Algebra & Number Theory

Volume 9

2015

No. 1

msp

Algebra & Number Theory

msp.org/ant

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

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

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

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

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

ALGEBRA AND NUMBER THEORY 9:1 (2015)
dx.doi.org/10.2140/ant.2015.9.1

On Previdi's delooping conjecture for K-theory

Sho Saito

We prove a modified version of Previdi's conjecture stating that the Waldhausen space (K-theory space) of an exact category is delooped by the Waldhausen space (K-theory space) of Beilinson's category of generalized Tate vector spaces. Our modified version states the delooping with nonconnective K-theory spectra, extending and almost including Previdi's original statement. As a consequence we obtain that the negative K-groups of an exact category are given by the 0th K-groups of the idempotent-completed iterated Beilinson categories, extending a theorem of Drinfeld that the first negative K-group of a ring is isomorphic to the 0th K-group of the exact category of Tate modules.

1. Introduction

In his Ph.D. thesis, Previdi [2010] developed a categorical generalization of Kapranov's work [2001] on dimensional and determinantal theories for Tate vector spaces over a field. His main results are formulated in terms of algebraic K-theory, and he observes a certain relation between the K-groups $K_i(\mathcal{A})$ and $K_{i+1}(\underset{\longleftrightarrow}{\lim}\,\mathcal{A})$ for $i = 0, 1$, where $\mathcal{A}$ is an exact category and $\underset{\longleftrightarrow}{\lim}\,\mathcal{A}$ is an associated exact category introduced by Beilinson [1987]. (See Section 2 below.) Previdi concluded the thesis with the following conjecture, which would include all the higher analogues of that relation:

Conjecture 1.1 [Previdi 2010, 5.1.7]. *Write $S(\mathcal{A})$ for the geometric realization of the simplicial category $iS_\bullet(\mathcal{A})$ given by Waldhausen's $S_\bullet$-construction* [1985], *the homotopy groups of whose loop space are the algebraic K-theory groups of the exact category $\mathcal{A}$. If $\mathcal{A}$ is partially abelian, i.e., if it and its opposite have pullbacks of admissible monomorphisms with common target, then $S(\mathcal{A})$ is delooped by $S(\underset{\longleftrightarrow}{\lim}\,\mathcal{A})$. In particular, for such $\mathcal{A}$ there is an isomorphism between $K_i(\mathcal{A})$ and $K_{i+1}(\underset{\longleftrightarrow}{\lim}\,\mathcal{A})$ for every $i \geq 0$.*

In this article we prove the following modified version of the conjecture:

Supported by JSPS Research Fellowships for Young Scientists.
MSC2010: primary 19D35; secondary 14C35.
Keywords: negative K-theory, delooping, Tate vector space.

Theorem 1.2. *Let $\mathbb{K}(\mathcal{A})$ be the nonconnective K-theory spectrum of the exact category $\mathcal{A}$, whose i-th homotopy group is the i-th K-group of $\mathcal{A}$ if $i > 0$, the 0th K-group of the idempotent-completion of $\mathcal{A}$ if $i = 0$, and the $(-i)$-th negative K-group of $\mathcal{A}$ if $i < 0$.* (*See* [Schlichting 2006].) *Then there is a homotopy equivalence of spectra $\mathbb{K}(\mathcal{A}) \xrightarrow{\sim} \Omega\mathbb{K}(\underset{\longleftrightarrow}{\lim}\,\mathcal{A})$.*

Note that no assumption on $\mathcal{A}$ is necessary. We also remark that Theorem 1.2 includes almost all of the essential part of Conjecture 1.1. Indeed, there results an isomorphism $K_i(\mathcal{A}) \xrightarrow{\sim} K_{i+1}(\underset{\longleftrightarrow}{\lim}\,\mathcal{A})$ for any $\mathcal{A}$ and for every $i \geq 1$. If $\mathcal{A}$ is idempotent-complete (this is the case for most of the typical examples, such as the category $\mathcal{P}(R)$ of finitely generated projective modules over a ring R, the category of vector bundles on a scheme, or any abelian category) this holds also for $i = 0$. Theorem 1.2 moreover says that the i-th negative K-group $K_{-i}(\mathcal{A})$, $i > 0$, is isomorphic to the 0th K-group of the idempotent-completion of the i-times iterated Beilinson category $\underset{\longleftrightarrow}{\lim}{}^i\mathcal{A}$.

Applications to the study of generalized Tate vector spaces. Previdi's work has its background in the study of generalized Tate vector spaces. Recall that a *Tate vector space* over a discrete field k is a topological k-vector space of the form $P \oplus Q^*$, where P and Q are discrete spaces and $(-)^*$ denotes the topological dual. There is a canonical equivalence of the Beilinson category $\underset{\longleftrightarrow}{\lim}\,\mathrm{Vect}_0\, k$ of the exact category $\mathrm{Vect}_0\, k$ of finite-dimensional k-vector spaces, with the category of Tate k-vector spaces of countable type, i.e., Tate vector spaces of the form $P \oplus Q^*$ with P and Q discrete of countable dimensions. (See [Previdi 2011, 7.4].)

There are two generalizations of this notion, one of which due to Arkhipov and Kremnizer [2010] is the notion of an *n-Tate vector space* as an object of the n-times iterated Beilinson category $\underset{\longleftrightarrow}{\lim}{}^n\mathrm{Vect}_0\, k$, $n \geq 1$. The other one, due to Drinfeld [2006], replaces the field k with a general commutative ring R to get the notion of a *Tate R-module*. (We assume commutativity for simplicity, although Drinfeld's definition makes sense for noncommutative rings.) More precisely, Drinfeld defined an *elementary Tate R-module* to be a topological R-module of the form $P \oplus Q^*$, where P and Q are discrete projective R-modules, and a *Tate R-module* to be a direct summand of an elementary Tate R-module. Drinfeld [2006, Theorem 3.6(iii)] showed that the first negative K-group $K_{-1}(R)$ of the ring R is isomorphic to the 0th K-group of the exact category of Tate R-modules. A very important theorem on Tate R-modules, due to [Drinfeld 2006, Theorems 3.4, 3.7], is that they are Nisnevich-locally elementary, so that the presheaf of first negative K-groups on the Nisnevich site of Spec R becomes trivial after Nisnevich-sheafification.

The former of the two generalizations is obtained purely formally by iterating the Beilinson construction, whereas the latter is based on nontrivial facts in ring theory. In fact, these two generalizations can be combined together. The equivalence of $\underleftrightarrow{\lim}\,\mathrm{Vect}_0\, k$ with Tate k-vector spaces of countable type can be generalized to show that $\underleftrightarrow{\lim}\,\mathcal{P}(R)$ is very close to the category of elementary Tate R-modules. (More precisely, $\underleftrightarrow{\lim}\,\mathcal{P}(R)$ is equivalent to the category of topological R-modules isomorphic to extensions of P and Q^*, where P and Q are discrete R-modules obtained as the inductive limits of systems

$$P_1 \hookrightarrow P_2 \hookrightarrow P_3 \hookrightarrow \cdots \quad \text{and} \quad Q_1 \hookrightarrow Q_2 \hookrightarrow Q_3 \hookrightarrow \cdots$$

This in particular shows that the idempotent-completion of $\underleftrightarrow{\lim}\,\mathcal{P}(R)$ is very close to the category of Tate R-modules. Most objects of the latter category which one usually deals with can be considered as objects of the former, and vice versa. In this sense, we regard the idempotent-completion of $\underleftrightarrow{\lim}\,\mathcal{P}(R)$ as a categorical substitute for Drinfeld's category of Tate R-modules. It is thus plausible to define an *n-Tate R-module*, $n \geq 1$, as an object of the idempotent-completion of $\underleftrightarrow{\lim}^{\,n}\mathcal{P}(R)$. Theorem 1.2 then can be regarded as a generalization of Theorem 3.6(iii) of [Drinfeld 2006], as it says that the n-th negative K-group $K_{-n}(R)$ is isomorphic to the 0th K-group of n-Tate R-modules.

We also briefly discuss here a consequence of Theorem 1.2 on 1-Tate modules. Denote by $\mathcal{K}$ the sheaf of group-like E_∞-spaces on the Nisnevich site of Spec R, that sends an étale R-algebra S to the space $\Omega^\infty\mathbb{K}(S)$. We describe how our Theorem 1.2, together with Drinfeld's theorem on the Nisnevich-local vanishing of K_{-1}, provides a purely formal way to associate to a 1-Tate R-module M a $\mathcal{K}$-torsor with a canonical action of the sheaf of groups of automorphisms of M. We note that this construction was essentially explained by Drinfeld [2006, Section 5.5], who attributes it to Beilinson.

Firstly, Theorem 1.2 shows that, in the ∞-topos of sheaves of spaces on the Nisnevich site of Spec R, the sheaf $S \mapsto \Omega^\infty\mathbb{K}(\underleftrightarrow{\lim}\,\mathcal{P}(S))$ is an object whose loop-space object is $\mathcal{K}$. It is obviously a pointed object. In addition, Drinfeld's theorem on the Nisnevich-local vanishing of K_{-1} tells that this object is connected, i.e., $S \mapsto \Omega^\infty\mathbb{K}(\underleftrightarrow{\lim}\,\mathcal{P}(S))$ is the classifying-space object for the ∞-group object $\mathcal{K}$. Then by general theory a $\mathcal{K}$-torsor corresponds to a map from the terminal object to the sheaf $S \mapsto \Omega^\infty\mathbb{K}(\underleftrightarrow{\lim}\,\mathcal{P}(S))$, i.e., to a point of the space $\Omega^\infty\mathbb{K}(\underleftrightarrow{\lim}\,\mathcal{P}(R))$. Thus the 1-Tate R-module M, as an object of the idempotent-completion of $\underleftrightarrow{\lim}\,\mathcal{P}(R)$, defines such a torsor. The sheaf of groups of automorphisms of M acts on it since, in general, for any idempotent-complete exact category $\mathcal{A}$ and an object A of $\mathcal{A}$, the classifying space of $\mathrm{Aut}_{\mathcal{A}}\, A$ admits a natural, canonical mapping to $\Omega S(\mathcal{A}) = \Omega^\infty\mathbb{K}(\mathcal{A})$ which sends the base point to the point of $\Omega S(\mathcal{A}) = \Omega^\infty\mathbb{K}(\mathcal{A})$ defined by the object A. (This is the composition of the map $B\,\mathrm{Aut}_{\mathcal{A}}\, A \to Bi\mathcal{A}$ with the first structure map $Bi\mathcal{A} \to \Omega S(\mathcal{A})$ of Waldhausen's connective algebraic

K-theory spectrum of $\mathcal{A}$, where $i\mathcal{A}$ is the category of isomorphisms of $\mathcal{A}$, and B indicates the classifying space of a category.)

Organization and conventions. In Section 2 we recall the definition and properties of the Beilinson category $\underleftrightarrow{\lim}\,\mathcal{A}$, following [Beilinson 1987] and [Previdi 2011]. We recall the notions of ind- and pro-objects, introduce the categories $\mathrm{Ind}^a_{\mathbb{N}}\,\mathcal{A}$ and $\mathrm{Pro}^a_{\mathbb{N}}\,\mathcal{A}$, and discuss their relation to $\underleftrightarrow{\lim}\,\mathcal{A}$. All statements in this section are either results of [Beilinson 1987] and [Previdi 2011] or their immediate consequences.

Section 3 begins by recalling Schlichting's results [2004], which provide a powerful tool for constructing a homotopy fibration sequence of nonconnective K-theory spectra. We prove Theorem 1.2 according to the following strategy: We construct, using Schlichting's method, two homotopy fibration sequences which fit into the commutative diagram

$$\begin{tikzcd}
\mathbb{K}(\mathcal{A}) \arrow[r] \arrow[d] & \mathbb{K}(\mathrm{Ind}^a_{\mathbb{N}}\,\mathcal{A}) \arrow[r] \arrow[d] & \mathbb{K}(\mathrm{Ind}^a_{\mathbb{N}}\,\mathcal{A}/\mathcal{A}) \arrow[d] \\
\mathbb{K}(\mathrm{Pro}^a_{\mathbb{N}}\,\mathcal{A}) \arrow[r] & \mathbb{K}(\underleftrightarrow{\lim}\,\mathcal{A}) \arrow[r] & \mathbb{K}(\underleftrightarrow{\lim}\,\mathcal{A}/\,\mathrm{Pro}^a_{\mathbb{N}}\,\mathcal{A})
\end{tikzcd}$$

as the horizontal sequences. We then go on to show that the third vertical map is an equivalence, and that in the left-hand square the upper-right and lower-left corners are contractible, so that the stated homotopy equivalence is obtained. (We remark that the upper horizontal homotopy fibration sequence and its consequence that $\mathbb{K}(\mathcal{A})$ is delooped by $\mathbb{K}(\mathrm{Ind}^a_{\mathbb{N}}\,\mathcal{A}/\mathcal{A})$ are Schlichting's results [2004]. Our delooping is a combination of his delooping with its dual.)

We follow the notation adopted in [Previdi 2010; 2011]. For instance, we write $\mathrm{Ind}^a_{\mathbb{N}}\,\mathcal{A}$ for what is denoted by $\mathcal{F}\mathcal{A}$ in [Schlichting 2004], and $\mathrm{Fun}^a(\Pi,\mathcal{A})$ instead of the notation $\mathbf{A}^{\Pi}_a$ used in [Beilinson 1987]. We write $\tilde{\mathcal{A}}$ for the idempotent-completion of $\mathcal{A}$. By saying a functor $\mathcal{A}\hookrightarrow\mathcal{U}$ between exact categories is an *embedding of exact categories*, we mean that it is a fully faithful exact functor whose essential image is closed under extensions in $\mathcal{U}$ and such that a short sequence in $\mathcal{A}$ is exact if and only if its image in $\mathcal{U}$ is exact.

2. Beilinson's category $\underleftrightarrow{\lim}\,\mathcal{A}$

2A. ***ind- and pro-objects in a category.*** We first recall some generalities on ind- and pro-objects. For any category $\mathcal{C}$, the category $\mathrm{Ind}\,\mathcal{C}$ (resp. $\mathrm{Pro}\,\mathcal{C}$) of *ind-objects* (resp. *pro-objects*) in $\mathcal{C}$ is defined to have as objects functors $\mathcal{X}: J\to\mathcal{C}$ with domain J small and filtering (resp. $\mathcal{X}: I^{\mathrm{op}}\to\mathcal{C}$ with I small and filtering). The ind-object $\mathcal{X}: J\to\mathcal{C}$ (resp. pro-object $\mathcal{X}: I^{\mathrm{op}}\to\mathcal{C}$) defines a functor $\mathcal{C}^{\mathrm{op}}\to$ (sets), $C\mapsto \varinjlim_{j\in J}\mathrm{Hom}_{\mathcal{C}}(C,\mathcal{X}_j)$ (resp. $\mathcal{C}\to$ (sets), $C\mapsto\varinjlim_{i\in I}\mathrm{Hom}_{\mathcal{C}}(\mathcal{X}_i,C)$). A morphism $\mathcal{X}\to\mathcal{Y}$ of ind-objects (resp. pro-objects) is a natural transformation between the functors $\mathcal{C}^{\mathrm{op}} \to$ (sets) (resp. $\mathcal{C} \to$ (sets)) associated to $\mathcal{X}$ and $\mathcal{Y}$. Equivalently, the sets of morphisms of ind- and pro-objects can be defined to be the projective-inductive limits $\mathrm{Hom}_{\mathrm{Ind}\,\mathcal{C}}(\mathcal{X},\mathcal{Y}) = \varprojlim_j \varinjlim_l \mathrm{Hom}_{\mathcal{C}}(\mathcal{X}_j,\mathcal{Y}_l)$ and $\mathrm{Hom}_{\mathrm{Pro}\,\mathcal{C}}(\mathcal{X},\mathcal{Y}) = \varprojlim_k \varinjlim_i \mathrm{Hom}_{\mathcal{C}}(\mathcal{X}_i,\mathcal{Y}_k)$, respectively.

If $\mathcal{X}$ and $\mathcal{Y}$ have a common index category, a natural transformation $\mathcal{X} \to \mathcal{Y}$ between the functors $\mathcal{X}$ and $\mathcal{Y}$ defines a map between the ind- or pro-objects $\mathcal{X}$ and $\mathcal{Y}$. Conversely, every map of ind- or pro-objects $\mathcal{X} \to \mathcal{Y}$ can be "straightified" to a natural transformation, in the sense that there is a commutative diagram in $\mathrm{Ind}\,\mathcal{C}$ or $\mathrm{Pro}\,\mathcal{C}$

$$\begin{tikzcd}
\mathcal{X} \arrow[r] \arrow[d, "\sim"'] & \mathcal{Y} \arrow[d, "\sim"'] \\
\tilde{\mathcal{X}} \arrow[r] & \tilde{\mathcal{Y}}
\end{tikzcd}$$

with the vertical maps isomorphisms, $\tilde{\mathcal{X}}$ and $\tilde{\mathcal{Y}}$ having a common index category, and $\tilde{\mathcal{X}} \to \tilde{\mathcal{Y}}$ coming from a natural transformation. (See [Artin and Mazur 1969, Appendix] for details.)

If $\mathcal{C}$ is an exact category, the categories $\mathrm{Ind}\,\mathcal{C}$ and $\mathrm{Pro}\,\mathcal{C}$ possess exact structures. A pair of composable morphisms in $\mathrm{Ind}\,\mathcal{C}$ or $\mathrm{Pro}\,\mathcal{C}$ is a short exact sequence if it can be straightified to a sequence of natural transformations which is levelwise exact in $\mathcal{C}$ [Previdi 2011, 4.15, 4.16]. In this article we are mainly concerned with the full subcategories $\mathrm{Ind}^a\,\mathcal{C}$ and $\mathrm{Pro}^a\,\mathcal{C}$ of *admissible ind-* and *pro-objects* introduced in [Previdi 2011, 5.6]: An ind-object $\mathcal{X} : J \to \mathcal{C}$ (resp. pro-object $\mathcal{X} : I^{\mathrm{op}} \to \mathcal{C}$) is *admissible* if for every map $j \to j'$ in J (resp. $i \to i'$ in I) the morphism $X_j \hookrightarrow X_{j'}$ is an admissible monomorphism in $\mathcal{C}$ (resp. $X_i \twoheadleftarrow X_{i'}$ is an admissible epimorphism). These subcategories are extension-closed in the exact categories $\mathrm{Ind}\,\mathcal{C}$ and $\mathrm{Pro}\,\mathcal{C}$, respectively, so they have induced exact structures. Since an object C of $\mathcal{C}$ can be considered as an admissible ind- or pro-object which takes the constant value C (one can use any small and filtering category as the category of indices), there are embeddings of exact categories $\mathcal{C} \hookrightarrow \mathrm{Ind}^a\,\mathcal{C}$ and $\mathcal{C} \hookrightarrow \mathrm{Pro}^a\,\mathcal{C}$.

We write $\mathrm{Ind}^a_{\mathbb{N}}\,\mathcal{C}$ and $\mathrm{Pro}^a_{\mathbb{N}}\,\mathcal{C}$ for the full, extension-closed subcategories of $\mathrm{Ind}^a\,\mathcal{C}$ and $\mathrm{Pro}^a\,\mathcal{C}$ consisting of admissible ind- and pro-objects, respectively, indexed by the filtering category of natural numbers. (There is precisely one morphism $j \to k$ if $j \le k \in \mathbb{N}$.) The object C of $\mathcal{C}$ defines an object $C = C = C = \cdots$ in $\mathrm{Ind}^a_{\mathbb{N}}\,\mathcal{C}$ or $\mathrm{Pro}^a_{\mathbb{N}}\,\mathcal{C}$. Note that the resulting embedding $\mathcal{C} \hookrightarrow \mathrm{Ind}^a_{\mathbb{N}}\,\mathcal{C} \hookrightarrow \mathrm{Ind}^a\,\mathcal{C}$ (resp. $\mathcal{C} \hookrightarrow \mathrm{Pro}^a_{\mathbb{N}}\,\mathcal{C} \hookrightarrow \mathrm{Pro}^a\,\mathcal{C}$) is naturally isomorphic to the embedding $\mathcal{C} \hookrightarrow \mathrm{Ind}^a\,\mathcal{C}$ (resp. $\mathcal{C} \hookrightarrow \mathrm{Pro}^a\,\mathcal{C}$) mentioned above.

2B. ***Definition of*** $\underleftrightarrow{\lim}\,\mathcal{A}$. Let $\mathcal{A}$ be an exact category. We write Π for the ordered set $\{(i,j) \in \mathbb{Z} \times \mathbb{Z} \mid i \le j\}$, where $(i,j) \le (i',j')$ if $i \le i'$ and $j \le j'$. A functor $X : \Pi \to \mathcal{A}$, where Π is viewed as a filtering category, is *admissible* if for every triple $i \le j \le k$, the sequence $X_{i,j} \hookrightarrow X_{i,k} \twoheadrightarrow X_{j,k}$ is a short exact sequence in $\mathcal{A}$. We denote by $\mathrm{Fun}^a(\Pi, \mathcal{A})$ the exact category of admissible functors $X : \Pi \to \mathcal{A}$ and natural transformations, where a short sequence $X \to Y \to Z$ of natural transformations of admissible functors is a short exact sequence in $\mathrm{Fun}^a(\Pi, \mathcal{A})$ if $X_{i,j} \hookrightarrow Y_{i,j} \twoheadrightarrow Z_{i,j}$ is a short exact sequence in $\mathcal{A}$ for every $i \le j$. A bicofinal map $\phi : \mathbb{Z} \to \mathbb{Z}$ (ϕ is said to be *bicofinal* if it is nondecreasing and satisfies $\lim_{i\to\pm\infty} \phi(i) = \pm\infty$) induces a cofinal functor $\tilde{\phi} : \Pi \to \Pi$, $(i, j) \mapsto (\phi(i), \phi(j))$. If ϕ and $\psi : \mathbb{Z} \to \mathbb{Z}$ are bicofinal maps such that $\phi(i) \le \psi(i)$ for all i, and if $X : \Pi \to \mathcal{A}$ is an admissible functor, then there is a natural transformation $u_{X,\phi,\psi} : X \circ \tilde{\phi} \to X \circ \tilde{\psi}$.

Definition 2.1 [Beilinson 1987, A.3]. The category $\underleftrightarrow{\lim}\, \mathcal{A}$ is defined to be the localization of $\mathrm{Fun}^a(\Pi, \mathcal{A})$ by the morphisms $u_{X,\phi,\psi}$, where $X : \Pi \to \mathcal{A}$ is in $\mathrm{Fun}^a(\Pi, \mathcal{A})$ and $\phi \le \psi : \mathbb{Z} \to \mathbb{Z}$ are bicofinal.

If $X : \Pi \to \mathcal{A}$ is an admissible functor, we have for each $j \in \mathbb{Z}$ an admissible pro-object $X_{\bullet,j} : \{i \in \mathbb{Z} \mid i \le j\} \to \mathcal{A}$, $i \mapsto X_{i,j}$, in $\mathcal{A}$. We get in turn an admissible ind-object $\mathbb{Z} \to \mathrm{Pro}^a \mathcal{A}$, $j \mapsto X_{\bullet,j}$, in $\mathrm{Pro}^a \mathcal{A}$. Thus the admissible functor X can be viewed as an object of the iterated Ind-Pro category $\mathrm{Ind}^a\, \mathrm{Pro}^a \mathcal{A}$. If $\phi \le \psi : \mathbb{Z} \to \mathbb{Z}$ are bicofinal, the map $u_{X,\phi,\psi}$ defines an isomorphism between the ind-pro-objects $X \circ \tilde{\phi}$ and $X \circ \tilde{\psi}$. We get a functor $\underleftrightarrow{\lim}\, \mathcal{A} \to \mathrm{Ind}^a\, \mathrm{Pro}^a \mathcal{A}$. In view of the following theorem, we regard $\underleftrightarrow{\lim}\, \mathcal{A}$ as an exact subcategory of $\mathrm{Ind}^a\, \mathrm{Pro}^a \mathcal{A}$.

Theorem 2.2 [Previdi 2011, 5.8, 6.1]. *The functor* $\underleftrightarrow{\lim}\, \mathcal{A} \to \mathrm{Ind}^a\, \mathrm{Pro}^a \mathcal{A}$ *is fully faithful. Moreover, the image is closed under extensions in* $\mathrm{Ind}^a\, \mathrm{Pro}^a \mathcal{A}$. *In particular,* $\underleftrightarrow{\lim}\, \mathcal{A}$ *has an exact structure in which a sequence in* $\underleftrightarrow{\lim}\, \mathcal{A}$ *is exact if and only if its image in* $\mathrm{Ind}^a\, \mathrm{Pro}^a \mathcal{A}$ *is exact.*

By [Previdi 2011, 6.3], there are embeddings $\mathrm{Ind}^a_{\mathbb{N}} \mathcal{A} \hookrightarrow \underleftrightarrow{\lim}\, \mathcal{A}$ and $\mathrm{Pro}^a_{\mathbb{N}} \mathcal{A} \hookrightarrow \underleftrightarrow{\lim}\, \mathcal{A}$ of exact categories, respectively sending $X_1 \hookrightarrow X_2 \hookrightarrow X_3 \hookrightarrow \cdots \in \mathrm{ob}\, \mathrm{Ind}^a_{\mathbb{N}} \mathcal{A}$ to the object in $\underleftrightarrow{\lim}\, \mathcal{A}$ determined by $X_{i,j} = X_{0,j} = X_j$ for $i \le 0 < j$, and sending $X_1 \twoheadleftarrow X_2 \twoheadleftarrow X_3 \twoheadleftarrow \cdots \in \mathrm{ob}\, \mathrm{Pro}^a_{\mathbb{N}} \mathcal{A}$ to the object in $\underleftrightarrow{\lim}\, \mathcal{A}$ determined by $X_{i,j} = X_{i,1} = X_{-i+1}$ for $i \le 0 < j$.

We refer to [Previdi 2011] for detailed discussion of ind/pro-objects in exact categories.

3. Proof of Theorem 1.2

We prove the theorem using the s-filtering localization sequence constructed by Schlichting [2004].

Let $\mathcal{A} \hookrightarrow \mathcal{U}$ be an embedding of exact categories. Following [Schlichting 2004], we define a map in $\mathcal{U}$ to be a *weak isomorphism* with respect to $\mathcal{A} \hookrightarrow \mathcal{U}$ if it is either an admissible monomorphism that admits a cokernel in the essential image of $\mathcal{A} \hookrightarrow \mathcal{U}$ or an admissible epimorphism that admits a kernel in the essential image of $\mathcal{A} \hookrightarrow \mathcal{U}$. In particular, for every $A \in \operatorname{ob}\mathcal{A}$, the maps $0 \to A$ and $A \to 0$ are weak isomorphisms. The localization of $\mathcal{U}$ by weak isomorphisms with respect to $\mathcal{A}$ is denoted by $\mathcal{U}/\mathcal{A}$. Recall, from [Schlichting 2004], that the embedding $\mathcal{A} \hookrightarrow \mathcal{U}$ of exact categories is a *left s-filtering* if the following conditions are satisfied:

(1) If $A \twoheadrightarrow U$ is an admissible epimorphism in $\mathcal{U}$ with $A \in \operatorname{ob}\mathcal{A}$, then $U \in \operatorname{ob}\mathcal{A}$.

(2) If $U \hookrightarrow A$ is an admissible monomorphism in $\mathcal{U}$ with $A \in \operatorname{ob}\mathcal{A}$, then $U \in \operatorname{ob}\mathcal{A}$.

(3) Every map $A \to U$ in $\mathcal{U}$ with $A \in \operatorname{ob}\mathcal{A}$ factors through an object $B \in \operatorname{ob}\mathcal{A}$ such that $B \hookrightarrow U$ is an admissible monomorphism in $\mathcal{U}$.

(4) If $U \twoheadrightarrow A$ is an admissible epimorphism in $\mathcal{U}$ with $A \in \operatorname{ob}\mathcal{A}$, then there is an admissible monomorphism $B \hookrightarrow U$ with $B \in \operatorname{ob}\mathcal{A}$ such that the composition $B \twoheadrightarrow A$ is an admissible epimorphism in $\mathcal{A}$.

(Here $\operatorname{ob}\mathcal{A}$ denotes by slight abuse of notation the collection of objects of $\mathcal{U}$ contained in the essential image of $\mathcal{A} \hookrightarrow \mathcal{U}$.) A *right s-filtering* embedding is defined by dualizing the conditions above.

We use the following theorem, due to [Schlichting 2004, 1.16, 1.20, 2.10], as the main technical tool for the proof:

Theorem 3.1. *If $\mathcal{A} \hookrightarrow \mathcal{U}$ is left or right s-filtering, then the localization $\mathcal{U}/\mathcal{A}$ has an exact structure in which a short sequence is exact if and only if it is isomorphic to the image of a short exact sequence in $\mathcal{U}$. Moreover, the sequence of exact categories $\mathcal{A} \to \mathcal{U} \to \mathcal{U}/\mathcal{A}$ induces a homotopy fibration $\mathbb{K}(\mathcal{A}) \to \mathbb{K}(\mathcal{U}) \to \mathbb{K}(\mathcal{U}/\mathcal{A})$ of nonconnective K-theory spectra.*

Remark. Theorem 2.10 of [Schlichting 2004], which constructs this homotopy fibration sequence, is stated there under the assumption that $\mathcal{A}$ is idempotent-complete. But the theorem holds for general $\mathcal{A}$ in view of Lemma 1.20 of [loc. cit.], which assures, whenever $\mathcal{A} \hookrightarrow \mathcal{U}$ is left or right s-filtering, the existence of an extension-closed full subcategory $\widetilde{\mathcal{U}}^{\mathcal{A}}$ of $\widetilde{\mathcal{U}}$ such that $\mathcal{U}$ is cofinally contained in $\widetilde{\mathcal{U}}^{\mathcal{A}}$, the induced embedding $\widetilde{\mathcal{A}} \hookrightarrow \widetilde{\mathcal{U}}$ factors through a left or right s-filtering embedding $\widetilde{\mathcal{A}} \hookrightarrow \widetilde{\mathcal{U}}^{\mathcal{A}}$, and $\mathcal{U}/\mathcal{A} \xrightarrow{\sim} \widetilde{\mathcal{U}}^{\mathcal{A}}/\widetilde{\mathcal{A}}$ is an equivalence of exact categories. The homotopy fibration sequence $\mathbb{K}(\widetilde{\mathcal{A}}) \to \mathbb{K}(\widetilde{\mathcal{U}}^{\mathcal{A}}) \to \mathbb{K}(\widetilde{\mathcal{U}}^{\mathcal{A}}/\widetilde{\mathcal{A}})$ is equivalent to the sequence $\mathbb{K}(\mathcal{A}) \to \mathbb{K}(\mathcal{U}) \to \mathbb{K}(\mathcal{U}/\mathcal{A})$, since a cofinal embedding of exact categories induces an equivalence of nonconnective K-theory spectra.

Lemma 3.2. *For any exact category $\mathcal{A}$, the embedding $\mathcal{A} \hookrightarrow \operatorname{Ind}^a\mathcal{A}$ is left s-filtering.*

Proof. We start by checking condition (3) for being left s-filtering. Let X be an object of $\mathcal{A}$ and Y an admissible ind-object in $\mathcal{A}$ indexed by a small filtering category J. A morphism $f : X \to Y$ in $\operatorname{Ind}^a\mathcal{A}$ is an element of $\varinjlim_{j\in J} \operatorname{Hom}_{\mathcal{A}}(X, Y_j)$, i.e., is represented as the class of a map $f_{j_0} : X \to Y_{j_0}$ in $\mathcal{A}$ for some $j_0 \in J$. The canonical map $Y_{j_0} \hookrightarrow Y$ is an admissible monomorphism because the diagram $j_0/J \to \mathcal{A}$, $j \mapsto Y_j/Y_{j_0}$, serves as its cokernel, where j_0/J is the under-category of j_0. We get a factorization

$$f : X \xrightarrow{f_{j_0}} Y_{j_0} \hookrightarrow Y,$$

as desired.

Condition (1) follows from (3). Indeed, an admissible epimorphism $X \twoheadrightarrow Y$ with X in $\mathcal{A}$ factors through some Z in $\mathcal{A}$ such that $Z \hookrightarrow Y$ is an admissible monomorphism. The composition $X \twoheadrightarrow Y \twoheadrightarrow Y/Z$ is 0, but since this composition is also an admissible epimorphism, Y/Z must be 0. This forces Y to be essentially constant.

To prove (4), let $Y \twoheadrightarrow X$ be an admissible epimorphism in $\mathrm{Ind}^a \mathcal{A}$ with X in $\mathcal{A}$, whose kernel we denote by Z. The short exact sequence $0 \to Z \hookrightarrow Y \twoheadrightarrow X \to 0$ is isomorphic to a straight exact sequence $0 \to Z' \hookrightarrow Y' \twoheadrightarrow X' \to 0$, where Z', Y', and X' are all indexed by the same small filtering category J and are respectively isomorphic to Z, Y, and X. The isomorphism $X' \xrightarrow{\sim} X$ is a compatible collection of morphisms $g_j : X'_j \to X$ in $\mathcal{A}$, $j \in J$, such that there is a morphism $h : X \to X'_{j_0}$ for some $j_0 \in J$ such that $g_{j_0} \circ h = \mathrm{id}_X$ and $h \circ g_{j_0}$ is equivalent to $\mathrm{id}_{X'_{j_0}}$ in $\varinjlim_{j \in J} \mathrm{Hom}_{\mathcal{A}}(X'_{j_0}, X'_j)$. Since X' is an admissible ind-object, this implies that $h \circ g_{j_0} = \mathrm{id}_{X'_{j_0}}$, i.e., g_{j_0} is an isomorphism. (Note also that the g_j are isomorphisms for all $j \in j_0/J$.) The map $Y'_{j_0} \hookrightarrow Y' \xrightarrow{\sim} Y$ is an admissible monomorphism, as noted above, and its composition with $Y \twoheadrightarrow X$ equals the composition $Y'_{j_0} \twoheadrightarrow X'_{j_0} \xrightarrow[g_{j_0}]{\sim} X$, which is an admissible epimorphism in $\mathcal{A}$.

Finally, if $Y \hookrightarrow X$ is an admissible monomorphism with X in $\mathcal{A}$, its cokernel Z is in $\mathcal{A}$ by condition (1). Let $0 \to Y' \hookrightarrow X' \twoheadrightarrow Z' \to 0$ be a straightification of the exact sequence $0 \to Y \hookrightarrow X \twoheadrightarrow Z \to 0$, whose common indices we denote by J. Then an argument similar to above shows that there is a $j_0 \in J$ such that X'_j and Z'_j are isomorphic to X and Z, respectively, for every $j \in j_0/J$. It follows that Y'_j is essentially constant above j_0, and we conclude that Y is contained in the essential image of $\mathcal{A}$, verifying condition (2). □

We remark that, given a composable pair of embeddings of exact categories $\mathcal{A} \hookrightarrow \mathcal{V}$ and $\mathcal{V} \hookrightarrow \mathcal{U}$, if their composition is naturally isomorphic to a left s-filtering embedding $\mathcal{A} \hookrightarrow \mathcal{U}$ then $\mathcal{A} \hookrightarrow \mathcal{V}$ is also left s-filtering. This in particular implies that the embeddings $\mathcal{A} \hookrightarrow \mathrm{Ind}^a_{\mathbb{N}} \mathcal{A}$ and $\mathrm{Pro}^a_{\mathbb{N}} \mathcal{A} \hookrightarrow \underleftrightarrow{\lim} \mathcal{A}$ are left s-filtering. Hence by Theorem 3.1 we get two homotopy fibration sequences of nonconnective K-theory spectra $\mathbb{K}(\mathcal{A}) \to \mathbb{K}(\mathrm{Ind}^a_{\mathbb{N}} \mathcal{A}) \to \mathbb{K}(\mathrm{Ind}^a_{\mathbb{N}} \mathcal{A}/\mathcal{A})$ and $\mathbb{K}(\mathrm{Pro}^a_{\mathbb{N}} \mathcal{A}) \to \mathbb{K}(\underleftrightarrow{\lim} \mathcal{A}) \to \mathbb{K}(\underleftrightarrow{\lim} \mathcal{A}/\mathrm{Pro}^a_{\mathbb{N}} \mathcal{A})$. We compare these sequences to obtain Theorem 1.2.

Lemma 3.3. *There is an equivalence* $\mathrm{Ind}^a_{\mathbb{N}} \mathcal{A}/\mathcal{A} \xrightarrow{\sim} \underleftrightarrow{\lim} \mathcal{A}/\mathrm{Pro}^a_{\mathbb{N}} \mathcal{A}$.

Proof. We have a commutative diagram

$$\begin{tikzcd}
\mathcal{A} \arrow[r] \arrow[d] & \mathrm{Ind}^a_{\mathbb{N}}\,\mathcal{A} \arrow[d] \\
\mathrm{Pro}^a_{\mathbb{N}}\,\mathcal{A} \arrow[r] & \underset{\longleftrightarrow}{\lim}\,\mathcal{A}
\end{tikzcd}$$

whence there results a functor $F : \mathrm{Ind}^a_{\mathbb{N}}\,\mathcal{A}/\mathcal{A} \to \underset{\longleftrightarrow}{\lim}\,\mathcal{A}/\,\mathrm{Pro}^a_{\mathbb{N}}\,\mathcal{A}$.

To construct a quasi-inverse, first we note that the functor $\mathrm{Fun}^a(\Pi,\mathcal{A}) \to \mathrm{Ind}^a_{\mathbb{N}}\,\mathcal{A}$, $(X_{i,j})_{i\le j} \mapsto X_{0,1} \hookrightarrow X_{0,2} \hookrightarrow \cdots$, induces a functor $\widetilde{G} : \underset{\longleftrightarrow}{\lim}\,\mathcal{A} \to \mathrm{Ind}^a_{\mathbb{N}}\,\mathcal{A}/\mathcal{A}$. Indeed, if $\phi \le \psi : \mathbb{Z} \to \mathbb{Z}$ are bicofinal, the map $u_{X,\phi,\psi} : X\circ\widetilde{\phi} \to X\circ\widetilde{\psi}$ in $\mathrm{Fun}^a(\Pi,\mathcal{A})$ is sent to the map $X_{\phi(0),\phi(\bullet)} \to X_{\psi(0),\psi(\bullet)}$, which factors as $X_{\phi(0),\phi(\bullet)} \hookrightarrow X_{\phi(0),\psi(\bullet)} \twoheadrightarrow X_{\psi(0),\psi(\bullet)}$. The map $X_{\phi(0),\phi(\bullet)} \hookrightarrow X_{\phi(0),\psi(\bullet)}$ is an isomorphism in $\mathrm{Ind}^a_{\mathbb{N}}\,\mathcal{A}$, since it consists of natural isomorphisms

$$\varinjlim_j \mathrm{Hom}_{\mathcal{A}}(A, X_{\phi(0),\phi(j)}) \xrightarrow{\sim} \varinjlim_j \mathrm{Hom}_{\mathcal{A}}(A, X_{\phi(0),\psi(j)}), \quad A \in \mathrm{ob}\,\mathcal{A},$$

as ϕ and ψ are bicofinal. We also see that $X_{\phi(0),\psi(\bullet)} \twoheadrightarrow X_{\psi(0),\psi(\bullet)}$ is a weak isomorphism in $\mathrm{Ind}^a_{\mathbb{N}}\,\mathcal{A}$ with respect to $\mathcal{A}$, since it has constant kernel $X_{\phi(0),\psi(0)} = X_{\phi(0),\psi(0)} = \cdots$. The functor $\widetilde{G}$ thus defined takes weak isomorphisms in $\underset{\longleftrightarrow}{\lim}\,\mathcal{A}$ with respect to $\mathrm{Pro}^a_{\mathbb{N}}\,\mathcal{A}$ to weak isomorphisms in $\mathrm{Ind}^a_{\mathbb{N}}\,\mathcal{A}$ with respect to $\mathcal{A}$, since if $X \in \mathrm{ob}\,\underset{\longleftrightarrow}{\lim}\,\mathcal{A}$ is in the image of $\mathrm{Pro}^a_{\mathbb{N}}\,\mathcal{A}$, then its 0th row is constant: $X_{0,1} = X_{0,1} = \cdots$, i.e., $\widetilde{G}(X)$ is in the image of $\mathcal{A}$. Hence $\widetilde{G}$ factors through a functor $G : \underset{\longleftrightarrow}{\lim}\,\mathcal{A}/\,\mathrm{Pro}^a_{\mathbb{N}}\,\mathcal{A} \to \mathrm{Ind}^a_{\mathbb{N}}\,\mathcal{A}/\mathcal{A}$.

We have $G\circ F = \mathrm{id}_{\mathrm{Ind}^a_{\mathbb{N}}\,\mathcal{A}/\mathcal{A}}$ by definition. On the other hand, if $X = (X_{i,j})_{i\le j} \in \mathrm{ob}\,\underset{\longleftrightarrow}{\lim}\,\mathcal{A}$, then $F\circ G(X)$ is the object $\widetilde{X}$ of $\underset{\longleftrightarrow}{\lim}\,\mathcal{A}$ determined by $\widetilde{X}_{i,j} = \widetilde{X}_{0,j} = X_{0,j}$, $i \le 0 < j$. Define an admissible epimorphism $f_X : X \twoheadrightarrow \widetilde{X}$ in $\mathrm{Fun}^a(\Pi,\mathcal{A})$ (hence in $\underset{\longleftrightarrow}{\lim}\,\mathcal{A}$) by

$$(f_X)_{i,j} = \begin{cases} X_{i,j} = X_{i,j} & \text{for } 0 \le i \le j, \\ X_{i,j} \twoheadrightarrow X_{0,j} & \text{for } i \le 0 < j, \\ X_{i,j} \twoheadrightarrow 0 & \text{for } i \le j \le 0. \end{cases}$$

The kernel coincides with the image of $0 \twoheadleftarrow X_{-1,0} \twoheadleftarrow X_{-2,0} \twoheadleftarrow X_{-3,0} \twoheadleftarrow \cdots \in \mathrm{ob}\,\mathrm{Pro}^a_{\mathbb{N}}\,\mathcal{A}$ in $\underset{\longleftrightarrow}{\lim}\,\mathcal{A}$. Hence f_X is a weak isomorphism in $\underset{\longleftrightarrow}{\lim}\,\mathcal{A}$ with respect to $\mathrm{Pro}^a_{\mathbb{N}}\,\mathcal{A}$. Thus we get an isomorphism $f : \mathrm{id}_{\underset{\longleftrightarrow}{\lim}\,\mathcal{A}/\,\mathrm{Pro}^a_{\mathbb{N}}\,\mathcal{A}} \xrightarrow{\sim} F\circ G$, to conclude that G is a quasi-inverse to F. □

This means that in the commutative diagram of nonconnective K-theory spectra

$$\begin{tikzcd}
\mathbb{K}(\mathcal{A}) \arrow[r] \arrow[d] & \mathbb{K}(\mathrm{Ind}^a_{\mathbb{N}}\,\mathcal{A}) \arrow[r] \arrow[d] & \mathbb{K}(\mathrm{Ind}^a_{\mathbb{N}}\,\mathcal{A}/\mathcal{A}) \arrow[d] \\
\mathbb{K}(\mathrm{Pro}^a_{\mathbb{N}}\,\mathcal{A}) \arrow[r] & \mathbb{K}(\underset{\longleftrightarrow}{\lim}\,\mathcal{A}) \arrow[r] & \mathbb{K}(\underset{\longleftrightarrow}{\lim}\,\mathcal{A}/\,\mathrm{Pro}^a_{\mathbb{N}}\,\mathcal{A})
\end{tikzcd}$$

the third vertical map is an equivalence. Since the two horizontal sequences are homotopy fibrations, it follows that the square

$$\begin{tikzcd}
\mathbb{K}(\mathcal{A}) \arrow[r] \arrow[d] & \mathbb{K}(\mathrm{Ind}^a_{\mathbb{N}}\mathcal{A}) \arrow[d] \\
\mathbb{K}(\mathrm{Pro}^a_{\mathbb{N}}\mathcal{A}) \arrow[r] & \mathbb{K}(\underset{\longleftrightarrow}{\lim}\,\mathcal{A})
\end{tikzcd}$$

is homotopy-cartesian, i.e., $\mathbb{K}(\mathcal{A}) \xrightarrow{\sim} \mathrm{holim}(\mathbb{K}(\mathrm{Pro}^a_{\mathbb{N}}\mathcal{A}) \to \mathbb{K}(\underset{\longleftrightarrow}{\lim}\,\mathcal{A}) \leftarrow \mathbb{K}(\mathrm{Ind}^a_{\mathbb{N}}\mathcal{A}))$ is an equivalence. We finally note:

Lemma 3.4. *There are canonical contractions for the nonconnective K-theory spectra $\mathbb{K}(\mathrm{Ind}^a_{\mathbb{N}}\mathcal{A})$ and $\mathbb{K}(\mathrm{Pro}^a_{\mathbb{N}}\mathcal{A})$.*

Proof. The contraction for $\mathbb{K}(\mathrm{Ind}^a_{\mathbb{N}}\mathcal{A})$ comes from the canonical flasque structure on $\mathrm{Ind}^a_{\mathbb{N}}\mathcal{A}$ (i.e., an endofunctor whose direct sum with the identity functor is naturally isomorphic to itself), given as follows. Let $X = (X_j)_{j\geq 1} \in \mathrm{ob}\,\mathrm{Ind}^a_{\mathbb{N}}\mathcal{A}$ be an $\mathbb{N}$-indexed admissible ind-object in $\mathcal{A}$, whose structure maps we denote by $\rho = \rho_{j,j'} : X_j \hookrightarrow X_{j'}$, $j \leq j'$. Write $T(X) \in \mathrm{ob}\,\mathrm{Ind}^a_{\mathbb{N}}\mathcal{A}$ for the admissible ind-object

$$0 \to X_1 \xrightarrow{(\rho,0)} X_2 \oplus X_1 \xrightarrow{(\rho\oplus\rho,0)} X_3 \oplus X_2 \oplus X_1 \xrightarrow{(\rho\oplus\rho\oplus\rho,0)} \cdots .$$

A morphism $f \in \mathrm{Hom}_{\mathrm{Ind}^a_{\mathbb{N}}\mathcal{A}}(Y, X) = \underset{\longleftarrow}{\lim}_j \underset{\longrightarrow}{\lim}_l \mathrm{Hom}_{\mathcal{A}}(Y_j, X_l)$ with j-th component represented by $f_j : Y_j \to X_{l(j)}$ defines a morphism $T(f) : T(Y) \to T(X)$ whose j-th component is the class of the composition

$$\begin{aligned} Y_{j-1} \oplus \cdots \oplus Y_1 &\xrightarrow{f_{j-1}\oplus\cdots\oplus f_1} X_{l(j-1)} \oplus \cdots \oplus X_{l(1)} \\ &\xrightarrow{\rho\oplus\cdots\oplus\rho} X_{k+j-1} \oplus \cdots \oplus X_{k+1} \hookrightarrow T(X)_{k+j}, \end{aligned}$$

where k is chosen to be sufficiently large. The endofunctor T thus defined is a flasque structure on $\mathrm{Ind}^a_{\mathbb{N}}\mathcal{A}$ since $(X \oplus T(X))_j \xrightarrow{=} T(X)_{j+1}$ give a natural isomorphism of ind-objects.

The contraction for $\mathbb{K}(\mathrm{Pro}^a_{\mathbb{N}}\mathcal{A})$ follows from the contraction for $\mathbb{K}(\mathrm{Ind}^a_{\mathbb{N}}(-))$ via the identification $\mathrm{Pro}^a_{\mathbb{N}}\mathcal{A} = (\mathrm{Ind}^a_{\mathbb{N}}\mathcal{A}^{\mathrm{op}})^{\mathrm{op}}$ and the general equivalence $\mathbb{K}(\mathcal{B}^{\mathrm{op}}) \xrightarrow{\sim} \mathbb{K}(\mathcal{B})$. □

We now obtain the desired homotopy equivalence $\mathbb{K}(\mathcal{A}) = \mathrm{holim}(\mathbb{K}(\mathrm{Pro}^a_{\mathbb{N}}\mathcal{A}) \to \mathbb{K}(\underset{\longleftrightarrow}{\lim}\,\mathcal{A}) \leftarrow \mathbb{K}(\mathrm{Ind}^a_{\mathbb{N}}\mathcal{A})) \xrightarrow{\sim} \mathrm{holim}(* \to \mathbb{K}(\underset{\longleftrightarrow}{\lim}\,\mathcal{A}) \leftarrow *) = \Omega\mathbb{K}(\underset{\longleftrightarrow}{\lim}\,\mathcal{A})$, and the proof of Theorem 1.2 is complete.

Acknowledgements

First of all, I am greatly indebted to Marco Schlichting for many valuable ideas employed in this article. In particular, the key idea of constructing the s-filtering localization sequence $\mathbb{K}(\mathrm{Pro}^a_{\mathbb{N}}\,\mathcal{A}) \to \mathbb{K}(\underleftrightarrow{\lim}\,\mathcal{A}) \to \mathbb{K}(\underleftrightarrow{\lim}\,\mathcal{A}/\mathrm{Pro}^a_{\mathbb{N}}\,\mathcal{A})$ and comparing it with the sequence $\mathbb{K}(\mathcal{A}) \to \mathbb{K}(\mathrm{Ind}^a_{\mathbb{N}}\,\mathcal{A}) \to \mathbb{K}(\mathrm{Ind}^a_{\mathbb{N}}\,\mathcal{A}/\mathcal{A})$ essentially belongs to him. I am truly grateful to Oliver Bräunling, Michael Groechenig and Jesse Wolfson for pointing out a crucial mistake in the previous version of the article. They moreover suggested how to fix the proof, letting me notice that any exact category admits a left s-filtering embedding into the category of admissible ind-objects and how the assumption of idempotent-completeness can be removed in constructing the s-filtering localization sequences. I am also deeply grateful to Lars Hesselholt for commenting on early drafts of this work and for pointing out a misunderstanding of Previdi's result, and to Satoshi Mochizuki for answering many questions and suggesting valuable ideas in several helpful discussions. Finally, I thank Luigi Previdi for posing the nice conjecture and for answering my questions on its meaning.

References

[Arkhipov and Kremnizer 2010] S. Arkhipov and K. Kremnizer, "2-gerbes and 2-Tate spaces", pp. 23–35 in *Arithmetic and geometry around quantization*, edited by Ö. Ceyhan et al., Progr. Math. **279**, Birkhäuser, Boston, 2010. MR 2011g:22036 Zbl 1248.53024

[Artin and Mazur 1969] M. Artin and B. Mazur, *Etale homotopy*, Lecture Notes in Mathematics **100**, Springer, Berlin-New York, 1969. MR 39 #6883 Zbl 0182.26001

[Beilinson 1987] A. A. Beilinson, "How to glue perverse sheaves", pp. 42–51 in *K-theory, arithmetic and geometry* (Moscow, 1984–1986), edited by Y. I. Manin, Lecture Notes in Math. **1289**, Springer, Berlin, 1987. MR 89b:14028 Zbl 0651.14009

[Drinfeld 2006] V. Drinfeld, "Infinite-dimensional vector bundles in algebraic geometry: an introduction", pp. 263–304 in *The unity of mathematics*, edited by P. Etingof et al., Progr. Math. **244**, Birkhäuser, Boston, 2006. MR 2007d:14038 Zbl 1108.14012

[Kapranov 2001] M. Kapranov, "Semiinfinite symmetric powers", preprint, 2001. arXiv 0107089

[Previdi 2010] L. C. Previdi, *Generalized Tate spaces*, Ph.D. thesis, Yale University, Ann Arbor, MI, 2010, Available at http://search.proquest.com/docview/656256743. MR 2941474

[Previdi 2011] L. Previdi, "Locally compact objects in exact categories", *Internat. J. Math.* **22**:12 (2011), 1787–1821. MR 2872533 Zbl 1255.18012

[Schlichting 2004] M. Schlichting, "Delooping the K-theory of exact categories", *Topology* **43**:5 (2004), 1089–1103. MR 2005k:18023 Zbl 1059.18007

[Schlichting 2006] M. Schlichting, "Negative K-theory of derived categories", *Math. Z.* **253**:1 (2006), 97–134. MR 2006i:19003 Zbl 1090.19002

[Waldhausen 1985] F. Waldhausen, "Algebraic K-theory of spaces", pp. 318–419 in *Algebraic and geometric topology* (New Brunswick, NJ, 1983), edited by A. Ranicki et al., Lecture Notes in Math. **1126**, Springer, Berlin, 1985. MR 86m:18011 Zbl 0579.18006

Communicated by Mikhail Kapranov
Received 2013-07-16 Accepted 2014-12-10

sho.saito@math.nagoya-u.ac.jp *Graduate School of Mathematics, Nagoya University,*
Furocho, Chikusaku, Nagoya 464-8602, Japan

ALGEBRA AND NUMBER THEORY 9:1 (2015)
dx.doi.org/10.2140/ant.2015.9.13

Surpassing the ratios conjecture in the 1-level density of Dirichlet L-functions

Daniel Fiorilli and Steven J. Miller

We study the 1-level density of low-lying zeros of Dirichlet L-functions in the family of all characters modulo q, with $Q/2 < q \le Q$. For test functions whose Fourier transform is supported in $(-\frac{3}{2}, \frac{3}{2})$, we calculate this quantity beyond the square root cancellation expansion arising from the L-function ratios conjecture of Conrey, Farmer and Zirnbauer. We discover the existence of a new lower-order term which is not predicted by this powerful conjecture. This is the first family where the 1-level density is determined well enough to see a term which is not predicted by the ratios conjecture, and proves that the exponent of the error term $Q^{-1/2+\epsilon}$ in the ratios conjecture is best possible. We also give more precise results when the support of the Fourier transform of the test function is restricted to the interval $[-1, 1]$. Finally we show how natural conjectures on the distribution of primes in arithmetic progressions allow one to extend the support. The most powerful conjecture is Montgomery's, which implies that the ratios conjecture's prediction holds for any finite support up to an error $Q^{-1/2+\epsilon}$.

1. Introduction

In this paper we study the 1-level density of Dirichlet L-functions with modulus q. The goal is to compute this statistic for large support and small error terms, providing

MSC2010: primary 11M26, 11M50, 11N13; secondary 11N56, 15B52.

Keywords: low-lying zeros, Dirichlet L-functions, ratios conjecture, primes in arithmetic progressions, random matrix theory.

a test of the predictions of the lower order and error terms in the L-function ratios conjecture. In this introduction we assume the reader is familiar with low-lying zeros of families of L-functions and the ratios conjecture, and briefly describe our results. For completeness we provide a brief review of the subject in Section 2A, and state our results in full in Section 2B to Section 2D.

We let $\eta \in L^1(\mathbb{R})$ be an even real function such that $\widehat{\eta}$ is C^2 and has compact support. Denoting by $\rho_\chi = \frac{1}{2} + i\gamma_\chi$ the nontrivial zeros of $L(s,\chi)$ (i.e., those satisfying $0 < \Re(\rho_\chi) < 1$) and choosing Q a scaling parameter close to q, the 1-level density is[1]

$$D_{1;q}(\eta) := \frac{1}{\phi(q)} \sum_{\chi \bmod q} \sum_{\gamma_\chi} \eta\left(\gamma_\chi \frac{\log Q}{2\pi}\right). \tag{1-1}$$

Throughout this paper, a sum over $\chi \bmod q$ *always means a sum over all characters, including the principal character.* If we assume GRH then the γ_χ are real. As $\eta(y) = \widehat{(\widehat{\eta})}(y)$ is defined for complex values of y, it makes sense to consider (1-1) for complex γ_χ, in case GRH is false (in other words, GRH is only needed to interpret the 1-level density as a spacing statistic arising from an ordered sequence of real numbers, allowing for a spectral interpretation). We also study the average of (1-1) over the moduli $Q/2 < q \le Q$, which is easier to understand in general:

$$D_{1;Q/2,Q}(\eta) := \frac{1}{Q/2} \sum_{Q/2<q\le Q} D_{1;q}(\eta). \tag{1-2}$$

The powerful ratios conjecture of Conrey, Farmer and Zirnbauer [Conrey et al. 2008; Conrey et al. 2005b] yields a formula for $D_{1;Q/2,Q}(\eta)$, which is believed to hold up to an error of $O_\epsilon(Q^{-1/2+\epsilon})$. While there have been several papers [Conrey and Snaith 2007; 2008; David et al. 2013; Goes et al. 2010; Huynh et al. 2011; Miller 2008; 2009b; Miller and Montague 2011] showing agreement between various statistics involving L-functions and the ratios conjecture's predictions, evidence for this precise exponent in the error term is limited; the reason this exponent was chosen is the "philosophy of square root cancellation". While some of the families studied have 1-level densities that agree beyond square root cancellation, it is always for small support ($\operatorname{supp}(\widehat{\eta}) \subset (-1,1)$). Further, in no family studied were nonzero lower order terms beyond square root cancellation isolated in the 1-level density.

The motivation of this paper was to resolve these issues. As the ratios conjecture is used in a variety of problems, it is important to test its predictions in the greatest possible window. Our key findings are the following.

[1] Since $\widehat{\eta}$ is C^2, we have $\eta(\xi) \ll \xi^{-2}$ for large ξ; hence the sum over the zeros is absolutely convergent. While most of the literature uses ϕ as the test function, since we will use Euler's totient function extensively we use η.

- We uncover new, nonzero lower-order terms in the 1-level density for our families of Dirichlet characters. These terms are beyond what the ratios conjecture can predict, and suggest the possibility that a refinement may be possible and needed.
- We show (unconditionally) that the natural limit of accuracy of the L-function ratios conjecture is $\Omega(Q^{-1/2+o(1)})$. Thus the error term cannot be improved for a general family of L-functions, though of course its veracity for all families is still open.

The existence of lower-order terms beyond the ratios conjecture's prediction in statistics of L-functions is not without precedent. Indeed such terms have been isolated in the second moment of $|L(\frac{1}{2},\chi)|$ by Heath-Brown [1981], and for a more general shifted sum by Conrey [2007].

Before stating our main result, we give the ratios conjecture's prediction. This prediction is done for a slightly different family in [Goes et al. 2010], but it is trivial to convert from their formulation to the one below (we discuss the conversion in Section 2B).

Conjecture 1.1 (ratios conjecture). *The 1-level density* $D_{1;q}(\eta)$ (*from* (1-1) *with scaling parameter* $Q=q$) *equals*

$$\widehat{\eta}(0)\biggl(1-\frac{\log(8\pi e^{\gamma})}{\log q}-\frac{1}{\log q}\sum_{p\mid q}\frac{\log p}{p-1}\biggr)+\int_0^\infty\frac{\widehat{\eta}(0)-\widehat{\eta}(t)}{q^{t/2}-q^{-t/2}}\,dt+O_\epsilon\bigl(q^{-1/2+\epsilon}\bigr). \tag{1-3}$$

The 1-level density $D_{1;Q/2,Q}(\eta)$ (*from rescaling*[2] (1-3)) *equals*

$$\widehat{\eta}(0)\biggl(1-\frac{\log(4\pi e^{\gamma})+1}{\log Q}-\frac{1}{\log Q}\sum_{p}\frac{\log p}{p(p-1)}\biggr)+\int_0^\infty\frac{\widehat{\eta}(0)-\widehat{\eta}(t)}{Q^{t/2}-Q^{-t/2}}\,dt+O_\epsilon\bigl(Q^{-1/2+\epsilon}\bigr). \tag{1-4}$$

Surprisingly, our techniques are capable of not only verifying this prediction, but we are able to determine the 1-level density beyond what even the ratios conjecture predicts. In Theorem 1.2 we obtain a new (arithmetical) term of order $Q^{-1/2}/\log Q$, which is not predicted by the ratios conjecture.

[2] To rescale we multiply (1-3) by $\log q/\log Q$, replace $q^{t/2}-q^{-t/2}$ with $Q^{t/2}-Q^{-t/2}$ and average over $Q/2<q\le Q$. The term $\log q$ averages to $\log Q+\log 2-1+O(\log Q/Q)$, explaining the "additional" term $(\log 2-1)/\log Q$. Moreover the average of $\sum_{p\mid q}\frac{\log p}{p-1}$ over this range is easily shown to be $\sum_p\frac{1}{p(p-1)}+O(\log Q/Q)$.

Theorem 1.2. *Assume GRH. If the Fourier transform of the test function η is supported in $(-\frac{3}{2}, \frac{3}{2})$, then $D_{1;q/2,Q}(\eta)$ equals*

$$\widehat{\eta}(0)\left(1-\frac{\log(4\pi e^{\gamma})+1}{\log Q}-\frac{1}{\log Q}\sum_{p}\frac{\log p}{p(p-1)}\right) \\ +\int_0^{\infty}\frac{\widehat{\eta}(0)-\widehat{\eta}(t)}{Q^{t/2}-Q^{-t/2}}\,dt+\frac{Q^{-1/2}}{\log Q}S_{\eta}(Q), \quad (1\text{-}5)$$

where

$$S_{\eta}(Q) \;=\; C_1\widehat{\eta}(1)+C_2\frac{\widehat{\eta}'(1)}{\log Q}+O\left(\left(\frac{\log\log Q}{\log Q}\right)^2\right), \quad (1\text{-}6)$$

with

$$C_1 := (2-\sqrt{2})\,\zeta\left(\tfrac{1}{2}\right)\prod_{p}\left(1+\frac{1}{(p-1)p^{1/2}}\right),$$

$$C_2 := C_1\left(\frac{\sqrt{2}+4}{3}-\left(\frac{\zeta'}{\zeta}\left(\tfrac{1}{2}\right)-\sum_{p}\frac{\log p}{(p-1)p^{1/2}+1}\right)\right). \quad (1\text{-}7)$$

We can give a more precise formula for the term $S_{\eta}(Q)$: see Remark 2.5. While Theorem 1.2 is conditional on GRH, in Theorem 2.1 we prove a more precise and unconditional result for test functions η whose Fourier transform has support contained in $[-1,1]$.

