$

holds for every $x \in E_{\mathrm{tors}}(\overline{K})$. Here, $N(x)$ denotes the order of x. We can take $\gamma(E/K) = (\zeta(2) \cdot [\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_\infty \mathrm{Gal}(\overline{K}/K)])^{-1}$, which can be explicitly bounded thanks to the main theorem.

Remark 1.2. This corollary (with the same proof, but with a noneffective $\gamma(E/K)$) follows directly from the aforementioned theorem of Serre [1972, §4, Théorème 3]. The exponent 2 for $N(x)$ is best possible, as is easily seen from the proof by taking $N = \ell$, a prime large enough that $G_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$.

It should also be pointed out that for a general (possibly CM) elliptic curve, Masser [1989, p. 262]) proves an inequality of the form

$$[K(x) : K] \geq \gamma'(K) h(E)^{-3/2} \frac{N(x)}{\log N(x)},$$

where $\gamma'(K)$ is an effectively computable (but nonexplicit) constant that only depends on $[K : \mathbb{Q}]$.

We briefly sketch the proof strategy, highlighting differences and similarities between our approach and that of [Zywina 2011]. By a technique due to Masser and Wüstholz (cf. [Masser and Wüstholz 1993c; 1993a] and [Masser 1998]), and which is by now standard, it is possible to give a bound on the largest prime ℓ

for which the representation modulo ℓ is not surjective; an argument of Serre then shows that (for $\ell \geq 5$) this implies full ℓ-adic surjectivity. This eliminates all the primes larger than a computable bound (actually, of all those that do not divide a quantity that can be bounded explicitly in terms of E). We then have to deal with the case of nonsurjective reduction, that is, with a finite number of "small" primes.

In [Zywina 2011] these small primes are treated using two different techniques. All but a finite number of them are dealt with by studying a family of Lie algebras attached to G_ℓ; this analysis is greatly simplified by the fact that the reduction modulo ℓ of G_ℓ is not contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$, a result depending on the hard theorem of Mazur on cyclic ℓ-isogenies. The remaining primes belong to an explicit list (again given by Mazur's results), and are treated by an application of Faltings' theorem to certain modular curves. This approach, however, has two important drawbacks. On the one hand, effective results on cyclic isogenies do not seem — at present — to be available for arbitrary number fields, so the use of Mazur's theorem is a severe obstacle in generalizing this technique to number fields larger than $\mathbb{Q}$. On the other hand, and perhaps more importantly, the use of Faltings' theorem is a major hindrance to effectivity, since making the result explicit for a given number field K would require understanding the K-points of a very large number of modular curves, a task that currently seems to be far beyond our reach.

While we do not introduce any new ideas in the treatment of the large primes, relying by and large on the methods of Masser–Wüstholz, we do put forward a different approach for the small primes that allows us to bypass both the difficulties mentioned above. With respect to [Zywina 2011], the price to pay to avoid the use of Mazur's theorem is a more involved analysis of the Lie algebras associated with subgroups of $\mathrm{GL}_2(\mathbb{Z}_\ell)$, which is done here without using a congruence filtration, but dealing instead with all the orders at the same time; this approach seems to be more natural, and proves more suitable for generalization to arbitrary number fields. We also avoid the use of Faltings' theorem entirely. This too comes at a cost, namely replacing uniform bounds with functions of the Faltings height of the elliptic curve, but it has the advantage of giving a completely explicit result, which does not depend on the (potentially very complicated) arithmetic of the K-rational points on the modular curves.

The organization of the paper reflects the steps alluded to above: in Section 2 we recall an explicit form of the isogeny theorem (as proved by Gaudron and Rémond [2014] building on the work of Masser and Wüstholz) and an idea of Masser that will help improve many of the subsequent estimates by replacing an inequality with a divisibility condition. In Sections 3 through 6 we prove the necessary results on the relation between Lie algebras and closed subgroups of $\mathrm{GL}_2(\mathbb{Z}_\ell)$; the main technical tool we use to show that the Galois image is large is the following theorem, which is proved in Sections 4 (for odd ℓ) and 5 (for $\ell = 2$):

Theorem 1.3. *Let ℓ be an odd prime (resp. $\ell = 2$). For every closed subgroup G of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ (resp. every closed subgroup whose reduction modulo 2 is trivial if $\ell = 2$) define $L(G)$ to be the $\mathbb{Z}_\ell$-span of $\{g - \frac{\mathrm{tr}(g)}{2} \cdot \mathrm{Id} \mid g \in G\}$.*

Let H be a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$. There is a closed subgroup H_1 of H, of index at most 24 (resp. with trivial reduction modulo 2 and of index at most 192 for $\ell = 2$), such that the following implication holds for all positive integers s: if $L(H_1)$ contains $\ell^s \mathfrak{sl}_2(\mathbb{Z}_\ell)$, then H_1 itself contains

$$\mathcal{B}_\ell(4s) = \left\{ g \in \mathrm{SL}_2(\mathbb{Z}_\ell) \mid g \equiv \mathrm{Id} \pmod{\ell^{4s}} \right\} \quad (\textit{resp. } \mathcal{B}_2(6s) \textit{ for } \ell = 2).$$

The methods of these sections are then applied in Section 7 to get bounds valid for *every* prime ℓ (cf. Theorem 7.5, which might have some independent interest), while Section 8 deals with the large primes through the aforementioned ideas of Masser and Wüstholz. Finally, in Section 9 we put it all together to get the adelic estimate.

2. Preliminaries on isogeny bounds

The main tool that makes all the effective estimates possible is a very explicit isogeny-type theorem taken from [Gaudron and Rémond 2014], which builds on the seminal work of Masser and Wüstholz [1993b; 1993a]. To state it we will need some notation: we let $\alpha(g) = 2^{10} g^3$ and define, for any abelian variety A/K of dimension g,

$$b([K : \mathbb{Q}], g, h(A)) = \left((14g)^{64g^2} [K : \mathbb{Q}] \max(h(A), \log[K : \mathbb{Q}], 1)^2\right)^{\alpha(g)}.$$

Theorem 2.1 [Gaudron and Rémond 2014, Théorème 1.4; cf. also the section "Cas elliptique"]. *Let K be a number field and let A, A^* be two abelian K-varieties of dimension g. If A, A^* are isogenous over K, then there exists a K-isogeny $A^* \to A$ whose degree is bounded by $b([K : \mathbb{Q}], \dim(A), h(A))$.*

If E is an elliptic curve without complex multiplication over $\overline{K}$, then the same holds with $b([K : \mathbb{Q}], \dim(A), h(A))$ replaced by

$$10^{13} [K : \mathbb{Q}]^2 \max\left(h(E), \log[K : \mathbb{Q}], 1\right)^2.$$

Remark 2.2. As the notation suggests, the three arguments of b will always be the degree of a number field K, the dimension g of an abelian variety A/K and its stable Faltings height $h(A)$.

Remark 2.3. Unpublished results of Gaudron and Rémond show that if A is the N-th power of an elliptic curve E/K and if A^* is K-isogenous to A, then a K-isogeny $A^* \to A$ exists of degree at most $10^{13N} [K : \mathbb{Q}]^{2N} \max\left(h(E), \log[K : \mathbb{Q}], 1\right)^{2N}$.

The following theorem follows easily from the arguments in Masser's paper [1998]; however, since it is never stated explicitly in the form we need, in the interest of completeness we include a short proof.

Theorem 2.4. (*Masser*) *Suppose that A/K is an abelian variety that is isomorphic over K to a product $A_1^{e_1} \times \ldots \times A_n^{e_n}$, where $A_1, \ldots, A_n$ are simple over K, mutually nonisogenous over K, and have trivial endomorphism ring over K. Let $b \in \mathbb{R}$ be a constant with the following property: for every K-abelian variety A^* isogenous to A over K, there exists an isogeny $\psi : A^* \to A$ with $\deg \psi \leq b$. Then there exists an integer $b_0 \leq b$ with the following property: for every K-abelian variety A^* isogenous to A over K, there exists an isogeny $\psi_0 : A^* \to A$ with $\deg \psi_0 \mid b_0$.*

Proof. All the references in this proof are to [Masser 1998]. We briefly recall the notation of this paper first. Let m be a positive integer and G be a $\mathrm{Gal}(\overline{K}/K)$-submodule of $A[m]$. For every K-endomorphism τ of A we denote by $\ker_m \tau$ the intersection $\ker \tau \cap A[m]$; we also define

$$f_m(G) := \min_{\tau}[\ker_m \tau : G],$$

where the minimum is taken over all τ in $\mathrm{End}_K(A)$ with $G \subseteq \ker_m \tau$. By Lemma 3.3, we have $f_m(G) \leq b$ for every positive integer m and every Galois submodule G of $A[m]$. We set $b_0 := \max_{m,G} f_m(G)$, where the maximum is taken over all positive integers m and all Galois submodules G of $A[m]$: clearly we have $b_0 \leq b$. Now if A^* is a K-abelian variety that is K-isogenous to A over K, then by Lemma 4.1 there exists a K-isogeny $\psi : A^* \to A$ such that $\deg \psi \mid b_0$, and this establishes the theorem. Notice that in order to apply Lemma 4.1, we need $i(\mathrm{End}_K(A)) = 1$ (in the notation of [Masser 1998]), which can be deduced as on page 185, proof of Theorem 2. □

We will denote by $b_0(K, A)$ the minimal b_0 with the property of the theorem; in particular $b_0(K, A) \leq b([K : \mathbb{Q}], h(A), \dim(A))$. Consider now $b_0(K', A)$ as K' ranges over the finite extensions of K of degree at most d. On one hand, $b_0(K, A)$ divides $b_0(K', A)$; on the other hand $b_0(K', A) \leq b(d[K : \mathbb{Q}], h(A), \dim(A))$ stays bounded, and therefore the number

$$b_0(K, A; d) = \operatorname*{lcm}_{[K':K] \leq d} b_0(K', A)$$

is finite. The function $b_0(K, A; d)$ is studied in [Masser 1998, Theorem D], mostly through the following elementary lemma:

Lemma 2.5 [Masser 1998, Lemma 7.1]. *Let $X, Y \geq 1$ be real numbers and $\mathcal{B}$ be a family of natural numbers. Suppose that for every positive integer t and every subset A of $\mathcal{B}$ with $|A| = t$ we have $\mathrm{lcm}(A) \leq XY^t$. The least common multiple of the elements of $\mathcal{B}$ is then finite, and does not exceed $4^{eY} X^{1+\log(C)}$, where $e = \exp(1)$.*

By adapting Masser's argument to the function $b(d[K:\mathbb{Q}], h(A), \dim(A))$ at our disposal, it is immediate to prove:

Proposition 2.6. *If A of dimension $g \geq 1$ satisfies the hypotheses of Theorem 2.4, then*

$$b_0(K, A; d) \leq 4^{\exp(1)\cdot(d(1+\log d)^2)^{\alpha(g)}} b([K:\mathbb{Q}], \dim(A), h(A))^{1+\alpha(g)(\log(d)+2\log(1+\log d))}.$$

If E is an elliptic curve without complex multiplication over $\overline{K}$, then the number $b_0(K, E; d)$ is bounded by

$$4^{\exp(1)\cdot d^2(1+\log d)^2}\left(10^{13}[K:\mathbb{Q}]^2 \max(h(E), \log[K:\mathbb{Q}], 1)^2\right)^{1+2\log d+2\log(1+\log d)}.$$

Proof. We can clearly assume $d \geq 2$. We apply the lemma to $\mathcal{B} = \{b_0(K', A)\}_{[K':K]\leq d}$. Choose t elements of $\mathcal{B}$, corresponding to extensions $K_1, \ldots, K_t$ of K, and set $L = K_1 \cdots K_t$. We claim that

$$\max\{\log(d^t[K:\mathbb{Q}]), 1\} \leq (1+\log(d))^t \max\{1, \log[K:\mathbb{Q}]\}.$$

Indeed the right hand side is clearly at least 1, so it suffices to show the inequality

$$t\log(d) + \log[K:\mathbb{Q}] \leq (1+\log(d))^t \max\{1, \log[K:\mathbb{Q}]\}.$$

As $\log(d) > 0$, we have $(1+\log(d))^t \geq 1 + t\log(d)$ by Bernoulli's inequality, and the claim follows. We thus see that $\operatorname{lcm}(b_0(K_1, A), \ldots, b_0(K_t, A))$ divides

$$\begin{aligned} b_0(L, A) &\leq b([L:\mathbb{Q}], \dim(A), h(A)) \\ &\leq b(d^t[K:\mathbb{Q}], \dim(A), h(A)) \\ &\leq \left((d(1+\log d)^2)^{\alpha(g)}\right)^t b([K:\mathbb{Q}], \dim(A), h(A)), \end{aligned}$$

so we can apply Lemma 2.5 with

$$X = b([K:\mathbb{Q}], \quad \dim(A), h(A)), \quad Y = (d(1+\log d)^2)^{\alpha(g)}$$

to get the desired conclusion. The second statement is proved in the same way using the corresponding improved bound for elliptic curves. □

Remark 2.7. We are only going to use the function $b_0(K, A; d)$ for bounded values of d (in fact, $d \leq 24$), so the essential feature of the previous proposition is to show that, under this constraint, $b_0(K, A; d)$ is bounded by a polynomial in $b([K:\mathbb{Q}], \dim(A), h(A))$.

Also notice that, if $A = E^2$ is the square of an elliptic curve E/K, then using the improved version of Theorem 2.1 mentioned in Remark 2.3 we get

$$\begin{aligned} b_0(K, E^2; d) \leq\ & 4^{\exp(1)\cdot d^4(1+\log d)^4} \cdot \\ & \cdot\left(10^{26}[K:\mathbb{Q}]^4 \max(h(E), \log[K:\mathbb{Q}], 1)^4\right)^{1+4\log d+4\log(1+\log d)}. \end{aligned}$$

We record all these facts together as a theorem for later use:

Theorem 2.8. *Suppose A/K is an abelian variety, isomorphic over K to a product of simple abelian varieties, each having trivial endomorphism ring over K. There exists a positive integer $b_0(K, A)$, not exceeding $b([K:\mathbb{Q}], \dim(A), h(A))$, with the following property: if A^* is isogenous to A over K, then there exists an isogeny $A^* \to A$, defined over K, whose degree divides $b_0(K, A)$. Furthermore, for every fixed d the function*

$$b_0(K, A; d) = \operatorname{lcm}_{[K':K]\le d} b_0(K', A)$$

exists and is bounded by a polynomial in $b([K:\mathbb{Q}], \dim(A), h(A))$.

3. Group theory for $\mathbf{GL_2}(\mathbb{Z}_\ell)$

Let ℓ be any rational prime. The subject of the following four sections is the study of certain Lie algebras associated with closed subgroups of $\mathrm{GL}_2(\mathbb{Z}_\ell)$; the construction we present is inspired by Pink's paper [1993], but we will have to extend his results in various directions: in particular, our statements apply to $\mathrm{GL}_2(\mathbb{Z}_\ell)$ (and not just to $\mathrm{SL}_2(\mathbb{Z}_\ell)$), to *any* ℓ, including 2, and to arbitrary (not necessarily pro-ℓ) subgroups. The present section contains a few necessary, although elementary, preliminaries on congruence subgroups, and introduces the relevant objects and notations.

***Congruence subgroups of* $\mathbf{SL_2}(\mathbb{Z}_\ell)$.** We aim to study the structure of the congruence subgroups of $\mathrm{SL}_2(\mathbb{Z}_\ell)$, which we denote

$$\mathcal{B}_\ell(n) = \left\{x \in \mathrm{SL}_2(\mathbb{Z}_\ell) \mid x \equiv \mathrm{Id} \pmod{\ell^n}\right\}.$$

Notation. We let v_ℓ be the standard discrete valuation of $\mathbb{Z}_\ell$ and set $v = v_\ell(2)$ (namely $v = 0$ if $\ell \neq 2$ and $v = 1$ otherwise). We also let $\binom{1/2}{k}$ denote the generalized binomial coefficient $\binom{1/2}{k} = \frac{1}{k!}\prod_{i=0}^{k-1}\left(\frac{1}{2} - i\right)$ and define $\sqrt{1+t}$ to be the formal power series $\sum_{k\ge 0}\binom{1/2}{k}t^k$.

The first piece of information we need is the following description of a generating set for $\mathcal{B}_\ell(n)$:

Lemma 3.1. *For $n \ge 1$ the group $\mathcal{B}_\ell(n)$ is generated by the elements*

$$L_a = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}, \quad R_b = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad D_c = \begin{pmatrix} 1+c & 0 \\ 0 & \frac{1}{1+c} \end{pmatrix},$$

for a, b, c ranging over $\ell^n\mathbb{Z}_\ell$.

Proof. Let $x = \left(\begin{smallmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{smallmatrix}\right)$ be an element of $\mathcal{B}_\ell(n)$. Since $x_{11} \equiv 1 \pmod{\ell}$, it is in particular a unit, so $a = -\frac{x_{21}}{x_{11}}$ has valuation $v_\ell(a) = v_\ell(x_{21}) \geq n$, i.e., $a \in \ell^n \mathbb{Z}_\ell$. Next we compute

$$L_a x = \begin{pmatrix} x_{11} & x_{12} \\ 0 & ax_{12} + x_{22} \end{pmatrix};$$

we are thus reduced to the case $x_{21} = 0$. Under this hypothesis, and by choosing $b = -\frac{x_{12}}{x_{11}}$, it is easily seen that $x R_b \in \mathcal{B}_\ell(n)$ is diagonal, and since every diagonal matrix in $\mathcal{B}_\ell(n)$ is by definition of the form D_c for some $c \in \ell^n \mathbb{Z}_\ell$, we are done. □

We will also need a description of the derived subgroup of $\mathcal{B}_\ell(n)$; in order to prove the relevant result, we first need a simpleminded lemma on valuations that will actually come in handy in many instances:

Lemma 3.2. *Let $x \in \mathbb{Z}_\ell$. We have*:

(1) *For $\ell = 2$ and $v_2(x) \geq 3$, the series $\sqrt{1+x} = \sum_{k \geq 0} \binom{1/2}{k} x^k$ converges to the only solution λ of the equation $\lambda^2 = 1 + x$ that satisfies $\lambda \equiv 1 \pmod 4$. The inequality $v_2(\sqrt{1+x} - 1) \geq v_2(x) - 1$ holds.*

(2) *For $\ell \neq 2$ and $v_\ell(x) > 0$, the series $\sqrt{1+x} = \sum_{k \geq 0} \binom{1/2}{k} x^k$ converges to the only solution λ of the equation $\lambda^2 = 1 + x$ that satisfies $\lambda \equiv 1 \pmod{\ell}$. The equality $v_\ell(\sqrt{1+x} - 1) = v_\ell(x)$ holds.*

Proof. For $\ell = 2$, we have

$$v_2\left(\binom{1/2}{k}\right) = v_2\left(\frac{(1/2)(-1/2)\dots(-(2k-3)/2)}{k!}\right) = -k - v_2(k!) \geq -2k,$$

while for any other prime,

$$v_\ell\left(\binom{1/2}{k}\right) = v_\ell\left(\prod_{i=1}^{k-1}(2i-1)\right) - v_\ell(k!) \geq -v_\ell(k!) \geq -\frac{1}{\ell - 1}k.$$

Convergence of the series is then immediate in both cases, and the identity of power series $\left(\sum_{k \geq 0} \binom{1/2}{k} t^k\right)^2 = 1 + t$ implies that, for every x such that the series converges, $\sum_{k \geq 0} \binom{1/2}{k} x^k$ is indeed a solution to the equation $\lambda^2 = 1 + x$.

Let now $\ell = 2$. Note that in the series expansion $\sqrt{1+x} - 1 = \sum_{k \geq 1} \binom{1/2}{k} x^k$ all the terms, except perhaps the first one, have valuation at least

$$(v_2(x) - 2) \cdot 2 \geq v_2(x) - 1.$$

As for the first term, it is simply $\frac{x}{2}$, so it has exact valuation $v_2(x) - 1$ and we are done; a similar argument works for $\ell \neq 2$, except now $v_\ell(x/2) = v_\ell(x)$. The congruence $\sqrt{1+x} \equiv 1 \pmod 4$ (resp. modulo ℓ) now follows. □

Lemma 3.3. *For $n \geq 1$ the derived subgroup of $\mathcal{B}_\ell(n)$ contains $\mathcal{B}_\ell(2n + 2v)$.*

Proof. Take $R_b = \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$ with $b \equiv 0 \pmod{\ell^{2n+2v}}$ and set $\beta = \ell^n$. By the above lemma, $1 + \frac{b}{\beta}$ has a square root y congruent to 1 modulo ℓ that automatically satisfies $y \equiv 1 \pmod{\ell^n}$, so

$$M = \begin{pmatrix} y & 0 \\ 0 & \frac{1}{y} \end{pmatrix} \quad \text{and} \quad N = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}$$

both belong to $\mathcal{B}_\ell(n)$. It is immediate to compute

$$MNM^{-1}N^{-1} = \begin{pmatrix} 1 & \beta(y^2-1) \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix},$$

so R_b belongs to $\mathcal{B}_\ell(n)'$. Similar identities also show that, for every $a \equiv 0 \pmod{2^{2n+2v}}$, the derived subgroup $\mathcal{B}_\ell(n)'$ contains $\left(\begin{smallmatrix} 1 & 0 \\ a & 1 \end{smallmatrix}\right) = L_a$. To finish the proof (using Lemma 3.1) we now just need to show that $\mathcal{B}_\ell(n)'$ contains D_c for every $c \equiv 0 \pmod{\ell^{2n+2v}}$. This is done through an identity similar to the above; namely, we set

$$M = \begin{pmatrix} \sqrt{1+c} & 0 \\ \frac{-c}{\beta\sqrt{1+c}} & \frac{1}{\sqrt{1+c}} \end{pmatrix} \quad \text{and} \quad N = \begin{pmatrix} 1 & \beta \\ \frac{c}{\beta} & c+1 \end{pmatrix},$$

and compute that $MNM^{-1}N^{-1} = \left(\begin{smallmatrix} 1+c & 0 \\ 0 & 1/(1+c) \end{smallmatrix}\right) = D_c$. The only thing left to check is that M and N actually belong to $\mathcal{B}_\ell(n)$, which is easily done by observing that $\sqrt{1+c} \equiv 1 \pmod{\ell^n}$ by the series expansion and that $v_\ell\left(\frac{-c}{\beta\sqrt{1+c}}\right) \geq 2n+2v-n \geq n$. □

To conclude this paragraph we describe a finite set of generators for the congruence subgroups of $\mathrm{SL}_2(\mathbb{Z}_2)$:

Lemma 3.4. *Let $a, u \in \mathbb{Z}_2$ and $L_a = \left(\begin{smallmatrix} 1 & 0 \\ a & 1 \end{smallmatrix}\right)$. Let G be a closed subgroup of $\mathrm{SL}_2(\mathbb{Z}_2)$. If $L_a \in G$, then G also contains $L_{au} = \left(\begin{smallmatrix} 1 & 0 \\ au & 1 \end{smallmatrix}\right)$. Similarly, if G contains $R_b = \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$, then it also contains R_{bu} for every $u \in \mathbb{Z}_2$. Finally, if $c \equiv 0 \pmod 4$ and G contains $D_c = \left(\begin{smallmatrix} 1+c & 0 \\ 0 & 1/(1+c) \end{smallmatrix}\right)$, then G contains D_{cu} for every $u \in \mathbb{Z}_2$.*

Let $s \geq 2$ be an integer. If $a, b, c \in 4\mathbb{Z}_2$ are such that $\max\{v_2(a), v_2(b), v_2(c)\} \leq s$, and if G contains L_a, R_b and D_c, then G contains $\mathcal{B}_2(s)$.

Proof. We show that the set W consisting of the w in $\mathbb{Z}_2$ such that L_{aw} belongs to G is a closed subgroup of $\mathbb{Z}_2$ containing 1. Indeed, $L_{aw_1}L_{aw_2} = L_{a(w_1+w_2)}$ by a direct calculation, so in particular $L_{aw}^{-1} = L_{-aw}$; furthermore $1 \in W$ by hypothesis, and if w_n is a sequence of elements of W converging to w, then $\{L_{aw_n}\} \subseteq G$ converges to L_{aw}, and since G is closed, L_{aw} itself belongs to G, so $w \in W$. It follows that W is closed and contains the integers, and since $\mathbb{Z}$ is dense in $\mathbb{Z}_2$ we get $W = \mathbb{Z}_2$ as claimed. Given that $u \mapsto R_{bu}$ is a group morphism the same proof also works

for the family R_{bu}. The situation with the family D_{cu} is slightly different in that $u \mapsto D_{cu}$ is not a group morphism; however, if $w \in \mathbb{Z}_2$, then we see that

$$(D_c)^w = \begin{pmatrix} (1+c)^w & 0 \\ 0 & \frac{1}{(1+c)^w} \end{pmatrix}$$

is well-defined and belongs to G (indeed this is trivially true for $w \in \mathbb{Z}$, and then we just need argue by continuity). As $c \equiv 0 \pmod 4$, we also have the identity $(1+c)^w = \exp(w \log(1+c))$, since all the involved power series converge: more precisely, for any γ in $4\mathbb{Z}_2$ the series $\sum_{j=1}^{\infty} (-1)^{j+1} \frac{\gamma^j}{j}$ converges and defines $\log(1+\gamma)$, and since the inequality $v_2(\gamma^j) - v_2(j) > v_2(\gamma)$ holds for every $j \geq 2$ we have $v_2(\log(1+\gamma)) = v_2(\gamma) \geq 2$. Suppose now that $v_2(\gamma) \geq v_2(c)$: then $w = \frac{\log(1+\gamma)}{\log(1+c)}$ exists in $\mathbb{Z}_2$, so we can consider $(1+c)^w = \exp(w \log(1+c)) = \exp(\log(1+\gamma)) = 1+\gamma$ and therefore for any such γ the matrix D_γ belongs to G. The last statement is now an immediate consequence of Lemma 3.1. □

Lie algebras attached to subgroups of $\mathbf{GL_2(\mathbb{Z}_\ell)}$**.** Our study of the groups G_ℓ will go through suitable integral Lie algebras, for which we introduce the following definition:

Definition 3.5. Let A be a commutative ring. A *Lie algebra over* A is a finitely presented A-module M together with a bracket $[\cdot, \cdot] : M \times M \to M$ that is A-bilinear, antisymmetric and satisfies the Jacobi identity. For any A, the module $\mathfrak{sl}_2(A) = \{M \in M_2(A) \mid \mathrm{tr}(M) = 0\}$ endowed with the usual commutator is a Lie algebra over A. The same is true for $\mathfrak{gl}_2(A)$, the set of all 2×2 matrices with coefficients in A.

We restrict our attention to the case $A = \mathbb{Z}_\ell$, and try to understand closed subgroups G of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ by means of a surrogate of the usual Lie algebra construction. In order to do so, we introduce the following definitions, inspired by those of [Pink 1993]:

Definition 3.6. Let G be a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$; if $\ell = 2$, suppose that the image of G in $\mathrm{GL}_2(\mathbb{F}_2)$ is trivial. We set

$$\begin{aligned} \Theta : \ G &\to \mathfrak{sl}_2(\mathbb{Z}_\ell) \\ g &\mapsto g - \tfrac{1}{2}\,\mathrm{tr}(g) \cdot \mathrm{Id}\,. \end{aligned}$$

Note that this definition makes sense even for $\ell = 2$, since by hypothesis the 2-adic valuation of the trace of g is at least 1.

Definition 3.7. The *special Lie algebra* of G, denoted $L(G)$ (or simply L if no confusion can arise), is the closed subgroup of $\mathfrak{sl}_2(\mathbb{Z}_\ell)$ topologically generated by $\Theta(G)$. We further define $C(G)$, or simply C, as the closed subgroup of $\mathbb{Z}_\ell$ topologically generated by all the traces $\mathrm{tr}(xy)$ for x, y in $L(G)$.

Remark 3.8. (1) $L(G)$ is indeed a Lie algebra because of the identity

$$[\Theta(x), \Theta(y)] = \Theta(xy) - \Theta(yx).$$

(2) If G is a subgroup of H, then $L(G)$ is contained in $L(H)$.

(3) C is a $\mathbb{Z}_\ell$-module. Indeed it is a $\mathbb{Z}$-module, and the action of $\mathbb{Z}$ is continuous for the ℓ-adic topology, so it extends to an action of $\mathbb{Z}_\ell$ since C is closed. Therefore C is an ideal of $\mathbb{Z}_\ell$.

The key importance of $L(G)$, at least for odd ℓ, lies in the following result:

Theorem 3.9 [Pink 1993, Theorem 3.3]. *Let ℓ be an odd prime and G be a pro-ℓ subgroup of* $\mathrm{SL}_2(\mathbb{Z}_\ell)$. *Set $L_2 = [L(G), L(G)]$ and*

$$H_2 = \{x \in \mathrm{SL}_2(\mathbb{Z}_\ell) \mid \Theta(x) \in L_2, \mathrm{tr}(x) - 2 \in C(G)\}.$$

Then H_2 is the derived subgroup of G.

On the other hand, for $\ell = 2$ the property of Θ that will be crucial for our study of L is the following approximate addition formula:

Lemma 3.10 [Pink 1993, Formula 1.3]. *The identity*

$$2(\Theta(g_1g_2)-\Theta(g_1)-\Theta(g_2)) = [\Theta(g_1), \Theta(g_2)]+(\mathrm{tr}(g_1)-2)\Theta(g_2)+(\mathrm{tr}(g_2)-2)\Theta(g_1).$$

holds for every $g_1, g_2 \in \mathrm{GL}_2(\mathbb{Z}_\ell)$ if $\ell \neq 2$, and for every $g_1, g_2 \in \{x \in \mathrm{GL}_2(\mathbb{Z}_2) \mid \mathrm{tr}(x) \equiv 0 \pmod 2\}$ if $\ell = 2$.

In what follows, we will often want to recover partial information on G from information about the reduction of G modulo various powers of ℓ. It is thus convenient to use the following notation:

Notation. We denote by $G(\ell^n)$ the image of the reduction map $G \to \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$. We also let π be the projection map $G \to G(\ell)$.

We now record a simple fact about modules over DVRs we will need later:

Lemma 3.11. *Let A be a DVR, n a positive integer, M a subset of A^n and $N = \langle M \rangle$ the submodule of A^n generated by M. Denote by π_k the projection $A^n \to A$ on the k-th component. There exist a basis $x_1, \ldots, x_m$ of N consisting of elements of M and scalars $(\sigma_{ij})_{1 \leq j < i \leq m} \subseteq A$ with the following property: if we define inductively $t_1 = x_1$ and $t_i = x_i - \sum_{j<i} \sigma_{ij} t_j$ for $i \geq 2$, then $\pi_k\big(x_i - \sum_{j<l} \sigma_{ij} t_j\big) = 0$ for every $1 \leq k < l \leq i \leq m$. The t_j are again a basis of N.*

Proof. We proceed by induction on n. The case $n = 1$ is easy: M is just a subset of A, and the claim is that the ideal generated by M can also be generated by a single element of M, which is clear. Consider now a subset M of A^{n+1}. Let ν be the discrete valuation of A; the set $\{\nu(\pi_1(x)) \mid x \in M\}$ consists of nonnegative integers, therefore it admits a minimum k_1. Take x_1 to be any element of M such

that $v(\pi_1(x_1)) = k_1$. For every element $m \in M$ we can form $f(m) = m - \frac{\pi_1(m)}{\pi_1(x_1)}x_1$, which is again an element of A^{n+1} since by definition of x_1 we have $\pi_1(x_1) \mid \pi_1(m)$. It is clear enough that $\pi_1(f(m)) = 0$ for all $m \in M$. Therefore, $f(M)$ is a subset of $\{0\} \oplus A^n$, and it is also clear that the module generated by x_1 and $f(M)$ is again N. Apply the induction hypothesis to $f(M)$ (thought of as a subset of A^n). It yields a basis $f(x_2), \dots, f(x_m)$ of $f(M)$, scalars $(\tau_{ij})_{2 \le j < i \le m}$, and a sequence $u_2 = f(x_2), u_i = f(x_i) - \sum_{2 \le j < i} \tau_{ij} u_j$, such that $\pi_k\big(f(x_i) - \sum_{2 \le j < l} \tau_{ij} u_j\big) = 0$ for $2 \le k < l \le i \le m$. We also have $\pi_1\big(f(x_i) - \sum_{2 \le j < l} \tau_{ij} u_j\big) = 0$ if we view the u_i as elements of A^{n+1}. It is now enough to show that, with this choice of the x_i, it is possible to find scalars σ_{ij} for $1 \le j < i \le m$, in such a way that $t_i = u_i$ for $i \ge 2$, and this we prove again by induction. By definition, $u_2 = f(x_2) = x_2 - \frac{\pi_1(x_2)}{\pi_1(x_1)}x_1$, so we can take $\sigma_{21} = \frac{\pi_1(x_2)}{\pi_1(x_1)}$. Assuming we have proved the result up to level i, we have

$$u_{i+1} = f(x_{i+1}) - \sum_{2 \le j < i+1} \tau_{ij} u_j = x_{i+1} - \frac{\pi_1(x_{i+1})}{\pi_1(x_1)}x_1 - \sum_{2 \le j < i+1} \tau_{ij} t_j,$$

and we simply need to take $\sigma_{i+1,1} = \frac{\pi_1(x_{i+1})}{\pi_1(x_1)}$ and $\sigma_{ij} = \tau_{ij}$.