The first two terms in (1-5) agree with the ratios conjecture's prediction. As for the term $Q^{-1/2}S_{\eta}(Q)/\log Q$, its presence confirms that the error term $Q^{-1/2+o(1)}$ in the ratios conjecture is best possible, and suggests more generally that the 1-level density of a family ought to contain a (possibly oscillating) arithmetical term of order $Q^{-1/2+o(1)}$, a statement which should be tested in other families. Interestingly this new term contains the factors $\widehat{\eta}(1)$ and $\widehat{\eta}'(1)$, and is zero when $\widehat{\eta}$ is supported in $(-1,1)$. In this case we give a more precise estimate for the 1-level density in Theorem 2.1, in which a lower-order term of order $Q^{\sigma/2-1+o(1)}$ appears, where $\sigma=\sup(\operatorname{supp}\widehat{\eta})$. This term is a genuine lower-order term, and shows that for such test functions the ratios conjecture's prediction is not best possible. We thus show that a transition happens when σ is near 1. Indeed looking at the difference between the 1-level density and the ratios conjecture's prediction, that is defining

$$E_Q(\eta):=D_{1;Q/2,Q}(\eta)-\widehat{\eta}(0)\left(1-\frac{\log(4\pi e^{\gamma})+1}{\log Q}-\frac{1}{\log Q}\sum_{p}\frac{\log p}{p(p-1)}\right) \\ -\int_0^{\infty}\frac{\widehat{\eta}(0)-\widehat{\eta}(t)}{Q^{t/2}-Q^{-t/2}}\,dt, \quad (1\text{-}8)$$

our results imply that[3] $E_Q(\eta) = Q^{-\mu(\sigma)+o(1)}$, where

$$\mu(\sigma) = \begin{cases} \frac{\sigma}{2} - 1 & \text{if } \sigma \le 1, \\ -\frac{1}{2} & \text{if } 1 \le \sigma < \frac{3}{2}. \end{cases} \tag{1-9}$$

We conjecture that $\mu(\sigma)$ should equal $-\frac{1}{2}$ for all $\sigma \ge 1$, and that our new lower-order term $Q^{-1/2} S_\eta(Q)/\log Q$ should persist in this extended range.

Conjecture 1.3. *Theorem 1.2 holds for test functions η whose Fourier transform has arbitrarily large finite support σ.*

In Figure 1, the solid curve represents our results (Theorems 1.2 and 2.1), and the dashed line represents Conjecture 1.3; note the resemblance between this graph and the one appearing in Montgomery's pair correlation conjecture [Montgomery 1973]. We prove in Theorem 2.13 that Montgomery's conjecture on primes in arithmetic progressions implies that $\mu(\sigma) \le -\frac{1}{2}$ for all $\sigma \ge 1$.

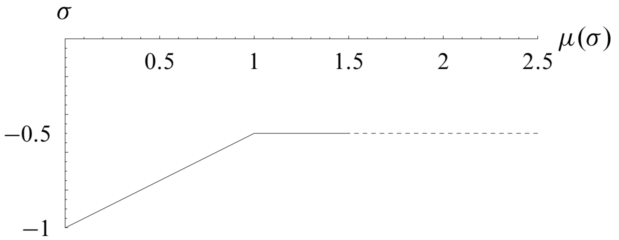

Figure 1. The graph of $\mu(\sigma)$.

We believe that this phenomenon is universal and should also happen in different families, in the sense that we believe that the ratios conjecture's prediction should be best possible for $\sigma \ge 1$, and should not be for $\sigma < 1$. For example, in [Miller 2009b] it is shown that if the Fourier transform of the involved test function is supported in $(-1, 1)$, then the ratios conjecture's prediction is not best possible and one can improve the remainder term; however, in this region of limited support there are no new, nonzero lower order terms unpredicted by the ratios conjecture. These results confirm the exceptional nature of the transition point $\sigma = 1$, as is the case in Montgomery's pair correlation conjecture [1973]. Indeed if this last conjecture were known to hold beyond the point $\alpha = 1$, then this would imply the nonexistence of Landau–Siegel zeros [Conrey and Iwaniec 2002].

Our plan of attack is to use the explicit formula to turn the 1-level density into an average of the various terms appearing in this formula. The bulk of the work is devoted to carefully estimating the contribution of the prime sum, which when summing over χ mod q becomes a sum over primes in the residue class 1 mod q,

[3] For $\sigma > 1$, this holds for test functions η for which either $\hat{\eta}(1) \ne 0$ or $\hat{\eta}'(1) \ne 0$ (see Theorem 1.2); see Theorem 2.1 if $\sigma \le 1$. If $\hat{\eta}(u)$ vanishes in a small interval around $u = 1$, then Theorem 2.6 gives the correct answer.

averaged over $q \sim Q$. Accordingly, the proof of Theorem 1.2 is based on ideas in [Fiorilli 2012], which improve on results of Fouvry [1985], Bombieri, Friedlander and Iwaniec [Bombieri et al. 1986], Friedlander and Granville [1992] and Friedlander, Granville, Hildebrandt and Maier [Friedlander et al. 1991]. Theorem 1.1 of [Fiorilli 2012] cannot be applied directly here, since this estimate is only valid when looking at primes up to x modulo q with $q \sim Q$, where Q is not too close to x. Additional estimates are needed, including a careful analysis of the range $x^{1-\epsilon} < Q \le x$, which required a combination of divisor switching techniques and precise estimates on the mean value of smoothed sums of the reciprocal of Euler's totient function. Additionally, in our analysis of the 1-level density after using the explicit formula and executing the sum over the family we obtain a sum over primes in the arithmetic progressions $1 \bmod q$; this is one of the cases where one obtains an asymptotic in [Fiorilli 2012, Theorem 1.1], which explains the occurrence of the lower-order term $Q^{-1/2} S_\eta(Q)/\log Q$ in Theorem 1.2.

The paper is organized as follows. In Section 2A we review previous results on low-lying zeros in families of L-functions and describe the motivation for the ratios conjecture. See for example [Goes et al. 2010; Miller 2009b] for a detailed description of how to apply the ratios conjecture to predict the 1-level density. We describe our unconditional results in Section 2B, and then improve our results in Section 2C by assuming GRH. In previous families there often is a natural barrier, and extending the support is related to standard conjectures (for example, in [Iwaniec et al. 2000] the authors show how cancellation in exponential sums involving square roots of primes leads to larger support for families of cuspidal newforms). A similar phenomenon surfaces here, where in Section 2D we show that increasing the support beyond $(-2, 2)$ is related to conjectures on the distribution of primes in residue classes. We analyze the increase in support provided by various conjectures. These range from a conjecture on the variance of primes in the residue classes, which allow us to reach $(-4, 4)$, to Montgomery's conjecture for a fixed residue, which gives us any finite support. The next sections contain the details of the proof; we state the explicit formula and prove some needed sums in Section 3, and then prove our theorems in the remaining sections.

2. Background and new results

2A. ***Background and previous results.*** Assuming GRH, the nontrivial zeros of any nice L-function lie on the critical line, and therefore it is possible to investigate statistics of its normalized zeros. These zeros are fundamental in many problems, ranging from the distribution of primes in congruence classes to the class number [Conrey and Iwaniec 2002; Goldfeld 1976; Gross and Zagier 1986; Rubinstein and Sarnak 1994]. Numerical and theoretical evidence [Hejhal 1994; Montgomery

1973; Odlyzko 1987; 2001; Rudnick and Sarnak 1996] support a universality in behavior of zeros of an individual automorphic L-function high above the central point, specifically that they are well-modeled by ensembles of random matrices (see [Firk and Miller 2009; Hayes 2003] for histories of the emergence of random matrix theory in number theory). The story is different for the low-lying zeros, the zeros near the central point. A convenient way to study these zeros is via the 1-level density, which we now describe. Let $\eta \in L^1(\mathbb{R})$ be an even real function whose Fourier transform

$$\hat{\eta}(y) = \int_{-\infty}^{\infty} \eta(x) e^{-2\pi i x y}\, dx \tag{2-1}$$

is C^2 and has compact support. Let $\mathscr{F}_N$ be a (finite) family of L-functions satisfying GRH.[4] The 1-level density associated to $\mathscr{F}_N$ is defined by

$$D_{1;\mathscr{F}_N}(\eta) = \frac{1}{|\mathscr{F}_N|} \sum_{g \in \mathscr{F}_N} \sum_j \eta\left(\frac{\log c_g}{2\pi} \gamma_g^{(j)}\right), \tag{2-2}$$

where $\frac{1}{2} + i\gamma_g^{(j)}$ runs through the nontrivial zeros of $L(s, g)$. Here c_g is the "analytic conductor" of g, and gives the natural scale for the low zeros. As η decays, only low-lying zeros (i.e., zeros within a distance $1/\log c_g$ of the central point $s = \frac{1}{2}$) contribute significantly. Thus the 1-level density can help identify the symmetry type of the family. To evaluate (2-2), one applies the explicit formula, converting sums over zeros to sums over primes.

Based in part on the function field analysis where $G(\mathscr{F})$ is the monodromy group associated to the family $\mathscr{F}$, Katz and Sarnak conjectured that for each reasonable irreducible family of L-functions there is an associated symmetry group $G(\mathscr{F})$ (one of the following five: unitary U, symplectic USp, orthogonal O, SO(even), SO(odd)), and that the distribution of critical zeros near $\frac{1}{2}$ mirrors the distribution of eigenvalues near 1. The five groups have distinguishable 1-level densities. To date, for suitably restricted test functions the statistics of zeros of many natural families of L-functions have been shown to agree with statistics of eigenvalues of matrices from the classical compact groups, including Dirichlet L-functions, elliptic curves, cuspidal newforms, Maass forms, number field L-functions, and symmetric powers of GL_2 automorphic representations [Alpoge and Miller 2014; Alpoge et al. 2014; Dueñez and Miller 2006; Fouvry and Iwaniec 2003; Gao 2005; Güloğlu 2005; Hughes and Miller 2007; Hughes and Rudnick 2003; Iwaniec et al. 2000; Katz and Sarnak 1999a; 1999b; Miller 2004; Miller and Peckner 2012; Ricotta and Royer 2011; Royer 2001; Rubinstein 2001; Shin and Templier 2012; Yang 2009; Young

[4] We often do not need GRH for the analysis, but only to interpret the results. If the GRH is true, the zeros lie on the critical line and can be ordered, which suggests the possibility of a spectral interpretation.

2006], to name a few, as well as nonsimple families formed by Rankin–Selberg convolution [Dueñez and Miller 2009].

In addition to predicting the main term (see for example [Conrey 2001; Katz and Sarnak 1999a; 1999b; Keating and Snaith 2000a; 2000b; 2003]), techniques from random matrix theory have led to models that capture the lower order terms in their full arithmetic glory for many families of L-functions (see for example the moment conjectures in [Conrey et al. 2005a] or the hybrid model in [Gonek et al. 2007]). Since the main terms agree with either unitary, symplectic or orthogonal symmetry, it is only in the lower order terms that we can break this universality and see the arithmetic of the family enter. These are therefore natural and important objects to study, and can be isolated in many families [Huynh et al. 2009; Miller 2009a; Young 2005]. We thus require a theory that is capable of making detailed predictions. Recently the L-function ratios conjecture [Conrey et al. 2008; 2005b] has had great success in determining lower order terms. Though a proof of the ratios conjecture for arbitrary support is well beyond the reach of current methods, it is an indispensable tool in current investigations as it allows us to easily write down the predicted answer to a remarkable level of precision, which we try to prove in as great a generality as possible.

To study the 1-level density, it suffices to obtain good estimates for

$$R_{\mathcal{F}_N}(\alpha,\gamma) := \frac{1}{|\mathcal{F}_N|}\sum_{g\in\mathcal{F}_N}\frac{L(\frac{1}{2}+\alpha,g)}{L(\frac{1}{2}+\gamma,g)}. \tag{2-3}$$

(In the current paper, the parameter Q plays the role of $|\mathcal{F}_N|$.) Asymptotic formulas for $R_{\mathcal{F}_N}(\alpha,\gamma)$ have been conjectured for a variety of families $\mathcal{F}_N$ (see [Conrey et al. 2008; Conrey and Snaith 2007; 2008; Goes et al. 2010; Huynh et al. 2011; Miller 2008; 2009b; Miller and Montague 2011]) and are believed to hold up to errors of size $|\mathcal{F}_N|^{-1/2+\epsilon}$ for any $\epsilon > 0$. The evidence for the correctness of this error term is limited to test functions with small support (frequently significantly less than $(-1,1)$), though in such regimes many of the above papers verify this prediction. Many of the steps in the ratios conjecture's recipe lead to the addition or omission of terms as large as those being considered, and thus there was uncertainty as to whether or not the resulting predictions should be accurate to square root cancellation. The results of the current paper can be seen as a confirmation that this is the right error term for the final predicted answer, at least in this family. Further, the novelty in our results resides in the fact that we are able to go beyond square root cancellation and we find a smaller term which is unpredicted by the ratios conjecture (see Theorem 1.2). For a precise explanation on how to derive the ratios conjecture's prediction in our family, we refer the reader to [Goes et al. 2010], and also recommend [Conrey and Snaith 2007] for an accessible overview of the ratios conjecture.

2B. ***Unconditional results.*** We now describe our unconditional results. We remind the reader that η is a real even function such that $\widehat{\eta}$ is C^2 and has compact support.

Theorem 2.1. *Suppose that the Fourier transform of the test function η is supported on the interval* $[-1,1]$, *so* $\sigma = \sup(\operatorname{supp}\widehat{\eta}) \le 1$. *There exists an absolute positive constant c* (*coming from the Prime Number Theorem*) *such that the 1-level density* $D_{1;q}(\eta)$ (*from* (1-1) *with scaling parameter* $Q = q$) *equals*

$$\widehat{\eta}(0)\biggl(1 - i\frac{\log(8\pi e^{\gamma})}{\log q} - \frac{1}{\log q}\sum_{p\mid q}\frac{\log p}{p-1}\biggr) + \int_0^\infty \frac{\widehat{\eta}(0)-\widehat{\eta}(t)}{q^{t/2}-q^{-t/2}}\,dt - \frac{2}{\phi(q)}\int_0^1 q^{u/2}\biggl(\frac{\widehat{\eta}(u)}{2} - \frac{\widehat{\eta}'(u)}{\log q}\biggr)du - \frac{2}{\log q}\sum_{\substack{p^{\nu}\| q\\ p^e\equiv 1 \bmod q/p^{\nu}\\ e,\nu\ge 1}}\frac{\log p}{\phi(p^{\nu})p^{e/2}}\widehat{\eta}\biggl(\frac{\log p^e}{\log q}\biggr) + O\biggl(\frac{q^{\sigma/2-1}}{e^{c\sqrt{\sigma\log q}}}\biggr). \tag{2-4}$$

Remark 2.2. The average over $Q/2 < q \le Q$ of the fourth term in (2-4) can be shown to be $O(Q^{-1})$, and is therefore negligible when considering $D_{1;Q/2,Q}(\eta)$ (see (3-16)). However, the term involving the second integral in (2-4) is of size $q^{\sigma/2-1-o(1)}$, and thus constitutes a genuine lower-order term, smaller than the error term in (1-3) predicted using the ratios conjecture.

Theorems 1.2 and 2.1 should be compared to the main result of Goes, Jackson, Miller, Montague, Ninsuwan, Peckner and Pham [Goes et al. 2010], where they show one can extend the support of $\widehat{\eta}$ to $[-2,2]$ and still get the main term, as well as the lower order terms down to a power savings. They only consider q prime, and thus the sum over primes p dividing q below in Theorem 2.3 is absorbed by their error term. We briefly discuss how one can easily extend their results to the case of general q. First note that $L(s,\chi)$ and $L(s,\chi^*)$ have the same zeros in the critical strip if χ^* is the primitive character of conductor q^* inducing the nonprincipal character χ of conductor q. We now have $\log q^*$, which can be converted to a sum over primes p dividing q by the same arguments as in the proof of Proposition 3.1. The rest of the expansion follows from expanding the digamma function Γ'/Γ in the integral in [Goes et al. 2010, Theorem 1.3] and then standard algebra (along the lines of the computations in Section 3). We use [Montgomery and Vaughan 2007, Lemma 12.14], which in our notation says that for $a, b > 0$ we have

$$\int_{-\infty}^{\infty}\frac{\Gamma'(a\pm ib\tau)}{\Gamma(a\pm ib\tau)}\eta(t)\,dt = \frac{\Gamma'(a)}{\Gamma(a)}\widehat{\eta}(0) + \frac{2\pi}{b}\int_0^\infty \frac{\exp(-2\pi a x/b)}{1-\exp(-2\pi x/b)}\bigl(\widehat{\eta}(0)-\widehat{\eta}(\mp x)\bigr)\,dx, \tag{2-5}$$

and the identity

$$\frac{\Gamma'(\frac{1}{4})}{\Gamma(\frac{1}{4})}+\frac{\Gamma'(\frac{3}{4})}{\Gamma(\frac{3}{4})} = -2\gamma-6\log 2, \tag{2-6}$$

with γ the Euler–Mascheroni constant. We then extend to $q\in(Q/2,Q]$ by rescaling the zeros by $\log Q$ and not $\log q$ and summing over the family; recall the technical issues involved in the rescaling are discussed in Footnote 2.

Theorem 2.3 (Goes, Jackson, Miller, Montague, Ninsuwan, Peckner, Pham [Goes et al. 2010]). *If $1<\sigma\le 2$, then the 1-level density $D_{1;q}(\eta)$ (from* (1-1) *with scaling parameter $Q=q$) equals*

$$\hat{\eta}(0)\left(1-\frac{\log(8\pi e^{\gamma})}{\log q}-\frac{1}{\log q}\sum_{p\mid q}\frac{\log p}{p-1}\right)+\int_0^{\infty}\frac{\hat{\eta}(0)-\hat{\eta}(t)}{q^{t/2}-q^{-t/2}}\,dt \\ +O\left(\frac{\log\log q}{\log q}q^{\sigma/2-1}\right), \tag{2-7}$$

and this agrees with the ratios conjecture.

Remark 2.4. Goes et al. [2010] actually proved (2-7) for any $\sigma\le 2$, with the additional error term $O(q^{-1/2+\epsilon})$. We preferred not to include the case $\sigma\le 1$, as Theorem 2.1 is more precise in this range.

2C. *Results under GRH.*

We first mention a more precise version of Theorem 1.2.

Remark 2.5. If in addition to the hypotheses of Theorem 1.2 we assume that the Fourier transform of the test function η is $K+1$ times continuously differentiable, then we can give a more precise expression for the term $S_\eta(Q)$ appearing in (1-5):

$$S_\eta(Q) = \sum_{i=0}^{K}\frac{a_i(\eta)}{(\log Q)^i}+O_{\epsilon,K}\left(\frac{1}{(\log Q)^{K+1-\epsilon}}\right), \tag{2-8}$$

where the $a_i(\eta)$ are constants depending (linearly) on the Taylor coefficients of $\hat{\eta}(t)$ at $t=1$. In fact, $S_\eta(Q)$ is a truncated linear functional, which composed with the Fourier transform operator is supported on $\{1\}$ (in the sense of distributions).

Our next result is an extension of Theorem 1.2, in the case where $\hat{\eta}(u)$ vanishes in a small interval to the right of $u=1$.

Theorem 2.6. *Assume GRH.*

(1) *If $\hat{\eta}$ is supported in $(-\frac{3}{2},-1-\kappa]\cup[-1,1]\cup[1+\kappa,\frac{3}{2})$ for some $\kappa>0$, then for any $\epsilon>0$ the average 1-level density $D_{1;Q/2,Q}(\eta)$ equals*

$$\widehat{\eta}(0)\left(1-\frac{1+\log(4\pi e^{\gamma})}{\log Q}-\frac{1}{\log Q}\sum_{p}\frac{\log p}{p(p-1)}\right)$$
$$+\int_0^{\infty}\frac{\widehat{\eta}(0)-\widehat{\eta}(t)}{Q^{t/2}-Q^{-t/2}}\,dt$$
$$-\frac{4\log 2}{Q}\frac{\zeta(2)\zeta(3)}{\zeta(6)}\int_0^1 Q^{u/2}\left(\frac{\widehat{\eta}(u)}{2}-\frac{\widehat{\eta}'(u)}{\log Q}\right)du$$
$$-\int_{1+\kappa}^{4/3}((u-1)\log Q+C_6)Q^{-u/2}\left(\frac{\widehat{\eta}(u)}{2}-\frac{\widehat{\eta}'(u)}{\log Q}\right)du$$
$$+\ O_{\epsilon}\big(Q^{-1/2-\kappa+\epsilon}+Q^{-2/3}\log Q+Q^{\sigma-2}\log Q\big), \tag{2-9}$$

with $C_6 := \log(\pi/2)+1+\gamma+\sum_p \frac{\log p}{p(p-1)}$.

(*For* $\sigma \geq \frac{4}{3}$, *unless* $\widehat{\eta}(x)$ *has some mass near* $x=\lambda$ *for some* $1<\lambda<4-2\sigma$, *the fourth term in* (2-9) *goes in the error term, and hence* (2-9) *reduces to* (2-10). *However, if* $1<\sigma<\frac{4}{3}$, *it is always a genuine lower-order term.*)

(2) *If* f *is supported in* $(-2,-a]\cup[-1,1]\cup[a,2)$ *for some* $1\leq a<2$ (*if* $a=1$, *we have the full interval* $(-2,2)$), *then* $D_{1;Q/2,Q}(\eta)$ *equals*

$$\widehat{\eta}(0)\left(1-\frac{1+\log(4\pi e^{\gamma})}{\log Q}-\frac{1}{\log Q}\sum_{p}\frac{\log p}{p(p-1)}\right)$$
$$+\int_0^{\infty}\frac{\widehat{\eta}(0)-\widehat{\eta}(t)}{Q^{t/2}-Q^{-t/2}}\,dt$$
$$-\frac{4\log 2}{Q}\frac{\zeta(2)\zeta(3)}{\zeta(6)}\int_0^1 Q^{u/2}\left(\frac{\widehat{\eta}(u)}{2}-\frac{\widehat{\eta}'(u)}{\log Q}\right)du$$
$$+O\big(Q^{-a/2}+Q^{\sigma-2}\log Q\big). \tag{2-10}$$

Unless $a>1$ *and* $\sigma<\frac{3}{2}$, *the third term of* (2-10) *goes in the error term.*

2D. ***Results beyond GRH.*** As the GRH is insufficient to compute the 1-level density for test functions supported beyond $[-2,2]$, we explore the consequences of other standard conjectures in number theory involving the distribution of primes among residue classes. Before stating these conjectures, we first set the notation. Let

$$\psi(x) := \sum_{n\leq x}\Lambda(n), \qquad \psi(x,q,a) := \sum_{\substack{n\leq x\\ n\equiv a \bmod q}}\Lambda(n),$$
$$E(x,q,a) := \psi(x,q,a)-\frac{\psi(x)}{\phi(q)}. \tag{2-11}$$

If we assume GRH, we have

$$\psi(x) = x + O\big(x^{1/2}(\log x)^2\big), \quad E(x,q,a) = O\big(x^{1/2}(\log x)^2\big). \tag{2-12}$$

Our first result uses GRH and the following de-averaging hypothesis, which depends on a parameter $\delta \in [0,1]$.

Hypothesis 2.7. We have

$$\sum_{\frac{Q}{2}<q\le Q} \left|\psi(x;q,1) - \frac{\psi(x)}{\phi(q)}\right|^2 \ll Q^{\delta-1} \sum_{\frac{Q}{2}<q\le Q} \sum_{\substack{1\le a\le q\\(a,q)=1}} \left|\psi(x;q,a) - \frac{\psi(x)}{\phi(q)}\right|^2. \tag{2-13}$$

This hypothesis is trivially true for $\delta = 1$, and while it is unlikely to be true for $\delta = 0$, it is reasonable to expect it to hold for any $\delta > 0$. What we need is some control over biases of primes congruent to 1 mod q; Hypothesis 2.7 can be interpreted as bounding the average of $|\psi(x;q,1) - \psi(x)/\phi(q)|^2$ in terms of the average variance.[5]

Under these hypotheses, we show how to extend the support to a wider but still limited range.

Theorem 2.8. *Assume GRH and Hypothesis 2.7 for some $\delta \in (0,1)$. The average 1-level density $D_{1;Q/2,Q}(\widehat{\eta})$ equals*

$$\widehat{\eta}(0)\left(1 - \frac{1+\log(4\pi e^{\gamma})}{\log Q} - \frac{1}{\log Q}\sum_p \frac{\log p}{p(p-1)}\right) + \int_0^\infty \frac{\widehat{\eta}(0) - \widehat{\eta}(t)}{Q^{t/2} - Q^{-t/2}}\,dt$$
$$+ O\big(Q^{(\delta-1)/2}(\log Q)^{3/2} + Q^{(\sigma+2\delta)/4-1}(\log Q)^{1/3}\big), \tag{2-14}$$

which is asymptotic to $\widehat{\eta}(0)$ provided the support of $\widehat{\eta}$ is contained in $(-4+2\delta, 4-2\delta)$.

The proof of Theorem 2.8 is given in Section 6. It uses a result of Goldston and Vaughan [1997], which is an improvement of results of Barban, Davenport, Halberstam, Hooley, Montgomery and others.

Remark 2.9. In Theorem 2.8 we study the weighted 1-level density

$$D_{1;Q/2,Q}(\eta) := \sum_{Q/2<q\le Q} \frac{1}{\phi(q)} \sum_{\chi \bmod q} \sum_{\gamma_\chi} \eta\left(\gamma_\chi \frac{\log Q}{2\pi}\right), \tag{2-15}$$

which is technically easier to study than the unweighted version

$$D^{\text{unweighted}}_{1;Q/2,Q}(\eta) := \frac{1}{9/\pi^2 (Q/2)^2} \sum_{Q/2<q\le Q} \sum_{\chi \bmod q} \sum_{\gamma_\chi} \eta\left(\gamma_\chi \frac{\log Q}{2\pi}\right). \tag{2-16}$$

[5] Note that we only need this de-averaging hypothesis for the special residue class $a = 1$.

This is similar to many other families of L-functions, such as cuspidal newforms [Iwaniec et al. 2000; Miller and Montague 2011] and Maass forms [Alpoge et al. 2014; Alpoge and Miller 2014], where the introduction of weights (arising from the Petersson and Kuznetsov trace formulas) facilitates evaluating the arithmetical terms.

Finally, we show how we can determine the 1-level density for arbitrary finite support, under a hypothesis of Montgomery [1970].

Hypothesis 2.10 (Montgomery). For any a, q such that $(a,q)=1$ and $q \le x$, we have

$$\psi(x;q,a) - \frac{\psi(x)}{\phi(q)} \ll_\epsilon x^\epsilon \Big(\frac{x}{q}\Big)^{1/2}. \tag{2-17}$$

It is by gaining some savings in q in the error $E(x,q,a)$ that we can increase the support for families of Dirichlet L-functions. The following weaker version of Montgomery's conjecture, which depends on a parameter $\theta \in (0, \frac{1}{2}]$, also suffices to increase the support beyond $[-2, 2]$.

Hypothesis 2.11. For any a, q such that $(a,q)=1$ and $q \le x$, we have

$$\psi(x;q,1) - \frac{\psi(x)}{\phi(q)} \ll_\epsilon \frac{x^{1/2+\epsilon}}{q^\theta}. \tag{2-18}$$

Hypothesis 2.12. Fix $\epsilon > 0$. We have for $x^\epsilon \le q \le \sqrt{x}$ that

$$\sum_{\substack{n\le x\\ n\equiv 1 \bmod q}} \Lambda(n)\Big(1-\frac{n}{x}\Big) - \frac{1}{\phi(q)} \sum_{n\le x} \Lambda(n)\Big(1-\frac{n}{x}\Big) = o\big(x^{1/2}\big). \tag{2-19}$$

Note that this is a weighted version of $\psi(x;q,1) - \psi(x)/\phi(q)$; that is, we added the weight $\big(1-n/x\big)$. The reason for this is that it makes the count smoother, and this makes it easier to analyze in general since the Mellin transform of $g(y) := 1-y$ in the interval $[0, 1]$ is decaying faster in vertical strips than that of $g(y) \equiv 1$.

Amongst the last three hypotheses, Hypothesis 2.12 is the weakest, but it is still sufficient to derive the asymptotic in the 1-level density for test functions with arbitrary large support.

Theorem 2.13. *Suppose that the Fourier transform of η has arbitrarily large* (*but compact*) *support.*

(1) *If we assume Hypothesis 2.12, the 1-level density $D_{1;q}(\eta)$ equals $\hat{\eta}(0) + o(1)$, agreeing with the scaling limit of unitary matrices.*

(2) *If we assume Hypothesis 2.11 for some* $0 < \theta \le \frac{1}{2}$, *then* $D_{1;q}(\eta)$ *equals*

$$\widehat{\eta}(0)\left(1 - \frac{\log(8\pi e^{\gamma})}{\log q} - \frac{1}{\log q}\sum_{p\mid q}\frac{\log p}{p-1}\right) + \int_0^{\infty}\frac{\widehat{\eta}(0)-\widehat{\eta}(t)}{q^{t/2}-q^{-t/2}}\,dt + O_{\epsilon}\big(q^{-\theta+\epsilon}\big). \quad (2\text{-}20)$$

Remark 2.14. Under GRH, the left-hand side of (2-19) is $O(x^{1/2}\log q)$. Therefore, if we win by more than a logarithm over GRH, then we have the expected asymptotic for the 1-level density for $\widehat{\eta}$ of arbitrarily large finite support.

Interestingly, if we assume Montgomery's conjecture (Hypothesis 2.10), then we can take $\theta = \frac{1}{2}$ in (2-20), and doing so we end up precisely with the ratios conjecture's prediction; see (1-3).

We derive the explicit formula for the families of Dirichlet characters in Section 3, as well as some useful estimates for some of the resulting sums. We give the unconditional results in Section 4, Theorems 2.1 and 2.3. The proofs of Theorems 1.2 and 2.6 are conditional on GRH, and use results in [Friedlander and Granville 1992] and [Fiorilli 2012]; we give them in Section 5. We conclude with an analysis of the consequences of the hypotheses on the distribution of primes in residue classes, using the de-averaging hypothesis to prove Theorem 2.8 in Section 6 and Montgomery's hypothesis to prove Theorem 2.13 in Section 7.

3. The explicit formula and needed sums

Our starting point for investigating the behavior of low-lying zeros is the explicit formula, which relates sums over zeros to sums over primes. We follow the derivation in [Montgomery and Vaughan 2007] (see also [Iwaniec et al. 2000; Rudnick and Sarnak 1996] and [Davenport 1980; Iwaniec and Kowalski 2004] for all needed results about Dirichlet L-functions). We first derive the expansion for Dirichlet characters with fixed conductor q, and then extend to $q \in (Q/2, Q]$. We conclude with some technical estimates that will be of use in proving Theorem 1.2. Here and throughout, we will set $f := \widehat{\eta}$. Note that η is real and even, and thus so is the case for f, and moreover we have $\widehat{f} = \eta$.

3A. *The explicit formula for fixed q.*

Proposition 3.1 (explicit formula for the family of Dirichlet characters modulo q). *Let f be an even, twice differentiable test function with compact support. Denote the nontrivial zeros of $L(s,\chi)$ by*

$$\rho_{\chi} = \tfrac{1}{2} + i\gamma_{\chi}.$$

Then the 1-level density $D_{1,q}(\widehat{f})$ equals

$$\begin{aligned}\frac{1}{\phi(q)}&\sum_{\chi \bmod q}\sum_{\gamma_\chi}\widehat{f}\Big(\gamma_\chi\frac{\log Q}{2\pi}\Big)\\ &= \frac{f(0)}{\log Q}\Big(\log q-\log(8\pi e^{\gamma})-\sum_{p|q}\frac{\log p}{p-1}\Big)+\int_0^\infty\frac{f(0)-f(t)}{Q^{t/2}-Q^{-t/2}}\,dt\\ &\quad -\frac{2}{\log Q}\sum_{\substack{p^\nu\|q\\ p^e\equiv 1 \bmod q/p^\nu\\ e,\nu\ge 1}}\frac{\log p}{\phi(p^\nu)p^{e/2}}f\Big(\frac{\log p^e}{\log Q}\Big)\\ &\quad -\frac{2}{\log Q}\Big(\sum_{n\equiv 1 \bmod q}-\frac{1}{\phi(q)}\sum_n\Big)\frac{\Lambda(n)}{n^{1/2}}f\Big(\frac{\log n}{\log Q}\Big)+O\Big(\frac{1}{\phi(q)}\Big).\end{aligned}\tag{3-1}$$

Proof. We start with Weil's explicit formula for $L(s,\chi)$, with $\chi \bmod q$ a nonprincipal character (we add the contribution from the principal character later). We can replace $L(s,\chi)$ by $L(s,\chi^*)$ (where χ^* is the primitive character of conductor q^* inducing χ), since these have the same nontrivial zeros. Taking

$$F(x) := \frac{2\pi}{\log Q}f\Big(\frac{2\pi x}{\log Q}\Big)$$

in Theorem 12.13 of [Montgomery and Vaughan 2007] (whose conditions are satisfied by our restrictions on f), we find

$$\Phi(s) = \widehat{f}\Big(\frac{\log Q}{2\pi}\frac{(s-\frac{1}{2})}{i}\Big),$$

and

$$\begin{aligned}\sum_{\rho_\chi}\widehat{f}\Big(\frac{\log Q}{2\pi}\gamma_\chi\Big) &= \frac{f(0)}{\log Q}\Big(\log\frac{q^*}{\pi}+\frac{\Gamma'}{\Gamma}\Big(\frac{1}{4}+\frac{a(\chi)}{2}\Big)\Big)\\ &\quad -\frac{2}{\log Q}\sum_{n=1}^{\infty}\frac{\Lambda(n)\Re(\chi^*(n))}{n^{1/2}}f\Big(\frac{\log n}{\log Q}\Big)\\ &\quad +\frac{4\pi}{\log Q}\int_0^\infty\frac{e^{-(1+2a(\chi))\pi x}}{1-e^{-4\pi x}}\Big(f(0)-f\Big(\frac{2\pi x}{\log Q}\Big)\Big)dx,\end{aligned}\tag{3-2}$$

where $a(\chi)=0$ for the half of the characters with $\chi(-1)=1$ and 1 for the half with $\chi(-1)=-1$. Making the substitution $t=2\pi x/\log Q$ in the integral and summing over $\chi\ne\chi_0$, we find

$$\begin{aligned}\sum_{\chi\neq\chi_0}\sum_{\gamma_\chi}\widehat{f}\Big(\gamma_\chi\frac{\log Q}{2\pi}\Big)&\\ &= \frac{f(0)}{\log Q}\bigg(\sum_{\chi\neq\chi_0}\log(q^*/\pi)+\frac{\phi(q)}{2}\frac{\Gamma'}{\Gamma}\Big(\frac{3}{4}\Big)+\frac{\phi(q)}{2}\frac{\Gamma'}{\Gamma}\Big(\frac{1}{4}\Big)\bigg)\\ &\quad+\phi(q)\int_0^\infty\frac{Q^{-3t/2}+Q^{-t/2}}{1-Q^{-2t}}\big(f(0)-f(t)\big)\,dt\\ &\quad-\frac{2}{\log Q}\bigg(\phi(q)\sum_{n\equiv 1 \bmod q}-\sum_n\bigg)\frac{\Lambda(n)}{n^{1/2}}f\Big(\frac{\log n}{\log Q}\Big)\\ &\quad-\frac{2}{\log Q}\sum_{\chi\neq\chi_0}\sum_n\frac{\Lambda(n)\Re\big(\chi^*(n)-\chi(n)\big)}{n^{1/2}}f\Big(\frac{\log n}{\log Q}\Big)\\ &\quad+O(1). \qquad (3\text{-}3)\end{aligned}$$

To get (3-3) from (3-2) we added zero by writing $\chi^*(n)$ as $\big(\chi^*(n)-\chi(n)\big)+\chi(n)$. Summing $\chi(n)$ over all $\chi \bmod q$ gives $\phi(q)$ if $n\equiv 1 \bmod q$ and 0 otherwise; as our sum omits the principal character, the sum of $\chi(n)$ over the nonprincipal characters yields the sum on the third line above. We also replaced $(\phi(q)-1)/2$ by $\phi(q)/2$ in the first term, hence the $O(1)$.

We use [Fiorilli and Martin 2013, Proposition 3.3] for the first term (which involves the sum over the conductor of the inducing character). We then use the duplication formula of the digamma function $\psi(z)=\Gamma'(z)/\Gamma(z)$ to simplify the next two terms, namely $\psi(\frac{1}{4})+\psi(\frac{3}{4})$. As $\psi(\frac{1}{2})=-\gamma-2\ln 2$ (Equation 6.3.3 of [Abramowitz and Stegun 1972]) and $\psi(2z)=\frac{1}{2}\psi(z)+\frac{1}{2}\psi(z+\frac{1}{2})+\ln 2$ (Equation 6.3.8, [ibid.]), setting $z=\frac{1}{4}$ yields $\psi(\frac{1}{4})+\psi(\frac{3}{4})=-2\gamma-6\ln 2$. We keep the next two terms as they are, and then apply [Fiorilli and Martin 2013, Proposition 3.4] (with $r=1$) for the last term, obtaining that it equals

$$-\frac{2}{\log Q}\sum_n\frac{\Lambda(n)}{n^{1/2}}f\Big(\frac{\log n}{\log Q}\Big)\Re\bigg(\sum_{\chi\neq\chi_0}\big(\chi^*(n)-\chi(n)\big)\bigg). \qquad (3\text{-}4)$$

Writing $n=p^e$, this term is zero unless $p\mid q$. If $p\mid q$, then it is zero unless $p^e\equiv 1 \bmod q/p^\nu$, where $\nu\geq 1$ is the largest ν such that $p^\nu\mid q$. Therefore this term equals

$$-\frac{2}{\log Q}\sum_p\sum_{\substack{p^\nu\| q\\ p^e\equiv 1 \bmod q/p^\nu\\ e,\nu\geq 1}}\frac{\Lambda(p^e)}{\phi(p^\nu)p^{e/2}}f\Big(\frac{\log p^e}{\log Q}\Big). \qquad (3\text{-}5)$$

Combining this with some elementary algebra yields

$$\begin{aligned}\frac{1}{\phi(q)}&\sum_{\chi\neq\chi_0}\sum_{\gamma_\chi}\widehat{f}\Big(\gamma_\chi\frac{\log Q}{2\pi}\Big)\\ &=\frac{f(0)}{\log Q}\Big(\log q-\log(8\pi e^{\gamma})-\sum_{p\mid q}\frac{\log p}{p-1}\Big)+\int_0^\infty\frac{f(0)-f(t)}{Q^{t/2}-Q^{-t/2}}\,dt\\ &\quad-\frac{2}{\log Q}\Big(\sum_{n\equiv 1 \bmod q}-\frac{1}{\phi(q)}\sum_{n}\Big)\frac{\Lambda(n)}{n^{1/2}}f\Big(\frac{\log n}{\log Q}\Big)\\ &\quad-\frac{2}{\log Q}\sum_{\substack{p^\nu\| q\\ p^e\equiv 1 \bmod q/p^\nu\\ e,\nu\geq 1}}\frac{\log p}{\phi(p^\nu)p^{e/2}}f\Big(\frac{\log p^e}{\log Q}\Big)+O\Big(\frac{1}{\phi(q)}\Big).\end{aligned}\tag{3-6}$$

Finally, since the nontrivial zeros of $L(s,\chi_0)$ coincide with those of $\zeta(s)$, the difference between the left-hand side of (3-1) and that of (3-6) is

$$\frac{1}{\phi(q)}\sum_{\gamma_\zeta}\widehat{f}\Big(\gamma_\zeta\frac{\log Q}{2\pi}\Big)\ll\frac{1}{\phi(q)}\tag{3-7}$$

(since f is twice continuously differentiable, $\widehat{f}(y)\ll 1/y^2$), completing the proof.[6] □

3B. ***The averaged explicit formula for $q\in(Q/2,Q]$.*** We now average the explicit formula for $D_{1;q}(\widehat{f})$ (Proposition 3.1) over $q\in(Q/2,Q]$. We concentrate on deriving useful expansions, which we then analyze in later sections when we determine the allowable support.

Proposition 3.2 (explicit formula for the averaged family of Dirichlet characters modulo q). *The averaged 1-level density,* $D_{1;Q/2,Q}(\widehat{f})$, *equals*

$$\begin{aligned}\frac{1}{Q/2}&\sum_{Q/2<q\leq Q}D_{1;q}(\widehat{f})\\ &=\frac{f(0)}{\log Q}\Big(\log Q-1-\gamma-\log(4\pi)-\sum_{p}\frac{\log p}{p(p-1)}\Big)+\int_0^\infty\frac{f(0)-f(t)}{Q^{t/2}-Q^{-t/2}}\,dt\\ &\quad+\frac{2}{Q/2}\sum_{Q/2<q\leq Q}\int_0^\infty\Big(\frac{f(u)}{2}-\frac{f'(u)}{\log Q}\Big)\frac{\psi(Q^u;q,1)-\psi(Q^u)/\phi(q)}{Q^{u/2}}\,du\\ &\quad+O\Big(\frac{1}{Q}\Big).\end{aligned}\tag{3-8}$$

[6] While the explicit formula for $\zeta(s)$ has a term arising from its pole at $s=1$, that term does not matter here as it is insignificant upon division by the family's size.

Setting

$$\psi_2(x;q,a) := \sum_{\substack{n\le x\\ n\equiv a \bmod q}} \Lambda(n)\Big(1-\frac{n}{x}\Big), \quad \psi_2(x) := \sum_{n\le x} \Lambda(n)\Big(1-\frac{n}{x}\Big), \tag{3-9}$$

the last integral in (3-8) *may be replaced with*

$$-2\int_0^\infty \Big(\frac{3f(u)}{4}-\frac{2f'(u)}{\log Q}+\frac{f''(u)}{(\log Q)^2}\Big)\frac{\psi_2(Q^u;q,1)-\psi_2(Q^u)/\phi(q)}{Q^{u/2}}\,du. \tag{3-10}$$

Proof. The main term in the expansion of $D_{1;q}(\widehat{f})$ from Proposition 3.1 is

$$T_1(q) := \frac{f(0)}{\log Q}\Big(\log q - \log(8\pi e^\gamma) - \sum_{p\mid q}\frac{\log p}{p-1}\Big). \tag{3-11}$$

Using the antiderivative of $\log x$ is $x\log x - x$, one easily finds its average over $Q/2 < q \le Q$ is

$$\frac{1}{Q/2}\sum_{Q<q\le 2Q} T_1(q) \\ = \frac{f(0)}{\log Q}\Big(\log Q - 1 - \gamma - \log(4\pi) - \sum_p \frac{\log p}{p(p-1)}\Big) + O\Big(\frac{1}{Q}\Big). \tag{3-12}$$

We now turn to the lower-order term

$$T_2(q) := -\frac{2}{\log Q}\sum_{\substack{p^\nu \| q\\ p^e\equiv 1 \bmod q/p^\nu\\ e,\nu\ge 1}} \frac{\log p}{\phi(p^\nu)p^{e/2}} f\Big(\frac{\log p^e}{\log Q}\Big). \tag{3-13}$$

Before determining its average behavior, we note that its size can vary greatly with q. It is very small for prime q (so $\nu = 1$ and $p = q$ in the sum), since

$$T_2(q) \ll \frac{1}{\log Q}\sum_{e\ge 1}\frac{\log q}{\phi(q)q^{e/2}} \ll \frac{1}{(q-1)(q^{1/2}-1)}; \tag{3-14}$$

however, it can be as large as $C/(\sqrt{q}\log Q)$ for other values of q (such as $q = 2(2^e-1)$). This is, more or less, as large as it can get, since for general q we have

$$T_2(q) \ll \frac{1}{\log Q}\sum_{\substack{p^\nu\| q\\ e,\nu\ge 1\\ p^e\le Q^\sigma}} \frac{\log p}{\phi(p^\nu)(q/p^\nu)^{1/2}} \ll \frac{(\log q)^{1/2}}{q^{1/2}\log\log q}. \tag{3-15}$$

On average, however, $T_2(q)$ is very small:

$$\begin{aligned}\frac{1}{Q/2}\sum_{Q/2<q\le Q} T_2(q) &\ll \frac{1}{Q}\sum_{Q/2<q\le Q}\ \sum_{\substack{p^\nu \| q\\ p^e\equiv 1 \bmod q/p^\nu\\ e,\nu\ge 1}} \frac{\log p}{p^{\nu+e/2}}\\ &\ll \frac{1}{Q}\sum_{\substack{p^\nu\\ \nu,e\ge 1}} \frac{\log p}{p^{\nu+e/2}} \sum_{\substack{q\le Q\\ p^\nu | q\\ \frac{q}{p^\nu}|p^e-1}} 1 \ll \frac{1}{Q}\sum_{\substack{p^\nu\\ \nu,e\ge 1}} \frac{\log p}{p^{\nu+e/2}}\tau(p^e-1)\\ &\ll_\epsilon \frac{1}{Q}\sum_{\substack{p^\nu\\ \nu,e\ge 1}} \frac{\log p}{p^{\nu+(1-\epsilon)e/2}} \ll \frac{1}{Q}\sum_p \frac{\log p}{p^{3/2-\epsilon/2}} \ll \frac{1}{Q}. \end{aligned} \tag{3-16}$$

While we will not rewrite the next lower order term, it is instructive to determine its size. Set

$$T_3(q) := \int_0^\infty \frac{f(0)-f(t)}{Q^{t/2}-Q^{-t/2}}\,dt. \tag{3-17}$$

Letting $t = 2\pi x/\log Q$, we find

$$T_3(q) = \frac{2\pi}{\log Q}\int_0^\infty \frac{f(0)-f(2\pi x/\log Q)}{2\sinh(\pi x)}\,dx. \tag{3-18}$$

Since f is twice differentiable with compact support, $|f(0)-f(x)| \ll |x|$, thus

$$T_3(q) \ll \frac{2\pi}{\log Q}\int_0^\infty \frac{x}{2\sinh(\pi x)}\,dx = \frac{\pi}{4\log Q}. \tag{3-19}$$

As

$$\int_0^\infty \frac{x^k\,dx}{\sinh(\pi x)} = \frac{2^{k+1}-1}{2^k\pi^{k+1}}\Gamma(k+1)\zeta(k+1), \tag{3-20}$$

if f has a Taylor series of order $K+1$ we have

$$T_3(q) = \sum_{k=1}^{K} \frac{(2^{k+1}-1)\zeta(k+1)f^{(k)}(0)}{\log^{k+1} Q} + O\left(\frac{1}{\log^{K+1} Q}\right). \tag{3-21}$$

If the Taylor coefficients of f decay very fast, we can even make our bounds uniform and get an error term smaller than a negative power of Q.

The remaining term from Proposition 3.1 is the most important, and controls the allowable support. The arithmetic lives here, as this term involves primes in arithmetic progressions. It is

$$\begin{aligned} T_4(q) &:= -\frac{2}{\log Q}\biggl(\sum_{n\equiv 1 \bmod q} - \frac{1}{\phi(q)}\sum_n\biggr)\frac{\Lambda(n)}{n^{1/2}} f\biggl(\frac{\log n}{\log Q}\biggr) \\ &= -\frac{2}{\log Q}\int_1^\infty t^{-1/2} f\biggl(\frac{\log t}{\log Q}\biggr)\, d\biggl(\psi(t;q,1) - \frac{\psi(t)}{\phi(q)}\biggr) \\ &= \frac{2}{\log Q}\int_1^\infty \frac{\frac12 f\bigl(\frac{\log t}{\log Q}\bigr) - \frac{1}{\log Q} f'\bigl(\frac{\log t}{\log Q}\bigr)}{t^{3/2}}\biggl(\psi(t;q,1) - \frac{\psi(t)}{\phi(q)}\biggr)\, dt. \end{aligned} \tag{3-22}$$

The claim in the proposition follows by changing variables by setting $t = Q^u$; specifically, the final integral is

$$T_4(q) = 2\int_0^\infty \biggl(\frac{f(u)}{2} - \frac{f'(u)}{\log Q}\biggr)\frac{\psi(Q^u;q,1) - \psi(Q^u)/\phi(q)}{Q^{u/2}}\, du. \tag{3-23}$$

We give an alternative expansion for the final integral. This expansion involves a smoothed sum of $\Lambda(n)$, which will be technically easier to analyze when we turn to determining the allowable support under Montgomery's hypothesis (Theorem 2.13(1)). Recall

$$\psi_2(x;q,a) := \sum_{\substack{n\le x\\ n\equiv a \bmod q}} \Lambda(n)\Bigl(1 - \frac{n}{x}\Bigr), \quad \psi_2(x) := \sum_{n\le x} \Lambda(n)\Bigl(1-\frac{n}{x}\Bigr), \tag{3-24}$$

We integrate by parts in (3-22). Since

$$\begin{aligned} &\int_1^x \biggl(\psi(t;q,1) - \frac{\psi(t)}{\phi(q)}\biggr)\, dt \\ &\qquad = \int_1^x \biggl(\sum_{\substack{n\le t\\ n\equiv 1 \bmod q}} \Lambda(n) - \frac{1}{\phi(q)}\sum_{n\le t}\Lambda(n)\biggr)\, dt \\ &\qquad = \sum_{\substack{n\le x\\ n\equiv 1 \bmod q}} \Lambda(n)\int_n^x dt - \frac{1}{\phi(q)}\sum_{n\le x}\Lambda(n)\int_n^x dt \\ &\qquad = x\biggl(\sum_{\substack{n\le x\\ n\equiv 1 \bmod q}} \Lambda(n)\Bigl(1-\frac{n}{x}\Bigr) - \frac{1}{\phi(q)}\sum_{n\le x}\Lambda(n)\Bigl(1-\frac{n}{x}\Bigr)\biggr), \end{aligned} \tag{3-25}$$

we find

$$T_4(q) = -2\int_0^\infty \biggl(\frac{3f(u)}{4} - \frac{2f'(u)}{\log Q} + \frac{f''(u)}{(\log Q)^2}\biggr)\frac{\psi_2(Q^u;q,1) - \psi_2(Q^u)/\phi(q)}{Q^{u/2}}\, du, \tag{3-26}$$

completing the proof. □

Remark 3.3. It will be convenient later that in the averaged case ψ and ψ_2 are both evaluated at $(Q^u; q, 1)$ and not $(q^u; q, 1)$; this is because we are rescaling all L-function zeros by the same quantity (a global rescaling instead of a local rescaling).

3C. ***Technical estimates.*** In the proof of Theorem 2.6, we need the following estimation of a weighted sum of the reciprocal of the totient function.

Lemma 3.4. *Let ϕ be Euler's totient function. We have*

$$\sum_{r \le R} \frac{1}{\phi(r)} \biggl(R^{1/2} + \frac{r}{R^{1/2}} - 2r^{1/2} \biggr) = D_1 R^{1/2} \log R + D_2 R^{1/2} + D_3 + O\biggl(\frac{\log R}{R^{1/2}} \biggr), \tag{3-27}$$

where

$$D_1 := \frac{\zeta(2)\zeta(3)}{\zeta(6)}, \quad D_2 := D_1 \biggl(\gamma - 3 - \sum_p \frac{\log p}{p^2 - p + 1} \biggr),$$
$$D_3 := -2\zeta(i\tfrac{1}{2}i)i \prod_p \biggl(i1 + \frac{1}{(p-1)p^{1/2}} \biggr). \tag{3-28}$$

More generally, if $P(u) := \sum_{i=0}^{d} a_i u^i$ is a polynomial of degree d and of norm

$$\|P\| := \max_i |a_i|, \tag{3-29}$$

then

$$\sum_{r \le R} \frac{1}{\phi(r)} \int_{\frac{\log r}{\log R}}^{1} P(u) \biggl(R^{u/2} - \frac{r}{R^{u/2}} \biggr) \, du = E_1 \log R \int_{-\infty}^{1} R^{u/2} u P(u) \, du + E_2 \int_{-\infty}^{1} R^{u/2} P(u) \, du + \sum_{j=1}^{d+1} \frac{F_j(P)}{(\log R)^j} + O_d\bigl(R^{-1/2} \|P\| \bigr), \tag{3-30}$$

where

$$E_1 := \frac{\zeta(2)\zeta(3)}{\zeta(6)}, \quad E_2 := E_1 \biggl(\gamma - 1 - \sum_p \frac{\log p}{p^2 - p + 1} \biggr), \tag{3-31}$$

and the $F_j(P)$ are constants depending on P which can be computed explicitly.

For example,

$$F_1(P) = -4\zeta\left(\tfrac{1}{2}\right)\prod_p\left(1+\frac{1}{(p-1)p^{1/2}}\right)\sum_{i=0}^{d}(-1)^i P^{(i)}(1)$$

$$F_2(P) = -4\zeta\left(\tfrac{1}{2}\right)\prod_p\left(1+\frac{1}{(p-1)p^{1/2}}\right) \times\left(\frac{\zeta'}{\zeta}\left(\tfrac{1}{2}\right)-\sum_p\frac{\log p}{(p-1)p^{1/2}+1}\right)\sum_{i=1}^{d}(-1)^i P^{(i)}(1). \tag{3-32}$$

Finally,

$$\begin{aligned}\sum_{r\le R}\frac{1}{\phi(r)}\int_{\frac{\log(r/2)}{\log(R/2)}}^{1} P(u)\left((R/2)^{u/2}-\frac{r}{2(R/2)^{u/2}}\right)du &= E_1\log(R/2)\int_{-\infty}^{1}(R/2)^{u/2}uP(u)\,du \\ &\quad + (E_2+E_1\log 2)\int_{-\infty}^{1}(R/2)^{u/2}P(u)\,du \\ &\quad + \sum_{j=1}^{d+1}\frac{F_j^{(2)}(P)}{(\log(R/2))^j}+O_d\left(R^{-1/2}\|P\|\right),\end{aligned} \tag{3-33}$$

where the first two constants are given by

$$F_1^{(2)}(P) := \frac{F_1(P)}{\sqrt{2}}$$

$$F_2^{(2)}(P) := -2\sqrt{2}\zeta\left(\tfrac{1}{2}\right)\prod_p\left(1+\frac{1}{(p-1)p^{1/2}}\right) \times\left(\frac{\zeta'}{\zeta}\left(\tfrac{1}{2}\right)-\sum_p\frac{\log p}{(p-1)p^{1/2}+1}+\log 2\right)\sum_{i=1}^{d}(-1)^i P^{(i)}(1). \tag{3-34}$$

Remark 3.5. It is possible to improve the estimates in (3-27), (3-30) and (3-33) to ones with an error term of $O_{\epsilon,d}(R^{-5/4+\epsilon}\|P\|)$; however, this is not needed for our purposes.

Proof. By Mellin inversion, for $c\ge 2$ the left-hand side of (3-27) equals

$$\begin{aligned}\frac{1}{2\pi i}\int_{\Re(s)=c} Z(s)\left(\frac{R^{s+1/2}}{s}+\frac{R^{s+1/2}}{s+1}-2\frac{R^{s+1/2}}{s+\frac{1}{2}}\right)ds \\ = \frac{1}{2\pi i}\int_{\Re(s)=c} Z(s)\frac{R^{s+1/2}}{2s(s+\frac{1}{2})(s+1)}\,ds,\end{aligned} \tag{3-35}$$

where

$$Z(s) := \sum_{n\geq 1} \frac{1}{n^s\phi(n)}. \tag{3-36}$$

Taking Euler products,

$$Z(s) = \zeta(s+1)\zeta(s+2)Z_2(s), \tag{3-37}$$

where

$$Z_2(s) := \prod_p \left(1 + \frac{1}{p(p-1)}\left(\frac{1}{p^{s+1}} - \frac{1}{p^{2s+2}}\right)\right), \tag{3-38}$$

which converges for $\Re(s) > -\frac{3}{2}$. We shift the contour of integration to the left to the line $\Re(s) = -3/2+\epsilon$. By a standard residue calculation, we get that (3-35) equals

$$D_1 R^{1/2}\log R + D_2 R^{1/2} + D_3 + D_4 \frac{\log R}{R^{1/2}} + \frac{D_5}{R^{1/2}} \\ + \frac{1}{2\pi i}\int_{\Re(s)=-\frac{3}{2}+\epsilon} Z(s) \frac{R^{s+1/2}}{2s(s+1/2)(s+1)}\, ds \tag{3-39}$$

for some constants D_4 and D_5. The proof now follows from standard bounds on the zeta function, which show that this integral is $\ll_\epsilon R^{-1+\epsilon}$. See the proof of [Fiorilli 2012, Lemma 6.9] for more details.

We now move to (3-30). The Mellin transform in this case is (for $\Re(s) > 0$)

$$\begin{aligned}\alpha(s) &:= \int_0^R r^{s-1} \int_{\frac{\log r}{\log R}}^1 P(u)\left(R^{u/2} - \frac{r}{R^{u/2}}\right) du\, dr \\ &= \int_{-\infty}^1 P(u) \int_0^{R^u} r^{s-1}\left(R^{u/2} - \frac{r}{R^{u/2}}\right) dr\, du \\ &= \int_{-\infty}^1 P(u)\frac{R^{u(s+1/2)}}{s(s+1)}\, du,\end{aligned} \tag{3-40}$$

which is now defined for $\Re(s) > -\frac{1}{2}$. To meromorphically extend $\alpha(s)$ to the whole complex plane, we integrate by parts n times:

$$\alpha(s) = \frac{R^{s+1/2}}{s(s+1)} \sum_{i=0}^{n} \frac{(-1)^i P^{(i)}(1)}{(s+1/2)^{i+1}(\log R)^{i+1}}, \tag{3-41}$$

which is a meromorphic function with poles at the points $s = 0, -\frac{1}{2}, -1$. The integral we need to compute is

$$\frac{1}{2\pi i}\int_{\Re(s)=1} Z(s)\alpha(s)\, ds. \tag{3-42}$$

We remark that

$$\alpha(-\tfrac{3}{2}+\epsilon+it) \ll_{\epsilon,d} \frac{R^{-1+\epsilon}}{t^3}\|P\|, \tag{3-43}$$

hence the proof is similar as in the previous case, since by shifting the contour of integration to the left, we have

$$\frac{1}{2\pi i}\int_{\Re(s)=1} Z(s)\alpha(s)\,ds \;=\; A + O_{\epsilon,d}\big(R^{-1+\epsilon}\|P\|\big), \tag{3-44}$$

where A is the sum of the residues of $Z(s)\alpha(s)$ for $-\frac{3}{2}+\epsilon \le \Re(s) \le 2$. Note that if $\beta(s) := s(s+1)\alpha(s)$, then

$$\beta(0) \;=\; \int_{-\infty}^{1} R^{u/2}P(u)\,du, \qquad \beta'(0) \;=\; \log R\int_{-\infty}^{1} R^{u/2}uP(u)\,du, \tag{3-45}$$

so the residue at $s=0$ equals

$$\frac{\zeta(2)\zeta(3)}{\zeta(6)}\beta(0)\bigg(\frac{\beta'}{\beta}(0)+\gamma-1-\sum_p\frac{\log p}{p^2-p+1}\bigg). \tag{3-46}$$

For the pole at $s=-\frac{1}{2}$, we need to use the analytic continuation of $\alpha(s)$ provided in (3-41), which shows that this residue equals

$$\sum_{j=1}^{n+1}\frac{F_j(P)}{(\log R)^j}, \tag{3-47}$$

where the $F_j(P)$ are constants depending on P which can be computed explicitly. For example,

$$\begin{aligned} F_1(P) \;&=\; -4\zeta(\tfrac{1}{2})\prod_p\bigg(1+\frac{1}{(p-1)p^{1/2}}\bigg)\sum_{i=0}^{d}(-1)^iP^{(i)}(1)\\ F_2(P) \;&=\; -4\zeta(\tfrac{1}{2})\prod_p\bigg(1+\frac{1}{(p-1)p^{1/2}}\bigg)\\ &\qquad\times\bigg(\frac{\zeta'}{\zeta}(\tfrac{1}{2})-\sum_p\frac{\log p}{(p-1)p^{1/2}+1}\bigg)\sum_{i=1}^{d}(-1)^iP^{(i)}(1). \end{aligned} \tag{3-48}$$

Moreover, $F_i(P) \ll_d \|P\|$ for all i.

At $s=-1$, we have a double pole with residue

$$R^{-1/2}\sum_{j=0}^{n+1}\frac{G_j(P)}{(\log R)^j}, \tag{3-49}$$

for some constants $G_j(P) \ll_d \|P\|$, hence the proof of (3-30) is complete.

For the proof of (3-33), we proceed in the same way, noting that the Mellin transform is

$$\alpha_2(s) = \frac{2^s}{s(s+1)} \int_{-\infty}^{1} P(u)(R/2)^{u(s+1/2)}\, du, \tag{3-50}$$

which completes the proof of Lemma 3.4. □

4. Unconditional results (Theorems 2.1 and 2.3)

Using the expansion for the 1-level density $D_{1,q}(\widehat{f})$ and the averaged 1-level density $D_{1;Q/2,Q}(\widehat{f})$ from Propositions 3.1 and 3.2, we prove our unconditional results.

Proof of Theorem 2.1. We start from Proposition 3.1. The only term of (3-1) we need to understand is the last one (the "prime sum"), which is given by

$$T_4(q) := 2\int_0^1 \biggl(\frac{f(u)}{2} - \frac{f'(u)}{\log q}\biggr) \frac{\psi(q^u; q, 1) - \psi(q^u)/\phi(q)}{q^{u/2}}\, du. \tag{4-1}$$

(We used that the support of f is contained in $[-1, 1]$ and we made the substitution $t = q^u$.) However, since there are no integers congruent to 1 mod q in the interval $[2, q^u]$ when $u \le 1$ (this is also true when q^u is replaced by Q^u, with $Q/2 < q \le Q$), the $\psi(q^u; q, 1)$ term equals zero. By the Prime Number Theorem there is an absolute, computable constant $c > 0$ such that

$$\begin{aligned} T_4(q) &= -2\int_0^1 \biggl(\frac{f(u)}{2} - \frac{f'(u)}{\log q}\biggr) \frac{\psi(q^u)}{q^{u/2}\phi(q)}\, du \\ &= -\frac{2}{\phi(q)} \int_0^1 q^{u/2} \biggl(\frac{f(u)}{2} - \frac{f'(u)}{\log q}\biggr) du \\ &\qquad\qquad + O\biggl(\frac{1}{\phi(q)} \int_0^\sigma \frac{q^{u/2}}{e^{c\sqrt{u \log q}}}\, du\biggr), \end{aligned} \tag{4-2}$$

and the error term is

$$\ll \frac{q^{\sigma/4}}{\phi(q)} \int_0^{\sigma/2} e^{-c\sqrt{u\log q}}\, du + \frac{e^{-c\sqrt{(\sigma/2)\log q}}}{\phi(q)} \int_{\sigma/2}^{\sigma} q^{u/2}\, du \ll \frac{q^{\sigma/2-1}}{e^{c'\sqrt{\sigma \log q}}} \tag{4-3}$$

for q large enough (in terms of σ), completing the proof. □

Proof of Theorem 2.3. Starting again from (3-1), we have from (3-15)

$$-\frac{2}{\log Q} \sum_{\substack{p^\nu \| q \\ p^e \equiv 1 \bmod q/p^\nu \\ e,\nu \ge 1}} \frac{\log p}{\phi(p^\nu) p^{e/2}} f\biggl(\frac{\log p^e}{\log Q}\biggr) \ll \frac{(\log q)^{1/2}}{q^{1/2} \log\log q}; \tag{4-4}$$

hence this goes in the error term and the only term we need to worry about is the last one.

As our support exceeds $[-1, 1]$, the $\psi(q^u; q, 1)$ no longer trivially vanishes, and the last term is

$$T_4(q) = 2\int_0^2 \left(\frac{f(u)}{2} - \frac{f'(u)}{\log q}\right) \frac{\psi(q^u; q, 1) - \psi(q^u)/\phi(q)}{q^{u/2}}\, du. \tag{4-5}$$

In the proof of Theorem 2.1 above we showed that the contribution from the integral where $0 \le u \le 1$ is $O(q^{-1/2})$.

For any fixed $\epsilon > 0$, trivial bounds for the region $1 \le u \le 1+\epsilon$ yield a contribution that is

$$\ll \int_1^{1+\epsilon} (u \log q) q^{u/2-1}\, du \ll q^{-1/2+\epsilon}. \tag{4-6}$$

We use the Brun–Titchmarsh Theorem (see [Montgomery and Vaughan 1973]) for the region where $1 + \epsilon \le u \le 2$, which asserts that for $q < x$,

$$\pi(x; q, a) \le \frac{2x}{\phi(q)\log(x/q)}. \tag{4-7}$$

We first bound the contribution from prime powers as follows. First there are at most $2e^{\omega(q)}$ residue classes $b \bmod q$ such that $b^e \equiv 1 \bmod q$, and so using that $\omega(q) \ll \log q/\log\log q$ we compute

$$\begin{aligned}\sum_{e\ge 2} \sum_{\substack{p\le x^{1/e}\\ p^e\equiv 1 \bmod q}} \log p &\ll \sum_{2\le e\le \frac{2}{\epsilon}} e^{\omega(q)} \max_{b \bmod q}\Bigg(\sum_{\substack{p\le x^{1/e}\\ p\equiv b \bmod q}} \log p\Bigg) + \sum_{\frac{2}{\epsilon}\le e\le 2\log x} \sum_{p\le x^{1/e}} \log p\\ &\ll \sum_{2\le e\le \frac{2}{\epsilon}} e^{\omega(q)}\left(1 + \frac{x^{1/e}}{q}\right)\log x + \sum_{\frac{2}{\epsilon}\le e\le 2\log x} x^{1/e}\\ &\ll \left(\frac{2}{\epsilon}\right)^{\omega(q)+1}\left(1 + \frac{x^{1/2}}{q}\right)\log x + x^{\epsilon/2}\log x\\ &\ll_\epsilon x^\epsilon\left(1 + \frac{x^{1/2}}{q}\right),\end{aligned} \tag{4-8}$$

provided q is large enough in terms of ϵ.

Thus, for $1 + \epsilon \le u \le 2$, we have

$$\psi(q^u; q, 1) \ll_\epsilon \frac{q^{u-1}\log(q^u)\log\log q}{(u-1)\log q} + q^\epsilon + q^{u/2-1+\epsilon} \ll_\epsilon q^{u-1}\log\log q, \tag{4-9}$$

which bounds the integral from $1 + \epsilon$ to σ by

$$\ll \int_{1+\epsilon}^{\sigma} q^{u/2-1}\log\log q\, du \ll \frac{\log\log q}{\log q} q^{\sigma/2-1}, \tag{4-10}$$

completing the proof. □

5. Results under GRH (Theorems 1.2 and 2.6)

In this section we assume GRH (but none of the stronger results about the distribution of primes among residue classes) and prove Theorems 1.2 and 2.6. The main ingredient in the proofs are the results of [Fouvry 1985; Bombieri et al. 1986; Friedlander and Granville 1992; Fiorilli 2012]. The following is the needed conditional version.

Theorem 5.1. *Assume GRH. Fix an integer $a \neq 0$ and $\epsilon > 0$. For $M = M(x) \leq x^{1/4}$, we have*

$$\sum_{\substack{\frac{x}{2M} < q \leq \frac{x}{M} \\ (q,a)=1}} \left(\psi(x;q,a) - \Lambda(a) - \frac{\psi(x)}{\phi(q)} \right) = \frac{\phi(a)}{a} \frac{x}{2M} \mu_0(a,M) + O_{a,\epsilon}\left(\frac{x}{M^{3/2-\epsilon}} + \sqrt{x} M (\log x)^2 \right), \tag{5-1}$$

where

$$\mu_0(a,M) := \begin{cases} -\frac{1}{2}\log M - \frac{1}{2}C_6 & \text{if } a = \pm 1 \\ -\frac{1}{2}\log p & \text{if } a = \pm p^e \\ 0 & \text{otherwise,} \end{cases} \tag{5-2}$$

with

$$C_6 := \log \pi + 1 + \gamma + \sum_p \frac{\log p}{p(p-1)}. \tag{5-3}$$

Proof. See [Fiorilli 2012, Remark 1.5]. Note that the restriction $M = o(x^{1/4}/\log x)$ is required for the error term to be negligible compared to the main term, but it can be changed to $M \leq x^{1/4}$. □

We now proceed to prove Theorems 1.2 and 2.6. Note that by the averaged 1-level density (Proposition 3.2), the proof is completed by analyzing the average of $T_4(q)$:

$$\frac{1}{Q/2} \sum_{Q/2 < q \leq Q} T_4(q) = 2\int_0^{\sigma} \left(\frac{f(u)}{2} - \frac{f'(u)}{\log Q} \right) \frac{1}{Q/2} \sum_{Q/2 < q \leq Q} \frac{\psi(Q^u;q,1) - \psi(Q^u)/\phi(q)}{Q^{u/2}}\, du. \tag{5-4}$$

We break the integral into regions and bound each separately. Going through the proof of Theorem 2.1 and applying GRH, we see that the contribution to the integral from $u \in [0,1]$ equals

$$-\frac{4\log 2}{Q}\frac{\zeta(2)\zeta(3)}{\zeta(6)}\int_0^1 Q^{u/2}\left(\frac{f(u)}{2}-\frac{f'(u)}{\log Q}\right)du + O\left(\frac{\log^2 Q}{Q}\right). \tag{5-5}$$

We now analyze the three cases of the theorem, corresponding to different support restrictions for our test function.

Proof of Theorem 2.6 (2). To prove (2-10), we need to understand the part of the integral in (5-4) with $a \le u \le 2$. Arguing as in [Friedlander and Granville 1992] (see also the proof of [Fiorilli 2012, Proposition 6.1]), we have, for $x^{1/2} \le Q \le x$,

$$\sum_{Q/2<q\le Q}\left(\psi(x;q,1)-\frac{\psi(x)}{\phi(q)}\right) \ll Q\,(\log(x/Q)+1)+\frac{x^{3/2}(\log x)^2}{Q}. \tag{5-6}$$

The basic idea to obtain this last estimate is to write

$$\sum_{Q/2<q\le Q}\psi(x;q,1)=\sum_{\substack{n\le x\\ n-1=qr\\ Q/2<q\le Q}}\Lambda(n),$$

and to turn this into a sum over $r \le 2(x-1)/Q$ of the function

$$\psi(x;r,1)-\psi(rQ/2+1;r,1).$$

One then applies GRH and estimates the resulting sum over r using estimates on the summatory function of $1/\phi(r)$. Applying (5-6), the part of the integral in (5-4) with $a \le u \le 2$ is

$$\begin{aligned} &\ll \int_a^\sigma \left(Q^{-u/2}(\log(Q^{u-1})+1)+Q^{u-2}(\log(Q^u))^2\right)du \qquad (5\text{-}7)\\ &\ll Q^{-a/2}+Q^{\sigma-2}\log Q, \end{aligned}$$

□

Proof of Theorem 2.6 (1). We need to study the part of the integral in (5-4) with $1+\kappa \le u \le \frac{3}{2}$. We first see that by (5-7), the part of the integral with $\frac{4}{3} \le u \le \frac{3}{2}$ is

$$\ll Q^{-2/3}+Q^{\sigma-2}\log Q. \tag{5-8}$$

We turn to the part of the integral with $1+\kappa \le u \le \frac{4}{3}$. We have by Theorem 5.1 (setting $x := Q^u$ and $M := Q^{u-1}$) that it is

$$= 2\int_{1+\kappa}^{4/3}\Big(\frac{f(u)}{2}-\frac{f'(u)}{\log Q}\Big)Q^{-u/2}\Big(-\tfrac{1}{2}\log(Q^{u-1})-\tfrac{1}{2}C_6 + O_\epsilon\big(Q^{\frac{1-u}{2}(1-\epsilon)}+Q^{\frac{3}{2}u-2}(\log Q^u)^2\big)\Big)\,du$$

$$= -\int_{1+\kappa}^{4/3}\big((u-1)\log Q + C_6\big)Q^{-u/2}\Big(\frac{f(u)}{2}-\frac{f'(u)}{\log Q}\Big)\,du + O_\epsilon\Big(\frac{Q^{-1/2-\kappa(1-\epsilon)}}{\log Q}+Q^{-2/3}\log Q\Big); \quad (5\text{-}9)$$

hence (2-9) holds. □

Proof of Theorem 1.2. We now turn to (1-5), with f supported in $(-\frac{3}{2},\frac{3}{2})$. Set

$$\kappa := \frac{A\log\log Q}{\log Q},$$

with $A \geq 1$ a constant. As the big-O constant in (5-9) is independent of κ, we may use (5-9) to estimate the contribution to (5-4) from $u \in [1+\kappa, 4/3]$. This part of the integral contributes

$$-\int_{1+\kappa}^{4/3}\big((u-1)\log Q + C_6\big)Q^{-u/2}\Big(\frac{f(u)}{2}-\frac{f'(u)}{\log Q}\Big)\,du + O_\epsilon\Big(\frac{Q^{-1/2}}{(\log Q)^{A(1-\epsilon)+1}}\Big) \ll \frac{Q^{-1/2}}{(\log Q)^{A/2}}. \quad (5\text{-}10)$$

The part of the integral with $\frac{4}{3} \leq u \leq \frac{3}{2}$ was already shown to be $\ll Q^{-2/3} + Q^{\sigma-2}\log Q$, and hence is absorbed into the error term since $\sigma < \frac{3}{2}$.

We now come to the heart of the argument, the part of the integral where $1 \leq u \leq 1+\kappa$. Since $f \in C^2(\mathbb{R})$, we have that in our range of u, the function $g(u) := \frac{1}{2}f(u) - f'(u)/\log Q$ satisfies

$$\begin{aligned} g(u) &= \frac{f(1)}{2}+\frac{f'(1)}{2}(u-1)+O\big((u-1)^2\big)-\frac{f'(1)}{\log Q}+O\Big(\frac{u-1}{\log Q}\Big) \\ &= P(u-1)+O\Big(\frac{(\log\log Q)^2}{(\log Q)^2}\Big), \end{aligned} \quad (5\text{-}11)$$

where

$$P(u) := \frac{f(1)}{2}-\frac{f'(1)}{\log Q}+\frac{f'(1)}{2}u.$$

At this point, if f were $C^K(\mathbb{R})$, we could take its Taylor expansion and get an error of

$$O_{\epsilon,A}\big((\log\log Q)^K/(\log Q)^K\big).$$

We cannot apply Theorem 5.1 directly since the error term is not got enough for moderate values of M. Instead, we argue as in the proof of [Fiorilli 2012, Proposition 6.1]. Slightly modifying the proof and using GRH, we get

$$\begin{aligned}\sum_{Q/2<q\le Q}\left(\psi(x;q,a)-\frac{\psi(x)}{\phi(q)}\right) \\ = x\left(-C_1-\sum_{r<\frac{x-1}{Q}}\frac{1}{\phi(r)}\left(1-\frac{r}{x/Q}\right)+\sum_{r<\frac{x-1}{Q/2}}\frac{1}{\phi(r)}\left(1-\frac{r}{2x/Q}\right)\right) \\ +O_\epsilon\left(\frac{x^{3/2+\epsilon/2}}{Q}\right),\end{aligned} \tag{5-12}$$

with

$$C_1 := \frac{\zeta(2)\zeta(3)}{\zeta(6)}\log 2. \tag{5-13}$$

(We used that $\sum_{Q/2<q\le Q}=\sum_{Q/2<q\le x}-\sum_{Q<q\le x}$, as in the proof of [Fiorilli 2013, Theorem 4.1*].) The contribution of the error term in (5-12) to the part of the integral in (5-4) with $1\le u\le 1+\kappa$ is (remember $\kappa\log Q = A\log\log Q$)

$$\ll \int_1^{1+\kappa}\frac{1}{Q/2}\frac{Q^{3u/2+\epsilon u/2}/Q}{Q^{u/2}}\,du \ll_\epsilon Q^{-1+\epsilon}. \tag{5-14}$$

Therefore, all that remains to complete the proof of Theorem 1.2 it to estimate the contribution to (5-4) from $u\in[1,1+\kappa]$. Using [Fiorilli 2012, Lemma 5.9] to bound the error in replacing $g(u)$ with $P(u-1)$, we find

$$\begin{aligned}2\int_1^{1+\kappa}g(u)\frac{Q^{u/2}}{Q/2}\left(-C_1-\sum_{r<\frac{Q^u-1}{Q}}\frac{1}{\phi(r)}\left(1-\frac{r}{Q^{u-1}}\right)+\sum_{r<\frac{Q^u-1}{Q/2}}\frac{1}{\phi(r)}\left(1-\frac{r}{2Q^{u-1}}\right)\right)du \\ = 4\int_1^{1+\kappa}P(u-1)Q^{u/2-1} \\ \left(-C_1-\sum_{r\le\frac{Q^u-1}{Q}}\frac{1}{\phi(r)}\left(1-\frac{r}{Q^{u-1}}\right)+\sum_{r\le\frac{Q^u-1}{Q/2}}\frac{1}{\phi(r)}\left(1-\frac{r}{2Q^{u-1}}\right)\right)du \\ +O\left(\frac{Q^{-1/2}(\log\log Q)^2}{(\log Q)^3}\right);\end{aligned} \tag{5-15}$$

we changed $r<\cdots$ to $r\le\cdots$ in the sums above, which gives a negligible error term.

Setting $R := Q^\kappa - 1/Q$, we compute that

$$\begin{aligned}
&\int_1^{1+\kappa} P(u-1) Q^{\frac{u}{2}-1} \sum_{r \le \frac{Q^u-1}{Q}} \frac{1}{\phi(r)}\Big(1-\frac{r}{Q^{u-1}}\Big)\,du \\
&\quad = \frac{1}{Q}\sum_{r\le Q^\kappa-\frac{1}{Q}} \frac{1}{\phi(r)} \int_{1+\frac{\log(r+Q^{-1})}{\log Q}}^{1+\kappa} P(u-1)\Big(Q^{u/2}-\frac{r}{Q^{u/2-1}}\Big)\,du \\
&\quad = \frac{1}{Q}\sum_{r\le R}\frac{1}{\phi(r)}\int_{1+\kappa\frac{\log r}{\log R}}^{1+\kappa} P(u-1)\Big(Q^{u/2}-\frac{r}{Q^{u/2-1}}\Big)\,du + O_\epsilon\big(Q^{-3/2+\epsilon}\big),
\end{aligned}$$

the error term coming from the fact that we replaced $\log(r+Q^{-1})$ by $\log r$. Performing two changes of variables, we obtain that this is

$$\begin{aligned}
&= Q^{-1/2}\sum_{r\le R}\frac{1}{\phi(r)}\int_{\kappa\frac{\log r}{\log R}}^{\kappa} P(u)\Big(Q^{u/2}-\frac{r}{Q^{u/2}}\Big)\,du + O_\epsilon\big(Q^{-3/2+\epsilon}\big) \\
&= Q^{-1/2}\sum_{r\le R}\frac{1}{\phi(r)}\int_{\frac{\log r}{\log R}}^{1} \kappa P(\kappa v)\Big(R^{v/2}-\frac{r}{R^{v/2}}\Big)\,dv + O_\epsilon\big(Q^{-3/2+\epsilon}\big). \qquad (5\text{-}16)
\end{aligned}$$

Let

$$\begin{aligned}
F_1 &:= -4\zeta(\tfrac{1}{2})\prod_p\Big(1+\frac{1}{(p-1)p^{1/2}}\Big), \\
F_2 &:= F_1\Big(\frac{\zeta'}{\zeta}(\tfrac12)-\sum_p\frac{\log p}{(p-1)p^{1/2}+1}\Big). \qquad (5\text{-}17)
\end{aligned}$$

By Lemma 3.4, we find that (5-16) equals

$$\begin{aligned}
&\frac{\kappa}{Q^{1/2}}\Big(E_1\log R\int_{-\infty}^1 R^{u/2} v P(\kappa v)\,dv + E_2\int_{-\infty}^1 R^{v/2}P(\kappa v)\,dv \\
&\qquad\qquad + F_1\frac{P(\kappa)-\kappa P'(\kappa)}{\log R} + F_2\frac{-\kappa P'(\kappa)}{(\log R)^2} + O\big(R^{-1/2}\big)\Big) \\
&= Q^{-1/2}\Big(E_1\log Q\int_{-\infty}^{\kappa} Q^{u/2}uP(u)\,du + E_2\int_{-\infty}^{\kappa} Q^{u/2}P(u)\,du \\
&\qquad\qquad + F_1\frac{\frac{f(1)}{2}-\frac{f'(1)}{\log Q}}{\log Q} - F_2\frac{f'(1)}{2(\log Q)^2} + O\big(R^{-1/2}\big)\Big). \qquad (5\text{-}18)
\end{aligned}$$

We obtain in an analogous way with $R := 2Q^{\kappa} - 2/Q$ that

$$\int_1^{1+\kappa} P(u-1)Q^{u/2-1} \sum_{r \le 2\frac{Q^u-1}{Q}} \frac{1}{\phi(r)}\Bigl(1-\frac{r}{2Q^{u-1}}\Bigr)\,du$$
$$= Q^{-1/2}\sum_{r\le R}\frac{1}{\phi(r)}\int_{\frac{\log(r/2)}{\log(R/2)}}^{1}\kappa P(\kappa v)\Bigl((R/2)^{v/2}-\frac{r}{2(R/2)^{v/2}}\Bigr)\,dv$$
$$+O_\epsilon\bigl(Q^{-3/2+\epsilon}\bigr), \quad (5\text{-}19)$$

which by Lemma 3.4 is

$$= \frac{\kappa}{Q^{1/2}}\Bigl(E_1\log(R/2)\int_{-\infty}^{1}(R/2)^{v/2}vP(\kappa v)\,dv$$
$$+(E_2+E_1\log 2)\int_{-\infty}^{1}(R/2)^{v/2}P(\kappa v)\,dv$$
$$+\sum_{j=1}^{n}\frac{F_j^{(2)}}{(\log(R/2))^j}+O\bigl(R^{-1/2}\bigr)\Bigr)$$
$$= Q^{-1/2}\Bigl(E_1\log Q\int_{-\infty}^{\kappa}Q^{u/2}uP(u)\,du$$
$$+(E_2+E_1\log 2)\int_{-\infty}^{\kappa}Q^{u/2}P(u)\,dv+\frac{F_1}{\sqrt{2}}\frac{\frac{f(1)}{2}-\frac{f'(1)}{\log Q}}{\log Q}$$
$$-\frac{F_2+F_1\log 2}{\sqrt{2}}\frac{f'(1)}{2(\log Q)^2}+O\bigl(R^{-1/2}\bigr)\Bigr). \quad (5\text{-}20)$$

We now substitute (5-18) and (5-20) in (5-15), to get that (5-15) is (notice the remarkable cancellations)

$$= -4C_1\int_1^{1+\kappa}P(u-1)Q^{u/2-1}\,du + 4E_1\log 2Q^{-1/2}\int_{-\infty}^{\kappa}Q^{u/2}P(u)\,du$$
$$+4Q^{-1/2}\Bigl(-F_1\frac{\frac{f(1)}{2}-\frac{f'(1)}{\log Q}}{\log Q}+F_2\frac{f'(1)}{2(\log Q)^2}$$
$$+\frac{F_1}{\sqrt{2}}\frac{\frac{f(1)}{2}-\frac{f'(1)}{\log Q}}{\log Q}-\frac{F_2+F_1\log 2}{\sqrt{2}}\frac{f'(1)}{2(\log Q)^2}\Bigr)$$
$$+O\Bigl(Q^{-1/2}\frac{(\log\log Q)^2}{(\log Q)^3}+\frac{Q^{-\frac{1}{2}}}{(\log Q)^{A/2}}\Bigr), \quad (5\text{-}21)$$

which by (3-31) and (5-13) is

$$= 4\log 2\frac{\zeta(2)\zeta(3)}{\zeta(6)}\int_{-\infty}^{1} P(u-1)Q^{u/2-1}\,du \\ +(2-\sqrt{2})Q^{-1/2}\biggl(-F_1\frac{f(1)}{\log Q}+\Bigl(F_2-\frac{\sqrt{2}+4}{3}F_1\Bigr)\frac{f'(1)}{(\log Q)^2}\biggr) \\ +O\biggl(Q^{-1/2}\frac{(\log\log Q)^2}{(\log Q)^3}+\frac{Q^{-1/2}}{(\log Q)^{A/2}}\biggr). \qquad (5\text{-}22)$$

But, yet another cancellation is coming: we have

$$\int_{-\infty}^{1} P(u-1)Q^{u/2-1}\,du \\ =\int_{-\infty}^{1} g(u)Q^{u/2-1}\,du+O\biggl(Q^{-1/2}\frac{(\log\log Q)^2}{(\log Q)^3}\biggr), \qquad (5\text{-}23)$$

and so by (5-5) this term cancels (up to the error term $O(Q^{-1})$) with the part of the integral of $T_4(Q)$ with $u \le 1$ (which is coming from a totally different part of the problem, where there are no primes in arithmetic progressions involved)!

Combining all the terms,

$$\frac{1}{Q/2}\sum_{Q/2<q\le Q} T_4(Q) \\ =(2-\sqrt{2})Q^{-1/2}\biggl(-F_1\frac{f(1)}{\log Q}+\Bigl(F_2-\frac{\sqrt{2}+4}{3}F_1\Bigr)\frac{f'(1)}{(\log Q)^2}\biggr) \\ +O\biggl(\frac{Q^{-1/2}}{(\log Q)^{A/2}}+Q^{-1/2}\frac{(\log\log Q)^2}{(\log Q)^3}\biggr). \qquad (5\text{-}24)$$

The proof is completed by taking $A = 6$. □

6. Results under de-averaging hypothesis (Theorem 2.8)

In this section we assume the de-averaging hypothesis (Hypothesis 2.7), which relates the variance in the distribution of primes congruent to 1 to the average variance over all residue classes. Explicitly, we assume (2-13) holds for some $\delta \in (0,1]$, and show how this allows us to compute the main term in the averaged 1-level density, $D_{1;Q/2,Q}(\widehat{f})$, for test functions f supported in $[-4+2\delta, 4-2\delta]$. (Remember that this hypothesis is trivially true for $\delta = 1$, and expected to hold for any $\delta > 0$.)

Proof of Theorem 2.8. Starting from (3-23), we have

$$T_4(q) = 2\int_0^{\infty}\Bigl(\frac{f(u)}{2}-\frac{f'(u)}{\log Q}\Bigr)\frac{\psi(Q^u;q,1)-\psi(Q^u)/\phi(q)}{Q^{u/2}}\,du. \qquad (6\text{-}1)$$

Feeding this into Proposition 3.2, we are left with determining

$$\begin{aligned}\frac{1}{Q/2}&\sum_{Q/2<q\le Q} T_4(q)\\&=\frac{1}{Q/2}\int_0^{\sigma}\left(\frac{f(u)}{2}-\frac{f'(u)}{\log Q}\right)Q^{-u/2}\sum_{Q/2<q\le Q}\left(\psi(Q^u;q,1)-\frac{\psi(Q^u)}{\phi(q)}\right)du. \qquad (6\text{-}2)\end{aligned}$$

We have already seen in the proof of Theorem 2.1 that the part of the integral in (6-2) with $0\le u\le 1$ is $O(Q^{-1/2})$. For the part where $u\ge 1$, the Cauchy–Schwarz inequality shows that its contribution to the integral in (6-2) is

$$\ll \frac{1}{Q/2}\int_1^{\sigma} Q^{-u/2}\left|\sum_{Q/2<q\le Q}\left(\psi(Q^u;q,1)-\frac{\psi(Q^u)}{\phi(q)}\right)^2\right|^{1/2}\left|\sum_{Q/2<q\le Q}1^2\right|^{1/2}du. \qquad (6\text{-}3)$$

Now, by Hypothesis 2.7, this is

$$\begin{aligned}\ll \frac{1}{Q/2}&\int_1^{\sigma} Q^{-u/2}Q^{(\delta-1)/2}\\&\times\left(\sum_{Q/2<q\le Q}\sum_{\substack{1\le a\le q\\(a,q)=1}}\left(\psi(Q^u;q,a)-\frac{\psi(Q^u)}{\phi(q)}\right)^2\right)^{1/2}Q^{1/2}\,du. \qquad (6\text{-}4)\end{aligned}$$

We now use a result in [Goldston and Vaughan 1997], which states that under GRH we have for $1\le Q\le x$ that

$$\begin{aligned}&\sum_{q\le Q}\sum_{\substack{1\le a\le q\\(a,q)=1}}\left(\psi(x;q,a)-\frac{\psi(x)}{\phi(q)}\right)^2\\&\quad=Qx\log Q-cxQ+O_\epsilon\big(Q^2(x/Q)^{1/4+\epsilon}+x^{3/2}(\log 2x)^{5/2}(\log\log 3x)^2\big), \qquad (6\text{-}5)\end{aligned}$$

where

$$c:=\gamma+\log 2\pi+1+\sum_p\frac{\log p}{p(p-1)}.$$

We now split the range of integration into the two subintervals $1\le u\le 2$ and $2\le u\le\sigma$. In the first range, we have, for $\epsilon>0$ small enough, $u+1\ge\max(\frac{7}{4}+\frac{1}{4}u+\epsilon(u-1),\frac{3}{2}u)$, so (6-5) implies that

$$\sum_{q\le Q}\sum_{\substack{1\le a\le q\\(a,q)=1}}\left(\psi(x;q,a)-\frac{\psi(x)}{\phi(q)}\right)^2\ll Qx(\log x)^3 \qquad (6\text{-}6)$$

(which, up to x^ϵ, follows from the original result in [Hooley 1975]), so we get that the part of (6-4) with $1 \le u \le 2$ is

$$\ll\ Q^{\delta/2-1}\int_1^2 Q^{-u/2}Q^{(u+1)/2}(\log Q)^{3/2}\,du\ \ll\ Q^{(\delta-1)/2}(\log Q)^{3/2}, \tag{6-7}$$

which is $o(1)$ if $\delta < 1$.

We now examine the second interval, that is $2 \le u \le \sigma$. In this range, (6-5) becomes

$$\sum_{q\le Q}\ \sum_{\substack{1\le a\le q\\(a,q)=1}}\biggl(\psi(x;q,a)-\frac{\psi(x)}{\phi(q)}\biggr)^2 \ll x^{3/2}(\log x)^{5/2}(\log\log x)^2 \tag{6-8}$$

(which, up to a factor of x^ϵ, follows from Hooley's original result). We thus get that the part of (6-4) with $2 \le u \le \sigma$ is

$$\begin{aligned}&\ll \frac{Q^{\delta/2}}{Q/2}\int_2^\sigma Q^{-u/2}Q^{3u/4}(u\log Q)^{5/4}\log\log(Q^u)\,du\\ &\ll Q^{(\sigma+2\delta)/4-1}(\log Q)^{1/4}\log\log Q.\end{aligned} \tag{6-9}$$

If $\sigma < 4-2\delta$ then the above is $o(1)$, completing the proof. □

7. Results under Montgomery's hypothesis (Theorem 2.13)

We continue our investigations beyond the GRH, and assume a smoothed version of Montgomery's hypothesis, Hypothesis 2.12. Interestingly, this assumption allows us to compute the main term of the 1-level density, $D_{1;q}(\widehat{f})$, for test functions of arbitrarily large (but finite) support. While similar results have been previously observed [Miller and Sarnak 2003], we include a proof both for completeness and because these observations are not in the literature.

Proof of Theorem 2.13. As we are fixing the modulus, we take $Q := q$. By the explicit formula from Proposition 3.1, we have

$$\begin{aligned}D_{1;q}(\widehat{f}) &= \frac{f(0)}{\log q}\biggl(\log q-\log(8\pi e^\gamma)-\sum_{p\mid q}\frac{\log p}{p-1}\biggr)\\ &\quad+\int_0^\infty\frac{f(0)-f(t)}{q^{t/2}-q^{-t/2}}\,dt\\ &\quad-\frac{2}{\log q}\biggl(\sum_{n\equiv 1 \bmod q}-\frac{1}{\phi(q)}\sum_n\biggr)\frac{\Lambda(n)}{n^{1/2}}f\biggl(\frac{\log n}{\log q}\biggr)+O\biggl(\frac{1}{\phi(q)}\biggr).\end{aligned} \tag{7-1}$$

Let $\sigma := \sup(\operatorname{supp} f) < \infty$. We proved in Section 4 that the only terms that are not $O(1/\log q)$ are the leading term $f(0)$ and possibly the prime sum, which we now study. We have

$$T_4(q) = 2\int_0^\infty \biggl(\frac{f(u)}{2} - \frac{f'(u)}{\log q}\biggr) \frac{\psi(q^u;q,1) - \psi(q^u)/\phi(q)}{q^{u/2}}\,du. \tag{7-2}$$

In the proof of Theorem 2.1 we determined that the part of the integral with $0 \le u \le 1$ is $O(q^{-1/2})$. From the proof of Theorem 2.3, the part with $1 \le u \le 2$ is $O(\log\log q/\log q)$.

Proof of (1). For the rest of the integral, we use Hypothesis 2.12. Note that $u \ge 2$, so $x = q^u \ge q^2$ with $u \le \sigma$, hence we can replace $o_{x\to\infty}$ by $o_{q\to\infty}$. An integration by parts gives that the rest of the integral is

$$\begin{aligned} &= 0 - \biggl(\frac{f(2)}{2} - \frac{f'(2)}{\log q}\biggr) \frac{\psi_2(q^2;q,1) - \psi_2(q^2)/\phi(q)}{q} \\ &\qquad - 2\int_0^\infty \biggl(\frac{3f(u)}{4} - \frac{2f'(u)}{\log q} + \frac{f''(u)}{(\log q)^2}\biggr) \frac{\psi_2(q^u;q,1) - \psi_2(q^u)/\phi(q)}{q^{u/2}}\,du \\ &= \frac{o(q)}{q} + \int_2^\sigma \bigl(|f(u)| + |f'(u)| + |f''(u)|\bigr) \frac{o(q^{u/2})}{q^{u/2}}\,du = o(1), \end{aligned} \tag{7-3}$$

proving the claim. Note that we are using the smoothed version of the prime sum.

Proof of (2). We already know that the part of the integral with $0 \le u \le 1$ is $\ll q^{-1/2}$. Taking $\epsilon := \epsilon'/\sigma$ in Hypothesis 2.11, the rest of the integral is $O\bigl(\int_1^\sigma q^{\epsilon u - \theta}\,du\bigr)$, which is $O\bigl(q^{\epsilon' - \theta}\bigr)$ and thus negligible if we may take $\theta > 0$. □

Remark 7.1. Depending on our assumptions about the size of the error term in the distribution of primes in residue classes, we may allow σ to grow with Q at various explicit rates.

Acknowledgments

The authors thank Andrew Granville, Chris Hughes, Jeffrey Lagarias, Zeév Rudnick and Peter Sarnak for many enlightening conversations, and the referee for many helpful suggestions. Fiorilli was supported by an NSERC doctoral, and later on postdoctoral fellowship, as well as NSF grant DMS-0635607, and pursued this work at the Université de Montréal, the Institute for Advanced Study and the University of Michigan. Miller was partially supported by NSF grants DMS-0600848, DMS-0970067 and DMS-1265673.

References

[Abramowitz and Stegun 1972] M. Abramowitz and I. A. Stegun (editors), *Handbook of mathematical functions with formulas, graphs, and mathematical tables*, 10th ed., National Bureau of Standards Applied Mathematics Series **55**, U.S. Government Printing Office, Washington, D.C., 1972. Zbl 0543.33001

[Alpoge and Miller 2014] L. Alpoge and S. J. Miller, “Low-lying zeros of Maass form L-functions”, preprint, 2014. To appear in IMRN.

[Alpoge et al. 2014] L. Alpoge, N. Amersi, G. Iyer, O. Lazareva, S. J. Miller, and L. Zhang, “Maass waveforms and low-lying zeros”, preprint, 2014. arXiv 1306.5886

[Bombieri et al. 1986] E. Bombieri, J. B. Friedlander, and H. Iwaniec, “Primes in arithmetic progressions to large moduli”, *Acta Math.* **156**:3-4 (1986), 203–251. MR 88b:11058 Zbl 0588.10042

[Conrey 2001] J. B. Conrey, “L-functions and random matrices”, pp. 331–352 in *Mathematics unlimited—2001 and beyond*, edited by B. Engquist and W. Schmid, Springer, Berlin, 2001. MR 2002g:11134 Zbl 1048.11071

[Conrey 2007] J. B. Conrey, “The mean-square of Dirichlet L-functions”, preprint, 2007. arXiv 0708.2699v1

[Conrey and Iwaniec 2002] B. Conrey and H. Iwaniec, “Spacing of zeros of Hecke L-functions and the class number problem”, *Acta Arith.* **103**:3 (2002), 259–312. MR 2003h:11103 Zbl 1007.11051

[Conrey and Snaith 2007] J. B. Conrey and N. C. Snaith, “Applications of the L-functions ratios conjectures”, *Proc. Lond. Math. Soc.* (3) **94**:3 (2007), 594–646. MR 2009a:11179 Zbl 1183.11050

[Conrey and Snaith 2008] J. B. Conrey and N. C. Snaith, “Triple correlation of the Riemann zeros”, *J. Théor. Nombres Bordeaux* **20**:1 (2008), 61–106. MR 2009f:11109 Zbl 1208.11103

[Conrey et al. 2005a] J. B. Conrey, D. W. Farmer, J. P. Keating, M. O. Rubinstein, and N. C. Snaith, “Integral moments of L-functions”, *Proc. London Math. Soc.* (3) **91**:1 (2005), 33–104. MR 2006j:11120 Zbl 1075.11058

[Conrey et al. 2005b] J. B. Conrey, D. W. Farmer, and M. R. Zimbauer, “Howe pairs, supersymmetry, and ratios of random characteristic polynomials for the unitary groups U_N”, preprint, 2005. arXiv math-ph/0511024

[Conrey et al. 2008] B. Conrey, D. W. Farmer, and M. R. Zirnbauer, “Autocorrelation of ratios of L-functions”, *Commun. Number Theory Phys.* **2**:3 (2008), 593–636. MR 2009j:11138 Zbl 1178.11056

[Davenport 1980] H. Davenport, *Multiplicative number theory*, 2nd ed., Graduate Texts in Mathematics **74**, Springer, New York, 1980. MR 82m:10001 Zbl 0453.10002

[David et al. 2013] C. David, D. K. Huynh, and J. Parks, “One-level density of families of elliptic curves and the ratio conjectures”, preprint, 2013. arXiv 1309.1027

[Dueñez and Miller 2006] E. Dueñez and S. J. Miller, “The low lying zeros of a GL(4) and a GL(6) family of L-functions”, *Compos. Math.* **142**:6 (2006), 1403–1425. MR 2007k:11141 Zbl 1124.11040

[Dueñez and Miller 2009] E. Dueñez and S. J. Miller, “The effect of convolving families of L-functions on the underlying group symmetries”, *Proc. Lond. Math. Soc.* (3) **99**:3 (2009), 787–820. MR 2010k:11145 Zbl 1244.11079

[Fiorilli 2012] D. Fiorilli, “Residue classes containing an unexpected number of primes”, *Duke Math. J.* **161**:15 (2012), 2923–2943. MR 2999316 Zbl 1264.11081

[Fiorilli 2013] D. Fiorilli, “The influence of the first term of an arithmetic progression”, *Proc. Lond. Math. Soc.* (3) **106**:4 (2013), 819–858. MR 3056294 Zbl 06170788

[Fiorilli and Martin 2013] D. Fiorilli and G. Martin, “Inequities in the Shanks–Rényi prime number race: An asymptotic formula for the densities”, *J. Reine Angew. Math.* **676** (2013), 121–212. MR 3028758 Zbl 1276.11150

[Firk and Miller 2009] F. W. K. Firk and S. J. Miller, “Nuclei, primes and the random matrix connection”, *Symmetry* **1**:1 (2009), 64–105. MR 2012h:11126

[Fouvry 1985] É. Fouvry, "Sur le problème des diviseurs de Titchmarsh", *J. Reine Angew. Math.* **357** (1985), 51–76. MR 87b:11090 Zbl 0547.10039

[Fouvry and Iwaniec 2003] E. Fouvry and H. Iwaniec, "Low-lying zeros of dihedral L-functions", *Duke Math. J.* **116**:2 (2003), 189–217. MR 2003k:11139 Zbl 1028.11055

[Friedlander and Granville 1992] J. B. Friedlander and A. Granville, "Relevance of the residue class to the abundance of primes", pp. 95–103 in *Proceedings of the Amalfi Conference on Analytic Number Theory* (Maiori, 1989), edited by E. Bombieri et al., Univ. Salerno, Salerno, 1992. MR 94i:11067 Zbl 0795.11040

[Friedlander et al. 1991] J. Friedlander, A. Granville, A. Hildebrand, and H. Maier, "Oscillation theorems for primes in arithmetic progressions and for sifting functions", *J. Amer. Math. Soc.* **4**:1 (1991), 25–86. MR 92a:11103 Zbl 0724.11040

[Gao 2005] P. Gao, *N-level density of the low-lying zeros of quadratic Dirichlet L-functions*, Ph.D. thesis, University of Michigan, 2005, http://search.proquest.com/docview/305462205.

[Goes et al. 2010] J. Goes, S. Jackson, S. J. Miller, D. Montague, K. Ninsuwan, R. Peckner, and T. Pham, "A unitary test of the ratios conjecture", *J. Number Theory* **130**:10 (2010), 2238–2258. MR 2011g:11162 Zbl 1276.11141

[Goldfeld 1976] D. M. Goldfeld, "The class number of quadratic fields and the conjectures of Birch and Swinnerton–Dyer", *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* (4) **3**:4 (1976), 624–663. MR 56 #8529 Zbl 0345.12007

[Goldston and Vaughan 1997] D. A. Goldston and R. C. Vaughan, "On the Montgomery–Hooley asymptotic formula", pp. 117–142 in *Sieve methods, exponential sums, and their applications in number theory* (Cardiff, 1995), edited by G. R. H. Greaves et al., London Math. Soc. Lecture Note Ser. **237**, Cambridge Univ. Press, 1997. MR 99d:11099 Zbl 0929.11034

[Gonek et al. 2007] S. M. Gonek, C. P. Hughes, and J. P. Keating, "A hybrid Euler–Hadamard product for the Riemann zeta function", *Duke Math. J.* **136**:3 (2007), 507–549. MR 2008e:11100 Zbl 1171.11049

[Gross and Zagier 1986] B. H. Gross and D. B. Zagier, "Heegner points and derivatives of L-series", *Invent. Math.* **84**:2 (1986), 225–320. MR 87j:11057 Zbl 0608.14019

[Güloğlu 2005] A. M. Güloğlu, "Low-lying zeroes of symmetric power L-functions", *Int. Math. Res. Not.* **2005**:9 (2005), 517–550. MR 2006g:11180 Zbl 1168.11312

[Hayes 2003] B. Hayes, "The spectrum of Riemannium", *American Scientist* **91**:4 (2003), 296–300.

[Heath-Brown 1981] D. R. Heath-Brown, "An asymptotic series for the mean value of Dirichlet L-functions", *Comment. Math. Helv.* **56**:1 (1981), 148–161. MR 83c:10059 Zbl 0457.10020

[Hejhal 1994] D. A. Hejhal, "On the triple correlation of zeros of the zeta function", *Int. Math. Res. Not.* **1994**:7 (1994), 294–302. MR 96d:11093 Zbl 0813.11048

[Hooley 1975] C. Hooley, "On the Barban–Davenport–Halberstam theorem, I", *J. Reine Angew. Math.* **274/275** (1975), 206–223. MR 52 #3090a Zbl 0304.10027

[Hughes and Miller 2007] C. P. Hughes and S. J. Miller, "Low-lying zeros of L-functions with orthogonal symmetry", *Duke Math. J.* **136**:1 (2007), 115–172. MR 2009b:11145 Zbl 1124.11041

[Hughes and Rudnick 2003] C. P. Hughes and Z. Rudnick, "Linear statistics of low-lying zeros of L-functions", *Q. J. Math.* **54**:3 (2003), 309–333. MR 2005a:11131 Zbl 1068.11055

[Huynh et al. 2009] D. K. Huynh, J. P. Keating, and N. C. Snaith, "Lower order terms for the one-level density of elliptic curve L-functions", *J. Number Theory* **129**:12 (2009), 2883–2902. MR 2010i:11094 Zbl 1205.11077

[Huynh et al. 2011] D. K. Huynh, S. J. Miller, and R. Morrison, "An elliptic curve test of the L-functions ratios conjecture", *J. Number Theory* **131**:6 (2011), 1117–1147. MR 2012d:11142 Zbl 1235.11084

[Iwaniec and Kowalski 2004] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications **53**, Amer. Math. Soc., Providence, RI, 2004. MR 2005h:11005 Zbl 1059.11001

[Iwaniec et al. 2000] H. Iwaniec, W. Luo, and P. Sarnak, "Low lying zeros of families of L-functions", *Inst. Hautes Études Sci. Publ. Math.* 91 (2000), 55–131. MR 2002h:11081 Zbl 1012.11041

[Katz and Sarnak 1999a] N. M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications **45**, Amer. Math. Soc., Providence, RI, 1999. MR 2000b:11070 Zbl 0958.11004

[Katz and Sarnak 1999b] N. M. Katz and P. Sarnak, "Zeroes of zeta functions and symmetry", *Bull. Amer. Math. Soc.* (*N.S.*) **36**:1 (1999), 1–26. MR 2000f:11114 Zbl 0921.11047

[Keating and Snaith 2000a] J. P. Keating and N. C. Snaith, "Random matrix theory and $\zeta(1/2+it)$", *Comm. Math. Phys.* **214**:1 (2000), 57–89. MR 2002c:11107 Zbl 1051.11048

[Keating and Snaith 2000b] J. P. Keating and N. C. Snaith, "Random matrix theory and L-functions at $s=1/2$", *Comm. Math. Phys.* **214**:1 (2000), 91–110. MR 2002c:11108 Zbl 1051.11047

[Keating and Snaith 2003] J. P. Keating and N. C. Snaith, "Random matrices and L-functions", *J. Phys. A* **36**:12 (2003), 2859–2881. MR 2004d:11090 Zbl 1074.11053

[Miller 2004] S. J. Miller, "One- and two-level densities for rational families of elliptic curves: Evidence for the underlying group symmetries", *Compos. Math.* **140** (2004), 952–992. MR 2005c:11085 Zbl 1120.11026

[Miller 2008] S. J. Miller, "A symplectic test of the L-functions ratios conjecture", *Int. Math. Res. Not.* **2008**:3 (2008), Art. ID rnm146. MR 2009h:11139 Zbl 1225.11104

[Miller 2009a] S. J. Miller, "Lower order terms in the 1-level density for families of holomorphic cuspidal newforms", *Acta Arith.* **137**:1 (2009), 51–98. MR 2010f:11146 Zbl 1214.11100

[Miller 2009b] S. J. Miller, "An orthogonal test of the L-functions ratios conjecture", *Proc. Lond. Math. Soc.* (3) **99**:2 (2009), 484–520. MR 2011g:11163 Zbl 1170.11027

[Miller and Montague 2011] S. J. Miller and D. Montague, "An orthogonal test of the L-functions ratios conjecture, II", *Acta Arith.* **146**:1 (2011), 53–90. MR 2012k:11139 Zbl 1233.11054

[Miller and Peckner 2012] S. J. Miller and R. Peckner, "Low-lying zeros of number field L-functions", *J. Number Theory* **132**:12 (2012), 2866–2891. MR 2965197 Zbl 06097268

[Miller and Sarnak 2003] S. J. Miller and P. Sarnak, personal communication, 2003.

[Montgomery 1970] H. L. Montgomery, "Primes in arithmetic progressions", *Michigan Math. J.* **17** (1970), 33–39. MR 41 #1660 Zbl 0209.34804

[Montgomery 1973] H. L. Montgomery, "The pair correlation of zeros of the zeta function", pp. 181–193 in *Analytic number theory* (St. Louis, MO, 1972), edited by H. G. Diamond, Amer. Math. Soc., Providence, R.I., 1973. MR 49 #2590 Zbl 0268.10023

[Montgomery and Vaughan 1973] H. L. Montgomery and R. C. Vaughan, "The large sieve", *Mathematika* **20** (1973), 119–134. MR 51 #10260 Zbl 0296.10023

[Montgomery and Vaughan 2007] H. L. Montgomery and R. C. Vaughan, *Multiplicative number theory, I: Classical theory*, Cambridge Studies in Advanced Mathematics **97**, Cambridge University Press, 2007. MR 2009b:11001 Zbl 1142.11001

[Odlyzko 1987] A. M. Odlyzko, "On the distribution of spacings between zeros of the zeta function", *Math. Comp.* **48**:177 (1987), 273–308. MR 88d:11082 Zbl 0615.10049

[Odlyzko 2001] A. M. Odlyzko, "The 10^{22}-nd zero of the Riemann zeta function", pp. 139–144 in *Dynamical, spectral, and arithmetic zeta functions* (San Antonio, TX, 1999), edited by M. L. Lapidus and M. van Frankenhuysen, Contemp. Math. **290**, Amer. Math. Soc., Providence, RI, 2001. MR 2003h:11109 Zbl 1022.11042

[Ricotta and Royer 2011] G. Ricotta and E. Royer, "Statistics for low-lying zeros of symmetric power L-functions in the level aspect", *Forum Math.* **23**:5 (2011), 969–1028. MR 2012k:11057 Zbl 1264.11080

[Royer 2001] E. Royer, "Petits zéros de fonctions L de formes modulaires", *Acta Arith.* **99**:2 (2001), 147–172. MR 2002g:11063 Zbl 0984.11024

[Rubinstein 2001] M. Rubinstein, "Low-lying zeros of L-functions and random matrix theory", *Duke Math. J.* **109**:1 (2001), 147–181. MR 2002f:11114 Zbl 1014.11050

[Rubinstein and Sarnak 1994] M. Rubinstein and P. Sarnak, "Chebyshev's bias", *Experiment. Math.* **3**:3 (1994), 173–197. MR 96d:11099 Zbl 0823.11050

[Rudnick and Sarnak 1996] Z. Rudnick and P. Sarnak, "Zeros of principal L-functions and random matrix theory", *Duke Math. J.* **81**:2 (1996), 269–322. MR 97f:11074 Zbl 0866.11050

[Shin and Templier 2012] S. W. Shin and N. Templier, "Sato–Tate theorem for families and low-lying zeros of automorphic L-functions", preprint, 2012. arXiv 1208.1945v2

[Yang 2009] A. Yang, *Distribution problems associated to zeta functions and invariant theory*, Ph.D. thesis, Princeton University, 2009, http://search.proquest.com/docview/304982142.

[Young 2005] M. P. Young, "Lower-order terms of the 1-level density of families of elliptic curves", *Int. Math. Res. Not.* **2005**:10 (2005), 587–633. MR 2006c:11076 Zbl 1071.11030

[Young 2006] M. P. Young, "Low-lying zeros of families of elliptic curves", *J. Amer. Math. Soc.* **19**:1 (2006), 205–250. MR 2006d:11072 Zbl 1086.11032

Communicated by Peter Sarnak
Received 2013-09-27 Revised 2014-04-02 Accepted 2014-05-24

fiorilli@umich.edu *Department of Mathematics, University of Michigan,*
530 Church Street, Ann Arbor, MI 48109, United States

sjm1@williams.edu *Mathematics and Statistics, Williams College, 18 Hoxsey St,*
Bronfman Science Center, Williamstown, MA 01267,
United States

ALGEBRA AND NUMBER THEORY 9:1 (2015)
dx.doi.org/10.2140/ant.2015.9.53

Eisenstein Hecke algebras and conjectures in Iwasawa theory

Preston Wake

We formulate a weak Gorenstein property for the Eisenstein component of the p-adic Hecke algebra associated to modular forms. We show that this weak Gorenstein property holds if and only if a weak form of Sharifi's conjecture and a weak form of Greenberg's conjecture hold.

1. Introduction

In this paper, we study the relationship between the Iwasawa theory of cyclotomic fields and certain ring-theoretic properties of the Hecke algebra acting on modular forms. This continues work started in our previous paper [Wake 2013].

The philosophy of our work is that simplicity of the Iwasawa theory should correspond to simplicity of Hecke algebras. This philosophy comes from remarkable conjectures formulated by Sharifi [2011].

In [Wake 2013], we showed, under some assumptions, that if the Hecke algebra for modular forms is Gorenstein, then the plus part of the corresponding ideal class group is zero. In particular, we gave an example to show that this Hecke algebra is not always Gorenstein.

Since the Hecke algebra is not always Gorenstein, it is natural to ask if there is a weaker ring-theoretic property that we can expect the Hecke algebra to have. In the present work, we formulate such a weaker property based on whether certain localizations of the Hecke algebra are Gorenstein. In a vague sense, we think of this condition as something like "the obstructions to Gorenstein-ness are finite".

We show that this weak Gorenstein property holds if and only if a weak form of Sharifi's conjecture and a weak form of Greenberg's conjecture both hold. In particular, the weak Gorenstein property holds in every known example.

We make a few remarks before stating our results more precisely.

Notation. In order to state our results more precisely, we introduce some notation, coinciding with that of [Wake 2013].

MSC2010: primary 11R23; secondary 11F33.

Keywords: Iwasawa theory, Hecke algebra, Gorenstein, Eisenstein, Sharifi's conjecture, Greenberg conjecture.

Let $p \geq 5$ be a prime, and let N be an integer such that $p \nmid \varphi(N)$ and $p \nmid N$. Let $\theta : (\mathbb{Z}/Np\mathbb{Z})^\times \to \overline{\mathbb{Q}}_p^\times$ be an even character and let $\chi = \omega^{-1}\theta$, where $\omega : (\mathbb{Z}/Np\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{Z}_p^\times$ denotes the Teichmüller character. We assume that θ satisfies the same conditions as in [Fukaya and Kato 2012] — namely that (1) θ is primitive, (2) if $\chi|_{(\mathbb{Z}/p\mathbb{Z})^\times} = 1$, then $\chi|_{(\mathbb{Z}/N\mathbb{Z})^\times}(p) \neq 1$, and (3) if $N = 1$, then $\theta \neq \omega^2$.

A subscript θ or χ will denote the eigenspace for that character for the $(\mathbb{Z}/Np\mathbb{Z})^\times$-action (see Section 1C).

Let $\Lambda = \mathbb{Z}_p[\![\mathbb{Z}_{p,N}^\times]\!]_\theta$ be the Iwasawa algebra, where $\mathbb{Z}_{p,N}^\times = \mathbb{Z}_p^\times \times (\mathbb{Z}/N\mathbb{Z})^\times$. Let $\mathfrak{m}_\Lambda$ be the maximal ideal of Λ.

Let $\mathfrak{H}$ (resp. $\mathfrak{h}$) be the θ-Eisenstein component of the Hecke algebra for Λ-adic modular forms (resp. cusp forms). Let $\mathcal{I}$ (resp. I) be the Eisenstein ideal of $\mathfrak{H}$ (resp. $\mathfrak{h}$), and let $I_{\mathfrak{H}} \supset \mathcal{I}$ be the preimage of I in $\mathfrak{H}$. Let H be the cohomology group on which $\mathfrak{h}$ acts (see Section 3A).

Let $\mathbb{Q}_\infty = \mathbb{Q}(\zeta_{Np^\infty})$; let M be the maximal abelian p-extension of $\mathbb{Q}_\infty$ unramified outside Np, and let L be the maximal abelian p-extension of $\mathbb{Q}_\infty$ unramified everywhere. Let $\mathfrak{X} = \mathrm{Gal}(M/\mathbb{Q}_\infty)$ and $X = \mathrm{Gal}(L/\mathbb{Q}_\infty)$.

1A. *Statement of results.*

1A1. *Weakly Gorenstein Hecke algebras.* We define what it means for the Hecke algebras $\mathfrak{h}$ and $\mathfrak{H}$ to be weakly Gorenstein. In the case of $\mathfrak{h}$, the definition comes from a condition that appears in work of Fukaya and Kato [2012, Section 7.2.10] on Sharifi's conjecture, and is related to a condition that appears in [Sharifi 2007].

Definition 1.1. We say that $\mathfrak{h}$ is *weakly Gorenstein* if $\mathfrak{h}_\mathfrak{p}$ is Gorenstein for every prime ideal $\mathfrak{p} \in \mathrm{Spec}(\mathfrak{h})$ of height 1 such that $I \subset \mathfrak{p}$.

We say that $\mathfrak{H}$ is *weakly Gorenstein* if $\mathfrak{H}_\mathfrak{p}$ is Gorenstein for every prime ideal $\mathfrak{p} \in \mathrm{Spec}(\mathfrak{H})$ of height 1 such that $I_{\mathfrak{H}} \subset \mathfrak{p}$.

In general, neither the algebra $\mathfrak{h}$ nor the algebra $\mathfrak{H}$ is Gorenstein. However, we conjecture that they are both weakly Gorenstein:

Conjecture 1.2. The Hecke algebras $\mathfrak{h}$ and $\mathfrak{H}$ are weakly Gorenstein.

1A2. *Relation to ideal class groups.* These ring-theoretic properties of Hecke algebras are related to ideal class groups via Sharifi's conjecture [2011]. Sharifi has constructed a map

$$\Upsilon : X_\chi(1) \to H^-/IH^-$$

which he conjectures to be an isomorphism.

A weaker conjecture is that Υ is a pseudoisomorphism — recall that a morphism of Λ-modules is called a pseudoisomorphism if its kernel and cokernel are both finite. If Υ is a pseudoisomorphism, then $\mathfrak{h}$ is weakly Gorenstein if and only X_χ

is pseudocyclic (see Section 5A below). We have the following analogous result for $\mathfrak{H}$. In the statement of the theorem, ξ_χ is a characteristic power series for $X_\chi(1)$ as a Λ-module.

Theorem 1.3. *Consider the following conditions*:

(1) $\mathfrak{H}$ *is weakly Gorenstein.*

(2) $\operatorname{coker}(\Upsilon)$ *is finite.*

(3) $X_\theta/\xi_\chi X_\theta$ *is finite.*

Condition (1) *holds if and only if conditions* (2) *and* (3) *both hold.*

Remark 1.4. Note that if $X_\chi = 0$, then all three conditions hold trivially. Indeed, if $X_\chi = 0$, then $\mathfrak{H} = \Lambda$, the domain and codomain of Υ are 0, and ξ_χ is a unit (see [Wake 2013, Remark 1.3]).

Remark 1.5. The conditions (2) and (3) are conjectured to hold in general (see Section 1B). In particular, they hold in all known examples.

Remark 1.6. Condition (2) is equivalent to the condition that Υ is an injective pseudoisomorphism (see Proposition 7.4).

Remark 1.7. Condition (3) is strange: ξ_χ is the opposite of the usual p-adic zeta function that is related to X_θ. That is, X_θ is annihilated by $\xi_{\chi^{-1}}$, and not (at least not for any obvious reason) by ξ_χ.

The proof of Theorem 1.3 will be given in Section 7.

1A3. *Strong and weak versions of Sharifi's conjecture.* One consequence of Sharifi's conjecture is that $X_\chi(1) \cong H^-/IH^-$ as Λ-modules. Since X_χ has no p-torsion, this would imply that H^-/IH^- has no p-torsion, which Sharifi [2011, Remark, p. 51] explicitly conjectured.

A theorem of Ohta implies that if $\mathfrak{H}$ is Gorenstein, then $X_\chi(1) \cong H^-/IH^-$ (see Theorem 5.11 below). Moreover, Ohta also proves that $\mathfrak{H}$ is Gorenstein under a certain hypothesis ([Ohta 2007, Theorem I], for example). Sharifi [2011, Proposition 4.10] used this as evidence for his conjecture.

Since it is now known that $\mathfrak{H}$ is not always Gorenstein [Wake 2013, Corollary 1.4], one may wonder if Sharifi's conjecture should be weakened to the statement "Υ is a pseudoisomorphism" (see Conjecture 4.2 below). Fukaya and Kato [2012] have partial results on this version of the conjecture. When neither $\mathfrak{h}$ nor $\mathfrak{H}$ is Gorenstein, we know of no evidence for Sharifi's conjecture that Υ is an isomorphism (and not just a pseudoisomorphism); we hope that our next result can be used to provide evidence. This result concerns a module $H^-/I\widetilde{H}^-_{\mathrm{DM}}$. As explained in Section 5, $H^-/I\widetilde{H}^-_{\mathrm{DM}}$ measures how much the ring $\mathfrak{H}$ is "not Gorenstein".

For a finitely generated Λ-module M, let

$$d_{\mathfrak{m}_\Lambda}(M) = \dim_{\Lambda/\mathfrak{m}_\Lambda}(M/\mathfrak{m}_\Lambda M).$$

Note that $d_{\mathfrak{m}_\Lambda}(M)$ is the minimal number of generators of M as a Λ-module.

Theorem 1.8. *Assume that $X_\theta \neq 0$ and that $\mathfrak{h}$ is weakly Gorenstein. Then we have*

$$d_{\mathfrak{m}_\Lambda}(H^-/I\widetilde{H}^-_{\mathrm{DM}}) \geq d_{\mathfrak{m}_\Lambda}(X_\chi),$$

with equality if and only if Υ is an isomorphism.

If, in addition, $\#(X_\theta) = \#(\Lambda/\mathfrak{m}_\Lambda)$, then Υ is an isomorphism if and only if

$$\#(H^-/I\widetilde{H}^-_{\mathrm{DM}}) = \#(\Lambda/\mathfrak{m}_\Lambda)^{d_{\mathfrak{m}_\Lambda}(X_\chi)}.$$

This theorem may be used to provide evidence for Sharifi's conjecture that Υ is an isomorphism in two ways. The first way is philosophical: although the ring $\mathfrak{H}$ is not always Gorenstein, we may like to believe that $\mathfrak{H}$ is "as close to being Gorenstein as possible". This translates to the belief that $H^-/I\widetilde{H}^-_{\mathrm{DM}}$ is as small as possible; the theorem says that $H^-/I\widetilde{H}^-_{\mathrm{DM}}$ is smallest when Υ is an isomorphism.

The second way is a method for providing computational evidence: Theorem 1.8 may allow one to compute examples where Υ is an isomorphism but where $\mathfrak{H}$ is not Gorenstein. We now outline a scheme for doing this. First, one finds an imaginary quadratic field with noncyclic p-class group; this provides a character χ of order 2 such that $X_\theta \neq 0$ and such that $\mathfrak{H}$ is not Gorenstein (see [Wake 2013, Corollary 1.4]). However, $\mathfrak{h}$ will be weakly Gorenstein by Lemma 5.8 below (or else we have found a counterexample to a famous conjecture!). The assumptions for Theorem 1.8 are then satisfied. Then, if one can compute $H^-/I\widetilde{H}^-_{\mathrm{DM}}$ and X_χ sufficiently well, one can verify that $d_{\mathfrak{m}_\Lambda}(H^-/I\widetilde{H}^-_{\mathrm{DM}}) = d_{\mathfrak{m}_\Lambda}(X_\chi)$.

The proof of Theorem 1.8 will be given in Section 8.

1B. *Relation to known results and conjectures.*

Our results are related to previous results and conjectures of various authors, including Fukaya and Kato, Greenberg, Ohta, Sharifi, Skinner and Wiles and the present author. In the main text, we try to survey these results and conjectures. However, since this is an area with many conjectures, and many of the results are about the interrelation of the conjectures or proofs of special cases of the conjectures, the reader may find it difficult to see what is known, what is unknown, and what exactly is conjectured.

In this section, we try to write down the conjectures and results in a compact but clear fashion. This involves creating an unorthodox naming convention, which we hope will aid in understanding the connections between the statements. The reader may wish to skip this section, and use it as a reference when reading the main text.

1B1. *Naming convention.* We use C(Y) to denote a conjecture about Y, Q(Y) to denote a question about Y (a statement that is not conjectured to be true or false), and A(Y) to denote an assumption about Y (a statement that is *known* to be false in general).

Numbered statement are listed in increasing order of logical strength. For example, Q(Y II) is a questionable statement about Y that implies C(Y I), a conjectural statement about Y.