As for the last statement, observe that the matrix giving the transformation from the x_i to the t_j is unitriangular, hence invertible. □

***Subgroups of* $\mathbf{GL_2}(\mathbb{Z}_\ell)$, $\mathbf{SL_2}(\mathbb{Z}_\ell)$, *and their reduction modulo* ℓ.** In view of the next sections, it is convenient to recall some well-known facts about the subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$, starting with the following definition:

Definition 3.12. A subgroup J of $\mathrm{GL}_2(\mathbb{F}_\ell)$ is said to be:

- *split Cartan*, if J is conjugated to the subgroup of diagonal matrices. In this case the order of J is prime to ℓ.
- *nonsplit Cartan*, if there exists a subalgebra A of $\mathrm{M}_2(\mathbb{F}_\ell)$ that is a field and such that $J = A^\times$. The order of J is prime to ℓ, and J is conjugated to $\left\{\left(\begin{smallmatrix} a & b\varepsilon \\ b & a \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_\ell)\right\}$, where ε is a fixed quadratic nonresidue.
- *the normalizer of a split (resp. nonsplit) Cartan*, if there exists a split (resp. nonsplit) Cartan subgroup $\mathcal{C}$ such that J is the normalizer of $\mathcal{C}$. The index $[J : \mathcal{C}]$ is 2, and ℓ does not divide the order of J (unless $\ell = 2$).
- *Borel*, if J is conjugated to the subgroup of upper-triangular matrices. In this case J has a unique ℓ-Sylow, consisting of the matrices of the form $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$.
- *exceptional*, if the projective image $\mathbb{P}J$ of J in $\mathrm{PGL}_2(\mathbb{F}_\ell)$ is isomorphic to either A_4, S_4 or A_5, in which case the order of $\mathbb{P}J$ is either 12, 24 or 60.

The above classes essentially exhaust all the subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$. More precisely, we have:

Theorem 3.13 (Dickson's classification, cf. [Serre 1972]). *Let ℓ be a prime number and J be a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$. Then we have*:

- *if ℓ divides the order of J, then either J contains $\mathrm{SL}_2(\mathbb{F}_\ell)$ or it is contained in a Borel subgroup*;
- *if ℓ does not divide the order of J, then J is contained in a (split or nonsplit) Cartan subgroup, in the normalizer of one, or in an exceptional group.*

As subgroups of $\mathrm{SL}_2(\mathbb{F}_\ell)$ are in particular subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$, the above classification also covers all subgroups of $\mathrm{SL}_2(\mathbb{F}_\ell)$. Cartan subgroups of $\mathrm{SL}_2(\mathbb{F}_\ell)$ are cyclic (both in the split and nonsplit case).

The next lemma can be proved by direct inspection of the group structure of A_4, S_4 and A_5, and will help us quantify how far exceptional subgroups are from being abelian:

Lemma 3.14. *The groups A_4 and S_4 have abelian subgroups of order N if and only if $1 \le N \le 4$. The group A_5 has abelian subgroups of order N if and only if $1 \le N \le 5$.*

The following lemma, due to Serre, will prove extremely useful in showing that $G_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$ using only information about the reduction of G_ℓ modulo ℓ:

Lemma 3.15. *Let $\ell \ge 5$ be a prime and G be a closed subgroup of $\mathrm{SL}_2(\mathbb{Z}_\ell)$. If the image of G in $\mathrm{SL}_2(\mathbb{F}_\ell)$ is equal to $\mathrm{SL}_2(\mathbb{F}_\ell)$, then $G = \mathrm{SL}_2(\mathbb{Z}_\ell)$. Similarly, if H is a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ whose image in $\mathrm{GL}_2(\mathbb{F}_\ell)$ contains $\mathrm{SL}_2(\mathbb{F}_\ell)$, then $H' = \mathrm{SL}_2(\mathbb{Z}_\ell)$.*

Proof. The first statement is [Serre 1998, IV-23, Lemma 3]. For the second, consider the closed subgroup H' of $\mathrm{SL}_2(\mathbb{Z}_\ell)$. Since by assumption we have $\ell > 3$, the finite group $\mathrm{SL}_2(\mathbb{F}_\ell)$ is perfect, so the image of H' in $\mathrm{SL}_2(\mathbb{F}_\ell)$ contains $\mathrm{SL}_2(\mathbb{F}_\ell)' = \mathrm{SL}_2(\mathbb{F}_\ell)$. It then follows from the first part of the lemma that $H' = \mathrm{SL}_2(\mathbb{Z}_\ell)$, as claimed. □

The following definition will prove useful to translate statements about subgroups of $\mathrm{SL}_2(\mathbb{Z}_\ell)$ into analogous results for subgroups of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ and vice versa:

Definition 3.16. Let G be a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ (resp. $\mathrm{GL}_2(\mathbb{F}_\ell)$). The *saturation* of G, denoted $\mathrm{Sat}(G)$, is the group generated in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ (resp. $\mathrm{GL}_2(\mathbb{F}_\ell)$) by G and $\mathbb{Z}_\ell^\times \cdot \mathrm{Id}$ (resp. $\mathbb{F}_\ell^\times \cdot \mathrm{Id}$). The group G is said to be *saturated* if $G = \mathrm{Sat}(G)$. We also denote by $G^{\det=1}$ the group $G \cap \mathrm{SL}_2(\mathbb{Z}_\ell)$ (resp. $G \cap \mathrm{SL}_2(\mathbb{F}_\ell)$).

Lemma 3.17. (1) *For every closed subgroup G of $\mathrm{GL}_2(\mathbb{Z}_\ell)$, the groups G and $\mathrm{Sat}(G)$ have the same derived subgroup and the same special Lie algebra.*

(2) *The two associations $G \mapsto G^{\det=1}$ and $H \mapsto \mathrm{Sat}(H)$ are mutually inverse bijections between the sets*

$$\mathcal{G} = \left\{ \textit{subgroups } G \textit{ of } \mathrm{GL}_2(\mathbb{Z}_\ell) \;\middle|\; \begin{array}{c} G \textit{ is saturated}, \\ \det(g) \textit{ is a square for every } g \textit{ in } G \end{array} \right\}$$

and

$$\mathcal{H} = \big\{\textit{subgroups } H \textit{ of } \mathrm{SL}_2(\mathbb{Z}_\ell) \mid -\mathrm{Id} \in H\big\}.$$

For every G in $\mathcal{G}$, the groups G and $G^{\det=1}$ have the same derived subgroup and the same special Lie algebra.

(3) *The map $G \mapsto \mathrm{Sat}(G)$ commutes with reducing modulo ℓ, i.e.,*

$$(\mathrm{Sat}(G))(\ell) = \mathrm{Sat}(G(\ell)).$$

If ℓ is odd and G is saturated, we also have $G(\ell)^{\det=1} = G^{\det=1}(\ell)$.

Proof. (1) The statement is obvious for the derived subgroup. As for the special Lie algebra, let λg be any element of $\mathrm{Sat}(G)$, where $\lambda \in \mathbb{Z}_\ell^\times$ and $g \in G$. As $L(G)$ is a $\mathbb{Z}_\ell$-module, $\Theta(\lambda g) = \lambda\Theta(g)$ belongs to $L(G)$, hence $L(\mathrm{Sat}(G)) \subseteq L(G)$. The other inclusion is trivial.

(2) The first statement is immediate to check since the determinant of any homothety is a square; the other follows by writing $G = \mathrm{Sat}(H)$ and applying (1) to $(\mathrm{Sat}(H))^{\det=1} = H$ and $\mathrm{Sat}(H)$.

(3) This is clear for the saturation. For $G \mapsto G^{\det=1}$, note that $G(\ell)^{\det=1}$ contains $G^{\det=1}(\ell)$, so we need to show the opposite inclusion. Take any matrix $[g]$ in $G(\ell)^{\det=1}$. By definition, $[g]$ is the reduction of a certain $g \in G$ whose determinant is 1 modulo ℓ. As ℓ is odd and $\det(g)$ is congruent to 1 modulo ℓ, we can apply Lemma 3.2 and write $\det(g) = \lambda^2$, where $\lambda = \sqrt{1 + (\det(g) - 1)}$ is congruent to 1 modulo ℓ. As G is saturated, it contains $\lambda^{-1}\,\mathrm{Id}$, hence also $\lambda^{-1}g$, whose determinant is 1 by construction. Furthermore, as $\lambda \equiv 1 \pmod{\ell}$, the two matrices $\lambda^{-1}g$ and g are congruent modulo ℓ. We have thus found an element of G of determinant 1 that maps to $[g]$, so $G^{\det=1} \to G(\ell)^{\det=1}$ is surjective. □

Finally, since we will be mainly concerned with the pro-ℓ part of our groups, we will find it useful to give this object a name:

Notation. If G is a closed subgroup of $\mathrm{SL}_2(\mathbb{Z}_\ell)$, we write $N(G)$ for its maximal normal subgroup that is a pro-ℓ group.

The following lemma shows that $N(G)$ is well-defined and describes it:

Lemma 3.18. *Let G be a closed subgroup of $\mathrm{SL}_2(\mathbb{Z}_\ell)$ and $\pi : G \to G(\ell)$ the projection modulo ℓ. Then G admits a unique maximal normal pro-ℓ subgroup $N(G)$, which can be described as follows.*

(1) *If $G(\ell)$ is of order prime to ℓ, then $N(G) = \ker\pi$ and $G(\ell) \cong \frac{G}{N(G)}$.*

(2) *If the order of $G(\ell)$ is divisible by ℓ, and if $G(\ell)$ is contained in a Borel subgroup, then $N(G)$ is the inverse image in G of the unique ℓ-Sylow S of $G(\ell)$.*

(3) *If $G(\ell)$ is all of $\mathrm{SL}_2(\mathbb{F}_\ell)$, then $N(G) = \ker\pi$ and $G(\ell) \cong \frac{G}{N(G)}$.*

Proof. Let N be a pro-ℓ normal subgroup of G. The image $\pi(N)$ is a normal pro-ℓ subgroup of $G(\ell)$, hence it is trivial in cases (1) and (3) and it is either trivial or the unique ℓ-Sylow of $G(\ell)$ in case (2). In cases (1) and (3) it follows that $N \subseteq \ker \pi$, and since $\ker \pi$ is pro-ℓ we see that $\ker \pi$ is the unique maximal normal pro-ℓ subgroup of G. In case (2), let S be the unique ℓ-Sylow of $G(\ell)$. It is clear that N is contained in $\pi^{-1}(S)$, which on the other hand is pro-ℓ and normal in G. Indeed, by choosing an appropriate (triangular) basis for $G(\ell)$ we can define a map $G \to G(\ell) \to \mathbb{F}_\ell^\times$ with kernel $\pi^{-1}(S)$ via

$$g \mapsto \begin{pmatrix} a & b \\ 0 & 1/a \end{pmatrix} \mapsto a. \qquad \square$$

4. Recovering G from $L(G)$, when ℓ is odd

Our purpose in this section (for $\ell \neq 2$) and the next (for $\ell = 2$) is to prove results that yield information on G from analogous information on $L(G)$.

Theorem 4.1. *Let ℓ be an odd prime and G a closed subgroup of $\mathrm{SL}_2(\mathbb{Z}_\ell)$.*

(i) *Suppose that $G(\ell)$ is contained in a Cartan or Borel subgroup, and that $|G/N(G)| \neq 4$. Then the following implication holds for all positive integers s:*
($\star$) *if $L(G)$ contains $\ell^s \mathfrak{sl}_2(\mathbb{Z}_\ell)$, then $L(N(G))$ contains $\ell^{2s}\mathfrak{sl}_2(\mathbb{Z}_\ell)$.*

(ii) *Without any assumption on G, there is a closed subgroup H of G that satisfies $[G : H] \leq 12$ and the conditions in (i) (so H has property ($\star$)).*

Theorem 4.2. *Let ℓ be an odd prime, and G a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$.*

(i) *Suppose that G satisfies the two conditions:*
(a) $\det(g)$ *is a square in $\mathbb{Z}_\ell^\times$ for every $g \in G$;*
(b) $\mathrm{Sat}(G)^{\det=1}$ *satisfies the hypotheses of Theorem 4.1(i).*
Then the following implication holds for all positive integers s:
($\star\star$) *if $L(G)$ contains $\ell^s \mathfrak{sl}_2(\mathbb{Z}_\ell)$, then G' contains $\mathcal{B}_\ell(4s)$.*

(ii) *Without any assumption on G, either $G' = \mathrm{SL}_2(\mathbb{Z}_\ell)$ or there is a closed subgroup H of G that satisfies both $[G : H] \leq 24$ and the conditions in (i) (so H has property ($\star\star$)).*

Remark 4.3. Condition (b) can be made more explicit using the description of the maximal normal pro-ℓ subgroup given in Lemma 3.18. The conditions on G can be translated into conditions on $(\mathrm{Sat}(G))^{\det=1}(\ell)$: this group should be cyclic or have order divisible by ℓ and be contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$. In the first case we require $|(\mathrm{Sat}(G))^{\det=1}(\ell)| \neq 4$; in the second case we need $|\mathrm{Sat}(G)^{\det=1}(\ell)/S| \neq 4$, where S is the unique ℓ-Sylow of $\mathrm{Sat}(G)^{\det=1}(\ell)$. With this description, it is clear that condition (b) is true if $\mathrm{Sat}(G)^{\det=1}(\ell)$ is contained in a Borel or Cartan subgroup and has order not divisible by 4.

Let us remark that the statements numbered (ii) in the above theorems require a case by case analysis, which will be carried out on pages 2370–2372 for Theorem 4.2 (the proof of Theorem 4.1(ii) is perfectly analogous). In this proof we will also show that part (i) of Theorem 4.2 can be reduced to the corresponding statement in Theorem 4.1, so the core of the problem lies in proving the result for $\mathrm{SL}_2(\mathbb{Z}_\ell)$. Before delving into the details of the proof (that involves a certain amount of calculations) we describe the general idea, which is on the contrary quite simple. The following paragraph should only be considered as outlining the main ideas, without any pretense of formality.

If G is as in Theorem 4.1(i), then $G/N(G)$ is cyclic, and we can fix a generator $[g] \in G/N(G)$ that lifts to a certain $g \in G$. The operator $\varphi : x \mapsto g^{-1}xg$ acts on G, and, since it fixes Id, also on $L(G)$. Furthermore, it preserves $L(N(G)) \subseteq L(G)$ by normality of $N(G)$ in G, and obviously it fixes $\Theta(g)$. If we were working over $\mathbb{Q}_\ell$ instead of $\mathbb{Z}_\ell$, we would have a decomposition $L(G) \cong \langle \Theta(g) \rangle \oplus M$, where M is a φ-stable subspace of dimension 2, and the projection operator $p : L(G) \to M$ could be expressed as a polynomial in φ. We would also expect M to consist of elements coming from $N(G)$, because $\langle \Theta(g) \rangle$ is simply the special Lie algebra of $\langle g \rangle$; this would provide us with many nontrivial elements in $L(N(G))$. We would finally deduce the equality $L(N(G)) = \mathfrak{sl}_2(\mathbb{Q}_\ell)$ by exploiting the fact that $L(N(G))$ is a Lie algebra of dimension at least 2 that is also stable under φ. This point of view also suggests that we cannot expect the theorem to hold when $G(\ell)$ is exceptional: if $G/N(G)$ is a simple group, then we expect the special Lie algebra of G not to be solvable, and since the only nonsolvable subalgebra of $\mathfrak{sl}_2(\mathbb{Q}_\ell)$ is $\mathfrak{sl}_2(\mathbb{Q}_\ell)$ itself, $L(G)$ should be very large even if $N(G)$ is very small.

In what follows we prove (i) of Theorem 4.1 first when $|G/N(G)| = 2$ and then in case $G(\ell)$ is respectively contained in a split Cartan, Borel, or nonsplit Cartan subgroup; we then discuss the optimality of the statement, showing through examples that it cannot be extended to the exceptional case and that ℓ^{2s} cannot be replaced by anything smaller. Finally, on pages 2370–2372 we finish the proof of Theorem 4.2.

Notation. For $x \in L(G)$, we set $\pi_{ij}(x) = x_{ij}$, the coefficient in the i-th row and j-th column of the matrix representation of x in $\mathfrak{sl}_2(\mathbb{Z}_\ell)$. The maps π_{ij} are obviously linear and continuous.

The case $|G/N(G)| = 2$. Suppose first that $G(\ell)$ is contained in a Cartan subgroup, so that $G/N(G) \cong G(\ell)$. The only nontrivial element x in $G(\ell)$ satisfies the relations $x^2 = \mathrm{Id}$ and $\det(x) = 1$, so it must be $-\mathrm{Id}$. It follows that G contains an element g of the form $-\mathrm{Id} + \ell A$ for a certain $A \in \mathrm{M}_2(\mathbb{Z}_\ell)$. Considering the sequence

$$g^{\ell^n} = (-\mathrm{Id} + \ell A)^{\ell^n} = -\mathrm{Id} + O(\ell^{n+1}),$$

and given that G is closed, we see that $-\mathrm{Id}$ is in G. Next observe that for every $h \in G$, either h or $-h$ belongs to $N(G)$. If g_1, g_2, g_3 are elements of G such that $\Theta(g_1), \Theta(g_2), \Theta(g_3)$ is a basis for $L(G)$, then on the one hand for each i either g_i or $-g_i$ belongs to $N(G)$, and on the other hand $\Theta(-g_i) = -\Theta(g_i)$, so $L(G) = L(N(G))$ and the claim follows.

Next suppose $G(\ell)$ is contained in a Borel subgroup. We can assume that the order of $G(\ell)$ is divisible by ℓ, for otherwise $G(\ell)$ is cyclic and we are back in the previous case. The canonical projection $G \to G/N(G)$ factors as

$$\begin{array}{ccccc} G & \to & G(\ell) & \to & \mathbb{F}_\ell^\times \\ g & \mapsto & \begin{pmatrix} a & b \\ 0 & 1/a \end{pmatrix} & \mapsto & a, \end{array}$$

so if $G/N(G)$ has order 2, $G(\ell)$ contains an element of the form $\left(\begin{smallmatrix} -1 & b \\ 0 & -1 \end{smallmatrix}\right)$. Taking the ℓ-th power of this element shows that $G(\ell)$ contains $-\mathrm{Id}$ and we conclude as above.

The split Cartan case. Suppose that $G(\ell)$ is contained in a split Cartan, so that, by choosing a suitable basis, we can assume that $G(\ell)$ is contained in the subgroup of diagonal matrices of $\mathrm{SL}_2(\mathbb{F}_\ell)$. Fix an element $g \in G$ such that $[g] \in G(\ell)$ is a generator. By assumption, the order of $[g]$ is not 4, and by the previous paragraph we can assume it is not 2; furthermore it is not divisible by ℓ. The minimal polynomial of $[g]$ is then separable, and $[g]$ has two distinct eigenvalues in $\mathbb{F}_\ell^\times$. It follows that g can be diagonalized over $\mathbb{Z}_\ell$ (its characteristic polynomial splits by Hensel's lemma), and there is a basis in which $g = \left(\begin{smallmatrix} a & 0 \\ 0 & 1/a \end{smallmatrix}\right)$, where a is an ℓ-adic unit. Note that our assumption $|G(\ell)| \nmid 4$ implies in particular that $a^4 \not\equiv 1 \pmod{\ell}$. A fortiori ℓ does not divide $a^2 - 1$, so the diagonal coefficients of $\Theta(g) = \left(\begin{smallmatrix} a^2-1/(2a) & 0 \\ 0 & -(a^2-1/)(2a) \end{smallmatrix}\right)$ are ℓ-adic units. The following lemma allows us to choose a basis of $L(G)$ containing $\Theta(g)$:

Lemma 4.4. *Suppose $g \in G$ is such that $\Theta(g)$ is not zero modulo ℓ. The algebra $L(G)$ admits a basis of the form $\Theta(g), \Theta(g_2), \Theta(g_3)$, where g_2, g_3 are in G.*

Proof. Recall that $L(G)$ is of rank 3 since it contains $\ell^s \mathfrak{sl}_2(\mathbb{Z}_\ell)$. Start by choosing $g_1, g_2, g_3 \in G$ such that $\Theta(g_1), \Theta(g_2), \Theta(g_3)$ is a basis for $L(G)$. As $\Theta(g)$ is not zero modulo ℓ, from an equality of the form

$$\Theta(g) = \sum_{i=1}^{3} \lambda_i \Theta(g_i)$$

we deduce that at least one of the λ_i is an ℓ-adic unit, and we can assume without loss of generality that it is λ_1. But then

$$\Theta(g_1) = \lambda_1^{-1}(\Theta(g) - \lambda_2\Theta(g_2) - \lambda_3\Theta(g_3)),$$

and we can replace g_1 with g. □

Recall that we denote by φ the endomorphism of $\mathfrak{sl}_2(\mathbb{Z}_\ell)$ given by $x \mapsto g^{-1}xg$. We now prove that $L(N(G))$ is φ-stable and, more generally, describe the φ-stable subalgebras of $\mathfrak{sl}_2(\mathbb{Z}_\ell)$.

Lemma 4.5. *Let ℓ be an odd prime, G a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$, N a normal closed subgroup of G and g an element of G. The special Lie algebra $L(N)$ is stable under φ.*

Proof. As $\Theta(N)$ generates $L(N)$, it is enough to prove that φ stabilizes $\Theta(N)$. Let $x = \Theta(n)$ for a certain $n \in N$: then

$$g^{-1}xg = g^{-1}(n - \tfrac{\mathrm{tr}(n)}{2}\,\mathrm{Id})g = g^{-1}ng - \tfrac{\mathrm{tr}(g^{-1}ng)}{2}\,\mathrm{Id} = \Theta(g^{-1}ng),$$

and this last element is in $\Theta(N)$ since N is normal in G. □

Lemma 4.6. *Let s be a nonnegative integer. Let L be a φ-stable Lie subalgebra of $\mathfrak{sl}_2(\mathbb{Z}_\ell)$ and x_{11}, x_{12}, x_{21}, y_{11}, y_{12}, y_{21} be elements of $\mathbb{Z}_\ell$ with $v_\ell(x_{21}) \le s$ and $v_\ell(y_{12}) \le s$. If L contains both $l_1 = \left(\begin{smallmatrix} x_{11} & x_{12} \\ x_{21} & -x_{11} \end{smallmatrix}\right)$ and $l_2 = \left(\begin{smallmatrix} y_{11} & y_{12} \\ y_{21} & -y_{11} \end{smallmatrix}\right)$, then it contains all of $\ell^{2s}\mathfrak{sl}_2(\mathbb{Z}_\ell)$.*

Proof. Consider first the case $x_{12} = y_{21} = 0$. We compute

$$\varphi(l_1) = \begin{pmatrix} x_{11} & 0 \\ a^2 x_{21} & -x_{11} \end{pmatrix},$$

so L contains $\left(\begin{smallmatrix} x_{11} & 0 \\ a^2x_{21} & -x_{11} \end{smallmatrix}\right) - l_1 = \left(\begin{smallmatrix} 0 & 0 \\ (a^2-1)x_{21} & 0 \end{smallmatrix}\right)$, where by our hypothesis on a the valuation of the bottom left coefficient is at most s. Analogously, L contains $\left(\begin{smallmatrix} 0 & (a^2-1)y_{12} \\ 0 & 0 \end{smallmatrix}\right)$, and since it is a Lie algebra, it also contains the commutator

$$\left[\begin{pmatrix} 0 & (a^2-1)y_{12} \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ (a^2-1)x_{21} & 0 \end{pmatrix}\right] = \begin{pmatrix} (a^2-1)^2 x_{21}y_{12} & 0 \\ 0 & -(a^2-1)^2 x_{21}y_{12} \end{pmatrix},$$

whose diagonal coefficients have valuation at most $2s$. This establishes the lemma in case x_{12} and y_{21} are both zero, since the three elements we have found generate $\ell^{2s}\mathfrak{sl}_2(\mathbb{Z}_\ell)$. The general case is then reduced to the previous one by replacing l_1, l_2 by

$$a^2\varphi(l_1) - l_1 = \begin{pmatrix} (a^2-1)x_{11} & 0 \\ (a^4-1)x_{21} & -(a^2-1)x_{11} \end{pmatrix}$$

and $a^{-2}\varphi(l_2) - l_2$, and noticing that since $\ell \nmid a^4 - 1$ we have $v_\ell((a^4-1)x_{21}) = v_\ell(x_{21})$ and $v_\ell((a^{-4}-1)y_{12}) = v_\ell(y_{12})$). □

We know from Lemma 4.5 that $L(N(G))$ is φ-stable, so in order to apply Lemma 4.6 to $L(N(G))$ we just need to find two elements l_1, l_2 in $L(N(G))$ with the property that $v_\ell \circ \pi_{21}(l_1) \le s$ and $v_\ell \circ \pi_{12}(l_2) \le s$. Since the values of the diagonal coefficients do not matter for the application of this lemma we will simply

write $*$ for any diagonal coefficient appearing from now on. In particular we write $g_2, g_3, \Theta(g_2), \Theta(g_3)$ in coordinates as follows:

$$g_i = \begin{pmatrix} * & g_{12}^{(i)} \\ g_{21}^{(i)} & * \end{pmatrix}, \quad \Theta(g_i) = \begin{pmatrix} * & g_{12}^{(i)} \\ g_{21}^{(i)} & * \end{pmatrix}.$$

As $[g]$ generates $G(\ell)$, for $i = 2, 3$ there exist $k_i \in \mathbb{N}$ such that $[g_i] = [g]^{k_i}$, or equivalently such that $g^{-k_i} g_i \in N(G)$. Since $\Theta(g), \Theta(g_2), \Theta(g_3)$ generate $\ell^s \mathfrak{sl}_2(\mathbb{Z}_\ell)$, but the off-diagonal coefficients of $\Theta(g)$ vanish, we can choose two indices $i_1, i_2 \in \{2, 3\}$ such that $v_\ell \circ \pi_{21}(\Theta(g_{i_1})) \leq s$ and $v_\ell \circ \pi_{12}(\Theta(g_{i_2})) \leq s$. On the other hand, $L(N(G))$ contains

$$\Theta(g^{-k_i} g_i) = \Theta\left(\begin{pmatrix} a^{-k_i} & 0 \\ 0 & a^{k_i} \end{pmatrix}\begin{pmatrix} * & g_{12}^{(i)} \\ g_{21}^{(i)} & * \end{pmatrix}\right) = \begin{pmatrix} * & a^{-k_i} g_{12}^{(i)} \\ a^{k_i} g_{21}^{(i)} & * \end{pmatrix},$$

where $a^{\pm k_i}$ is an ℓ-adic unit. The ℓ-adic valuation of the off-diagonal coefficients of $\Theta(g^{-k_i} g_i)$ is then the same as that of the corresponding coefficients of $\Theta(g_i)$, and we find two elements $l_1 = \Theta(g^{-k_{i_1}} g_{i_1})$ and $l_2 = \Theta(g^{-k_{i_2}} g_{i_2})$ that satisfy $v_\ell \circ \pi_{21}(l_1) \leq s$ and $v_\ell \circ \pi_{12}(l_2) \leq s$, as required. We can now apply Lemma 4.6 with $(L, g, l_1, l_2) = (L(N(G)), g, \Theta(g_{i_1}), \Theta(g_{i_2}))$ and deduce that $L(N(G))$ contains $\ell^{2s} \mathfrak{sl}_2(\mathbb{Z}_\ell)$, as claimed.

The Borel case. Suppose $G(\ell)$ is included in a Borel subgroup. If the order of $G(\ell)$ is prime to ℓ, then $G(\ell)$ is in fact contained in a split Cartan subgroup, and we are reduced to the previous case. We can therefore assume without loss of generality that the order of $G(\ell)$ is divisible by ℓ. In this case, we know that $N(G)$ is the inverse image in G of the unique ℓ-Sylow of $G(\ell)$, and that the canonical projection $G \to G/N(G)$ factors as

$$\begin{array}{ccccc} G & \to & G(\ell) & \to & \mathbb{F}_\ell^\times \\ g & \mapsto & \begin{pmatrix} a & b \\ 0 & 1/a \end{pmatrix} & \mapsto & a. \end{array}$$

Let H be the image of this map. The group H is cyclic and we can assume that its order does not divide 4: it is not 4 by hypothesis and if it is 1 or 2, we are done. Let g be any inverse image in G of a generator of H. The matrix representing g can be diagonalized over $\mathbb{Z}_\ell$ since the characteristic polynomial of $[g] \in G(\ell)$ is separable, and the same exact argument as in the previous paragraph shows that we can choose a basis of $L(G)$ of the form $\Theta(g), \Theta(g_2), \Theta(g_3)$. By definition of H, we see that for $i = 2, 3$, there is an integer k_i such that $[g_i] = [g]^{k_i}$ in $G/N(G)$, and the rest of the proof is identical to that of the previous paragraph.

The nonsplit Cartan case. Suppose now that $G(\ell)$ is contained in a nonsplit Cartan subgroup. Fix a $g \in G$ such that $[g]$ generates $G(\ell)$. We know that $[g]$ is of the

form $\left(\begin{smallmatrix}[a] & [b\varepsilon]\\ [b] & [a]\end{smallmatrix}\right)$, where $[\varepsilon]$ is a fixed quadratic nonresidue modulo ℓ. In order to put g into a standard form we need the following elementary lemma, which is an ℓ-adic analogue of the Jordan canonical form over the reals.

Lemma 4.7. *Up to a choice of basis of $\mathbb{Z}_\ell^2$, the matrix representing g can be chosen to be of the form $\left(\begin{smallmatrix}a & b\varepsilon\\ b & a\end{smallmatrix}\right)$ for certain a, b, ε lifting $[a], [b], [\varepsilon]$, and where moreover a, b are ℓ-adic units.*

Proof. The characteristic polynomial of $[g]$ splits over $\mathbb{F}_\ell[\sqrt{[\varepsilon]}]$, so by Hensel's lemma the characteristic polynomial of g splits over $\mathbb{Z}_\ell[\sqrt{\varepsilon}]$. The two eigenvalues of g in $\mathbb{Z}_\ell[\sqrt{\varepsilon}]$ are of the form $a \pm b\sqrt{\varepsilon}$ for certain $a, b \in \mathbb{Z}_\ell$ (the notation is coherent: since the eigenvalues of $[g]$ are simply the projections of the eigenvalues of g, the elements a, b map to $[a], [b]$ modulo ℓ, respectively).