1B2. *Finiteness conditions.* We consider the following statements about finiteness and cyclicity of class groups:

C(Fin I): $X_\theta/\xi_\chi X_\theta$ is finite.
C(Fin II): X_θ is finite.
A(Fin III): $X_\theta = 0$.
A(Fin IV): $\mathfrak{X}_\theta = 0$.
C(Cyc I): $\mathfrak{X}_\theta \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is cyclic as a $\Lambda \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$-module.
A(Cyc II): $\mathfrak{X}_\theta$ is cyclic as a Λ-module.
C(Cyc’ I): $X_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is cyclic as a $\mathbb{Z}_p[\![\mathbb{Z}_{p,N}^\times]\!]_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$-module.
A(Cyc’ II): X_χ is cyclic as a $\mathbb{Z}_p[\![\mathbb{Z}_{p,N}^\times]\!]_\chi$-module.

There are implications A(Fin III) $\implies$ A(Cyc II) and C(Fin II) $\implies$ C(Cyc I). In the case $N = 1$, A(Fin III) is actually a conjecture, known as the Kummer–Vandiver conjecture. The conjectures C(Fin II), C(Cyc I) and C(Cyc’ I) are due to Greenberg [2001, Conjecture 3.5]. Note that there is no relation between the conjectures C(Cyc’ I) and C(Cyc I) for our fixed choices of χ and θ (the modules are *not* adjoint — see Proposition 2.2).

As far as we know, the conjecture C(Fin I) has never been considered before.

1B3. *Gorenstein conditions.* We consider the following statements about Hecke algebras:

C($\mathfrak{h}$ I): $\mathfrak{h}$ is weakly Gorenstein.
A($\mathfrak{h}$ II): $\mathfrak{h}$ is Gorenstein.
C($\mathfrak{H}$ I): $\mathfrak{H}$ is weakly Gorenstein.
A($\mathfrak{H}$ II): $\mathfrak{H}$ is Gorenstein.

The fact that $\mathfrak{h}$ is not always Gorenstein is can be deduced from results of Ohta (following ideas of Kurihara [1993] and Harder and Pink [1992], who considered the case $N = 1$). Ohta ([2007, Corollary 4.2.13], for example) proved the implication A($\mathfrak{h}$ II) $\implies$ A(Cyc’ II).

The fact that $\mathfrak{H}$ is not always Gorenstein is [Wake 2013, Corollary 1.4]. The weakly Gorenstein conjectures are ours (although this paper shows that they are the consequence of conjectures by other authors).

1B4. *Conjectures of Sharifi type.* We consider the following versions of Sharifi's conjecture. They concern maps ϖ and Υ that were defined by Sharifi.

C(Υ I): coker(Υ) is finite.
C(Υ II): Υ is an isomorphism.
C(S. I): The maps Υ and ϖ are pseudoisomorphisms.
C(S. II): The maps Υ and ϖ are inverse isomorphisms modulo torsion.
C(S. III): The maps Υ and ϖ are inverse isomorphisms.

Note that C(S. I) implies C(Υ I), and C(S. III) is equivalent to C(S. II) + C(Υ II).

See [Sharifi 2011, Conjectures 4.12, 5.2 and 5.4] for the original statements of the conjecture and [Fukaya and Kato 2012, Section 7.1] for some modified statements.

1B5. *A question about zeta functions.* We consider the following statement about p-adic zeta functions, which appears in [Fukaya and Kato 2012]:

Q(ξ): The factorization of ξ_χ in Λ has no prime element occurring with multiplicity > 1.

This statement holds in every known example (see [Greenberg 2001, p. 12]). It is the author's impression that this statement is believed to hold in general, but that there is not enough evidence to call it a conjecture.

1B6. *Relations between the conditions.* Fukaya and Kato have recently made progress towards Sharifi's conjecture. They showed the implications C($\mathfrak{h}$ I) $\Longrightarrow$ C(S. I) and Q(ξ) $\Longrightarrow$ C(S. II) [2012, Theorem 7.2.6]. They also show that if Q(ξ) and at least one of A($\mathfrak{h}$ II) or A($\mathfrak{H}$ II) hold, then C(S. III) holds [2012, Corollary 7.2.7]. Moreover, it can be shown that, if C(Υ I), then C(Cyc' I) is equivalent to C($\mathfrak{h}$ I) (cf. Section 5.1 below). Therefore, their results imply that C($\mathfrak{h}$ I) is equivalent to C(S. I) + C(Cyc' I).

Sharifi [2011, Proposition 4.10], using [Ohta 2003], has shown that A($\mathfrak{H}$ II) $\Longrightarrow$ C(Υ II). As far as we know, there are no results on C(S. III) when neither A($\mathfrak{h}$ II) nor A($\mathfrak{H}$ II) hold.

Ohta [2003] has also shown that A(Fin IV) $\Longrightarrow$ A($\mathfrak{H}$ II). Similar results were obtained by Skinner and Wiles [1997] by a different method.

In our previous work [Wake 2013], we showed that C(Υ II) and A(Fin III) together imply A($\mathfrak{H}$ II), and moreover that if $X_\chi \neq 0$, then A($\mathfrak{H}$ II) implies A(Fin III).

The main result of this paper is that C($\mathfrak{H}$ I) is equivalent to C(Υ I)+C(Fin I).

1C. ***Conventions.*** If $\phi : G \to \overline{\mathbb{Q}}_p^\times$ is a character of a group G, we let $\mathbb{Z}_p[\phi]$ denote the $\mathbb{Z}_p$-algebra generated by the values of ϕ, on which G acts through ϕ. If M is a $\mathbb{Z}_p[G]$-module, denote by M_ϕ the ϕ-eigenspace:

$$M_\phi = M \otimes_{\mathbb{Z}_p[G]} \mathbb{Z}_p[\phi].$$

For a field K, let $G_K = \mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group. For a $G_{\mathbb{Q}}$-module M, let M^+ and M^- denote the eigenspaces of complex conjugation.

We fix a system of primitive Np^r-th roots of unity (ζ_{Np^r}) with the property that $\zeta_{Np^{r+1}}^p = \zeta_{Np^r}$.

2. Conjectures in Iwasawa theory

2A. ***Iwasawa theory of cyclotomic fields.*** We review some important results from the classical Iwasawa theory of cyclotomic fields. Nice references for this material include [Greenberg 2001], [Greither 1992], and [Washington 1997].

2A1. *Class groups and Galois groups.* The main object of study is the inverse limit of the p-power torsion part of the ideal class group $\mathrm{Cl}(\mathbb{Q}(\zeta_{Np^r}))$. By class field theory, there is an isomorphism

$$X \cong \varprojlim \mathrm{Cl}(\mathbb{Q}(\zeta_{Np^r}))\{p\},$$

where, as in the introduction, $X = \mathrm{Gal}(L/\mathbb{Q}_\infty)$ with L the maximal abelian pro-p-extension of $\mathbb{Q}_\infty$ unramified everywhere, and where $(-)\{p\}$ denotes the p-Sylow subgroup.

A closely related object is $\mathfrak{X} = \mathrm{Gal}(M/\mathbb{Q}_\infty)$, where M is the maximal abelian pro-p-extension of $\mathbb{Q}_\infty$ unramified outside Np. We will explain the relation between X and $\mathfrak{X}$ below.

2A2. *Iwasawa algebra.* The natural action of $\mathrm{Gal}(\mathbb{Q}(\zeta_{Np^r})/\mathbb{Q})$ on $\mathrm{Cl}(\mathbb{Q}(\zeta_{Np^r}))\{p\}$ makes X a module over the group ring $\varprojlim \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_{Np^r})/\mathbb{Q})]$.

We fix a choice of isomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_{Np^r})/\mathbb{Q}) \cong (\mathbb{Z}/Np^r\mathbb{Z})^\times$, and this induces an isomorphism $\varprojlim \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_{Np^r})/\mathbb{Q})] \cong \mathbb{Z}_p[\![\mathbb{Z}_{p,N}^\times]\!]$, where we define $\mathbb{Z}_{p,N}^\times = \mathbb{Z}_p^\times \times (\mathbb{Z}/N\mathbb{Z})^\times$. Note that the surjection $\mathbb{Z}_{p,N}^\times \to (\mathbb{Z}/Np\mathbb{Z})^\times$ splits canonically. We use this to identify $\mathbb{Z}_{p,N}^\times$ with $\Gamma \times (\mathbb{Z}/Np\mathbb{Z})^\times$, where Γ is the torsion-free part of $\mathbb{Z}_{p,N}^\times$ (note that $\Gamma \cong \mathbb{Z}_p$).

The ring $\mathbb{Z}_p[\![\mathbb{Z}_{p,N}^\times]\!]$ is, in general, a product of rings. To simplify things, we consider only a particular eigenspace for the action of the torsion subgroup $(\mathbb{Z}/Np\mathbb{Z})^\times$ of $\mathbb{Z}_{p,N}^\times$. We define $\Lambda = \mathbb{Z}_p[\![\mathbb{Z}_{p,N}^\times]\!]_\theta$. There are isomorphisms $\Lambda \cong \mathcal{O}[\![\Gamma]\!] \cong \mathcal{O}[\![T]\!]$, where $\mathcal{O}$ is the $\mathbb{Z}_p$-algebra generated by the values of θ. Note that $\mathcal{O}$ is the valuation ring of a finite extension of $\mathbb{Q}_p$, and so Λ is a noetherian regular local ring of dimension 2 with finite residue field.

2A3. *The operators τ and ι.* We introduce two operations ι and τ on the rings $\mathbb{Z}_p[\![\mathbb{Z}_{p,N}^\times]\!]$ and Λ, and related functors $M \mapsto M^\#$ and $M \mapsto M(r)$. This is a technical part, and the reader may wish to ignore any instance of these on a first reading.

Let $\iota\colon \mathbb{Z}_p[\![\mathbb{Z}_{p,N}^\times]\!] \to \mathbb{Z}_p[\![\mathbb{Z}_{p,N}^\times]\!]$ by the involution given by $c \mapsto c^{-1}$ on $\mathbb{Z}_{p,N}^\times$. Let $\tau : \mathbb{Z}_p[\![\mathbb{Z}_{p,N}^\times]\!] \to \mathbb{Z}_p[\![\mathbb{Z}_{p,N}^\times]\!]$ be the morphism induced by $[c] \mapsto \bar{c}[c]$ for $c \in \mathbb{Z}_{p,N}^\times$, where $[c] \in \mathbb{Z}_p[\![\mathbb{Z}_{p,N}^\times]\!]$ is the group element and where $\bar{c} \in \mathbb{Z}_p^\times$ is the projection of c.

Note that ι and τ do not commute, but $\iota\tau = \tau^{-1}\iota$. In particular, $\tau^r\iota$ is an involution for any $r \in \mathbb{Z}$.

For a $\mathbb{Z}_p[\![\mathbb{Z}_{p,N}^\times]\!]$-module M, we let $M^\#$ (resp. $M(r)$) be the same abelian group, with $\mathbb{Z}_p[\![\mathbb{Z}_{p,N}^\times]\!]$-action changed by ι (resp. τ^r). Note that the functors $M \mapsto M^\#$ and $M \mapsto M(r)$ are exact.

2A4. *p-adic zeta functions and characteristic ideals.* We define $\xi_{\chi^{-1}}, \xi_\chi \in \Lambda$ to be generators of the principal ideals $\mathrm{Char}_\Lambda(X_{\chi^{-1}}^\#(1))$ and $\mathrm{Char}_\Lambda(X_\chi(1))$ respectively (see the Appendix for a review of characteristic ideals).

The Iwasawa main conjecture (now a theorem of Mazur and Wiles [1984]) states that (a certain choice of) $\xi_{\chi^{-1}}$ and ξ_χ can be constructed by p-adically interpolating values of Dirichlet L-functions.

Remark 2.1. In [Wake 2013], we viewed X_χ and $X_{\chi^{-1}}$ as Λ-modules via the isomorphisms

$$\tau : \mathbb{Z}_p[\![\mathbb{Z}_{p,N}^\times]\!]_\chi \xrightarrow{\sim} \Lambda, \quad \iota\tau : \mathbb{Z}_p[\![\mathbb{Z}_{p,N}^\times]\!]_{\chi^{-1}} \xrightarrow{\sim} \Lambda.$$

We learned from the referee that this is an unusual choice of notation, and so we have adopted the above convention, which we learned is more standard.

The element ξ of [Wake 2013] is the ξ_χ of this paper. However, the element denoted $\xi_{\chi^{-1}}$ in that paper would be denoted $\iota\tau\xi_{\chi^{-1}}$ in this paper. We hope this doesn't cause confusion.

2A5. *Adjoints.* For a finitely generated Λ-module M, let $\mathrm{E}^i(M) = \mathrm{Ext}^i_\Lambda(M, \Lambda)$. These are called the (*generalized*) *Iwasawa adjoints* of M.

This theory is important to us because of the following fact, which is well-known to experts.

Proposition 2.2. *The $\mathbb{Z}_p[\![\mathbb{Z}_{p,N}^\times]\!]$-modules $X_{\chi^{-1}}$ and $\mathfrak{X}_\theta$ are both torsion and have no nonzero finite submodule, and we have*

$$\mathfrak{X}_\theta \cong \mathrm{E}^1(X_{\chi^{-1}}(-1)).$$

In particular, we have $\mathrm{Char}_\Lambda(\mathfrak{X}_\theta) = (\xi_{\chi^{-1}})$ *as ideals in* Λ.

Proof. The first sentence is explained in [Wake 2013, Corollary 4.4]. The second sentence follows from the fact that for any finitely generated, torsion Λ-module M, there is a pseudoisomorphism $E^1(M) \to M^\#$ [Neukirch et al. 2008, Proposition 5.5.13, p. 319]. Since $\mathrm{Char}_\Lambda(-)$ is a pseudoisomorphism invariant, we have

$$\mathrm{Char}_\Lambda\big(\mathrm{E}^1(X_{\chi^{-1}}(-1))\big) = \mathrm{Char}_\Lambda\big((X_{\chi^{-1}}(-1))^\#\big) = \mathrm{Char}_\Lambda\big(X_{\chi^{-1}}^\#(1)\big) = (\xi_{\chi^{-1}}),$$

and so the second sentence follows from the first. □

2A6. *Exact sequence.* There is an exact sequence

$$\Lambda/\xi_{\chi^{-1}} \longrightarrow \mathfrak{X}_\theta \longrightarrow X_\theta \longrightarrow 0, \tag{2-3}$$

coming from class field theory and Coleman power series (see, e.g., [Wake 2013, Sections 3 and 5]). From Proposition 2.2 and the fact that $\Lambda/\xi_{\chi^{-1}}$ has no finite submodule, we can see that X_θ is finite (resp. zero) if and only if the leftmost arrow in (2-3) is injective (resp. an isomorphism).

2B. *Finiteness and cyclicity of class groups.*

We discuss some statements of finiteness and cyclicity of ideal class groups.

2B1. *Kummer–Vandiver conjecture.* We first consider the case $N = 1$.

Conjecture 2.4 (Kummer–Vandiver). Assume $N = 1$. Then $X^+ = 0$.

Lemma 2.5. *Assume $N = 1$. If* Conjecture 2.4 *is true, then $\mathfrak{X}_\theta$ and $X_{\chi^{-1}}$ are cyclic.*

Proof. If $X_\theta = 0$, we see from (2-3) that $\mathfrak{X}_\theta$ is cyclic. We wish to show that $X_{\chi^{-1}}$ is cyclic. It is enough to show that $X_{\chi^{-1}}(-1)$ is cyclic, and we claim that this follows from the fact that $\mathfrak{X}_\theta$ is cyclic by Proposition 2.2 and standard arguments from [Neukirch et al. 2008]. Indeed, we have isomorphisms

$$X_{\chi^{-1}}(-1) \cong \mathrm{E}^1\big(\mathrm{E}^1(X_{\chi^{-1}}(-1))\big) \cong \mathrm{E}^1(\mathfrak{X}_\theta)$$

coming from [Neukirch et al. 2008, Proposition 5.5.8(iv), p. 316] and Proposition 2.2, respectively. So it is enough to show that $\mathrm{E}^1(\mathfrak{X}_\theta)$ is cyclic whenever $\mathfrak{X}_\theta$ is. But this is clear from [Neukirch et al. 2008, Proposition 5.5.3(iv), p. 313], which says that the projective dimension of $\mathfrak{X}_\theta$ is 1; if $\mathfrak{X}_\theta$ is generated by one element, then there is exactly one relation, and the dual of the resulting presentation gives a cyclic presentation of $\mathrm{E}^1(\mathfrak{X}_\theta)$. □

2B2. *Greenberg's conjecture.* For general $N > 1$, there are examples where X_χ is not cyclic, and so X^+ is not always zero. However, it may still be true that X^+ is finite:

Conjecture 2.6 [Greenberg 2001, Conjecture 3.4]. The module X^+ is finite.

The following lemma may be proved in the same manner as Lemma 2.5:

Lemma 2.7. *The following are equivalent*:

(1) *X_θ is finite.*

(2) *The map $\Lambda/\xi_{\chi^{-1}} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \to \mathfrak{X}_\theta \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ induced by the map in* (2-3) *is an isomorphism.*

3. Hecke algebras and modular forms

In this section, we introduce Hecke algebras for modular forms to the story.

3A. ***Hecke algebras and Eisenstein ideals.*** We introduce the objects from the theory of modular forms that we will need. See [Wake 2014] for a more detailed treatment of this theory.

3A1. *Modular curves and Hecke operators.* Let $Y_1(Np^r)/\mathbb{Q}$ be the moduli space for pairs (E, P), where $E/\mathbb{Q}$ is an elliptic curve and $P \in E$ is a point of order Np^r. Let $X_1(Np^r)/\mathbb{Q}$ be the compactification of $Y_1(Np^r)$ obtained by adding cusps.

There is an action of $(\mathbb{Z}/Np^r\mathbb{Z})^\times$ on $Y_1(Np^r)$, where $a \in (\mathbb{Z}/Np^r\mathbb{Z})^\times$ acts by $a(E, P) = (E, aP)$. This is called the action of diamond operators $\langle a\rangle$. There are also Hecke correspondences $T^*(n)$ on $Y_1(Np^r)$ and $X_1(Np^r)$. We consider these as endomorphisms of the cohomology.

We define the Hecke algebra of $Y_1(Np^r)$ to be the algebra generated by the $T^*(n)$ for all integers n and the $\langle a\rangle$ for all $a \in (\mathbb{Z}/Np^r\mathbb{Z})^\times$. We define the Eisenstein ideal to be the ideal of the Hecke algebra generated by $1 - T^*(l)$ for all primes $l \mid Np$ and by $1 - T^*(l) + l\langle l\rangle^{-1}$ for all primes $l \nmid Np$.

3A2. *Ordinary cohomology.* Let

$$H' = \varprojlim H^1(\overline{X}_1(Np^r), \mathbb{Z}_p)^{\mathrm{ord}}_\theta$$

and

$$\widetilde{H}' = \varprojlim H^1(\overline{Y}_1(Np^r), \mathbb{Z}_p)^{\mathrm{ord}}_\theta,$$

where the superscript "ord" denotes the ordinary part for the dual Hecke operator $T^*(p)$, and the subscript refers to the eigenspace for the diamond operators.

3A3. *Eisenstein parts.* Let $\mathfrak{h}'$ and $\mathfrak{H}'$ be the algebras of dual Hecke operators acting on H' and $\widetilde{H}'$, respectively. Let I and $\mathcal{I}$ be the Eisenstein ideals of $\mathfrak{h}'$ and $\mathfrak{H}'$. Let $\mathfrak{H}$ denote the *Eisenstein component* $\mathfrak{H} = \mathfrak{H}'_{\mathfrak{m}}$, the localization at the unique maximal ideal $\mathfrak{m}$ containing $\mathcal{I}$. We can define the Eisenstein component $\mathfrak{h}$ of $\mathfrak{h}'$ analogously. Let $\widetilde{H} = \widetilde{H}' \otimes_{\mathfrak{H}'} \mathfrak{H}$ and $H = H' \otimes_{\mathfrak{h}'} \mathfrak{h}$ be the Eisenstein components.

There is a natural surjection $\mathfrak{H} \twoheadrightarrow \mathfrak{h}$ by restriction. Let $I_{\mathfrak{H}} \subset \mathfrak{H}$ be the kernel of the composite map $\mathfrak{H} \twoheadrightarrow \mathfrak{h} \twoheadrightarrow \mathfrak{h}/I$. Note that $\mathcal{I} \subsetneq I_{\mathfrak{H}}$.

3B. ***Properties of the Hecke modules.*** We first recall some properties of the Hecke modules $\widetilde{H}$ and H and Hecke algebras $\mathfrak{H}$ and $\mathfrak{h}$. See [Fukaya and Kato 2012, Section 6] for a simple and self-contained exposition of this.

3B1. *Control theorem.* There are natural maps $\Lambda \to \mathfrak{h}$ and $\Lambda \to \mathfrak{H}$ given by diamond operators. It is a theorem of Hida that these maps are finite and flat. In particular, $\mathfrak{h}$ and $\mathfrak{H}$ are noetherian local rings of dimension 2 with (the same) finite residue field.

Let $\mathfrak{h}^\vee$ (resp. $\mathfrak{H}^\vee$) denote the $\mathfrak{h}$-module (resp. $\mathfrak{H}$-module) $\mathrm{Hom}_\Lambda(\mathfrak{h}, \Lambda)$ (resp. $\mathrm{Hom}_\Lambda(\mathfrak{H}, \Lambda)$). We will call these the *dualizing modules* for the respective algebras.

3B2. *Eichler–Shimura isomorphisms.* Ohta ([2007, Section 4.2], for example) has proven theorems on the Hecke module structure of $\widetilde{H}$ and H. See [Wake 2014] for a different approach. The main result we need is the following, which appears in this form in [Fukaya and Kato 2012, Section 6.3]:

Theorem 3.1. *There are isomorphisms of Hecke-modules $H^+ \cong \mathfrak{h}$, $H^- \cong \mathfrak{h}^\vee$ and $\widetilde{H}^- \cong \mathfrak{H}^\vee$.*

3B3. *Boundary at the cusps.* The cokernel of the natural map $H \to \widetilde{H}$ is described as the boundary at cusps. Ohta [2003, Theorem 1.5.5] has shown that the module of cusps is free of rank one as a Λ-module. That is, there is an exact sequence of $\mathfrak{H}$-modules

$$0 \longrightarrow H \longrightarrow \widetilde{H} \longrightarrow \Lambda \longrightarrow 0.$$

Moreover, there is a canonical element $\{0, \infty\} \in \widetilde{H}$ that gives a generator of $\widetilde{H}/H$. This is proven in [Sharifi 2011, Lemma 4.8], following [Ohta 2003, Theorem 2.3.6] (cf. [Fukaya and Kato 2012, Section 6.2.5]).

3B4. *Relation between Hecke and Iwasawa algebras.* The following is a consequence of the Iwasawa main conjecture. See [Fukaya et al. 2014, Section 2.5.3] for a nice explanation.

Proposition 3.2. *The natural inclusions $\Lambda \to \mathfrak{H}$ and $\Lambda \to \mathfrak{h}$ induce isomorphisms*

$$\Lambda \xrightarrow{\sim} \mathfrak{H}/\mathcal{I} \quad \text{and} \quad \Lambda/\xi_\chi \xrightarrow{\sim} \mathfrak{h}/I.$$

3B5. *Drinfeld–Manin modification.* Let $\widetilde{H}_{\mathrm{DM}} = \widetilde{H} \otimes_{\mathfrak{H}} \mathfrak{h}$. By the previous two paragraphs, there is an exact sequence of $\mathfrak{h}$-modules

$$0 \longrightarrow H \longrightarrow \widetilde{H}_{\mathrm{DM}} \longrightarrow \Lambda/\xi_\chi \longrightarrow 0.$$

By abuse of notation, we let $\{0, \infty\} \in \widetilde{H}_{\mathrm{DM}}$ be the image of $\{0, \infty\} \in \widetilde{H}$.

4. Sharifi's conjecture

In this section, we will discuss some remarkable conjectures that were formulated by Sharifi [2011]. Sharifi gave a conjectural construction of a map

$$\varpi : H^-/IH^- \to X_\chi(1),$$

and constructed a map

$$\Upsilon : X_\chi(1) \to H^-/IH^-.$$

Conjecture 4.1 (Sharifi). The maps Υ and ϖ are inverse isomorphisms.

We refer to [Sharifi 2011] and [Fukaya and Kato 2012] for the original constructions, and [Fukaya et al. 2014] for a nice survey of the known results. There is also the following weaker version, which appears as [Fukaya and Kato 2012, Conjecture 7.1.2]. It allows for the possibility that the p-torsion part (tor) of H^-/IH^- is nonzero (note that Conjecture 4.1 implies that (tor) $= 0$, and that Sharifi [2011, Remark, p. 51] specifically notes this).

Conjecture 4.2. The maps Υ and ϖ are inverses up to torsion. That is, $\Upsilon \circ \varpi$ is the identity map on $(H^-/IH^-)/(\mathrm{tor})$ and $\varpi \circ \Upsilon$ is the identity map on $X_\chi(1)$.

The following is [Fukaya and Kato 2012, Theorem 7.2.6(2)]. This result is not needed in the remainder of the paper, except to say that Conjecture 4.2 holds in every known example.

Theorem 4.3. *If ξ_χ has no multiple roots, then* Conjecture 4.2 *is true. In particular, if ξ_χ has no multiple roots and H^-/IH^- has no nonzero finite submodule, then* Conjecture 4.1 *is true.*

The paper [Fukaya and Kato 2012] also has results on Sharifi's conjecture when $H^-/IH^- \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is generated by one element. This is related to Gorenstein conditions on Hecke algebras, the subject of the next section.

5. Gorenstein Hecke algebras

In this section we discuss to what extent the Hecke algebras $\mathfrak{h}$ and $\mathfrak{H}$ are Gorenstein. The relevant characterization of being Gorenstein is the following:

Definition 5.1. Let k be a regular local ring, and let $k \to R$ be a finite, flat ring homomorphism. Then R is *Gorenstein* if $\mathrm{Hom}_k(R, k)$ is a free R-module of rank 1.

This definition is seen to be equivalent to the usual one from homological algebra, but is more useful for our purposes. In our applications we will take $k = \Lambda$ and $R = \mathfrak{h}$, $\mathfrak{H}$ or their localizations. Asking whether $\mathfrak{h}$ or $\mathfrak{H}$ is Gorenstein is the same as asking whether $\mathfrak{h}^\vee$ or $\mathfrak{H}^\vee$ is free of rank 1. This is relevant in light of Theorem 3.1.

5A. *Conditions on* $\mathfrak{h}$.

We consider under what conditions $\mathfrak{h}$ is Gorenstein or weakly Gorenstein.

5A1. *Gorenstein.* The following lemma is explained in [Fukaya and Kato 2012, Section 7.2.12]:

Lemma 5.2. *The following are equivalent*:

(1) $\mathfrak{h}$ *is Gorenstein.*

(2) H^-/IH^- *is cyclic as an* $\mathfrak{h}$*-module.*

(3) H^-/IH^- *is a free* $\mathfrak{h}/I$*-module of rank* 1.

Proof. This follows from the fact that $H^- \cong \mathfrak{h}^\vee$, that $\mathfrak{h}^\vee$ is a faithful $\mathfrak{h}$-module, and Nakayama's lemma. □

One may ask whether $\mathfrak{h}$ is always Gorenstein. The following result is based on ideas of Kurihara [1993] and Harder and Pink [1992], who proved it in the case $N = 1$. The result in this form was proven by Ohta.

Theorem 5.3. *Suppose that $\mathfrak{h}$ is Gorenstein. Then $X_\chi(1)$ is cyclic as a Λ-module.*

Proof. This is proven, for example, in [Ohta 2007, Corollary 4.2.13], where it is the implication "(ii) $\Longrightarrow$ (i)". Note that the proof of "(ii) $\Longrightarrow$ (i)" given there does not require the assumption that $\mathfrak{H}$ is Gorenstein. □

As remarked in Section 2B2, there are examples where X_χ is not cyclic and therefore where $\mathfrak{h}$ is not Gorenstein. One could also ask if the converse holds.

Lemma 5.4. *Suppose that $H^-/IH^- \cong X_\chi(1)$. Then $\mathfrak{h}$ is Gorenstein if and only if $X_\chi(1)$ is cyclic as a Λ-module.*

Proof. This follows from Lemma 5.2. □

In particular, we have the following:

Corollary 5.5. *Assume $N = 1$, and assume Sharifi's conjecture* (Conjecture 4.1) *and the Kummer–Vandiver theorem* (Conjecture 2.4). *Then $\mathfrak{h}$ is Gorenstein.*

5A2. *Weakly Gorenstein.* We recall that $\mathfrak{h}$ is said to be *weakly Gorenstein* if $\mathfrak{h}_\mathfrak{p}$ is Gorenstein for every prime ideal $\mathfrak{p} \in \operatorname{Spec}(\mathfrak{h})$ of height 1 such that $I \subset \mathfrak{p}$. This definition is relevant in light of the following lemma:

Lemma 5.6 [Fukaya and Kato 2012, Section 7.2.10]. *The following are equivalent*:

(1) *$\mathfrak{h}$ is weakly Gorenstein.*

(2) *$(H^-/IH^-) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is cyclic as an $\mathfrak{h}/I \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$-module.*

(3) *$(H^-/IH^-) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is a free $\mathfrak{h}/I \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$-module of rank* 1.

The following result on Sharifi's conjecture assumes that $\mathfrak{h}$ is weakly Gorenstein:

Theorem 5.7 [Fukaya and Kato 2012, Theorem 7.2.8(1)]. *Assume that $\mathfrak{h}$ is weakly Gorenstein. Then $\Upsilon \colon X_\chi(1) \to (H^-/IH^-)/(\mathrm{tor})$ and $\varpi \colon (H^-/IH^-)/(\mathrm{tor}) \to X_\chi(1)$ are isomorphisms.*

Their work also implies the following result on the converse:

Lemma 5.8. *Assume that* $\operatorname{coker}(\Upsilon)$ *is finite and that $X_\chi(1) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is cyclic. Then $\mathfrak{h}$ is weakly Gorenstein.*

Proof. If $\operatorname{coker}(\Upsilon)$ is finite, then $\Upsilon : X_\chi(1) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \to (H^-/IH^-) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is surjective, so this follows from Lemma 5.6. □

Since this lemma applies whenever Conjecture 4.2 and Conjecture 2.6 hold, we should conjecture that $\mathfrak{h}$ is always weakly Gorenstein:

Conjecture 5.9. The ring $\mathfrak{h}$ is weakly Gorenstein.

5B. ***Conditions on $\mathfrak{H}$.*** We consider under what conditions $\mathfrak{H}$ is Gorenstein or weakly Gorenstein.

5B1. *Gorenstein.* Recall that $\widetilde{H}^-_{\mathrm{DM}}/H^- \cong \mathfrak{h}/I$. In particular, the natural inclusion $I\widetilde{H}^-_{\mathrm{DM}} \subset \widetilde{H}^-_{\mathrm{DM}}$ lands in H^-. The following proposition is proven in [Wake 2013]. It can also be proven along the same lines as the proof of Proposition 5.13.

Proposition 5.10. *The following are equivalent*:

(1) *$\mathfrak{H}$ is Gorenstein.*

(2) *$\widetilde{H}^-_{\mathrm{DM}}$ is a free $\mathfrak{h}$-module of rank* 1.

(3) *$I\widetilde{H}^-_{\mathrm{DM}} = H^-$.*

It was proven by Ohta [2007, Theorem I] that $\mathfrak{H}$ is Gorenstein if $\mathfrak{X}_\theta = 0$. Similar results were obtained earlier by Skinner and Wiles [1997].

The following theorem illustrates the importance of the condition that $\mathfrak{H}$ is Gorenstein. It was first proven by Sharifi, following [Ohta 2003].

Theorem 5.11. *Suppose that $\mathfrak{H}$ is Gorenstein. Then Υ is an isomorphism.*

Proof. This is proven in [Sharifi 2011, Proposition 4.10], where the assumption "$p \nmid B_{1,\theta^{-1}}$" is not needed in the proof — all that is needed is the weaker assumption that $\mathfrak{H}$ is Gorenstein. □

Sharifi used this as evidence for his conjecture. However, it is not true that $\mathfrak{H}$ is always Gorenstein; the following is the main result of [Wake 2013]:

Theorem 5.12. *If $\mathfrak{H}$ is Gorenstein, then either $X_\theta = 0$ or $X_\chi = 0$. Moreover, there are examples where $X_\theta \neq 0$ and $X_\chi \neq 0$, and so $\mathfrak{H}$ is not always Gorenstein.*

5B2. *Weakly Gorenstein.* Recall that $\mathfrak{H}$ is said to be *weakly Gorenstein* if $\mathfrak{H}_\mathfrak{p}$ is Gorenstein for every prime ideal $\mathfrak{p} \in \mathrm{Spec}(\mathfrak{H})$ such that $I_\mathfrak{H} \subset \mathfrak{p}$.

Proposition 5.13. *Let $\mathcal{P} \subset \mathrm{Spec}(\mathfrak{H})$ be the set of height* 1 *prime ideals $\mathfrak{p}$ such that $I_\mathfrak{H} \subset \mathfrak{p}$. The following are equivalent*:

(1) *$H^-/I\widetilde{H}^-_{\mathrm{DM}}$ is finite.*

(2) *As a module over $\mathfrak{h} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, $\widetilde{H}^-_{\mathrm{DM}}/I\widetilde{H}^-_{\mathrm{DM}} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is generated by $\{0, \infty\}$.*

(3) *For any $\mathfrak{p} \in \mathcal{P}$, $(\widetilde{H}^-)_\mathfrak{p}$ is generated by $\{0, \infty\}$.*

(4) *For any $\mathfrak{p} \in \mathcal{P}$, $(\widetilde{H}^-)_\mathfrak{p}$ is generated by* 1 *element.*

(5) *For any $\mathfrak{p} \in \mathcal{P}$, $(\widetilde{H}^-)_\mathfrak{p}$ is free of rank* 1 *as an $\mathfrak{H}_\mathfrak{p}$-module.*

(6) *$\mathfrak{H}$ is weakly Gorenstein.*

Proof. (1) $\Longrightarrow$ (2): Follows from taking $\otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ in the exact sequence

$$0 \to H^-/I\widetilde{H}^-_{\mathrm{DM}} \to \widetilde{H}^-_{\mathrm{DM}}/I\widetilde{H}^-_{\mathrm{DM}} \to \widetilde{H}^-_{\mathrm{DM}}/H^- \to 0.$$

(2) $\Longrightarrow$ (3): Since $\mathfrak{H}/I_{\mathfrak{H}} \xrightarrow{\sim} \mathfrak{h}/I$, we have that

$$\widetilde{H}^-_{\mathrm{DM}}/I\widetilde{H}^-_{\mathrm{DM}} \cong \widetilde{H}^-_{\mathrm{DM}} \otimes_{\mathfrak{h}} \mathfrak{h}/I \cong \widetilde{H}^- \otimes_{\mathfrak{H}} \mathfrak{H}/I_{\mathfrak{H}}.$$

For any $\mathfrak{p} \in \mathcal{P}$, we have that p is invertible in $\mathfrak{H}_{\mathfrak{p}}$, so $(\widetilde{H}^-_{\mathrm{DM}}/I\widetilde{H}^-_{\mathrm{DM}})_{\mathfrak{p}} = (\widetilde{H}^-/I_{\mathfrak{H}}\widetilde{H}^-)_{\mathfrak{p}}$ is generated by $\{0, \infty\}$. By Nakayama's lemma, we have (3).

(3) $\Longrightarrow$ (4): Clear.

(4) $\Longrightarrow$ (5): By Theorem 3.1, $(\widetilde{H}^-)_{\mathfrak{p}}$ is a dualizing module for $\mathfrak{H}_{\mathfrak{p}}$, and so it is faithful. Then, if it is generated by 1 element, it is free.

(5) $\Longleftrightarrow$ (6): Since $(\widetilde{H}^-)_{\mathfrak{p}}$ is a dualizing module for $\mathfrak{H}_{\mathfrak{p}}$, this is clear.

(5) $\Longrightarrow$ (1): Note that $H^-/I\widetilde{H}^-_{\mathrm{DM}}$ is a $\mathfrak{H}/I_{\mathfrak{H}}$-module. To show (1), it suffices (by Lemma A.1) to show that $H^-/I\widetilde{H}^-_{\mathrm{DM}}$ is not supported on any nonmaximal prime ideals of $\mathfrak{H}/I_{\mathfrak{H}}$. Since the nonmaximal prime ideals of $\mathfrak{H}/I_{\mathfrak{H}}$ are exactly the images under $\mathfrak{H} \twoheadrightarrow \mathfrak{H}/I_{\mathfrak{H}}$ of elements of $\mathcal{P}$, it is enough to show that $\mathrm{Supp}_{\mathfrak{H}}(H^-/I\widetilde{H}^-_{\mathrm{DM}}) \cap \mathcal{P}$ is empty.

Let $\mathfrak{p} \in \mathcal{P}$. By (5) we see that $(\widetilde{H}^-/I_{\mathfrak{H}}\widetilde{H}^-)_{\mathfrak{p}}$ is free of rank 1 as an $(\mathfrak{H}/I_{\mathfrak{H}})_{\mathfrak{p}}$-module. But, since $\mathfrak{H}/I_{\mathfrak{H}} \xrightarrow{\sim} \mathfrak{h}/I$, $(\widetilde{H}^-_{\mathrm{DM}}/H^-)_{\mathfrak{p}}$ is also free of rank 1 as an $(\mathfrak{H}/I_{\mathfrak{H}})_{\mathfrak{p}}$-module. Then the natural surjective map

$$(\widetilde{H}^-_{\mathrm{DM}}/I\widetilde{H}^-_{\mathrm{DM}})_{\mathfrak{p}} = (\widetilde{H}^-/I_{\mathfrak{H}}\widetilde{H}^-)_{\mathfrak{p}} \twoheadrightarrow (\widetilde{H}^-_{\mathrm{DM}}/H^-)_{\mathfrak{p}}$$

must be an isomorphism. This implies that the kernel $(H^-/I\widetilde{H}^-_{\mathrm{DM}})_{\mathfrak{p}}$ is zero. □

6. Pairing with cyclotomic units

In this section, we recall some results from [Wake 2013] that will be used in the proof of Theorem 1.3.

6A. ***The Kummer pairing.*** As in [Wake 2013, Section 3.2], we will make use of a pairing between $\mathfrak{X}$ and global units. Let E denote the pro-p part of the closure of the global units in $\varprojlim(\mathbb{Z}[\zeta_{Np^r}] \otimes \mathbb{Z}_p)^\times$.

There is a pairing of $\mathbb{Z}_p[[\mathbb{Z}^\times_{p,N}]]$-modules

$$[\ ,\ ]_{\mathrm{Kum}} : E \times \mathfrak{X}^\#(1) \to \mathbb{Z}_p[[\mathbb{Z}^\times_{p,N}]].$$

It is essentially defined as the "Λ-adic version" of the pairing

$$\mathbb{Z}_p[\zeta_{Np^r}]^\times \times \mathfrak{X} \to \mu_{p^r}, \quad (u, \sigma) \mapsto \frac{\sigma(u^{1/p^r})}{u^{1/p^r}}.$$

We refer to [Wake 2013, Section 3.2] for the detailed definition.

6A1. *The map ν.* The Kummer pairing gives a homomorphism of Λ-modules $E_\theta \to \mathrm{Hom}(\mathfrak{X}_{\chi^{-1}}, \Lambda^\#(1))$. There is a special element $\mathbf{1}-\boldsymbol{\zeta} \in E_\theta$, namely, the image of $(1-\zeta_{Np^r})_r \in \varprojlim(\mathbb{Z}[\zeta_{Np^r}]^\times \otimes \mathbb{Z}_p)$.

We define ν to be the image of $\mathbf{1}-\boldsymbol{\zeta}$ under the Kummer pairing. So

$$\mathfrak{X}_{\chi^{-1}} \xrightarrow{\nu} \Lambda^\#(1)$$

is a morphism of $\mathbb{Z}_p[\![\mathbb{Z}_{p,N}^\times]\!]_{\chi^{-1}}$-modules.

The importance of ν comes from the following lemma, which relates ν to X^+:

Lemma 6.1. *There exists a natural commutative diagram of $\mathbb{Z}_p[\![\mathbb{Z}_{p,N}^\times]\!]$-modules with exact rows*:

$$\begin{tikzcd}
0 \arrow[r] & U_{\chi^{-1}}(-1) \arrow[r] \arrow[d, "\wr"] & \mathfrak{X}_{\chi^{-1}}(-1) \arrow[r] \arrow[d, "\nu(-1)"] & X_{\chi^{-1}}(-1) \arrow[r] & 0 \\
0 \arrow[r] & \Lambda^\# \arrow[r] & \Lambda^\# \arrow[r] & \Lambda^\#/\iota\xi_{\chi^{-1}} \arrow[r] & 0
\end{tikzcd}$$

Let $\bar{\nu} : X_{\chi^{-1}}(-1) \to \Lambda^\#/\iota\xi_{\chi^{-1}}$ be the induced map, and let C denote $\mathrm{coker}(\bar{\nu})$. *Then we have an equality of characteristic ideals*

$$\mathrm{Char}_\Lambda(X_\theta) = \mathrm{Char}_\Lambda(C^\#).$$

Proof. The existence of the commutative diagram is from [Wake 2013, Lemma 4.5] (note that the element denoted by $\xi_{\chi^{-1}}$ in that work would be denoted $\iota\tau\xi_{\chi^{-1}}$ here).

Let $C = \mathrm{coker}(\bar{\nu})$. By [Wake 2013, Proposition 4.8(1) and Lemma 4.6], there is an exact sequence

$$0 \longrightarrow \mathrm{E}^1(C) \longrightarrow \Lambda/\xi_{\chi^{-1}} \longrightarrow \mathfrak{X}_\theta \longrightarrow X_\theta \longrightarrow 0.$$

Since $\mathrm{Char}_\Lambda(\mathfrak{X}_\theta) = (\xi_{\chi^{-1}})$, we have $\mathrm{Char}_\Lambda(E^1(C)) = \mathrm{Char}_\Lambda(X_\theta)$. We claim that $\mathrm{Char}_\Lambda(E^1(C)) = \mathrm{Char}_\Lambda(C^\#)$. This follows from [Neukirch et al. 2008, Proposition 5.5.13, p. 319], as in the proof of Proposition 2.2 above. □

6A2. *The map ν'.* Let $\nu' : \mathfrak{X}_{\chi^{-1}} \to (\Lambda/\xi_\chi)^\#(1)$ be the composite

$$\mathfrak{X}_{\chi^{-1}} \xrightarrow{\nu} \Lambda^\#(1) \to \Lambda^\#(1)/\iota\tau\xi_\chi\Lambda^\#(1) = (\Lambda/\xi_\chi)^\#(1).$$

Lemma 6.2. *We have that* $\mathrm{coker}(\nu')$ *is finite if and only if $X_\theta/\xi_\chi X_\theta$ is finite. Moreover*, $\mathrm{coker}(\nu') = 0$ *if and only if $X_\chi = 0$ or $X_\theta = 0$.*

Proof. Let $C = \mathrm{coker}(\bar{\nu})$. From Lemma 6.1, we see that $C \cong \mathrm{coker}(\nu(-1))$. We see from the definition of ν' that

$$\mathrm{coker}(\nu') \cong C(1)/\tau^{-1}\iota\xi_\chi C(1) = (C/\iota\xi_\chi C)(1).$$

Note that since $(C/\iota\xi_\chi C)^\# \cong C^\#/\xi_\chi C^\#$, we have that $\mathrm{coker}(\nu')$ is finite if and only if $C^\#/\xi_\chi C^\#$ is finite.

Recall from Lemma 6.1 that $\mathrm{Char}_\Lambda(C^\#) = \mathrm{Char}_\Lambda(X_\theta)$. We apply Lemma A.4 to the case $M = \Lambda/\xi_\chi$, $N = C^\#$, and $N' = X_\theta$ to get that $C^\#/\xi_\chi C^\#$ is finite if and only if $X_\theta/\xi_\chi X_\theta$ is finite. This completes the proof of the first statement.

For the second statement, notice that if $X_\chi = 0$, then ξ_χ is a unit, so $\mathrm{coker}(\nu') = 0$. If $X_\chi \neq 0$, then ξ_χ is not a unit and, by Nakayama's lemma, $\mathrm{coker}(\nu') = 0$ if and only if $C = 0$. It remains to prove that $C = 0$ if and only if $X_\theta = 0$, and this follows from [Wake 2013]. Indeed, if $X_\theta = 0$, then [Wake 2013, Proposition 4.8(2)] implies that $C = 0$. Conversely, if $C = 0$, then [Wake 2013, Proposition 4.8(1), Corollary 4.7] together imply that X_θ is finite, and then we can apply [Wake 2013, Proposition 4.8(2)] to conclude that $X_\theta = 0$. □

6B. ***The map ν as an extension class.*** Fukaya and Kato [2012, Section 9.6] gave an interpretation of ν as an extension class. We review this here, and refer to [Wake 2013, Section 2.3] for more details.

There is an exact sequence

$$0 \longrightarrow H^+/IH^+ \longrightarrow \widetilde{H}_{\mathrm{DM}}/K \longrightarrow \widetilde{H}_{\mathrm{DM}}/H \longrightarrow 0, \tag{6-3}$$

where K is the kernel of the natural map $H \to H^+/IH^+$ (and so $K \cong H^- \oplus IH^+$ as $\mathfrak{h}$-modules). It can be shown that $H \to H^+/IH^+$ respects the $G_{\mathbb{Q}}$-action ([Sharifi 2011]; cf. [Fukaya and Kato 2012, Proposition 6.3.2]), and so (6-3) is an extension of $\widetilde{H}_{\mathrm{DM}}/H$ by H^+/IH^+ as $\mathfrak{h}[G_{\mathbb{Q}}]$-modules. By considering this extension as a Galois cocycle, we obtain a homomorphism of $\mathbb{Z}_p[\![\mathbb{Z}_{p,N}^\times]\!]_{\chi^{-1}}$-modules

$$\Theta : \mathfrak{X}_{\chi^{-1}} \to (\Lambda/\xi_\chi)^\#(1).$$

By [Fukaya and Kato 2012, Theorem 9.6.3], we have:

Theorem 6.4 [Wake 2013, Proposition 3.4]. *We have* $\nu' = \Theta$.

7. Relationship between the Hecke and Iwasawa sides

The goal of this section is to complete the proof of Theorem 1.3.

7A. ***The key diagram.*** First we consider a commutative diagram coming from the maps of Section 6. Let $\nu'' = (\nu')^\#(1) : \mathfrak{X}^\#_{\chi^{-1}}(1) \to \Lambda/\xi_\chi$, so that ν'' is a map of Λ-modules. Then we have the diagram of Λ-modules

$$\begin{tikzcd}
\mathfrak{X}^\#_{\chi^{-1}}(1) \otimes_\Lambda X_\chi(1) \arrow[r, "\nu''\otimes 1"] \arrow[d, "\Phi"] & \Lambda/\xi_\chi \otimes_\Lambda X_\chi(1) \arrow[d, "\Upsilon"] \\
H^-/IH^- \arrow[r, equal] & H^-/IH^-
\end{tikzcd}$$

where $\Phi = \Theta^{\#}(1) \otimes \Upsilon$. It is commutative by Theorem 6.4. This is a slight reformulation of the diagram $(*)$ in [Wake 2013, Section 1.3]. We record the result of applying the Snake Lemma to this diagram as a lemma:

Lemma 7.1. *There is an exact sequence*

$$\ker(\Phi) \longrightarrow \ker(\Upsilon) \longrightarrow \operatorname{coker}(\nu'') \otimes_{\Lambda} X_{\chi}(1) \longrightarrow \operatorname{coker}(\Phi) \longrightarrow \operatorname{coker}(\Upsilon) \longrightarrow 0.$$

7A1. *Some lemmas.*

Lemma 7.2. *We have* $\operatorname{coker}(\Phi) = H^-/I\widetilde{H}^-_{\mathrm{DM}}$.

Proof. This is a slight reformulation of [Wake 2013, Proposition 2.2], which states that the image of Φ is $I\{0, \infty\}$. Since $\{0, \infty\}$ generates $\widetilde{H}^-_{\mathrm{DM}}/H^-$, we see that the images of $I\{0, \infty\}$ and $I\widetilde{H}^-_{\mathrm{DM}}$ in H^-/IH^- are the same. □

Lemma 7.3. *We have that* $\operatorname{coker}(\nu'') \otimes_{\Lambda} X_{\chi}(1)$ *is finite if and only if* $X_{\theta}/\xi_{\chi}X_{\theta}$ *is finite.*

Proof. Let $C'' = \operatorname{coker}(\nu'')$. Since $\nu'' = (\nu')^{\#}(1)$, it is clear that C'' is finite if and only if $\operatorname{coker}(\nu')$ is finite. By Lemma 6.2 it suffices to show that $C'' \otimes_{\Lambda} X_{\chi}(1)$ is finite if and only if C'' is finite.

Now apply Lemma A.3 to $M = C''$ and $N = X_{\chi}(1)$ to get that $C'' \otimes_{\Lambda} X_{\chi}(1)$ is finite if and only if $C''/\operatorname{Char}_{\Lambda}(X_{\chi}(1))C''$ is finite. However, $\operatorname{Char}_{\Lambda}(X_{\chi}(1)) = (\xi_{\chi})$, which annihilates C''. So $C'' = C''/\operatorname{Char}_{\Lambda}(X_{\chi}(1))C''$ and the lemma follows. □

Proposition 7.4. *Suppose that* $\operatorname{coker}(\Upsilon)$ *is finite. Then* Υ *is injective.*

Proof. It is well-known (see [Fukaya and Kato 2012, Section 7.1.3]) that

$$\operatorname{Fitt}_{\Lambda}(H^-/IH^-) \subset (\xi_{\chi}).$$

We apply Lemma A.7 to the case $M = X_{\chi}(1)$, $N = H^-/IH^-$ and $f = \Upsilon$. It says that if $\operatorname{coker}(\Upsilon)$ is finite, then $\ker(\Upsilon)$ is finite. But $X_{\chi}(1)$ has no finite submodule, so the result follows. □

7A2. *The proof of Theorem 1.3.* We can now prove Theorem 1.3, which we restate here for convenience.

Theorem 1.3. *Both* $\operatorname{coker}(\Upsilon)$ *and* $X_{\theta}/\xi_{\chi}X_{\theta}$ *are finite if and only if* $\mathfrak{H}$ *is weakly Gorenstein.*

Proof. First assume that $\operatorname{coker}(\Upsilon)$ and $X_{\theta}/\xi_{\chi}X_{\theta}$ are finite. By Lemma 7.3 we have that $\operatorname{coker}(\nu'') \otimes_{\Lambda} X_{\chi}(1)$ is finite. By Lemma 7.1, we see that $\operatorname{coker}(\Phi)$ is finite. By Lemma 7.2, $H^-/I\widetilde{H}^-_{\mathrm{DM}}$ is finite. By Proposition 5.13, we have that $\mathfrak{H}$ is weakly Gorenstein.

Now assume that $\mathfrak{H}$ is weakly Gorenstein. Then, as above, $\operatorname{coker}(\Phi)$ is finite. By Lemma 7.1, we see that $\operatorname{coker}(\Upsilon)$ is finite. By Proposition 7.4, we see that $\ker(\Upsilon) = 0$. Again using Lemma 7.1 we see that $\operatorname{coker}(\nu'') \otimes_{\Lambda} X_{\chi}(1) \subset \operatorname{coker}(\Phi)$, and so $\operatorname{coker}(\nu'') \otimes_{\Lambda} X_{\chi}(1)$ is finite. By Lemma 7.3, we have that $X_{\theta}/\xi_{\chi}X_{\theta}$ is finite. □

8. Application to Sharifi's conjecture

For a finitely generated Λ-module M, let

$$d_{\mathfrak{m}_\Lambda}(M) = \dim_{\Lambda/\mathfrak{m}_\Lambda}(M/\mathfrak{m}_\Lambda M).$$

Note that, by Nakayama's lemma, $d_{\mathfrak{m}_\Lambda}(M)$ is the minimal number of generators of M. In particular, $d_{\mathfrak{m}_\Lambda}(M) = 0$ if and only if $M = 0$.

We can now prove Theorem 1.8, which we restate here for convenience:

Theorem 1.8. *Assume that $X_\theta \neq 0$ and that $\mathfrak{h}$ is weakly Gorenstein.*

Then we have

$$d_{\mathfrak{m}_\Lambda}(H^-/I\widetilde{H}^-_{\mathrm{DM}}) \geq d_{\mathfrak{m}_\Lambda}(X_\chi(1)),$$

with equality if and only if Υ is an isomorphism.

If, in addition, $\#(X_\theta) = \#(\Lambda/\mathfrak{m}_\Lambda)$, then Υ is an isomorphism if and only if

$$\#(H^-/I\widetilde{H}^-_{\mathrm{DM}}) = \#(\Lambda/\mathfrak{m}_\Lambda)^{d_{\mathfrak{m}_\Lambda}(X_\chi(1))}.$$

Proof. By Theorem 5.7, we have that $\mathrm{coker}(\Upsilon)$ is finite. By Proposition 7.4, we have $\ker(\Upsilon) = 0$. By Lemma 7.1, we have an exact sequence

$$0 \longrightarrow \mathrm{coker}(\nu'') \otimes_\Lambda X_\chi(1) \longrightarrow \mathrm{coker}(\Phi) \longrightarrow \mathrm{coker}(\Upsilon) \longrightarrow 0.$$

Theorem 5.7 implies that $\mathrm{coker}(\Upsilon) \xrightarrow{\sim} (\mathrm{tor}) \to \mathrm{coker}(\Phi)$ gives a spitting of this sequence. This gives us an isomorphism

$$H^-/I\widetilde{H}^-_{\mathrm{DM}} = \mathrm{coker}(\Phi) \cong (\mathrm{coker}(\nu'') \otimes_\Lambda X_\chi(1)) \oplus \mathrm{coker}(\Upsilon),$$

and so

$$\begin{aligned} d_{\mathfrak{m}_\Lambda}(H^-/I\widetilde{H}^-_{\mathrm{DM}}) &= d_{\mathfrak{m}_\Lambda}(\mathrm{coker}(\nu'') \otimes_\Lambda X_\chi(1)) + d_{\mathfrak{m}_\Lambda}(\mathrm{coker}(\Upsilon)) \\ &= d_{\mathfrak{m}_\Lambda}(\mathrm{coker}(\nu''))d_{\mathfrak{m}_\Lambda}(X_\chi(1)) + d_{\mathfrak{m}_\Lambda}(\mathrm{coker}(\Upsilon)). \end{aligned}$$

We claim that in fact

$$d_{\mathfrak{m}_\Lambda}(H^-/I\widetilde{H}^-_{\mathrm{DM}}) = d_{\mathfrak{m}_\Lambda}(X_\chi(1)) + d_{\mathfrak{m}_\Lambda}(\mathrm{coker}(\Upsilon)),$$

from which the first statement of the theorem follows.

To prove the claim, note that it is clear if $d_{\mathfrak{m}_\Lambda}(X_\chi(1)) = 0$. Now assume $d_{\mathfrak{m}_\Lambda}(X_\chi(1)) \neq 0$. Then we claim that $d_{\mathfrak{m}_\Lambda}(\mathrm{coker}(\nu'')) = 1$. Indeed, since $\mathrm{coker}(\nu'')$ is cyclic it suffices to show $\mathrm{coker}(\nu'') \neq 0$. But since $X_\chi(1) \neq 0$, Lemma 6.2 implies that $\mathrm{coker}(\nu'') \neq 0$ if and only if $X_\theta \neq 0$, which we are assuming. This completes the proof of the claim and of the first statement.

For the second statement, notice that the assumption can only occur if $X_\theta \cong \Lambda/\mathfrak{m}_\Lambda$. By [Wake 2013, Proposition 4.8], this implies that $\operatorname{coker}(\overline{\nu})^\# \cong \Lambda/\mathfrak{m}_\Lambda$. As in Lemma 6.2, where we computed $\operatorname{coker}(\nu')$ in terms of $\operatorname{coker}(\overline{\nu})$, we compute

$$\operatorname{coker}(\nu'') \cong \operatorname{coker}(\overline{\nu})^\# / \xi_\chi \operatorname{coker}(\overline{\nu})^\#,$$

so

$$\operatorname{coker}(\nu'') \cong \begin{cases} \Lambda/\mathfrak{m}_\Lambda & \text{if } X_\chi(1) \neq 0, \\ 0 & \text{if } X_\chi(1) = 0. \end{cases}$$

In either case,

$$\operatorname{coker}(\nu'') \otimes_\Lambda X_\chi(1) \cong (\Lambda/\mathfrak{m}_\Lambda)^{d_{\mathfrak{m}_\Lambda}(X_\chi(1))},$$

and the statement follows from the established isomorphism

$$H^-/I\widetilde{H}^-_{\mathrm{DM}} \cong (\operatorname{coker}(\nu'') \otimes_\Lambda X_\chi(1)) \oplus \operatorname{coker}(\Upsilon). \qquad \square$$

Appendix: some commutative algebra

We review some lemmas from commutative algebra that are used in the body of the paper. The results of this appendix are well-known; we include them for completeness.

Finite modules. We begin with a review of some generalities about finite modules (meaning modules of finite cardinality). Let $(A, \mathfrak{m})$ be a noetherian local ring, and assume that the residue field $A/\mathfrak{m}$ is finite. For an A-module M, we use the notation $\operatorname{Supp}_A(M)$ for the set $\{\mathfrak{p} \in \operatorname{Spec}(A) \mid M_\mathfrak{p} \neq 0\}$.

Lemma A.1. *Let M be a finitely generated A-module. The following are equivalent*:

(1) $\mathfrak{m}^n M = 0$ *for some n.*

(2) *M is finite.*

(3) *M is an Artinian A-module.*

(4) $\operatorname{Supp}_A(M) \subset \{\mathfrak{m}\}$.

Proof. For (4) $\Longrightarrow$ (1), since M is finitely generated, it is enough to prove the case where $M \cong A/I$ for an ideal I. By (4) we have that $\operatorname{Spec}(A/I) \subset \{\mathfrak{m}\}$. This implies that A/I is Artinian, which implies that $\mathfrak{m}^n(A/I) = 0$ for some n. The implications (1) $\Longrightarrow$ (2) $\Longrightarrow$ (3) $\Longrightarrow$ (1) $\Longrightarrow$ (4) are clear. □

Corollary A.2. *Suppose M and N are finitely generated A-modules. Then $M \otimes_A N$ is finite if and only if* $\operatorname{Supp}_A(N) \cap \operatorname{Supp}_A(M) \subset \{\mathfrak{m}\}$.

Proof. This is clear from Lemma A.1, since

$$\operatorname{Supp}_A(M \otimes_A N) = \operatorname{Supp}_A(N) \cap \operatorname{Supp}_A(M). \qquad \square$$

Λ-modules. Let Λ be a noetherian regular local ring of dimension 2 with finite residue field. For example, let $\Lambda = \mathbb{O}[[T]]$, where $\mathbb{O}$ is the valuation ring of a finite extension of $\mathbb{Q}_p$.

Characteristic ideals. For a finitely generated torsion Λ-module M, define the characteristic ideal of M to be

$$\mathrm{Char}_\Lambda(M) = \prod_{\mathfrak{p}} \mathfrak{p}^{l_{\mathfrak{p}}(M)},$$

where $\mathfrak{p}$ ranges over all height-1 primes of Λ and $l_{\mathfrak{p}}(M)$ is the length of $M_{\mathfrak{p}}$ as a $\Lambda_{\mathfrak{p}}$-module. Note that $l_{\mathfrak{p}}(M) > 0$ if and only if $\mathfrak{p} \in \mathrm{Supp}_\Lambda(M)$.

It follows from the definition that Char_Λ is multiplicative on exact sequences and that $\mathrm{Char}_\Lambda(M)$ is a principal ideal. By Lemma A.1, $\mathrm{Char}_\Lambda(M) = \Lambda$ if and only if $\Lambda/\mathrm{Char}_\Lambda(M)$ is finite if and only if M is finite. We have the following consequence of Corollary A.2:

Lemma A.3. *Let N and M be finitely generated Λ-modules and suppose that N is torsion. Then $M \otimes_\Lambda N$ is finite if and only if $M/\mathrm{Char}_\Lambda(N)M$ is finite.*

Proof. This is clear from Corollary A.2, as $\mathrm{Supp}_\Lambda(N) = \mathrm{Supp}_\Lambda(\Lambda/\mathrm{Char}_\Lambda(N))$. □

In the body of the paper, we often use Lemma A.3 in the following form:

Lemma A.4. *Let N, N', and M be finitely generated Λ-modules, and suppose that N and N' are torsion and that $\mathrm{Char}_\Lambda(N) = \mathrm{Char}_\Lambda(N')$. Then $M \otimes_\Lambda N$ is finite if and only if $M \otimes_\Lambda N'$ is finite.*

Fitting ideals. Let R be a commutative, noetherian ring. For a finitely generated R-module M, we define $\mathrm{Fitt}_R(M) \subset R$, the Fitting ideal of M, as follows. Let

$$R^m \xrightarrow{A} R^n \longrightarrow M \longrightarrow 0$$

be a presentation of M. Then $\mathrm{Fitt}_R(M)$ is defined to be the R-module generated by all the (n,n)-minors of the matrix A. This does not depend on the choice of resolution (see [Mazur and Wiles 1984, Appendix]).

The following lemma is a result of the independence of resolution:

Lemma A.5. *If $\phi : R \to R'$ is a ring homomorphism and M is an R-module, then*

$$\mathrm{Fitt}_{R'}(M \otimes_R R') \subset R'$$

is the ideal generated by $\phi(\mathrm{Fitt}_R(M))$.