By the definition of eigenvalue, we can find a vector $\mathbf{v}_+ \in \mathbb{Z}_\ell[\sqrt{\varepsilon}]^2$ such that $g\mathbf{v}_+ = (a + b\sqrt{\varepsilon})\mathbf{v}_+$. Normalize $\mathbf{v}_+$ in such a way that at least one of its coordinates is an ℓ-adic unit, write $\mathbf{v}_+ = \mathbf{w} + \mathbf{z}\sqrt{\varepsilon}$ for certain $\mathbf{w}, \mathbf{z} \in \mathbb{Z}_\ell^2$, and set $\mathbf{v}_- = \mathbf{w} - \mathbf{z}\sqrt{\varepsilon}$. As g has its coefficients in $\mathbb{Z}_\ell$, the vector $\mathbf{v}_-$ is an eigenvector for g, associated with the eigenvalue $a - b\sqrt{\varepsilon}$. The projections of $\mathbf{v}_\pm$ in $\left(\mathbb{F}_\ell[\sqrt{[\varepsilon]}]\right)^2$ are therefore nonzero eigenvectors of $[g]$ corresponding to different eigenvalues, hence they are linearly independent. It follows that $\mathbf{w} = \frac{\mathbf{v}_+ + \mathbf{v}_-}{2}$, $\mathbf{z} = \frac{\mathbf{v}_+ - \mathbf{v}_-}{2\sqrt{\varepsilon}}$ are independent modulo $\ell\mathbb{Z}_\ell[\sqrt{\varepsilon}]$, and since $\mathbf{w}, \mathbf{z}$ lie in $\mathbb{Z}_\ell^2$ they are a fortiori independent modulo ℓ. The matrix $(\mathbf{z} \mid \mathbf{w})$ is then invertible modulo ℓ, so it lies in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ and can be used as base-change matrix. It is now straightforward to check that in this basis the element g is represented by the matrix $\left(\begin{smallmatrix}a & b\varepsilon\\ b & a\end{smallmatrix}\right)$. Finally notice that a and b are units: if $[b] = 0$ or $[a] = 0$, it is easy to check that the order of $G(\ell)$ divides 4, contradicting the assumptions. □

We can also assume that G contains $-\mathrm{Id}$, since replacing G with $G \cdot \{\pm \mathrm{Id}\}$ alters neither the derived subgroup nor the special Lie algebra of G. By Lemma 4.4, the algebra $L(G)$ admits a basis of the form $\Theta(g)$, $\Theta(g_2)$, $\Theta(g_3)$, where g is as above and g_2, g_3 are in G. We write in coordinates

$$g_2 = \begin{pmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{pmatrix}, \quad \Theta(g_2) = \begin{pmatrix} \frac{y_{11}-y_{22}}{2} & y_{12} \\ y_{21} & -\frac{y_{11}-y_{22}}{2} \end{pmatrix},$$

$$g_3 = \begin{pmatrix} z_{11} & z_{12} \\ z_{21} & z_{22} \end{pmatrix}, \quad \Theta(g_3) = \begin{pmatrix} \frac{z_{11}-z_{22}}{2} & z_{12} \\ z_{21} & -\frac{z_{11}-z_{22}}{2} \end{pmatrix}.$$

Projection operators, φ-stable subalgebras. Recall that φ denotes $x \mapsto g^{-1}xg$. Following our general strategy, we now describe projection operators associated with the action of φ and φ-stable subalgebras of $\mathfrak{sl}_2(\mathbb{Z}_\ell)$.

Lemma 4.8. *Let $E, F \in \mathbb{Z}_\ell$. If the matrix $\left(\begin{smallmatrix} -F & -\varepsilon E \\ E & F \end{smallmatrix}\right)$ belongs to $L(N(G))$, then $L(N(G))$ also contains*

$$\begin{pmatrix} -F & 0 \\ 0 & F \end{pmatrix}, \quad \begin{pmatrix} -E & 0 \\ 0 & E \end{pmatrix}, \quad \begin{pmatrix} 0 & -\varepsilon E \\ E & 0 \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} 0 & -\varepsilon F \\ F & 0 \end{pmatrix}.$$

Proof. We know from Lemma 4.5 that $L(N(G))$ is φ-stable, so the identity

$$\frac{1}{2ab}\left(\varphi\begin{pmatrix} -F & -\varepsilon E \\ E & F \end{pmatrix} - (a^2 + b^2\varepsilon)\begin{pmatrix} -F & -\varepsilon E \\ E & F \end{pmatrix}\right) = \begin{pmatrix} -\varepsilon E & -\varepsilon F \\ F & \varepsilon E \end{pmatrix} \quad (4\text{-}1)$$

shows that $\left(\begin{smallmatrix} -\varepsilon E & -\varepsilon F \\ F & \varepsilon E \end{smallmatrix}\right)$ is in $L(N(G))$. At least one of F/E and E/F is an ℓ-adic integer, and we can assume it is F/E (the other case being perfectly analogous). In particular we have $v_\ell(F) \geq v_\ell(E)$. It follows that $L(N(G))$ contains

$$\frac{F}{E}\begin{pmatrix} -F & -\varepsilon E \\ E & F \end{pmatrix} - \begin{pmatrix} -\varepsilon E & -\varepsilon F \\ F & \varepsilon E \end{pmatrix} = \begin{pmatrix} \frac{\varepsilon E^2 - F^2}{E} & 0 \\ 0 & -\frac{\varepsilon E^2 - F^2}{E} \end{pmatrix}.$$

If $v_\ell(F) > v_\ell(E)$, we have $v_\ell(\varepsilon E^2 - F^2) = 2v_\ell(E)$, while if $v_\ell(F) = v_\ell(E)$ we can write

$$F = \ell^{v_\ell(E)}\zeta, \quad E = \ell^{v_\ell(E)}\gamma,$$

where ζ, γ are not zero modulo ℓ. In this second case we have $\varepsilon E^2 - F^2 = \ell^{2v_\ell(E)}(\varepsilon\gamma^2 - \zeta^2)$, and $(\varepsilon\gamma^2 - \zeta^2)$ does not vanish modulo ℓ since $[\varepsilon]$ is not a square in $\mathbb{F}_\ell^\times$. Hence $v_\ell(\varepsilon E^2 - F^2) = 2v_\ell(E)$ holds in any case, and (due to the denominator E) we have found in $L(N(G))$ a matrix whose off-diagonal coefficients vanish and whose diagonal coefficients have the same valuation as E. By the stability of $L(N(G))$ under multiplication by ℓ-adic units we have thus proved that $L(N(G))$ contains $\left(\begin{smallmatrix} -E & 0 \\ 0 & E \end{smallmatrix}\right)$. Identity (4-1) applied to this element shows that $L(N(G))$ also contains $\left(\begin{smallmatrix} 0 & -\varepsilon E \\ E & 0 \end{smallmatrix}\right)$. Since $\left(\begin{smallmatrix} -F & -\varepsilon E \\ -E & F \end{smallmatrix}\right)$ is in $L(N(G))$ by assumption, taking the difference of these two matrices shows that $\left(\begin{smallmatrix} -F & 0 \\ 0 & F \end{smallmatrix}\right)$ is in $L(N(G))$ as well. Applying Equation (4-1) to this last matrix we finally deduce that $L(N(G))$ also contains $\left(\begin{smallmatrix} 0 & -\varepsilon F \\ F & 0 \end{smallmatrix}\right)$. □

Lemma 4.9. *Let E, F be elements of $\mathbb{Z}_\ell$ satisfying $\min\{v_\ell(F), v_\ell(E)\} \leq s$. If $\left(\begin{smallmatrix} -F & -\varepsilon E \\ E & F \end{smallmatrix}\right)$ belongs to $L(N(G))$, then $L(N(G))$ contains $\ell^{2s}\mathfrak{sl}_2(\mathbb{Z}_\ell)$.*

Proof. Suppose $v_\ell(F) \leq s$, the other case being similar. The special Lie algebra $L(N(G))$ contains $\left(\begin{smallmatrix} -F & 0 \\ 0 & F \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & -\varepsilon F \\ F & 0 \end{smallmatrix}\right)$ by the previous lemma, so (given that $v_\ell(F) \leq s$) it also contains $\ell^s\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, $\ell^s\left(\begin{smallmatrix} 0 & -\varepsilon \\ 1 & 0 \end{smallmatrix}\right)$. Taking the commutator of these two elements yields another element of $L(N(G))$, namely

$$\left[\ell^s\begin{pmatrix} 0 & -\varepsilon \\ 1 & 0 \end{pmatrix}, \ell^s\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right] = \ell^{2s}\begin{pmatrix} 0 & 2\varepsilon \\ 2 & 0 \end{pmatrix}.$$

Finally, since

$$\frac{1}{2}\ell^{2s}\begin{pmatrix}0 & 2\varepsilon\\ 2 & 0\end{pmatrix}+\ell^{2s}\begin{pmatrix}0 & -\varepsilon\\ 1 & 0\end{pmatrix}=\ell^{2s}\begin{pmatrix}0 & 0\\ 2 & 0\end{pmatrix},$$

it is immediately checked that $L(N(G))$ contains a basis of $\ell^{2s}\mathfrak{sl}_2(\mathbb{Z}_\ell)$, as desired. □

The case $g_2, g_3 \notin N(G)$. Let us assume for now that $g_i \notin N(G)$ and $-g_i \notin N(G)$ for $i = 2, 3$. We will deal later with the case when some of these elements already belong to $N(G)$. Given that by hypothesis $L(G)$ contains $\ell^s\mathfrak{sl}_2(\mathbb{Z}_\ell)$, we must have a representation

$$\ell^s\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}=\sum_{i=1}^{3}\lambda_i\Theta(g_i)$$

for certain scalars $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{Z}_\ell$. However, since the diagonal coefficients of $\Theta(g)$ vanish, there exists an index $i \in \{2, 3\}$ such that $v_\ell \circ \pi_{11}(\Theta(g_i)) \le s$. Renumbering g_2, g_3 if necessary, we can assume $i = 2$. In coordinates, the condition $v_\ell \circ \pi_{11}(\Theta(g_2)) \le s$ becomes $v_\ell(y_{11} - y_{22}) \le s$.

Now, since $[g]$ generates $G(\ell)$, there is an integer k such that $[g]^{-k} = [g_2]$ in $G(\ell)$; in other words, both g_2g^k and g^kg_2 are trivial modulo ℓ and therefore belong to $N(G)$. It is immediate to check that the matrix g^k is of the form $\left(\begin{smallmatrix}c & d\varepsilon\\ d & c\end{smallmatrix}\right)$ for certain $c, d \in \mathbb{Z}_\ell$. Now if d is 0 modulo ℓ, then (since $c^2 - \varepsilon d^2 \equiv 1 \pmod{\ell}$) we have $c \equiv \pm 1 \pmod{\ell}$, so either g_2 or $-g_2$ reduces to the identity modulo ℓ and is therefore in $N(G)$, contradicting our assumption. Hence d is an ℓ-adic unit. We then introduce

$$g_4 = \begin{pmatrix}c & d\varepsilon\\ d & c\end{pmatrix}\begin{pmatrix}y_{11} & y_{12}\\ y_{21} & y_{22}\end{pmatrix},\quad g_5 = \begin{pmatrix}y_{11} & y_{12}\\ y_{21} & y_{22}\end{pmatrix}\begin{pmatrix}c & d\varepsilon\\ d & c\end{pmatrix}.$$

By construction, g_4 and g_5 are elements of $N(G)$, whence $\Theta(g_4), \Theta(g_5)$ are elements of $L(N(G))$. In particular, $L(N(G))$ contains their difference

$$\Theta(g_4) - \Theta(g_5) = g_4 - g_5 = \begin{pmatrix}-d(y_{12} - \varepsilon y_{21}) & d\varepsilon(-y_{11} + y_{22})\\ d(y_{11} - y_{22}) & d(y_{12} - \varepsilon y_{21})\end{pmatrix},$$

where $v_\ell \circ \pi_{21}(\Theta(g_4) - \Theta(g_5)) \le s$ and $v_\ell \circ \pi_{12}(\Theta(g_4) - \Theta(g_5)) \le s$, because d, ε are ℓ-adic units. Applying Lemma 4.9 to the element $\Theta(g_4) - \Theta(g_5)$ we have just constructed we therefore deduce $L(N(G)) \supseteq \ell^{2s}\mathfrak{sl}_2(\mathbb{Z}_\ell)$, as desired.

The case when one generator belongs to $N(G)$. Let $x = \left(\begin{smallmatrix}x_{11} & x_{12}\\ x_{21} & -x_{11}\end{smallmatrix}\right)$ denote any element of $\mathfrak{sl}_2(\mathbb{Z}_\ell)$. It is easy to check that

$$\frac{1}{2ab}\big((3 + 4\varepsilon b^2)(\varphi x - x) - \varphi(\varphi x - x)\big) = \begin{pmatrix}x_{12} - \varepsilon x_{21} & 2\varepsilon x_{11}\\ -2x_{11} & -x_{12} + \varepsilon x_{21}\end{pmatrix},$$

and, furthermore, if x belongs to $L(N(G))$, then $\left(\begin{smallmatrix}x_{12}-\varepsilon x_{21} & 2\varepsilon x_{11}\\ -2x_{11} & -x_{12}+\varepsilon x_{21}\end{smallmatrix}\right)$ is in $L(N(G))$ as well.

Suppose now that either g_2 or $-g_2$ (resp. g_3 or $-g_3$) belongs to $N(G)$. Since $\Theta(-g_i) = -\Theta(g_i)$, we can assume that g_2 (resp. g_3) itself belongs to $N(G)$. Take $\left(\begin{smallmatrix} x_{11} & x_{12} \\ x_{21} & -x_{11} \end{smallmatrix}\right)$ to be $\Theta(g_2)$ (resp. $\Theta(g_3)$). Subtracting $\frac{x_{21}}{b}\Theta(g_1)$ from $\Theta(g_2)$ we get $\left(\begin{smallmatrix} x_{11} & x_{12}-\varepsilon x_{21} \\ 0 & -x_{11} \end{smallmatrix}\right) \in L(G)$, and since we know that

$$\Theta(g_2) - \tfrac{\pi_{21}(\Theta(g_2))}{b}\Theta(g_1) \quad \text{and} \quad \Theta(g_3) - \tfrac{\pi_{21}(\Theta(g_3))}{b}\Theta(g_1)$$

together span $\ell^s\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \oplus \ell^s\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$, we see that at least one of the coefficients of the matrix $\Theta(g_2) - \frac{\pi_{21}(\Theta(g_2))}{b}\Theta(g_1) = \Theta(g_2) - \frac{x_{21}}{b}\Theta(g_1)$ must have valuation at most s, that is $\min\{v_\ell(x_{11}), v_\ell(x_{12} - \varepsilon x_{21})\} \leq s$. We now apply Lemma 4.9 to $\left(\begin{smallmatrix} x_{12}-\varepsilon x_{21} & 2\varepsilon x_{11} \\ -2x_{11} & -x_{12}+\varepsilon x_{21} \end{smallmatrix}\right)$, which is in $L(N(G))$, to deduce $L(N(G)) \supseteq \ell^{2s}\mathfrak{sl}_2(\mathbb{Z}_\ell)$, and we are done.

Optimality. The following examples show that it is neither possible to extend Theorem 4.2 to the exceptional case, nor to improve the exponent $2s$.

Proposition 4.10. *Let ℓ be a prime $\equiv 1 \pmod 4$. For every $t \geq 1$, there exists a closed subgroup G of $\mathrm{SL}_2(\mathbb{Z}_\ell)$ whose special Lie algebra is $\mathfrak{sl}_2(\mathbb{Z}_\ell)$ and whose maximal pro-ℓ subgroup is contained in $\mathcal{B}_\ell(t)$.*

Proof. Notice that the following six elements form a finite subgroup H of $\mathrm{PSL}_2(\mathbb{Z}[i])$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad \begin{pmatrix} -i & i \\ 0 & i \end{pmatrix}, \quad \begin{pmatrix} i & 0 \\ i & -i \end{pmatrix},$$

and that H is isomorphic to S_3: indeed, it is the group of permutations of $\{0, 1, \infty\} \subset \mathbb{P}^1(\mathbb{Z}[i])$. The inverse image $\tilde{H}$ of H in $\mathrm{SL}_2(\mathbb{Z}[i])$ is therefore a finite group of cardinality 12. Now since $\ell \equiv 1 \pmod 4$ there is a square root of -1 in $\mathbb{Z}_\ell$, so $\mathbb{Z}[i] \hookrightarrow \mathbb{Z}_\ell$ and $\tilde{H} \hookrightarrow \mathrm{SL}_2(\mathbb{Z}_\ell)$. Consider $G = \tilde{H} \cdot \mathcal{B}_\ell(t) \subset \mathrm{SL}_2(\mathbb{Z}_\ell)$. It is clear that $\mathcal{B}_\ell(t)$ is normal in G. Since $\frac{G}{\mathcal{B}_\ell(t)}$ is isomorphic to a quotient of $\tilde{H}$ (and therefore has order prime to ℓ), the subgroup $\mathcal{B}_\ell(t)$ is clearly the maximal pro-ℓ subgroup of G. Furthermore, the special Lie algebra of G contains the three elements

$$\Theta\left(\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}\right) = \begin{pmatrix} -1/2 & 1 \\ -1 & 1/2 \end{pmatrix}, \ \Theta\left(\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}\right) = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \ \Theta\left(\begin{pmatrix} i & 0 \\ i & -i \end{pmatrix}\right) = \begin{pmatrix} i & 0 \\ i & -i \end{pmatrix},$$

that are readily checked to be a basis of $\mathfrak{sl}_2(\mathbb{Z}_\ell)$. □

On the other hand, the following example shows that there exist subgroups of $\mathrm{SL}_2(\mathbb{Z}_\ell)$ such that $L(G)$ contains $\ell^s\mathfrak{sl}_2(\mathbb{Z}_\ell)$, but $L(N(G))$ only contains $\ell^{2s}\mathfrak{sl}_2(\mathbb{Z}_\ell)$. Fix $s \geq 1$, an integer $N > 4$ and a prime ℓ congruent to 1 modulo N; then $\mathbb{Z}_\ell^\times$ contains a primitive N-th root of unity a, and we let $g = \left(\begin{smallmatrix} a & 0 \\ 0 & 1/a \end{smallmatrix}\right)$. The module $M = \ell^s\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) \oplus \ell^s\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right) \oplus \ell^{2s}\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ is a Lie subalgebra of $\mathfrak{sl}_2(\mathbb{Z}_\ell)$, so by Theorem 3.4 of [Pink 1993]

$$H = \left\{x \in \mathrm{SL}_2(\mathbb{Z}_\ell) \mid \mathrm{tr}(x) \equiv 2 \pmod{\ell^{2s}}, \Theta(x) \in M\right\}$$

is a pro-ℓ group with special Lie algebra M. Let G be the group generated by g and H. Up to units, $\Theta(g)$ equals $\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$, so $L(G)$ contains all of $\ell^s\mathfrak{sl}_2(\mathbb{Z}_\ell)$. On the other hand, H is normal in G: one simply needs to check that $g^{-1}Mg = M$, and this is obvious from the equality

$$g^{-1}\begin{pmatrix} x_{11} & x_{12}\\ x_{21} & -x_{11}\end{pmatrix}g = \begin{pmatrix} x_{11} & \frac{x_{12}}{a^2}\\ a^2x_{21} & -x_{11}\end{pmatrix}.$$

Finally, H is maximal among the pro-ℓ subgroups of G, since G/H is a quotient of $\langle g\rangle \cong \mathbb{Z}/N\mathbb{Z}$, hence of order prime to ℓ. Therefore $N(G) = H$ and $L(N(G)) = L(H) = M$ contains $\ell^t\mathfrak{sl}_2(\mathbb{Z}_\ell)$ only for $t \geq 2s$.

Proof of Theorem 4.2. We now prove (i) of Theorem 4.2 by reducing it to the corresponding statement in Theorem 4.1.

As G and $\mathrm{Sat}(G)$ have the same special Lie algebra and derived subgroup, we can assume $G = \mathrm{Sat}(G)$. As G is saturated and satisfies the condition on the determinant, we know from Lemma 3.17 that $G = \mathrm{Sat}(H)$ for $H = G^{\det=1}$. By the same lemma, we also have $L(H) = L(G)$ and $G' = H'$.

By assumption, H satisfies the hypotheses of Theorem 4.1(i), so H has property $(\star)$. As $L(G) = L(H)$ contains $\ell^s\mathfrak{sl}_2(\mathbb{Z}_\ell)$, we deduce that $L_0 = L(N(H))$ contains $\ell^{2s}\mathfrak{sl}_2(\mathbb{Z}_\ell)$, and since $N(H)$ is a pro-ℓ group we can apply Theorem 3.9 to it. In order to do so, we need to estimate $C(N(H)) = \mathrm{tr}(L_0 \cdot L_0)$ and $[L_0, L_0]$. Note that

$$C(N(H)) \ni \mathrm{tr}\left(\ell^{2s}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\cdot \ell^{2s}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\right) = 2\ell^{4s},$$

so given that ℓ is odd we have $C(L_0) \supseteq (2\ell^{4s}) = (\ell^{4s})$. Likewise,

$$[L_0, L_0] \supseteq [\ell^{2s}\mathfrak{sl}_2(\mathbb{Z}_\ell), \ell^{2s}\mathfrak{sl}_2(\mathbb{Z}_\ell)] = \ell^{4s}\mathfrak{sl}_2(\mathbb{Z}_\ell),$$

so the derived subgroup of $N(H)$ (which is clearly included in $H' = G'$) is

$$N(H)' = \left\{x \in \mathrm{SL}_2(\mathbb{Z}_\ell) \mid \mathrm{tr}\, x - 2 \in C(N(H)), \Theta(x) \in [L_0, L_0]\right\},$$

and by the above it contains

$$\left\{x \in \mathrm{SL}_2(\mathbb{Z}_\ell) \mid \mathrm{tr}\, x \equiv 2 \pmod{\ell^{4s}}, \Theta(x) \equiv 0 \pmod{\ell^{4s}}\right\} \supseteq \mathcal{B}_\ell(4s),$$

which concludes the proof of (i).

We are now left with the task of proving (ii). Consider first the map

$$G \xrightarrow{\det} \mathbb{Z}_\ell^\times \to \frac{\mathbb{Z}_\ell^\times}{\mathbb{Z}_\ell^{\times 2}} \cong \frac{\mathbb{Z}}{2\mathbb{Z}}$$

and let G_1 be its kernel. Then $[G : G_1] \leq 2$, so we can replace G by G_1 and assume that the condition on the determinant is satisfied. We are reduced to showing that,

under this hypothesis, either $G' = \mathrm{SL}_2(\mathbb{Z}_\ell)$ or there exists a subgroup H of index at most 12 that satisfies the right conditions on $\mathrm{Sat}(H)^{\det=1}$. For notational simplicity, we let π denote the projection map $G \to G(\ell)$. We now distinguish cases according to ℓ and $G(\ell)$ (cf. Theorem 3.13):

(-) if $\ell \geq 5$ and $G(\ell)$ contains $\mathrm{SL}_2(\mathbb{F}_\ell)$, then it follows from Lemma 3.15 that $G' = \mathrm{SL}_2(\mathbb{Z}_\ell)$.

(-) if $\ell = 3$, we let S denote either a 3-Sylow of $G(3)$ if the order of $G(3)$ is a multiple of 3, or the trivial group $\{\mathrm{Id}\}$ if it is not. Notice that $G(3)$ is a subgroup of $\{g \in \mathrm{GL}_2(\mathbb{F}_3) \mid \det(g) \text{ is a square}\}$, which has order 24, so the index $[G(3) : S]$ is at most 8. We set $H = \pi^{-1}(S)$. It is clear that $[G : H] \leq 8$, and H satisfies the conditions in (i) by Remark 4.3, because $(\mathrm{Sat}\, H)^{\det=1}(3)$ is either $\{\pm \mathrm{Id}\}$ or a group of order 6.

(-) if $G(\ell)$ is exceptional, then by Lemma 3.14 there exists a cyclic subgroup B of $\mathbb{P}G(\ell)$ with $[\mathbb{P}G(\ell) : B] \leq 12$: such a B can be taken to have order 3 (resp. 5) if $\mathbb{P}G(\ell)$ is isomorphic to A_4 or S_4 (resp. to A_5). Fix a generator $[b]$ of B and let ξ be the composition $G \to G(\ell) \to \mathbb{P}G(\ell)$. We set $H := \xi^{-1}(B)$; it is clear that $[G : H] \leq 12$. Let now $b \in G(\ell)$ be an element that maps to $[b]$ in B, and let m be the (odd) order of $[b]$. We know that $\det b$ is a square in $\mathbb{F}_\ell^\times$, hence there exists a $\lambda \in \mathbb{F}_\ell^\times$ such that $\det(\lambda b) = 1$. Notice now that $(\lambda b)^m$ is a homothety (it projects to the trivial element in $\mathbb{P}G(\ell)$) and has determinant 1, so it is either Id or $-\mathrm{Id}$; replacing λ by $-\lambda$ if necessary, we can assume that $(\lambda b)^m = -\mathrm{Id}$. By construction, every element in $(\mathrm{Sat}(H)^{\det=1})(\ell) = \mathrm{Sat}(H(\ell))^{\det=1}$ can be written as $\pm(\lambda b)^n$ for some $n \in \mathbb{N}$ and for some choice of sign. Now using the fact that $(\lambda b)^m = -\mathrm{Id}$, we see that $(\mathrm{Sat}(H)^{\det=1})(\ell)$ is cyclic, generated by λb: since the order of λb is either 6 or 10, H satisfies the conditions in (i) by Remark 4.3.

(-) if $G(\ell)$ is contained in a (split or nonsplit) Cartan subgroup, then the same is true for the group $(\mathrm{Sat}(G)^{\det=1})(\ell)$. If $(\mathrm{Sat}(G)^{\det=1})(\ell)$ does not have order 4, we are done, so suppose it does. Then $\mathbb{P}G(\ell)$ has at most 4 elements, and we can take

$$H = \ker(G \to G(\ell) \to \mathbb{P}G(\ell)).$$

This H has index at most 4 in G, and $H(\ell)$ has trivial image in $\mathbb{P}\mathrm{GL}_2(\mathbb{F}_\ell)$, so $H(\ell)$ is contained in the homotheties subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$. Therefore $(\mathrm{Sat}(H))^{\det=1}(\ell) = \mathrm{Sat}(H(\ell))^{\det=1} = \{\pm \mathrm{Id}\}$ and H satisfies the conditions in (i).

(-) if $G(\ell)$ is contained in the normalizer of a (split or nonsplit) Cartan subgroup $\mathcal{C}$, but not in $\mathcal{C}$ itself, then G has a subgroup G_1 of index 2 whose image modulo ℓ is contained in $\mathcal{C}$, and we are reduced to the Cartan case.

(-) if $G(\ell)$ is contained in a Borel subgroup, then the same is true for $\mathrm{Sat}(G)^{\det=1}(\ell)$. To ease the notation, we set $G_2 = \mathrm{Sat}(G)^{\det=1}$. We can also assume that ℓ divides the order of $G(\ell)$ (hence that of $G_2(\ell)$ as well), for otherwise we are back to the (split) Cartan case. Now if $|G_2/N(G_2)| \neq 4$ we can set $H = G$; if, on the contrary, $|G_2/N(G_2)| = 4$ we consider the group morphism

$$\begin{array}{rccccc} \tau: & G & \to & G(\ell) & \to & \mathbb{F}_\ell^\times \\ & g & \mapsto & [g] = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} & \mapsto & a/c. \end{array}$$

Every $g \in G$ is of the form λg_2 for suitable $\lambda \in \mathbb{Z}_\ell^\times$ and $g_2 \in G_2$, and since $\tau(\lambda g_2) = \tau(g_2)$, we deduce $\tau(G) = \tau(G_2)$. On the other hand, when restricted to G_2 the function τ becomes

$$g \mapsto [g] = \begin{pmatrix} a & b \\ 0 & 1/a \end{pmatrix} \mapsto a^2,$$

and as we have already remarked $g \mapsto [g] = \left(\begin{smallmatrix} a & b \\ 0 & 1/a \end{smallmatrix}\right) \mapsto a$ is the quotient map $G_2 \twoheadrightarrow G_2/N(G_2)$. Hence τ factors through the quotient $G_2/N(G_2)$ and we have $|\tau(G)| = (|\tau(G_2)|)\,|\,4$. We take H to be the kernel of τ. Then it is clear that $[G : H]$ divides 4, and we claim that H satisfies the conditions in (i). To check this last claim, notice first that $H(\ell)$ is a subgroup of $G(\ell)$, so it is contained in a Borel subgroup. We also have $\ker\pi \subseteq H$, so $G/H \cong \frac{G/\ker\pi}{H/\ker\pi} = \frac{G(\ell)}{H(\ell)}$; in particular $[G(\ell) : H(\ell)]$ divides 4, and therefore the order of $H(\ell)$ is divisible by ℓ. Finally, any matrix $\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)$ in $H(\ell)$ satisfies $a/c = 1$ by construction, so the intersection $\mathrm{Sat}(H(\ell)) \cap \mathrm{SL}_2(\mathbb{F}_\ell)$ consists of matrices $\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)$ with $a = c$ and $ac = 1$; hence $a = c = \pm 1$. This implies that the quotient of $\mathrm{Sat}(H)^{\det=1}(\ell)$ by its ℓ-Sylow has at most 2 elements, and since this quotient is exactly $\mathrm{Sat}(H)^{\det=1}/N(\mathrm{Sat}(H)^{\det=1})$, the result follows. □

Remark 4.11. For future applications, we remark that the same proof shows that the inequality $[G : H] \leq 24$ appearing in Theorem 4.2(ii) can be replaced by the condition $[G : H] \mid 48$, and even by $[G : H] \mid 24$ if in addition G satisfies $\det(G) \subseteq \mathbb{Z}_\ell^{\times 2}$.

5. Recovering G from $L(G)$, when $\ell = 2$

We now consider closed subgroups of $\mathrm{GL}_2(\mathbb{Z}_2)$, and endeavor to show results akin to those of the previous section. For $\mathrm{GL}_2(\mathbb{Z}_2)$, the statement is as follows:

Theorem 5.1. *Let G be a closed subgroup of* $\mathrm{GL}_2(\mathbb{Z}_2)$.

(1) *Suppose that $G(4)$ is trivial and* $\det(G) \equiv 1 \pmod 8$. *The following implication holds for all positive integers n: if $L(G)$ contains $2^n\mathfrak{sl}_2(\mathbb{Z}_2)$, then the derived subgroup G' of G contains the principal congruence subgroup $\mathcal{B}_2(12n+2)$.*

(2) *Without any assumption on G, the subgroup*

$$H = \ker(G \to G(4)) \cap \ker\big(G \to G(8) \xrightarrow{\det} (\mathbb{Z}/8\mathbb{Z})^\times\big)$$

satisfies $[G : H] \leq 2 \cdot 96 = 192$ and the conditions in (i).

Note that (ii) is immediate: the order of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ is 96, and once we demand that $G(4)$ is trivial, the determinant modulo 8 can only take two different values. As in the previous section, the core of the problem lies in understanding the subgroups of $\mathrm{SL}_2(\mathbb{Z}_2)$, so until the very last paragraph of this section the letter G will denote a closed subgroup of $\mathrm{SL}_2(\mathbb{Z}_2)$. In view of the result we want to prove, we will also enforce the assumption that G has trivial reduction modulo 4; indeed in this context the relevant statement is:

Theorem 5.2. *Let G be a closed subgroup of $\mathrm{SL}_2(\mathbb{Z}_2)$ whose reduction modulo 4 is trivial, and let s be an integer no less than 2. If $L(G)$ contains $2^s\mathfrak{sl}_2(\mathbb{Z}_2)$, then G contains $\mathcal{B}_2(6s)$.*

The idea of the proof is quite simple: despite the fact there is in general no reason why $\Theta(G)$ should be a group under addition, we will show that for every pair x, y of elements of $\Theta(G)$ it is possible to find an element that is reasonably close to $x + y$ and that lies again in $\Theta(G)$. The error term will turn out to be quadratic in x and y, which is not quite good enough by itself, since a correction of this order of magnitude could still be large enough to destroy any useful information about $x + y$; the technical step needed to make the argument work is that of multiplying all the elements we have to deal with by a power of 2 large enough so that the quadratic error term becomes negligible with respect to the linear part. The rest of the proof is really just careful bookkeeping of the correction terms appearing in the various addition formulas. We shall continue using the notation from the previous section:

Notation. For $x \in L := L(G)$, we set $\pi_{ij}(x) = x_{ij}$, the coefficient in the i-th row and j-th column of the matrix representation of x in $\mathfrak{sl}_2(\mathbb{Z}_2)$. The maps π_{ij} are linear and continuous.

We start with a compactness lemma. Our arguments only yield (arbitrarily good) approximations of elements of $\Theta(G)$, and we need to know that this is enough to show that the matrices we are approximating actually belong to $\Theta(G)$.

Lemma 5.3. *Let G be a closed subgroup of $\mathrm{SL}_2(\mathbb{Z}_\ell)$, g an element of G, and $e \geq 2$. Suppose that $\Theta(g) \equiv 0 \pmod{2^e}$. Then $\mathrm{tr}(g) - 2$ is divisible by 2^{2e}. Moreover, $\Theta^{-1} : \Theta(G) \cap 2^2\mathfrak{sl}_2(\mathbb{Z}_2) \to G$ is well-defined and continuous, and the intersection $\Theta(G) \cap 2^2\mathfrak{sl}_2(\mathbb{Z}_2)$ is compact.*

Proof. Write $\Theta(g) = \left(\begin{smallmatrix} a & b \\ c & -a \end{smallmatrix}\right)$ and $g = \frac{\mathrm{tr}(g)}{2}\,\mathrm{Id} + \Theta(g)$. As G is a subgroup of $\mathrm{SL}_2(\mathbb{Z}_2)$, we have the identity

$$1 = \det g = \det\left(\tfrac{\mathrm{tr}(g)}{2}\,\mathrm{Id} + \Theta(g)\right) = \left(\tfrac{\mathrm{tr}(g)}{2}\right)^2 - a^2 - bc.$$

Furthermore, G (hence g) is trivial modulo 4 by assumption, so an immediate calculation shows that $1 = \det(g) \equiv 1 + (\mathrm{tr}(g) - 2) \pmod 8$. It follows that $\frac{\mathrm{tr}(g)}{2}$ is the unique solution to the equation $\lambda^2 = 1 + a^2 + bc$ that is congruent to 1 modulo 4, hence $\frac{\mathrm{tr}(g)}{2} = \sqrt{1 + a^2 + bc} = \sum_{j=0}^{\infty} \binom{1/2}{j} (a^2 + bc)^j$ by Lemma 3.2. Given that $a^2 + bc \equiv 0 \pmod{2^{2e}}$ and $2e > 3$, using again Lemma 3.2 we find

$$v_2(\mathrm{tr}(g) - 2) = v_2\left(2\left(\tfrac{\mathrm{tr}(g)}{2} - 1\right)\right) = 1 + v_2\left(\sqrt{1 + (a^2 + bc)} - 1\right) \geq 2e.$$

The case $e = 2$ of the above computation shows that every $x \in 2^2\mathfrak{sl}_2(\mathbb{Z}_2)$ admits exactly one inverse image in $\mathrm{SL}_2(\mathbb{Z}_2)$ that reduces to the identity modulo 4, so $\Theta : \mathcal{B}_2(2) \to 2^2\mathfrak{sl}_2(\mathbb{Z}_2)$ is a continuous bijection: we have just described the (two-sided) inverse, so we only need to check that the image of $\mathcal{B}_2(2)$ under Θ does indeed land in $2^2\mathfrak{sl}_2(\mathbb{Z}_2)$. We have to show that if $g = \left(\begin{smallmatrix} d & b \\ c & e \end{smallmatrix}\right)$ is any element of $\mathcal{B}_2(2)$, then $\Theta(g) = \left(\begin{smallmatrix} (d-e)/2 & b \\ c & (e-d)/2 \end{smallmatrix}\right)$ has all its coefficients divisible by 4. This is obvious for b and c. For the diagonal ones, note that $de - bc = 1$, so $de \equiv 1 \pmod 8$ and hence $d \equiv e \pmod 8$ and $\frac{d-e}{2} \equiv 0 \pmod 4$ as required. Observe now that $a^2 + bc = \frac{1}{2}\,\mathrm{tr}(\Theta(g)^2)$, so we can write

$$\Theta^{-1}(x) = x + \sqrt{1 + \tfrac{1}{2}\,\mathrm{tr}(x^2)} \cdot \mathrm{Id},$$

which is manifestly continuous. Therefore, Θ establishes a homeomorphism between $\mathcal{B}_2(2)$ and $2^2\mathfrak{sl}_2(\mathbb{Z}_2)$.

In particular, the map $\Theta^{-1} : \Theta(G) \cap 2^2\mathfrak{sl}_2(\mathbb{Z}_2) \to G$ is well-defined and continuous, and we finally deduce that the intersection $\Theta(G) \cap 2^2\mathfrak{sl}_2(\mathbb{Z}_2) = \Theta(G \cap \mathcal{B}_2(2))$ is compact, since this is true for $G \cap \mathcal{B}_2(2)$ and Θ is continuous. □

The core of the proof of Theorem 5.2 is contained in the following lemma:

Lemma 5.4. *Let e_1, e_2 be integers not less than 2 and x_1, x_2 be elements of $\Theta(G)$. Suppose that $x_1 \equiv 0 \pmod{2^{e_1}}$ and $x_2 \equiv 0 \pmod{2^{e_2}}$. Then $\Theta(G)$ contains an element y congruent to $x_1 + x_2$ modulo $2^{e_1+e_2-1}$. If, furthermore, both x_1 and x_2 are in upper-triangular form, then we can find such a y having the same property.*

Proof. Write $x_1 = \Theta(g_1)$, $x_2 = \Theta(g_2)$ and set $y = \Theta(g_1 g_2)$. Applying Lemma 3.10, we find

$$2(y - x_1 - x_2) = [x_1, x_2] + (\mathrm{tr}(g_1) - 2)x_2 + (\mathrm{tr}(g_2) - 2)x_1.$$

Consider the 2-adic valuation of the terms on the right. The commutator $[x_1, x_2]$ is clearly 0 modulo $2^{e_1+e_2}$. We also have $\mathrm{tr}(g_1) - 2 \equiv 0 \pmod{2^{2e_1}}$ and $\mathrm{tr}(g_2) - 2 \equiv$

$0 \pmod{2^{2e_2}}$ by Lemma 5.3, so the last two terms are divisible by $2^{2e_1+e_2}$ and $2^{e_1+2e_2}$, respectively. It follows that the right hand side of this equality is zero modulo $2^{e_1+e_2}$, and upon dividing by 2 we get the first statement in the lemma.

For the last claim, simply note that if x_1, x_2 are upper-triangular then the same is true for all of the error terms, so $y = x_1 + x_2 + (\text{triangular error terms})$ is indeed triangular. □

As a first application, we show that the image of Θ is stable under multiplication by 2 (up to units):

Lemma 5.5. *Let $x \in \Theta(G)$ and $m \in \mathbb{N}$. There exists a unit $\lambda \in \mathbb{Z}_2^\times$ such that $\lambda \cdot 2^m x$ again belongs to $\Theta(G)$.*

Proof. Clearly there is nothing to prove for $m = 0$, so let us start with the case $m = 1$. Write $x = \Theta(g)$ for a certain $g \in G$. By our assumptions on G, the trace of g is congruent to 2 modulo 4, so $\lambda = \frac{\mathrm{tr}(g)}{2}$ is a unit in $\mathbb{Z}_2$. We can therefore form $\tilde{g} = \frac{1}{\lambda} g$, which certainly exists as a matrix in $\mathrm{GL}_2(\mathbb{Z}_2)$, even though it does not necessarily belong to G. Our choice of $\tilde{g}$ is made so as to ensure $\mathrm{tr}(\tilde{g}) = 2$, so the formula given in Lemma 3.10 (applied with $g_1 = g_2 = \tilde{g}$) yields

$$2(\Theta(\tilde{g}^2) - \Theta(\tilde{g}) - \Theta(\tilde{g})) = [\Theta(\tilde{g}), \Theta(\tilde{g})] + (\mathrm{tr}(\tilde{g}) - 2)\Theta(\tilde{g}) + (\mathrm{tr}(\tilde{g}) - 2)\Theta(\tilde{g}),$$

where the right hand side vanishes. We deduce $\Theta(\tilde{g}^2) = 2\Theta(\tilde{g})$, and it is now immediate to check that $\Theta(g^2) = \lambda \cdot 2\Theta(g)$, whence the claim for $m = 1$. An immediate induction then proves the general case. □

We now take the first step towards understanding the structure of $\Theta(G)$, namely showing that a suitable basis of L can be found inside $\Theta(G)$. Note that L, being open, is automatically of rank 3.

Lemma 5.6. *There exist a basis $\{x_1, x_2, x_3\} \subseteq \Theta(G)$ of L and scalars $\tilde{\sigma}_{21}$, $\tilde{\sigma}_{31}$, $\tilde{\sigma}_{32} \in \mathbb{Z}_2$ with the following properties: $\pi_{21}(x_2 - \tilde{\sigma}_{21}x_1) = 0$, $\pi_{21}(x_3 - \tilde{\sigma}_{31}x_1) = 0$ and*

$$\pi_{21}(x_3 - \tilde{\sigma}_{31}x_1 - \tilde{\sigma}_{32}(x_2 - \tilde{\sigma}_{21}x_1)) = \pi_{11}(x_3 - \tilde{\sigma}_{31}x_1 - \tilde{\sigma}_{32}(x_2 - \tilde{\sigma}_{21}x_1)) = 0.$$

Remark 5.7. The slightly awkward equations appearing in the statement of this lemma actually have a simple interpretation: they represent that it is possible to subtract a suitable multiple of x_1 from x_2 and x_3 so as to make them upper-triangular, and that it is then further possible to subtract one of the matrices thus obtained from the other so as to leave it with only one nonzero coefficient (in the top right corner).

Proof. This is immediate from Lemma 3.11, which can be applied after identifying $\mathfrak{sl}_2(\mathbb{Z}_2) \cong \mathbb{Z}_2^3$ via $\left(\begin{smallmatrix} a & b \\ c & -a \end{smallmatrix}\right) \mapsto (c, a, b)$. Note that with this identification, the three canonical projections $\mathbb{Z}_2^3 \to \mathbb{Z}_2$ become π_{21}, π_{11} and π_{12}, respectively, and the vanishing conditions in the statement become exactly those of Lemma 3.11. □

As previously mentioned, in order to make the quadratic error terms appearing in Lemma 5.4 negligible, we need to work with matrices that are highly divisible by 2:

Lemma 5.8. *Let x_1, x_2, x_3 be a basis of L. There exist elements $y_1, y_2, y_3 \in \Theta(G)$ and units $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{Z}_2^\times$ such that $y_i = \lambda_i \cdot 2^{4s} x_i$ for $i = 1, 2, 3$; in particular, y_1, y_2, y_3 are zero modulo 2^{4s}, and the module generated by y_1, y_2, y_3 over $\mathbb{Z}_2$ contains $2^{5s}\mathfrak{sl}_2(\mathbb{Z}_2)$.*

Proof. Everything is obvious (by Lemma 5.5) except perhaps the last statement. Note that y_1, y_2, y_3 differ from $2^{4s}x_1, 2^{4s}x_2, 2^{4s}x_3$ only by multiplication by units, so these two sets generate over $\mathbb{Z}_2$ the same module M. But the x_i generate $L \supseteq 2^s\mathfrak{sl}_2(\mathbb{Z}_2)$, hence $M = 2^{4s}L$ contains $2^{5s}\mathfrak{sl}_2(\mathbb{Z}_2)$. □

Notation. Let x_1, x_2, x_3 be a basis of L as in Lemma 5.6, and let y_1, y_2, y_3 be the elements given by Lemma 5.8 when applied to x_1, x_2, x_3. The properties of the x_i become corresponding properties of the y_i:

- there is a scalar $\sigma_{21} \in \mathbb{Z}_2$ such that
$$y_2 - \sigma_{21} \cdot y_1 = \begin{pmatrix} b_{11} & b_{12} \\ 0 & -b_{11} \end{pmatrix} \in \mathfrak{sl}_2(\mathbb{Z}_2);$$
- there are scalars σ_{31}, σ_{32} such that
$$y_3 - \sigma_{31} y_1 = \begin{pmatrix} d_{11} & d_{12} \\ 0 & -d_{11} \end{pmatrix} \in \mathfrak{sl}_2(\mathbb{Z}_2),$$
$$y_3 - \sigma_{31} y_1 - \sigma_{32}(y_2 - \sigma_{21} \cdot y_1) = \begin{pmatrix} 0 & c_{12} \\ 0 & 0 \end{pmatrix} \in \mathfrak{sl}_2(\mathbb{Z}_2).$$

To ease the notation a little we set

$$t_1 = y_1 = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & -a_{11} \end{pmatrix}, \quad t_2 = \begin{pmatrix} b_{11} & b_{12} \\ 0 & -b_{11} \end{pmatrix} \quad \text{and} \quad t_3 = \begin{pmatrix} 0 & c_{12} \\ 0 & 0 \end{pmatrix}.$$

It is clear that $\{t_1, t_2, t_3\}$ and $\{y_1, y_2, y_3\}$ generate the same module M over $\mathbb{Z}_2$, so in particular M contains $2^{5s}\mathfrak{sl}_2(\mathbb{Z}_2)$.

Lemma 5.9. *The 2-adic valuations of a_{21}, b_{11} and c_{12} do not exceed $5s$.*

Proof. We can express $\left(\begin{smallmatrix} 0 & 0 \\ 2^{5s} & 0 \end{smallmatrix}\right)$ as a $\mathbb{Z}_2$-linear combination

$$\begin{pmatrix} 0 & 0 \\ 2^{5s} & 0 \end{pmatrix} = \lambda_1 t_1 + \lambda_2 t_2 + \lambda_3 t_3$$

of t_1, t_2, t_3, for a suitable choice of $\lambda_1, \lambda_2, \lambda_3$ in $\mathbb{Z}_2$. Comparing the bottom-left coefficients, we find $\lambda_1 a_{21} = 2^{5s}$, so $v_2(a_{21}) \leq 5s$, as claimed.

The same argument, applied to the representation of $\left(\begin{smallmatrix} 2^{5s} & 0 \\ 0 & -2^{5s} \end{smallmatrix}\right)$ (resp. $\left(\begin{smallmatrix} 0 & 2^{5s} \\ 0 & 0 \end{smallmatrix}\right)$) as a combination of t_1, t_2, t_3, gives $b_{11} \mid 2^{5s}$ (resp. $c_{12} \mid 2^{5s}$) and finishes the proof of the lemma. □

For future reference, and since it is easy to lose track of all the notation, we record here two facts we will need later:

Remark 5.10. We have $\sigma_{32} = \frac{d_{11}}{b_{11}}$ and $v_2(d_{12} - \sigma_{32} b_{12}) = v_2(c_{12}) \leq 5s$.

We now further our investigation of the approximate additive structure of $\Theta(G)$. Since essentially all of the arguments are based on sequences of approximations the following notation will turn out to be very useful.

Notation. We write $a = b + O(2^n)$ if $a \equiv b \pmod{2^n}$.

Lemma 5.11. *Let $a_1, a_2 \in \Theta(G) \cap 2^{4s}\mathfrak{sl}_2(\mathbb{Z}_2)$ and $\xi \in \mathbb{Z}_2$. Then $\Theta(G)$ contains an element z congruent to $a_1 - \xi a_2$ modulo 2^{8s-1}. If moreover a_1, a_2 are upper-triangular, then z can be chosen to have the same property.*

Proof. We construct a sequence $(z_n)_{n\geq 0}$ of elements of $\Theta(G)$ and a sequence $(\xi_n)_{n\geq 0}$ of elements of $\mathbb{Z}_2$ satisfying $\xi_n = \xi + O(2^n)$ and

$$z_n = a_1 - \xi_n a_2 + O(2^{8s-1}).$$

We can take $z_0 = a_1$ and $\xi_0 = 0$. Given z_n, ξ_n, we proceed as follows. If we let $w_n = v_2(\xi_n - \xi)$, then $w_n \geq n$ by the induction hypothesis, and by Lemma 5.5 we can find a unit λ_n such that $2^{w_n}\lambda_n a_2$ also belongs to $\Theta(G)$. Note that both z_n and $2^{w_n}\lambda_n a_2$ are zero modulo 2^{4s}. Apply Lemma 5.4 to $(x_1, x_2) = (z_n, 2^{w_n}\lambda_n a_2)$: it yields the existence of an element z_{n+1} of $\Theta(G)$ of the form $z_n + 2^{w_n}\lambda_n a_2 + O(2^{8s-1})$. We take $\xi_{n+1} = (\xi_n - 2^{w_n}\lambda_n)$; let us check that ξ_{n+1}, z_{n+1} have the right properties. Clearly,

$$z_{n+1} = z_n + 2^{w_n}\lambda_n a_2 + O(2^{8s-1}) = a_1 - (\xi_n - 2^{w_n}\lambda_n)a_2 + O(2^{8s-1}).$$

On the other hand, the definition of w_n implies that $\xi_n - \xi = 2^{w_n} \cdot \mu_n$ where μ_n is a unit, so

$$\begin{aligned} v_2(\xi_{n+1} - \xi) &= v_2((\xi_n - 2^{w_n}\lambda_n) - \xi) \\ &= v_2(2^{w_n} \cdot \mu_n - 2^{w_n} \cdot \lambda_n) \\ &= w_n + v_2(\mu_n - \lambda_n) \geq w_n + 1 \geq n + 1, \end{aligned}$$

since μ_n, λ_n are both units and therefore odd. To conclude the proof it is simply enough to take $z = z_{8s-1}$: indeed

$$\begin{aligned} a_1 - \xi a_2 - z_{8s-1} &= a_1 - \xi a_2 - (a_1 - \xi_{8s-1} a_2 + O(2^{8s-1})) \\ &= (\xi_{8s-1} - \xi)a_2 + O(2^{8s-1}) \\ &= O(2^{8s-1}) \end{aligned}$$

as required. The proof in the upper-triangular case goes through completely unchanged, simply using the corresponding second part of Lemma 5.4. □

The above lemma is still not sufficient, since it cannot guarantee that we will ever find a matrix with a coefficient that vanishes exactly. This last remaining obstacle is overcome through the following result:

Lemma 5.12. *Let $a_1, a_2 \in \Theta(G) \cap 2^{4s}\mathfrak{sl}_2(\mathbb{Z}_2)$ and $\xi \in \mathbb{Z}_2$. Suppose that for a certain pair (i, j), the (i, j)-th coefficient of $a_1 - \xi a_2$ vanishes while $v_2 \circ \pi_{ij}(a_2) \leq 5s$. Then $\Theta(G)$ contains an element z whose (i, j)-th coefficient is zero and that is congruent to $a_1 - \xi a_2$ modulo 2^{7s-1}. If, furthermore, a_1, a_2 are upper-triangular, then this z can be chosen to be upper-triangular as well (while still satisfying $\pi_{ij}(z) = 0$).*

Proof. Let z_0 be the element whose existence is guaranteed by Lemma 5.11 when applied to a_1, a_2, ξ. We propose to build a sequence $(z_n)_{n\geq 0}$ of elements of $\Theta(G)$ satisfying the following conditions:

(1) $z_{n+1} \equiv z_n \pmod{2^{7s-1}}$, and therefore $z_n \equiv z_0 \equiv 0 \pmod{2^{4s}}$;

(2) the sequence $w_n = v_2 \circ \pi_{ij}(z_n)$ is monotonically strictly increasing; in particular we have $w_n \geq w_0 \geq 8s - 1$.

Suppose we have constructed z_n, w_n and let $k = v_2 \circ \pi_{ij}(a_2) \leq 5s$. By Lemma 5.5, we can find a unit λ such that $2^{w_n-k}\lambda a_2$ also belongs to $\Theta(G)$ (note that $w_n \geq 8s-1 \geq 5s \geq k$). We know that $z_n \equiv 0 \pmod{2^{4s}}$ and $2^{w_n-k}\lambda a_2 \equiv 0 \pmod{2^{w_n-k+4s}}$ (note that $a_2 \equiv 0 \pmod{2^{4s}}$). Apply Lemma 5.4 to $(x_1, x_2) = (z_n, 2^{w_n-k}\lambda a_2)$: it yields the existence of an element z_{n+1} of $\Theta(G)$ that is congruent to $z_n + 2^{w_n-k}\lambda a_2$ modulo $2^{(4s+w_n-k)+4s-1}$.

We can write $\pi_{ij}(z_n) = 2^{w_n}\mu_n$ and $\pi_{ij}(a_2) = 2^k\xi$ with $\mu_n, \xi \in \mathbb{Z}_2^\times$, so

$$v_2 \circ \pi_{ij}(z_n + 2^{w_n-k}\lambda a_2) = v_2(2^{w_n}\mu_n + 2^{w_n-k}2^k \cdot \xi\lambda) = w_n + v_2(\mu_n + \xi\lambda),$$

and since μ_n, ξ and λ are all odd the last term is at least $w_n + 1$. As k is at most $5s$ by hypothesis we deduce

$$\begin{aligned} w_{n+1} &= v_2 \circ \pi_{ij}(z_{n+1}) \\ &= v_2 \circ \pi_{ij}\big(z_n + 2^{w_n-k}\lambda a_2 + O(2^{(4s+w_n-k)+4s-1})\big) \\ &\geq \min\big\{v_2 \circ \pi_{ij}(z_n + 2^{w_n-k}\lambda a_2), 8s - 1 + w_n - k\big\} \\ &> w_n. \end{aligned}$$

As $2^{w_n-k}\lambda a_2 \equiv 0 \pmod{2^{w_n-k+4s}}$, the difference $z_{n+1} - z_n$ is zero modulo 2^{w_n-s}, hence a fortiori modulo 2^{7s-1} since $w_n \geq w_0 \geq 8s - 1$.

Lemma 5.3 says that $\Theta(G) \cap 2^2\mathfrak{sl}_2(\mathbb{Z}_2)$ is compact, so z_n admits a subsequence converging to a certain $z \in \Theta(G)$. By continuity of π_{ij}, it is immediate to check that $\pi_{ij}(z) = 0$, and since every z_n is congruent modulo 2^{7s-1} to z_0 the same is true for z. Given that z_0 is congruent to $a_1 - \xi a_2$ modulo 2^{8s-1}, the last assertion follows.

Finally, the upper-triangular case is immediate, since it is clear from the construction that if a_1, a_2 are upper-triangular then the same is true for all the approximations z_n. □

The result we were really aiming for follows at once:

Proposition 5.13. *Let G be a closed subgroup of $\mathrm{SL}_2(\mathbb{Z}_2)$ whose reduction modulo 2 is trivial, and let s be an integer no less than 2. If $L(G)$ contains $2^s\mathfrak{sl}_2(\mathbb{Z}_2)$, then $\Theta(G)$ contains both an element of the form $\left(\begin{smallmatrix} 0 & \tilde{c}_{12} \\ 0 & 0 \end{smallmatrix}\right)$, where $v_2(\tilde{c}_{12}) \le 5s$, and one of the form $\left(\begin{smallmatrix} f_{11} & 0 \\ 0 & -f_{11} \end{smallmatrix}\right)$, where $v_2(f_{11}) \le 6s$.*

Proof. We apply Lemma 5.12 to $a_1 = y_2$, $a_2 = y_1$, $\xi = \sigma_{21}$, $(i, j) = (2, 1)$; the hypotheses are satisfied since $y_1 \equiv y_2 \equiv 0 \pmod{2^{4s}}$ and $v_2 \circ \pi_{21}(y_1) \le 5s$ by Lemma 5.9. It follows that $\Theta(G)$ contains a matrix $\tilde{b}$ of the form $\left(\begin{smallmatrix} \tilde{b}_{11} & \tilde{b}_{12} \\ 0 & -\tilde{b}_{11} \end{smallmatrix}\right)$, where we have $\tilde{b}_{ij} \equiv b_{ij} \pmod{2^{7s-1}}$ for every $1 \le i, j \le 2$; in particular, $v_2(\tilde{b}_{11}) \le 5s$.

The same lemma, applied to $a_1 = y_3$, $a_2 = y_1$ and $\xi = \sigma_{31}$, implies that $\Theta(G)$ contains a matrix $\tilde{d}$ of the form $\left(\begin{smallmatrix} \tilde{d}_{11} & \tilde{d}_{12} \\ 0 & -\tilde{d}_{11} \end{smallmatrix}\right)$, where for every i, j we have $\tilde{d}_{ij} \equiv d_{ij} \pmod{2^{7s-1}}$; in particular,

$$v_2(\tilde{d}_{11}) \ge \min\{7s - 1, v_2(d_{11})\} \ge v_2(b_{11}) = v_2(\tilde{b}_{11}).$$

Now since $v_2(\tilde{d}_{11}) \ge v_2(\tilde{b}_{11})$, we can find a scalar ζ such that

$$\tilde{d} - \zeta\tilde{b} = \begin{pmatrix} \tilde{d}_{11} & \tilde{d}_{12} \\ 0 & -\tilde{d}_{11} \end{pmatrix} - \zeta\begin{pmatrix} \tilde{b}_{11} & \tilde{b}_{12} \\ 0 & -\tilde{b}_{11} \end{pmatrix} = \begin{pmatrix} 0 & e_{12} \\ 0 & 0 \end{pmatrix},$$

so applying once again Lemma 5.12 (more precisely, the version for triangular matrices) we find that $\Theta(G)$ contains a certain matrix $\tilde{e} = \left(\begin{smallmatrix} 0 & \tilde{e}_{12} \\ 0 & 0 \end{smallmatrix}\right)$, where $\tilde{e}_{12} \equiv e_{12} \pmod{2^{7s-1}}$. Observe now that

$$\zeta = \frac{\tilde{d}_{11}}{\tilde{b}_{11}} = \frac{d_{11} + O(2^{7s-1})}{b_{11} + O(2^{7s-1})} = \frac{d_{11}}{b_{11}} + O(2^{7s-1-v_2(b_{11})}) = \frac{d_{11}}{b_{11}} + O(2^{2s-1}),$$

so upon multiplying by $\tilde{b}_{12}$, which is divisible by 2^{4s}, we obtain the congruence $\zeta\tilde{b}_{12} \equiv \frac{d_{11}}{b_{11}}\tilde{b}_{12} \pmod{2^{6s-1}}$. Since furthermore $\tilde{b}_{12} \equiv b_{12} \pmod{2^{6s-1}}$ we deduce $\zeta\tilde{b}_{12} \equiv \frac{d_{11}}{b_{11}}b_{12} \pmod{2^{6s-1}}$. But then the inequality $v_2(c_{12}) \le 5s$ (cf. Remark 5.10) implies

$$\begin{aligned} v_2(\tilde{e}_{12}) &= v_2\big(e_{12} + O(2^{7s-1})\big) \\ &= v_2\big(\tilde{d}_{12} - \zeta\tilde{b}_{12} + O(2^{7s-1})\big) \\ &= v_2\big(d_{12} - \tfrac{d_{11}}{b_{11}}b_{12} + O(2^{6s-1})\big) \\ &= v_2\big(c_{12} + O(2^{6s-1})\big) \\ &\le 5s. \end{aligned}$$

The existence of the diagonal element is now almost immediate: indeed, we can apply once more Lemma 5.12 to the difference

$$2^s\begin{pmatrix} \tilde{b}_{11} & \tilde{b}_{12} \\ 0 & -\tilde{b}_{11} \end{pmatrix} - \frac{2^s\tilde{b}_{12}}{\tilde{e}_{12}}\begin{pmatrix} 0 & \tilde{e}_{12} \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} \tilde{b}_{11} & 0 \\ 0 & -\tilde{b}_{11} \end{pmatrix},$$

the hypotheses being satisfied since clearly $2^s\tilde{b} \equiv 0 \pmod{2^{5s}}$ and $v_2(\tilde{e}_{12}) \leq 5s$ for what we have just seen. It follows that $\Theta(G)$ contains a matrix $\left(\begin{smallmatrix} f_{11} & 0 \\ 0 & -f_{11} \end{smallmatrix}\right)$ congruent to $2^s\left(\begin{smallmatrix} \tilde{b}_{11} & 0 \\ 0 & -\tilde{b}_{11} \end{smallmatrix}\right)$ modulo 2^{7s-1}, and this is enough to deduce

$$v_2(f_{11}) = v_2(2^s b_{11} + O(2^{7s-1})) = s + v_2(b_{11}) \leq 6s. \qquad \square$$

Proof of Theorem 5.2. With all the preliminaries in place this is now quite easy: by Proposition 5.13 we know that $\Theta(G)$ contains an element of the form $\left(\begin{smallmatrix} 0 & \tilde{c}_{12} \\ 0 & 0 \end{smallmatrix}\right)$, where $v_2(\tilde{c}_{12}) \leq 5s$, and by the explicit description of Θ^{-1} (Lemma 5.3) this element must come from $R_{\tilde{c}_{12}} = \left(\begin{smallmatrix} 1 & \tilde{c}_{12} \\ 0 & 1 \end{smallmatrix}\right) \in G$. Similarly, if we let f denote the diagonal element $\left(\begin{smallmatrix} f_{11} & 0 \\ 0 & -f_{11} \end{smallmatrix}\right)$, then

$$\Theta^{-1}(f) = \begin{pmatrix} f_{11} & 0 \\ 0 & -f_{11} \end{pmatrix} + \sqrt{1 + \tfrac{1}{2}\operatorname{tr}(f^2)} \cdot \mathrm{Id}$$

is an operator of the form $D_c = \left(\begin{smallmatrix} 1+c & 0 \\ 0 & 1/(c+1) \end{smallmatrix}\right)$, where

$$\begin{aligned} v_2(c) &= v_2\Big(f_{11} + \sqrt{1 + \tfrac{1}{2}\operatorname{tr}(f^2)} - 1\Big) \\ &= v_2\big(f_{11} + O(2^{2v_2(f_{11})-1})\big) \\ &= v_2(f_{11}) \leq 6s. \end{aligned}$$

Observe now that replacing G with G^t, the group $\{g^t \mid g \in G\}$ endowed with the obvious product $g_1^t \cdot g_2^t = (g_2 g_1)^t$, simply exchanges $L(G)$ for $L(G)^t$, so if $L(G)$ contains the (symmetric) set $2^s\mathfrak{sl}_2(\mathbb{Z}_2)$, then the same is true for $L(G^t)$. Thus G^t contains $R_{2^{5s}}$ and G contains $L_{2^{5s}}$. We have just shown that G contains L_a, R_b and D_c for certain a, b, c of valuation at most $6s$, so it follows from Lemma 3.4 that G contains $\mathcal{B}_2(6s)$. $\square$

Remark 5.14. The above result should be thought of as an analogue of Theorem 3.9 for $\ell = 2$, even though the present result is actually much weaker. It would of course be interesting to have a complete classification result for pro-2 groups purely in terms of Lie algebras, but as pointed out in [Pink 1993] the problem seems to be substantially harder than for $\ell \neq 2$.

It is now easy to deduce Theorem 5.1(i):

Proof. The proof follows closely that of Theorem 4.2(i): we can replace G first by $H = G \cdot (1 + 8\mathbb{Z}_2)$ and then by $H_0 = H \cap \mathrm{SL}_2(\mathbb{Z}_2)$ without altering $L(G)$ or G', so we are reduced to working with subgroups of $\mathrm{SL}_2(\mathbb{Z}_2)$. Note now that $n \geq 2$, since by hypothesis every element in G (and hence in H_0) has its off-diagonal coefficients divisible by 4. Theorem 5.2 then guarantees that H_0 contains $\mathcal{B}_2(6n)$, so $G' = H_0'$ contains $\mathcal{B}_2(12n + 2)$ because of Lemma 3.3. $\square$

6. Lie algebras modulo ℓ^n

Fix any prime number ℓ and let L be a topologically open and closed, $\mathbb{Z}_\ell$-Lie subalgebra of $\mathfrak{sl}_2(\mathbb{Z}_\ell)$. The same arguments of the previous section, namely an application of Lemma 3.11, yield the existence of a basis of L of the form

$$x_1 = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & -a_{11} \end{pmatrix}, \quad x_2 = \begin{pmatrix} b_{11} & b_{12} \\ 0 & -b_{11} \end{pmatrix}, \quad x_3 = \begin{pmatrix} 0 & c_{12} \\ 0 & 0 \end{pmatrix}.$$

Definition 6.1. A basis of this form will be called a *reduced* basis.

There is clearly no uniqueness of such an object, but in what follows we will just assume that the choice of a reduced basis has been made.

Notation. We let $k(L)$, or simply k, denote the number $\min_{m\in L} v_\ell(m_{21})$, where m_{21} is the bottom-left coefficient of m in the standard matrix representation of elements of $\mathfrak{sl}_2(\mathbb{Z}_\ell)$. Furthermore, for every positive n we denote by $L(\ell^n)$ be the image of the mod-ℓ^n reduction map $\pi_n : L \to \mathfrak{sl}_2(\mathbb{Z}/\ell^n\mathbb{Z})$; clearly $L(\ell^n)$ is a Lie algebra over $\mathbb{Z}/\ell^n\mathbb{Z}$.