We consider the case $R = \Lambda$. The following relation to Char_Λ is a well-known:

Lemma A.6. *If M is finitely generated and torsion, then $\mathrm{Char}_\Lambda(M)$ is the unique principal ideal such that $\mathrm{Fitt}_\Lambda(M) \subset \mathrm{Char}_\Lambda(M)$ and $\mathrm{Char}_\Lambda(M)/\mathrm{Fitt}_\Lambda(M)$ is finite.*

Proof. Using Lemma A.5, we see that for any prime $\mathfrak{p}$ of Λ,

$$\mathrm{Fitt}_{\Lambda_{\mathfrak{p}}}(M_{\mathfrak{p}}) = \mathrm{Fitt}_{\Lambda}(M)_{\mathfrak{p}}.$$

Using that $\Lambda_{\mathfrak{p}}$ is a DVR for a height-1 prime $\mathfrak{p}$, we have $\mathrm{Fitt}_{\Lambda_{\mathfrak{p}}}(M_{\mathfrak{p}}) = \mathfrak{p}^{l_{\mathfrak{p}}(M)}$ by the structure theorem for modules over a PID. We have then $\mathrm{Fitt}_{\Lambda}(M)_{\mathfrak{p}} = \mathrm{Char}_{\Lambda}(M)_{\mathfrak{p}}$ for all $\mathfrak{p}$ of height 1. Lemma A.1 then implies that $\mathrm{Char}_{\Lambda}(M)/\mathrm{Fitt}_{\Lambda}(M)$ is finite.

For uniqueness, suppose $\mathrm{Fitt}_{\Lambda}(M) \subset (f)$ has finite quotient. Then $\mathrm{Fitt}_{\Lambda}(M)_{\mathfrak{p}} = (f)_{\mathfrak{p}}$ for each height-1 prime $\mathfrak{p}$. This determines the prime factorization of f. □

Using this relation, we can deduce the following:

Lemma A.7. *Let M and N be two finitely generated torsion Λ-modules. Assume that* $\mathrm{Fitt}_{\Lambda}(N) \subset \mathrm{Char}_{\Lambda}(M)$. *If a morphism $f : M \to N$ has finite cokernel, then it has finite kernel.*

Proof. Indeed, if f has finite cokernel, then

$$\mathrm{Char}_{\Lambda}(M) = \mathrm{Char}_{\Lambda}(\ker(f))\,\mathrm{Char}_{\Lambda}(N), \quad \text{and so} \quad \mathrm{Char}_{\Lambda}(M) \subset \mathrm{Char}_{\Lambda}(N).$$

Since $\mathrm{Char}_{\Lambda}(N)/\mathrm{Fitt}_{\Lambda}(N)$ is finite, this implies that $\mathrm{Char}_{\Lambda}(M)/\mathrm{Fitt}_{\Lambda}(N)$ is finite. By Lemma A.6, this implies that $\mathrm{Char}_{\Lambda}(N) = \mathrm{Char}_{\Lambda}(M)$. The result follows by multiplicativity of characteristic ideals. □

Acknowledgments

We owe a great debt to Romyar Sharifi for his interest in and careful reading of our previous paper [Wake 2013]. It was he who asked what happens when X_θ is finite, and suggested that the answer could be found by the methods of that paper. We thank him for his interest and insight.

We also thank Takako Fukaya for answering our questions, Ralph Greenberg for his interest in this problem, and Chris Skalit for helpful discussions about commutative algebra.

This work was done while the author received partial support from NSERC of Canada. We thank them for the support.

Some of the ideas for this work were developed while the author enjoyed a short stay at the Université Paris-Sud. We thank the university for their hospitality, and Olivier Fouquet for his invitation and many interesting discussions during the stay.

We thank the anonymous referee for a detailed and encouraging report that contained many helpful comments and corrections. We especially appreciate a suggestion about the notation, which has made the paper much more readable.

Finally, we thank Professor Kazuya Kato. It was he who introduced us to this interesting area and who encouraged us to write up these results. We thank him for his questions, comments and corrections, great and small, and for his patient advice and wisdom.

References

[Fukaya and Kato 2012] T. Fukaya and K. Kato, "On conjectures of Sharifi", preprint, 2012.

[Fukaya et al. 2014] T. Fukaya, K. Kato, and R. Sharifi, "Modular symbols in Iwasawa theory", pp. 176–220 in *Iwasawa Theory 2012*, edited by T. Bouganis and O. Venjakob, Springer, Berlin, 2014.

[Greenberg 2001] R. Greenberg, "Iwasawa theory—past and present", pp. 335–385 in *Class field theory—its centenary and prospect* (Tokyo, 1998), edited by K. Miyake, Adv. Stud. Pure Math. **30**, Math. Soc. Japan, Tokyo, 2001. MR 2002f:11152 Zbl 0998.11054

[Greither 1992] C. Greither, "Class groups of abelian fields, and the main conjecture", *Ann. Inst. Fourier* (*Grenoble*) **42**:3 (1992), 449–499. MR 93j:11071 Zbl 0729.11053

[Harder and Pink 1992] G. Harder and R. Pink, "Modular konstruierte unverzweigte abelsche p-Erweiterungen von $\mathbf{Q}(\zeta_p)$ und die Struktur ihrer Galoisgruppen", *Math. Nachr.* **159** (1992), 83–99. MR 95b:11100 Zbl 0773.11069

[Kurihara 1993] M. Kurihara, "Ideal class groups of cyclotomic fields and modular forms of level 1", *J. Number Theory* **45**:3 (1993), 281–294. MR 94j:11115 Zbl 0797.11087

[Mazur and Wiles 1984] B. Mazur and A. Wiles, "Class fields of abelian extensions of $\mathbf{Q}$", *Invent. Math.* **76**:2 (1984), 179–330. MR 85m:11069 Zbl 0545.12005

[Neukirch et al. 2008] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, 2nd ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences] **323**, Springer, Berlin, 2008. MR 2008m:11223 Zbl 1136.11001

[Ohta 2003] M. Ohta, "Congruence modules related to Eisenstein series", *Ann. Sci. École Norm. Sup.* (4) **36**:2 (2003), 225–269. MR 2004d:11045 Zbl 1047.11046

[Ohta 2007] M. Ohta, "Companion forms and the structure of p-adic Hecke algebras, II", *J. Math. Soc. Japan* **59**:4 (2007), 913–951. MR 2009c:11062 Zbl 1187.11014

[Sharifi 2007] R. T. Sharifi, "Iwasawa theory and the Eisenstein ideal", *Duke Math. J.* **137**:1 (2007), 63–101. MR 2008e:11135 Zbl 1131.11068

[Sharifi 2011] R. Sharifi, "A reciprocity map and the two-variable p-adic L-function", *Ann. of Math.* (2) **173**:1 (2011), 251–300. MR 2012a:11178 Zbl 1248.11085

[Skinner and Wiles 1997] C. M. Skinner and A. J. Wiles, "Ordinary representations and modular forms", *Proc. Nat. Acad. Sci. U.S.A.* **94**:20 (1997), 10520–10527. MR 98h:11068 Zbl 0924.11044

[Wake 2013] P. Wake, "Hecke algebras associated to Λ-adic modular forms", *J. Reine Angew. Math.* (online publication April 2013).

[Wake 2014] P. Wake, "The Λ-adic Eichler–Shimura isomorphism and p-adic étale cohomology", preprint, 2014. arXiv 1303.0406

[Washington 1997] L. C. Washington, *Introduction to cyclotomic fields*, 2nd ed., Graduate Texts in Mathematics **83**, Springer, New York, 1997. MR 97h:11130 Zbl 0966.11047

Communicated by Mark Kisin
Received 2014-01-16 Revised 2014-10-13 Accepted 2014-12-06

pwake@math.uchicago.edu *Department of Mathematics, University of Chicago,*
Eckhart Hall, Chicago, IL 60637, United States

ALGEBRA AND NUMBER THEORY 9:1 (2015)
dx.doi.org/10.2140/ant.2015.9.77

Adequate groups of low degree

Robert Guralnick, Florian Herzig and Pham Huu Tiep

The notion of adequate subgroups was introduced by Jack Thorne. It is a weakening of the notion of big subgroups used in generalizations of the Taylor–Wiles method for proving the automorphy of certain Galois representations. Using this idea, Thorne was able to strengthen many automorphy lifting theorems. It was shown by Guralnick, Herzig, Taylor, and Thorne that if the dimension is small compared to the characteristic, then all absolutely irreducible representations are adequate. Here we extend that result by showing that, in almost all cases, absolutely irreducible kG-modules in characteristic p whose irreducible G^+-summands have dimension less than p (where G^+ denotes the subgroup of G generated by all p-elements of G) are adequate.

Guralnick was partially supported by NSF DMS-1001962, DMS-1302886, and the Simons Foundation Fellowship 224965. He also thanks the Institute for Advanced Study for its support. Herzig was partially supported by a Sloan Fellowship and an NSERC grant. Tiep was partially supported by NSF DMS-1201374 and the Simons Foundation Fellowship 305247. We thank the referee for careful reading of the paper, and Frank Lübeck and Klaus Lux for help with several computations.

MSC2010: primary 20C20; secondary 11F80.

Keywords: Artin–Wedderburn theorem, irreducible representations, automorphic representations, Galois representations, adequate representations.

1. Introduction

Throughout the paper, let k be a field of characteristic p and let V be a finite-dimensional vector space over k. Let $\rho : G \to \mathrm{GL}(V)$ be an absolutely irreducible representation. Thorne [2012] called (G, V) *adequate* if the following conditions hold (we rephrase the conditions slightly by combining two of the properties into one):

(i) p does not divide $\dim V$.

(ii) $\mathrm{Ext}^1_G(V, V) = 0$.

(iii) $\mathrm{End}(V)$ is spanned by the elements $\rho(g)$ with $\rho(g)$ semisimple.

We remark that recently Thorne has shown that one can relax condition (i) above (see [Thorne 2015, Corollary 7.3] and [Guralnick et al. 2014, §1]).

If G is a finite group of order prime to p, then it is well known that (G, V) is adequate. In this case, condition (iii) is often referred to as Burnside's lemma. It is a trivial consequence of the Artin–Wedderburn theorem. Also, (G, V) is adequate if G is a connected algebraic group over $k = \bar{k}$ and V is a rational irreducible kG-module; see [Guralnick 2012a, Theorem 1.2].

The adequacy conditions are a generalization to higher dimension of the conditions used by Wiles and Taylor in studying the automorphic lifts of certain 2-dimensional Galois representations, and they are a weakening of the previously introduced *bigness* condition [Clozel et al. 2008]. Thorne [2012] strengthened the existing automorphy lifting theorems for n-dimensional Galois representations assuming the weaker adequacy hypotheses. We refer the reader to [Thorne 2012] for more references and details.

The following theorem was proved in [Guralnick et al. 2012, Theorem 9]:

Theorem 1.1. *Let k be a field of characteristic p and G a finite group. Let V be an absolutely irreducible faithful kG-module. Let G^+ denote the subgroup generated by the p-elements of G. If* $\dim W \le (p-3)/2$ *for an absolutely irreducible kG^+-submodule W of V, then (G, V) is adequate.*

The example $G = \mathrm{SL}_2(p)$ with V irreducible of dimension $(p-1)/2$ shows that the previous theorem is the best possible. However, the counterexamples are rare. Our first goal is to prove a similar theorem under the assumption that $\dim W < p$. We show that almost always (G, V) is adequate; see Corollary 1.4. Indeed, we show that the spanning condition always holds under the weaker hypothesis. We show that there are only a handful of examples where $\mathrm{Ext}^1_G(V, V) \neq 0$. See Theorems 1.2 and 1.3 for more precise statements.

Theorem 1.1 was crucial in several recent applications of automorphy lifting theorems, such as [Barnet-Lamb et al. 2014; Calegari 2012; Dieulefait 2014]. In fact, the main two technical hypotheses in the most recent automorphy lifting theorems are potential diagonalizability (a condition in p-adic Hodge theory) and adequacy of the residual image [Dieulefait and Gee 2012]. Since some important applications of automorphy lifting theorems [Breuil et al. 2001; Khare and Wintenberger 2009; Dieulefait 2014] require working with primes p that are small relative to the dimension of the Galois representation, we expect that our results will be useful in obtaining further arithmetic applications of automorphy lifting theorems. (Note that adequacy of 2-dimensional linear groups has been analyzed in Appendix A of [Barnet-Lamb et al. 2013].)

An outgrowth of our results leads us to prove an analogue of [Guralnick 1999] and answer a question of Serre on complete reducibility of finite subgroups of orthogonal and symplectic groups of small degree. This is done in the sequel [Guralnick et al. 2014], where we essentially classify indecomposable modules in characteristic p of dimension less than $2p-2$. We also extend adequacy results to the case of linear groups of degree p and generalize the asymptotic result [Guralnick 2012a, Theorem 1.2] to disconnected algebraic groups $\mathcal{G}$ (with $p \nmid [\mathcal{G}:\mathcal{G}^0]$), allowing at the same time that p divides the dimension of the $\mathcal{G}$-module.

Note that if the kernel of ρ has order prime to p, then there is no harm in passing to the quotient. So we will generally assume that either ρ is faithful or more generally has kernel of order prime to p. Also, note that the dimensions of cohomology groups and the dimension of the span of the semisimple elements in G in $\mathrm{End}(V)$ do not change under extension of scalars. Hence, most of the time we will work over an algebraically closed field k.

Following [Guralnick 2012b], we say that the representation $\rho : G \to \mathrm{GL}(V)$, or the pair (G, V), is *weakly adequate* if $\mathrm{End}(V)$ is spanned by the elements $\rho(g)$ with $\rho(g)$ semisimple.

Our main results are the following:

Theorem 1.2. *Let k be a field of characteristic p and G a finite group. Let V be an absolutely irreducible faithful kG-module. Let G^+ denote the subgroup generated by the p-elements of G. If $p > \dim W$ for an irreducible kG^+-submodule W of V, then (G, V) is weakly adequate.*

Theorem 1.3. *Let $k = \bar{k}$ be a field of characteristic p and G a finite group. Let V be an irreducible faithful kG-module. Let G^+ denote the subgroup generated by the p-elements of G. Suppose that $p > d := \dim W$ for an irreducible kG^+-submodule W of V, and let $H < \mathrm{GL}(W)$ be induced by the action of G^+ on W. Then one of the following holds*:

(a) *p is a Fermat prime, $d = p-1$, G^+ is solvable* (*and so G is p-solvable*), *and $H/\boldsymbol{O}_{p'}(H) = C_p$.*

(b) *$H^1(G, k) = 0$. Furthermore*, *either $\mathrm{Ext}^1_G(V, V) = 0$, or one of the following holds*:

(i) $H = \mathrm{PSL}_2(p)$ *or* $\mathrm{SL}_2(p)$, *and* $d = (p \pm 1)/2$.

(ii) $H = \mathrm{SL}_2(p) \times \mathrm{SL}_2(p^a)$ (*modulo a central subgroup*), $d = p - 1$, *and* W *is a tensor product of a* $(p-1)/2$*-dimensional* $\mathrm{SL}_2(p)$*-module and a* 2*-dimensional* $\mathrm{SL}_2(p^a)$*-module.*

(iii) $p = (q+1)/2$, $d = p - 1$, *and* $H \cong \mathrm{SL}_2(q)$.

(iv) $p = 2^f + 1$ *is a Fermat prime*, $d = p - 2$, *and* $H \cong \mathrm{SL}_2(2^f)$.

(v) $(H, p, d) = (3\mathsf{A}_6, 5, 3)$ *and* $(2\mathsf{A}_7, 7, 4)$.

(vi) $(H, p, d) = (\mathrm{SL}_2(3^a), 3, 2)$ *and* $a \geq 2$.

Theorems 1.2 and 1.3 immediately imply:

Corollary 1.4. *Let k be a field of characteristic p and G a finite group. Let V be an absolutely irreducible faithful kG-module, and let G^+ denote the subgroup generated by the p-elements of G. Suppose that the dimension of any irreducible kG^+-submodule in V is less than p. Let W be an irreducible $\bar{k}G^+$-submodule of $V \otimes_k \bar{k}$. Then (G, V) is adequate, unless the group $H < \mathrm{GL}(W)$ induced by the action of G^+ on W is as described in one of the exceptional cases* (a), (b)(i)–(vi) *listed in Theorem 1.3.*

Corollary 1.5. *Let k be a field of characteristic p and G a finite group. Let V be an absolutely irreducible faithful kG-module, and let G^+ denote the subgroup generated by the p-elements of G. Suppose that the dimension d of any irreducible kG^+-submodule in V is less than $p-3$. Let W be an irreducible $\bar{k}G^+$-submodule of $V \otimes_k \bar{k}$. Then (G, V) is adequate, unless $d = (p \pm 1)/2$ and the group $\overline{H} < \mathrm{PGL}(W)$ induced by the action of G^+ on W is* $\mathrm{PSL}_2(p)$.

One should emphasize that, in all the aforementioned results, the dimension bound $\dim W < p$ is imposed only on an irreducible G^+-summand of V. In general, G/G^+ can be an arbitrary p'-group, and likewise, $\dim V/\dim W$ can be arbitrarily large. So a major portion of the proofs, especially for Theorem 1.2, is spent establishing the results under these more general hypotheses.

This paper is organized as follows. In Section 2, based on results of [Blau and Zhang 1993], we describe the structure of (non-p-solvable) finite linear groups $G < \mathrm{GL}(V)$ such that the dimension of irreducible G^+-summands in V is less than p; see Theorem 2.4. Sections 3 and 4 are devoted to establish weak adequacy for Chevalley groups in characteristic p. In Sections 5 and 6, we prove adequacy for the remaining families of finite groups occurring in Theorem 2.4 and complete the proof of Theorem 1.2. In Section 7, we collect various facts concerning extensions and self-extensions of simple modules. The main result of Section 8, Proposition 8.2, classifies self-dual indecomposable $\mathrm{SL}_2(q)$-modules for $p \mid q$. In Section 9, we describe the structure of finite groups G possessing a reducible indecomposable module of dimension $\leq 2p - 3$ (Proposition 9.7). Theorem 1.3 and Corollary 1.4 are proved in Section 10.

Notation. If V is a kG-module and $X \leq G$ is a subgroup, then V_X denotes the restriction of V to X. The containments $X \subset Y$ (for sets) and $X < Y$ (for groups) are strict. Fix a prime p and an algebraically closed field k of characteristic p. Then for any finite group G, $\mathrm{IBr}_p(G)$ is the set of isomorphism classes of irreducible kG-representations (or their Brauer characters, depending on the context), $\mathfrak{d}_p(G)$ denotes the smallest degree of the nontrivial $\varphi \in \mathrm{IBr}_p(G)$, and $B_0(G)$ denotes the principal p-block of G. Sometimes we use $\mathbb{1}$ to denote the principal representation. $\boldsymbol{O}_p(G)$ is the largest normal p-subgroup of G, $\boldsymbol{O}^p(G)$ is the smallest normal subgroup N of G subject to G/N being a p-group, and similarly for $\boldsymbol{O}_{p'}(G)$ and $\boldsymbol{O}^{p'}(G) = G^+$. Furthermore, the *Fitting subgroup* $F(G)$ is the largest nilpotent normal subgroup of G, and $E(G)$ is the product of all subnormal quasisimple subgroups of G, so that $F^*(G) = F(G)E(G)$ is the *generalized Fitting subgroup* of G. Given a finite-dimensional kG-representation $\Phi : G \to \mathrm{GL}(V)$, we denote by $\mathcal{M}$ the k-span

$$\langle \Phi(g) : \Phi(g) \text{ semisimple} \rangle_k.$$

If M is a finite-length module over a ring R, then define $\mathrm{soc}_i(M)$ by $\mathrm{soc}_0(M) = 0$ and $\mathrm{soc}_j(M)/\mathrm{soc}_{j-1}(M) = \mathrm{soc}(M/\mathrm{soc}_{j-1}(M))$. If $M = \mathrm{soc}_j(M)$ with j minimal, we say that j is the *socle length* of M.

2. Linear groups of low degree

First we describe the structure of absolutely irreducible non-p-solvable linear groups of low degree, relying on the main result of [Blau and Zhang 1993]:

Theorem 2.1. *Let W be a faithful, absolutely irreducible kH-module for a finite group H with $\boldsymbol{O}^{p'}(H) = H$. Suppose that $1 < \dim W < p$. Then one of the following cases holds, where $P \in \mathrm{Syl}_p(H)$:*

(a) *p is a Fermat prime, $|P| = p$, $H = \boldsymbol{O}_{p'}(H)P$ is solvable, $\dim W = p-1$, and $\boldsymbol{O}_{p'}(H)$ is absolutely irreducible on W.*

(b) $|P| = p$, $\dim W = p-1$, *and one of the following conditions holds*:

- (b1) $(H, p) = (\mathrm{SU}_n(q), (q^n+1)/(q+1))$, $(\mathrm{Sp}_{2n}(q), (q^n+1)/2)$, $(2\mathsf{A}_7, 5)$, $(3J_3, 19)$, *or* $(2Ru, 29)$.
- (b2) $p = 7$ *and* $H = 6_1 \cdot \mathrm{PSL}_3(4)$, $6_1 \cdot \mathrm{PSU}_4(3)$, $2J_2$, $3\mathsf{A}_7$, *or* $6\mathsf{A}_7$.
- (b3) $p = 11$ *and* $H = M_{11}$, $2M_{12}$, *or* $2M_{22}$.
- (b4) $p = 13$ *and* $H = 6 \cdot Suz$ *or* $2\mathrm{G}_2(4)$.

(c) $|P| = p$, $\dim W = p-2$, *and* $(H, p) = (\mathrm{PSL}_n(q), (q^n-1)/(q-1))$, (A_p, p), $(3\mathsf{A}_6, 5)$, $(3\mathsf{A}_7, 5)$, $(M_{11}, 11)$, *or* $(M_{23}, 23)$.

(d) $(H, p, \dim W) = (2\mathsf{A}_7, 7, 4)$, $(J_1, 11, 7)$.

(e) *Extraspecial case*: $|P| = p = 2^n + 1 \geq 5$, $\dim W = 2^n$, $\boldsymbol{O}_{p'}(H) = R\boldsymbol{Z}(H)$, $R = [P, R]\boldsymbol{Z}(R) \in \mathrm{Syl}_2(\boldsymbol{O}_{p'}(H))$, $[P, R]$ *is an extraspecial* 2*-group of order* 2^{1+2n}, *and* $V_{[P,R]}$ *is absolutely irreducible. Furthermore*, $S := H/\boldsymbol{O}_{p'}(H)$ *is simple nonabelian*, *and either* $S = \mathrm{Sp}_{2a}(2^b)'$ *or* $\Omega^-_{2a}(2^b)'$ *with* $ab = n$ *or* $S = \mathrm{PSL}_2(17)$ *and* $p = 17$.

(f) $\mathrm{Lie}(p)$ *case*: $H/\boldsymbol{Z}(H)$ *is a direct product of simple groups of Lie type in characteristic* p.

Furthermore, *in the cases* (b)–(d), H *is quasisimple with* $\boldsymbol{Z}(H)$ *a* p'*-group.*

Proof. We apply Theorem A of [Blau and Zhang 1993] and arrive at one of the possibilities (a)–(j) listed there. Note that possibility (j) is restated as our case (f), and possibilities (f)–(i) do not occur since H is absolutely irreducible. Possibility (a) does not arise either since $\dim W > 1$, and possibility (b) is restated as our case (a). Next, in the case of possibility (c), either we are back to our case (a), or else we are in case (e), where the simplicity of S follows from the assumption that $H = \boldsymbol{O}^{p'}(H)$. (Also, $S \not\cong \Omega^+_{2a}(2^b)$ since $|S|_p = |P| = p$.)

In the remaining cases (d), (e), and (g) of [Blau and Zhang 1993, Theorem A], we have that $H/\boldsymbol{Z}(H) = S$ is a simple nonabelian group, and $\boldsymbol{Z}(H)$ is a cyclic p'-group by Schur's lemma. Hence, $H^{(\infty)}$ is a perfect normal subgroup of p'-index in $H = \boldsymbol{O}^{p'}(H)$. It follows that $H = H^{(\infty)}$ and so it is quasisimple. Also, the possibilities for $(S, \dim W, p)$ are listed. Using

- [Guralnick and Tiep 1999] if $S = \mathrm{PSL}_n(q)$,
- [Guralnick et al. 2002] if $S = \mathrm{PSU}_n(q)$ or $\mathrm{PSp}_{2n}(q)$,
- [Guralnick and Tiep 2005, Lemma 6.1] if $S = \mathsf{A}_p$ and $p \geq 17$, and
- [Jansen et al. 1995] for the other simple groups,

we arrive at cases (b)–(d). □

Next we prove some technical lemmas in the spirit of [Blau and Zhang 1993, Lemma 3.10].

Lemma 2.2. *Let* G *be a finite group with normal subgroups* K_1 *and* K_2 *such that* $K_1 \cap K_2 \leq \boldsymbol{O}_{p'}(G)$. *For any finite group* X, *let* $\overline{X}$ *denote* $X/\boldsymbol{O}_{p'}(X)$. *Suppose that* $\overline{G/K_1} \cong \prod_{i\in I} M_i$ *and* $\overline{G/K_2} \cong \prod_{j\in J} N_j$ *are direct products of simple nonabelian groups. Then there are some sets* $I' \subseteq I$ *and* $J' \subseteq J$ *such that*

$$\overline{G} \cong \prod_{i\in I'} M_i \times \prod_{j\in J'} N_j.$$

Proof. For $i = 1, 2$, let $K_i \leq H_i \lhd G$ be such that $H_i/K_i = \boldsymbol{O}_{p'}(G/K_i)$. Then

$$G/H_1 \cong \prod_{i\in I} M_i, \quad G/H_2 \cong \prod_{j\in J} N_j.$$

By [Blau and Zhang 1993, Lemma 3.9], there are sets $I' \subseteq I$ and $J' \subseteq J$ such that

$$G/(H_1 \cap H_2) \cong \prod_{i \in I'} M_i \times \prod_{j \in J'} N_j.$$

It remains to show that $H_1 \cap H_2 = \boldsymbol{O}_{p'}(G)$. Certainly, $H_1 \cap H_2 \geq \boldsymbol{O}_{p'}(G)$. Conversely,

$$(H_1 \cap K_2)/(K_1 \cap K_2) \hookrightarrow H_1/K_1, \quad (H_1 \cap H_2)/(H_1 \cap K_2) \hookrightarrow H_2/K_2,$$

and $K_1 \cap K_2 \leq \boldsymbol{O}_{p'}(G)$. It follows that $H_1 \cap H_2$ is a p'-group. □

Lemma 2.3. *Let G be a finite group with a faithful kG-module V. Suppose that $V = W_1 \oplus \cdots \oplus W_t$ is a direct sum of kG-submodules, and let $H_i \leq \mathrm{GL}(W_i)$ be the linear group induced by the action of G on W_i. Suppose that $S_i := H_i/\boldsymbol{O}_{p'}(H_i)$ is a simple nonabelian group for each i. Then there is a subset $J \subseteq \{1, 2, \ldots, t\}$ such that*

$$G/\boldsymbol{O}_{p'}(G) \cong \prod_{j \in J} S_j.$$

In particular, if $\boldsymbol{O}_{p'}(H_i) = 1$ for all i, then $G \cong \prod_{j \in J} S_j$.

Proof. We proceed by induction on t. The induction base $t = 1$ is obvious. For the induction step, let K_i denote the kernel of the action of G on W_i, so that $H_i = G/K_i$. The faithfulness of V implies that $\bigcap_{i=1}^t K_i = 1$. Adopt the bar notation $\overline{X}$ of Lemma 2.2. By the assumption, $\overline{G/K_1} \cong S_1$. Next, observe that $L := \bigcap_{i=2}^t K_i$ is the kernel of the action of G on $V' := W_2 \oplus \cdots \oplus W_t$, and the action of G/L on W_i induces H_i for all $i \geq 2$. Applying the induction hypothesis to G/L acting on V', we see that $\overline{G/L} \cong \prod_{j \in J'} S_j$ for some $J' \subseteq \{2, 3, \ldots, t\}$. Also, $K_1 \cap L = 1$. Hence we can apply Lemma 2.2 to get $\overline{G} \cong \prod_{j \in J} S_j$ for some $J \subseteq \{1, 2, 3, \ldots, t\}$.

Finally, if $\boldsymbol{O}_{p'}(H_i) = 1$ for all i, then the action of $\boldsymbol{O}_{p'}(G)$ on W_i induces a normal p'-subgroup of H_i for all i, whence $\boldsymbol{O}_{p'}(G) \leq \bigcap_{i=1}^t K_i = 1$, and we are done. □

Theorem 2.4. *Let V be a finite-dimensional vector space over an algebraically closed field k of characteristic p and $G < \mathrm{GL}(V)$ a finite irreducible subgroup. Suppose that an irreducible G^+-submodule W of V has dimension $< p$ and G^+ is not solvable. Then G^+ is perfect and has no composition factor isomorphic to C_p; in particular, $H^1(G, k) = 0$. Furthermore, if H is the image of G^+ in $\mathrm{GL}(W)$, then one of the following statements holds*:

(i) *One of the cases* (b)–(d) *of Theorem 2.1 holds for H, and $G^+/\boldsymbol{Z}(G^+) = S_1 \times \cdots \times S_n \cong S^n$ is a direct product of n copies of the simple nonabelian group $S = H/\boldsymbol{Z}(H)$. Here, G permutes these n direct factors $S_1, \ldots, S_n$ transitively. Furthermore, $G^+ = L_1 * \cdots * L_n$ is a central product of quasisimple groups L_i, each being a central cover of S, and the action of G^+ on each irreducible G^+-submodule W_i of W induces a quasisimple subgroup of* $\mathrm{GL}(W_i)$. *Finally, if H is* *the full covering group of S or if $H = S$, then*

$$G^+ = L_1 \times L_2 \times \cdots \times L_n \cong H^n.$$

(ii) *Case* (e) *of Theorem 2.1 holds for H. Furthermore, $\boldsymbol{O}_{p'}(G^+)$ is irreducible on any irreducible G^+-submodule W_i of V, and $G^+/\boldsymbol{O}_{p'}(G^+) \cong S^m$ is a direct product of $m \geq 1$ copies of the simple nonabelian group S listed in case* (e) *of Theorem 2.1.*

(iii) *Case* (f) *of Theorem 2.1 holds for H, and $G^+ = L_1 * \cdots * L_n$ is a central product of quasisimple groups L_i of Lie type in characteristic p with $\boldsymbol{Z}(L_i)$ a p'-group.*

Proof. (a) By Clifford's theorem, $V_{G^+} \cong e\sum_{i=1}^t W_i$ for some $e, t \geq 1$, and $\{W_1, \ldots, W_t\}$ is a full set of representatives of isomorphism classes of G-conjugates of $W \cong W_1$. Let $\Phi_i : G^+ \to \mathrm{GL}(W_i)$ denote the corresponding representation, and let $K_i := \mathrm{Ker}(\Phi_i)$, so that $G^+/K_i \cong H$ for all i, where we denote by H the subgroup of $\mathrm{GL}(W)$ induced by the action of G^+ on W. The faithfulness of the action of G on V implies that $\bigcap_{i=1}^t K_i = 1$. In particular, G^+ injects into $\prod_{i=1}^t (G^+/K_i) \cong H^t$. Hence case (a) of Theorem 2.1 is impossible since G^+ is not solvable. In case (f) of Theorem 2.1, an argument similar to the proof of Lemma 2.3 shows that $G^+/\boldsymbol{Z}(G^+) = S_1 \times \cdots \times S_n$ is a direct product of simple groups S_i of Lie type in characteristic p. Since $G^+ = \boldsymbol{O}^{p'}(G^+)$ and $\boldsymbol{O}_p(G^+) \leq \boldsymbol{O}_p(G) = 1$, it then follows that G^+ equals $L_1 * \cdots * L_n$, a central product of quasisimple groups L_i of Lie type in characteristic p with $\boldsymbol{Z}(L_i)$ a p'-group (just take L_i to be a perfect inverse image of S_i in G^+), i.e., (iii) holds. In the remaining cases (b)–(e) of Theorem 2.1, $H/\boldsymbol{O}_{p'}(H) \cong S$, where S is a nonabelian simple group described in Theorem 2.1(b)–(e). By Lemma 2.3, $G^+/\boldsymbol{O}_{p'}(G^+) \cong S^n$, a direct product of $n \geq 1$ copies of S. Thus in all cases, G^+ has no composition factor isomorphic to C_p and $\boldsymbol{Z}(G^+) \leq \boldsymbol{O}_{p'}(G^+)$. Furthermore, $G^+ = (G^+)^{(\infty)}\boldsymbol{O}_{p'}(G^+)$ and so $(G^+)^{(\infty)}$ is a normal subgroup of p'-index in $G^+ = \boldsymbol{O}^{p'}(G^+)$, whence G^+ is perfect. Thus the first claim of Theorem 2.4 holds in all cases.

(b) Suppose next that we are in the cases (b)–(d) of Theorem 2.1. Then H is quasisimple and $\boldsymbol{Z}(H)$ is a p'-group; in particular, $\boldsymbol{O}_{p'}(H) = \boldsymbol{Z}(H)$ and $H/\boldsymbol{Z}(H) = S$. Note that $\Phi_i(\boldsymbol{O}_{p'}(G^+))$ is a normal p'-subgroup of $H_i = \Phi_i(G^+) \cong H$, whence $\Phi_i(\boldsymbol{O}_{p'}(G^+)) \leq \boldsymbol{Z}(H_i)$. Thus, for any $z \in \boldsymbol{O}_{p'}(G^+)$ and any $g \in G^+$, $[z, g]$ acts trivially on each W_i and so $[z, g] \in \bigcap_{i=1}^t K_i = 1$, i.e., $z \in \boldsymbol{Z}(G^+)$. We have shown that $\boldsymbol{O}_{p'}(G^+) = \boldsymbol{Z}(G^+) =: Z$.

Now we can write $G^+/Z = S_1 \times \cdots \times S_n$ with $S_i \cong S$. Let M_i denote the full inverse image of S_i in G^+ and let $L_i := M_i^{(\infty)}$. Then $M_i = L_iZ$, $L_i/(L_i \cap Z) \cong M_i/Z \cong S$, and so L_i is quasisimple and a central cover of S. Next, for $i \neq j$ we have $[L_i, L_j] \leq Z$ and so, since L_i is perfect,

$$[L_i, L_j] = [[L_i, L_i], L_j] = 1$$

by the three subgroups lemma. It follows that $M := L_1L_2 \cdots L_n$ is a central product of the L_i. But $G^+ = MZ$ and G^+ is perfect, so $G^+ = M$.

The remaining claims in (i) are obvious if $t = 1$, so we will now assume that $t > 1$. First we show that G acts transitively on $\{S_1, \dots, S_n\}$. Relabeling the W_i suitably we may assume that $K_1Z/Z \geq \prod_{i \neq 1} S_i$ and $K_2Z/Z \geq \prod_{i \neq 2} S_i$. But $G^+/K_j = \Phi_j(G^+)$ is quasisimple, so in fact $K_jZ/Z = \prod_{i \neq j} S_i$ for $j = 1, 2$. By Clifford's theorem, $W_2 = W_1^g$ for some $g \in G$. Now g sends K_1 to K_2, and so it sends S_1 to S_2, as desired. If furthermore $H = S$, then $\boldsymbol{O}_{p'}(H) = 1$, whence $G^+ = S_1 \times \cdots \times S_n \cong H^n$ by Lemma 2.3. Consider the opposite situation: H is the full covering group of S. Again relabeling the W_i suitably and arguing as above, we may assume that $K_1Z/Z = \prod_{i \neq 1} S_i$. In this case, $K_1Z \geq L_i$ for $i \geq 2$, whence $L_i = [L_i, L_i] \leq [K_1Z, K_1Z] \leq K_1$ and $K_1 \geq L_2L_3 \cdots L_n$. It also follows that $G^+ = K_1L_1$ and so $L_1/(K_1 \cap L_1) \cong G^+/K_1 \cong H$. Recall that L_1 is perfect and $L_1/(L_1 \cap Z) \cong S$, i.e., L_1 is a central extension of the simple group S. But H is the full covering group of S, so $|L_1| \leq |H|$. It follows that $L_1 \cap K_1 = 1$ and $L_1 \cong H$; in particular, $L_1 \cap \prod_{j \neq 1} L_j = 1$. Similarly, $L_i \cong H$ and $L_i \cap \prod_{j \neq i} L_j = 1$ for all i. Thus $G^+ = L_1 \times \cdots \times L_n \cong H^n$.

(c) Assume now that we are in case (e) of Theorem 2.1. Then $P_i := \Phi_i(\boldsymbol{O}_{p'}(G^+))$ is again a normal p'-subgroup of H_i, and so $P_i \leq \boldsymbol{O}_{p'}(H_i)$. On the other hand, H_i/P_i is a quotient of $G^+/\boldsymbol{O}_{p'}(G^+) \cong S^n$, whence all composition factors of H_i/P_i are isomorphic to S. Since $H_i/\boldsymbol{O}_{p'}(H_i) \cong S$, we conclude that $P_i = \boldsymbol{O}_{p'}(H_i)$; in particular, $\boldsymbol{O}_{p'}(G^+)$ is irreducible on W_i. □

3. Weak adequacy for $\mathrm{SL}_2(\mathbb{F}_p)$

Proposition 3.1. *Any nontrivial irreducible representation V of* $\mathrm{SL}_2(\mathbb{F}_p)$ *over* $\overline{\mathbb{F}}_p$ *is weakly adequate except when* $\dim V = p$ *and* $p \leq 3$.

Remark 3.2. When $p \leq 3$ the p'-elements of $\mathrm{SL}_2(\mathbb{F}_p)$ generate a normal subgroup of index p. If moreover $\dim V = p$ then this subgroup does not act irreducibly; hence V cannot be weakly adequate.

The rest of the section is devoted to proving Proposition 3.1. Note that $p > 2$. In the following we write $V = L(a)$ with $0 < a \leq p - 1$. If $a \leq (p-3)/2$ then the argument of [Guralnick et al. 2012, Theorem 9] applies. (Let $\mathcal{T} \subset \mathrm{SL}_2$ denote the diagonal maximal torus. Then distinct weights of $\mathcal{T}_{/\overline{\mathbb{F}}_p}$ on $L(a)$ restrict distinctly to $\mathcal{T}(\mathbb{F}_p)$, and $\operatorname{End} V$ is semisimple by [Serre 1994] with p-restricted highest weights.) We will assume from now on that $a \geq (p-1)/2$.

Lemma 3.3. *Suppose that* $(p-1)/2 \leq a \leq p-1$. *Then*

$$\operatorname{head}_{\mathrm{SL}_2}(L(a) \otimes L(a)) \cong \bigoplus_{i=0}^{(p-1)/2} L(2i).$$

Moreover, if $a \neq p-1$, $\mathrm{head}_{\mathrm{SL}_2(\mathbb{F}_p)}(L(a)\otimes L(a)) = \mathrm{head}_{\mathrm{SL}_2}(L(a)\otimes L(a))$, *whereas if* $a = p-1$,

$$\mathrm{head}_{\mathrm{SL}_2(\mathbb{F}_p)}(L(a)\otimes L(a)) \cong \bigoplus_{i=0}^{(p-1)/2} L(2i) \oplus L(p-1).$$

Proof. By [Doty and Henke 2005, Lemmas 1.1, 1.3], we see that for SL_2,

$$L(a)\otimes L(a) \cong \bigoplus_{i=0}^{p-2-a} L(2i) \oplus \bigoplus_{i=p-1-a}^{(p-3)/2} T(2p-2-2i) \oplus L(p-1), \tag{3-1}$$

where the tilting module $T(2p-2-r)$ for $0 \le r \le p-2$ is uniserial of the form $(L(r) \mid L(2p-2-r) \mid L(r))$. This proves the first part of the lemma. As is pointed out in Lemma 1.1 of [Doty and Henke 2005], $T(2p-2-r) \cong Q(r)$ for $0 \le r \le p-2$, which implies that $T(2p-2-r)|_{\mathrm{SL}_2(\mathbb{F}_p)}$ is projective. See also [Jantzen 2003, §2.7].

Noting that $L(2p-2-r)|_{\mathrm{SL}_2(\mathbb{F}_p)} \cong L(p-1-r) \oplus L(p-3-r)$ and using that $L(p-1)$ is the only irreducible projective $\mathrm{SL}_2(\mathbb{F}_p)$-module, it follows that

$$T(2p-2-r)|_{\mathrm{SL}_2(\mathbb{F}_p)} \cong \begin{cases} U(r) & \text{if } 0 < r \le p-2, \\ U(0) \oplus L(p-1) & \text{if } r = 0, \end{cases} \tag{3-2}$$

where $U(i)$ denotes the projective cover of $L(i)$. The claim follows. □

In the following, we will think of $V \cong L(a)$ as the space of homogeneous polynomials in X, Y of degree a.

Lemma 3.4. $(\mathrm{End}\, V)^{\mathcal{U}} \cong \bigoplus_{k=0}^{a} \overline{\mathbb{F}}_p \cdot (X(\partial/\partial Y))^k$, *where* $\mathcal{U} = \left(\begin{smallmatrix} 1 & * \\ & 1 \end{smallmatrix}\right) \subset \mathrm{SL}_2$.

Proof. The torus $\mathcal{T} = \left(\begin{smallmatrix} * & \\ & * \end{smallmatrix}\right) \subset \mathrm{SL}_2$ acts on $(\mathrm{End}\, V)^{\mathcal{U}}$, and, for $\lambda \in X(\mathcal{T})$,

$$\mathrm{Hom}_{\mathcal{T}}(\lambda, (\mathrm{End}\, V)^{\mathcal{U}}) \cong \mathrm{Hom}_{\mathrm{SL}_2}(V(\lambda), \mathrm{End}\, V). \tag{3-3}$$

So it follows from (3-1) that $\dim(\mathrm{End}\, V)^{\mathcal{U}} = a+1$. (Namely, $\lambda = 0, 2, \dots, 2a$ each work once.) A simple calculation shows that $X(\partial/\partial Y)$ is $\mathcal{U}$-invariant; hence, so are $(X(\partial/\partial Y))^k$, $(0 \le k \le a)$, which are clearly nonzero. Since $(X(\partial/\partial Y))^k$ has weight $2k$, they are linearly independent. □

By Lemma 3.4 and (3-1), for $0 \le k \le a$, the SL_2-representation generated by $(X(\partial/\partial Y))^k$ is $V(2k) \subset \mathrm{End}(V)$.

Lemma 3.5. *The weight-*0 *subspace in* $V(2k) \subset \mathrm{End}\, V$ *is the line spanned by*

$$\Delta_k := \sum_{i=0}^{k} (-1)^{k-i} \binom{k}{i}^2 X^i Y^{k-i} \Big(\frac{\partial}{\partial X}\Big)^i \Big(\frac{\partial}{\partial Y}\Big)^{k-i} \qquad (0 \le k \le a).$$

Proof. We compute the weight-0 part of $\left(\begin{smallmatrix}1 & \\ -1 & 1\end{smallmatrix}\right) \cdot (X(\partial/\partial Y))^k$. Take $f \in \overline{\mathbb{F}}_p[X, Y]$ homogeneous of degree a. Under $\left(\begin{smallmatrix}1 & \\ -1 & 1\end{smallmatrix}\right) \cdot (X(\partial/\partial Y))^k$ the element f is sent to

$$\begin{aligned}\left(\begin{pmatrix}1 & \\ -1 & 1\end{pmatrix} \cdot \left(X\frac{\partial}{\partial Y}\right)^k\right) f(X+Y, Y) \\ &= \begin{pmatrix}1 & \\ -1 & 1\end{pmatrix}\left[X^k \sum_{i=0}^{k} \binom{k}{i}\left(\left(\frac{\partial}{\partial X}\right)^i \left(\frac{\partial}{\partial Y}\right)^{k-i} f\right)(X+Y, Y)\right] \\ &= (X-Y)^k \sum_{i=0}^{k} \binom{k}{i}\left(\frac{\partial}{\partial X}\right)^i \left(\frac{\partial}{\partial Y}\right)^{k-i} f.\end{aligned}$$

The weight-0 part is the part that does not change the monomial degree, so it is Δ_k. Finally, note that $\Delta_k \neq 0$ as $\Delta_k(X^a) \neq 0$. □

Now suppose that $0 \le k \le (p-1)/2$. By the SL_2-invariant trace pairing on $\operatorname{End} V$, the element $\Delta_k \in \operatorname{soc}_{\mathrm{SL}_2}(\operatorname{End} V)$ induces an element $\delta_k \in (\operatorname{head}_{\mathrm{SL}_2}(\operatorname{End} V))^*$ that is zero on all irreducible constituents of $\operatorname{head}_{\mathrm{SL}_2}(\operatorname{End} V)$ except for $L(2k)$. Let $\pi_\ell \in \operatorname{End} V$ $(0 \le \ell \le a)$ denote the projection $X^i Y^{a-i} \mapsto \delta_{i\ell} X^i Y^{a-i}$.

Lemma 3.6. *If $0 \le k \le (p-1)/2$, then $\delta_k(\pi_\ell)$ is a polynomial in ℓ of degree exactly k.*

Proof. Note that $\delta_k(\pi_\ell) = \operatorname{tr}(\pi_\ell \circ \Delta_k)$ is the eigenvalue of Δ_k on $X^\ell Y^{a-\ell}$, and hence equals

$$\sum_{i=0}^{k} (-1)^{k-i} \binom{k}{i}^2 \ell(\ell-1) \cdots (\ell-i+1)(a-\ell)(a-\ell-1) \cdots (a-\ell-k+i+1).$$

This is a polynomial in ℓ of degree at most k. The coefficient of ℓ^k is $\sum_{i=0}^{k} \binom{k}{i}^2 = \binom{2k}{k} \not\equiv 0 \pmod p$, as $k < p/2$. □

Let us denote this polynomial by $p_k(z) \in \mathbb{F}_p[z]$.

Proof of Proposition 3.1. Recall that $(p-1)/2 \le a \le p-1$. Let $\mathcal{M}$ denote the span of the image of the p'-elements in $\operatorname{End} V$, and let M denote the image of $\mathcal{M}$ in $\operatorname{head}_{\mathrm{SL}_2(\mathbb{F}_p)}(\operatorname{End} V)$. Since $\mathcal{M}$ is $\mathrm{SL}_2(\mathbb{F}_p)$-stable, it suffices to show that $M = \operatorname{head}_{\mathrm{SL}_2(\mathbb{F}_p)}(\operatorname{End} V)$.

(a) Suppose that $a < p-1$. By Lemma 3.3, $\operatorname{head}_{\mathrm{SL}_2(\mathbb{F}_p)}(\operatorname{End} V) \cong \bigoplus_{i=0}^{(p-1)/2} L(2i)$. Suppose that M does not contain $L(2k)$ for some $0 \le k \le (p-1)/2$. Then δ_k annihilates the image of all p'-elements. The images of the diagonal elements of $\mathrm{SL}_2(\mathbb{F}_p)$ in $\operatorname{End}(V)$ span the subspace with basis

$$\pi_i \left(a - \frac{p-3}{2} \le i \le \frac{p-3}{2}\right) \quad \pi_i + \pi_{i+\frac{p-1}{2}} \left(0 \le i \le a - \frac{p-1}{2}\right).$$

Hence

$$\begin{aligned} p_k(i) &= 0 \quad \left(a - \frac{p-3}{2} \le i \le \frac{p-3}{2}\right), \\ p_k(i) + p_k\left(i + \frac{p-1}{2}\right) &= 0 \quad \left(0 \le i \le a - \frac{p-1}{2}\right). \end{aligned} \tag{3-4}$$

Now repeat the same argument with a nonsplit Cartan subgroup. After a linear change of variables $(X, Y) \mapsto (X', Y')$ over $\mathbb{F}_{p^2}$, this subgroup acts as

$$\left\{ \begin{pmatrix} x & \\ & x^p \end{pmatrix} : x \in \mathbb{F}_{p^2}^\times,\ x^{p+1} = 1 \right\}.$$

In this new basis of V we have corresponding elements Δ'_k, δ'_k, π'_ℓ. However, p_k is unchanged, as it is given by the explicit formula in the proof of Lemma 3.6. We thus get

$$\begin{aligned} p_k(i) &= 0 \quad \left(a - \frac{p-1}{2} \le i \le \frac{p-1}{2}\right), \\ p_k(i) + p_k\left(i + \frac{p+1}{2}\right) &= 0 \quad \left(0 \le i \le a - \frac{p+1}{2}\right). \end{aligned} \tag{3-5}$$

From (3-4) and (3-5) we get that $p_k(\ell) = 0$ for all $0 \le \ell \le a$. This contradicts the fact that $\deg p_k = k \le (p-1)/2 \le a$.

(b) Suppose that $a = p - 1$, so that $p \ge 5$ by our assumption. By Lemma 3.3, $\mathrm{head}_{\mathrm{SL}_2(\mathbb{F}_p)}(\mathrm{End}\, V) \cong \bigoplus_{i=0}^{(p-1)/2} L(2i) \oplus L(p-1)$.

(b1) Suppose that M does not contain $L(2k)$ for some $k \le (p-3)/2$. Then δ_k and δ'_k annihilate the image of all p'-elements, so by an argument analogous to the one in (a) we get

$$\begin{aligned} p_k(i) + p_k\left(i + \frac{p-1}{2}\right) &= 0 \quad \left(0 < i < \frac{p-1}{2}\right), \\ p_k(0) + p_k\left(\frac{p-1}{2}\right) + p_k(p-1) &= 0; \end{aligned} \tag{3-6}$$

$$\begin{aligned} p_k(i) + p_k\left(i + \frac{p+1}{2}\right) &= 0 \quad \left(0 \le i \le \frac{p-3}{2}\right), \\ p_k\left(\frac{p-1}{2}\right) &= 0. \end{aligned} \tag{3-7}$$

Then $p_k(z+1) - p_k(z)$ is a polynomial of degree $k - 1 < (p-1)/2$ with zeroes at $z = 0, 1, \dots, (p-5)/2$ and $z = (p+1)/2, (p+3)/2, \dots, p-2$. As $p-3 \ge (p-1)/2$, it follows that $p_k(z+1) \equiv p_k(z)$; hence by (3-7) we get $p_k(\ell) = 0$ for all $0 \le \ell \le p-1$, contradicting the fact that p_k has degree $0 \le k < p$.

(b2) Suppose that M does not contain $L(p-1)^{\oplus 2}$. Note first that the second copy of $L(p-1) \subset \operatorname{End}(V)$ is contained in the Weyl module $V(2p-2) \hookrightarrow T(2p-2)$. Using (3-2) we have $V(2p-2)|_{\mathrm{SL}_2(\mathbb{F}_p)} \cong L(p-1) \oplus M$, where $0 \to L(0) \to M \to L(p-3) \to 0$ is nonsplit. It follows using (3-3) that $V(2p-2)^{\mathcal{U}(\mathbb{F}_p)} = V(2p-2)^{\mathcal{U}}$ (both are two-dimensional). Hence there is a $\mathcal{U}(\mathbb{F}_p)$-fixed vector in the second copy of $L(p-1)$ of the form $v := (X(\partial/\partial Y))^{p-1} + c$ for some $c \in \overline{\mathbb{F}}_p$. We first compute c. Note that if V is an $\mathrm{SL}_2(\mathbb{F}_p)$-representation over $\overline{\mathbb{F}}_p$ and $v \neq 0$ is fixed by the Borel subgroup $B := \left(\begin{smallmatrix} * & * \\ & * \end{smallmatrix}\right) \subset \mathrm{SL}_2(\mathbb{F}_p)$, then v generates the p-dimensional irreducible representation of $\mathrm{SL}_2(\mathbb{F}_p)$ if and only if

$$\sum_{\mathrm{SL}_2(\mathbb{F}_p)/\left(\begin{smallmatrix} * & * \\ & * \end{smallmatrix}\right)} gv = 0 \iff \sum_{u \in \mathbb{F}_p} \begin{pmatrix} 1 & \\ -u & 1 \end{pmatrix} v + \begin{pmatrix} & -1 \\ 1 & \end{pmatrix} v = 0.$$

As in Lemma 3.5,

$$\begin{pmatrix} 1 & \\ -u & 1 \end{pmatrix} \cdot \Bigl(X \frac{\partial}{\partial Y}\Bigr)^{p-1} = (X - uY)^{p-1} \sum_{i=0}^{p-1} (-u)^i \Bigl(\frac{\partial}{\partial X}\Bigr)^i \Bigl(\frac{\partial}{\partial Y}\Bigr)^{p-1-i};$$

hence

$$\sum_{u \in \mathbb{F}_p} \begin{pmatrix} 1 & \\ -u & 1 \end{pmatrix} \cdot \Bigl[\Bigl(X \frac{\partial}{\partial Y}\Bigr)^{p-1} + c\Bigr] = -\Bigl[\Delta_{p-1} + Y^{p-1} \cdot \Bigl(\frac{\partial}{\partial X}\Bigr)^{p-1}\Bigr].$$

Since

$$\begin{pmatrix} & -1 \\ 1 & \end{pmatrix} \cdot \Bigl[\Bigl(X \frac{\partial}{\partial Y}\Bigr)^{p-1} + c\Bigr] = \Bigl(Y \frac{\partial}{\partial X}\Bigr)^{p-1} + c,$$

we deduce that $c = -1$.

Consider the annihilator $M^{\perp} \subset \operatorname{soc}_{\mathrm{SL}_2(\mathbb{F}_p)}(\operatorname{End} V)$ of M under the trace pairing. By assumption, $N := M^{\perp} \cap L(p-1)^{\oplus 2} \neq 0$. Let $\psi \in N^B - \{0\}$, so that by the previous paragraph we can write $\psi = \lambda (X(\partial/\partial Y))^{(p-1)/2} + \mu\bigl((X(\partial/\partial Y))^{p-1} - 1\bigr)$ for some $(\lambda, \mu) \in \overline{\mathbb{F}}_p^2 - \{0\}$. As $\psi \in M^{\perp}$, we get by a simple calculation that $0 = \operatorname{tr}\bigl(\left(\begin{smallmatrix} \alpha & \\ & \alpha^{-1} \end{smallmatrix}\right) \circ \psi\bigr) = -\mu$ for any $\alpha \in \mathbb{F}_p^{\times} - \{\pm 1\} \neq \varnothing$. Thus we may assume that $\psi = (X(\partial/\partial Y))^{(p-1)/2}$. As the $\mathrm{SL}_2(\mathbb{F}_p)$-subrepresentation of $\operatorname{End}(V)$ generated by ψ is the unique SL_2-subrepresentation $L(p-1) \subset \operatorname{End}(V)$, we see that N contains Δ_k and Δ'_k for $k = (p-1)/2$, so δ_k and δ'_k annihilate M. Now the argument of (b1) gives a contradiction. □

4. Weak adequacy for Chevalley groups

Lemma 4.1. *Suppose $(X, \Phi, X^{\vee}, \Phi^{\vee})$ is a reduced based root datum with Φ irreducible.*

(a) *If* Φ *is not of type* A_1, *then*

$$2\alpha_0^\vee \leq \sum_{\alpha \in \Phi_+} \alpha^\vee,$$

where $\alpha_0^\vee$ *is the highest coroot.*

(b) *If* Φ *is not of type* A_1, A_2, A_3, *or* B_2, *then*

$$4\beta_0^\vee \leq \sum_{\alpha \in \Phi_+} \alpha^\vee,$$

where $\beta_0^\vee$ *is the highest short coroot.*

Proof. (a) Let $\{\alpha_i : i = 1, \dots, r\}$ denote the simple roots. Then $\langle \alpha_0^\vee, \alpha_i \rangle \geq 0$ for all i and $\langle \alpha_0^\vee, \alpha_j \rangle > 0$ for some j. Since $\alpha_0^\vee \neq \alpha_j^\vee$ (as Φ is not of type A_1), $\beta^\vee := \alpha_0^\vee - \alpha_j^\vee \in \Phi^\vee$. Since $\alpha_0^\vee = \alpha_j^\vee + \beta^\vee$ it follows that $\beta^\vee > 0$. Also, $\alpha_j^\vee \neq \beta^\vee$, as Φ is reduced. Hence

$$2\alpha_0^\vee = \alpha_0^\vee + \alpha_j^\vee + \beta^\vee \leq \sum_{\alpha \in \Phi_+} \alpha^\vee.$$

(b) We pass to the dual root system to simplify notation. We want to show that

$$4\beta_0 \leq \sum_{\alpha \in \Phi_+} \alpha,$$

where β_0 is the highest short root. It suffices to express β_0 as sum of positive roots in three nontrivial ways that do not overlap (similarly as in the proof of (a)). If Φ is not simply laced, we only need two nontrivial ways because we can also use that $\beta_0 < \alpha_0$, where α_0 is the highest root.

In the following we use Bourbaki notation:

- Type A_{n-1} ($n \geq 5$):

$$\beta_0 = \varepsilon_1 - \varepsilon_n = (\varepsilon_1 - \varepsilon_i) + (\varepsilon_i - \varepsilon_n) \quad (1 < i < n).$$

- Type B_n ($n \geq 3$):

$$\beta_0 = \varepsilon_1 = (\varepsilon_1 - \varepsilon_i) + \varepsilon_i \quad (1 < i \leq n).$$

If $n = 3$, we also use $\beta_0 < \alpha_0 = \varepsilon_1 + \varepsilon_2$.

- Type C_n ($n \geq 3$):

$$\beta_0 = \varepsilon_1 + \varepsilon_2 = (\varepsilon_1 - \varepsilon_i) + (\varepsilon_2 + \varepsilon_i) = (\varepsilon_1 + \varepsilon_i) + (\varepsilon_2 - \varepsilon_i) \quad (2 < i \leq n).$$

If $n = 3$, we also use $\beta_0 < \alpha_0 = 2\varepsilon_1$.

- Type D_n $(n \geq 4)$:

$$\beta_0 = \varepsilon_1 + \varepsilon_2 = (\varepsilon_1 - \varepsilon_i) + (\varepsilon_2 + \varepsilon_i) = (\varepsilon_1 + \varepsilon_i) + (\varepsilon_2 - \varepsilon_i) \quad (2 < i \leq n).$$

- Type E_6:

$$\beta_0 = \tfrac{1}{2}(\varepsilon_1 + \varepsilon_2 + \varepsilon_3 + \varepsilon_4 + \varepsilon_5 - \varepsilon_6 - \varepsilon_7 + \varepsilon_8).$$

Note that $\beta_0 - (\varepsilon_i + \varepsilon_j)$ and $\varepsilon_i + \varepsilon_j$ are positive $(1 \leq i < j \leq 5)$.

- Type E_7:

$$\beta_0 = \varepsilon_8 - \varepsilon_7 = \tfrac{1}{2}\Bigl(\varepsilon_8 - \varepsilon_7 + \varepsilon_6 + \sum_{i=1}^{5}(-1)^{v(i)}\varepsilon_i\Bigr) + \tfrac{1}{2}\Bigl(\varepsilon_8 - \varepsilon_7 - \varepsilon_6 - \sum_{i=1}^{5}(-1)^{v(i)}\varepsilon_i\Bigr),$$

where $\sum_{i=1}^{5} v(i)$ is odd.

- Type E_8:

$$\beta_0 = \varepsilon_7 + \varepsilon_8 = (-\varepsilon_i + \varepsilon_7) + (\varepsilon_i + \varepsilon_8) \quad (1 \leq i < 7).$$

- Type F_4:

$$\beta_0 = \varepsilon_1 = (\varepsilon_1 - \varepsilon_i) + \varepsilon_i \quad (1 < i \leq 4).$$

- Type G_2:

$$\beta_0 = 2\alpha_1 + \alpha_2 = \alpha_1 + (\alpha_1 + \alpha_2)\beta_0 < 3\alpha_1 + \alpha_2\beta_0 < \alpha_0 = 3\alpha_1 + 2\alpha_2. \qquad \square$$

We now prove variants of several results in [Guralnick et al. 2012].

Lemma 4.2. *Suppose that $\mathscr{G}$ is a connected, simply connected, semisimple algebraic group over $\overline{\mathbb{F}}_p$ and $\Theta : \mathscr{G} \to \mathrm{GL}(V)$ a semisimple finite-dimensional representation. Let $\mathscr{G} > \mathscr{B} > \mathscr{T}$ denote a Borel subgroup and a maximal torus, and suppose that*

$$\text{for any irreducible component } V' \text{ of } V \text{ and for any two distinct weights } \mu_1, \mu_2 \text{ of } \mathscr{T} \text{ on } V', \text{ we have } \mu_1 - \mu_2 \notin pX(\mathscr{T}). \tag{4-1}$$

Then there exist connected, simply connected, semisimple algebraic subgroups $\mathscr{I}$ and $\mathscr{J}$ of $\mathscr{G}$ such that $\mathscr{G} = \mathscr{I} \times \mathscr{J}$, $\Theta(\mathscr{J}) = 1$, and Θ induces a central isogeny of $\mathscr{I}$ onto its image, which is a semisimple algebraic group. Moreover, assumption (4-1) *holds if for all irreducible constituents V' of V the highest weight of V' is p-restricted and either*

(i) $\dim V' < p$, *or*

(ii) $\dim V' \leq p$ *and either $p \neq 2$ or $\mathscr{G}$ has no* SL_2*-factor.*

Proof. Write $V = \bigoplus V_i$ with V_i irreducible and $\mathscr{G} = \prod_{s \in S} \mathscr{G}_s$ with each $\mathscr{G}_s$ almost simple. The last sentence of the proof of Lemma 4 in [Guralnick et al. 2012] together with (4-1) show that the conclusion of that lemma holds for $\Theta_i \colon \mathscr{G} \to \mathrm{GL}(V_i)$ for all i. Hence there exists $S_i \subset S$ such that $\ker \Theta_i = \prod_{s \in S_i} \mathscr{G}_s \times Z_i$, where Z_i is a central subgroup of $\prod_{s \notin S_i} \mathscr{G}_s$ (maybe nonreduced). Then $\ker \Theta = \bigcap \ker \Theta_i = \prod_{s \in \bigcap S_i} \mathscr{G}_s \times Z$, where Z is a central subgroup of $\prod_{s \notin \bigcap S_i} \mathscr{G}_s$. So we can take $\mathscr{I} = \prod_{s \notin \bigcap S_i} \mathscr{G}_s$ and $\mathscr{J} = \prod_{s \in \bigcap S_i} \mathscr{G}_s$.