Remark 6.2. It is apparent from the definition of a reduced basis that $k(L) = v_\ell(a_{21})$. Also notice that, by definition, the images of x_1, x_2, x_3 in $L(\ell^n)$ generate it as a $(\mathbb{Z}/\ell^n\mathbb{Z})$-module.

The following statement allows us to deduce properties of $G(\ell^n)$ from corresponding properties of $L(\ell^n)$:

Proposition 6.3. *Let L be as above, and assume that L is obtained as $\overline{\Theta(G)}$ for a certain closed subgroup G of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ (whose reduction modulo 2 is trivial if $\ell = 2$). For every integer $m \geq 1$, let $G(\ell^m)$ be the image of G in $\mathrm{GL}_2(\mathbb{Z}/\ell^m\mathbb{Z})$, and let $j_m = |\{i \in \{1,2,3\} \mid x_i \not\equiv 0 \pmod{\ell^m}\}|$ (that is, exactly j_m among x_1, x_2 and x_3 are nonzero modulo ℓ^m). For every $n \geq 1$ the following are the only possibilities (recall that $v = v_\ell(2)$):*

- *j_n is at most 1 and $G(\ell^n)$ is abelian.*
- *$j_n = 2$ and either $j_{2n} = 3$ or $G(\ell^{n-k(L)+1-2v})$ is contained in the subgroup of upper-triangular matrices (up to a change of coordinates in $\mathrm{GL}_2(\mathbb{Z}_\ell)$).*
- *$j_n = 3$ and L contains $\ell^{n+2k(L)-1}\mathfrak{sl}_2(\mathbb{Z}_\ell)$.*

Remark 6.4. The exponent $n + 2k(L) - 1$ is best possible: fix integers $k \geq 0$, $n \geq 1$ and let L be the Lie algebra generated (as a $\mathbb{Z}_\ell$-module) by $x_1 = \left(\begin{smallmatrix} 1 & 0 \\ \ell^k & -1 \end{smallmatrix}\right)$, $x_2 = \left(\begin{smallmatrix} \ell^{k+n-1} & 0 \\ 0 & -\ell^{k+n-1} \end{smallmatrix}\right)$, and $x_3 = \left(\begin{smallmatrix} 0 & \ell^{n-1} \\ 0 & 0 \end{smallmatrix}\right)$. Then clearly $k(L) = k$, $j_n(L) = 3$, and it is easy to check that $n + 2k - 1$ is the smallest exponent s such that $\ell^s\mathfrak{sl}_2(\mathbb{Z}_\ell)$ is contained in L.

Proof. Assume first $j_n \leq 1$. It is clear that every element of $G(\ell^n)$ can we written as $\lambda\,\mathrm{Id} + m_n$ for some $\lambda \in \mathbb{Z}/\ell^n\mathbb{Z}$ and $m_n \in L(\ell^n)$. Now L is generated by x_1, x_2, x_3,

so in turn every m_n is of the form $\pi_n(\mu_1 x_1 + \mu_2 x_2 + \mu_3 x_3)$, and since at most one of $\pi_n(x_1), \pi_n(x_2), \pi_n(x_3)$ is nonzero we can find an $l_n \in L(\ell^n)$ such that, for every m_n, there exists a scalar $\mu \in \mathbb{Z}/\ell^n\mathbb{Z}$ with $m_n = \mu\, l_n$. It follows that every element of $G(\ell^n)$ can be written as $\lambda\,\mathrm{Id} + \mu\, l_n$ for suitable λ, μ, and since Id and l_n commute, our claim follows.

Next consider the case $j_n = 2$. We can safely assume that $j_{2n} = 2$, for otherwise we are done (notice that $j_{2n} \geq j_n = 2$). Under this assumption, it is clear that for $i = 1, 2, 3$, we have $\pi_n(x_i) = 0$ if and only if $\pi_{2n}(x_i) = 0$. Suppose first $\pi_n(x_1) = 0$, so that $k(L) \geq 1$. Then $G(\ell^n)$ is a subset of

$$\mathbb{Z}/\ell^n\mathbb{Z} \cdot \mathrm{Id} + \mathbb{Z}/\ell^n\mathbb{Z} \cdot \pi_n(x_2) + \mathbb{Z}/\ell^n\mathbb{Z} \cdot \pi_n(x_3),$$

and Id, $\pi_n(x_2)$, $\pi_n(x_3)$ are upper-triangular matrices. So $G(\ell^n)$, and hence also $G(\ell^{n-k(L)+1-2v})$ since $k(L) \geq 1$, is in triangular form.

Suppose next $\pi_n(x_1) \neq 0$. Assume that $\pi_n(x_3) = 0$ (the other case being analogous, as we are only going to use that x_2 is upper-triangular). L is a Lie algebra, hence so is $L(\ell^{2n})$; furthermore, every element in $L(\ell^{2n})$ is a combination of $\pi_{2n}(x_1)$, $\pi_{2n}(x_2)$ with coefficients in $\mathbb{Z}/\ell^{2n}\mathbb{Z}$. In particular, there exist $\xi_1, \xi_2 \in \mathbb{Z}/\ell^{2n}\mathbb{Z}$ such that

$$\begin{aligned} -2b_{11}x_1 + 2a_{11}x_2 &= \begin{pmatrix} -a_{21}b_{12} & 4(a_{11}b_{12} - a_{12}b_{11}) \\ 0 & a_{21}b_{12} \end{pmatrix} \\ &\equiv \xi_1 x_1 + \xi_2 x_2 \pmod{\ell^{2n}}. \end{aligned}$$

Matching the bottom-left coefficients, we find $\xi_1 a_{21} \equiv 0 \pmod{\ell^{2n}}$, so, using $v_\ell(a_{21}) = k(L)$, we immediately deduce $\xi_1 \equiv 0 \pmod{\ell^{2n-k(L)}}$. Reducing the above congruence modulo $\ell^{2n-k(L)}$ we then have the relations

$$\begin{cases} -a_{21}b_{12} \equiv \xi_2 b_{11} \pmod{\ell^{2n-k(L)}} \\ 4(a_{11}b_{12} - a_{12}b_{11}) \equiv \xi_2 b_{12} \pmod{\ell^{2n-k(L)}}. \end{cases} \tag{6-1}$$

We now introduce the vector $y = \left(\begin{smallmatrix} b_{12} \\ -2b_{11} \end{smallmatrix}\right) \in \mathbb{Z}_\ell^2$. An immediate calculation shows that this is an exact eigenvector for x_2 (associated with the eigenvalue $-b_{11}$), and on the other hand it is also an approximate eigenvector for $2x_1$, in the sense that $2x_1 \cdot y \equiv (\xi_2 - 2a_{11})y \pmod{\ell^{2n-k(L)}}$. Indeed,

$$2x_1 \cdot y = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & -a_{11} \end{pmatrix} \begin{pmatrix} 2b_{12} \\ -4b_{11} \end{pmatrix} = \begin{pmatrix} 2a_{11}b_{12} - 4a_{12}b_{11} \\ 2a_{21}b_{12} + 4a_{11}b_{11} \end{pmatrix},$$

and using (6-1) we find

$$\begin{aligned} 2x_1 \cdot y = \begin{pmatrix} 2a_{11}b_{12} - 4a_{12}b_{11} \\ 2a_{21}b_{12} + 4a_{11}b_{11} \end{pmatrix} &\equiv \begin{pmatrix} 2a_{11}b_{12} + \xi_2 b_{12} - 4a_{11}b_{12} \\ -2\xi_2 b_{11} + 4a_{11}b_{11} \end{pmatrix} \\ &\equiv (\xi_2 - 2a_{11})y \pmod{\ell^{2n-k(L)}}, \end{aligned}$$

as claimed.

Now if $\ell \neq 2$ we immediately deduce $x_1 \cdot y \equiv (\xi_2/2 - a_{11})y \pmod{\ell^{2n-k(L)}}$. If, on the other hand $\ell = 2$, then we would like to prove that $v_2(\xi_2) \geq 1$ in order to be able to divide by 2. Observe that y is not zero modulo 2^{n+1}, since its coordinates are (up to a factor of 2) the entries of x_2, which we have assumed not to reduce to zero in $L(2^n)$.

Let $\alpha = \min\{v_2(2b_{11}), v_2(b_{21})\} \leq n$ and reduce the last congruence modulo $2^{\alpha+1}$. Then $2x_1 \cdot y \equiv x_1 \cdot (2y) \equiv 0 \pmod{2^{\alpha+1}}$, so $(\xi_2 - 2a_{11})y \equiv 0 \pmod{2^{\alpha+1}}$, which implies that ξ_2 is even (that is to say, $v_2(\xi_2) \geq 1$), for otherwise multiplying by $\lambda - 2a_{11}$ would be invertible modulo $2^{\alpha+1}$ and we would find $y \equiv 0 \pmod{2^{\alpha+1}}$, contradicting the definition of α. It follows that we can indeed divide the above congruence by 2 to get

$$x_1 \cdot y \equiv (\xi_2/2 - a_{11})y \pmod{2^{2n-k(L)-1}}.$$

Equivalently, the following congruence holds for *every* prime ℓ:

$$x_1 \cdot y \equiv \big(\xi_2/2 - a_{11}\big)y \pmod{\ell^{2n-k(L)-v}}.$$

Note now that it is in fact true for *every* ℓ that y is not zero modulo ℓ^{n+v} (its coordinates are, up to a factor of 2, the entries of x_2, which we have assumed not to reduce to zero modulo ℓ^n).

Let again $\alpha = \min\{v_\ell(2b_{11}), v_\ell(b_{21})\} \leq n - 1 + v$ and set $\tilde{y} = \ell^{-\alpha} y$. Dividing the congruence $x_1 \cdot y \equiv (\xi_2/2 - a_{11})y \pmod{\ell^{2n-k(L)-v}}$ by ℓ^α, we get $x_1 \cdot \tilde{y} \equiv \big(\xi_2/2 - a_{11}\big)\tilde{y} \pmod{\ell^{n-k(L)+1-2v}}$, where $\tilde{y} = \binom{\tilde{y}_1}{\tilde{y}_2}$ is a vector with at least one coordinate an ℓ-adic unit. Assume by symmetry that $v_\ell(\tilde{y}_1) = 0$ and introduce the base-change matrix $P = \left(\begin{smallmatrix} \tilde{y}_1 & 0 \\ \tilde{y}_2 & 1 \end{smallmatrix}\right)$: this is then an element of $\mathrm{GL}_2(\mathbb{Z}_\ell)$, since its determinant $\tilde{y}_1$ is not divisible by ℓ.

An element of $G(\ell^{n-k(L)+1-2v})$ will be of the form $g = \lambda\,\mathrm{Id} + \mu_1 x_1 + \mu_2 x_2$, so by construction conjugating G via P puts $G(\ell^{n-k(L)+1-2v})$ in upper-triangular form. Indeed, the first column of x_i (for $i = 1, 2$) in the coordinates defined by P is given by

$$\begin{aligned} P^{-1} x_i P \binom{1}{0} &= P^{-1} x_i \cdot \tilde{y} = P^{-1}\big((\xi_2/2 - a_{11})\tilde{y} + \ell^{n-k(L)+1-2v} w\big) \\ &= (\xi_2/2 - a_{11})\binom{1}{0} + \ell^{n-k(L)+1-2v} P^{-1} w \\ &\equiv (\xi_2/2 - a_{11})\binom{1}{0} \pmod{\ell^{n-k(L)+1-2v}} \end{aligned}$$

where w is a suitable vector in $\mathbb{Z}_\ell^2$ (that vanishes for $i = 2$).

Finally, suppose $j_n = 3$. Then we have in particular $\pi_n(x_3) \neq 0$, so $v_\ell(c_{12}) \leq n-1$. As L is a Lie algebra, we see that it contains

$$x_4 = [x_1, x_3] - 2a_{11}x_3 = \begin{pmatrix} -a_{21}c_{12} & 0 \\ 0 & a_{21}c_{12} \end{pmatrix},$$

whose diagonal entries have valuation at most $v_\ell(a_{21}) + v_\ell(c_{12}) \leq k(L) + (n-1)$. Furthermore, L also contains the linear combination

$$x_5 = \ell^{n+k(L)-1}x_1 + \frac{\ell^{n+k(L)-1}a_{11}}{a_{21}c_{12}}x_4 - \frac{\ell^{n+k(L)-1}a_{12}}{c_{12}}x_3 = \begin{pmatrix} 0 & 0 \\ \ell^{n+k(L)-1}a_{21} & 0 \end{pmatrix}.$$

Notice that the coefficients $\frac{\ell^{n+k(L)-1}a_{11}}{a_{21}c_{12}}$ and $\frac{\ell^{n+k(L)-1}a_{12}}{c_{12}}$ have positive ℓ-adic valuation by what we have already shown, and that the valuation of the only nonzero coefficient of x_5 is $n + 2k(L) - 1$. Setting

$$s_1 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad s_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad s_3 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},$$

we see that L contains the three elements $x_3 = c_{12}s_1$, $x_4 = -a_{21}c_{12}s_2$, $x_5 = \ell^{n+k(L)-1}a_{21}s_3$. By what we have already proved, we have

$$\max\{v_\ell(c_{12}), v_\ell(-a_{21}c_{12}), v_\ell(\ell^{n+k(L)-1}a_{21})\} = n + 2k(L) - 1,$$

so the $\mathbb{Z}_\ell$-module generated by x_3, x_4, x_5 contains $\ell^{n+2k(L)-1}\mathfrak{sl}_2(\mathbb{Z}_\ell)$, and a fortiori so does L. □

Corollary 6.5. *Let G be a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ satisfying property (⋆⋆) of Theorem 4.2 (resp. $G(4) = \{\mathrm{Id}\}$ and $\det(G) \equiv 1 \pmod 8$ if $\ell = 2$). Then for every positive integer $n \geq k(L(G))$, at least one of the following holds*:

(1) *$G(\ell^n)$ is abelian.*

(2) *$G(\ell^{n-k(L(G))+1-2v})$ is contained in the subgroup of upper-triangular matrices (up to a change of coordinates in $\mathrm{GL}_2(\mathbb{Z}_\ell)$).*

(3) *G' contains the principal congruence subgroup*

$$\mathcal{B}_\ell(16n-4) = (\mathrm{Id} + \ell^{16n-4}\mathfrak{gl}_2(\mathbb{Z}_\ell)) \cap \mathrm{SL}_2(\mathbb{Z}_\ell)$$

if ℓ is odd, and it contains $\mathcal{B}_2(48n-10)$ if $\ell = 2$.

Proof. To ease the notation, set $L = L(G)$. Consider $L(\ell^n)$ and distinguish cases depending on j_n as in the statement of the previous proposition. If $j_n \leq 1$ we are in case (1) and we are done. If $j_n \geq 2$ we begin by proving that either (2) holds or L contains $\ell^{4n-1}\mathfrak{sl}_2(\mathbb{Z}_\ell)$.

If $j_n = 2$ and $j_{2n} = 2$, then we are in situation (2) by the previous proposition. If, on the other hand, $j_n = 2$ and $j_{2n} = 3$, then (again by Proposition 6.3) we have

$$L \supseteq \ell^{2n+2k(L)-1}\mathfrak{sl}_2(\mathbb{Z}_\ell) \supseteq \ell^{4n-1}\mathfrak{sl}_2(\mathbb{Z}_\ell)$$

since $n \geq k(L)$. Finally, for $j_n = 3$ the proposition yields directly

$$L \supseteq \ell^{n+2k(L)-1}\mathfrak{sl}_2(\mathbb{Z}_\ell) \supseteq \ell^{3n-1}\mathfrak{sl}_2(\mathbb{Z}_\ell).$$

In all cases, property (⋆⋆) (resp. Theorem 5.1(i) for $\ell = 2$) now implies that G' contains $\mathcal{B}_\ell(16n-4)$ (resp. $\mathcal{B}_2(48n-10)$) as claimed. □

7. Application to Galois groups

We now plan to apply the above machinery to the Galois representations attached to an elliptic curve. Let therefore K be a number field and E an elliptic curve over K without (potential) complex multiplication.

Notation. ℓ is any rational prime, n a positive integer and G_ℓ the image of $\mathrm{Gal}(\overline{K}/K)$ inside $\mathrm{Aut}\, T_\ell(E) \cong \mathrm{GL}_2(\mathbb{Z}_\ell)$. As before, v is 0 or 1 according to whether ℓ is odd or even, respectively.

If ℓ is odd (resp. $\ell = 2$), then by Theorem 4.2 (resp. Theorem 5.1) we know that either G_ℓ contains a subgroup H_ℓ satisfying $[G_\ell : H_\ell] \leq 24$ (respectively $[G_\ell : H_\ell] \leq 192$ for $\ell = 2$) and the hypotheses of Corollary 6.5, or otherwise $G'_\ell = \mathrm{SL}_2(\mathbb{Z}_\ell)$. In this second case, we put $H_\ell = G_\ell$.

We also denote by K_ℓ the extension of K fixed by H_ℓ. The degree $[K_\ell : K]$ is then bounded by 24 for odd ℓ, and by $2 \cdot |\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})| = 2 \cdot 96$ for $\ell = 2$. For a fixed ℓ, upon replacing K with K_ℓ we are reduced to the case where G_ℓ satisfies the hypotheses of Corollary 6.5. In order to apply this result we want to have numerical criteria to exclude the "bad" cases (1) and (2). These numerical bounds form the subject of Lemma 7.1 and Proposition 7.4 below, whose proofs are inspired by the arguments of [Masser and Wüstholz 1993c; 1989].

Lemma 7.1. *If $\ell^n \nmid b_0(K, E)$, the group $G_\ell(\ell^n)$ cannot be put in triangular form.*

Proof. Suppose that $G_\ell(\ell^n)$ is contained (up to a change of basis) in the group of upper-triangular matrices. The subgroup Γ of $E[\ell^n]$ given (in the coordinates in which $G_\ell(\ell^n)$ is triangular) by

$$\Gamma = \left\{ \begin{pmatrix} a \\ 0 \end{pmatrix} \mid a \in \mathbb{Z}/\ell^n\mathbb{Z} \right\}$$

is $\mathrm{Gal}(\overline{K}/K)$-stable, hence defined over K. Consider then $E^* = E/\Gamma$ and the natural projection $\pi : E \to E^*$ of degree $|\Gamma| = \ell^n$. By Theorem 2.8, we also have an isogeny $E^* \to E$ of degree b, with $b \mid b_0(K, E)$. Composing the two, we get an endomorphism of E that kills Γ, and therefore corresponds (since $\binom{1}{0}$ is annihilated by ℓ^n) to multiplication by a certain $\ell^n d$, $d \in \mathbb{Z}$. Taking degrees, we get $\ell^n \cdot b = |\Gamma| \cdot b = d^2 \ell^{2n}$, so $\ell^n \mid b$ and $\ell^n \mid b_0(K, E)$. □

Corollary 7.2. *Let L be the special Lie algebra of G_ℓ (supposing that $G_\ell(2)$ is trivial if $\ell = 2$). The inequality $k(L) \leq v_\ell(b_0(K, E))$ holds, so that in particular $\ell^{k(L)} \mid b_0(K, E)$.*

Proof. Let $t = v_\ell(b_0(K, E))$. If by contradiction we had $k(L) \geq t + 1$, then $L(\ell^{t+1})$ would be triangular, and therefore so would be $G_\ell(\ell^{t+1}) \subseteq \mathbb{Z}/\ell^{t+1}\mathbb{Z} \cdot \mathrm{Id} + L(\ell^{t+1})$, which is absurd, since $\ell^{t+1} \nmid b_0(K, E)$. □

Corollary 7.3. *If $\ell^n \nmid b_0(K, E)$, the group $G_\ell(\ell^n)$ does not consist entirely of scalar matrices. In particular, this is true for $G_\ell(\ell^{v_\ell(b_0(K,E))+1})$.*

Proposition 7.4. *If ℓ^{2n} does not divide $b_0(K, E)^4 b_0(K, E \times E)$, the group $G_\ell(\ell^n)$ is not abelian. In particular, the group $G_\ell(\ell)$ is not abelian if ℓ does not divide $b_0(K, E) b_0(K, E \times E)$.*

Proof. For simplicity, set $d = b_0(K, E)$. By Corollary 7.3, there is an $\alpha \in G_\ell$ whose image modulo $\ell^{1+v_\ell(d)}$ is not a scalar matrix. Suppose now that $G_\ell(\ell^n)$ is abelian. The subgroup $\Gamma = \{(x, \alpha(x)) \mid x \in E[\ell^n]\} \subset E \times E$ is defined over K, since for any $\gamma \in G_\ell(\ell^n)$ we have $\gamma \cdot (x, \alpha(x)) = (\gamma \cdot x, \gamma \cdot \alpha(x)) = (\gamma \cdot x, \alpha(\gamma \cdot x))$ as $G_\ell(\ell^n)$ is commutative. We can therefore form the quotient K-variety $E^* = (E \times E)/\Gamma$, which comes equipped with a natural isogeny $E \times E \twoheadrightarrow E^*$ of degree $|\Gamma| = E[\ell^n] = \ell^{2n}$; on the other hand, Theorem 2.8 yields the existence of a K-isogeny $E^* \to E \times E$ of degree $b \mid b_0(K, E \times E)$. Composing the two, we obtain an endomorphism ψ of $E \times E$, which (given that E does not admit complex multiplication) can be represented as a 2×2 matrix $\left(\begin{smallmatrix} e_{11} & e_{12} \\ e_{21} & e_{22} \end{smallmatrix}\right)$ with coefficients in $\mathbb{Z}$ and nonzero determinant.

Now since ψ kills Γ, we must have $e_{11}x + e_{12}\alpha(x) = 0$ and $e_{21}x + e_{22}\alpha(x) = 0$ for every $x \in E[\ell^n]$. Let $\eta = \min\{v_\ell(e_{ij})\}$ and suppose by contradiction that $\eta < n - v_\ell(d)$. For the sake of simplicity, let us assume this minimum is attained for e_{12} (the other cases being completely analogous: the situation is manifestly symmetric in the index i, and to show that it is symmetric in j, it is enough to compose with α^{-1}, which is again a nonscalar matrix). Dividing the equation $e_{11}x + e_{12}\alpha(x) = 0$ by ℓ^η, we get

$$\frac{e_{11}}{\ell^\eta} x + \frac{e_{12}}{\ell^\eta} \alpha(x) \equiv 0 \pmod{\ell^{n-\eta}}, \quad \forall x \in E[\ell^n],$$

whence

$$\frac{e_{11}}{\ell^\eta} x + \frac{e_{12}}{\ell^\eta} \alpha(x) = 0, \quad \forall x \in E[\ell^{n-\eta}],$$

where now $\frac{e_{12}}{\ell^\eta}$ is invertible modulo $\ell^{n-\eta}$, being relatively prime to ℓ. Multiplying by the inverse of $\frac{e_{12}}{\ell^\eta}$, we then find that

$$\alpha(x) = -\frac{e_{11}}{\ell^\eta} \left(\frac{e_{12}}{\ell^\eta}\right)^{-1} x, \quad \forall x \in E[\ell^{n-\eta}],$$

i.e., α is a scalar modulo $\ell^{n-\eta}$. By definition of α, this implies $\ell^{n-\eta} \mid d$, so $n - \eta \leq v_\ell(d)$, a contradiction. It follows that $\ell^{2n}\ell^{-2v_\ell(d)} \mid \ell^{2\eta} \mid \det\left(\begin{smallmatrix} e_{11} & e_{12} \\ e_{21} & e_{22} \end{smallmatrix}\right)$. Squaring this last divisibility, we find

$$\ell^{4n}\ell^{-4v_\ell(d)} \mid \left(\det\begin{pmatrix} e_{11} & e_{12} \\ e_{21} & e_{22} \end{pmatrix}\right)^2 = \deg(\psi) = b\ell^{2n},$$

so $\ell^{2n}\ell^{-4v_\ell(d)} \mid b$ and $\ell^{2n} \mid \ell^{4v_\ell(d)} b_0(K, E \times E) \mid d^4 b_0(K, E \times E)$. The second assertion follows immediately from the fact that ℓ is prime. □

With these results at hand it is now immediate to deduce the following theorem, where we use the notation introduced at the beginning of this section and the symbol $\mathcal{B}_\ell(n)$ of Section 3.

Theorem 7.5. *Let ℓ be a prime and set $D(\ell) = b_0(K_\ell, E)^5 b_0(K_\ell, E \times E)$. Let n be a positive integer. Suppose that ℓ^{n-v} does not divide $D(\ell)$: then H'_ℓ contains $\mathcal{B}_\ell(16n-4)$ for odd ℓ, and it contains $\mathcal{B}_2(48n-10)$ for $\ell = 2$.*

Proof. By the discussion at the beginning of this section, there are two possibilities: if the derived subgroup G'_ℓ is all of $\mathrm{SL}_2(\mathbb{Z}_\ell)$, then the conclusion is obvious since $H_\ell = G_\ell$; if this is not the case, then H_ℓ satisfies the hypotheses of Corollary 6.5. Note that the image of $\mathrm{Gal}(\overline{K_\ell}/K_\ell)$ in $\mathrm{Aut}\, T_\ell(E)$ is exactly H_ℓ by construction. We wish to apply Corollary 6.5 to $G = H_\ell$, assuming that ℓ^{n-v} does not divide $D(\ell)$.

Since $\ell^{k(L)} \mid b_0(K_\ell, E)$ by Corollary 7.2, we deduce that $\ell^{n-k(L)-v}$ does not divide $b_0(K_\ell, E)^4 b_0(K_\ell, E \times E)$, and a fortiori $\ell^{n-k(L)+1-2v} \nmid b_0(K_\ell, E)^4 b_0(K_\ell, E \times E)$. Lemma 7.1 then implies that $G(\ell^{n-k(L)+1-2v})$ cannot be put in triangular form, and on the other hand $\ell^{n-v} \nmid b_0(K_\ell, E)^5 b_0(K_\ell, E \times E)$ implies that ℓ^{2n} does not divide $b_0(K_\ell, E)^4 b_0(K_\ell, E \times E)$, so $G(\ell^n)$ is not abelian (thanks to Proposition 7.4). It then follows from Corollary 6.5 that $G' = H'_\ell$ contains the principal congruence subgroup $\mathcal{B}_\ell(16n-4)$ (resp. $\mathcal{B}_\ell(48n-10)$ for $\ell = 2$). □

Corollary 7.6. *Let the notation be as above. The index $[\mathrm{SL}_2(\mathbb{Z}_\ell) : (H'_\ell \cap \mathcal{B}_\ell(1))]$ is of the form $|\mathrm{SL}_2(\mathbb{F}_\ell)| B(\ell)$, where for $\ell \neq 2$ the number $B(\ell)$ is a power of ℓ dividing $\ell^{33} \cdot D(\ell)^{48}$ (resp. $B(2)$ is a power of 2 dividing $2^{255} D(2)^{144}$).*

Proof. We can write the index $[\mathrm{SL}_2(\mathbb{Z}_\ell) : (H'_\ell \cap \mathcal{B}_\ell(1))]$ as

$$[\mathrm{SL}_2(\mathbb{Z}_\ell) : \mathcal{B}_\ell(1)] \cdot [\mathcal{B}_\ell(1) : (H'_\ell \cap \mathcal{B}_\ell(1))] = |\mathrm{SL}_2(\mathbb{F}_\ell)| \cdot [\mathcal{B}_\ell(1) : (H'_\ell \cap \mathcal{B}_\ell(1))],$$

so we just need to prove that $B(\ell) = [\mathcal{B}_\ell(1) : (H'_\ell \cap \mathcal{B}_\ell(1))]$ divides $\ell^{33} D(\ell)^{48}$ (and the analogous statement for $\ell = 2$). Notice that since $\mathcal{B}_\ell(1)$ is a pro-ℓ group, the number $B(\ell)$ is a power of ℓ.

Choose n such that $\ell^{n-v} \parallel D(\ell)$. Then $\ell^{n+1-v} \nmid D(\ell)$, and therefore the above theorem implies that H'_ℓ contains $\mathcal{B}_\ell(16(n+1)-4) \subseteq \mathcal{B}_\ell(1)$ (resp. $\mathcal{B}_2(48(n+1)-10)$ for $\ell = 2$): the index of $\mathcal{B}_\ell(16(n+1)-4)$ in $\mathcal{B}_\ell(1)$ is $\ell^{3(16(n+1)-5)}$, so we get

$$[\mathcal{B}_\ell(1) : (H'_\ell \cap \mathcal{B}_\ell(1))] \mid \ell^{48n+33} \mid \ell^{33} \cdot D(\ell)^{48}$$

for $\ell \neq 2$, and likewise we have

$$[\mathcal{B}_2(1) : (H'_2 \cap \mathcal{B}_2(1))] \mid 2^{3(48(n-1)+85)} \mid 2^{255} D(2)^{144}$$

for $\ell = 2$. □

8. The determinant and the large primes

We now turn to studying the determinant of the adelic representation and the behavior at the very large primes.

Proposition 8.1. *The index*

$$\Big[\widehat{\mathbb{Z}}^\times : \prod_\ell \det \rho_\ell(\mathrm{Gal}(\bar{K}/K))\Big]$$

is bounded by $[K : \mathbb{Q}]$.

Proof. The Weil pairing induces an identification of the determinant $\mathrm{Gal}(\bar{K}/K) \xrightarrow{\rho_\ell} G_\ell \xrightarrow{\det} \mathbb{Z}_\ell^\times$ with $\mathrm{Gal}(\bar{K}/K) \xrightarrow{\chi_\ell} \mathbb{Z}_\ell^\times$, where χ_ℓ denotes the ℓ-adic cyclotomic character. By Galois theory, we have

$$\prod_\ell \det \rho_\ell\big(\mathrm{Gal}(\bar{K}/K)\big) = \prod_\ell \chi_\ell\big(\mathrm{Gal}(\bar{K}/K)\big) \cong \mathrm{Gal}\big(K(\mu_\infty)/K\big).$$

Let $F = K \cap \mathbb{Q}(\mu_\infty)$, which is a finite Galois extension of $\mathbb{Q}$. As $\mathbb{Q}(\mu_\infty)$ is Galois over $\mathbb{Q}$, the restriction map $\mathrm{Gal}(K(\mu_\infty)/K) \to \mathrm{Gal}(\mathbb{Q}(\mu_\infty)/F)$ is well-defined and induces an isomorphism. Therefore

$$\begin{aligned}\Big[\widehat{\mathbb{Z}}^\times : \prod_\ell \chi_\ell(\mathrm{Gal}(\bar{K}/K))\Big] &= \big[\mathrm{Gal}\big(\mathbb{Q}(\mu_\infty)/\mathbb{Q}\big) : \mathrm{Gal}\big(\mathbb{Q}(\mu_\infty)/F\big)\big] \\ &= [F : \mathbb{Q}] \le [K : \mathbb{Q}],\end{aligned}$$

as claimed. □

We will also need a surjectivity result (on SL_2) modulo ℓ for every ℓ sufficiently large: as previously mentioned, these are essentially the ideas of [Masser and Wüstholz 1993c] and [Masser 1998], in turn inspired by those of Serre.

Lemma 8.2. *If* $\ell \nmid b_0(K, E \times E; 2) b_0(K, E; 60)$, *then the group* $G_\ell(\ell)$ *contains* $\mathrm{SL}_2(\mathbb{F}_\ell)$.

Proof. Let ℓ be a prime for which $G_\ell(\ell)$ does not contain $\mathrm{SL}_2(\mathbb{F}_\ell)$ and let, for the sake of clarity, $G = G_\ell(\ell)$. By Theorem 3.13, if G does not contain $\mathrm{SL}_2(\mathbb{F}_\ell)$, then the following are the only possibilities:

(I) G is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$: by definition, such a subgroup fixes a line, therefore $\ell \mid b_0(K, E)$ by Lemma 7.1.

(II) G is contained in the normalizer of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$: let $\mathcal{C}$ be this Cartan subgroup and N its normalizer. By Dickson's classification, $\mathcal{C}$ has index 2 in N, so the morphism

$$\mathrm{Gal}(\bar{K}/K) \to G \to \frac{G}{G \cap \mathcal{C}} \hookrightarrow \frac{N}{\mathcal{C}}$$

induces a quadratic character of $\mathrm{Gal}(\overline{K}/K)$, whose kernel corresponds to a certain field K' satisfying $[K' : K] \le |N/\mathcal{C}| = 2$. By construction, the image of $\mathrm{Gal}(\overline{K'}/K')$ in $\mathrm{Aut}(E[\ell])$ is contained in $\mathcal{C}$, so applying Proposition 7.4 to $E_{K'}$ we get

$$\ell \mid b_0(K', E) b_0(K', E \times E) \mid b_0(K, E; 2) b_0(K, E \times E; 2).$$

Notice that this also covers the case of G being contained in a Cartan subgroup.

(III) The projectivization $\mathbb{P}G$ of G is a finite group of order at most 60: we essentially copy the previous argument. Let $H = \mathbb{P}G$; then we have a morphism

$$\mathrm{Gal}(\overline{K}/K) \to G \to \frac{\mathbb{F}_\ell^\times G}{\mathbb{F}_\ell^\times} = H$$

whose kernel defines an extension K'' of K with $[K'' : K] = |H| \le 60$ and such that the image of the representation of $\mathrm{Gal}(\overline{K''}/K'')$ on $E[\ell]$ is contained in $\mathbb{F}_\ell^\times$: Lemma 7.1 then yields $\ell \mid b_0(K'', E) \mid b_0(K, E; 60)$.

It is then apparent that the lemma is true with the condition

$$\ell \nmid b_0(K, E) b_0(K, E \times E) b_0(K, E; 2) b(K, E \times E; 2) b_0(K, E; 60);$$

however, since

$$b_0(K, E) \mid b_0(K, E; 2) \mid b_0(K, E; 60), \quad b_0(K, E \times E) \mid b_0(K, E \times E; 2),$$

and since ℓ is prime, we see that ℓ divides

$$b_0(K, E) b_0(K, E \times E) b_0(K, E; 2) b_0(K, E \times E; 2) b_0(K, E; 60)$$

if and only if it divides $b(K, E \times E; 2) b_0(K, E; 60)$, which finishes the proof. □

Corollary 8.3. *Let* $\Psi = 30 \cdot b_0(K, E \times E; 2) b_0(K, E; 60)$. *If* $\ell \nmid \Psi$, *then* G'_ℓ *is all of* $\mathrm{SL}_2(\mathbb{Z}_\ell)$.

Proof. The previous lemma implies that $G_\ell(\ell)$ contains $\mathrm{SL}_2(\mathbb{F}_\ell)$, and by hypothesis ℓ is strictly larger than 3, so the corollary follows from Lemma 3.15. □

9. The adelic index and some consequences

We have thus acquired a good understanding of the ℓ-adic representation for every prime ℓ, and we are now left with the task of bounding the overall index of the full adelic representation. The statement we are aiming for is:

Theorem 9.1. *Let* E/K *be an elliptic curve without complex multiplication with stable Faltings height* $h(E)$. *Let* $\rho_\infty : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2\left(\widehat{\mathbb{Z}}\right)$ *be the adelic Galois representation associated with* E, *and set*

$$\Psi = 2 \cdot 3 \cdot 5 \cdot b_0(K, E \times E; 2) b_0(K, E; 60), \; D(\infty) = b_0(K, E; 24)^5 b_0(K, E \times E; 24).$$

Let moreover K_2 be as in Section 7 and put

$$D(2) = b_0(K_2, E)^5 b_0(K_2, E \times E).$$

With this notation, we have

$$\left[\mathrm{GL}_2\left(\widehat{\mathbb{Z}}\right) : \rho_\infty \mathrm{Gal}(\overline{K}/K)\right] \leq [K : \mathbb{Q}] \cdot 2^{222} \cdot D(2)^{144} \cdot \mathrm{rad}(\Psi)^{36} \cdot D(\infty)^{48},$$

where $\mathrm{rad}(\Psi) = \prod_{\ell | \Psi} \ell$ *is the product of the primes dividing* Ψ.

The strategy of proof, which essentially goes back to Serre, is to pass to a suitable extension of K over which the adelic representation decomposes as a direct product and then use the previous bounds. For this, we will need some preliminaries. If L is any number field, we let $L_{\mathrm{cyc}} = L(\mu_\infty)$ be its maximal cyclotomic extension. From the exact sequence

$$1 \to \frac{\mathrm{SL}_2(\widehat{\mathbb{Z}})}{\mathrm{Gal}(\overline{K}/K_{\mathrm{cyc}})} \to \frac{\mathrm{GL}_2(\widehat{\mathbb{Z}})}{\rho_\infty\big(\mathrm{Gal}(\overline{K}/K)\big)} \to \frac{\widehat{\mathbb{Z}}^\times}{\det \circ \rho_\infty\big(\mathrm{Gal}(\overline{K}/K)\big)} \to 1$$

we see that $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_\infty\big(\mathrm{Gal}(\overline{K}/K)\big)]$ equals

$$[\widehat{\mathbb{Z}}^\times : \det \circ \rho_\infty\big(\mathrm{Gal}(\overline{K}/K)\big)] \cdot [\mathrm{SL}_2(\widehat{\mathbb{Z}}) : \rho_\infty\big(\mathrm{Gal}(\overline{K}/K_{\mathrm{cyc}})\big)],$$

where the first term is bounded by $[K : \mathbb{Q}]$ thanks to Proposition 8.1. It thus remains to understand the term $[\mathrm{SL}_2(\widehat{\mathbb{Z}}) : \rho_\infty\big(\mathrm{Gal}(\overline{K}/K_{\mathrm{cyc}})\big)]$. Let $\mathcal{P}$ be the (finite) set consisting of 2, 3, 5, and the prime numbers ℓ for which G_ℓ does not contain $\mathrm{SL}_2(\mathbb{Z}_\ell)$, and let F be the field generated over K by $\bigcup_{\ell \in \mathcal{P}} E[\ell]$. It is clear that

$$[\mathrm{SL}_2(\widehat{\mathbb{Z}}) : \rho_\infty\big(\mathrm{Gal}(\overline{K}/K_{\mathrm{cyc}})\big)] \leq [\mathrm{SL}_2(\widehat{\mathbb{Z}}) : \rho_\infty\big(\mathrm{Gal}(\overline{K}/F_{\mathrm{cyc}})\big)].$$

Notation. We set $S = \rho_\infty\big(\mathrm{Gal}(\overline{K}/F_{\mathrm{cyc}})\big) \subseteq \mathrm{SL}_2(\widehat{\mathbb{Z}}) = \prod_\ell \mathrm{SL}_2(\mathbb{Z}_\ell)$ and let S_ℓ be the projection of S on $\mathrm{SL}_2(\mathbb{Z}_\ell)$.

The core of the argument is contained in the following proposition.

Proposition 9.2. *Let $B(\ell)$ be as in Corollary 7.6 and $D(2)$ be as in the statement of Theorem 9.1. The following hold*:

(1) $S = \prod_\ell S_\ell$.

(2) *For $\ell \in \mathcal{P}$, $\ell \neq 2$, we have*

$$\left[\mathrm{SL}_2(\mathbb{Z}_\ell) : S_\ell\right] \mid (|\mathrm{SL}_2(\mathbb{F}_\ell)| \cdot B(\ell));$$

for $\ell = 2$, we have

$$\left[\mathrm{SL}_2(\mathbb{Z}_2) : S_2\right] < 2^{258} D(2)^{144}.$$

(3) *For $\ell \notin \mathcal{P}$, the equality $S_\ell = \mathrm{SL}_2(\mathbb{Z}_\ell)$ holds.*

Proof. (1) This would follow from [Serre 2013, Théorème 1], but since we do not need the added generality and the proof is quite short we include it here for the reader's convenience.

Regard S as a closed subgroup of $\prod_\ell S_\ell \subseteq \prod_\ell \mathrm{SL}_2(\mathbb{Z}_\ell) = \mathrm{SL}_2(\widehat{\mathbb{Z}})$. For each finite set of primes B, let $p_B\colon S \to S_B = \prod_{\ell\in B} S_\ell$ be the canonical projection. We plan to show that for every such B containing $\mathcal{P}$ we have $p_B(S) = S_B$. Indeed let us consider the case $B = \mathcal{P}$ first. Our choice of F implies that $S_\ell = \rho_\ell(\mathrm{Gal}(\overline{F}/F))$ is a pro-ℓ group for every $\ell \in \mathcal{P}$: the group S_ℓ has trivial reduction modulo ℓ by construction, and therefore S_ℓ admits the usual congruence filtration by the kernels of the reductions modulo ℓ^k for varying k. Now a pro-ℓ group is obviously pronilpotent, so $p_B(S)$ is pronilpotent as well and therefore it is the product of its pro-Sylow subgroups (which are just the S_ℓ). To treat the general case, we recall some terminology from [Serre 1998]. Following Serre, we say that a finite simple group Σ *occurs* in the profinite group Y if there exist a closed subgroup Y_1 of Y and an open normal subgroup Y_2 of Y_1 such that $\Sigma \cong Y_1/Y_2$. We also write $\mathrm{Occ}(Y)$ for the set of isomorphism classes of finite simple nonabelian groups occurring in Y. From [Serre 1998, IV-25] we obtain the following description of the sets $\mathrm{Occ}(\mathrm{GL}_2(\mathbb{Z}_p))$:

- $\mathrm{Occ}(\mathrm{GL}_2(\mathbb{Z}_p)) = \varnothing$ for $p = 2, 3$;
- $\mathrm{Occ}(\mathrm{GL}_2(\mathbb{Z}_5)) = \{A_5\}$;
- $\mathrm{Occ}(\mathrm{GL}_2(\mathbb{Z}_p)) = \{\mathrm{PSL}_2(\mathbb{F}_p), A_5\}$ for $p \equiv \pm 1 \pmod 5$, $p > 5$;
- $\mathrm{Occ}(\mathrm{GL}_2(\mathbb{Z}_p)) = \{\mathrm{PSL}_2(\mathbb{F}_p)\}$ for $p \equiv \pm 2 \pmod 5$, $p > 5$.

Let B be a finite set of primes containing $\mathcal{P}$ and satisfying $p_B(S) = S_B$, and fix a prime $\ell_0 \notin B$. We claim that $p_{B\cup\{\ell_0\}}(S) = S_{B\cup\{\ell_0\}}$. Notice first that $\mathrm{PSL}_2(\mathbb{F}_{\ell_0})$ occurs in S_{ℓ_0} and therefore in $p_{B\cup\{\ell_0\}}(S)$. Set $N_{\ell_0} = \ker(p_{B\cup\{\ell_0\}}(S) \to p_B(S))$. From the exact sequence

$$1 \to N_{\ell_0} \to p_{B\cup\{\ell_0\}}(S) \to p_B(S) \to 1, \tag{9-1}$$

we see that $\mathrm{Occ}(p_{B\cup\{\ell_0\}}(S)) = \mathrm{Occ}(p_B(S)) \cup \mathrm{Occ}(N_{\ell_0})$. On the other hand, the only finite nonabelian simple groups that can occur in $p_B(S)$ are A_5 and groups of the form $\mathrm{PSL}_2(\mathbb{F}_\ell)$ for $\ell \neq \ell_0$, so $\mathrm{PSL}_2(\mathbb{F}_{\ell_0})$ does not occur in $p_B(S)$ (notice that $\mathrm{PSL}_2(\mathbb{F}_{\ell_0}) \ncong A_5$ since $\ell_0 \neq 5$), and therefore it must occur in N_{ℓ_0}. Denote by $\overline{N_{\ell_0}}$ the image of N_{ℓ_0} in $\mathrm{SL}_2(\mathbb{F}_{\ell_0})$. The kernel of $N_{\ell_0} \to \mathrm{SL}_2(\mathbb{F}_{\ell_0})$ is a pro-ℓ_0 group, so $\mathrm{Occ}\left(N_{\ell_0}\right)$ equals $\mathrm{Occ}\left(\overline{N_{\ell_0}}\right)$ and therefore $\overline{N_{\ell_0}}$ projects surjectively onto $\mathrm{PSL}_2(\mathbb{F}_{\ell_0})$. Hence we have $\overline{N_{\ell_0}} = \mathrm{SL}_2(\mathbb{F}_{\ell_0})$ by [Serre 1998, IV-23, Lemma 2], and by Lemma 3.15 this implies $N_{\ell_0} = \mathrm{SL}_2(\mathbb{Z}_{\ell_0})$: by (9-1) we then have $p_{B\cup\{\ell_0\}}(S) = p_B(S) \times \mathrm{SL}_2(\mathbb{Z}_{\ell_0})$, as claimed. By induction, the equality $p_B(S) = S_B$ holds for any finite set of primes B containing $\mathcal{P}$, and since S is profinite we deduce that $S = \prod_\ell S_\ell$.

(2) The group S_ℓ is the kernel of the projection map $(G_\ell \cap \mathrm{SL}_2(\mathbb{Z}_\ell)) \to \mathrm{SL}_2(\mathbb{F}_\ell)$; as such, it contains the intersection $H'_\ell \cap B_\ell(1)$ (notation as in Section 7), so we just need to invoke Corollary 7.6 to have

$$\big[\,\mathrm{SL}_2(\mathbb{Z}_\ell) : S_\ell\big] \mid \big[\,\mathrm{SL}_2(\mathbb{Z}_\ell) : (H'_\ell \cap B_\ell(1))\big] \mid |\mathrm{SL}_2(\mathbb{F}_\ell)|B(\ell),$$

as claimed. On the other hand, the group H_2 is a subgroup of $\rho_2\big(\mathrm{Gal}(\overline{K}/K(E[4]))\big)$ for $\ell = 2$, while S_2 is $\rho_2\big(\mathrm{Gal}(\overline{K}/K_{\mathrm{cyc}}(E[2]))\big)$, so S_2 is larger than $H'_2 \cap \mathcal{B}_2(1)$ and we can again use the bound of Corollary 7.6, which now reads

$$\big[\,\mathrm{SL}_2(\mathbb{Z}_2) : S_2\big] \leq 2^{255} D(2)^{144} |\mathrm{SL}_2(\mathbb{F}_2)| < 2^{258} D(2)^{144}.$$

(3) As $\ell \notin \mathcal{P}$, we know that $\rho_\ell(\mathrm{Gal}(\overline{K}/K))$ contains $\mathrm{SL}_2(\mathbb{Z}_\ell)$, so $\mathrm{PSL}_2(\mathbb{F}_\ell)$ occurs in $\rho_\ell(\mathrm{Gal}(\overline{K}/K))$. Consider the Galois group $\mathrm{Gal}(F/K)$: it is by construction a subquotient of $\prod_{p\in\mathcal{P}} \mathrm{GL}_2(\mathbb{Z}_p)$, so the only groups that can occur in it are those in $\bigcup_{p\in\mathcal{P}} \mathrm{Occ}(\mathrm{GL}_2(\mathbb{Z}_p))$, and in particular $\mathrm{PSL}_2(\mathbb{F}_\ell)$ does not occur in $\mathrm{Gal}(F/K)$. Now $\rho_\ell(\mathrm{Gal}(\overline{K}/K))$ is an extension of a quotient of $\mathrm{Gal}(F/K)$ by $\rho_\ell(\mathrm{Gal}(\overline{K}/F))$, so $\mathrm{PSL}_2(\mathbb{F}_\ell)$ occurs in $\rho_\ell\big(\mathrm{Gal}(\overline{K}/F)\big)$, and furthermore $\rho_\ell(\mathrm{Gal}(\overline{K}/F))$ is an extension of an abelian group by $\rho_\ell(\mathrm{Gal}(\overline{K}/F_{\mathrm{cyc}}))$, so the group $\mathrm{PSL}_2(\mathbb{F}_\ell)$ also occurs in $\rho_\ell(\mathrm{Gal}(\overline{K}/F_{\mathrm{cyc}})) = S_\ell$: reasoning as in (1), we then see that S_ℓ projects surjectively onto $\mathrm{PSL}_2(\mathbb{F}_\ell)$, and therefore $S_\ell = \mathrm{SL}_2(\mathbb{Z}_\ell)$. □

The proof of Theorem 9.1 is now immediate:

Proof of Theorem 9.1. We have already seen that $\big[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_\infty(\mathrm{Gal}(\overline{K}/K))\big]$ equals $[\mathbb{Z}^\times : \det\circ\rho_\infty\,\mathrm{Gal}(\overline{K}/K)] \cdot [\mathrm{SL}_2(\widehat{\mathbb{Z}}) : \rho_\infty(\mathrm{Gal}(\overline{K}/K_{\mathrm{cyc}}))]$. Now the first factor in this product is at most $[K : \mathbb{Q}]$, while the second is bounded by $[\mathrm{SL}_2(\widehat{\mathbb{Z}}) : S]$; it follows that the adelic index is bounded by

$$\begin{aligned}
[K : \mathbb{Q}] \cdot [\mathrm{SL}_2(\widehat{\mathbb{Z}}) : S] &\leq [K : \mathbb{Q}] \cdot \prod_{\ell\in\mathcal{P}} [\mathrm{SL}_2(\mathbb{Z}_\ell) : S_\ell] \\
&\leq [K : \mathbb{Q}] \cdot \prod_{\ell\mid\Psi} [\mathrm{SL}_2(\mathbb{Z}_\ell) : S_\ell] \\
&< [K : \mathbb{Q}] \cdot 2^{258} \cdot D(2)^{144} \cdot \prod_{\ell\mid\Psi,\ell\neq 2} |\mathrm{SL}_2(\mathbb{F}_\ell)| \cdot \prod_{\ell\mid\Psi,\ell\neq 2} B(\ell),
\end{aligned} \tag{9-2}$$

where we have used the fact that $\ell \nmid \Psi \Rightarrow \ell \notin \mathcal{P}$. We now observe that, by construction, for all odd primes ℓ we have $v_\ell(D(\infty)) \geq v_\ell(D(\ell))$, so by Corollary 7.6 the quantity $\prod_{\ell\mid\Psi,\ell\neq 2} B(\ell)$ divides

$$\prod_{\ell\mid\Psi,\ell\neq 2} \ell^{33}\ell^{48v_\ell(D(\ell))} \mid \prod_{\ell\mid\Psi,\ell\neq 2} \ell^{33}\ell^{48v_\ell(D(\infty))},$$

which in turn divides $\left(\frac{\mathrm{rad}(\Psi)}{2}\right)^{33} \cdot D(\infty)^{48}$. Combining this fact with Equation (9-2) and the trivial bound $|\mathrm{SL}_2(\mathbb{F}_\ell)| < \ell^3$ we find that the adelic index is at most

$$[K:\mathbb{Q}] \cdot 2^{225} \cdot D(2)^{144} \cdot \left(\prod_{\ell \mid \Psi, \ell \neq 2} \ell^3 \right) \cdot \mathrm{rad}(\Psi)^{33} \cdot D(\infty)^{48},$$

which in turn is less than $[K:\mathbb{Q}] \cdot 2^{222} \cdot D(2)^{144} \cdot \mathrm{rad}(\Psi)^{36} \cdot D(\infty)^{48}$, whence the theorem. □

Using the estimates of Proposition 2.6 to bound Ψ, $D(2)$ and $D(\infty)$, we get:

Corollary 9.3. *Let E/K be an elliptic curve that does not admit complex multiplication. The inequality*

$$[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_\infty\big(\mathrm{Gal}(\overline{K}/K)\big)] < \gamma_1 \cdot [K:\mathbb{Q}]^{\gamma_2} \cdot \max\big\{1, h(E), \log[K:\mathbb{Q}]\big\}^{2\gamma_2}$$

holds, where $\gamma_1 = \exp(10^{21483})$ and $\gamma_2 = 2.4 \cdot 10^{10}$.

Remark 9.4. With some work, the techniques used in [Le Fourn 2015] (cf. especially Theorem 4.2 of *op. cit.*) could be used to improve the above bound on Ψ; unfortunately, the same methods do not seem to be easily applicable to bound $D(\infty)$. Notice that our estimates for Ψ and $D(\infty)$ are essentially of the same order of magnitude, so using a finer bound for Ψ without changing the one for $D(\infty)$ would only yield a minor improvement of the final result.

On the other hand, it is easy to see that using the improved version of the isogeny theorem mentioned in Remarks 2.3 and 2.7, one can prove

$$\big[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : \rho_\infty\big(\mathrm{Gal}(\overline{K}/K)\big)\big] < \gamma_3 \cdot \big([K:\mathbb{Q}] \cdot \max\big\{1, h(E), \log[K:\mathbb{Q}]\big\}\big)^{\gamma_4}$$

with $\gamma_3 = \exp(1.9 \cdot 10^{10})$ and $\gamma_4 = 12395$.

The field generated by a torsion point. As an easy consequence of our main result, we can also prove:

Corollary 9.5. *Let E/K be an elliptic curve that does not admit complex multiplication. There exists a constant $\gamma(E/K)$ such that the inequality*

$$[K(x):K] \geq \gamma(E/K) N(x)^2$$

holds for every $x \in E_{\mathrm{tors}}(\overline{K})$. Here, $N(x)$ denotes the order of x. We can take $\gamma(E/K) = (\zeta(2) \cdot [\mathrm{GL}_2\left(\widehat{\mathbb{Z}}\right) : \rho_\infty \mathrm{Gal}(\overline{K}/K)])^{-1}$, which can be explicitly bounded thanks to the main theorem.

Proof. For any such x, set $N = N(x)$ and choose a point $y \in E[N]$ such that (x, y) is a basis of $E[N]$ as $(\mathbb{Z}/N\mathbb{Z})$-module. Let $G(N)$ be the image of $\mathrm{Gal}(\overline{K}/K)$ inside $\mathrm{Aut}\, E[N]$, which we identify with $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ via the basis (x, y). We have a tower of extensions $K(E[N])/K(x)/K$, where $K(E[N])$ is Galois over K and

therefore over $K(x)$. The Galois groups of these extensions are given — essentially by definition — by

$$\mathrm{Gal}(K(E[N])/K) = G(N) \quad \text{and} \quad \mathrm{Gal}(K(E[N])/K(x)) = \mathrm{Stab}(x),$$

where $\mathrm{Stab}(x) = \{\sigma \in G(N) \mid \sigma(x) = x\}$. It follows that

$$[K(x) : K] = \frac{[K(E[N]) : K]}{[K(E[N]) : K(x)]} = \frac{|G(N)|}{|\mathrm{Stab}(x)|},$$

and furthermore it is easy to check that

$$|G(N)| = \frac{|\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})|}{[\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : G(N)]} = \frac{N^3\varphi(N)\prod_{p|N}\left(1-\frac{1}{p^2}\right)}{[\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : G(N)]}.$$

On the other hand, the stabilizer of x in $G(N)$ is contained in the stabilizer of x in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, which is simply

$$\left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \,\middle|\, a \in \mathbb{Z}/N\mathbb{Z},\ b \in (\mathbb{Z}/N\mathbb{Z})^\times \right\},$$

so $|\mathrm{Stab}(x)| \leq |\mathbb{Z}/N\mathbb{Z}| \cdot |(\mathbb{Z}/N\mathbb{Z})^\times| = N\varphi(N)$. Finally, the index of $G(N)$ inside $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is certainly not larger than the index of G_∞ inside $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. Putting everything together we obtain

$$[K(x) : K] = \frac{N^3\varphi(N)\prod_{p|N}\left(1-\frac{1}{p^2}\right)}{[\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : G(N)] \cdot |\mathrm{Stab}(x)|} \geq \frac{N^3\varphi(N)\prod_{p \text{ prime}}\left(1-\frac{1}{p^2}\right)}{N\varphi(N) \cdot [\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G_\infty]},$$

and the corollary follows by remarking that $\prod_{p \text{ prime}}\left(1-\frac{1}{p^2}\right) = \frac{1}{\zeta(2)}$. □

Acknowledgements

It is a pleasure to thank my advisor, N. Ratazzi, for suggesting the problem, for his unfailing support, and for the many helpful discussions. I am grateful to the anonymous referee for the numerous helpful suggestions. I would also like to thank G. Rémond and É. Gaudron for their many valuable comments on a preliminary version of this text, and J.-P. Serre for pointing out a problem in a later version. The author gratefully acknowledges financial support from the Fondation Mathématique Jacques Hadamard (grant ANR-10-CAMP-0151-02 in the "Programme des Investissements d'Avenir").

References

[Gaudron and Rémond 2014] É. Gaudron and G. Rémond, "Polarisations et isogénies", *Duke Math. J.* **163**:11 (2014), 2057–2108. MR 3263028 Zbl 1303.11068

[Le Fourn 2015] S. Le Fourn, "Surjectivity of Galois representations associated with quadratic Q-curves", *Math. Ann.* (online publication August 2015).

[Masser 1989] D. W. Masser, "Counting points of small height on elliptic curves", *Bull. Soc. Math. France* **117**:2 (1989), 247–265. MR 90k:11068 Zbl 0723.14026

[Masser 1998] D. Masser, "Multiplicative isogeny estimates", *J. Austral. Math. Soc. Ser. A* **64**:2 (1998), 178–194. MR 2000a:11089 Zbl 0906.11031

[Masser and Wüstholz 1989] D. W. Masser and G. Wüstholz, "Some effective estimates for elliptic curves", pp. 103–109 in *Arithmetic of complex manifolds* (Erlangen, 1988), edited by W. P. Barth and H. Lange, Lecture Notes in Math. **1399**, Springer, Berlin, 1989. MR 90j:11046 Zbl 0701.14034

[Masser and Wüstholz 1993a] D. Masser and G. Wüstholz, "Isogeny estimates for abelian varieties, and finiteness theorems", *Ann. of Math.* (2) **137**:3 (1993), 459–472. MR 95d:11074 Zbl 0804.14019

[Masser and Wüstholz 1993b] D. Masser and G. Wüstholz, "Periods and minimal abelian subvarieties", *Ann. of Math.* (2) **137**:2 (1993), 407–458. MR 94g:11040 Zbl 0796.11023

[Masser and Wüstholz 1993c] D. W. Masser and G. Wüstholz, "Galois properties of division fields of elliptic curves", *Bull. London Math. Soc.* **25**:3 (1993), 247–254. MR 94d:11036 Zbl 0809.14026

[Pink 1993] R. Pink, "Classification of pro-p subgroups of SL_2 over a p-adic ring, where p is an odd prime", *Compositio Math.* **88**:3 (1993), 251–264. MR 94m:20066 Zbl 0820.20055

[Serre 1972] J.-P. Serre, "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques", *Invent. Math.* **15**:4 (1972), 259–331. MR 52 #8126 Zbl 0235.14012

[Serre 1998] J.-P. Serre, *Abelian ℓ-adic representations and elliptic curves*, Research Notes in Mathematics **7**, A K Peters, Ltd., Wellesley, MA, 1998. MR 98g:11066 Zbl 0902.14016

[Serre 2013] J.-P. Serre, "Un critère d'indépendance pour une famille de représentations ℓ-adiques", *Comment. Math. Helv.* **88**:3 (2013), 541–554. MR 3093502 Zbl 1317.14040

[Zywina 2011] D. Zywina, "Bounds for Serre's open image theorem", preprint, 2011. arXiv 1102.4656

Communicated by Barry Mazur
Received 2015-05-07 Revised 2015-09-01 Accepted 2015-10-06

davide.lombardo@math.u-psud.fr

Département de Mathématiques Bâtiment 425,
Université Paris-Sud 11, Faculté des Sciences d'Orsay,
91405 Orsay Cedex, France

ALGEBRA AND NUMBER THEORY 9:10 (2015)
dx.doi.org/10.2140/ant.2015.9.2397

On 0-cycles with modulus

Amalendu Krishna

Given a nonsingular surface X over a field and an effective Cartier divisor D, we provide an exact sequence connecting $\mathrm{CH}_0(X, D)$ and the relative K-group $K_0(X, D)$. We use this exact sequence to answer a question of Kerz and Saito whenever X is a resolution of singularities of a normal surface. This exact sequence and two vanishing theorems are used to show that the localization sequence for ordinary Chow groups does not extend to Chow groups with modulus. This in turn shows that the additive Chow groups of 0-cycles on smooth projective schemes cannot always be represented as reciprocity functors.

1. Introduction

The idea of algebraic cycles with modulus was first conceived by Bloch and Esnault [2003b; 2003a]. One main motivation behind such a theory is to develop a theory of motivic cohomology which can describe the relative K-theory of smooth schemes relative to closed subschemes. A potential candidate for such a theory was later constructed and studied by Park [2009], Krishna and Levine [2008] and more recently by Kerz and Saito [2015] and Binda and Saito [2014]. It was conjectured in [Krishna and Levine 2008] that there should exist a spectral sequence consisting of these motivic cohomology groups whose abutment is the relative K-theory.

The results of this text were partly motivated by the following question of Kerz and Saito [2015, Question V]. Let X be a smooth quasiprojective scheme of dimension d over a field k and let $D \hookrightarrow X$ be an effective Cartier divisor. Let $\mathrm{CH}_0(X, D)$ denote the Chow group 0-cycles on X with modulus D. Let $\mathcal{K}^M_{d,(X,D)}$ denote the relative Milnor K-theory sheaf on X. Let U be an open subscheme of X whose complement is a divisor.

Question 1.1. Assume that X is projective and k is a perfect field of positive characteristic. Is there an isomorphism

$$\varprojlim_D \mathrm{CH}_0(X, D) \xrightarrow{\sim} \varprojlim_D H^d_{\mathrm{nis}}(X, \mathcal{K}^M_{d,(X,D)}),$$

where the limits are taken over all effective divisors on X with support outside U?

MSC2010: primary 14C25; secondary 14F30, 14G40.
Keywords: algebraic cycles, modulus condition, K-theory.

It follows from the main results of [Kato and Saito 1986; 2015] and [Rülling and Saito 2015] that this question has a positive solution if k is finite and the support of $X \setminus U$ is a normal crossing divisor. As explained in [Kerz and Saito 2015], the above question is part of the bigger question of whether the Chow groups with modulus satisfy Nisnevich or Zariski descent. As we shall see shortly, the above question is also directly related to the conjectured connection between the cycles with modulus and the relative K-theory.

Main results. Let $\mathrm{Pic}(X, D)$ denote the isomorphism classes of pairs $(\mathcal{L}, \phi)$, where $\mathcal{L}$ is a line bundle on X and ϕ is an isomorphism $\phi : \mathcal{L}|_D \xrightarrow{\sim} \mathcal{O}_D$. We prove the following result as a partial answer to the above question.

Theorem 1.2. *Let k be any field and let X be a nonsingular quasiprojective surface over k with an effective Cartier divisor D. Then there is an exact sequence*

$$\mathrm{CH}_0(X, D) \xrightarrow{\mathrm{cyc}_{(X,D)}} K_0(X, D) \longrightarrow \mathrm{Pic}(X, D) \longrightarrow 0. \tag{1-1}$$

In particular, $\mathrm{cyc}_{(X,D)}$ *induces a surjective map* $\mathrm{CH}_0(X, D) \twoheadrightarrow H^2_{\mathrm{nis}}(X, \mathcal{K}^M_{2,(X,D)})$.

Remark 1.3. The map $\mathrm{cyc}_{(X,D)}$ turns out to be injective as well if X is affine. A proof of this using completely different type of argument will appear in [Binda and Krishna $\geq$ 2015].

Let us now assume that X is a resolution of singularities of a normal surface Y and let U denote the regular locus of Y. Then we can use Theorem 1.2 to obtain the following finer result which fully answers Question 1.1 for a special class of surfaces.

Theorem 1.4. *Let k be any field and let X be a resolution of singularities of a normal surface Y. Let U denote the regular locus of Y. Then the cycle class map* $\mathrm{CH}_0(X, D) \to H^2_{\mathrm{nis}}(X, \mathcal{K}^M_{2,(X,D)})$ *induces an isomorphism*

$$\varprojlim_D \mathrm{CH}_0(X, D) \xrightarrow{\sim} \varprojlim_D H^2_{\mathrm{nis}}(X, \mathcal{K}^M_{2,(X,D)}),$$

where the limits are taken over all effective divisors on X with support outside U.

Localization sequence for Chow groups with modulus. Since the introduction of the Chow groups with modulus, various authors have been trying to prove several properties of these Chow groups which are analogous to the well-known properties of Bloch's higher Chow groups. It was shown in [Krishna and Park 2014] recently that the Chow groups with modulus satisfy projective bundle and blowup formulas. It was however not known if the localization sequence for Bloch's higher Chow groups is true for Chow groups with modulus. We use Theorem 1.2 to show that the Chow groups with modulus do not admit such a localization sequence. In fact, we show that even the localization sequence for the ordinary Chow groups (in the

sense of [Fulton 1998]) does not admit extension to Chow groups with modulus. Answering this question was another motivation of this note.