To prove the last part, we may suppose that V is irreducible. So $V \cong \bigotimes_{s \in S} V_s$, where V_s is an irreducible $\mathscr{G}_s$-representation. It is easy to see that if (4-1) fails, then it fails for $\mathscr{G}_s \to \mathrm{GL}(V_s)$ for some $s \in S$, so we may assume that $\mathscr{G}$ is almost simple.

(a) First suppose that $\mathscr{G} \cong \mathrm{SL}_2$. The highest weight of V is $\left(\begin{smallmatrix} x & \\ & x^{-1} \end{smallmatrix}\right) \mapsto x^a$, for some $0 \le a \le p-1$, and $a \ne p-1$ if $p = 2$. Therefore the weights of $\operatorname{ad} V$ are $\left(\begin{smallmatrix} x & \\ & x^{-1} \end{smallmatrix}\right) \mapsto x^b$, where $b \in \{-2a, -2a+2, \dots, 2a-2, 2a\}$. It follows that (4-1) holds because $b \equiv 0 \pmod{p}$ implies that $b = 0$.

(b) Next suppose that $\mathscr{G} \not\cong \mathrm{SL}_2$. Let λ denote the highest weight of V; it is p-restricted by assumption. By Lemma 4.1(a) and Jantzen's inequality [1997, Lemma 1.2] we get

$$|\langle \mu, \beta^\vee \rangle| \le \langle \lambda, \alpha_0^\vee \rangle \le \tfrac{1}{2} \Big\langle \lambda, \sum_{\alpha > 0} \alpha^\vee \Big\rangle < \tfrac{1}{2} \dim V \le \frac{p}{2}$$

for all weights μ of V and all roots β. Hence $|\langle \mu_1 - \mu_2, \beta^\vee \rangle| < p$ for all root β and all weights μ_i of V, so (4-1) holds. □

Lemma 4.3. *Suppose that $\mathscr{G} \le \prod \mathrm{GL}(W_i)$ is a connected reductive group over $\overline{\mathbb{F}}_p$, where for all i the representation W_i is irreducible with p-restricted highest weight and has dimension $\le p$. Let $\mathscr{T}$ be a maximal torus and $\mathscr{U}$ the unipotent radical of a Borel subgroup of $\mathscr{G}$ that contains $\mathscr{T}$. Let $V = \bigoplus W_i$.*

(i) *The maps* exp *and* log *induce inverse isomorphisms of varieties between* $\operatorname{Lie} \mathscr{U} \le \operatorname{End}(V)$ *and* $\mathscr{U} \le \mathrm{GL}(V)$.

(ii) *For any positive root α we have* $\exp(\operatorname{Lie} \mathscr{U}_\alpha) = \mathscr{U}_\alpha$.

(iii) *The map* $\exp : \operatorname{Lie} \mathscr{U} \to \mathscr{U}$ *depends only on $\mathscr{G}$ and $\mathscr{U}$, but not on V, W_i, or the representation* $\mathscr{G} \hookrightarrow \mathrm{GL}(V)$.

(iv) *If θ is an automorphism of $\mathscr{G}$ that preserves $\mathscr{T}$ and $\mathscr{U}$, then we have a commutative diagram*

$$\begin{tikzcd}
\operatorname{Lie} \mathscr{U} \arrow[r, "d\theta"] \arrow[d, "\exp"'] & \operatorname{Lie} \mathscr{U} \arrow[d, "\exp"] \\
\mathscr{U} \arrow[r, "\theta"] & \mathscr{U}
\end{tikzcd}$$

Proof. The proof is the same as that of [Guralnick et al. 2012, Lemma 5], where there was an extra assumption on the μ_i. The assumption on the weights μ_i is *only* used to prove that $X_{\alpha,n}$ acts trivially on $V = \bigoplus W_i$ for all $n \geq p$. Fix any i. It is enough to show that $X_{\alpha,n}$ acts trivially on W_i for all $n \geq p$. So it is enough to show that W_i cannot have two weights λ and $\lambda + n\alpha$ ($\alpha \in \Phi$, $n \geq p$). As $\dim W_i \leq p$, it follows from [Jantzen 1997] that the weights of W_i are the same as those of the irreducible characteristic-0 representation of the same highest weight. But in characteristic 0 it is known that if λ and $\lambda + n\alpha$ are weights of an irreducible representation, then so are $\lambda, \lambda + \alpha, \lambda + 2\alpha, \ldots, \lambda + n\alpha$, so $\dim W_i > n \geq p$, contradicting the assumption. □

Proposition 4.4. *Let $p > 3$ be prime. Suppose that V is a finite-dimensional vector space over $\bar{\mathbb{F}}_p$ and that $G \leq \mathrm{GL}(V)$ is a finite subgroup that acts semisimply on V. Let $G^+ \leq G$ be the subgroup generated by p-elements of G. Then V is a semisimple G^+-module. Let $d \geq 1$ be the maximal dimension of an irreducible G^+-submodule of V. Suppose that $p > d$ and that G^+ is a central product of quasisimple Chevalley groups in characteristic p. Then there exists an algebraic group $\mathcal{G}$ over $\mathbb{F}_p$ and a semisimple representation $\Theta : \mathcal{G}_{/\bar{\mathbb{F}}_p} \to \mathrm{GL}(V)$ with the following properties*:

(i) *The connected component $\mathcal{G}^0$ is semisimple simply connected.*

(ii) $\mathcal{G} \cong \mathcal{G}^0 \rtimes H$, *where H is a finite group of order prime to p.*

(iii) $\Theta(\mathcal{G}(\mathbb{F}_p)) = G$.

(iv) $\ker(\Theta) \cap \mathcal{G}^0(\mathbb{F}_p)$ *is central in* $\mathcal{G}^0(\mathbb{F}_p)$.

Moreover, any highest weight of $\mathcal{G}^0_{/\bar{\mathbb{F}}_p}$ on V is p-restricted. Also, G does not have any composition factor of order p.

Proof. The proof is essentially identical to the proof of [Guralnick et al. 2012, Proposition 7]. We do not get $\langle \lambda, \alpha^\vee \rangle < (p-1)/2$ in Step 2, but this was only used to apply Lemmas 4 and 5 in [Guralnick et al. 2012]. By Lemmas 4.2 and 4.3 above one can bypass this assumption, as we now explain. Both times Lemma 4 in [Guralnick et al. 2012] is applied, condition (ii) in Lemma 4.2 holds. In Step 4 we can apply Lemma 4.3 instead of Lemma 5 in [Guralnick et al. 2012] because $\overline{\mathcal{I}}$ acts irreducibly on W_i and its highest weight is p-restricted (as $\mathcal{I} \to \overline{\mathcal{I}}$ is a central isogeny). Similarly we can avoid Lemma 5 in [Guralnick et al. 2012] in Step 5, noting that the highest weights of V' are Galois-conjugate to the highest weights of V and recalling that $\psi_{/\bar{\mathbb{F}}_p}$ is a central isogeny onto its image. Finally, note that (iv) follows by construction. □

Theorem 4.5. *Suppose that $p > 3$, V is a finite-dimensional vector space over $\overline{\mathbb{F}}_p$, and $G \leq \mathrm{GL}(V)$ is a finite subgroup that acts irreducibly on V. Let $G^+ \leq G$ be the subgroup generated by p-elements of G. Let $d \geq 1$ be the maximal dimension of an irreducible G^+-submodule of V. Suppose that $p > d$ and that G^+ is a central product of quasisimple Chevalley groups in characteristic p. Then the set of p'-elements of G spans* ad V *as an $\overline{\mathbb{F}}_p$-vector space.*

Remark 4.6. Theorem 4.5 generalizes [Guralnick et al. 2012, Theorem 9]. We take the opportunity to point out a small gap in the last paragraph of the proof of that theorem. In the notation there, it is implicitly assumed that (i) $r(T(\mathbb{F}_l)) \subset r(H)$, so that the span of $r(H)$ equals the span of $r(T(\overline{\mathbb{F}}_l)H)$, and (ii) H normalizes the pair (B, T). Both assumptions are satisfied provided that when we apply [Guralnick et al. 2012, Proposition 7] in the proof of Theorem 9 there, we take r, $G = G^0 \rtimes H$, $B, T, \ldots$ as constructed in the proof of that proposition.

Proof. Without loss of generality $d > 1$. Let Θ: $\mathscr{G}_{/\overline{\mathbb{F}}_p} \to \mathrm{GL}(V)$ be as in Proposition 4.4. Then $V = \bigoplus W_i$, where W_i is an irreducible $\mathscr{G}^0_{/\overline{\mathbb{F}}_p}$-subrepresentation with p-restricted highest weight. Write $\mathscr{G}^0_{/\overline{\mathbb{F}}_p} \cong \mathscr{G}_1 \times \cdots \times \mathscr{G}_r$, where $\mathscr{G}_i$ is almost simple over $\overline{\mathbb{F}}_p$. Let $\mathscr{G}^0 > \mathscr{B} > \mathscr{T}$ denote a Borel subgroup and a maximal torus, and let Φ denote the roots of $\mathscr{G}^0_{/\overline{\mathbb{F}}_p}$ with respect to $\mathscr{T}_{/\overline{\mathbb{F}}_p}$.

(a) We consider the case where one of the W_i (equivalently any) is tensor-decomposable as a $\mathscr{G}^0_{/\overline{\mathbb{F}}_p}$-representation. Note that $W_i \cong X_{i1} \boxtimes \cdots \boxtimes X_{ir}$, where X_{ij} is an irreducible $\mathscr{G}_j$-representation with p-restricted highest weight. Since $\dim X_{ij} \leq p-1$, its highest weight lies in the lowest alcove [Jantzen 1997; Serre 1994]; hence X_{ij} is tensor-indecomposable (as the highest weight is in the lowest alcove, we are reduced to the characteristic-0 case, where this is well known). Hence our assumption implies that $X_{ij} \not\cong \mathbb{1}$ for at least two values of j. Hence $\dim X_{ij} \leq (p-1)/2$ for all i, j. Therefore $X^*_{ik} \otimes X_{jk}$ is a semisimple $\mathscr{G}_k$-representation by [Serre 1994], so End V is a semisimple $\mathscr{G}^0_{/\overline{\mathbb{F}}_p}$-representation. Moreover, all its highest weights are p-restricted: this follows exactly as in Step 2 of the proof of [Guralnick et al. 2012, Proposition 7] (use that $\dim X_{ij} \leq (p-1)/2$). Hence any $\mathscr{G}^0(\mathbb{F}_p)$-submodule of End V is a $\mathscr{G}^0(\overline{\mathbb{F}}_p)$-submodule.

Furthermore, arguing as in Step 2 of the proof of [Guralnick et al. 2012, Proposition 7] for each $\mathscr{G}_k$, we deduce that for all weights μ of the maximal torus $\mathscr{T}_{/\overline{\mathbb{F}}_p}$ on V we have $|\langle \mu, \alpha^\vee \rangle| < (p-1)/2$ for all $\alpha \in \Phi$. We conclude as in the last paragraph of the proof of [Guralnick et al. 2012, Theorem 9].

(b) We consider the case when $\mathscr{G}^0_{/\overline{\mathbb{F}}_p}$ has no factors of type A_1, A_2, A_3, or B_2. We claim $|\langle \mu, \alpha^\vee \rangle| < (p-1)/4$ for all weights μ of $\mathscr{T}_{/\overline{\mathbb{F}}_p}$ on V and for all short coroots $\alpha^\vee \in \Phi^\vee$. It suffices to show that $\langle \lambda, \beta_0^\vee \rangle < (p-1)/4$ for all highest weights λ of $\mathscr{T}_{/\overline{\mathbb{F}}_p}$ on V and all highest short coroots $\beta_0^\vee$ (one for each component of $\mathscr{G}^0_{/\overline{\mathbb{F}}_p}$). So it is enough to show that if $\mathscr{G}'$ is an almost simple, simply connected group over

$\bar{\mathbb{F}}_p$, not of type A_1, A_2, A_3, or B_2, then $\langle\lambda, \beta_0^\vee\rangle < (p-1)/4$ for all p-restricted weights λ of $\mathscr{G}'$ such that $\dim L(\lambda) < p$, where $\beta_0^\vee$ is the highest short coroot of $\mathscr{G}'$. But this follows from Lemma 4.1(b) and Jantzen's inequality, and this proves the claim.

Since the short coroots span $X_*\big(\mathscr{T}_{/\bar{\mathbb{F}}_p}\big) \otimes \mathbb{Q}$ over $\mathbb{Q}$, Lemma 3 of [Guralnick et al. 2012] plus the claim show that distinct weights of $\mathscr{T}_{/\bar{\mathbb{F}}_p}$ on $\operatorname{End} V$ (and V) remain distinct on $\mathscr{T}(\mathbb{F}_p)$. Then [Guralnick 2012a, Lemma 1.1] shows that any $\mathscr{G}^0(\mathbb{F}_p)$-subrepresentation of $\operatorname{End} V$ is $\mathscr{G}^0(\bar{\mathbb{F}}_p)$-stable, so we can conclude as in the last paragraph of the proof of Theorem 9 in [Guralnick et al. 2012].

(c) If neither (a) nor (b) apply, then the W_i are tensor-indecomposable; in particular, the almost simple factors of $\mathscr{G}^0_{/\bar{\mathbb{F}}_p}$ are pairwise isomorphic. (Write $\mathscr{G}^0 \cong \prod \mathscr{H}_i$, where the subgroups $\mathscr{H}_i$ are almost simple over $\mathbb{F}_p$. Note that, for each i, $\mathscr{G}^0(\mathbb{F}_p)$ acts irreducibly on W_i with all but one $\mathscr{H}_j(\mathbb{F}_p)$ acting trivially. As $\mathscr{G}(\mathbb{F}_p)$ is irreducible on V and, by Proposition 4.4(iv), the subgroups $\mathscr{H}_i(\mathbb{F}_p)$ are pairwise isomorphic and, as $p > 3$, so are the $\mathscr{H}_i$.) Hence $\mathscr{G}^0_{/\bar{\mathbb{F}}_p} \cong \mathrm{SL}_2^n$, SL_3^n, SL_4^n, or Sp_4^n for some $n \geq 1$.

(d) We consider the case where $\mathscr{G}^0_{/\bar{\mathbb{F}}_p} \cong \mathrm{SL}_3^n$, SL_4^n, or Sp_4^n. We claim that for all weights μ of $\mathscr{T}_{/\bar{\mathbb{F}}_p}$ on V and for all $\alpha \in \Phi$,

$$|\langle\mu, \alpha^\vee\rangle| < \tfrac{1}{2}(p-1). \tag{4-2}$$

To see this, note that $|\langle\mu, \alpha^\vee\rangle| \leq \langle\lambda, \alpha_0^\vee\rangle$ for some highest weight λ of V and some highest coroot $\alpha_0^\vee$. Applying Lemma 4.1(a) to the component Φ_j of Φ such that $\alpha_0^\vee \in \Phi_j^\vee$ and using Jantzen's inequality, we get

$$\langle\lambda, \alpha_0^\vee\rangle \leq \tfrac{1}{2} \sum_{\Phi_{j,+}} \langle\lambda, \alpha^\vee\rangle < \tfrac{1}{2}(p-1).$$

By Lemma 3 in [Guralnick et al. 2012], (4-2) shows that distinct weights of $\mathscr{T}_{/\bar{\mathbb{F}}_p}$ on V remain distinct on $\mathscr{T}(\mathbb{F}_p)$. As usual, it thus suffices to show that $\operatorname{End} V$ is a semisimple $\mathscr{G}^0_{/\bar{\mathbb{F}}_p}$-module with p-restricted highest weights. We can argue independently for each factor of $\mathscr{G}^0_{/\bar{\mathbb{F}}_p}$, so it will suffice to show that if X, Y are nontrivial irreducible $\mathscr{G}'$-representations which are conjugate by $\operatorname{Aut}(\mathscr{G}')$ (with $\mathscr{G}' = \mathrm{SL}_3$, SL_4, or Sp_4) with p-restricted highest weights λ, λ' of dimension less than p, then $X \otimes Y$ is semisimple with p-restricted highest weights. By [Jantzen 1997; Serre 1994], λ and λ' lie in the lowest alcove, so $\operatorname{ch} L(\lambda)$ and $\operatorname{ch} L(\lambda')$ are given by Weyl's character formula.

In the following, note that $\langle\lambda, \beta_0^\vee\rangle = \langle\lambda', \beta_0^\vee\rangle$.

If $\mathscr{G}' \cong \mathrm{SL}_4$, write $\lambda = r\varpi_1 + s\varpi_2 + t\varpi_3$ $(r, s, t \geq 0)$, where ϖ_i is the i-th fundamental weight. Then

$$\begin{aligned} p - 1 \geq \dim L(\lambda) &= \frac{[(r+1)(s+1)(t+1)][(r+s+2)(s+t+2)](r+s+t+3)}{2 \cdot 2 \cdot 3} \\ &\geq \frac{(r+s+t+1)(r+s+t+2)(r+s+t+3)}{2 \cdot 3}. \end{aligned}$$

If $\langle \lambda, \beta_0^\vee \rangle = r+s+t \geq (p-1)/4$, then

$$p - 1 \geq \frac{\frac{p+3}{4} \cdot \frac{p+7}{4} \cdot \frac{p+11}{4}}{6}.$$

Equivalently, $(p-5)[(p+13)^2 - 292] \leq 0$, i.e., $p = 5$. In this case, equality holds throughout so $\lambda = \varpi_1$ or ϖ_3. The maximal weight of $X \otimes Y$, namely $2\varpi_1$ or $\varpi_1 + \varpi_3$ or $2\varpi_3$, lies in the closure of the lowest alcove. Then $X \otimes Y$ is semisimple by the linkage principle (or just [Jantzen 2003, Proposition II.4.13]) and it has p-restricted highest weights. If $\langle \lambda, \beta_0^\vee \rangle < (p-1)/4$ the argument in (b) goes through instead.

If $\mathscr{G}' \cong \mathrm{Sp}_4$, write $\lambda = r\varpi_1 + s\varpi_2$ with $r, s \geq 0$ (type B_2). Then

$$\begin{aligned} p - 1 \geq \dim L(\lambda) &= \frac{[(r+1)(s+1)](r+s+2)(2r+s+3)}{6} \\ &\geq \frac{(r+s+1)(r+s+2)(r+s+3)}{6}. \end{aligned}$$

If $\langle \lambda, \beta_0^\vee \rangle = r+s \geq (p-1)/4$, then $p = 5$ as above and $\lambda = \varpi_2$. Again, $X \otimes Y$ has maximal weight $2\varpi_2$ lying in the closure of the lowest alcove; hence $X \otimes Y$ is semisimple with p-restricted highest weights. If $\langle \lambda, \beta_0^\vee \rangle < (p-1)/4$ we are done as in (b).

If $\mathscr{G}' \cong \mathrm{SL}_3$, write $\lambda = r\varpi_1 + s\varpi_2$ $(r, s \geq 0)$. If $r + s \geq (p-1)/2$, then

$$\begin{aligned} p - 1 \geq \dim L(\lambda) &= \frac{[(r+1)(s+1)](r+s+2)}{2} \\ &\geq \frac{(r+s+1)(r+s+2)}{2} \geq \frac{\frac{p+1}{2} \cdot \frac{p+3}{2}}{2}. \end{aligned}$$

Equivalently $(p-2)^2 + 7 \leq 0$, which is impossible. Hence $r + s \leq (p-3)/2$, which implies that the maximal weight of $X \otimes Y$ lies in the lowest alcove. So $X \otimes Y$ is semisimple with p-restricted highest weights.

(e) We consider the case where $\mathscr{G}^0_{/\overline{\mathbb{F}}_p} \cong \mathrm{SL}_2^n$ and each W_i is tensor-indecomposable as a $\mathscr{G}^0_{/\overline{\mathbb{F}}_p}$-representation. Here, $\mathscr{G}^0(\mathbb{F}_p) \cong \mathrm{SL}_2(\mathbb{F}_q)^m$, where $[\mathbb{F}_q : \mathbb{F}_p] \cdot m = n$. Also, V is irreducible, each W_i is tensor-indecomposable, and SL_2 has no outer automorphism. It follows that $V \cong \left[\bigoplus_{i=1}^{\ell} V_i\right]^{\oplus k}$ as $\mathscr{G}^0_{/\overline{\mathbb{F}}_p}$-representations, where each V_i is of the form $\mathbb{1} \boxtimes \cdots \boxtimes V_0 \boxtimes \cdots \boxtimes \mathbb{1}$ (precisely one factor is V_0), the V_i are pairwise nonisomorphic, and V_0 is an irreducible SL_2-representation such that $1 < \dim V_0 < p$ with p-restricted highest weight.

(e1) We claim that the span of the p'-elements of $\mathscr{G}^0(\mathbb{F}_p)$ in $\operatorname{End} V$ contains the span of $\mathscr{T}(\bar{\mathbb{F}}_p)$ in $\operatorname{End} V$.

If $q > p$, note from the description of V_i above that distinct weights of $\mathscr{T}_{/\bar{\mathbb{F}}_p}$ on V remain distinct on $\mathscr{T}(\mathbb{F}_p)$. Hence the span of $\mathscr{T}(\mathbb{F}_p)$ in $\operatorname{End} V$ equals the span of $\mathscr{T}(\bar{\mathbb{F}}_p)$ in $\operatorname{End} V$.

If $q = p$, we will show that the p'-elements of $\mathscr{G}^0(\mathbb{F}_p)$ span the same subspace of $\operatorname{End} V$ as does all of $\mathscr{G}^0(\bar{\mathbb{F}}_p)$. First, from Proposition 4.4(iv), we deduce that $\ell = n$. As the V_i are distinct and irreducible $\mathscr{G}^0_{/\bar{\mathbb{F}}_p}$-representations, by the Artin–Wedderburn theorem we need to show that the p'-elements in $\mathscr{G}^0(\mathbb{F}_p)$ span $\prod_{i=1}^n \operatorname{End}(V_i)$, or equivalently its $\mathscr{G}^0(\mathbb{F}_p)$-head. (Note that the span of the p'-elements is $\mathscr{G}^0(\mathbb{F}_p)$-stable.) By Lemma 3.3, we see that the n representations $\operatorname{head}_{\mathscr{G}^0(\mathbb{F}_p)}(\operatorname{End}(V_i))$ have no $\mathscr{G}^0(\mathbb{F}_p)$-irreducible constituent in common except for the trivial direct summand of scalar matrices in $\operatorname{End}(V_i)$. By Proposition 3.1, the image of the p'-elements span $\operatorname{End}(V_i)$ for any i. Hence it suffices to show that the image of the p'-elements under the map

$$\begin{aligned}\mathscr{G}^0(\mathbb{F}_p) &\to \bar{\mathbb{F}}_p^n,\\ g &\mapsto (\operatorname{tr}(g|_{V_i}))_{i=1}^n\end{aligned}$$

spans $\mathbb{F}_p^n$. Note that as $1 < \dim V_0 < p$, the split torus $\left(\begin{smallmatrix} * & \\ & * \end{smallmatrix}\right) < \mathrm{SL}_2(\mathbb{F}_p)$ has a nontrivial eigenvalue χ on V_0 with multiplicity 1 or 2. Given $1 \le i \le n$, there exists an element in $\mathbb{F}_p[\mathscr{T}(\mathbb{F}_p)]$ that projects onto the $1 \otimes \cdots \otimes \chi \otimes \cdots \otimes 1$ eigenspace in any $\mathscr{T}(\mathbb{F}_p)$-representation, so as $p > 2$ it has nonzero trace on V_i but is zero on $\bigoplus_{j \ne i} V_j$. This proves the claim.

(e2) We claim that $\operatorname{head}_{\mathscr{G}^0_{/\bar{\mathbb{F}}_p}}(\operatorname{End} V) = \operatorname{head}_{\mathscr{G}^0(\mathbb{F}_p)}(\operatorname{End} V)$, and moreover that any highest weight of this representation is p-restricted.

If $d \le (p+1)/2$, then by [Serre 1994] $\operatorname{End} V$ is a semisimple $\mathscr{G}^0_{/\bar{\mathbb{F}}_p}$-module and clearly any highest weight of $\operatorname{End} V$ is p-restricted. The claim follows.

If $d \ge (p+3)/2$, note that head is compatible with direct sums, so we can consider each $V_i^* \otimes V_j$ separately. If $i \ne j$, then $V_i^* \otimes V_j$ is irreducible with p-restricted highest weight. If $i = j$, from Lemma 3.3 we get

$$\operatorname{head}_{\mathrm{SL}_2}(V_0^* \otimes V_0) \cong L(0) \oplus L(2) \oplus \cdots \oplus L(p-1).$$

In particular, any highest weight of $\operatorname{head}_{\mathscr{G}^0_{/\bar{\mathbb{F}}_p}}(V_i^* \otimes V_i)$ is p-restricted. By Lemma 3.3, showing

$$\operatorname{head}_{\mathscr{G}^0_{/\bar{\mathbb{F}}_p}}(V_i^* \otimes V_i) = \operatorname{head}_{\mathscr{G}^0(\mathbb{F}_p)}(V_i^* \otimes V_i)$$

is equivalent (after a Frobenius twist) to showing that

$$\mathrm{head}_{\mathrm{SL}_2}(T(2p-2-2j)) = \mathrm{head}_{\mathrm{SL}_2(\mathbb{F}_q)}(T(2p-2-2j))$$

for $0 \leq j \leq (p-3)/2$. If $q = p$ this follows from Lemma 3.3, as $d < p$. This in turn implies the statement for $q > p$, as any irreducible SL_2-constituent of $T(2p-2-2j)$ restricts irreducibly to $\mathrm{SL}_2(\mathbb{F}_q)$ if $q > p$ and semisimply to $\mathrm{SL}_2(\mathbb{F}_p)$. This proves the claim.

(e3) Now, let $\mathcal{M}$ denote the span of the images of the p'-elements of $\mathscr{G}(\mathbb{F}_p)$ in $\mathrm{head}_{\mathscr{G}^0(\mathbb{F}_p)}(\mathrm{End}(V))$. Note that $\mathcal{M}$ is a $\mathscr{G}^0(\mathbb{F}_p)$-subrepresentation. To prove weak adequacy, it suffices to show that $\mathcal{M} = \mathrm{head}_{\mathscr{G}^0(\mathbb{F}_p)}(\mathrm{End}(V))$. By (e2) we have that $\mathrm{head}_{\mathscr{G}^0_{/\bar{\mathbb{F}}_p}}(\mathrm{End}(V)) = \mathrm{head}_{\mathscr{G}^0(\mathbb{F}_p)}(\mathrm{End}(V))$ and that distinct irreducible $\mathscr{G}^0_{/\bar{\mathbb{F}}_p}$-subrepresentations of $\mathrm{head}_{\mathscr{G}^0_{/\bar{\mathbb{F}}_p}}(\mathrm{End}(V))$ restrict to distinct irreducible $\mathscr{G}^0(\mathbb{F}_p)$-representations. Hence, any $\mathscr{G}^0(\mathbb{F}_p)$-subrepresentation of $\mathrm{head}_{\mathscr{G}^0_{/\bar{\mathbb{F}}_p}}(\mathrm{End}(V))$ is $\mathscr{G}^0(\bar{\mathbb{F}}_p)$-stable. By (e1), we know that $\mathcal{M}$ contains the span of the image of $\mathscr{T}(\bar{\mathbb{F}}_p) \cdot H$. Therefore, by Lemma 8 in [Guralnick et al. 2012], $\mathcal{M}$ contains the span of the image of $\mathscr{G}(\bar{\mathbb{F}}_p)$. But the latter span equals $\mathrm{head}_{\mathscr{G}^0_{/\bar{\mathbb{F}}_p}}(\mathrm{End}(V))$ by the Artin–Wedderburn theorem. □

5. Weak adequacy in cross-characteristic

Recall that, given a finite-dimensional absolutely irreducible representation $\Phi : G \to \mathrm{GL}(V)$, the pair (G, V) is called *weakly adequate* if $\mathrm{End}(V)$ equals

$$\mathcal{M} := \langle \Phi(g) \in \Phi(G) : \Phi(g) \text{ semisimple} \rangle_k.$$

Assume $k = \bar{k}$ has characteristic p. First, we recall:

Lemma 5.1 [Guralnick 2012b, Lemma 2.3]. *If $G < \mathrm{GL}(V)$ is p-solvable and $p \nmid \dim V$, then (G, V) is weakly adequate.*

In general, a key tool to prove weak adequacy is provided by the following criterion:

Lemma 5.2. *Let V be a finite-dimensional vector space over k and $G \leq \mathrm{GL}(V)$ a finite irreducible subgroup. Write $V|_{G^+} = e\sum_{i=1}^{t} W_i$, where the G^+-modules W_i are irreducible and pairwise nonisomorphic. Suppose there is a subgroup $Q \leq G^+$ such that*

(i) *$\{Q^g : g \in G\} = \{Q^x : x \in G^+\}$, and*

(ii) *the Q-modules W_i are irreducible and pairwise nonisomorphic,*

then $\mathbf{N}_G(Q)$ is an irreducible subgroup of $\mathrm{GL}(V)$. If, furthermore,

(iii) *$\mathbf{N}_{G^+}(Q)$ is a p'-group,*

then (G, V) is weakly adequate.

Proof. The condition (i) is equivalent to the equality $G = NG^+$, where $N := \mathbf{N}_G(Q)$. Since G/G^+ is a p'-group, this implies that N is a p'-group if $\mathbf{N}_{G^+}(Q)$ is a p'-group. By the Artin–Wedderburn theorem, it therefore suffices to show that N is irreducible on V.

Set $V_i = eW_i$ so that $V = \bigoplus_{i=1}^m V_i$, $G_1 := I_G(W_1) = \mathrm{Stab}_G(V_1)$ the inertia group of the G^+-module W_1 in G, and $N_1 := N \cap G_1$. Then we have that $G_1 = N_1G^+$ and $[N : N_1] = [G : G_1] = t$. Trivially, the condition (ii) implies that the N^+-modules W_i $(1 \le i \le t)$, are irreducible and pairwise nonisomorphic, where we set $N^+ := \mathbf{N}_{G^+}(Q)$. It now follows that $N_1 = I_N(W_1)$, the inertia group of the N^+-module W_1 in N; moreover, N acts transitively on $\{V_1, \dots, V_t\}$, and $V|_N = \mathrm{Ind}_{N_1}^N(V_1|_{N_1})$. By the Clifford correspondence, it suffices to show that the N_1-module V_1 is irreducible.

Let Φ denote the corresponding representation of G_1 on V_1 and let Ψ denote the corresponding representation of G^+ on W_1. By [Navarro 1998, Theorem 8.14], there is a projective representation Ψ_1 of G_1 such that

$$\Psi_1(n) = \Psi(n), \quad \Psi_1(xn) = \Psi_1(x)\Psi_1(n), \quad \Psi_1(nx) = \Psi_1(n)\Psi_1(x)$$

for all $n \in G^+$ and $x \in G_1$. Let α denote the factor set on G_1/G^+ induced by Ψ_1. By [Navarro 1998, Theorem 8.16], there is an e-dimensional projective representation Θ of G_1/G^+ with factor set α^{-1} such that $\Phi(g) = \Theta(g) \otimes \Psi_1(g)$ for all $g \in G_1$. (Here and in what follows, we will write $\Theta(g)$ instead of $\Theta(gG^+)$.) Since Φ is irreducible, Θ is irreducible.

Observe that N_1/N^+ is canonically isomorphic to G_1/G^+. Restricting to N_1, we then have that $\Phi(g) = \Theta(g) \otimes \Psi_1(g)$ for all $g \in N_1$, $\Psi_1(n) = \Psi(n)$ for all $n \in N^+$, $(\Psi_1)_{N_1}$ is a projective representation of N_1 with factor set α, and Θ_{N_1/N^+} is a projective representation of N_1/N^+ with factor set α^{-1}. Furthermore, Θ_{N_1/N^+} is irreducible. It follows by [Navarro 1998, Theorem 8.18] that Φ_{N_1} is irreducible, as stated. □

In certain cases we will also need the following modification of Lemma 5.2:

Lemma 5.3. *Let V be a finite-dimensional vector space over k and $G \le \mathrm{GL}(V)$ a finite irreducible subgroup. Write $V|_{G^+} = e\sum_{i=1}^t W_i$, where the G^+-modules W_i are irreducible and pairwise nonisomorphic. Suppose there is a subgroup $Q \le G^+$ with the following properties*:

(i) $\{Q^g : g \in G\} = \{Q^x : x \in G^+\}$.

(ii) *$W_i \cong A_i \oplus B_i$ as Q-modules, where all the $2t$ Q-modules A_i and B_j are irreducible and pairwise nonisomorphic.*

If $\{A_1, \dots, A_t\}$ and $\{B_1, \dots, B_t\}$ are two disjoint N-orbits on $\mathrm{IBr}(Q)$ for $N := \mathbf{N}_G(Q)$, then we have that $V_N \cong A \oplus B$ as N-modules, where A and B are irreducible, $A_Q \cong e\big(\bigoplus_{i=1}^t A_i\big)$, and $B_Q \cong e\big(\bigoplus_{i=1}^t B_i\big)$. On the other hand, if $\{A_1, B_1, \dots, A_t, B_t\}$ forms a single N-orbit, then N is irreducible on V.

Proof. Again, the condition (i) implies that $G = NG^+$. Adopt the notation G_1, N_1, N^+, Φ, Ψ, Ψ_1, α of the proof of Lemma 5.2. As shown there, there is an irreducible e-dimensional projective representation Θ of G_1/G^+ with factor set α^{-1} such that $\Phi(g) = \Theta(g) \otimes \Psi_1(g)$ for all $g \in G_1$. Also, N_1/N^+ is canonically isomorphic to G_1/G^+. According to (ii), $(W_i)_Q \cong A_i \oplus B_i$, with $A_i \not\cong B_i$. Hence we can decompose $(V_i)_Q = C_i \oplus D_i$, where $(C_i)_Q \cong eA_i$ and $(D_i)_Q \cong eB_i$, and define $A := \bigoplus_{i=1}^t C_i$, $B := \bigoplus_{i=1}^t D_i$.

(a) First we consider the case where $\{A_1, \dots, A_t\}$ and $\{B_1, \dots, B_t\}$ are two disjoint N-orbits. Then, for any $x \in N$, every composition factor of the Q-module xA is of the form A_j for some j, and every composition factor of B is of the form $B_{j'}$ for some j'. Hence we conclude that $xA = A$, and similarly $xB = B$. Thus A and B are N-modules. Certainly, N permutes $C_1, \dots, C_t$ transitively and N_1 fixes C_1. But $t = [N : N_1]$; hence $N_1 = \mathrm{Stab}_N(C_1)$ and $A = \mathrm{Ind}_{N_1}^N(C_1)$. Since $(C_i)_Q = eA_i$ and the Q-modules A_i are pairwise nonisomorphic, we also see that $N_1 = I_N(A_1)$. Similarly, $N_1 = I_N(B_1)$ and $B = \mathrm{Ind}_{N_1}^N(D_1)$. Therefore, by the Clifford correspondence, it suffices to prove that the N_1-modules C_1 and D_1 are irreducible.

Recall the decompositions $(W_1)_Q = A_1 \oplus B_1$ and $\Phi(g) = \Theta(g) \otimes \Psi_1(g)$ for all $g \in G_1$. Without loss, we may assume that the representation Ψ of G^+ on W_1 is written with respect to some basis $(v_1, \dots, v_{a+b})$ which is the union of a basis $(v_1, \dots, v_a)$ of A_1 and a basis $(v_{a+1}, \dots, v_{a+b})$ of B_1. Since $\Phi(g) = \Theta(g) \otimes \Psi_1(g)$ for all $g \in G_1$ acting on V_1, we can also choose a basis

$$\{u_i \otimes v_j : 1 \le i \le e, 1 \le j \le a+b\}$$

of V_1 such that $\Theta(g)$ is written with respect to $\{u_1, \dots, u_e\}$ and $\Psi_1(g)$ is written with respect to $\{v_1, \dots, v_{a+b}\}$. For any $x \in N_1$, writing $\Theta(x) = (\theta_{i'i})$ and $\Psi_1(x) = (\psi_{j'j})$, we then have that

$$\Phi(x)(u_i \otimes v_j) = \sum_{i',j'} \theta_{i'i}\psi_{j'j} u_{i'} \otimes v_{j'}.$$

Recall we are also assuming that the Q-modules A_1 and B_1 are not N-conjugate. Therefore, $\Phi(x)$ fixes each of

$$C_1 = \langle u_i \otimes v_j : 1 \le i \le e, 1 \le j \le a \rangle_k, \quad D_1 = \langle u_i \otimes v_j : 1 \le i \le e, a+1 \le j \le a+b \rangle_k.$$

In particular, $\theta_{i'i}\psi_{j'j} = 0$ whenever $j' > a$ and $j \le a$. Now if $\psi_{j'j} \ne 0$ for some $j \le a$ and some $j' > a$, we must have $\theta_{i'i} = 0$ for all i, i', i.e., $\Theta(x) = 0$, a contradiction. Similarly, $\psi_{j'j} = 0$ whenever $j > a$ and $j' \le a$. Therefore, we can write

$$\Psi_1(x) = \mathrm{diag}(\Psi_{1A}(x), \Psi_{1B}(x)) \tag{5-1}$$

in the chosen basis $\{v_1, \dots, v_{a+b}\}$. It also follows that $\Psi(y)$ fixes each of A_1 and B_1 for all $y \in N^+$, i.e., A_1 and B_1 are irreducible N^+-modules.

Now, $\Psi_1(x)\Psi_1(y) = \alpha(x, y)\Psi_1(xy)$ for any $x, y \in N_1$. Together with (5-1) this implies that

$$\Psi_{1A}(x)\Psi_{1A}(y) = \alpha(x, y)\Psi_{1A}(xy), \quad \Psi_{1B}(x)\Psi_{1B}(y) = \alpha(x, y)\Psi_{1B}(xy),$$

i.e., both Ψ_{1A} and Ψ_{1B} are projective representations of N_1 with factor set α. Since $\Psi_1(x) = \Psi(x)$ for all $x \in N^+$ and (5-1) certainly holds for $x \in N^+$, we also see that Ψ_{1A} extends the representation of N^+ on A_1, and similarly Ψ_{1B} extends the representation of N^+ on B_1. By [Navarro 1998, Theorem 8.18], the formulae

$$\Phi_A(g) := \Theta(g) \otimes \Psi_{1A}(g), \quad \Phi_B(g) := \Theta(g) \otimes \Psi_{1B}(g)$$

for $g \in N_1$ define irreducible (linear) representations of N_1 of dimension ea and eb (acting on C_1 and D_1, respectively), and so we are done.

(b) Next we consider the case N acts transitively on $\{A_1, \dots, B_t\}$. In this case, $N_1^\circ := I_N(A_1)$ has index $2t$ in N and is contained in N_1. Note that there is some $g \in N$ such that $B_1^g \cong A_1$ as Q-modules. Certainly, such g must belong to N_1, and also g interchanges C_1 and D_1. Applying the arguments of (a) to g, we see that $\Psi_1(g)$ interchanges A_1 and B_1. It follows that $(\Psi_1)_{N_1}$ is irreducible. In turn, this implies by [Navarro 1998, Theorem 8.18] that Φ_{N_1} is irreducible, i.e., N_1 is irreducible on V_1. But $[N_1 : N_1^\circ] = 2$ and $V_1 = C_1 \oplus D_1$ as N_1°-modules. Hence C_1 is an irreducible N_1°-module. Since $N_1^\circ = I_N(A_1)$ and C_1 is the A_1-isotypic component for Q on V, we conclude by Clifford's theorem that N is irreducible on V. □

Lemma 5.4. *Let V be a finite-dimensional vector space over k and $G \le \mathrm{GL}(V)$ a finite irreducible subgroup. Write $V|_{G^+} = e\sum_{i=1}^t W_i$, where the G^+-modules W_i are irreducible and pairwise nonisomorphic. Suppose there is a subgroup $Q \le G^+$ with the following properties*:

(a) $\{Q^g : g \in G\} = \{Q^x : x \in G^+\}$.

(b) $(W_i)_Q \cong A_i \oplus B_{i1} \oplus \cdots \oplus B_{is}$, *where $a := \dim A_i \neq \dim B_{il}$ for all $1 \le i \le t$ and all $1 \le l \le s$, the Q-modules A_i, B_{il} are irreducible, and the Q-modules A_i $(1 \le i \le t)$ are pairwise nonisomorphic.*

Then the following statements hold:

(i) *Denoting $N := \mathbf{N}_G(Q)$, we have that $V_N \cong A \oplus B$ as N-modules, where A is irreducible, $A_Q \cong e\big(\bigoplus_{i=1}^t A_i\big)$ and $B_Q \cong e\big(\bigoplus_{i,l} B_{il}\big)$.*

(ii) *Assume that N is a p'-subgroup, G^+ is perfect, and that, whenever $i \neq j$, no G^+-composition factor of $W_i^* \otimes W_j$ is trivial. If all G^+-composition factors of* $\mathrm{End}(V)/\mathcal{M}$ *(if there are any) are trivial, then in fact* $\mathcal{M} = \mathrm{End}(V)$.

Proof. (i) follows from same proof as Lemma 5.3. For (ii), note that since G^+ is perfect it must act trivially on $\mathscr{E}/\operatorname{End}(V)$, i.e., $\mathcal{M} \supseteq [\operatorname{End}(V), G^+]$. It follows that

$$\mathcal{M} \supseteq [\mathscr{E}_{1i}, G^+] \tag{5-2}$$

for $\mathscr{E}_{1i} := \operatorname{End}(V_i)$. On the other hand, $\operatorname{Hom}(V_i, V_j) = [\operatorname{Hom}(V_i, V_j), G^+]$, and so

$$\mathcal{M} \supseteq \bigoplus_{1 \le i \ne j \le t} \operatorname{Hom}(V_i, V_j).$$

It suffices to show that $\mathcal{M} \supseteq \mathscr{E}_{11}$ (and so by symmetry $\mathcal{M} \supseteq \mathscr{E}_{1i}$ for all i).

Applying the Artin–Wedderburn theorem to N, we see that

$$\mathcal{M} \supset \operatorname{End}(A) \supseteq \operatorname{End}(C_1), \tag{5-3}$$

where $(C_1)_Q \cong eA_1$. Also, as in the proof of Lemma 5.3, we can write

$$V_1 = U \otimes W_1, \quad C_1 = U \otimes A_1,$$

such that U affords a projective representation Θ of $G_1/G^+ \cong N_1/N^+$, W_1 affords a projective representation Ψ_1 of G_1 that extends the representation Ψ of G^+ on W_1, and $\Phi(g) = \Theta(g) \otimes \Psi_1(g)$ for the representation Φ of G_1 on V_1.

Note that the subspace $\operatorname{End}(W_1)^\circ$ consisting of all transformations with trace 0 is a G^+-submodule X of codimension 1 of $\operatorname{End}(W_1)$. Next, as a G^+-module,

$$\mathscr{E}_{11} = \operatorname{End}(V_1) \cong \operatorname{End}(U) \otimes \operatorname{End}(W_1) \cong e^2 \operatorname{End}(W_1).$$

So we see that $\mathscr{E}_{11}^+ := \operatorname{End}(U) \otimes \operatorname{End}(W_1)^\circ$ is a submodule of codimension e^2 in $\mathscr{E}_{11}$, and all G^+-composition factors of $\mathscr{E}_{11}/\mathscr{E}_{11}^+$ are trivial. Since G^+ is perfect, it follows that $\mathscr{E}_{11}^+ \supseteq [\mathscr{E}_{11}, G^+]$. But

$$\begin{aligned}\dim \operatorname{Hom}_{kG^+}(\mathscr{E}_{11}, k) &= e^2 \dim \operatorname{Hom}_{kG^+}(\operatorname{End}(W_1), k) \\ &= e^2 \dim \operatorname{Hom}_{kG^+}(W_1, W_1) = e^2.\end{aligned}$$

Hence, $\mathscr{E}_{11}^+ = [\mathscr{E}_{11}, G^+]$, and so by (5-2) we have that

$$\mathcal{M} \supset \mathscr{E}_{11}^+ = \operatorname{End}(U) \otimes \operatorname{End}(W_1)^\circ.$$

On the other hand, by (5-3) we also have that

$$\mathcal{M} \supset \operatorname{End}(C_1) = \operatorname{End}(U) \otimes \operatorname{End}(A_1).$$

Obviously, $\operatorname{End}(W_1)^\circ + \operatorname{End}(A_1) = \operatorname{End}(W_1)$ (as $\operatorname{End}(A_1)$ contains elements with nonzero trace). Hence we conclude that $\mathcal{M} \supseteq \mathscr{E}_{11}$, as stated. □

We also record the following trivial observation:

Lemma 5.5. *Let E be a kG-module of finite length with submodules X and M. Suppose that $N \le G$ and that the N-modules X and E/X share no common composition factor* (*up to isomorphism*). *Suppose that the multiplicity of each composition factor C of X is at most its multiplicity as a composition factor of M* (*for instance, X is a subquotient of M*). *Then $M \supseteq X$.*

Proof. The hypothesis implies that the N-modules X and E/M have no common composition factor. On the other hand, $X/(M \cap X) \cong (X+M)/M \subseteq E/M$ as N-modules. It follows that $X = M \cap X$, as stated. □

Proposition 5.6. *Let* (G, V) *be as in the extraspecial case* (ii) *of Theorem 2.4. Then* (G, V) *is weakly adequate.*

Proof. Decompose $V_{G^+} = e\sum_{i=1}^{t} W_i$ as in Lemma 5.2. Recall by Theorem 2.4(ii) that $R := \boldsymbol{O}_{p'}(G^+) \lhd G$ acts irreducibly on each W_i. First we show that if $i \neq j$ then the R-modules W_i and W_j are nonisomorphic. Assume the contrary: $W_i \cong W_j$ as R-modules. Then the G^+-modules W_i and W_j are two extensions to $G^+ \rhd R$ of the R-module W_i. By [Navarro 1998, Corollary 8.20], $W_j \cong W_i \otimes U$ (as G^+-modules) for some one-dimensional G^+/R-module U. But G^+/R is perfect by Theorem 2.4(ii). It follows that U is the trivial module and $W_i \cong W_j$ as G^+-modules, a contradiction.

For future use, we also show that the G^+-module W_i has a unique complex lift. Indeed, the existence of a complex lift χ of W_i was established in [Blau and Zhang 1993, Theorem B]. Suppose that χ' is another complex lift. Then both χ and χ' are extensions of $\alpha := \chi_R$, and α is irreducible since R is irreducible on W_i. Then, again by [Navarro 1998, Corollary 8.20], $\chi' = \chi\lambda$ for some linear character λ of G^+/R, and so $\lambda = 1_{G^+/R}$ as G^+/R is perfect. Thus $\chi' = \chi$.

Now we write $G^+/R = S_1 \times \cdots \times S_n$ with $S_i \cong S$ as in Theorem 2.4(ii). We will define the subgroup $Q > R$ of G^+ with

$$Q/R = Q_1 \times \cdots \times Q_n$$

as follows. If $p = 17$ and $S = \mathrm{PSL}_2(17)$, then Q_i is a dihedral subgroup of order 16. If $S = \Omega_{2a}^-(2^b)'$ with $ab = n$ (and $a \ge 2$ as S is simple nonabelian), then Q_i is chosen to be the first parabolic subgroup (which is the normalizer of an isotropic 1-space in the natural module $\mathbb{F}_{2^b}^{2a}$, of index $(2^n+1)(2^{n-b}-1)/(2^b-1)$). If $S = \mathrm{Sp}_4(2)' \cong \mathsf{A}_6$, choose $Q_i \cong 3^2 : 4$, of order 36. If $S = \mathrm{Sp}_4(2^b)$ with $b \ge 2$, we fix a prime divisor r of b and choose $Q_i \cong \mathrm{Sp}_4(2^{b/r})$. For $S = \mathrm{Sp}_{2a}(2^b)$ with $a \ge 3$, we choose Q_i to be the first parabolic subgroup (which is the normalizer of a 1-space in the natural module $\mathbb{F}_{2^b}^{2a}$, of index $2^{2n}-1$). In all cases, our choice of Q_i ensures that the p'-subgroup Q_i is a maximal subgroup of S_i and, moreover, that the S_i-conjugacy class of Q_i is $\mathrm{Aut}(S_i)$-invariant. In particular, $\boldsymbol{N}_{G^+}(Q) = Q$. Also note that any

$g \in G$ normalizes R and permutes the simple factors S_i of G^+/R; in fact, its action on G^+/R belongs to $\mathrm{Aut}(S^n) = \mathrm{Aut}(S) \wr \mathsf{S}_n$. It follows that Q satisfies conditions (i) and (iii) of Lemma 5.2. Since $W_i \not\cong W_j$ as R-modules for $i \neq j$, $W_i \not\cong W_j$ as Q-modules as well. Hence we are done by Lemma 5.2. □

Theorem 5.7. *Suppose* (G, V) *is as in case* (i) *of Theorem 2.4. Then* (G, V) *is weakly adequate unless one of the following possibilities occurs for the group* $H < \mathrm{GL}(W)$ *induced by the action of* G^+ *on any irreducible* G^+*-submodule* W *of* V:

(i) $p = (q^n - 1)/(q - 1)$, *with* $n \geq 3$ *a prime, and* $H \cong \mathrm{PSL}_n(q)$.

(ii) $(p, H, \dim W) = (5, 2\mathsf{A}_7, 4), (7, 6_1{\cdot}\mathrm{PSL}_3(4), 6), (11, 2M_{12}, 10)$, *or* $(19, 3J_3, 18)$.

Proof. (a) Arguing as in part (b) of the proof of Theorem 2.4 (and using its notation), we see that for each i there is some k_i such that the kernel K_i of the action of G^+ on W_i contains $\prod_{j \neq k_i} L_j$, and so G^+ acts on W_i as $H_i = L_{k_i}/(L_{k_i} \cap K_i)$. We aim to define a subgroup $Q > \mathbf{Z}(G^+)$ of G^+ such that

$$Q = Q_1 * Q_2 * \cdots * Q_n,$$

where $Q_i/\mathbf{Z}(L_i) \leq L_i/\mathbf{Z}(L_i) =: S_i \cong S$ and Q satisfies the conditions of Lemma 5.2. In fact, we will find Q_i so that the p'-subgroup $Q_i/\mathbf{Z}(L_i)$ is a maximal subgroup of S_i and, moreover, the S_i-conjugacy class of $Q_i/\mathbf{Z}(L_i)$ is $\mathrm{Aut}(S_i)$-invariant. To this end, we first find Q_1; then for each $i > 1$, we can fix an element $g_i \in G$ conjugating S_1 to S_i and choose $Q_i = Q_1^{g_i}$. Since G fixes G^+ and $\mathbf{Z}(G^+)$ and induces a subgroup of $\mathrm{Aut}(S) \wr \mathsf{S}_n$ while acting on $G^+/\mathbf{Z}(G^+) \cong S^n$, it follows that Q satisfies conditions (i) and (iii) of Lemma 5.2. Moreover, in the cases where

$$G^+ = L_1 \times \cdots \times L_n \cong H^n, \tag{5-4}$$

then we can also write $Q = Q_1 \times \cdots \times Q_n$, which simplifies some parts of the arguments.

(b1) Suppose first that we are in the case (b1) of Theorem 2.1. Assume that $(H, p) = (\mathrm{Sp}_{2n}(q), (q^n + 1)/2)$. Here H is the full cover of S, so (5-4) holds. Then we choose Q_i to be the last parabolic subgroup of $\mathrm{Sp}_{2n}(q)$ (which is the stabilizer of a maximal totally isotropic subspace in the natural module $\mathbb{F}_q^{2n}$). Then $Q_i/\mathbf{Z}(L_i)$ is a maximal p'-subgroup of S_i and, moreover, the S_i-conjugacy class of $Q_i/\mathbf{Z}(L_i)$ is $\mathrm{Aut}(S_i)$-invariant. By [Guralnick et al. 2002, Theorem 2.1], the H-module W is one of the two Weil modules of dimension $(q^n - 1)/2$ of $H \cong \mathrm{Sp}_{2n}(q)$. Furthermore, by [Guralnick et al. 2002, Lemma 7.2], the restrictions of these two Weil modules of L_i to Q_i are irreducible and nonisomorphic. It follows that if $W_i \not\cong W_j$ as G^+-modules and $K_i = K_j$, then $W_i \not\cong W_j$ as Q-modules. On the other hand, if $K_i \neq K_j$, then $k_i \neq k_j$ (otherwise we would have $K_i = K_j = \prod_{a \neq k_i} L_a$ since L_{k_i} acts faithfully on V_i), whence $K_i \cap Q \neq K_j \cap Q$

and so $W_i \not\cong W_j$ as Q-modules. Thus condition (ii) of Lemma 5.2 holds as well, and so we are done.

Consider the case $(H, p) = (2Ru, 29)$. Then H is the full cover of S and so (5-4) holds. Choose Q_i to be a unique (up to L_i-conjugacy) maximal subgroup of type $(2 \times \mathrm{PSU}_3(5)) : 2$ of L_i; see [Conway et al. 1985]. Note that L_i has a unique conjugacy class $3A$ of elements of order 3. By using [Jansen et al. 1995] and [Conway et al. 1985], and comparing the character values at this class $3A$, we see that L_i has two irreducible p-Brauer characters φ_1, φ_2, of degree 28, and their restrictions to Q_i yield the same irreducible character of Q_i. Now, if $K_i \neq K_j$, then $k_i \neq k_j$ (as W is a faithful kH-module), whence $K_i \cap Q \neq K_j \cap Q$ and so $W_i \not\cong W_j$ as Q-modules. Suppose that $K_i = K_j$. By Clifford's theorem, there is some $g \in G$ such that $W_j = W_i^g$ as G^+-modules, and so as L_i-modules as well. In this case, g induces an automorphism of $L_i = 2Ru$. But all automorphisms of Ru are inner [Conway et al. 1985], so W_i and W_j afford the same Brauer L_i-character, whence $W_i \cong W_j$ as G^+-modules. Thus condition (ii) of Lemma 5.2 holds as well, and so we are done.

Next assume that $(H, p) = (\mathrm{SU}_n(q), (q^n + 1)/(q + 1))$; in particular $n \geq 3$ is odd. Since H is simple, (5-4) holds. Then we choose Q_i to be the last parabolic subgroup of $\mathrm{SU}_n(q)$ (which is the stabilizer of a maximal totally isotropic subspace in the natural module $\mathbb{F}_{q^2}^n$). Then the p'-subgroup Q_i is a maximal subgroup of S_i and the S_i-conjugacy class of Q_i is $\mathrm{Aut}(S_i)$-invariant. Next, if $n \geq 5$ then by [Guralnick et al. 2002, Theorem 2.7], $\mathrm{PSU}_n(q)$ has a unique irreducible module over k of dimension $p - 1 = (q^n - q)/(q + 1)$, which is again a Weil module. Furthermore, Lemmas 12.5 and 12.6 of [Guralnick et al. 2002] show that the restriction of this Weil module of L_i to Q_i is irreducible. The same conclusions hold in the case $n = 3$ by Theorem 4.2 and the proof of Remark 3.3 of [Geck 1990]. It follows that if $W_i \not\cong W_j$ as G^+-modules, then $K_i \neq K_j$, $k_i \neq k_j$ (as W is a faithful kH-module), whence $K_i \cap Q \neq K_j \cap Q$ and so $W_i \not\cong W_j$ as Q-modules. Thus condition (ii) of Lemma 5.2 holds, and so we are done again.

Note that we have listed the cases $(p, H) = (5, 2\mathsf{A}_7)$ and $(19, 3J_3)$ as possible exceptions in (ii).

(b2) Suppose now that we are in the case (b2) of Theorem 2.1; in particular, $p = 7$ and $\dim W = 6$. Assume first that $S = \mathsf{A}_7$. The arguments in the cases $L_i \cong 3\mathsf{A}_7$ and $6\mathsf{A}_7$ are the same, so we assume $L_i \cong 6\mathsf{A}_7$. Then we choose $Q_i/\boldsymbol{Z}(L_i)$ to be a unique (up to L_i-conjugacy) maximal subgroup of type A_6. Restricting the faithful reducible complex characters of degree 4 of $2\mathsf{A}_7$ and 6 of $3\mathsf{A}_7$ [Conway et al. 1985] to Q_i (and comparing character values at elements of order 3), we see that $Q_i \cong 6\mathsf{A}_6$. Now, using [Jansen et al. 1995], one can check that L_i has six irreducible p-Brauer characters of degree 6, and their restrictions to Q_i are irreducible and distinct. Now we can argue as in the case of $\mathrm{Sp}_{2n}(q)$.

Assume now that $H = 2J_2$, and so (5-4) holds. Choose $Q_i/\boldsymbol{Z}(L_i)$ to be a unique (up to L_i-conjugacy) maximal subgroup of type $3 \cdot \mathrm{PGL}_2(9)$ (see [Conway et al. 1985]). Also, using [Jansen et al. 1995], one can check that L_i has two irreducible p-Brauer characters of degree 6, and their restrictions to Q_i are irreducible and distinct. Now we can argue as in the case of $\mathrm{Sp}_{2n}(q)$.

Suppose that $H = 6_1 \cdot \mathrm{PSU}_4(3)$. We will prove weak adequacy of (G, V) in two steps. First, we choose $M_i/\boldsymbol{Z}(L_i)$ to be a unique (up to S_i-conjugacy) maximal subgroup of type $T \cong \mathrm{SU}_3(3)$ of S_i (see [Conway et al. 1985]). Since T has trivial Schur multiplier, we have that $M_i \cong Z_i \times T$, where $Z_i := \boldsymbol{Z}(L_i)$. According to [Jansen et al. 1995], L_i has two irreducible p-Brauer characters of degree 6, which have different central characters. It follows that their restrictions to M_i are irreducible and distinct. Setting

$$M := M_1 * \cdots * M_n,$$

we conclude by Lemma 5.2 that $N := \boldsymbol{N}_G(M)$ is irreducible on V; furthermore, $N/M \cong G/G^+$ is a p'-group. But note that M is *not* a p'-group. Now, at the second step, we note that $M \lhd N$ and $N^+ := \boldsymbol{O}^{p'}(N) = \boldsymbol{O}^{p'}(M) \cong T^n$, and, moreover, each irreducible N^+-submodule in V has dimension 6. Also, recall that $T = \mathrm{SU}_3(3)$ and $p = 7$. So we are done by applying the result of the case of $\mathrm{PSU}_n(q)$.

(b3) Consider the case (b3) of Theorem 2.1; in particular, $p = 11$ and $\dim W = 10$. Putting the possibility $H = 2M_{12}$ as a possible exception in (ii), we may assume that $H = M_{11}$ or $2M_{22}$. Then we choose $Q_i/\boldsymbol{Z}(L_i)$ to be a unique (up to S_i-conjugacy) maximal subgroup of type $M_{10} \cong \mathsf{A}_6 \cdot 2_3$ or $\mathrm{PSL}_3(4)$, respectively, of S_i (see [Conway et al. 1985]). In the former case, H is simple and so (5-4) holds. In the latter case, since $H_j \cong 2M_{22}$, we see that the cyclic group $\boldsymbol{Z}(L_i) \lhd G^+$ must act as a central subgroup of order 1 or 2 of H_j on each W_j. Hence the faithfulness of G on V implies that $L_i \cong 2M_{22}$. Since $\mathrm{PSL}_3(4)$ has no nontrivial representation of degree 10, we must have that $Q_i \cong 2 \cdot \mathrm{PSL}_3(4)$ is quasisimple in this case. Now, using [Jansen et al. 1995], one can check that L_i has two irreducible p-Brauer characters of degree 10, and their restrictions to Q_i are irreducible and distinct. Hence we can argue as in the case of $\mathrm{Sp}_{2n}(q)$.

(b4) Suppose we are in the case (b4) of Theorem 2.1; in particular, $p = 13$ and $\dim W = 12$. Since H is the full cover of S, (5-4) holds. Then we may choose $Q_i/\boldsymbol{Z}(L_i)$ to be a unique (up to S_i-conjugacy) maximal subgroup of type $J_2 : 2$ or $\mathrm{SL}_3(4) : 2_3$, respectively, of S_i (see [Conway et al. 1985]). Since J_2 has no nontrivial representation of degree 12, in the former case we must have that $Q_i \cong (C_3 \times 2J_2) \cdot C_2$, where $C_3 = \boldsymbol{O}_3(\boldsymbol{Z}(L_i))$ and the C_2 induces an outer automorphism of J_2. Also, according to [Breuer et al.], L_i has precisely two irreducible p-Brauer characters of degree 12, which differ at the central elements of order 3. Using [Jansen et al.

1995], we can now check that the restrictions of these two characters to Q_i are irreducible and distinct, and then finish as in the case of $\mathrm{Sp}_{2n}(q)$. In the latter case of $L_i = 2\mathrm{G}_2(4)$, since $\mathrm{SL}_3(4)$ has no nontrivial representation of degree 12 we must have that $Q_i \cong (6 \cdot \mathrm{PSL}_3(4)) \cdot 2_3$. Now, using [Jansen et al. 1995], one can check that L_i has a unique irreducible p-Brauer character of degree 12, and its restriction to Q_i is irreducible. Hence we can argue as in the case of $\mathrm{PSU}_n(q)$.

(c) Now we consider case (c) of Theorem 2.1; in particular, $\dim W = p-2$. Assume that $H = \mathsf{A}_p$ with $p \geq 5$. Since H is simple, (5-4) holds. Choosing $Q_i \cong \mathsf{A}_{p-1}$, we see that the p'-subgroup Q_i is a maximal subgroup of S_i and that the S_i-conjugacy class of Q_i is $\mathrm{Aut}(S_i)$-invariant. Also, using [Guralnick and Tiep 2005, Lemma 6.1] for $p \geq 17$ and [Jansen et al. 1995] for $p \leq 13$, we see that H has a unique irreducible kH-module of dimension $p-2$, and the restriction of this module to A_{p-1} is irreducible. Now we can argue as in the case of $\mathrm{PSU}_n(q)$.

Next suppose that $(H, p) = (\mathrm{SL}_2(q), q+1)$; in particular, p is a Fermat prime and H is simple so (5-4) holds. Choosing $Q_i < \mathrm{SL}_2(q)$ to be a Borel subgroup (of index p), we see that Q_i is a maximal p'-subgroup of S_i and that the S_i-conjugacy class of Q_i is $\mathrm{Aut}(S_i)$-invariant. Also, using [Burkhardt 1976], one can check that H has a unique irreducible kH-module of dimension $p-2$, and the restriction of this module to Q_i is irreducible. Now argue as above.

Suppose that $p=5$ and $H = 3\mathsf{A}_6$ or $3\mathsf{A}_7$. First we note that $L_i \cong 3\mathsf{A}_s$ with $s=6$ or $s=7$ respectively. If not, then $L_i \cong 6\mathsf{A}_s$, but then, since $H_j \cong 3\mathsf{A}_s$, $\boldsymbol{O}_2(\boldsymbol{Z}(L_i))$ must act trivially on all W_i, contradicting the faithfulness of G on V. Now we choose Q_i to be the normalizer of a Sylow 3-subgroup in L_i, of order 108. It is straightforward to check that $\boldsymbol{N}_{S_i}(Q_i/\boldsymbol{Z}(L_i)) = Q_i/\boldsymbol{Z}(L_i)$ and that the S_i-conjugacy class of Q_i is $\mathrm{Aut}(S_i)$-invariant. Also, using [Jansen et al. 1995], one can check that H has two irreducible 5-Brauer characters of degree $p-2$, and the restrictions of them to Q_i are irreducible and distinct. Now we can argue as in the case of $\mathrm{Sp}_{2n}(q)$.

Suppose that $(p, H) = (11, M_{11})$ or $(23, M_{23})$. Again (5-4) holds as H is simple. Choosing Q_i to be $M_{10} \cong \mathsf{A}_6 \cdot 2_3$ (in the notation of [Conway et al. 1985]) or M_{22}, respectively, we have that Q_i is a unique maximal subgroup of L_i of the given p'-order up to L_i-conjugacy. Furthermore, L_i has a unique irreducible kH-module of dimension $p-2$, and the restriction of this module to Q_i is irreducible. Now argue as in the case of $\mathrm{PSU}_n(q)$.

(d) Finally, we consider case (d) of Theorem 2.1: $(p, H) = (11, J_1)$ or $(7, 2\mathsf{A}_7)$. Then we choose $Q_i/\boldsymbol{Z}(L_i)$ to be a unique (up to S_i-conjugacy) maximal subgroup of type $2^3 : 7 : 3$ or A_6, respectively (see [Conway et al. 1985]). In the former case, H is simple, and so (5-4) holds. In the latter case, note that L_i is $2\mathsf{A}_7$. If not, then $L_i \cong 6\mathsf{A}_7$, but then, since $H_j \cong 2\mathsf{A}_7$, $\boldsymbol{O}_3(\boldsymbol{Z}(L_i))$ must act trivially on all W_i, contradicting the faithfulness of G on V. It then follows that $Q_i \cong 2\mathsf{A}_6$ (as any

4-dimensional $k\mathsf{A}_6$-representation is trivial). Now, using [Jansen et al. 1995] one can check that H has a unique irreducible p-Brauer character of given degree, and its restriction to Q_i is irreducible. Now we can argue as in the case of $\mathrm{PSU}_n(q)$. □

Next we use Lemma 5.3 to handle three exceptions listed in Theorem 5.7:

Proposition 5.8. *In the case* $(p, H, \dim W) = (19, 3J_3, 18)$ *of* (ii) *of Theorem 5.7,* (G, V) *is weakly adequate.*

Proof. Since H is the full cover of S, we have $G^+ = L_1 \times \cdots \times L_n \cong H^n$. Since H acts faithfully on W, for each i there is some k_i such that the kernel K_i of the action of G^+ on W_i is precisely $\prod_{j \neq k_i} L_j$. We define a subgroup Q of G^+ such that

$$Q = Q_1 \times \cdots \times Q_n,$$

where $Q_i/\mathbf{Z}(L_i) \cong \mathrm{SL}_2(16) : 2$ is a maximal subgroup of $S_i = L_i/\mathbf{Z}(L_i) \cong J_3$. Since $\mathrm{SL}_2(16)$ has a trivial Schur multiplier and $\mathbf{Z}(L_i) \leq \mathbf{Z}(Q_i)$, we have that $Q_i \cong 3 \times (\mathrm{SL}_2(16) : 2)$. Furthermore, the S_i-conjugacy class of Q_i is $\mathrm{Aut}(S_i)$-invariant. Hence Q satisfies the condition (i) of Lemma 5.3.

Using [GAP 2004], one can check that L_i has exactly four irreducible 19-Brauer characters $\varphi_1, \varphi_2, \varphi_3, \varphi_4$ of degree 18, and $(\varphi_j)_{Q_i} = \alpha_j + \beta_j$, with α_j of degree 1 with kernel $[Q_i, Q_i]$, β_j of degree 17, and the β_j are all distinct. Now we show that Q fulfills the condition (ii) of Lemma 5.3. Suppose that $W_i \not\cong W_j$ as G^+-modules. Then Q acts coprimely on W_i, with character $\tilde{\alpha}_i + \tilde{\beta}_i$, where $\tilde{\alpha}_i$ has degree 1 and $\tilde{\beta}_i$ has degree 17. If $k_i \neq k_j$, then $\tilde{\alpha}_i$ and $\tilde{\alpha}_j$ have different kernels and so are distinct, and likewise $\tilde{\beta}_i$ and $\tilde{\beta}_j$ are distinct. Suppose now that $k_i = k_j$. Then, because of the condition $W_i \not\cong W_j$, we may assume that W_i and W_j both have kernel $K := L_2 \times \cdots \times L_n$, and afford L_1-characters φ_k and φ_l with $1 \leq k \neq l \leq 4$. Since the G-module V is irreducible, we have $W_i \not\cong W_j \cong W_i^g$ for some $g \in G$ which stabilizes K and $G^+/K \cong L_1$ but does not induce an inner automorphism of L_1. The latter condition implies that g interchanges the two classes of elements of order 5 and inverts the central element of order 3 of L_1 [Conway et al. 1985]. The same is true for Q_1. It follows that $\alpha_k \neq \alpha_l$, $\beta_k \neq \beta_l$, and so

$$\tilde{\alpha}_i \neq \tilde{\alpha}_j, \quad \tilde{\beta}_i \neq \tilde{\beta}_j,$$

as claimed.

By Lemma 5.3, $V \cong A \oplus B$ as a module over the p'-group $N := \mathbf{N}_G(Q)$, where the N-modules A and B are irreducible of dimension e and $17e$, respectively. Hence, by the Artin–Wedderburn theorem applied to N,

$$\mathcal{M} := \langle \Phi(g) : g \in G, g \text{ semisimple} \rangle_k$$

contains $\mathscr{A} := \mathrm{End}(A) \oplus \mathrm{End}(B) = (A^* \otimes A) \oplus (B^* \otimes B)$ (if Φ denotes the representation of G on V). As in Lemma 5.3 and its proof, write $A = \bigoplus_{i=1}^t C_i = e\bigl(\bigoplus_{i=1}^t A_i\bigr)$ and $B = \bigoplus_{i=1}^t D_i = e\bigl(\bigoplus_{i=1}^t B_i\bigr)$ as Q-modules, where A_i affords $\tilde{\alpha}_i$ and B_i affords $\tilde{\beta}_i$. Hence, the complement to $\mathscr{A}$ in $\mathrm{End}(V)$ affords the Q-character

$$\Delta := e^2 \sum_{i,j=1}^{t} (\tilde{\alpha}_i \overline{\tilde{\beta}_j} + \tilde{\beta}_i \overline{\tilde{\alpha}_j}).$$

In particular, all irreducible constituents of $\Delta_{[Q,Q]}$ are of degree 17. The same must be true for the quotient $\mathrm{End}(V)/\mathscr{M}$.

As a G^+-module,

$$\mathrm{End}(V) = \bigoplus_{i,j=1}^{t} (V_i^* \otimes V_j) \cong e^2 \biggl(\bigoplus_{i,j=1}^{t} W_i^* \otimes W_j \biggr).$$

Observe that the G^+-module $W_i^* \otimes W_j$ is irreducible of dimension 324 if $k_i \neq k_j$. Assume that $k_i = k_j$, say $k_i = k_j = 1$. Using [GAP 2004] one can check that no irreducible constituent of $\varphi_k \overline{\varphi_l}$ for $1 \le k, l \le 4$ can consist of only irreducible characters of degree 17 while restricted to the subgroup $\mathrm{SL}_2(16)$ of $L_1 = 3J_3$. It follows that no irreducible constituent of the G^+-module $\mathrm{End}(V)$ can consist of only irreducible constituents of dimension 17 while restricted to $[Q, Q]$. Hence $\mathscr{M} = \mathrm{End}(V)$. □

Proposition 5.9. *In the case* $(p, H, \dim W) = (11, 2M_{12}, 10)$ *of* (ii) *of Theorem 5.7,* (G, V) *is weakly adequate.*

Proof. As H is the full cover of S, we have that $G^+ = L_1 \times \cdots \times L_n \cong H^n$. Since H acts faithfully on W, for each i there is some k_i such that the kernel K_i of the action of G^+ on W_i is precisely $\prod_{j \neq k_i} L_j$. We define a subgroup Q of G^+ such that

$$Q = Q_1 \times \cdots \times Q_n,$$

where $Q_i/\mathbf{Z}(L_i) \cong 2_+^{1+4} \cdot \mathrm{S}_3$ is a maximal subgroup of $S_i = L_i/\mathbf{Z}(L_i) \cong M_{12}$. Note that the S_i-conjugacy class of Q_i is $\mathrm{Aut}(S_i)$-invariant. Hence Q satisfies condition (i) of Lemma 5.3.

Using [GAP 2004], one can check that L_i has exactly two irreducible 11-Brauer characters φ_1, φ_2 of degree 10, and $(\varphi_j)_{Q_i} = \alpha + \beta_j$, with α of degree 4, β_j of degree 6, and $\beta_1 \neq \beta_2$. Furthermore, $Z_i := \mathbf{Z}(Q_i) \cong C_2^2$, and

$$\alpha_{Z_i} = 4\lambda, \quad (\beta_j)_{Z_i} = 6\mu, \tag{5-5}$$

where λ and μ are the two linear characters of Z_i that are faithful on $\mathbf{Z}(L_i) < Z_i$. In particular,

$$(\alpha\beta_j)_{Z_i} = 24\nu \tag{5-6}$$

with $\nu := \lambda\mu \neq 1_{Z_i}$.

Now we show that Q fulfills condition (ii) of Lemma 5.3. Suppose that $W_i \not\cong W_j$ as G^+-modules. Then Q acts on W_i, with character $\tilde{\alpha}_i + \tilde{\beta}_i$, where $\tilde{\alpha}_i(1) = 4$ and $\tilde{\beta}_i(1) = 6$. If $k_i \neq k_j$, then $\tilde{\alpha}_i$ and $\tilde{\alpha}_j$ have different kernels and so are distinct, and likewise $\tilde{\beta}_i$ and $\tilde{\beta}_j$ are distinct. In particular, in this case $W_i^* \otimes W_j$ is also irreducible. Suppose now that $k_i = k_j$. Then, we may assume that W_i and W_j both have kernel $K := L_2 \times \cdots \times L_n$, and afford L_1-characters φ_k and φ_l with $1 \leq k, l \leq 2$. Since the G-module V is irreducible, we have $W_j \cong W_i^g$ for some $g \in G$ which stabilizes K, and $G^+/K \cong L_1$. But φ_k is $\mathrm{Aut}(L_1)$-invariant [Jansen et al. 1995], whence $l = k$, i.e., $W_j \cong W_i$, a contradiction.

By Lemma 5.3, $V \cong A \oplus B$ as a module over the p'-group $N := \boldsymbol{N}_G(Q)$, where the N-modules A and B are irreducible of dimensions $4e$ and $6e$, respectively. Hence, by the Artin–Wedderburn theorem applied to N,

$$\mathcal{M} := \langle \Phi(g) : g \in G,\ g \text{ semisimple} \rangle_k$$

contains $\mathcal{A} := \mathrm{End}(A) \oplus \mathrm{End}(B) = (A^* \otimes A) \oplus (B^* \otimes B)$ (if Φ denotes the representation of G on V). As in Lemma 5.3 and its proof, write $A = \bigoplus_{i=1}^t C_i = e\big(\bigoplus_{i=1}^t A_i\big)$ and $B = \bigoplus_{i=1}^t D_i = e\big(\bigoplus_{i=1}^t B_i\big)$ as Q-modules, where A_i affords $\tilde{\alpha}_i$ and B_i affords $\tilde{\beta}_i$. Hence, the complement to $\mathcal{A}$ in $\mathrm{End}(V)$ affords the Q-character

$$\Delta := e^2 \sum_{i,j=1}^{t} (\tilde{\alpha}_i \overline{\tilde{\beta}_j} + \tilde{\beta}_i \overline{\tilde{\alpha}_j}).$$

Together with (5-5) and (5-6), this implies that the restriction of any irreducible constituents of Δ to $\boldsymbol{Z}(Q) = Z_1 \times \cdots \times Z_n$ does *not* contain $1_{\boldsymbol{Z}(Q)}$. Thus $\boldsymbol{Z}(Q)$ acts fixed-point-freely on the quotient $\mathrm{End}(V)/\mathcal{M}$. Furthermore, the Q-character of this quotient does not contain $\overline{\tilde{\beta}_i}\tilde{\beta}_j$ (as an irreducible constituent of degree 36) for any $i \neq j$.

As a G^+-module,

$$\mathrm{End}(V) = \bigoplus_{i,j=1}^{t} (V_i^* \otimes V_j) \cong e^2 \bigg(\bigoplus_{i,j=1}^{t} W_i^* \otimes W_j \bigg).$$

Now, if $i \neq j$ then the G^+-module $W_i^* \otimes W_j$ is irreducible and its Brauer character, while restricted to Q, contains $\overline{\tilde{\beta}_i}\tilde{\beta}_j$. On the other hand, the Brauer character of $W_i^* \otimes W_i$ is the direct sum of 1_{G^+} and another irreducible character of degree 99 (as one can check using [GAP 2004]), whose restriction to $\boldsymbol{Z}(Q)$ contains $1_{\boldsymbol{Z}(Q)}$ (which can be seen from (5-5)). Hence we conclude that $\mathcal{M} = \mathrm{End}(V)$. □

Lemma 5.10. *Let* $\mathrm{char}(k) = 5$ *and let W be a faithful irreducible $k(2\mathsf{S}_7)$-module of dimension* 8, *with corresponding representation Θ. Decompose $W_L = W_1 \oplus W_2$ as L-modules for $L = 2\mathsf{A}_7$. Then there is a $5'$-element $z \in 2\mathsf{S}_7 \setminus L$ and a set $\mathcal{X} \subset L$ such that*

(i) *x and xz are $5'$-elements for all $x \in \mathcal{X}$, and*

(ii) $\langle \Theta(x) : x \in \mathcal{X} \rangle_k = \mathrm{End}(W_1) \oplus \mathrm{End}(W_2)$.

Proof. Using [Wilson et al.] and [GAP 2004], K. Lux verified that one can find an element $h \in 2\mathsf{S}_7 \setminus L$ (of order 12) and a set $\mathscr{X} \subset L$ satisfying condition (i) such that $\langle \Theta(xz) : x \in \mathscr{X}\rangle_k$ has dimension 32. Since $\Theta(z) \in \mathrm{GL}(W)$, it follows that $\langle \Theta(x) : x \in \mathscr{X}\rangle_k$ is a subspace of dimension 32 in $\mathrm{End}(W_1) \oplus \mathrm{End}(W_2)$. Since the latter also has dimension 32, we are done. □

Proposition 5.11. *In the case* $(p, H, \dim W) = (5, 2\mathsf{A}_7, 4)$ *of* (ii) *of Theorem 5.7,* (G, V) *is weakly adequate.*

Proof. (a) Recall that $G^+ = L_1 * \cdots * L_n$, and for each i there is some k_i such that the kernel K_i of G^+ contains $\prod_{j \neq k_i} L_j$. By relabeling the W_i, we may assume that $k_1 = 1$. Now, L_1 acts on each W_j either trivially or as the group $H_j \cong 2\mathsf{A}_7$. It follows that $\boldsymbol{O}_3(\boldsymbol{Z}(L_1))$ acts trivially on each W_j and so by faithfulness $\boldsymbol{O}_3(\boldsymbol{Z}(L_1)) = 1$, yielding $L_1 \cong 2\mathsf{A}_7$. On the other hand, $L_1/(K_1 \cap L_1) = H_1 \cong 2\mathsf{A}_7$, whence $K_1 \cap L_1 = 1$, $K_1 = \prod_{j \neq 1} L_j$. This is true for all i, so we have shown that

$$G^+ = L_1 \times L_2 \times \cdots \times L_n \cong H^n.$$

Certainly, G permutes the n components L_i, and this action is transitive by Theorem 2.4(i). Setting $J_1 := \boldsymbol{N}_G(L_1)$, one sees that $G_1 = I_G(W_1) = \mathrm{Stab}_G(V_1)$ is contained in J_1 (as it fixes $K_1 = \prod_{j>1} L_j$). Fix a decomposition $G = \bigcup_{i=1}^t g_i J_1$ with $g_1 = 1$ and $L_i = L_1^{g_i} = g_i L_1 g_i^{-1}$, and choose a subgroup $Q_1 < L_1$ such that $Q_1/\boldsymbol{Z}(L_1) \cong \mathrm{PSL}_2(7)$. Since involutions in A_7 lift to elements of order 4 in L_1, we see that $Q_1 \cong \mathrm{SL}_2(7)$. Now we define

$$Q = Q_1 \times Q_1^{g_2} \times \cdots \times Q_1^{g_n} < G^+.$$

Note that $\boldsymbol{N}_{G^+}(Q) = Q$ and so $N := \boldsymbol{N}_G(Q)$ is a p'-group. Also, L_1 has exactly two irreducible 5-Brauer characters φ_1, φ_2 of degree 4, restricting irreducibly and distinctly to Q_1.

(b) Consider the case where $k_i \neq k_j$ whenever $i \neq j$, i.e., $J_1 = G_1$ and $t = n$. We claim that Q satisfies the conditions of Lemma 5.2. Indeed, the condition $k_i \neq k_j$ implies that the Q-modules W_i and W_j are irreducible and nonisomorphic for $i \neq j$. Next, for any $x \in J_1$, since x fixes W_1 (up to isomorphism), x fixes the character φ of the L_1-module W_1 and so x cannot fuse the two classes $7A$ and $7B$ of elements of order 7 in L_1, whence x can induce only an inner automorphism of L_1. It follows that $Q_1^x = Q_1^t$ for some $t \in L_1$. Now we consider any $g \in G$. Then, for each i we can find j and $x_i \in J_1$ such that $gg_i = g_j x_i$. By the previous observation, there is some $t_i \in L_1$ such that $Q_1^{x_i} = Q_1^{t_i}$. Hence, setting $y_i = g_j t_i g_j^{-1} \in L_j$, we have that

$$Q_1^{gg_i} = Q_1^{g_j x_i} = g_j x_i Q_1 x_i^{-1} g_j^{-1} = g_j t_i Q_1 t_i^{-1} g_j^{-1} = y_i g_j Q_1 g_j^{-1} y_i^{-1} = (Q_1^{g_j})^{y_i}.$$

It follows that $Q^g = Q^y$ with $y = \prod_i y_i \in G^+$, i.e., Q fulfills condition (i) of Lemma 5.2. Now we can conclude by Lemma 5.2 that N is irreducible on V and so we are done.

(c) From now on we assume that, say, $k_1 = k_2$. Then W_1 and W_2 are nonisomorphic modules over $G^+/K_1 = L_1$. So we may assume that W_i affords the L_1-character φ_i for $i = 1, 2$. Note that any $x \in J_1$ sends W_1 to another irreducible G^+-module with the same kernel K_1, and so $\varphi_1^x \in \{\varphi_1, \varphi_2\}$. The irreducibility of G on V implies by Clifford's theorem that the induced action of J_1 on $\{\varphi_1, \varphi_2\}$ is transitive, with kernel G_1. We have shown that $[J_1 : G_1] = 2$ and $t = 2n$. We will label $g_i(W_1)$ as W_{2i-1} and $g_i(W_2)$ as W_{2i}. We also have that $W_2 \cong W_1^h$ for all $h \in J_1 \setminus G_1$. Comparing the kernels and the characters of Q on W_i, we see that the Q-modules W_i are all irreducible and pairwise nonisomorphic. Let

$$\begin{aligned}
\mathscr{E}_1 &:= \bigoplus_{i=1}^{t} \mathrm{End}(V_i) = \bigoplus_{i=1}^{n} \mathscr{A}_i, & \mathscr{A}_i &:= \mathrm{End}(V_{2i-1}) \oplus \mathrm{End}(V_{2i}),\\
\mathscr{E}_{21} &:= \bigoplus_{i=1}^{n} \mathscr{B}_i, & \mathscr{B}_i &:= \mathrm{Hom}(V_{2i-1}, V_{2i}) \oplus \mathrm{Hom}(V_{2i}, V_{2i-1}),\\
\mathscr{E}_{22} &:= \bigoplus_{\substack{1 \le i \ne j \le 2n\\ \{i,j\} \ne \{2a-1, 2a\}}} \mathrm{Hom}(V_i, V_j)
\end{aligned}$$

so that $\mathrm{End}(V) = \mathscr{E}_1 \oplus \mathscr{E}_{21} \oplus \mathscr{E}_{22}$. Note that the G^+-composition factors of $\mathscr{E}_{21}$ are all of dimensions 6 and 10, whereas the G^+-composition factors of $\mathscr{E}_1$ are either trivial or of dimension 15, as one can check using [Jansen et al. 1995]. Furthermore, the G^+-composition factors of $\mathscr{E}_{22}$ are all of dimension 16. In particular, no G^+-composition factor of $\mathrm{Hom}(W_i, W_j)$ is trivial when $i \ne j$. Similarly, whenever $i \ne j$, the only common G^+-composition factor shared by $\mathscr{A}_i$ and $\mathscr{A}_j$ is k, and $\mathscr{B}_i$ and $\mathscr{B}_j$ share no common G^+-composition factor.

(d) Here we show that $\mathscr{A}_i \oplus \mathscr{B}_i$ is a subquotient of $\mathscr{M}$. To this end, note that J_1 acts irreducibly on $V_1 \oplus V_2$. There is no loss in replacing G by the image of J_1 in $\mathrm{End}(V_1 \oplus V_2)$ and V by $V_1 \oplus V_2$. In doing so, we also get that $n = 1$, $G^+ = L_1$, $[G : G_1] = 2$, $K_1 = 1$, and $G_1 = C * L_1$, where $C := \boldsymbol{C}_G(L_1)$ is a $5'$-group. So for $i = 1, 2$ we can write $V_i = U_i \otimes W_i$ as G_1-modules, where U_i is an irreducible kC-module with corresponding representation Λ_i. Hence for the representation Φ_i of G_1 on V_i, we have $\Phi_i = \Lambda_i \otimes \Theta_i$, where Θ_i is the representation of L_1 on W_i. Finally, for the representation Φ of G on $V = V_1 \oplus V_2$, we have $\Phi(g) = \mathrm{diag}(\Phi_1(g), \Phi_2(g))$ whenever $g \in G_1$.

Recall the element $z \in 2\mathsf{S}_7$ and the set $\mathscr{X} \subset L_1$ constructed in Lemma 5.10. Now we fix a $5'$-element $h \in G \setminus G_1$ such that h induces the same action on $L_1/\boldsymbol{Z}(L_1) \cong \mathsf{A}_7$

as the action of z on A_7. It follows that for all elements $x \in \mathscr{X}$ and for all $u \in C$, ux and uxh are $5'$-elements, whence $\mathcal{M}$ contains the subspaces

$$\mathscr{C} := \langle \Phi(ux) : u \in C, x \in \mathscr{X} \rangle_k, \quad \mathscr{C}\Phi(h) := \{v\Phi(h) : v \in \mathscr{C}\}.$$

We also have that $\Theta_2 \cong \Theta_1^h = \Theta_1^z$. Setting $\Theta(x) = \operatorname{diag}(\Theta_1(x), \Theta_2(x))$ for $x \in \mathscr{X}$, we have by the construction of $\mathscr{X}$ that

$$\langle \Theta(x) : x \in \mathscr{X} \rangle_k = \operatorname{End}(W_1) \oplus \operatorname{End}(W_2).$$

Thus, for $X \in \operatorname{End}(W_1)$, we can write the element $\operatorname{diag}(X, 0)$ of $\operatorname{End}(W_1) \oplus \operatorname{End}(W_2)$ as $\operatorname{diag}(X, 0) = \sum_{x \in \mathscr{X}} a_x \Theta(x)$ for some $a_x \in k$; i.e.,

$$\sum_{x \in \mathscr{X}} a_x \Theta_1(x) = X, \quad \sum_{x \in \mathscr{X}} a_x \Theta_2(x) = 0.$$

On the other hand, applying the Artin–Wedderburn theorem to the representation Λ_i of the $5'$-group C on U_i, we have that

$$\langle \Lambda_i(u) : u \in C \rangle_k = \operatorname{End}(U_i).$$

In particular, any $Y \in \operatorname{End}(U_1)$ can be written as $Y = \sum_{u \in C} b_u \Lambda_1(u)$ for some $b_u \in k$. It follows that the element $\operatorname{diag}(Y \otimes X, 0)$ of

$$\operatorname{End}(U_1) \otimes \operatorname{End}(W_1) \cong \operatorname{End}(U_1 \otimes W_1) = \operatorname{End}(V_1) \hookrightarrow \operatorname{End}(V)$$

can be written as

$$\begin{aligned}\operatorname{diag}\Bigg(\sum_{u \in C,\ x \in \mathscr{X}} & b_u a_x \Lambda_1(u) \otimes \Theta_1(x), \sum_{u \in C,\ x \in \mathscr{X}} b_u a_x \Lambda_2(u) \otimes \Theta_2(x) \Bigg) \\ &= \sum_{u \in C,\ x \in \mathscr{X}} a_x b_u \cdot \operatorname{diag}(\Phi_1(ux), \Phi_2(ux)) = \sum_{u \in C,\ x \in \mathscr{X}} a_x b_u \Phi(ux),\end{aligned}$$

and so it belongs to $\mathscr{C}$. Thus $\mathscr{C} \supseteq \operatorname{End}(V_1)$, and similarly $\mathscr{C} \supseteq \operatorname{End}(V_2)$. Since G_1 stabilizes each of V_1 and V_2, we then have that

$$\mathscr{C} = \operatorname{End}(V_1) \oplus \operatorname{End}(V_2) = \mathscr{A}_1.$$

But $\Phi(h)$ interchanges V_1 and V_2. It follows that $\mathcal{M}$ also contains

$$\mathscr{C}\Phi(h) = \operatorname{Hom}(V_1, V_2) \oplus \operatorname{Hom}(V_2, V_1) = \mathscr{B}_1,$$

as stated.

(e) Next we show that $\mathscr{E}_{22}$ is a subquotient of $\mathcal{M}$. Choose $R_i \cong 2 \times (7:3) < L_i$, the normalizer of some Sylow 7-subgroup of L_i. Note that $N_{L_i}(R_i) = R_i$ and

$$(\varphi_j)_{R_1} = \alpha_j + \beta, \tag{5-7}$$

where α_j, $\beta \in \mathrm{Irr}(R_1)$ are of degree 3 and 1, respectively, and $\alpha_1 \neq \alpha_2$. Defining

$$R = R_1 \times R_2 \times \cdots \times R_n < G^+,$$

we see that R satisfies the conditions of Lemma 5.4. Hence the subspace $A = e\bigl(\bigoplus_{i=1}^t A_i\bigr)$ defined in Lemma 5.4 (with A_1 affording the R_1-character α_1) is irreducible over the p'-group $\boldsymbol{N}_G(R)$. By the Artin–Wedderburn theorem applied to $\boldsymbol{N}_G(R)$ acting on $V = A \oplus B$, $\mathcal{M}$ contains

$$\mathrm{End}(A) \supset \mathcal{D} := \bigoplus_{\substack{1 \le i \neq j \le 2n \\ \{i,j\} \neq \{2a-1,2a\}}} \mathrm{Hom}(eA_i, eA_j).$$

As noted previously, each summand $\mathrm{Hom}(V_i, V_j)$ in $\mathcal{E}_{22}$ is acted on trivially by $\prod_{s \neq k_i, k_j} L_s$, and affords the $L_{k_i} \times L_{k_j}$-character $\varphi \otimes \varphi'$, where $\varphi, \varphi' \in \{\varphi_1, \varphi_2\}$. Working modulo $\mathcal{E}_1 \oplus \mathcal{E}_{21}$ and using this observation and (5-7), we then see that all irreducible constituents of the R-character of the complement to $\mathcal{D}$ in $\mathcal{E}_{22}$ are of the form $\gamma_1 \otimes \gamma_2 \otimes \cdots \otimes \gamma_n$, where $\gamma_i \in \mathrm{Irr}(R_i)$ and *all but at most one* of them have degree 1 (and the remaining, if any, is some α_j of degree 3). The same is true for the complement to $\mathcal{M}$ in $\mathcal{E}_{22}$ (again modulo $\mathcal{E}_1 \oplus \mathcal{E}_{21}$). On the other hand, (5-7) and the aforementioned observation imply that the R-character of the G^+-composition factor $\mathrm{Hom}(W_i, W_j)$ contains an irreducible R-character of degree 9 (namely, an $R_{k_i} \times R_{k_j}$-character of the form $\alpha \otimes \alpha'$, with $\alpha, \alpha' \in \{\alpha_1, \alpha_2\}$). It follows that $\mathcal{E}_{22}$ is a subquotient of $\mathcal{M}$.

(f) The results of (d) and (e), together with the remarks made at the end of (c), imply that all G^+-composition factors of $\mathrm{End}(V)/\mathcal{M}$ (if any) are trivial. Hence by Lemma 5.4 we conclude that $\mathcal{M} = \mathrm{End}(V)$. □

6. Weak adequacy for special linear groups

The exception (i) in Theorem 5.7 requires much more effort to resolve. We begin by setting up some notation. Let $n \geq 3$ and let q be a prime power such that $p = (q^n - 1)/(q - 1)$. In particular, n is a prime, $q = q_0^f$ for some prime q_0 and some odd f, $\gcd(n, q-1) = 1$ and so $\mathrm{PSL}_n(q) = \mathrm{SL}_n(q) =: S$ and $G_n := \mathrm{GL}_n(q) = S \times \boldsymbol{Z}(G_n)$. Consider the natural module

$$\mathcal{N} = \mathbb{F}_q^n = \langle e_1, \ldots, e_n \rangle_{\mathbb{F}_q}$$

for G_n, and let

$$Q = RL = \mathrm{Stab}_S(\langle e_2, \ldots, e_n \rangle_{\mathbb{F}_q}),$$

where R is elementary abelian of order q^{n-1} and $L \cong \mathrm{GL}_{n-1}(q)$. Note that Q is a p'-group. It is well known (see [Guralnick and Tiep 1999, Theorem 1.1]) that $G_n/\boldsymbol{Z}(G_n)$ has a unique irreducible p-Brauer character δ of degree $p - 2$, where

$\delta(x) = \rho(x) - 2$ for all p'-elements $x \in G_n$, if we denote by ρ the permutation character of G_n acting on the set Ω of 1-spaces of $\mathcal{N}$. Let $\mathcal{D}$ denote a kG_n-module affording δ.

Lemma 6.1. *In the above notation, $\delta_Q = \alpha + \beta$, where $\alpha \in \operatorname{Irr}(Q)$ has degree $q^{n-1} - 1$, $\beta \in \operatorname{Irr}(Q)$ has degree $(q^{n-1} - q)/(q - 1)$, and*

$$\alpha_R = \sum_{1_R \neq \lambda \in \operatorname{Irr}(R)} \lambda, \quad \beta_R = \beta(1)1_R.$$

Proof. Note that all nontrivial elements in R are L-conjugate to a fixed transvection $t \in R$, and $\delta(t) = \rho(t) - 2 = (q^{n-1} - q)/(q - 1) - 1$. It follows that

$$\delta_R = \sum_{1_R \neq \lambda \in \operatorname{Irr}(R)} \lambda + \frac{q^{n-1} - q}{q - 1} \cdot 1_R.$$

Next, Q acts doubly transitively on the 1-spaces of $\langle e_2, \dots, e_n\rangle_{\mathbb{F}_q}$, with kernel containing R and with character $\beta + 1_Q$, where $\beta \in \operatorname{Irr}(Q)$ of degree $(q^{n-1} - q)/(q - 1)$. Hence β is an irreducible constituent of δ, and the statement follows. □

In the subsequent treatment of $\mathrm{SL}_n(q)$, it is convenient to adopt the labeling of irreducible $\mathbb{C}G_n$-modules as given in [James 1986], which uses Harish-Chandra induction, denoted $\circ$. Each such module is labeled as $S(s_1, \lambda_1) \circ \cdots \circ S(s_m, \lambda_m)$, where $s_i \in \overline{\mathbb{F}}_q^\times$ has degree d_i (over $\mathbb{F}_q$), λ_i is a partition of k_i, and $\sum_{i=1}^m k_i d_i = n$ [James 1986; Kleshchev and Tiep 2009]. Similarly, irreducible kG_n-modules are labeled as $D(s_1, \lambda_1) \circ \cdots \circ D(s_m, \lambda_m)$, with some extra conditions including s_i being a p'-element. For $\lambda \vdash n$, let $\chi^\lambda = S(1, \lambda)$ denote the unipotent character of $\mathrm{GL}_n(q)$ labeled by λ. We set the convention that $\chi^{(n-2,2)} = 0$ for $n = 3$. Also, note that $1_{G_n} = \chi^{(n)}$ and $\rho = 1_{G_n} + \chi^{(n-1,1)}$ (see, e.g., [Guralnick and Tiep 1999, Lemma 5.1]). We next establish the following result, which holds for arbitrary $\mathrm{GL}_n(q)$ with $n \geq 3$ and which is interesting in its own right:

Lemma 6.2. *In the above notation, we have the following decomposition of ρ^2 into irreducible constituents over $G_n = \mathrm{GL}_n(q)$:*

$$\rho^2 = 2\chi^{(n)} + 4\chi^{(n-1,1)} + \chi^{(n-2,2)} + 2\chi^{(n-2,1^2)} + \sum_{\substack{a \in \mathbb{F}_q^\times \\ a^2 = 1 \neq a}} S(a, (1^2)) \circ S(1, (n-2))$$
$$+ \sum_{\substack{a \in \overline{\mathbb{F}}_q^\times \\ a^{q-1} = 1 \neq a^2}} S(a, (1)) \circ S(a^{-1}, (1)) \circ S(1, (n-2))$$
$$+ \sum_{\substack{a \in \overline{\mathbb{F}}_q^\times \\ b^{q+1} = 1 \neq b^2}} S(b, (1)) \circ S(1, (n-2)).$$

Proof. Recall that ρ is the permutation character of G_n acting on Ω and also on the diagonal $\{(x,x) : x \in \Omega\}$ of $\Omega \times \Omega$, whereas ρ^2 is the permutation character of G_n acting on $\Omega \times \Omega$. Letting $H_n := \mathrm{Stab}_{G_n}(\langle e_1\rangle_{\mathbb{F}_q}, \langle e_2\rangle_{\mathbb{F}_q})$, we then see that

$$\rho^2 = \rho + \mathrm{Ind}_{H_n}^{G_n}(1_{H_n}).$$

Notice that $\mathrm{Ind}_{H_n}^{G_n}(1_{H_n})$ is just the Harish-Chandra induction of the character $\mathrm{Ind}_{H_2}^{G_2}(1_{H_2}) \otimes 1_{G_{n-2}}$ of the Levi subgroup $G_2 \times G_{n-2}$ of the parabolic subgroup

$$P := \mathrm{Stab}_{G_n}(\langle e_1, e_2\rangle_{\mathbb{F}_q})$$

of G_n, i.e.,

$$\mathrm{Ind}_{H_n}^{G_n}(1_{H_n}) = \mathrm{Ind}_{H_2}^{G_2}(1_{H_2}) \circ 1_{G_{n-2}}. \tag{6-1}$$

Consider the case of odd q. Then, according to the proof of [Navarro and Tiep 2010, Proposition 5.5],

$$\begin{aligned}\mathrm{Ind}_{H_2}^{G_2}(1_{H_2}) = {} & S(1,(2)) + 2S(1,(1^2)) + S(-1,(1^2)) \\ & +a \sum_{\substack{a\in\bar{\mathbb{F}}_q^\times \\ a^{q-1}=1\neq a^2}} S(a,(1)) \circ S(a^{-1},(1)) + \sum_{\substack{a\in\bar{\mathbb{F}}_q^\times \\ b^{q+1}=1\neq b^2}} S(b,(1)).\end{aligned} \tag{6-2}$$

Next, by [Guralnick and Tiep 1999, Lemma 5.1] we have

$$S(1,(2))\circ S(1,(n-2)) = \mathrm{Ind}_P^{G_n}(1_P) = \chi^{(n)}+\chi^{(n-1,1)}+\chi^{(n-2,2)}, \tag{6-3}$$

$$S(1,(1))\circ S(1,(1))\circ S(1,(n-2)) = \chi^{(n)}+2\chi^{(n-1,1)}+\chi^{(n-2,2)}+\chi^{(n-2,1^2)}. \tag{6-4}$$

Since $S(1,(1))\circ S(1,(1)) = S(1,(2)) + S(1,(1^2))$, the statement follows from (6-1)–(6-4) and properties of the Harish-Chandra induction in G_n (see [James 1986]).

The case q is even can be proved similarly, using

$$\begin{aligned}\mathrm{Ind}_{H_2}^{G_2}(1_{H_2}) = S(1,(2)) + 2S(1,(1^2)) + \sum_{\substack{a\in\bar{\mathbb{F}}_q^\times \\ a^{q-1}=1\neq a^2}} S(a,(1)) \circ S(a^{-1},(1)) \\ + \sum_{\substack{a\in\bar{\mathbb{F}}_q^\times \\ b^{q+1}=1\neq b^2}} S(b,(1))\end{aligned}$$

instead of (6-2). □

Lemma 6.3. *In the above notation, if $p = (q^n-1)/(q-1)$, we have the following decomposition of δ^2 into irreducible constituents over $S = \mathrm{SL}_n(q)$:*

$$\begin{aligned}\delta^2 = {} & 2D(1,(n)) + 2D(1,(n-1,1)) + D(1,(n-2,2)) + 2D(1,(n-2,1^2))\\ & + \sum_{\substack{a\in\mathbb{F}_q^\times\\ a^2=1\neq a}} D(a,(1^2))\circ D(1,(n-2))\\ & + \sum_{\substack{a\in\bar{\mathbb{F}}_q^\times\\ a^{q-1}=1\neq a^2}} D(a,(1))\circ D(a^{-1},(1))\circ D(1,(n-2))\\ & + \sum_{\substack{b\in\bar{\mathbb{F}}_q^\times\\ b^{q+1}=1\neq b^2}} D(b,(1))\circ D(1,(n-2)).\end{aligned}$$

In particular, if there is a composition factor U of the kS-module $\mathfrak{D}\otimes\mathfrak{D}$ with $U^R = 0$, then $n = 3$ and U affords the Brauer character $D(1, (1^3))$. Furthermore, the only composition factors of $\mathfrak{D}\otimes\mathfrak{D}$ that are not of p-defect zero are the ones with Brauer character $1_S = D(1, (n))$, $\delta = D(1, (n-1, 1))$, and $D(1, (n-2, 1^2))$.

Proof. Let us denote by χ° the restriction of any character χ of G_n to the set of p'-elements of G_n. Then

$$\delta^2 = (\rho^\circ - 2\cdot 1_{G_n})^2 = (\rho^\circ)^2 - 4(\chi^{(n-1,1)})^\circ,$$

and we can apply Lemma 6.2. Since $p = (q^n-1)/(q-1)$ (or more generally, if p is a primitive prime divisor of q^n-1), all complex characters in the decomposition for ρ^2 in Lemma 6.2 are of p-defect 0, except for $\chi^{(n)}$, $\chi^{(n-1,1)}$, and $\chi^{(n-2,1^2)}$. Furthermore, $(\chi^{(n-2,1^2)})^\circ = D(1, (n-1, 1)) + D(1, (n-2, 1^2))$ [Guralnick and Tiep 1999, Proposition 3.1 and §4]; in particular,

$$D(1,(n-2,1^2))(1) = \frac{(q^n-q)(q^n-2q^2+1)}{(q-1)(q^2-1)} + 1.$$

Since $G_n = S \times \mathbf{Z}(G_n)$, we arrive at the desired decomposition of δ^2. Also, the degree of any irreducible constituent ψ of δ^2 listed above is not divisible by $|R| - 1 = q^{n-1} - 1$, unless $n = 3$ and $\psi = D(1, (1^3))$, whence ψ_R must contain 1_R since L acts transitively on $\mathrm{Irr}(R) \setminus \{1_R\}$. In the exceptional case, ψ_R does not contain 1_R, as one can see by direct computation (or by using [Kleshchev and Tiep 2010, Theorem 5.4]). □

Corollary 6.4. *Assume that $p = (q^n - 1)/(q - 1)$ and $n \geq 5$. Then $S = \mathrm{SL}_n(q)$ is weakly adequate on $\mathfrak{D}$.*

Proof. By Lemma 6.1 and the Artin–Wedderburn theorem applied to Q, $\mathcal{M}$ contains the subspace $\mathcal{A} := (A\otimes A) \oplus (B\otimes B)$ of $\mathfrak{D}\otimes\mathfrak{D} = \mathrm{End}(\mathfrak{D})$, with A affording α and B affording β. Thus, the complement to $\mathcal{A}$ in $\mathrm{End}(V)$ affords the Q-character $\Delta := 2\alpha\beta$. It follows by Lemma 6.1 that Δ_R does *not* contain 1_R, whence R does not have any nonzero fixed point while acting on this complement. The same must be true for the quotient $\mathrm{End}(V)/\mathcal{M}$, which is a semisimple Q-module. Since $n > 3$, by Lemma 6.3 this can happen only when $\mathcal{M} = \mathrm{End}(V)$. □

Next we will extend the result of Corollary 6.4 to the case $n = 3$.

Proposition 6.5. *Assume that $p = (q^3 - 1)/(q - 1)$. Then $S = \mathrm{SL}_3(q)$ is weakly adequate on $\mathfrak{D}$.*

Proof. Note that δ is invariant under the graph automorphism τ of S, which interchanges the two conjugacy classes of the maximal parabolic subgroup

$$Q = RL = \mathrm{Stab}_S(\mathcal{U}) = \mathrm{Stab}_S(\langle e_1, e_2\rangle_{\mathbb{F}_q})$$

and its opposite

$$Q^\sharp = R^\sharp L^\sharp = \mathrm{Stab}_S(\langle e_1\rangle_{\mathbb{F}_q}).$$

Hence Lemma 6.1 also applies to $Q^\sharp$. To simplify the notation, we will drop the subscript $\mathbb{F}_q$ in various spans $\langle\,\cdot\,\rangle_{\mathbb{F}_q}$ in this proof.

First we will construct the Q-submodules $\mathcal{A}$, $\mathcal{B}$ affording the character α and β in $\mathfrak{D}$. Clearly, R has $q + 1$ fixed points in $\mathbb{P}\mathcal{U}$ and one orbit of length q^2,

$$\mathcal{O} := \{\langle e_3 + y\rangle : y \in \mathcal{U}\},$$

on $\Omega = \mathbb{P}\mathcal{N}$. Denoting $\mathcal{I} := \left\langle \sum_{\omega\in\mathbb{P}\mathcal{N}} \omega\right\rangle_k$, we can now decompose $\mathfrak{D} = \mathcal{A} \oplus \mathcal{B}$ as Q-modules, where

$$\mathcal{A} := [\mathfrak{D}, R] = \left(\left\{\sum_{y\in\mathcal{U}} a_y\langle e_3 + y\rangle \;:\; a_y \in k,\ \sum_{y\in\mathcal{U}} a_y = 0\right\} \oplus \mathcal{I}\right) \Big/ \mathcal{I},$$

$$\mathcal{B} := \boldsymbol{C}_{\mathfrak{D}}(R) = \left(\left\{\sum_{\omega\in\mathbb{P}\mathcal{U}} b_\omega\omega \;:\; b_\omega \in k,\ \sum_{\omega\in\mathbb{P}\mathcal{U}} b_\omega = 0\right\} \oplus \mathcal{I}\right) \Big/ \mathcal{I}.$$

Next, $R^\sharp$ has 1 fixed point $\langle e_1\rangle$ and $q + 1$ orbits of length q,

$$\mathcal{O}_\infty := \mathbb{P}\mathcal{U} \setminus \{\langle e_1\rangle\}, \quad \mathcal{O}_c := \{\langle e_3 + ce_2 + de_1\rangle : d \in \mathbb{F}_q\},\ c \in \mathbb{F}_q,$$

on $\mathbb{P}\mathcal{N}$. Then we can again decompose $\mathfrak{D} = \mathcal{A}^\sharp \oplus \mathcal{B}^\sharp$ as $Q^\sharp$-modules, where $\mathcal{A}^\sharp = [\mathfrak{D}, R^\sharp]$ and $\mathcal{B}^\sharp = \boldsymbol{C}_{\mathfrak{D}}(R^\sharp)$. Note that $\mathcal{O} = \mathbb{P}\mathcal{N} \setminus \mathbb{P}\mathcal{U} = \bigcup_{c\in\mathbb{F}_q} \mathcal{O}_c$. Hence, the $q(q - 1)$ vectors

$$v_{c,d} = \langle e_3 + ce_2 + de_1\rangle - \langle e_3 + ce_2\rangle, \quad c \in \mathbb{F}_q,\ d \in \mathbb{F}_q^\times$$

belong to $\mathcal{A} \cap \mathcal{A}^\sharp$, and similarly the $q - 1$ vectors

$$u_a = \langle e_2 + ae_1\rangle - \langle e_2\rangle, \quad a \in \mathbb{F}_q^\times$$

belong to $\mathscr{B} \cap \mathscr{A}^\sharp$, and they are linearly independent. Thus

$$u_a \otimes v_{c,d} \in (\mathscr{A}^\sharp \otimes \mathscr{A}^\sharp) \cap (\mathscr{B} \otimes \mathscr{A}) \quad \text{and} \quad v_{c,d} \otimes u_a \in (\mathscr{A}^\sharp \otimes \mathscr{A}^\sharp) \cap (\mathscr{A} \otimes \mathscr{B}),$$

and so both $(\mathscr{A}^\sharp \otimes \mathscr{A}^\sharp) \cap (\mathscr{B} \otimes \mathscr{A})$ and $(\mathscr{A}^\sharp \otimes \mathscr{A}^\sharp) \cap (\mathscr{A} \otimes \mathscr{B})$ have dimension at least $q(q-1)^2$. As a consequence,

$$\dim((\mathscr{A}^\sharp \otimes \mathscr{A}^\sharp) \cap (\mathscr{A} \otimes \mathscr{B} \oplus \mathscr{B} \otimes \mathscr{A})) \geq 2q(q-1)^2. \tag{6-5}$$

Since $\mathscr{D}$ is self-dual, it supports a nondegenerate S-invariant symmetric bilinear form $(\cdot\,,\cdot)$, with respect to which $\mathscr{A}$ and $\mathscr{B}$ are orthogonal, as are $\mathscr{A}^\sharp$ and $\mathscr{B}^\sharp$. As usual, we can now identify $\mathscr{D} \otimes \mathscr{D}$ with $\mathrm{End}(\mathscr{D})$ by sending $u \otimes v \in \mathscr{D} \otimes \mathscr{D}$ to

$$f_{u,v} : x \mapsto (x, u)v$$

for all $x \in \mathscr{D}$. Furthermore, in the proof of Corollary 6.4, we have already mentioned that $\mathscr{M}$ contains the subspaces $\mathrm{End}(\mathscr{A}) \oplus \mathrm{End}(\mathscr{B})$ (arguing with Q) and $\mathrm{End}(\mathscr{A}^\sharp)$ (arguing with $Q^\sharp$). It now follows from (6-5) that

$$\dim(\mathrm{End}(\mathscr{A}^\sharp) \cap (\mathrm{Hom}(\mathscr{A}, \mathscr{B}) \oplus \mathrm{Hom}(\mathscr{B}, \mathscr{A}))) \geq 2q(q-1)^2.$$

Hence for $q \geq 5$ we have that

$$\begin{aligned}\dim \mathrm{End}(\mathscr{D}) - \dim \mathscr{M} &\leq (q^2+q-1)^2 - (q^2-1)^2 - q^2 - 2q(q-1)^2 \\ &= 4q(q-1) < (q-1)(q^2-1) = \dim D(1, (1^3)).\end{aligned}$$

On the other hand, Lemma 6.3 and the proof of Corollary 6.4 show that the only S-composition factor of $\mathrm{End}(\mathscr{D})/\mathscr{M}$ (if any) is $D(1, (1^3))$. Hence, we conclude that $\mathscr{M} = \mathrm{End}(V)$ if $q \geq 5$. Since $p = (q^3-1)/(q-1)$, in the remaining cases we have $q = 2, 3$. The case $q = 2$ is already handled before as $S \cong \mathrm{PSL}_2(7)$, and the case $q = 3$ has been checked with a computer by F. Lübeck. □

Now we can prove the weak adequacy of G on V in the case the G^+-module is homogeneous.

Proposition 6.6. *Assume that $t = 1$, i.e., the G^+-module V is homogeneous in the case $(p, H, \dim W) = ((q^n-1)/(q-1), \mathrm{SL}_n(q), p-2)$ of Theorem 5.7. Then (G, V) is weakly adequate.*

Proof. Since $V|_{G^+} = eW$, by Theorem 2.4 we have that $G^+ = S = \mathrm{SL}_n(q)$. Recall that $\gcd(n, q-1) = 1$ and $q = q_0^f$, where q_0 is a prime and f is odd; in particular, $\mathrm{Out}\, S \cong C_{2f}$ is cyclic. It follows that $L := C \times S \lhd G = \langle L, \tau \rangle$ for some $\tau \in G$, and $C := \boldsymbol{C}_G(S)$ is a p'-group. Let Ψ denote the corresponding representation of S on W and Φ denote the corresponding representation of G on V. Then, by Corollary 6.4 and Proposition 6.5, we have that

$$\langle \Psi(y) : y \in S,\ y \text{ semisimple} \rangle_k = \mathrm{End}(W).$$

First we consider the case where V_L is irreducible. Then $V \cong U \otimes W$, where U is an irreducible kC-module and C acts trivially on W. Let Θ denote the corresponding representation of C on U. By the Artin–Wedderburn theorem, $\langle \Theta(x) : x \in C \rangle_k = \mathrm{End}(U)$. Since $\Phi(xy) = \Theta(x) \otimes \Psi(y)$ for $x \in C$, $y \in S$, and since C is a p'-group, we conclude that $\mathcal{M}$ contains $X \otimes Y$ for all $X \in \mathrm{End}(U)$ and $Y \in \mathrm{End}(W)$, i.e., $\mathcal{M} = \mathrm{End}(V)$.

Assume now that V_L is reducible. Note that V_L is semisimple and multiplicity-free, as G/L is cyclic. Since W is τ-invariant, it follows that

$$V_L = V_1 \oplus V_2 \oplus \cdots \oplus V_s \cong (U_1 \oplus U_2 \oplus \cdots \oplus U_s) \otimes W,$$

where $V_i = U_i \otimes W$ for some pairwise nonisomorphic irreducible kC-modules $U_1, \ldots, U_s$, $\langle \tau \rangle$ acts transitively on the set of isomorphism classes of $U_1, \ldots, U_s$, C acts trivially on W as before, and $\Phi(\tau)$ permutes the summands $V_1, \ldots, V_s$ transitively. Let Θ_i denote the corresponding representation of C on U_i, and let Θ denote the corresponding representation of C on $U := U_1 \oplus \cdots \oplus U_s$. Since $U_i \not\cong U_j$ for $i \neq j$, by the Artin–Wedderburn theorem, $\langle \Theta(x) : x \in C \rangle_k = \mathrm{End}(U_1) \oplus \cdots \oplus \mathrm{End}(U_s)$. It follows as above that $\mathcal{M}$ contains $X \otimes Y$ for all $Y \in \mathrm{End}(W)$ and all $X \in \mathrm{End}(U_i)$ (viewing X as an element of $\mathrm{End}(U)$ by letting it act as zero on U_j for all $j \neq i$). In other words, $\mathcal{M}$ contains the subspace $\mathrm{End}(V_1) \oplus \cdots \oplus \mathrm{End}(V_s)$ of $\mathrm{End}(V)$.

It remains to show that $\mathcal{M}$ contains $\mathrm{Hom}(V_i, V_j)$ for any $i \neq j$. Since $\Phi(\tau)$ permutes the summands $V_1, \ldots, V_s$ transitively, we can find $\sigma \in \langle \tau \rangle \setminus CS$ such that $\Phi(\sigma)$ sends V_i to V_j and such that σ induces a nontrivial outer automorphism of S. Observe that the condition $p = (q^n - 1)/(q - 1)$ implies that all elements in the coset $S\sigma$ are p'-elements. (Indeed, assume that $x\sigma$ has order divisible by p for some $x \in S$. Then some p'-power g of $x\sigma$ is a p-element in S. It follows that σ preserves the conjugacy class g^S, which is impossible by inspecting the eigenvalues of g.) So all elements in $L\sigma$ are p'-elements. Hence $\mathcal{M}$ also contains the subspace

$$\mathcal{A} := \langle \Phi(h\sigma) : h \in L \rangle_k = \langle \Phi(h) : h \in L \rangle_k \cdot \Phi(\sigma).$$

Again, by the Artin–Wedderburn theorem,

$$\langle \Phi(h) : h \in L \rangle_k = \mathrm{End}(V_1) \oplus \cdots \oplus \mathrm{End}(V_s).$$

Since $\Phi(\sigma)$ sends V_i (isomorphically) to V_j, we conclude that

$$\mathcal{A} \supset \mathrm{End}(V_j, V_j)\Phi(\sigma) = \mathrm{Hom}(V_i, V_j),$$

and so $\mathcal{M} = \mathrm{End}(V)$. □

Next we consider the subgroup

$$Q' = R'L' = \mathrm{Stab}_S(\langle e_n \rangle_{\mathbb{F}_q}, \langle e_2, \ldots, e_n \rangle_{\mathbb{F}_q}),$$

where R' is a q_0-group of special type of order q^{2n-3} and $L' \cong \mathrm{GL}_{n-2}(q) \times \mathrm{GL}_1(q)$. Note that the graph automorphism $x \mapsto {}^t x^{-1}$ of S sends Q' to $(Q')^g$, where $g \in S$ sends e_1 to e_n, e_n to $-e_1$, and fixes all other e_i. Since the S-conjugacy class of the p'-group Q' is fixed by all field automorphisms, it is $\mathrm{Aut}(S)$-invariant. Also, Q' is just the normalizer in S of the root subgroup $Z' := \mathbf{Z}(R') = [R', R']$ (of order q), whence $\mathbf{N}_S(Q') = Q'$.

Lemma 6.7. *In the above notation,* $\delta_{Q'} = \alpha' + \beta'_1 + \beta'_2 + \gamma' + 1_{Q'}$, *where* $\alpha' \in \mathrm{Irr}(Q')$ *has degree* $q^{n-2}(q-1)$, $\beta'_1, \beta'_2 \in \mathrm{Irr}(Q')$ *have degree* $q^{n-2}-1$, $\gamma' \in \mathrm{Irr}(Q')$ *has degree* $(q^{n-2}-q)/(q-1)$ *if* $n > 3$ *and is zero if* $n = 3$, *and*

$$\alpha'_{Z'} = q^{n-2} \sum_{1_{Z'} \neq \lambda \in \mathrm{Irr}(Z')} \lambda, \qquad Z' \leq \mathrm{Ker}(\beta'_1) \cap \mathrm{Ker}(\beta'_2) \cap \mathrm{Ker}(\gamma').$$

Proof. Note that all nontrivial elements in Z' are L'-conjugate to a fixed transvection $t \in Z'$, and $\delta(t) = \rho(t) - 2 = (q^{n-1}-q)/(q-1) - 1$. It follows that

$$\delta_{Z'} = q^{n-2} \sum_{1_{R'} \neq \lambda \in \mathrm{Irr}(Z')} \lambda + \left(2(q^{n-2}-1) + \frac{q^{n-2}-q}{q-1} + 1\right) \cdot 1_{Z'}.$$

Since R' is of special type, it also follows that $[\mathfrak{D}, Z']$ gives rise to an irreducible Q'-module of dimension $q^{n-2}(q-1)$, with character α'. Now we can write $R'/Z' = (R'_1/Z') \times (R'_2/Z')$ as a direct product of two L'-invariant subgroups. Next, Q' acts on the subset Ω' of Ω consisting of all 1-spaces of $\langle e_2, \ldots, e_n \rangle_{\mathbb{F}_q}$ (with kernel containing R'_1), with two orbits. Arguing as in the proof of Lemma 6.1, we see that this permutation action affords the Q'-character $\beta'_2 + \gamma' + 2 \cdot 1_{Q'}$, where the irreducible characters β'_2 and γ' (if $n > 3$; $\gamma' = 0$ if $n = 3$) have the indicated degrees. In general, Q' has three orbits on Ω, whence $1_{Q'}$ enters $\delta_{Q'}$. Also, note that t has an S-conjugate $t' \in R'_1 \setminus Z'$ and $\alpha'(t') = 0$. So if we set

$$\beta'_1(1) := \delta_{Q'} - (\alpha' + \beta'_2 + \gamma' + 1_{Q'}),$$

then we see that $\beta'_1 = \beta'_1(t) = q^{n-2} - 1$ and $\beta'_1(t') = -1$. Since L' acts transitively on the nontrivial elements of R'_1/Z', we conclude by Clifford's theorem that $\beta'_1 \in \mathrm{Irr}(Q')$. □

As mentioned above, $S = \mathrm{SL}_n(q)$ has a unique irreducible kS-module $\mathfrak{D}$ of dimension $p-2$. It follows by Theorem 2.4 that in the situation (i) of Theorem 5.7,

$$G^+ = S_1 \times \cdots \times S_t,$$

with $S_i \cong S$, and G^+ acts on W_i with kernel $K_i := \prod_{j \neq i} S_j$. Now, as G^+-modules, we have that

$$\mathcal{E} := \mathrm{End}(V) \cong \bigoplus_{1 \leq i,j \leq t} V_i^* \otimes V_j \cong e^2 \bigoplus_{1 \leq i,j \leq t} W_i^* \otimes W_j,$$

where $V_i^* \otimes V_i \cong \mathrm{End}(V_i)$ is acted on trivially by K_i, whereas $W_i^* \otimes W_j$ is an *irreducible* kG^+-module with kernel $K_i \cap K_j$ for $i \neq j$. It follows that the two G^+-submodules

$$\mathscr{E}_1 := \bigoplus_{1 \leq i \leq t} V_i^* \otimes V_i, \quad \mathscr{E}_2 := \bigoplus_{1 \leq i \neq j \leq t} V_i^* \otimes V_j$$

of $\mathrm{End}(V)$ share no common composition factor.

Now we can prove the main result of this section:

Theorem 6.8. *Suppose we are in the case* (i) *of Theorem 5.7, i.e.,* $(p, H, \dim W) = ((q^n - 1)/(q - 1), \mathrm{SL}_n(q), p - 2)$. *Then* (G, V) *is weakly adequate.*

Proof. (a) Consider the subgroup

$$Q'^t = Q' \times \cdots \times Q' = Q'_1 \times \cdots \times Q'_t < S_1 \times \cdots \times S_t$$

of G^+. By Lemma 6.7 and the discussion preceding it, Q'^t satisfies the hypotheses of Lemma 5.4, with A_i affording the Q'-character α', and $N_G(Q'^t)$ is a p'-group. Note that $A_i \not\cong A_j$ for $i \neq j$ since $K_i \cap Q'^t \neq K_j \cap Q'^t$. Also, the summands A and B of the Q'^t-module V constructed in Lemma 6.7 have no common composition factor and A is irreducible. Hence,

$$\mathscr{M} \supseteq \mathrm{End}(A) \supset e^2 \bigoplus_{1 \leq i \neq j \leq t} A_i^* \otimes A_j =: \mathscr{A}$$

by the Artin–Wedderburn theorem. Note that $\mathscr{A} \subset \mathscr{E}_2$. Furthermore, if Δ is the Q'^t-character of the complement of $\mathscr{A}$ in $\mathscr{E}_2$, then, by Lemma 6.7, each irreducible constituent of Δ, when restricted to

$$Z'^t = Z' \times \cdots \times Z' = Z'_1 \times \cdots \times Z'_t,$$

is trivial on (at least) *all but one* Z'_i. The same is true for the G^+-module $\mathscr{E}/(\mathscr{E}_1 + \mathscr{M})$. On the other hand, as mentioned above, all G^+-composition factors of $\mathscr{E}/\mathscr{E}_1 \cong \mathscr{E}_2$ are of the form $W_i^* \otimes W_j$ with $i \neq j$. The Brauer character of any such $W_i^* \otimes W_j$, being restricted to $S_i \times S_j$, is $\delta \otimes \delta$, and so it contains the $Q'_i \times Q'_j$-irreducible constituent $\alpha' \otimes \alpha'$ which is nontrivial at both Z'_i and Z'_j by Lemma 6.7. It follows that $\mathscr{E}_1 + \mathscr{M} = \mathscr{E}$, i.e., $\mathscr{M}$ surjects onto $\mathscr{E}_2$. Applying Lemma 5.5 to the subgroup $G^+ \leq G$, we conclude that $\mathscr{M} \supseteq \mathscr{E}_2$.