Let $m \geq 2$ be any integer and let D denote the Cartier divisor $\mathrm{Spec}(k[t]/(t^m))$ inside $\mathrm{Spec}(k[t])$. For any $Y \in \mathbf{Sch}/k$, the Cartier divisor $Y \times D \hookrightarrow Y \times \mathbb{A}^1_k$ is denoted by D itself.

Theorem 1.5. *Let k be an algebraically closed field of characteristic zero with infinite transcendence degree over $\mathbb{Q}$. Let Y be a connected projective curve over k of positive genus. Then for any inclusion $i : \{P\} \hookrightarrow Y$ of a closed point, the sequence*

$$\mathrm{CH}_0(\{P\} \times \mathbb{A}^1_k, D) \xrightarrow{i_*} \mathrm{CH}_0(Y \times \mathbb{A}^1_k, D) \xrightarrow{j^*} \mathrm{CH}_0(Y \setminus \{P\} \times \mathbb{A}^1_k, D) \longrightarrow 0$$

is not exact.

In particular, the localization sequence for Bloch's higher Chow groups does not extend to the Chow groups with modulus, even for a closed pair of smooth schemes.

The proof of this negative result is based on Theorem 1.2 and the following two vanishing theorems of independent interest.

Theorem 1.6. *Let k be any field and let Y be any nonsingular affine scheme over k of dimension $d \geq 1$. Then $\mathrm{CH}_0(Y \times \mathbb{A}^1_k, D) = 0$.*

Theorem 1.7. *Let k be an algebraic closure of a finite field and let X be a smooth affine scheme over k of dimension $d \geq 3$. Then for any effective Cartier divisor $D \hookrightarrow X$, we have $\mathrm{CH}_0(X, D) = 0$. Assuming D_{red} is a normal crossing divisor, we also have $H^d_{\mathrm{nis}}(X, \mathcal{K}^M_{d,(X,D)}) = 0$.*

Remark 1.8. Theorem 1.7 implies that the analogue of Question 1.1 has a positive solution for affine schemes over k of dimension at least three if D_{red} is a normal crossing divisor.

Remark 1.9. The assertion of Theorem 1.7 is true also for $d = 2$ and will appear in [Binda and Krishna $\geq$ 2015]. The proof in this note does show at least that $\mathrm{CH}_0(X, D)_{\mathbb{Q}} = 0$ even if X is a surface.

On the other hand, it is easily seen using the surjection $\mathrm{CH}_0(X, D) \twoheadrightarrow \mathrm{CH}_0(X)$ that $d \geq 2$ is a necessary condition for the vanishing of $\mathrm{CH}_0(X, D)$.

Additive Chow groups and reciprocity functors. Ivorra and Rülling [$\geq$ 2015] introduced the reciprocity functors $T(\mathcal{M}_1, \cdots, \mathcal{M}_r)$. These reciprocity functors are expected to describe the ordinary as well as the additive higher Chow groups of 0-cycles for smooth projective schemes over a field. In this direction, it was shown by Ivorra and Rülling [$\geq$ 2015, Corollary 5.2.5] that for a smooth projective scheme X of dimension d over a field k, there is an isomorphism $T(\mathbb{G}_m^{\times r}, \mathrm{CH}_0(X))(k) \simeq \mathrm{CH}^{d+r}(X, r)$. They also show that $T(\mathbb{G}_a, \mathrm{CH}_0(\mathrm{Spec}(k)))(k) \simeq \mathrm{CH}_0(\mathbb{A}^1_k, D_2)$ if $\mathrm{char}(k) = 0$, where $D_2 = \mathrm{Spec}(k[t]/(t^2))$. This was a verification of a special case of the general expectation that $T(\mathbb{G}_a, \mathrm{CH}_0(X))(k)$ should be isomorphic to

the additive Chow group $\mathrm{CH}_0(X \times \mathbb{A}^1_k, D_2)$ if X is a smooth projective scheme over k. However, combining Theorems 1.5 and 1.6 with [Rülling and Yamazaki 2014, Theorem 1.1], we prove:

Corollary 1.10. *Let k be an algebraically closed field of characteristic zero with infinite transcendence degree over $\mathbb{Q}$. Let Y be a connected projective curve over k of positive genus. Then $\mathrm{CH}_0(Y \times \mathbb{A}^1_k, D_2)$ cannot be described in terms of the reciprocity functors.*

Outline of proofs. We recall the definitions of Chow groups with modulus in Section 2. We then use the Thomason–Trobaugh spectral sequence to relate the cohomology of the sheaf $\mathcal{K}^M_{2,(X,D)}$ with the relative K-groups. We first prove an analogue of Theorem 1.2 for curves in Section 3 and deduce it for surfaces using Lemma 3.2. The proof of Theorem 1.2 is completed using some results of [Kato and Saito 1986] and Theorem 1.4 proven by using a combination of Theorem 1.2 and an explicit formula for the Chow group of 0-cycles on normal surfaces from [Krishna and Srinivas 2002].

We prove Theorem 1.6 by first reducing to the case of curves. This case is achieved with the help of an algebraic version of a sort of containment lemma. We prove Theorem 1.5 as a combination of Theorems 1.2 and 1.6. This reduces the problem to understanding a map of cohomology groups of the relative K-theory sheaves of nilpotent ideals. This in turn can be written as an explicit map of k-vector spaces, where k is the ground field. Theorem 1.7 is proven by reducing to the case of affine surfaces and empty Cartier divisor using some Bertini theorems.

2. Recollection of Chow group with modulus and relative K-theory

We fix a field k and let $\mathbf{Sch}/k$ denote the category of quasiprojective schemes over k. Let $\mathbf{Sm}/k$ denote the full subcategory of $\mathbf{Sch}/k$ consisting of nonsingular (regular) schemes. Given $X \in \mathbf{Sch}/k$, we shall write X_{sing} and X_{reg} for the closed and open subschemes of X, where X_{red} is singular and regular, respectively. In this text, a *curve* will mean an equidimensional quasiprojective scheme over k of dimension one. For a curve C, the scheme C^N will often denote the normalization of C_{red}. Given a closed immersion $Y \hookrightarrow X$ in $\mathbf{Sch}/k$, we let $|Y|$ denote the support of Y with the reduced induced closed subscheme structure.

For $X \in \mathbf{Sch}/k$, let $K(X)$ and $G(X)$ denote the K-theory spectra of perfect complexes and coherent sheaves on X, respectively. For a closed subscheme $Y \hookrightarrow X$, let $K(X, Y)$ denote the homotopy fiber of the restriction map $K(X) \to K(Y)$. For a sheaf $\mathcal{F}$ on the small Zariski (resp. Nisnevich) site of X, let $H^*_{\mathrm{zar}}(X, \mathcal{F})$ (resp. $H^*_{\mathrm{nis}}(X, \mathcal{F})$) denote the cohomology groups of $\mathcal{F}$. A cohomology group in this text without mention of the underlying site will indicate the Zariski cohomology.

Thomason–Trobaugh spectral sequence for K-theory with support and relative K-theory. Given a scheme X and a closed subscheme $Y \hookrightarrow X$, let $K^Y(X)$ denote the homotopy fiber of the restriction map of spectra $K(X) \to K(X \setminus Y)$. Let $\mathcal{K}_{i,(X,Y)}$ denote the Zariski sheaf on X whose stalk at a point $x \in X$ is the relative group $K_i(\mathcal{O}_{X,x}, \mathcal{O}_{Y,x})$ for $i \in \mathbb{Z}$. Given a closed point $x \in X_{\mathrm{reg}} \setminus Y$, the spectrum $K^{\{x\}}(Y)$ is contractible and hence there are natural maps of spectra

$$K(k(x)) \to K^{\{x\}}(X) \to K(X, D) \to K(X). \tag{2-1}$$

In particular, there is a commutative diagram of Thomason–Trobaugh spectral sequences [1990, Corollary 10.5]

$$\begin{array}{ccc} E_{2,x}^{p,q} = H^p_{\{x\}}(X, \mathcal{K}_{q,X}) & \Longrightarrow & K^{\{x\}}_{q-p}(X) \\ \downarrow & & \downarrow \\ E_{2,(X,Y)}^{p,q} = H^p(X, \mathcal{K}_{q,(X,Y)}) & \Longrightarrow & K_{q-p}(X, Y) \\ \downarrow & & \downarrow \\ E_{2,X}^{p,q} = H^p(X, \mathcal{K}_{q,X}) & \Longrightarrow & K_{q-p}(X) \end{array} \tag{2-2}$$

which is valid even when the Zariski cohomology is replaced by the Nisnevich cohomology.

Lemma 2.1. *Given a modulus pair (X, D) of dimension two over k, there is a short exact sequence*

$$0 \longrightarrow H^2_{\mathcal{C}}(X, \mathcal{K}_{2,(X,D)}) \longrightarrow K_0(X, D) \longrightarrow \mathrm{Pic}(X, D) \longrightarrow 0 \tag{2-3}$$

where $\mathcal{C}$ is either Zariski or Nisnevich cohomology. In particular, the map $H^2_{\mathrm{zar}}(X, \mathcal{K}_{2,(X,D)}) \to H^2_{\mathrm{nis}}(X, \mathcal{K}_{2,(X,D)})$ is an isomorphism.

Proof. Let $\mathcal{C}$ denote either the Zariski or the Nisnevich cohomology. Since the $\mathcal{C}$-cohomological dimension of X is two, the strongly convergent spectral sequence $E_2^{p,q} = H^p_{\mathcal{C}}(X, \mathcal{K}_{q,(X,D)}) \Rightarrow K_{q-p}(X, D)$ with differential $d_r : E_r^{p,q} \to E_r^{p+r,q+r-1}$ gives us an exact sequence

$$H^0_{\mathcal{C}}(X, \mathcal{K}_{1,(X,D)}) \xrightarrow{d_2^{0,1}} H^2_{\mathcal{C}}(X, \mathcal{K}_{2,(X,D)}) \longrightarrow K_0(X, D) \longrightarrow H^1_{\mathcal{C}}(X, \mathcal{K}_{1,(X,D)}) \longrightarrow 0. \tag{2-4}$$

By Hilbert's theorem 90, the map $H^1_{\mathrm{zar}}(X, \mathcal{K}_{1,(X,D)}) \to H^1_{\mathrm{nis}}(X, \mathcal{K}_{1,(X,D)})$ is an isomorphism and it follows from [Suslin and Voevodsky 1996, Lemma 2.1] that $H^1_{\mathrm{zar}}(X, \mathcal{K}_{1,(X,D)}) \xrightarrow{\sim} \mathrm{Pic}(X, D)$. We are thus left with showing that $d_2^{0,1} = 0$. We prove this for the Zariski cohomology as the same argument applies in the Nisnevich case.

Applying the above spectral sequence for $K_1(X, D)$, the equality $d_2^{0,1} = 0$ is equivalent to the assertion that the map $K_1(X, D) \to H^0(X, \mathcal{K}_{1,(X,D)})$ is surjective. To prove this, we let $f \in H^0(X, \mathcal{K}_{1,(X,D)})$. This is equivalent to a regular map $f : X \to \mathbb{G}_m$ such that $f|_D = 1$ and hence to a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K_1(\mathbb{G}_m, \{1\}) & \longrightarrow & K_1(\mathbb{G}_m) & \longrightarrow & K_1(\{1\}) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f^*} & & \downarrow{\scriptstyle f^*} & & \downarrow{\scriptstyle f^*} & & \\ & & K_1(X, D) & \longrightarrow & K_1(X) & \longrightarrow & K_1(D) & & \\ & & \downarrow & & \downarrow{\scriptstyle \delta} & & \downarrow & & \\ 0 & \longrightarrow & H^0(X, \mathcal{K}_{1,(X,D)}) & \longrightarrow & H^0(X, \mathcal{K}_{1,X}) & \longrightarrow & H^0(D, \mathcal{K}_{1,D}) & & \end{array} \tag{2-5}$$

If we let $\mathbb{G}_m = \mathrm{Spec}(k[t^{\pm 1}])$, then one can check (as is well known) that $\delta \circ f^*([t]) = f$. Since $t \in K_1(\mathbb{G}_m, \{1\})$, we see that $f^*([t]) \in K_1(X, D)$ and $\delta \circ f^*(t)$ dies in $H^0(D, \mathcal{K}_{1,D})$. Hence, it must lie in $H^0(X, \mathcal{K}_{1,(X,D)})$. It follows that the map $K_1(X, D) \to H^0(X, \mathcal{K}_{1,(X,D)})$ is surjective. □

Remark 2.2. The isomorphism $H^2_{\mathrm{zar}}(X, \mathcal{K}_{2,(X,D)}) \xrightarrow{\sim} H^2_{\mathrm{nis}}(X, \mathcal{K}_{2,(X,D)})$ was shown earlier by Kato and Saito [1986, Proposition 9.9] by a different method.

Chow groups of 0-cycles with modulus. We recall the definition of the Chow group of 0-cycles with modulus (see [Binda and Saito 2014, §2] or [Krishna and Park 2014, §2]).

Let X be a nonsingular scheme of pure dimension d and let $D \subsetneq X$ be an effective Cartier divisor on X. We shall call such a pair (X, D) of a nonsingular scheme and an effective Cartier divisor, a d-dimensional *modulus pair*. Let $\mathcal{Z}_0(X, D)$ denote the free abelian group on the closed points in $X \setminus D$. Let $C \hookrightarrow X \times \mathbb{P}^1_k$ be a closed irreducible curve satisfying:

(1) C is not contained in $X \times \{0, 1, \infty\}$.

(2) If $\nu : C^N \to X \times \mathbb{P}^1_k$ denotes the composite map from the normalization of C, then one has an inequality of Weil divisors on C^N:

$$\nu^*(D \times \mathbb{P}^1_k) \leq \nu^*(X \times \{1\}).$$

We call such curves admissible. Let $\mathcal{Z}_1(X, D)$ denote the free abelian group on admissible curves and let $\mathcal{R}_0(X, D)$ denote the image of the boundary map $(\partial_0 - \partial_\infty) : \mathcal{Z}_1(X, D) \to \mathcal{Z}_0(X, D)$. The Chow group of 0-cycles on X with modulus D is defined as the quotient

$$\mathrm{CH}_0(X, D) := \frac{\mathcal{Z}_0(X, D)}{\mathcal{R}_0(X, D)}.$$

To relate this definition of $\mathrm{CH}_0(X, D)$ with the one given by Kerz and Saito [2015], let $\pi_C : C^N \to C$ denote the normalization of an integral curve $C \hookrightarrow X$ which is not a component of D. Let $A_{C|D}$ and $A_{C^N|D}$ denote the semilocal rings of C and C^N at the supports of $C \cap D$ and $\pi_C^{-1}(C \cap D)$, respectively. Let $\mathcal{R}'_0(X, D)$ denote the subgroup of $\mathcal{Z}_0(X, D)$ given by the image

$$\coprod_{C \not\subset D} K_1(A_{C^N|D}, I_D) \xrightarrow{\mathrm{div}} \mathcal{Z}_0(X, D). \tag{2-6}$$

Note that the surjectivity of the map $K_2(A_{C^N|D}) \to K_2(\pi_C^*(D))$ implies that

$$\begin{aligned} K_1(A_{C^N|D}, I_D) &= \mathrm{Ker}(K_1(A_{C^N|D}) \to K_1(\pi_C^*(D)) \\ &= \varinjlim_U \mathrm{Ker}(\mathcal{O}(U)^\times \to \mathcal{O}(\pi_C^*(D))^\times), \end{aligned} \tag{2-7}$$

where U ranges over all open subschemes of C^N containing $\pi_C^*(D)$.

One can then check as in the classical case (see for instance [Binda and Saito 2014, Theorem 3.3]) that there is a canonical isomorphism

$$\frac{\mathcal{Z}_0(X, D)}{\mathcal{R}'_0(X, D)} \xrightarrow{\sim} \mathrm{CH}_0(X, D). \tag{2-8}$$

3. The cycle class map

Let (X, D) be a 2-dimensional modulus pair. In this section, we construct the cycle class map $\mathrm{CH}_0(X, D) \to H^2(X, \mathcal{K}_{2,(X,D)})$ and prove Theorems 1.2 and 1.4. More generally, we assume X is either a curve or a surface and let $P \in X \setminus D$ be a closed point. Let X_P denote the spectrum of the local ring $\mathcal{O}_{X,P}$. Assume $d = 1, 2$. It follows from (2-1) and (2-2) that there is a commutative diagram

$$\begin{array}{ccc} H^0(\{P\}, \mathcal{K}_{0,\{P\}}) & \longrightarrow & K_0(\{P\}) \\ \wr\downarrow & & \downarrow\wr \\ H^d_{\{P\}}(X, \mathcal{K}_{d,X}) & \longrightarrow & K_0^{\{P\}}(X) \\ \downarrow & & \downarrow \\ H^d(X, \mathcal{K}_{d,(X,D)}) & \longrightarrow & K_0(X, D) \end{array} \tag{3-1}$$

where the top vertical arrow on the left is an isomorphism by excision and the Gersten resolution for $\mathcal{K}_{d,X_P}$ and the one on the right is an isomorphism by the localization sequence for K-theory. We define the cycle class map

$$\mathrm{cyc}_{(X,D)} : \mathcal{Z}_0(X, D) \longrightarrow H^d(X, \mathcal{K}_{d,(X,D)}) \tag{3-2}$$

by letting $\mathrm{cyc}_{(X,D)}([P])$ be the image of $1 \in H^0(\{P\}, \mathcal{K}_{0,\{P\}}) \simeq \mathbb{Z}$ under the composite vertical arrow on the left in (3-1) and extending it linearly on all of $\mathcal{Z}_0(X, D)$. To show that this map kills rational equivalences, we first consider the case of curves.

Lemma 3.1. *Let (C, D) be an 1-dimensional modulus pair. Then the map $\mathrm{cyc}_{(C,D)}$ induces isomorphisms*

$$\mathrm{cyc}_{(C,D)} : \mathrm{CH}_0(C, D) \xrightarrow{\sim} H^1_{\mathrm{zar}}(C, \mathcal{K}_{1,(C,D)}) \xrightarrow{\sim} H^1_{\mathrm{nis}}(C, \mathcal{K}_{1,(C,D)}) \xrightarrow{\sim} \mathrm{Pic}(C, D) \xrightarrow{\sim} K_0(C, D).$$

Proof. For any reduced closed subset $S \subsetneq C$ such that $S \cap D = \varnothing$ and any open subset $U \subseteq X$, we have the localization fiber sequence of spectra

$$K(S \cap U) \longrightarrow K(U) \longrightarrow K(U \setminus S).$$

Taking the filtered colimit over closed subsets S as above under the inclusion, we get a short exact sequence of Zariski sheaves

$$0 \longrightarrow \mathcal{K}_{1,(C,D)} \longrightarrow j_*(\mathcal{K}_{1,(C_D,D)}) \longrightarrow \coprod_{P \notin D} (i_P)_*\big(K_0(k(P))\big) \longrightarrow 0 \tag{3-3}$$

on C, where C_D is the spectrum of the semilocal ring $A_{C|D}$ of C at $|D|$ and $j : C_D \hookrightarrow C$ is the inclusion map. This yields the cycle class map

$$\mathrm{cyc}_{(C,D)} : \coprod_{P \notin D} \mathbb{Z} \longrightarrow H^1(C, \mathcal{K}_{1,(C,D)}). \tag{3-4}$$

To show that this induces an isomorphism $\mathrm{CH}_0(C, D) \to H^1(C, \mathcal{K}_{1,(C,D)})$, we first claim that $j_*(\mathcal{K}_{1,(C_D,D)})$ is an acyclic Zariski sheaf. To prove this claim, it suffices to show that if $U \hookrightarrow C$ is open and U_D is the spectrum of the semilocal ring of U at $|U \cap D|$, then $H^i(U_D, \mathcal{K}_{1,(U_D,D)}) = 0$ for $i \geq 1$. But this is immediate from the exact sequence

$$0 \longrightarrow \mathcal{K}_{1,(U_D,D)} \longrightarrow \mathcal{K}_{1,U_D} \longrightarrow \mathcal{K}_{1,U\cap D} \longrightarrow 0$$

and the fact that U_D is a semilocal scheme.

It follows from the above claim that (3-3) is an acyclic resolution of $\mathcal{K}_{1,(C,D)}$ and in particular, there is an exact sequence

$$K_1(A_{C|D}, I_D) \xrightarrow{\mathrm{div}} \coprod_{P \notin D} \mathbb{Z} \longrightarrow H^1_{\mathrm{zar}}(C, \mathcal{K}_{1,(C,D)}) \longrightarrow 0.$$

By (2-8), this implies that the map (3-4) induces an isomorphism $\mathrm{CH}_0(C, D) \xrightarrow{\sim} H^1_{\mathrm{zar}}(C, \mathcal{K}_{1,(C,D)})$.

The isomorphism of the natural map $H^1_{\mathrm{zar}}(C, \mathcal{K}_{1,(C,D)}) \to H^1_{\mathrm{nis}}(C, \mathcal{K}_{1,(C,D)})$ follows easily from Hilbert's theorem 90.

We now consider the commutative diagram of homotopy fiber sequences

$$\begin{array}{ccccc} \coprod_{P\notin D} K(k(P)) & \longrightarrow & K(C) & \longrightarrow & K(A_{C|D}) \\ & & \downarrow & & \downarrow \\ & & K(A_{C|D}/I) & = & K(A_{C|D}/I) \end{array}$$

This yields a homotopy fiber sequence

$$\coprod_{P\notin D} K(k(P)) \longrightarrow K(C, D) \longrightarrow K(A_{C|D}, I)$$

and in particular, an exact sequence

$$K_1(A_{C|D}, I) \xrightarrow{\partial} \mathcal{Z}_0(C, D) \longrightarrow K_0(C, D) \longrightarrow 0$$

and we conclude from this that

$$\mathrm{Coker}(\partial) = \mathrm{CH}_0(C, D) \xrightarrow{\sim} K_0(C, D).$$

Finally, the isomorphism $H^1_{\mathrm{zar}}(C, \mathcal{K}_{1,(C,D)}) \xrightarrow{\sim} \mathrm{Pic}(C, D)$ follows from [Suslin and Voevodsky 1996, Lemma 2.1]. □

Lemma 3.2. *Let (X, D) be a 2-dimensional modulus pair and let $f : C \to X$ be a finite map, where C is a nonsingular curve such that $f^*(D)$ is a proper closed subscheme of C. Then there is a commutative diagram*

$$\begin{array}{ccc} \mathcal{Z}_0(C, f^*(D)) & \xrightarrow{\mathrm{cyc}_{(C,f^*(D))}} & H^1(C, \mathcal{K}_{1,(C,f^*(D))}) \\ {\scriptstyle f_*}\downarrow & & \downarrow{\scriptstyle f_*} \\ \mathcal{Z}_0(X, D) & \xrightarrow{\mathrm{cyc}_{(X,D)}} & H^2(X, \mathcal{K}_{2,(X,D)}) \end{array} \tag{3-5}$$

where f_* on the left is the pushforward map.

Proof. We set $E = f^*(D)$. Since $\iota_X : D \hookrightarrow X$ and $\iota_C : E \hookrightarrow C$ are Cartier divisors, $\mathrm{Tor}^i_{\mathcal{O}_X}(\mathcal{O}_D, f_*(\mathcal{O}_C)) = 0$ for $i > 0$. In particular, there is a commutative diagram

$$\begin{array}{ccc} K(C) & \xrightarrow{f_*} & K(X) \\ {\scriptstyle \iota_C^*}\downarrow & & \downarrow{\scriptstyle \iota_X^*} \\ K(E) & \xrightarrow[f_*]{} & K(D) \end{array} \tag{3-6}$$

As (3-6) makes sense for any open $U \hookrightarrow X$ and is functorial for restriction to open subsets, we see that it is in fact a diagram of presheaves of spectra on X_{zar}.

If we consider the homotopy cofibers of the horizontal arrows in (3-6), we obtain a commutative diagram of homotopy cofiber sequences of presheaves of spectra

on X_{zar}. Taking the long homotopy groups exact sequences, we obtain the associated diagram of the long exact sequences of the presheaves of homotopy groups. The exactness of the sheafification functor yields a commutative diagram of the long exact sequences of the sheaves of homotopy groups corresponding to (3-6).

Let $\widetilde{K}(X\setminus C)$ and $\widetilde{K}(D\setminus E)$ denote the homotopy cofibers of the top and bottom horizontal arrows in (3-6), respectively. Let $\widetilde{\mathcal{K}}_{i,X\setminus C}$ denote the Zariski sheaf on X associated to the presheaf of homotopy groups $U\mapsto \pi_i(\widetilde{K}(U\setminus C))$. Defining $\widetilde{\mathcal{K}}_{i,D\setminus E}$ in a similar way, we get a commutative diagram of the long exact sequences

$$\begin{array}{ccccccccccc}
\cdots & \longrightarrow & \widetilde{\mathcal{K}}_{3,X\setminus C} & \longrightarrow & f_*(\mathcal{K}_{2,C}) & \longrightarrow & \mathcal{K}_{2,X} & \longrightarrow & \widetilde{\mathcal{K}}_{2,X\setminus C} & \longrightarrow & f_*(\mathcal{K}_{1,C}) & \longrightarrow & \cdots \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
\cdots & \longrightarrow & \widetilde{\mathcal{K}}_{3,D\setminus E} & \longrightarrow & f_*(\mathcal{K}_{2,E}) & \longrightarrow & \mathcal{K}_{2,D} & \longrightarrow & \widetilde{\mathcal{K}}_{2,D\setminus E} & \longrightarrow & f_*(\mathcal{K}_{1,E}) & \longrightarrow & \cdots
\end{array} \tag{3-7}$$

If $\overline{C}$ is the image of $f: C\to X$, then we have a factorization $K(C)\to G(\overline{C})\to K(X)$ (see [Srinivas 1991, Proposition 5.12(i)]) and this shows that there is a factorization $\mathcal{K}_{i,X}\to\widetilde{\mathcal{K}}_{i,X\setminus C}\to j_*(\mathcal{K}_{i,X\setminus\overline{C}})\to j_*(K_i(k(X)))$, where $j: X\setminus\overline{C}\hookrightarrow X$ is the inclusion. The Gersten resolution says that the composite map is injective. Hence, the map $\mathcal{K}_{i,X}\to\widetilde{\mathcal{K}}_{i,X\setminus C}$ is injective. Since the map $f_*(\mathcal{K}_{i,C})\to f_*(\mathcal{K}_{i,E})$ is surjective for $i\le 2$, the above diagram refines to a commutative diagram of short exact sequences

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathcal{K}_{2,X} & \longrightarrow & \widetilde{\mathcal{K}}_{2,X\setminus C} & \longrightarrow & f_*(\mathcal{K}_{1,C}) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle\phi} & & \downarrow & & \\
0 & \longrightarrow & \mathcal{K}_{2,D} & \longrightarrow & \widetilde{\mathcal{K}}_{2,D\setminus E} & \longrightarrow & f_*(\mathcal{K}_{1,E}) & \longrightarrow & 0
\end{array} \tag{3-8}$$

Set $\widetilde{\mathcal{K}}_{2,(X,D)}=\mathrm{Ker}(\mathcal{K}_{2,X}\to\mathcal{K}_{2,D})$. Since the vertical arrows on the left and the right ends in (3-8) are surjective, the middle arrow is also surjective and there is a short exact sequence of the kernel sheaves

$$0\longrightarrow\widetilde{\mathcal{K}}_{2,(X,D)}\longrightarrow\mathrm{Ker}(\phi)\longrightarrow f_*(\mathcal{K}_{1,(C,E)})\longrightarrow 0. \tag{3-9}$$

Considering the long exact cohomology sequences with and without support and observing that $H^i(C,\, f_*(\mathcal{K}_{1,(C,E)}))\simeq H^i(C,\,\mathcal{K}_{1,(C,E)})$ (the higher direct images of $\mathcal{K}_{1,(C,E)}$ vanish as one can easily check), we get a commutative diagram

$$\begin{array}{ccccccc}
\coprod\limits_{Q\in\Sigma_P}\mathbb{Z} & \xrightarrow{\sim} & H^1_{\Sigma_P}(C,\mathcal{K}_{1,C}) & \xrightarrow{\sim} & H^1_{\Sigma_P}(C,\mathcal{K}_{1,(C,E)}) & \longrightarrow & H^1(C,\mathcal{K}_{1,(C,E)}) \\
{\scriptstyle f_*}\downarrow & & \downarrow & & \downarrow & & \downarrow \\
\mathbb{Z} & \xrightarrow{\sim} & H^2_{\{P\}}(X,\mathcal{K}_{2,X}) & \xrightarrow{\sim} & H^2_{\{P\}}(X,\widetilde{\mathcal{K}}_{2,(X,D)}) & \longrightarrow & H^2(X,\widetilde{\mathcal{K}}_{2,(X,D)})
\end{array} \tag{3-10}$$

for any closed point $P \in X \setminus D$ and $\Sigma_P = f^{-1}(P)$. It is well known that the leftmost vertical map is the pushforward map. Since the map $\mathcal{K}_{2,(X,D)} \to \widetilde{\mathcal{K}}_{2,(X,D)}$ is a surjective map whose kernel is supported on D, the map $H^2(X, \mathcal{K}_{2,(X,D)}) \to H^2(X, \widetilde{\mathcal{K}}_{2,(X,D)})$ is an isomorphism. This immediately yields (3-5). □

Proof of Theorem 1.2. In view of Lemma 2.1, the proof of Theorem 1.2 is reduced to showing that the cycle class map $\mathrm{cyc}_{(X,D)} : \mathcal{Z}_0(X, D) \to H^2(X, \mathcal{K}_{2,(X,D)})$ constructed in (3-2) kills the group of rational equivalences $\mathcal{R}'_0(X, D)$ (see (2-8)) and is surjective. So, let us take an integral curve $C \hookrightarrow X$ which is not contained in D and let $f : C^N \to X$ denote the induced map from the normalization of C. Letting $E = f^*(D)$ and $g \in \mathrm{Ker}(\mathcal{O}^\times_{C^N} \twoheadrightarrow \mathcal{O}^\times_E)$, we need to show that $\mathrm{cyc}_{(X,D)} \circ f_*(\mathrm{div}(g)) = 0$. For this, we consider the diagram

$$\begin{array}{ccccc} \mathcal{R}'_0(C^N, E) & \longrightarrow & \mathcal{Z}_0(C^N, E) & \xrightarrow{\mathrm{cyc}_{(C^N,E)}} & H^1(C^N, \mathcal{K}_{1,(C^N,E)}) \\ \downarrow{\scriptstyle f_*} & & \downarrow{\scriptstyle f_*} & & \downarrow{\scriptstyle f_*} \\ \mathcal{R}'_0(X, D) & \longrightarrow & \mathcal{Z}_0(X, D) & \xrightarrow{\mathrm{cyc}_{(X,D)}} & H^2(X, \mathcal{K}_{2,(X,D)}) \end{array} \tag{3-11}$$

in which the left square commutes by [Krishna and Park 2014, Proposition 2.10] and the right square commutes by Lemma 3.2. Since the composite horizontal map on the top is zero by Lemma 3.1, it follows that

$$\mathrm{cyc}_{(X,D)} \circ f_*(\mathrm{div}(g)) = f_* \circ \mathrm{cyc}_{(C^N,E)}(\mathrm{div}(g)) = 0.$$

The surjectivity of $\mathrm{cyc}_{(X,D)}$ now follows from Lemma 3.2, the isomorphism $\mathcal{K}^M_{2,(X,D)} \xrightarrow{\sim} \widetilde{\mathcal{K}}_{2,(X,D)}$, the diagram (3-1) and [Kato and Saito 1986, Theorem 2.5]. □

Proof of Theorem 1.4. Let $\pi : X \to Y$ be a resolution of singularities of a normal surface over any field k. We set $U = Y_{\mathrm{reg}}$ and $C(U) = \varprojlim_D \mathrm{CH}_0(X, D)$, where the limit is taken over all effective Cartier divisors on X with support outside U. Let $E \hookrightarrow X$ denote the reduced exceptional divisor. If $D \subsetneq X$ is an effective Cartier divisor with support $|D| \subseteq E$, then $mE - D$ must be an effective Cartier divisor some $m \gg 1$. This implies that the canonical maps

$$C(U) \to \varprojlim_m \mathrm{CH}_0(X, mE) \quad \text{and} \quad \varprojlim_D H^2(X, \mathcal{K}_{2,(X,D)}) \to \varprojlim_m H^2(X, \mathcal{K}_{2,(X,mE)})$$

are isomorphisms.

Let $\mathrm{CH}_0(Y)$ denote the Chow group of 0-cycles on Y in the sense of [Levine and Weibel 1985] and let $S \hookrightarrow Y$ denote the singular locus of Y with reduced

subscheme structure. We then have a commutative diagram

$$\begin{array}{ccccc}
\mathrm{CH}_0(Y) & \xrightarrow{\mathrm{cyc}_{(Y,mS)}} & H^2(Y,\mathcal{K}_{2,(Y,mS)}) & & \\
\downarrow{\scriptstyle \pi^*} & & \downarrow{\scriptstyle \pi^*} & \searrow^{\sim} & \\
\mathrm{CH}_0(X,mE) & \xrightarrow{\mathrm{cyc}_{(X,mE)}} & H^2(X,\mathcal{K}_{2,(X,mE)}) & & H^2(Y,\mathcal{K}_{2,Y}) \\
\downarrow & & \downarrow & \swarrow{\scriptstyle \pi^*} & \\
\mathrm{CH}_0(X) & \xrightarrow{\mathrm{cyc}_X} & H^2(X,\mathcal{K}_{2,X}) & &
\end{array} \tag{3-12}$$

The map $\mathrm{cyc}_{(Y,mS)}$ is defined exactly like $\mathrm{cyc}_{(X,mE)}$ and is an isomorphism by [Krishna 2015, Proposition 3.1]. The natural map $H^2(Y,\mathcal{K}_{2,(Y,mS)}) \to H^2(Y,\mathcal{K}_{2,Y})$ is an isomorphism also by [Krishna 2015, Proposition 3.1]. The map $\pi^*:\mathrm{CH}_0(Y)\to \mathrm{CH}_0(X,mE)$ is induced by the identity map $\pi^*:\mathcal{Z}_0(U)\to\mathcal{Z}_0(X,mE)$.

To show that it preserves rational equivalences, let $C\hookrightarrow Y$ be an integral curve not meeting S and let $h\in k(C)^\times$. Let $\Gamma_h\hookrightarrow C\times\mathbb{P}^1\hookrightarrow Y\times\mathbb{P}^1$ be the graph of the function $h:C\to\mathbb{P}^1$. It is then clear that $\Gamma_h\cap(S\times\mathbb{P}^1)=\varnothing$. In particular, $\pi^{-1}(\Gamma_h)\cap(E\times\mathbb{P}^1)=\varnothing$. This shows that $[\Gamma_h]\in\mathcal{Z}_1(X,mE)$ is an admissible 1-cycle such that

$$\pi^*(\mathrm{div}(h))=\pi^*([h^*(0)]-[h^*(\infty)])=\pi^*(\partial_0([\Gamma_h])-\partial_\infty([\Gamma_h]))=(\partial_0-\partial_\infty)([\Gamma_h]).$$

This shows the inclusion $\pi^*(\mathrm{div}(h))\subset\mathcal{R}_0(X,mE)$ and it yields the pullback $\pi^*:\mathrm{CH}_0(Y)\twoheadrightarrow\mathrm{CH}_0(X,mE)$. All other maps in (3-12) are naturally defined and all are surjective.

If we let $F^2K_0(X,mE)$ denote the image of the map $\mathrm{cyc}_{(X,mE)}:\mathrm{CH}_0(X,mE)\to K_0(X,mE)$, then it follows from Theorem 1.2 and Lemma 2.1 that $F^2K_0(X,mE)\to H^2(X,\mathcal{K}_{2,(X,mE)})$ is an isomorphism. We now apply [Krishna and Srinivas 2002, Theorem 1.1] to conclude that the map $H^2(Y,\mathcal{K}_{2,(Y,mS)})\to H^2(X,\mathcal{K}_{2,(X,mE)})$ is an isomorphism for all sufficiently large m. It follows that all arrows in the upper square of (3-12) are isomorphisms for all sufficiently large m. In particular, the map $\mathrm{cyc}_{(X,mE)}:\mathrm{CH}_0(X,mE)\to H^2(X,\mathcal{K}_{2,(X,mE)})$ is an isomorphism for all sufficiently large m and hence the map $C(U)\to\varprojlim_m H^2(X,\mathcal{K}_{2,(X,mE)})$ is an isomorphism. □

4. Vanishing theorems and failure of localization

Let k be a field and consider the effective Cartier divisor $D=\mathrm{Spec}(k[t]/t^m)$ on $\mathbb{A}^1_k=\mathrm{Spec}(k[t])$. Given $X\in\mathbf{Sch}/k$, let us denote the effective Cartier divisor $X\times D\hookrightarrow X\times\mathbb{A}^1_k$ by D itself. We shall prove Theorem 1.6 using the following algebraic result.

Lemma 4.1. *Let A be the coordinate ring of a smooth affine curve over k and let $\mathfrak{m}$ be a maximal ideal of $A[t]$ which contains the ideal $(t-a)$, where $a \in k^\times$. Then we can find a prime ideal $\mathfrak{p}$ of height one in $A[t]$ such that the following hold.*

(1) $\mathfrak{p} \subsetneq \mathfrak{m}$.

(2) $A[t]/\mathfrak{p}$ *is smooth.*

(3) $\mathfrak{m}/\mathfrak{p}$ *is a principal ideal.*

(4) $\mathfrak{p} + (t) = A[t]$.

Proof. Consider the maximal ideal $\mathfrak{m}' = \mathfrak{m} \cap A$ of A. Since A is a Dedekind domain, we can write $\mathfrak{m}' = (f_1, f_2)$. But this implies using our hypothesis that $\mathfrak{m} = (t-a, f_1, f_2) = (a^{-1}t - 1, f_1, f_2)$. In case $f_1 = f_2$, we take $\mathfrak{p} = (t-a)$ which clearly does the job. So we assume that $f_1 \neq f_2$.

Since $A_{\mathfrak{m}'}$ is a discrete valuation ring, $\mathfrak{m}'A_{\mathfrak{m}'}$ is a principal ideal. In particular, there is an element $f \in A$ such that $f \notin \mathfrak{m}'$ and $\mathfrak{m}'A_f$ is principal. As $f \notin \mathfrak{m}'$, we have $(f) + \mathfrak{m}' = A$, and this gives us an identity $\alpha f - \alpha_1 f_1 - \alpha_2 f_2 - 1 = 0$ in A. Setting $g = \alpha f$, we see that $\mathfrak{m}'A_g$ is also a principal ideal. Furthermore, we have

$$ga^{-1}t - 1 = g(a^{-1}t - 1) + g - 1 = g(a^{-1}t - 1) + \alpha_1 f_1 + \alpha_2 f_2 \in \mathfrak{m}. \tag{4-1}$$

If we set $\mathfrak{p} = (ga^{-1}t - 1) \subsetneq A[t]$, we have just shown that $\mathfrak{p} \subsetneq \mathfrak{m}$. Since $A[t]/\mathfrak{p} \simeq A_g$ and hence

$$\frac{\mathfrak{m}}{\mathfrak{p}} \simeq \frac{\mathfrak{m}A_g[t]}{\mathfrak{p}A_g[t]} \simeq \frac{(-g^{-1}(\alpha_1 f_1 + \alpha_2 f_2), f_1, f_2)A_g[t]}{\mathfrak{p}A_g[t]} \simeq \frac{(f_1, f_2)A_g[t]}{\mathfrak{p}A_g[t]} \simeq \mathfrak{m}'A_g,$$

we see that (2) and (3) are satisfied. The item (4) is clear. This proves the lemma. □

Proof of Theorem 1.6. We can assume that Y is connected. We set $X = Y \times \mathbb{A}^1_k$ and $U = Y \times \mathbb{G}_m$. Let $p : X \to \mathbb{A}^1_k$ and $q : X \to Y$ denote the projection maps. Let $P \in U$ be a closed point and set $P_1 = p(P)$ and $P_2 = q(P)$. Then $P_1 \in \mathbb{G}_m$ and $P_2 \in Y$ are closed points as well.

We can find a nonsingular curve $\iota : C \hookrightarrow Y$ containing P_2 (see [Kleiman and Altman 1979, Theorem 1] when k is infinite and [Poonen 2008, Theorem 1.1] when k is finite). It follows from [Krishna and Park 2014, Proposition 2.10] that there is a pushforward map $\iota_* : \mathrm{CH}_0(C \times \mathbb{A}^1_k, D) \to \mathrm{CH}_0(Y \times \mathbb{A}^1_k, D)$ such that the class $[P] \in \mathrm{CH}_0(Y \times \mathbb{A}^1_k, D)$ lies in the image of this map. We can therefore assume that Y is a curve.

Now P defines a unique closed point $P' \in X_{k(P)}$ such that $P = \pi(P')$, where $\pi : \mathrm{Spec}(k(P)) \to \mathrm{Spec}(k)$ is the finite map. This gives $[P] = \pi_*([P'])$ under the pushforward map $\pi_* : \mathrm{CH}_0(X_{k(P)}, D) \to \mathrm{CH}_0(X, D)$ (see [Krishna and Park 2014, Proposition 2.10]). It suffices therefore to show that the class $[P'] \in \mathrm{CH}_0(X_{k(P)}, D)$ dies. We can thus assume that $P_1 \in \mathbb{G}_m(k)$.

We can now apply Lemma 4.1 to get a smooth affine curve $i : C \hookrightarrow X$ which is a closed subset of X containing P such that $C \cap (Y \times D) = \varnothing$ and $P \in C$ is a principal Cartier divisor. In particular, the class $[P] \in \mathrm{CH}_0(C)$ is zero. On the other hand, the condition $C \cap (Y \times D) = \varnothing$ implies that the inclusion $\mathcal{Z}_0(C) \hookrightarrow \mathcal{Z}_0(X, D)$ defines a pushforward map $i_* : \mathrm{CH}_0(C) \to \mathrm{CH}_0(X, D)$ (see [Krishna and Park 2014, Corollary 2.11]) such that $i_*([P]) = [P] \in \mathrm{CH}_0(X, D)$. It follows that $[P] = 0$. This proves that $\mathrm{CH}_0(X, D) = 0$. The second part of the theorem now follows from Theorem 1.2. □

As an immediate consequence of Theorems 1.2 and 1.6, we get:

Corollary 4.2. *Given a nonsingular affine curve Y over a field k, we have*

$$K_0(Y \times \mathbb{A}^1_k, D) \xrightarrow{\sim} \mathrm{Pic}(Y \times \mathbb{A}^1_k, D).$$

Remark 4.3. Theorem 1.6 is known to fail when $d = 0$ (see [Bloch and Esnault 2003a]).

Proof of Theorem 1.7. Let the pair (X, D) be as in Theorem 1.7 and let $x \in X \setminus D$ be a closed point. We can assume that X is connected. We claim that there is a smooth affine closed subscheme $\iota : Y \hookrightarrow X$ of dimension $d-1$ such that $Y \cap D = \varnothing$ and $x \in Y$.

To prove the claim, let A denote the coordinate ring of X and let $I \hookrightarrow A$ denote the defining ideal of D. Let $\mathfrak{m} \hookrightarrow A$ denote the maximal ideal corresponding to $x \in X$. Our assumption implies that there exist elements $a \in \mathfrak{m}^2$ and $b \in I$ such that $a - b = 1$. We can now apply [Swan 1974, Theorems 1.3, 1.4] to conclude that for general $a' \in \mathfrak{m}^2$, the ring $A/(a - a'b)$ is integral and smooth. Setting $f = a - a'b$, we see that $f \in \mathfrak{m}$ and $f - 1 = a - a'b - 1 = b - a'b = b(1 - a') \in I$. This shows that $Y := \mathrm{Spec}(A/(f))$ satisfies our requirement.

Using the above claim and [Krishna and Park 2014, Corollary 2.11], we get a pushforward map $\iota_* : \mathrm{CH}_0(Y) \to \mathrm{CH}_0(X, D)$ whose image contains the cycle class $[x]$. The desired vanishing now follows because one knows that $\mathrm{CH}_0(Y) = 0$ (see for instance [Krishna and Srinivas 2007, Theorem 6.4.1]).

To prove the second assertion of the theorem, we first notice that for a closed point $x \in X \setminus D$, we have natural maps

$$K_0(k(x)) \xrightarrow{\sim} H^d_{\{x\}}(X, \mathcal{K}^M_{d,(X,D)}) \longrightarrow H^d_{\mathrm{zar}}(X, \mathcal{K}^M_{d,(X,D)}) \longrightarrow H^d_{\mathrm{nis}}(X, \mathcal{K}^M_{d,(X,D)}).$$

Setting $\mathrm{cyc}_{(X,D)}([x])$ to be the image of $1 \in K_0(k(x))$ under the composite map, we get a cycle class map $\mathrm{cyc}_{(X,D)} : \mathcal{Z}_0(X, D) \to H^d_{\mathrm{nis}}(X, \mathcal{K}^M_{d,(X,D)})$.

If D_{red} has normal crossings, then it follows from [Rülling and Saito 2015, Definition 3.4.1, Proposition 3.5] that $\mathrm{cyc}_{(X,D)}$ has a factorization $\mathrm{CH}_0(X, D) \to \mathbb{H}^{2d}_{\mathrm{nis}}(X, \mathcal{Z}(d)_{X|D}) \to H^d_{\mathrm{nis}}(X, \mathcal{K}^M_{d,(X,D)})$, where $\mathcal{Z}(d)_{X|D}$ is the sheaf of cycle complexes $U \mapsto \mathcal{Z}^d(U|D, 2d - \bullet)$ on X_{nis}. Moreover, it follows from [Kato and Saito

1986, Theorem 2.5] that the map $\mathrm{cyc}_{(X,D)} : \mathrm{CH}_0(X, D) \to H^d_{\mathrm{nis}}(X, \mathcal{K}^M_{d,(X,D)})$ is surjective. The vanishing of $H^d_{\mathrm{nis}}(X, \mathcal{K}^M_{d,(X,D)})$ now follows from the first part of the theorem. □

Proof of Theorem 1.5. In view of Theorem 1.6, the theorem is equivalent to the assertion that the pushforward map $\mathrm{CH}_0(\{P\} \times \mathbb{A}^1_k, D) \xrightarrow{i_*} \mathrm{CH}_0(Y \times \mathbb{A}^1_k, D)$ is not surjective. If we let $\pi : Y \to \mathrm{Spec}(k)$ denote the structure map, then the composite map $\mathrm{CH}_0(\{P\} \times \mathbb{A}^1_k, D) \xrightarrow{i_*} \mathrm{CH}_0(Y \times \mathbb{A}^1_k, D) \xrightarrow{\pi_*} \mathrm{CH}_0(\mathbb{A}^1_k, D)$ is an isomorphism. In particular, i_* is split injective. Our aim is to show that it is not surjective.

We set $X = Y \times \mathbb{A}^1_k$, $V = Y \setminus \{P\}$, $U = V \times \mathbb{A}^1_k$ and $Z = \{P\} \times \mathbb{A}^1_k$. For any $W \in \mathbf{Sch}/k$, we shall write $W \times D$ as W_D in this proof. In view of Theorem 1.2, it suffices to show that the composite map $\mathrm{CH}_0(Z, D) \xrightarrow{i_*} \mathrm{CH}_0(X, D) \xrightarrow{\mathrm{cyc}_{(X,D)}} H^2(X, \mathcal{K}_{2,(X,D)})$ is not surjective.

Let $\mathcal{H}^P_{Y_D}$ denote the exact category of coherent sheaves on Y_D which have cohomological dimension at most one and which are supported on $\{P\} \times D$ so that there is a commutative diagram of the fiber sequences of spectra (see [Srinivas 1991, Theorem 9.1])

$$\begin{array}{ccccc} K(Z) & \longrightarrow & K(X) & \longrightarrow & K(U) \\ \downarrow & & \downarrow & & \downarrow \\ K(\mathcal{H}^P_{Y_D}) & \longrightarrow & K(Y_D) & \longrightarrow & K(V_D) \end{array} \tag{4-2}$$

As in the proof of Lemma 3.2, this diagram canonically extends to a commutative diagram of presheaves of spectra. Let $\mathcal{K}^P_{i,Y_D}$ denote the Zariski sheaf on Z associated to the presheaf of homotopy groups $W \mapsto \pi_i(K(\mathcal{H}^P_{Y_D \cap W}))$. Sheafifying the associated presheaves of homotopy groups and arguing as in the proof of Lemma 3.2, we obtain the commutative diagrams of short exact sequence of Zariski sheaves

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \widetilde{\mathcal{K}}_{2,(X,D)} & \longrightarrow & j_*(\widetilde{\mathcal{K}}_{2,(U,D)}) & \longrightarrow & i_*(\mathcal{K}^P_{1,Z}) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathcal{K}_{2,X} & \longrightarrow & j_*(\widetilde{\mathcal{K}}_{2,U}) & \longrightarrow & \mathcal{K}_{1,Z} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathcal{K}_{2,Y_D} & \longrightarrow & j_*(\mathcal{K}_{1,V_D}) & \longrightarrow & \mathcal{K}^P_{1,Y_D} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array} \tag{4-3}$$

and

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{K}_{1,(Z,D)} & \longrightarrow & \mathcal{K}_{1,Z} & \longrightarrow & \mathcal{K}_{1,\{P\}_D} & \longrightarrow & 0 \\ & & \downarrow & & \| & & \downarrow & & \\ 0 & \longrightarrow & \mathcal{K}^P_{1,Z} & \longrightarrow & \mathcal{K}_{1,Z} & \longrightarrow & \mathcal{K}^P_{1,Y_D} & \longrightarrow & 0 \end{array} \tag{4-4}$$

These diagrams together give rise to a commutative diagram of exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^0(Z,\mathcal{K}_{1,Z}) & \xrightarrow{\iota^*_{(Z,D)}} & H^0(\{P\}_D,\mathcal{K}_{1,\{P\}_D}) & \xrightarrow{\partial_Z} & H^1(Z,\mathcal{K}_{1,(Z,D)}) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle i_*} & & \\ 0 & \longrightarrow & H^1(X,\mathcal{K}_{2,X}) & \xrightarrow{\iota^*_{(X,D)}} & H^1(Y_D,\mathcal{K}_{2,Y_D}) & \xrightarrow[\partial_X]{} & H^2(X,\mathcal{K}_{2,(X,D)}) & \longrightarrow & 0 \end{array} \tag{4-5}$$

The maps ∂_Z and ∂_X are surjective because $H^1(Z,\mathcal{K}_{1,Z}) \simeq \mathrm{CH}_0(Z) = 0 = \mathrm{CH}_2(X) \simeq H^2(X,\mathcal{K}_{2,X})$. By the homotopy invariance of K-theory, the composite map $H^0(Z,\mathcal{K}_{1,Z}) \xrightarrow{\iota^*_{(Z,D)}} H^0(\{P\}_D,\mathcal{K}_{1,\{P\}_D}) \longrightarrow H^0(\{P\},\mathcal{K}_{1,\{P\}})$ is an isomorphism. We claim that the composite map $H^1(X,\mathcal{K}_{2,X}) \xrightarrow{\iota^*_{(X,D)}} H^1(Y_D,\mathcal{K}_{2,Y_D}) \longrightarrow H^1(Y,\mathcal{K}_{2,Y})$ is also an isomorphism.

We have a commutative diagram

$$\begin{array}{ccc} K_1(Y) & \longrightarrow & H^0(Y,\mathcal{K}_{1,Y}) \\ \downarrow & & \downarrow \\ K_1(X) & \longrightarrow & H^0(X,\mathcal{K}_{1,X}) \end{array} \tag{4-6}$$

where the vertical arrows are isomorphisms and the horizontal arrows are split surjections. This implies that the induced pullback map $SK_1(Y) \to SK_1(X)$ is an isomorphism. We now have a commutative diagram

$$\begin{array}{ccc} SK_1(Y) & \longrightarrow & H^1(Y,\mathcal{K}_{2,Y}) \\ \downarrow & & \downarrow \\ SK_1(X) & \longrightarrow & H^1(X,\mathcal{K}_{2,X}) \end{array} \tag{4-7}$$

where the top horizontal arrow is an isomorphism and the bottom horizontal arrow is surjective (see [Krishna and Srinivas 2002, Lemma 2.3]). We have shown above that the left vertical arrow is an isomorphism. This implies that the right vertical arrow is surjective. On the other hand, it is split injective via the 0-section embedding. Hence, it is an isomorphism. This proves the claim.

The claim shows that the first horizontal arrows from left in both rows of (4-5) are split injective. Combining this with Lemmas 3.1 and 3.2, we can identify $i_* : \mathrm{CH}_0(Z, D) \to H^2(X, \mathcal{K}_{2,(X,D)})$ as the map

$$i_* : K_1(\{P\} \times D, \{P\} \times \{0\}) \to H^1(Y_D, \mathcal{K}_{2,(Y_D,Y)}). \tag{4-8}$$

Using [Krishna and Srinivas 2002, Corollary 4.2], this map is same as the map of $\mathbb{Q}$-vector spaces

$$i_* : I \to H^1\Big(Y_D, \frac{\Omega^1_{(Y_D,Y)/\mathbb{Q}}}{d(I_Y)}\Big), \tag{4-9}$$

where I is the ideal sheaf of $\mathrm{Spec}(k)$ inside D, $I_Y = I \otimes_k \mathcal{O}_Y$ and $\Omega^1_{(Y_D,Y)/\mathbb{Q}} = \mathrm{Ker}(\Omega^1_{Y_D/\mathbb{Q}} \twoheadrightarrow \Omega^1_{Y/\mathbb{Q}})$. We are thus reduced to showing that this map of $\mathbb{Q}$-vector spaces is not surjective. Notice that the assumption $m \geq 2$ implies that $I \neq 0$.

By [Krishna and Srinivas 2002, Lemma 4.3], there is a short exact sequence

$$0 \longrightarrow \Omega^1_{k/\mathbb{Q}} \otimes_k I_Y \longrightarrow \frac{\Omega^1_{(Y_D,Y)/\mathbb{Q}}}{d(I_Y)} \longrightarrow \frac{\Omega^1_{(Y_D,Y)/k}}{d_k(I_Y)} \longrightarrow 0.$$

It is easy to check by local calculations that $\frac{\Omega^1_{(Y_D,Y)/k}}{d(I_Y)} \simeq \Omega^1_{Y/\mathbb{Q}} \otimes_k d_k(I)$, where $d_k : I \to \Omega^1_{D/k}$ is the k-derivation. In particular, the above sequence can be written as

$$0 \to (I \otimes_k \Omega^1_{k/\mathbb{Q}}) \otimes_k \mathcal{O}_Y \to \mathcal{K}_{2,(Y_D,Y)} \to d_k(I) \otimes_k \Omega^1_{Y/k} \to 0. \tag{4-10}$$

Taking the associated long exact cohomology sequence, we get a commutative diagram

$$\begin{array}{l} d_k(I) \otimes_k H^0(Y, \Omega^1_{Y/k}) \xrightarrow{\partial} (I \otimes_k \Omega^1_{k/\mathbb{Q}}) \otimes_k H^1(Y, \mathcal{O}_Y) \\ \qquad\qquad\qquad\qquad \longrightarrow H^1(Y_D, \mathcal{K}_{2,(Y_D,Y)}) \longrightarrow d_k(I) \longrightarrow 0 \\ \qquad\qquad\qquad\qquad\qquad\qquad \uparrow{\scriptstyle i_*} \quad \nearrow{\scriptstyle d_k} \\ \qquad\qquad\qquad\qquad\qquad\qquad I \end{array} \tag{4-11}$$

with the top sequence exact.

It is straightforward to check that d_k is an isomorphism. On the other hand, as k has infinite transcendence degree over $\mathbb{Q}$ and Y has positive genus, we see that ∂ is a map of k-vector spaces whose source is finite dimensional but the target is infinite dimensional. This shows that there is a split exact sequence

$$0 \to \frac{(I \otimes_k \Omega^1_{k/\mathbb{Q}}) \otimes_k H^1(Y, \mathcal{O}_Y)}{d_k(I) \otimes_k H^0(Y, \Omega^1_{Y/k})} \to H^1(Y_D, \mathcal{K}_{2,(Y_D,Y)}) \to d_k(I) \to 0 \tag{4-12}$$

such that the first term is an infinite dimensional k-vector space and the composite map $I \xrightarrow{i_*} H^1(Y_D, \mathcal{K}_{2,(Y_D,Y)}) \to d_k(I)$ is an isomorphism. In particular, the cokernel of i_* is an infinite dimensional k-vector space. This finishes the proof of Theorem 1.5. □

Acknowledgements

The author would like to thank Jinhyun Park for his questions related to connections between additive Chow groups and reciprocity functors that led to the section on page 2399. The author would like to thank Marc Levine and Federico Binda for invitation to the university of Duisburg–Essen at Essen in April 2015, where this paper was revised. The author would also like to thank the referee for carefully reading the paper and suggesting valuable improvements.

References

[Binda and Krishna $\geq$ 2015] F. Binda and A. Krishna, "0-cycles with modulus", in preparation.

[Binda and Saito 2014] F. Binda and S. Saito, "Relative cycles with moduli and regulator maps", preprint, 2014. arXiv 1412.0385

[Bloch and Esnault 2003a] S. Bloch and H. Esnault, "The additive dilogarithm", *Doc. Math.* Extra Vol. (2003), 131–155. MR 2005e:19006 Zbl 1052.11048

[Bloch and Esnault 2003b] S. Bloch and H. Esnault, "An additive version of higher Chow groups", *Ann. Sci. École Norm. Sup.* (4) **36**:3 (2003), 463–477. MR 2004c:14035 Zbl 1100.14014

[Fulton 1998] W. Fulton, *Intersection theory*, 2nd ed., Springer, Berlin, 1998. MR 99d:14003 Zbl 0885.14002

[Ivorra and Rülling $\geq$ 2015] F. Ivorra and K. Rülling, "K-groups of reciprocity functors", preprint. To appear in *J. Algebr. Geom.* arXiv 1209.1217

[Kato and Saito 1986] K. Kato and S. Saito, "Global class field theory of arithmetic schemes", pp. 255–331 in *Applications of algebraic K-theory to algebraic geometry and number theory, Part I, II* (Boulder, CO, 1983), edited by S. J. Bloch et al., Contemp. Math. **55**, Amer. Math. Soc., Providence, RI, 1986. MR 88c:11041 Zbl 0614.14001

[Kerz and Saito 2015] M. Kerz and S. Saito, "Chow group of 0-cycles with modulus and higher dimensional class field theory", preprint, 2015. To appear in *Duke J. Math.* arXiv 1304.4400v4

[Kleiman and Altman 1979] S. L. Kleiman and A. B. Altman, "Bertini theorems for hypersurface sections containing a subscheme", *Comm. Algebra* **7**:8 (1979), 775–790. MR 81i:14007 Zbl 0401.14002

[Krishna 2015] A. Krishna, "0-cycles on singular schemes and class field theory", preprint, 2015. arXiv 1502.01515

[Krishna and Levine 2008] A. Krishna and M. Levine, "Additive higher Chow groups of schemes", *J. Reine Angew. Math.* **619** (2008), 75–140. MR 2009d:14005 Zbl 1158.14009

[Krishna and Park 2014] A. Krishna and J. Park, "A module structure and a vanishing theorem for cycles with modulus", preprint, 2014. arXiv 1412.7396

[Krishna and Srinivas 2002] A. Krishna and V. Srinivas, "Zero-cycles and K-theory on normal surfaces", *Ann. of Math.* (2) **156**:1 (2002), 155–195. MR 2003k:14005 Zbl 1060.14015

[Krishna and Srinivas 2007] A. Krishna and V. Srinivas, "Zero cycles on singular varieties", pp. 264–277 in *Algebraic cycles and motives. Vol. 1*, edited by J. Nagel and C. Peters, London Math. Soc. Lecture Note Ser. **343**, Cambridge Univ. Press, 2007. MR 2009b:14014 Zbl 1126.14011

[Levine and Weibel 1985] M. Levine and C. Weibel, "Zero cycles and complete intersections on singular varieties", *J. Reine Angew. Math.* **359** (1985), 106–120. MR 86k:14003 Zbl 0555.14004

[Park 2009] J. Park, "Regulators on additive higher Chow groups", *Amer. J. Math.* **131**:1 (2009), 257–276. MR 2009k:14012 Zbl 1176.14001

[Poonen 2008] B. Poonen, "Smooth hypersurface sections containing a given subscheme over a finite field", *Math. Res. Lett.* **15**:2 (2008), 265–271. MR 2009c:14037 Zbl 1207.14047

[Rülling and Saito 2015] K. Rülling and S. Saito, "Higher Chow groups with modulus and relative Milnor K-theory", preprint, 2015. arXiv 1504.02669

[Rülling and Yamazaki 2014] K. Rülling and T. Yamazaki, "K-groups of reciprocity functors for $\mathbb{G}_a$ and abelian varieties", *J. K-Theory* **14**:3 (2014), 556–569. MR 3349326 Zbl 06471847

[Srinivas 1991] V. Srinivas, *Algebraic K-theory*, Progress in Mathematics **90**, Birkhäuser, Boston, 1991. MR 92j:19001 Zbl 0722.19001

[Suslin and Voevodsky 1996] A. Suslin and V. Voevodsky, "Singular homology of abstract algebraic varieties", *Invent. Math.* **123**:1 (1996), 61–94. MR 97e:14030 Zbl 0896.55002

[Swan 1974] R. G. Swan, "A cancellation theorem for projective modules in the metastable range", *Invent. Math.* **27** (1974), 23–43. MR 51 #12856 Zbl 0297.14003

[Thomason and Trobaugh 1990] R. W. Thomason and T. Trobaugh, "Higher algebraic K-theory of schemes and of derived categories", pp. 247–435 in *The Grothendieck Festschrift, Vol. III*, edited by P. Cartier et al., Progr. Math. **88**, Birkhäuser, Boston, 1990. MR 92f:19001 Zbl 0731.14001

Communicated by Hélène Esnault
Received 2015-06-02 Revised 2015-09-16 Accepted 2015-11-09

amal@math.tifr.res.in *School of Mathematics, Tata Institute of Fundamental Research, 1 Homi Bhabha Road, Colaba, Mumbai 400005, India*

Guidelines for Authors

Authors may submit manuscripts in PDF format on-line at the Submission page at the ANT website.

Originality. Submission of a manuscript acknowledges that the manuscript is original and and is not, in whole or in part, published or under consideration for publication elsewhere. It is understood also that the manuscript will not be submitted elsewhere while under consideration for publication in this journal.

Language. Articles in *ANT* are usually in English, but articles written in other languages are welcome.

Length There is no a priori limit on the length of an *ANT* article, but *ANT* considers long articles only if the significance-to-length ratio is appropriate. Very long manuscripts might be more suitable elsewhere as a memoir instead of a journal article.

Required items. A brief abstract of about 150 words or less must be included. It should be self-contained and not make any reference to the bibliography. If the article is not in English, two versions of the abstract must be included, one in the language of the article and one in English. Also required are keywords and subject classifications for the article, and, for each author, postal address, affiliation (if appropriate), and email address.

Format. Authors are encouraged to use LaTeX but submissions in other varieties of TeX, and exceptionally in other formats, are acceptable. Initial uploads should be in PDF format; after the refereeing process we will ask you to submit all source material.

References. Bibliographical references should be complete, including article titles and page ranges. All references in the bibliography should be cited in the text. The use of BibTeX is preferred but not required. Tags will be converted to the house format, however, for submission you may use the format of your choice. Links will be provided to all literature with known web locations and authors are encouraged to provide their own links in addition to those supplied in the editorial process.

Figures. Figures must be of publication quality. After acceptance, you will need to submit the original source files in vector graphics format for all diagrams in your manuscript: vector EPS or vector PDF files are the most useful.

Most drawing and graphing packages (Mathematica, Adobe Illustrator, Corel Draw, MATLAB, etc.) allow the user to save files in one of these formats. Make sure that what you are saving is vector graphics and not a bitmap. If you need help, please write to graphics@msp.org with details about how your graphics were generated.

White space. Forced line breaks or page breaks should not be inserted in the document. There is no point in your trying to optimize line and page breaks in the original manuscript. The manuscript will be reformatted to use the journal's preferred fonts and layout.

Proofs. Page proofs will be made available to authors (or to the designated corresponding author) at a Web site in PDF format. Failure to acknowledge the receipt of proofs or to return corrections within the requested deadline may cause publication to be postponed.

Algebra & Number Theory

Volume 9 No. 10 2015

1937-0652(2015)9:10;1-#