(b) We already mentioned that the G^+-modules $\mathscr{E}_1 = \bigoplus_{i=1}^t \mathscr{E}_{1i}$ and $\mathscr{E}_2$ share no common composition factor; in particular, k is not a composition factor of $\mathscr{E}_2$. Furthermore, since $\prod_{j \neq i} S_j$ acts trivially on V_i, we see that for distinct $i \neq j$ the only common G^+-composition factor that $\mathscr{E}_{1i}$ and $\mathscr{E}_{1j}$ can share is the principal character 1_{G^+}. Recall that $\mathscr{E}_{1i} \cong \mathscr{D} \otimes \mathscr{D}$ as S_i-modules. The irreducibility of G on V implies that $G_i := \mathrm{Stab}_G(V_i)$ acts irreducibly on V_i, and certainly $G^+ \lhd G_i$ acts homogeneously on V_i. By Proposition 6.6 applied to G_i, $\mathscr{E}_{1i}$ is a subquotient of $\mathscr{M}$. We have therefore shown that all *nontrivial* G^+-composition factors of $\mathscr{E} = \mathrm{End}(V)$ also occur in $\mathscr{M}$ with the same multiplicity, and so all the composition factors of the G^+-module $\mathscr{E}/\mathscr{M}$ (if any) are trivial. Applying Lemma 5.4 to the subgroup $Q'^t < G^+$, we conclude that $\mathscr{M} = \mathscr{E}$. □

Finally we can prove:

Theorem 6.9. *Suppose* (G, V) *is as in the case* (i) *of Theorem 2.4. Then* (G, V) *is weakly adequate.*

Proof. In view of Theorems 5.7, 6.8, and Propositions 5.8, 5.9, 5.11, we need to handle the case $(p, H, \dim W) = (7, 6{\cdot}\mathrm{PSL}_3(4), 6)$. In this case, L_i acts on each W_j either trivially or as $H_j \cong 6 \cdot \mathrm{PSL}_3(4)$. It follows by the faithfulness of G on V that $\mathbf{Z}(L_i)$ has exponent 6, and so L_i is (isomorphic to) either $X := (2 \times 2) \cdot 3 \cdot \mathrm{PSL}_3(4)$ or a quotient $6 \cdot \mathrm{PSL}_3(4)$ of X. We can also find k_i such that the kernel K_i of $G^+ = L_1 * \cdots * L_n$ acting on W_i contains $\prod_{j \neq k_i} L_j$. Without loss we may assume $k_1 = 1$.

(a) We claim that L_1 contains a subgroup $Q_1 = Z_1 \times \mathsf{A}_5$, whose conjugacy class is $\mathrm{Aut}(L_1)$-invariant (with $Z_1 := \mathbf{Z}(L_1)$). For this purpose, without loss of generality we may assume that $L_1 \cong X$. We consider a Levi subgroup $C_3 \times \mathrm{SL}_2(4) \cong C_3 \times \mathsf{A}_5$ of $\mathrm{SL}_3(4)$ which acts semisimply on the natural module $\mathbb{F}_4^3$. Then its conjugacy class in $\mathrm{SL}_3(4)$ is fixed by all the outer automorphisms of $\mathrm{SL}_3(4)$. Consider a faithful representation $\Lambda : X \to \mathrm{GL}_{18}(\mathbb{C})$ which is the sum of three irreducible representations, on which X acts with different kernels $\cong C_2$, and let Y be the full inverse image of A_5 in X. Note that involutions in $\mathrm{PSL}_3(4)$ lift to involutions in $6 \cdot \mathrm{PSL}_3(4)$, whereas involutions in A_5 lift to elements of order 4 in $2 \cdot \mathsf{A}_5$ [Conway et al. 1985]. It follows that $\Lambda(x)$ has order 2 for the inverse image $x \in X$ of any involution in A_5, and so $|x| = 2$. Hence $Y \cong (2 \times 2) \times \mathsf{A}_5$, and the claim follows.

Defining $Q_i < L_i$ similarly, we see that

$$Q = Q_1 * Q_2 * \cdots * Q_n$$

satisfies condition (i) of Lemma 5.3. Since Q_1 is self-normalizing in L_1, we see that $\mathbf{N}_{G^+}(Q) = Q$ and that $N := \mathbf{N}_G(Q)$ is a p'-group.

We will now inflate Brauer characters of L_1 acting on W_1 to X and then replace L_1 by X. According to [Jansen et al. 1995], L_1 has exactly six irreducible 7-Brauer characters φ_s of degree 6, $1 \leq s \leq 6$, lying above the six distinct characters λ_s of Z_1 (with kernels the three distinct central subgroups of order 2), and $(\varphi_s)_{Q_1} = \lambda_s \otimes (\alpha + \beta)$, where $\alpha \neq \beta \in \mathrm{Irr}(\mathsf{A}_5)$, and either

$$\{\alpha, \beta\} = \{1a, 5a\} \tag{6-6}$$

or

$$\{\alpha, \beta\} = \{3a, 3b\}, \tag{6-7}$$

depending on whether φ_s takes value 2 or -2 on involutions in A_5. (Here we adopt the notation that $\mathrm{Irr}(\mathsf{A}_5) = \{1a, 3a, 3b, 4a, 5a\}$.) In either case, we have that $(W_1)_Q = A_1 \oplus B_1$, where the Q-modules A_1 and B_1 are irreducible and nonisomorphic. As shown in the proof of Lemma 5.2, $NG^+ = G$ and $N_1G^+ = G_1 := \mathrm{Stab}_G(V_1)$ for $N_1 := N_{G_1}(Q)$. So we fix a decomposition $G = \bigsqcup_{i=1}^t g_iG_1$ with $g_i \in N$, $g_1 = 1$, and define $A_i := g_i(A_1) \subset W_i$ and $B_i := g_i(B_1) \subset W_i$. In particular, either (6-6) holds for all $(W_i)_Q$, or (6-7) holds for all $(W_i)_Q$.

We claim that Q also satisfies condition (ii) of Lemma 5.3. Indeed, assume that $W_i \not\cong W_j$. Now if $k_i \neq k_j$, then $L_{k_i} > Q_{k_i}$ acts trivially on W_j, but $\mathbf{Z}(Q_{k_i}) = Z_{k_i}$ acts nontrivially by scalars on W_i. In the case $k_i = k_j$, we may assume that $K_i \geq \prod_{s>1} L_s$, and so W_i and W_j afford the L_1-characters $\varphi, \varphi' \in \{\varphi_1, \ldots, \varphi_6\}$, lying above *different* characters λ, λ' of Z_1. Now $\mathbf{Z}(Q_1) = Z_1$ acts on W_i and W_j by scalars but via different characters λ, λ', so we are done.

(b) Suppose we are in the case of (6-7) and, moreover, $G_1 = \mathrm{Stab}_G(V_1)$ interchanges the two classes $5A = x^{L_1}$ and $5B = (x^2)^{L_1}$ of elements of order 5 of $L_1 = 6_1 \cdot \mathrm{PSL}_3(4)$. Certainly, we can choose $x \in \mathsf{A}_5 < Q_1$. Since $N_1G^+ = G_1$, we can find some element $g \in N_1$ that interchanges the classes $5A$ and $5B$. In this case g also interchanges the characters $\alpha = 3a$ and $\beta = 3b$ of A_5, but fixes W_1 and the central character $\lambda \in \{\lambda_1, \ldots, \lambda_6\}$ of Z_1. It follows that $\{A_1, \ldots, B_t\}$ forms a single N-orbit, and so by Lemma 5.3 the p'-group N acts irreducibly on V, and we are done.

(c) From now on we may assume that we are *not* in the case considered in (b). We claim that $\{A_1, \ldots, A_t\}$ and $\{B_1, \ldots, B_t\}$ are two distinct N-orbits. Assume the contrary. Then by the construction of A_i and B_j there must be some $h \in N$ such that $B_1 \cong A_1^h$. This is clearly impossible in the case of (6-6). In the case of (6-7), $h \in G_1$ and furthermore h fuses the two classes of elements of order 5 in A_5. Hence $h \in G_1$ fuses the classes $5A$ and $5B$ of L_1, contrary to our assumption.

Now we can apply Lemma 5.3 to see that $V_N = A \oplus B$ and so

$$\mathcal{M} \supseteq \mathrm{End}(A) \oplus \mathrm{End}(B) \tag{6-8}$$

by the Artin–Wedderburn theorem. We also decompose $\mathrm{End}(V) = \mathscr{E}_1 \oplus \mathscr{E}_2$ as G^+-modules, and note that the Q-modules

$$\mathscr{E}_1 := \bigoplus_{i=1}^{t} \mathrm{End}(V_i) \cong e^2 \bigoplus_{i=1}^{t} W_i^* \otimes W_i,$$
$$\mathscr{E}_2 := \bigoplus_{1 \leq i \neq j \leq t} \mathrm{Hom}(V_i, V_j) \cong e^2 \bigoplus_{1 \leq i \neq j \leq t} W_i^* \otimes W_j$$

share no common composition factor. Indeed, the p'-group $\mathbf{Z}(G^+) = Z_1 * \cdots * Z_n \leq \mathbf{Z}(Q)$ acts trivially on $\mathscr{E}_1$ and nontrivially by scalars on each $W_i^* \otimes W_j$ when $i \neq j$.

Moreover, if $k_i \neq k_j$, say $K_i \geq \prod_{s\neq 1} L_s$ and $K_j \geq \prod_{s\neq 2} L_s$, then $W_i^* \otimes W_j$ and $W_j^* \otimes W_i$ are irreducible over $L_1 \times L_2$ (and are acted on trivially by $\prod_{s>2} L_s$), with nontrivial central characters $\nu_1^{-1} \otimes \nu_2$ and $\nu_1 \otimes \nu_2^{-1}$ over $Z_1 * Z_2$, where $\nu_1, \nu_2 \in \{\lambda_1, \dots, \lambda_6\}$ have order 6. If $W_i \not\cong W_j$ but $k_i = k_j$, say $k_i = k_j = 1$, then W_i and W_j afford the L_1-characters $\varphi \neq \varphi'$ lying above different characters $\lambda \neq \lambda'$ of Z_1. We distinguish different scenarios for λ and λ':

(c1) λ and λ' coincide at $\boldsymbol{O}_2(Z_1)$ (then they must be different at $\boldsymbol{O}_3(Z_1)$, and in fact $\lambda' = \lambda^{-1}$). Here, $W_i^* \otimes W_j$ and $W_j^* \otimes W_i$ are reducible over L_1 (and are acted on trivially by $\prod_{s>1} L_s$), with distinct nontrivial central characters λ^{-2} and λ^2 over Z_1. Furthermore, the L_1-character of $W_i^* \otimes W_j$ is $\gamma_3 + \delta_3$, where $\gamma_3 \in \mathrm{IBr}(L_1)$ has degree 15, $\delta_3 \in \mathrm{IBr}(L_1)$ has degree 21, and

$$(\gamma_3)_{\mathsf{A}_5} = 3a + 3b + 4a + 5a, \quad (\delta_3)_{\mathsf{A}_5} = 2 \cdot 1a + 4a + 3 \cdot 5a. \tag{6-9}$$

(c2) λ and λ' coincide at $\boldsymbol{O}_3(Z_1)$ (then they must be different at $\boldsymbol{O}_2(Z_1)$). Here, $W_i^* \otimes W_j$ and $W_j^* \otimes W_i$ again are reducible over L_1 (and are acted on trivially by $\prod_{s>1} L_s$), with the same nontrivial central character $\lambda^{-1}\lambda'$ over Z_1. Furthermore, the L_1-character of $W_i^* \otimes W_j$ is $\gamma_2 + \delta_2$, where $\gamma_2 \in \mathrm{IBr}(L_1)$ has degree 10, $\delta_2 \in \mathrm{IBr}(L_1)$ has degree 26, and

$$(\gamma_2)_{\mathsf{A}_5} = 1a + 4a + 5a, \quad (\delta_2)_{\mathsf{A}_5} = 1a + 3a + 3b + 4a + 3 \cdot 5a. \tag{6-10}$$

Here we have used the fact that the character of $W_i^* \otimes W_j$ takes value $(\pm 2)^2 = 4$ at involutions in A_5.

(c3) λ and λ' differ at both $\boldsymbol{O}_2(Z_1)$ and $\boldsymbol{O}_3(Z_1)$. Here, $W_i^* \otimes W_j$ and $W_j^* \otimes W_i$ are irreducible over L_1 (and are acted on trivially by $\prod_{s>1} L_s$), with distinct nontrivial central characters $\lambda^{-1}\lambda'$ and $\lambda(\lambda')^{-1}$ over Z_1. Furthermore, the L_1-character of $W_i^* \otimes W_j$ is γ_6, where $\gamma_6 \in \mathrm{IBr}(L_1)$ has degree 36 and

$$(\gamma_6)_{\mathsf{A}_5} = 2 \cdot 1a + 3a + 3b + 2 \cdot 4a + 4 \cdot 5a. \tag{6-11}$$

(d) According to (6-8), $\mathcal{M}$ contains the subspace $\mathcal{A} := \mathrm{End}(C_1) \oplus \mathrm{End}(D_1)$ of $\mathrm{End}(V_1)$, which affords the character $e^2(\alpha^2 + \beta^2)$ of $\mathsf{A}_5 < Q_1$ (and is acted on trivially by Z_1). Note that the L_1-character of $\mathrm{End}(W_1)$ is $\varphi_i\overline{\varphi}_i = 1_{L_1} + \psi$, where $\psi \in \mathrm{IBr}(L_1)$ of degree 35 and

$$\psi_{\mathsf{A}_5} = 1a + 3a + 3b + 2 \cdot 4a + 4 \cdot 5a.$$

On the other hand, the A_5-character of the complement to $\mathcal{A}$ in $\mathrm{End}(V_1)$ is

$$e^2(\alpha + \beta)^2 - e^2(\alpha^2 + \beta^2) = 2e^2\alpha\beta,$$

which is $2e^2 \cdot 5a$ in the case of (6-6) and $2e^2(4a + 5a)$ in the case of (6-7); in particular, it does *not* contain $1a$. It follows by the observation right after (6-8) and Lemma 5.5 that $\mathcal{M} \supseteq \mathrm{End}(V_1)$ and so $\mathcal{M} \supseteq \mathcal{E}_1$.

(e) By (6-8), $\mathcal{M}$ contains the subspace $\mathcal{B}_{ij} := \mathrm{Hom}(C_i, C_j) \oplus \mathrm{Hom}(D_i, D_j)$ of $\mathcal{E}_{ij} := \mathrm{Hom}(V_i, V_j)$ whenever $i \neq j$ (recall that $(C_i)_Q \cong eA_i$ and $(D_i)_Q \cong eB_i$). We distinguish two cases according to whether k_i and k_j are equal or not.

First suppose that $k_i \neq k_j$, say $k_i = 1$ and $k_j = 2$. Then $\mathcal{E}_{ij}$ affords the $L_1 \times L_2$-character $e^2\overline{\theta}_1 \otimes \theta_2$ (where $\theta_i \in \mathrm{IBr}(L_i)$ has degree 6) and is acted on trivially by $\prod_{s>2} L_s$. Now the $Q_1 \times Q_2$-character of the complement to $\mathcal{B}_{ij}$ in $\mathrm{Hom}(V_i, V_j)$ when restricted to the subgroup $\mathsf{A}_5 \times \mathsf{A}_5$ is

$$e^2(\alpha_1 + \beta_1) \otimes (\alpha_2 + \beta_2) - e^2(\alpha_1 \otimes \alpha_2 + \beta_1 \otimes \beta_2) = e^2(\alpha_1 \otimes \beta_2 + \beta_1 \otimes \alpha_2)$$

(where α_1, β_1 play the role of α and β for the first factor A_5 and similarly for α_2, β_2). Also, the restriction of $\overline{\theta}_1 \otimes \theta_2$ to $\mathsf{A}_5 \times \mathsf{A}_5$ always contains an irreducible constituent distinct from $\alpha_1 \otimes \beta_2$ and $\beta_1 \otimes \alpha_2$, namely $\beta_1 \otimes \beta_2$.

Assume now that $k_i = k_j = 1$. Then the A_5-character of the complement to $\mathcal{B}_{ij}$ in $\mathcal{E}_{ij}$ is

$$e^2(\alpha + \beta)^2 - e^2(\alpha^2 + \beta^2) = 2e^2\alpha\beta,$$

which is $2e^2 \cdot 5a$ in the case of (6-6) and $2e^2(4a + 5a)$ in the case of (6-7). On the other hand, according to (6-9)–(6-11), the restriction to A_5 of each of the irreducible constituents γ and δ of $W_i^* \otimes W_j$ always contains either $1a$ or $3a$.

Now assume that $\mathcal{M} \neq \mathrm{End}(V)$. Working modulo $\mathcal{E}_1 \subset \mathcal{M}$, we see that $\mathcal{M} \supseteq \mathcal{B} := \bigoplus_{i \neq j} \mathcal{B}_{ij}$ has a nonzero complement in $\mathcal{E}_2 = \bigoplus_{i \neq j} \mathcal{E}_{ij}$. But the above analysis shows that *any* G^+-composition factor of $\mathcal{E}_2$ contains a Q-irreducible constituent which is *not* a Q-constituent of the complement to $\mathcal{B}$ in $\mathcal{E}_2$, a contradiction. □

Proof of Theorem 1.2. (a) First we consider the case where k is algebraically closed. Assume that G^+ is p-solvable. Then G is also p-solvable. Furthermore, $\dim V / \dim W$ divides $|G/G^+|$ by [Navarro 1998, Theorem 8.30], and so $p \nmid \dim V$. So we are done by Lemma 5.1. So we may now assume that G^+ is not p-solvable, $p > \dim W > 1$, and apply Theorem 2.4 to G. Then the statement follows from Theorem 4.5 in the case that G^+ is a central product of quasisimple groups of Lie type in characteristic p (if in addition $p > 3$), and from the results of Sections 5 and 6 in the remaining cases.

Suppose that $p = 3$ and $G^+ = L_1 * \cdots * L_n$ is a central product of quasisimple groups of Lie type in characteristic p (with $\mathbf{Z}(L_i)$ a p'-group for each i; see Theorem 2.4(iii)). Write $V_{G^+} = e \bigoplus_{i=1}^t W_i$ as usual. It is well known that the only quasisimple groups of Lie type in characteristic p that have a faithful representation of degree 2 over k are $\mathrm{SL}_2(p^a)$. Since $\dim W = 2$, we must have that $L_j \cong \mathrm{SL}_2(q)$ for a power $q > 3$ of 3 for all j (as the G^+-modules W_i are G-conjugate); moreover, for each i, there is a unique k_i such that L_j acts nontrivially on W_i precisely when $j = k_i$. Note that L_i contains a unique conjugacy class of cyclic subgroups T_i of order C_{q-1}. It is straightforward to check that the restrictions of all Brauer characters $\varphi \in \mathrm{IBr}_p(L_i)$ of degree 2 to $Q_i := N_{L_i}(T_i)$ are all irreducible and pairwise distinct. Letting $Q := Q_1 * \cdots * Q_n$ and arguing as in case (b1) of the proof of Theorem 5.7, we see that Q satisfies all the hypotheses of Lemma 5.2, whence we are done.

(b) Now we consider the general case. We will view G as a subgroup of $\mathrm{GL}(V)$ and let $\mathcal{M} := \langle g : g \in G \text{ semisimple}\rangle_k$ as usual. Since the kG-module V is absolutely irreducible, the $\bar{k}G$-module $\overline{V} := V \otimes_k \bar{k}$ is irreducible, and the condition $d < p$ implies that the dimension of any irreducible G^+-submodule in $\overline{V}$ is also less than p. By the previous case, $\mathcal{M} \otimes_k \bar{k} = \mathrm{End}(\overline{V})$. It follows that $\dim_k \mathcal{M} = (\dim V)^2$ and so $\mathcal{M} = \mathrm{End}(V)$.

□

7. Extensions and self-extensions, I: Generalities

First we record a convenient criterion about self-extensions in blocks of cyclic defect:

Lemma 7.1. *Suppose that G is a finite group and that V is an irreducible $\overline{\mathbb{F}}_pG$-representation that belongs to a block of cyclic defect. Then* $\mathrm{Ext}^1_G(V, V) \neq 0$ *if and only if V admits at least two nonisomorphic lifts to characteristic* 0. *In this case*, $\dim \mathrm{Ext}^1_G(V, V) = 1$.

Proof. Let B denote the block of V. If B has defect 0, V is projective and lifts uniquely to characteristic 0. Otherwise, B is a Brauer tree algebra. Note that $\mathrm{Ext}^1_G(V, V) \neq 0$ if and only if V embeds as subrepresentation of $\mathcal{P}(V)/V$. The Brauer tree shows that this happens if and only if either (i) B has an exceptional vertex and V is the unique edge incident with it, or (ii) B does not have an exceptional vertex and V is the unique edge of the tree. In (i), each exceptional representation in B lifts V, in (ii) both ordinary representations in B lift V, and it is clear that V has at most one lift in all other cases. To verify the final claim, note that $\mathrm{Hom}(V, \mathcal{P}(V)/V) \cong \mathrm{Ext}^1_G(V, V)$, and that in a Brauer tree algebra V occurs at most once in $\mathrm{soc}(\mathcal{P}(V)/V)$. □

In fact, as pointed out to us by V. Paskunas, one direction of Lemma 7.1 holds for any finite group G: if $\mathrm{Ext}^1_G(V, V) = 0$ then V has at most one characteristic-0 lift. Indeed, if V has no self-extension, we may first realize all characteristic-0 lifts over some finite extension $\mathbb{E}$ of $\mathbb{Q}_p$, as well as V over the residue field of $\mathbb{E}$. Then the universal deformation ring R of V over the ring $\mathbb{O}_{\mathbb{E}}$ is a quotient of $\mathbb{O}_{\mathbb{E}}$. But then $|\mathrm{Hom}_{\mathbb{O}_{\mathbb{E}}\text{-alg}}(R, \mathbb{O}_{\mathbb{E}})| \leq 1$, i.e., V has at most one characteristic-0 lift.

We will frequently use the following simple observations:

Lemma 7.2. *Let V be a finite-dimensional vector space over k and $G \le \mathrm{GL}(V)$ a finite absolutely irreducible subgroup. Write $V|_{G^+} = e\bigoplus_{i=1}^t W_i$, where the G^+-modules W_i are absolutely irreducible and pairwise nonisomorphic. Suppose that $\mathrm{Ext}^1_{G^+}(W_i, W_j) = 0$ for all i, j. Then $\mathrm{Ext}^1_G(V, V) = 0$.*

Proof. Since G^+ contains a Sylow p-subgroup of G, $\mathrm{Ext}^1_G(V, V)$ embeds in

$$\mathrm{Ext}^1_{G^+}(V_{G^+}, V_{G^+}) = \mathrm{Ext}^1_{G^+}\left(e\bigoplus_{i=1}^t W_i, e\bigoplus_{i=1}^t W_i\right) \cong e^2 \bigoplus_{i,j} \mathrm{Ext}^1_{G^+}(W_i, W_j) = 0. \quad \square$$

Lemma 7.3. *Let N be a normal subgroup of a finite group X and let A and B be finite-dimensional $k(X/N)$-modules. Consider $\mathrm{Ext}^1_X(A, B)$, where we inflate A and B to kX-modules.*

(i) *If $\mathrm{Ext}^1_X(A, B) = 0$, then $\mathrm{Ext}^1_{X/N}(A, B) = 0$.*

(ii) *If $\mathrm{Ext}^1_{X/N}(A, B) = 0$ and $\boldsymbol{O}^p(N) = N$, then $\mathrm{Ext}^1_X(A, B) = 0$.*

Proof. (i) is trivial. For (ii), let V be any extension of the kX-module A by the kX-module B, and let $\Phi : X \to \mathrm{GL}(V)$ denote the corresponding representation. Since N acts trivially on A and B, we see that $\Phi(N)$ is a p-group. But $\boldsymbol{O}^p(N) = N$; hence $\Phi(N) = 1$, i.e., N acts trivially on V. Now, $V \cong A \oplus B$ as $\mathrm{Ext}^1_{X/N}(A, B) = 0$. $\square$

Next we recall Holt's inequality in cohomology [1980]:

Lemma 7.4. *Let G be a finite group, $N \lhd G$, and let V be a finite-dimensional kG-module. Then for any integer $m \ge 0$ we have*

$$\dim H^m(G, V) \le \sum_{j=0}^m \dim H^j(G/N, H^{m-j}(N, V)).$$

From now on we again assume that k is algebraically closed.

Corollary 7.5. *Let $G = G_1 \times G_2$ be a direct product of finite groups and let V_i be a nontrivial irreducible kG_i-module for $i = 1, 2$.*

(i) *If we view $V_1 \otimes V_2$ as a kG-module, then $H^1(G, V_1 \otimes V_2) = 0$.*

(ii) *If we inflate V_1 and V_2 to kG-modules, then $\mathrm{Ext}^1_G(V_1, V_2) = 0$.*

Proof. For (i), applying Lemma 7.4 to $N := G_1$ we get

$$\dim H^1(G, V) \le \dim H^0(G_2, H^1(G_1, V)) + \dim H^1(G_2, H^0(G_1, V)).$$

Now the G_1-module V is a direct sum of $\dim V_2$ copies of V_1 and V_1 is nontrivial irreducible, whence $H^0(G_1, V) = 0$. Next, $H^1(G_1, V) \cong H^1(G_1, V_1) \otimes V_2$ as G_2-modules, with G_2 acting trivially on the first tensor factor. It follows that

$$H^0(G_2, H^1(G_1, V)) \cong H^1(G_1, V_1) \otimes H^0(G_2, V_2) = 0$$

as V_2 is nontrivial irreducible, and so we are done.

Part (ii) follows from (i) since $\mathrm{Ext}^1_G(V_1, V_2) \cong H^1(G, V_1^* \otimes V_2)$ and V_1^* is a nontrivial absolutely irreducible kG_1-module. □

Corollary 7.6. *Let the finite group H be a central product of quasisimple subgroups $H = H_1 * \cdots * H_n$, where $\boldsymbol{Z}(H_i)$ is a p'-group for all i. For $i = 1, 2$, let W_i be a nontrivial irreducible kH-module such that the action of H on W_i induces a quasisimple subgroup of* $\mathrm{GL}(W_i)$. *Suppose that the kernels of the actions of H on W_1 and on W_2 are different. Then* $\mathrm{Ext}^1_H(W_1, W_2) = 0$.

Proof. View H as a quotient of $L := H_1 \times \cdots \times H_n$ by a central p'-subgroup and inflate W_i to a kL-module. Next, write $W_i = W_1^i \otimes \cdots \otimes W_n^i$ for some absolutely irreducible kH_j-module W_j^i, $1 \le i \le 2$, $1 \le j \le n$. Since H_j is quasisimple, if $\dim W_j^i = 1$ then H_j acts trivially on W_i. On the other hand, if $\dim W_j^i > 1$, then H_j induces a quasisimple subgroup of $\mathrm{GL}(W_j^i)$. Hence, the condition that the action of H on W_i induces a quasisimple subgroup of $\mathrm{GL}(W_i)$ implies that $\dim W_j^i > 1$ for exactly one index $j = k_i$, whence the kernel of L on W_i is

$$H_1 \times \cdots \times H_{k_i - 1} \times \boldsymbol{C}_{H_{k_i}}(W_{k_i}^i) \times H_{k_i + 1} \times \cdots \times H_n.$$

Note that the hypothesis on H_i imply that $\prod_{j \ne k_1,\, k_2} H_j$ has no nontrivial p-quotient. Hence, by Lemma 7.3 there is no loss in taking the quotient of L by $\prod_{j \ne k_1,\, k_2} H_j$. If $k_1 \ne k_2$, then we are reduced to the case where $L = H_{k_1} \times H_{k_2}$, W_1 is a nontrivial H_{k_1}-module inflated to L and W_2 is a nontrivial H_{k_2}-module inflated to L, whence we are done by Corollary 7.5(ii). Suppose now that $k_1 = k_2$, say $k_1 = k_2 = 1$ for brevity. Then we are reduced to the case where $L = H_1$ and $K_1 \ne K_2$, with $K_i = \boldsymbol{C}_{H_1}(W_1^i) \le \boldsymbol{Z}(H_1)$. By Schur's lemma, $\boldsymbol{Z}(H_1)$ acts on W_i by scalars and semisimply, via a linear character λ_i. Since $K_1 \ne K_2$, we see that $\lambda_1 \ne \lambda_2$. It follows (by considering $\boldsymbol{Z}(H_1)$-blocks, or by considering λ_i-eigenspaces for $\boldsymbol{Z}(H_1)$ in any extension of W_1 by W_2) that $\mathrm{Ext}^1_L(W_1, W_2) = 0$. □

More generally, we record the following consequence of the Künneth formula:

Lemma 7.7 [Benson 1998, 3.5.6]. *Let H be a finite group. Assume that H is a central product of subgroups H_i for $1 \le i \le t$ and that $\boldsymbol{Z}(H)$ is a p'-group. Let X and Y be irreducible kH-modules. Write $X = X_1 \otimes \cdots \otimes X_t$ and $Y = Y_1 \otimes \cdots \otimes Y_t$, where X_i and Y_i are irreducible kH_i-modules.*

(i) *If $X_i \ncong Y_i$ for at least two i, then* $\mathrm{Ext}^1_H(X, Y) = 0$.

(ii) *If $X_1 \ncong Y_1$ but $X_i \cong Y_i$ for $i > 1$, then* $\mathrm{Ext}^1_H(X, Y) \cong \mathrm{Ext}^1_{H_1}(X_1, Y_1)$.

(iii) *If $X_i \cong Y_i$ for all i, then* $\mathrm{Ext}^1_H(X, Y) \cong \bigoplus_i \mathrm{Ext}^1_{H_i}(X_i, Y_i)$.

We continue with several general remarks:

Lemma 7.8. *Let V be a kG-module of finite length.*

(i) *Suppose that X is a composition factor of V such that V has no indecomposable subquotient of length* 2 *with X as a composition factor. Then $V \cong X \oplus M$ for some submodule $M \subset X$.*

(ii) *Suppose that* $\operatorname{Ext}^1_G(X, Y) = 0$ *for any two composition factors X, Y of V. Then V is semisimple.*

Proof. (i) We will assume that $V \ncong X$. Let U be a submodule of V of smallest length that has X as a composition factor. First we show that $U \cong X$. If not, then U has a composition series $U = U_0 > U_1 > \cdots > U_m = 0$ for some $m \geq 2$. Note that $U/U_1 \cong X$, as otherwise X would be a composition factor of $U_1 \subset U$, contradicting the choice of U. Now U/U_2 is a subquotient of length 2 of V with X as a quotient. By the hypothesis, $U/U_2 = U'/U_2 \oplus U''/U_2$ with $U'/U_2 \cong X$ and $U'' \supset U_2$, again contradicting the choice of U.

Now let M be a submodule of V of largest length such that $M \cap U = 0$. In particular, $V/M \supseteq (M+U)/M \cong X$. Assume furthermore that $V \neq M + U$. Then we can find a submodule $V' \subseteq V$ such that $V'/(M+U)$ is simple. Again, V'/M is a subquotient of length 2 of V with X as a submodule. So by the hypothesis, $V'/M = (M+U)/M \oplus N/M$ for some submodule $N \subseteq V$ containing M properly. But then

$$N \cap U = (N \cap (M+U)) \cap U = M \cap U = 0,$$

contrary to the choice of M. Thus $V = M \oplus U$ is decomposable.

(ii) Induction on the length of V. If V is not simple, then by (i) we have $V \cong V' \oplus V''$ for some nonzero submodules V' and V''. Now apply the induction hypothesis to V' and V''. □

Lemma 7.9. *Let V be a kG-module. Suppose that U is a composition factor of V of multiplicity* 1 *and that U occurs both in* soc V *and* head V. *Then $V \cong U \oplus M$ for some submodule $M \subset V$.*

Proof. Let $U_1 \cong U$ be a submodule of V. Since U occurs in head V, there is $M \subset V$ such that $V/M \cong U$. Now if $M \supseteq U_1$, then U would have multiplicity ≥ 2 in V. Hence $V = U_1 \oplus M$. □

Lemma 7.10. *Let V be a kG-module of finite length. Suppose the set of isomorphism classes of composition factors of V is a disjoint union $\mathscr{X} \cup \mathscr{Y}$ of nonempty subsets such that, for any $U \in \mathscr{X}$ and $W \in \mathscr{Y}$, there is no indecomposable subquotient of length* 2 *of V with composition factors U and W. Then V is decomposable.*

Proof. Let X and Y denote the largest submodules of V with all composition factors belonging to $\mathscr{X}$ and $\mathscr{Y}$, respectively. By definition, $X \cap Y = 0$. We claim that $V = X \oplus Y$. If not, we can find a submodule $Z \supset X \oplus Y$ of V such that

$U := Z/(X \oplus Y)$ is a simple G-module. Suppose for instance that $U \in \mathcal{X}$. Applying Lemma 7.8(i) to the G-module Z/X and its composition factor U, we see that $Z/X \cong U \oplus Y$. This implies that Z contains a submodule T with $T/X \cong U$, contradicting the choice of X.

Now $X, Y \neq 0$ as $\mathcal{X}, \mathcal{Y} \neq \varnothing$. It follows that V is decomposable. □

Lemma 7.11. *Let V be an indecomposable kG-module.*

(i) *If the G^+-module V_{G^+} admits a composition factor L of dimension* 1, *then all composition factors of V_{G^+} belong to $B_0(G^+)$.*

(ii) *Suppose a normal p'-subgroup N of G acts by scalars on a composition factor L of the G-module V. Then N acts by scalars on V. If in addition V is faithful then $N \leq \mathbf{Z}(G)$.*

Proof. (i) Since $G^+ = \boldsymbol{O}^{p'}(G^+)$, it must act trivially on L. Let X (resp. Y) denote the largest submodule of the G^+-module V with all composition factors belonging (resp. not belonging) to $B_0(G^+)$. By their definition and the definition of G^+-blocks, $V = X \oplus Y$. Note that both X and Y are G-stable as $G^+ \lhd G$. Since V is indecomposable, we see that $Y = 0$ and $V = X$.

(ii) Note that N acts completely reducibly on V and G permutes the N-homogeneous components of V. Since V is indecomposable, it follows that this action is transitive, whence all composition factors of the N-module V are G-conjugate. But, among them, the (unique) linear composition factor of L_N is certainly G-invariant. Hence this is the unique composition factor of V_N, and so N acts by scalars on V. □

8. Indecomposable representations of $\mathrm{SL}_2(q)$

We first prove a lemma:

Lemma 8.1. *Suppose that S, T are irreducible* $\mathrm{SL}_2(\mathbb{F}_q)$*-representations over $\overline{\mathbb{F}}_p$ with $q = p^n$, $n \geq 2$, and E is a nonsplit extension of T by S. Then* $\dim E \geq p$ *and $S \not\cong T$. Moreover, if* $\dim S = \dim T$ *then* $\dim E \geq (p^2 - 1)/2$.

Proof. This is immediate from Corollary 4.5(a) in [Andersen et al. 1983]. □

Proposition 8.2. *Suppose that V is a reducible, self-dual, indecomposable representation of* $\mathrm{SL}_2(\mathbb{F}_q)$ *over $\overline{\mathbb{F}}_p$, where $q = p^n$. If* $\dim V < 2p - 2$, *then $q = p$ and one of the following holds*:

(i) $\dim V = p$ *and* $V \cong \mathcal{P}(\mathbb{1})$.

(ii) $\dim V = p + 1$ *and V is the unique nonsplit self-extension of* $L((p-1)/2)$.

(iii) $\dim V = p - 1$ *and V is the unique nonsplit self-extension of* $L((p-3)/2)$.

Conversely, all the listed cases give rise to examples.

Proof. Note that $p > 2$.

(a) Suppose first that $q = p$. If V is projective, then since $\dim V < 2p$, we must have $V \cong \mathcal{P}(\mathbb{1})$, which is uniserial of shape $(L(0) \mid L(p-3) \mid L(0))$ and of dimension p. (See for example [Alperin 1986].) If V is nonprojective, then, as $\mathrm{SL}_2(p)$ has a cyclic Sylow p-subgroup, V is one of the "standard modules" described in [Janusz 1969, §5]. As V is self-dual, the standard modules are described by paths in the Brauer tree as in [Janusz 1969, (5.2)(b)] with $P_0 = Q = P_{k+1}$. By inspecting the Brauer trees of $\mathrm{SL}_2(p)$ (see, e.g., [Alperin 1986]) and using that $\dim V < 2p-2$, we deduce moreover that $k = 1$ above, obtaining the modules in (ii), (iii).

In case (i), it is obvious that the module is self-dual since it is $\mathcal{P}(\mathbb{1})$. In cases (ii) and (iii) the uniqueness of the isomorphism class of the extension implies that it is self-dual.

(b) Now suppose that $q > p$. We need to show that no such V exists. (In fact we will show this holds even under the weaker bound $\dim V < 2p$.) Pick an irreducible subrepresentation $L(\lambda)$ of V, where $\lambda = \sum_{i=0}^{n-1} p^i \lambda_i$, $0 \le \lambda_i \le p-1$. Then V has a subquotient isomorphic to a nonsplit extension $0 \to L(\lambda) \to E \to L(\mu) \to 0$, where $\mu = \sum_{i=0}^{n-1} p^i \mu_i$, $0 \le \mu_i \le p-1$. By Lemma 8.1 we know that $\lambda \ne \mu$; hence $2\dim L(\lambda) + \dim L(\mu) < 2p$. By Corollary 4.5(a) in [Andersen et al. 1983] we deduce that, up to a cyclic relabeling of the indices, $\lambda = \lambda_0 + p$, $\mu = p-2-\lambda_0$, and $\mu > (2p-3)/3 \ge 1$. In particular, μ uniquely determines λ. Hence, if $\operatorname{soc} V$ contains two nonisomorphic irreducible representations, then V admits indecomposable subrepresentations of length two that intersect in zero, so $\dim V \ge 2p$ by Lemma 8.1. Therefore, $\operatorname{soc} V \cong L(\lambda)^{\oplus r}$ for some $r \ge 1$.

Suppose first that $r \ge 2$. We claim that $\operatorname{soc}_2 V / \operatorname{soc} V \cong L(\mu)^{\oplus s}$ for some $0 \le \mu < p^n$ and some $s \ge 1$. (Here $\operatorname{soc}_i M$ is the increasing filtration determined by $\operatorname{soc}_0 M = 0$ and $\operatorname{soc}_i M / \operatorname{soc}_{i-1} M = \operatorname{soc}(M / \operatorname{soc}_{i-1} M)$. Note that the socle filtration is compatible with subobjects.) Note that any constituent of $\operatorname{soc}_2 V / \operatorname{soc} V$ extends $L(\lambda)$, and hence by above it is uniquely determined, unless $n = 2$ and $\lambda_0 = 1$. In the latter case, the constituents can be $L(\mu')$, $L(\mu'')$, where $\mu' = p-3$, $\mu'' = p(p-3)$. But only one of them can occur since $\dim L(\lambda) + \dim L(\mu') + \dim L(\mu'') = 2p$, and this proves the claim. Note that $L(\mu)$ can occur only once in V by Lemma 8.1; in particular, $s = 1$. We claim that $\dim \operatorname{Ext}^1(L(\mu), L(\lambda)) \ge r \ge 2$. Otherwise, $\operatorname{soc}_2 V$ is decomposable, so we obtain a splitting $\pi : \operatorname{soc}_2 V \to L(\lambda) \subset \operatorname{soc} V$. But $\operatorname{Ext}^1(V/\operatorname{soc}_2 V, L(\lambda)) = 0$, so we can extend π to a splitting of V, a contradiction. Hence $\dim \operatorname{Ext}^1(L(\mu), L(\lambda)) \ge 2$ and by Corollary 4.5(b) in [Andersen et al. 1983] we deduce that $n = 2$ and $\lambda_i, \mu_i \in \{(p-3)/2, (p-1)/2\}$ for all i. (Note that we can get all four combinations with $\lambda_i + \mu_i = p-2$, unlike what is claimed in that corollary.) This contradicts that $|\{\lambda_i, \mu_i : 0 \le i \le n-1\}| \ge 3$ (by above).

Suppose that $r = 1$, so $\operatorname{soc} V$ is irreducible. Note that $\operatorname{soc}_3 V = V$ by Lemma 8.1, as each constituent in a socle layer extends at least one constituent of the previous socle layer. As $\operatorname{soc} V$ is irreducible, V embeds in the projective indecomposable module $U_n(\lambda)$ whose socle is $L(\lambda)$. We have $V \subset \operatorname{soc}_3 U_n(\lambda)$. Note that $\lambda_i < p-1$ for all i, as $\dim V < 2p$. By Lemma 8.1, $L(\lambda)$ does not occur in $\operatorname{soc}_2 U_n(\lambda)/\operatorname{soc} U_n(\lambda)$. Also, $L(\lambda)$ occurs precisely n times in $\operatorname{soc}_3 U_n(\lambda)/\operatorname{soc}_2 U_n(\lambda)$. (Theorems 4.3 and 3.7 in [Andersen et al. 1983] imply that this is the case, unless $n = 2$ and $\lambda_i \in \{(p-3)/2, (p-1)/2\}$ for all i. But by above $\lambda_i < (p-3)/3 \leq (p-3)/2$ for some i.) Let $M_i = L(\lambda_0) \otimes L(\lambda_1)^{(p)} \otimes \cdots \otimes Q_1(\lambda_i)^{(p^i)} \otimes \cdots \otimes L(\lambda_{n-1})^{(p^{n-1})}$ and $M := M_0 + \cdots + M_{n-1} \subset U_n(\lambda)$ in the notation of [Andersen et al. 1983, §3]. Note by Theorems 4.3 and 3.7 in [Andersen et al. 1983] that $\operatorname{soc}_2 U_n(\lambda) \subset M \subset \operatorname{soc}_3 U_n(\lambda)$ and that $M/\operatorname{soc}_2 U_n(\lambda) \cong L(\lambda)^{\oplus n}$. Therefore $V \subset M$, so

$$\frac{V}{L(\lambda)} \subset \frac{M}{L(\lambda)} = \frac{M_0}{L(\lambda)} \oplus \cdots \oplus \frac{M_{n-1}}{L(\lambda)}.$$

As $\operatorname{head}(M_i/L(\lambda)) \cong L(\lambda)$, there exists i such that $V/L(\lambda)$ surjects onto $M_i/L(\lambda)$. Thus $\dim V \geq \dim M_i \geq 2p$.

□

9. Finite groups with indecomposable modules of small dimension

Throughout this section, we assume that $k = \bar{k}$ is a field of characteristic $p > 3$. We want to describe the structure of finite groups G that admit reducible indecomposable modules of dimension $\leq 2p-2$. The next results essentially reduce us to the case of quasisimple groups.

Lemma 9.1. *Let G be a finite group, $p > 3$, and V be a faithful kG-module of dimension $< 2p$. Suppose that $\boldsymbol{O}_p(G) = 1$ and $\boldsymbol{O}_{p'}(G) \leq \boldsymbol{Z}(G)$. Then $F(G) = \boldsymbol{O}_{p'}(G) = \boldsymbol{Z}(G)$, $F^*(G) = E(G)\boldsymbol{Z}(G)$, and $G^+ = E(G)$ is either trivial or a central product of quasisimple groups of order divisible by p. In particular, G has no composition factor isomorphic to C_p, and so $H^1(G,k) = 0$.*

Proof. (a) Since $\boldsymbol{O}_p(G) = 1$, $Z := \boldsymbol{Z}(G) \leq F(G) \leq \boldsymbol{O}_{p'}(G)$. It follows that $F(G) = Z = \boldsymbol{O}_{p'}(G)$, and $F^*(G) = E(G)Z$. If moreover $E(G) = 1$, then

$$Z = F(G) = F^*(G) \geq \boldsymbol{C}_G(F^*(G)) = G,$$

whence G is an abelian p'-group, and $G^+ = 1 = E(G)$.

(b) Assume now that $E(G) > 1$ and write $E(G) = L_1 * \cdots * L_t$, a central product of $t \geq 1$ quasisimple subgroups. Since $\boldsymbol{O}_{p'}(E(G)) \leq \boldsymbol{O}_{p'}(G) = Z$, $p \mid |L_i|$ for all i.

Next we show that $\boldsymbol{N}_G(L_i)/\boldsymbol{C}_G(L_i)L_i$ is a p'-group for all i. Indeed, note that the L_i-module V admits a nontrivial composition factor U of dimension $< 2p$. Otherwise it has a composition series with all composition factors being trivial, whence L_i acts on V as a p-group. Since V is faithful and L_i is quasisimple, this is a contradiction. So we can apply Theorem 2.1 and [Guralnick et al. 2014, Theorem 2.1] to the image of L_i in $\mathrm{GL}(U)$. In particular, denoting $S_i := L_i/\mathbf{Z}(L_i)$, one can check that $\mathrm{Out}\, S_i$ is a p'-group, unless it is a simple group of Lie type in characteristic p. In the former case we are done since $\mathbf{N}_G(L_i)/\mathbf{C}_G(L_i)L_i \hookrightarrow \mathrm{Out}\, S_i$. Consider the latter case. Observe that $\mathbf{Z}(L_i) \le \mathbf{Z}(E(G)) \le F(G)$ is a p'-group. So we may replace L_i by its simply connected isogenous version $\mathcal{G}^F$, where $F : \mathcal{G} \to \mathcal{G}$ is a Steinberg endomorphism on a simple simply connected algebraic group $\mathcal{G}$ in characteristic p. If moreover p divides $|\mathbf{N}_G(L_i)/\mathbf{C}_G(L_i)L_i|$, then $\mathbf{N}_G(L_i)$ induces an outer automorphism σ of L_i of order p. As $p > 3$, this can happen only when σ is a field automorphism. More precisely, L_i is defined over a field $\mathbb{F}_{p^{bp}}$ (for some $b \ge 1$), where $\mathbb{F}_{p^{bp}}$ is the smallest splitting field for L_i [Kleidman and Liebeck 1990, Proposition 5.4.4] and σ is induced by the field automorphism $x \mapsto x^{p^b}$. Since $\dim U \ge 2 > (\dim V)/p$, U must be σ-invariant. In turn, this implies by [Kleidman and Liebeck 1990, Proposition 5.4.2] that U and its (p^b)-th Frobenius twist are isomorphic. In this case, the proofs of Proposition 5.4.6 and Remark 5.4.7 of [Kleidman and Liebeck 1990] show that $\dim U \ge 2^p > 2p$, a contradiction.

(c) Recall that $\mathbf{C}_G(E(G)) = \mathbf{C}_G(F^*(G)) \le F^*(G) = E(G)Z$, whence $\mathbf{C}_G(E(G)) = Z$. Also, G acts via conjugation on the set $\{L_1, \dots, L_t\}$, with kernel (say) N. We claim that $p \nmid |G/N|$. If not, then we may assume that some p-element $g \in G$ permutes $L_1, \dots, L_p$ cyclically. Arguing as in (b), we see that L_1 acts nontrivially on some composition factor U of the $E(G)$-module V, and we can write $U = U_1 \otimes \cdots \otimes U_t$, where $U_i \in \mathrm{IBr}_p(L_i)$. If U is not g-invariant, then $\dim V \ge p(\dim U) \ge 2p$, a contradiction. Hence U is g-invariant. It follows that $2 \le \dim U_1 = \cdots = \dim U_p$ and so $\dim U \ge 2^p > 2p$, again a contradiction.

Now $N/E(G)Z$ embeds in $\prod_{i=1}^t \mathrm{Out}\, L_i$. Furthermore, the projection of N into $\mathrm{Out}\, L_i$ induces a subgroup of $\mathbf{N}_G(L_i)/\mathbf{C}_G(L_i)L_i$, which is a p'-group by (b). It follows that $N/E(G)Z$ is a p'-group, and so $G^+ = E(G)$. The last statement also follows. □

The next result on H^1 follows from standard results on H^1 — see [Guralnick et al. 2007, Lemma 5.2] and the main result of [Guralnick 1999].

Lemma 9.2. *Let G be a finite group and let V be a faithful irreducible kG-module. Assume that $H^1(G, V) \ne 0$. Then $\mathbf{O}_{p'}(G) = \mathbf{O}_p(G) = 1$, $E(G) = L_1 \times \cdots \times L_t$ and $V_{E(G)} = W_1 \oplus \cdots \oplus W_t$, where the L_i are isomorphic nonabelian simple groups of order divisible by p, W_i is an irreducible kL_i-module, and L_j, $j \ne i$ acts trivially on W_i. Moreover,* $\dim H^1(G, V) \le \dim H^1(L_1, W_1)$, $\dim W_i \ge p-2$ *and* $\dim V \ge t(p-2)$. *In particular, if G is not almost simple, then either* $\dim V = 2p-4, 2p-2$ *or* $\dim V \ge 2p$, *or* $(p, \dim V) = (5, 9)$.

Lemma 9.3. *Let V be a faithful indecomposable kG-module with two composition factors V_1, V_2. Assume that $\boldsymbol{O}_p(G) = 1$ and $\dim V \leq 2p - 2$. If $J := \boldsymbol{O}_{p'}(G^+) \not\leq \boldsymbol{Z}(G^+)$, then*:

(i) $p = 2^a + 1$ *is a Fermat prime.*

(ii) $\dim V_1 = \dim V_2 = p - 1$.

(iii) $J/\boldsymbol{Z}(J)$ *is elementary abelian of order* 2^{2a}.

(iv) $H^1(G^+, k) \neq 0$.

Proof. Since $\mathrm{Ext}^1_G(V_1, V_2) \hookrightarrow \mathrm{Ext}^1_{G^+}(V_1, V_2)$, there are irreducible G^+-submodules W_i of V_i for $i = 1, 2$ such that $\mathrm{Ext}^1_{G^+}(W_1, W_2) \neq 0$. Assume that J acts by scalars on at least one of the W_i. Then, by Lemma 7.11(ii), J acts by scalars on both W_1 and W_2. If W_1' is any G^+-composition factor of V_1, then W_1' is G-conjugate to W_1. But $J \lhd G$, so we see that J acts by scalars on W_1'. Thus J acts by scalars on all G^+-composition factors of V_1, and similarly for V_2. Consider a basis of V consistent with a G^+-composition series of V, and any $x \in J$ and $y \in G^+$. Then $[x, y]$ acts as the identity transformation on each G^+-composition factor in this series, and so it is represented by an upper unitriangular matrix in the chosen basis. The same is true for any element in $[J, G^+] \lhd G$. Since V is faithful, we see that $[J, G^+] \leq \boldsymbol{O}_p(G) = 1$ and so $J \leq \boldsymbol{Z}(G^+)$, a contradiction.

Thus J cannot act by scalars on any W_i. Let Φ_i denote the representation of G^+ on W_i. Then $H := \Phi_i(G^+) < \mathrm{GL}(W_i)$ has no nontrivial p'-quotient, and contains a nonscalar normal p'-subgroup $\Phi_i(J)$. Applying Theorem 2.1 and also [Blau and Zhang 1993, Theorem A] to H, we conclude that $p = 2^a + 1$ is a Fermat prime, $\dim W_i = p - 1$, and $Q := \boldsymbol{O}_{p'}(H)$ acts irreducibly on W_i. Furthermore, $\boldsymbol{Z}(Q) = \boldsymbol{Z}(H)$, and H/Q acts irreducibly on $Q/\boldsymbol{Z}(Q)$, an elementary abelian 2-group of order 2^{2a}. Now $\Phi_i(J)$ is a normal p'-subgroup of H that is *not* contained in $\boldsymbol{Z}(Q)$. It follows that $\Phi_i(J)\boldsymbol{Z}(Q) = Q$, $\boldsymbol{Z}(\Phi_i(J)) = \Phi_i(J) \cap \boldsymbol{Z}(Q)$, J is irreducible on W_i, and $\Phi_i(J)/\boldsymbol{Z}(\Phi_i(J)) \cong Q/\boldsymbol{Z}(Q)$ is elementary abelian of order 2^{2a}. Since $\dim V \leq 2p - 2$, it also follows that $W_i = V_i$.

Letting $A := V_1^* \otimes V_2$, we then see that $A = [J, A] \oplus \boldsymbol{C}_A(J)$ as J-modules. Next,

$$0 \neq \mathrm{Ext}^1_G(V_1, V_2) \cong H^1(G, A) \cong H^1(G, \boldsymbol{C}_A(J)),$$

since $H^1(G, [J, A]) = 0$ by the inflation restriction sequence. It follows that $\boldsymbol{C}_A(J) \neq 0$. But J is irreducible on both V_1 and V_2, so we must have that $\dim \boldsymbol{C}_A(J) = 1$ and $V_1 \cong V_2$ as J-modules. Since G^+ acts trivially on any 1-dimensional module, it follows that $H^1(G^+, k) \neq 0$. Since $W_1 \cong W_2$ as J-modules and V is a faithful semisimple J-module, we also see that $\mathrm{Ker}(\Phi_1) \cap J = \mathrm{Ker}(\Phi_2) \cap J = 1$. Thus Φ_i is faithful on J, and so $J/\boldsymbol{Z}(J)$ is elementary abelian of order 2^{2a}. □

Lemma 9.4. *Let V be a faithful indecomposable kG-module with two composition factors V_1, V_2 of dimension > 1, $p > 3$, and $\mathbf{O}_p(G) = 1$.*

(i) *Assume that $\mathbf{O}_{p'}(G^+) \le \mathbf{Z}(G^+)$, and either* $\dim V < 2p - 2$ *or* $\dim V_1 = \dim V_2 = p - 1$. *If G^+ is not quasisimple, then $G^+ = L_1 * L_2$ is a central product of two quasisimple groups,* $\dim V_1 = \dim V_2 = p - 1$ *and, up to relabeling the L_i, one of the following holds:*

   (a) *$V_i = A_i \otimes B$ as G^+-modules, where $A_i \in \mathrm{IBr}_p(L_1)$ is of dimension $(p-1)/2$ and $B \in \mathrm{IBr}_p(L_2)$ is of dimension 2; furthermore,* $\mathrm{Ext}^1_{L_1}(A_1, A_2) \ne 0$.

   (b) *$V_i = (A_i \otimes k) \oplus (k \otimes B_i)$ as G^+-modules, where $A_i \in \mathrm{IBr}_p(L_1)$ has dimension $(p-1)/2$, and some $g \in G$ interchanges L_1 with L_2 and A_i with B_i. Furthermore,* $\mathrm{Ext}^1_{L_1}(A_1, A_2) \ne 0$.

(ii) *If* $\dim V < 2p - 2$, *then G^+ is quasisimple.*

Proof. (i) By Lemma 9.1 applied to G^+, $G^+ = (G^+)^+ = E(G^+) = L_1 * L_2 * \cdots * L_t$, a central product of t quasisimple groups. Suppose $t > 1$. Since $\mathrm{Ext}^1_G(V_1, V_2) \hookrightarrow \mathrm{Ext}^1_{G^+}(V_1, V_2)$, there are irreducible G^+-submodules W_i of V_i for $i = 1, 2$ such that $\mathrm{Ext}^1_{G^+}(W_1, W_2) \ne 0$. Write $W_i = W_{i1} \otimes \cdots \otimes W_{it}$, where W_{ij} is an irreducible L_j-module. By Lemma 7.7, we may assume that $W_{1j} \cong W_{2j}$ for $j = 2, \dots, t$, and either $\mathrm{Ext}^1_{L_1}(W_{11}, W_{21}) \ne 0$, or $W_{11} \cong W_{21}$ and $\mathrm{Ext}^1_{L_j}(W_{1j}, W_{2j}) \ne 0$ for some j. Interchanging L_1 and L_j in the latter case, we can always assume that $\mathrm{Ext}^1_{L_1}(W_{11}, W_{21}) \ne 0$. By [Guralnick 1999, Theorem A], we then have

$$\dim W_{11} + \dim W_{21} \ge p - 1 > 2. \tag{9-1}$$

Now if W_{1j} is nontrivial for some $j \ge 2$, say $W_{12} \not\cong k$, then

$$\dim V \ge \dim W_1 + \dim W_2 \ge 2(\dim W_{11} + \dim W_{21}) = 2p - 2.$$

It follows that $V_i = W_i = W_{i1} \otimes W_{i2} \otimes k \otimes \cdots \otimes k$, $\dim W_{i1} = (p-1)/2$, and $\dim W_{i2} = 2$. Furthermore, $t = 2$ as V is faithful, and we arrive at (a).

We may now assume that $W_{1j} \cong W_{2j} \cong k$ for all $j > 1$. Suppose that G normalizes L_1. Since every G^+-composition factor of V_1 is G-conjugate to W_1, it follows that L_2 acts trivially on all composition factors of V_1. The same is true for V_2. As L_2 is quasisimple, we see that L_2 acts trivially on V, contrary to the faithfulness of V. Thus there must be some $g \in G$ conjugating L_1 to L_j for some $j > 1$, say $L_1^g = L_2$. By (9-1) we may assume that $W_{11} \not\cong k$. Then $g(W_1) \not\cong W_1$, as L_2 acts trivially on W_1 but not on $g(W_1)$. Thus $(V_1)_{G^+}$ has at least two distinct simple summands W_1 and $g(W_1)$. If furthermore $W_{21} \not\cong k$, then $(V_2)_{G^+}$ also has at least two distinct simple summands W_2 and $g(W_2)$, and so

$$\dim V \ge 2(\dim W_1 + \dim W_2) = 2(\dim W_{11} + \dim W_{21}) \ge 2p - 2.$$

In this case, we must have that $V_i = W_i \oplus g(W_i)$, $\dim W_i = (p-1)/2$, and $t = 2$ as V is faithful, and we arrive at (b).

Consider the case $W_{21} \cong k$. Now (9-1) implies that $\dim W_1 = \dim W_{11} \geq p-2$, whence $\dim V_1 \geq 2p-4$. On the other hand, $\dim V_2 \geq 2$. It follows that $2p-4 = 2$, again a contradiction.

(ii) By Lemma 9.3, $\boldsymbol{O}_{p'}(G^+) \leq \boldsymbol{Z}(G^+)$. Hence we are done by (i). □

Lemma 9.5. *Let H be a quasisimple finite group of Lie type in characteristic $p > 3$. Assume that $V_1, V_2 \in \mathrm{IBr}_p(H)$ satisfy $\dim V_1 + \dim V_2 < 2p$.*

(i) *If $H \ncong \mathrm{SL}_2(q),\ \mathrm{PSL}_2(q)$, then $\mathrm{Ext}^1_H(V_1, V_2) = 0$. In particular, there is no reducible indecomposable kG-module with $G^+ \cong H$ and $\dim V < 2p$.*

(ii) *Suppose $H \cong \mathrm{SL}_2(q)$ or $\mathrm{PSL}_2(q)$, $\mathrm{Ext}^1_H(V_1, V_2) \neq 0$, and $\dim V_1 = \dim V_2$. Then $q = p$ and $V_1 = L((p-3)/2)$ or $L((p-1)/2)$.*

Proof. (i) Note that $\boldsymbol{Z}(H)$ is a p'-group as $p > 3$. Hence, we can replace H by the fixed-point subgroup $\mathscr{G}^F$ for some Steinberg endomorphism $F : \mathscr{G} \to \mathscr{G}$ on some simple simply connected algebraic group $\mathscr{G}$ defined over a field of characteristic p (see Lemma 7.3). Hence, if $H \ncong \mathrm{Sp}_{2n}(5)$, the result follows by [McNinch 1999, Theorem 1.1]. In the exceptional case $H = \mathrm{Sp}_{2n}(5)$, we have $p = 5$ and so we are only considering modules of dimension at most 9. If $n \geq 3$, then $\dim V_1 + \dim V_2 > 10$ unless at least one of the V_i is trivial and the other is either trivial or the natural module of dimension $2n$, and in both cases $\mathrm{Ext}^1_H(V_1, V_2) = 0$. If $n = 2$, one just computes that all the relevant $\mathrm{Ext}^1_H(V_1, V_2)$ are trivial (done by Lux).

Suppose now that V is a reducible indecomposable kG-module with $G^+ \cong H$ and $\dim V < 2p$. By Lemma 7.8(ii), there are composition factors V_1, V_2 of V such that $\mathrm{Ext}^1_G(V_1, V_2) \neq 0$. It then follows that $\mathrm{Ext}^1_H(W_1, W_2) \neq 0$ for some simple H-summands W_i of V_i for $i = 1, 2$ and $\dim W_1 + \dim W_2 < 2p$, a contradiction.

(ii) Again we can replace H by $\mathrm{SL}_2(q)$. The statement then follows from Lemma 8.1 when $q > p$, and from [Andersen et al. 1983] if $q = p$. □

There are a considerable number of examples of nonsplit extensions $(V_1|V_2)$ with G^+ nonquasisimple and $\dim V_1 + \dim V_2 = 2p-2$. For example, suppose that $G = \mathrm{SL}_2(p) \times \mathrm{SL}_2(p)$ and $V_1 = L(1) \otimes L(a)$ and $V_2 = L(1) \otimes L(p-a-3)$. Then by [Andersen et al. 1983] and Lemma 7.7, $\mathrm{Ext}^1_G(V_1, V_2) \neq 0$. For our adequacy results, we do need to consider the case where $\dim V_1 = \dim V_2 = p-1$ in more detail:

Lemma 9.6. *Let V be a faithful indecomposable kG-module with two composition factors V_1, V_2, both of dimension $p-1$. Assume that $p > 3$ and $\boldsymbol{O}_p(G) = 1$. Then one of the following holds:*

(i) *$\boldsymbol{O}_{p'}(G^+) \nleq \boldsymbol{Z}(G^+)$ and Lemma 9.3 applies.*

(ii) *G^+ is quasisimple.*

(iii) $G^+ = \mathrm{SL}_2(p) \times \mathrm{SL}_2(p^a)$ (*modulo some central subgroup*) *and one of the following holds*:

(a) $V_1 \cong V_2 \cong L((p-3)/2) \otimes L(1)^{(p^b)}$ *as* G^+*-modules* (*for some* $0 \le b < a$).

(b) $a = 1$ *and* $V_1 \cong V_2 \cong X \oplus Y$, *where* G^+ *acts as a quasisimple group on* X, Y *and* $\dim X = \dim Y = (p-1)/2$ (*so* $X, Y \cong L((p-3)/2)$ *for the copy of* $\mathrm{SL}_2(p)$ *acting nontrivially on* X *or* Y).

Proof. Assume that neither (i) nor (ii) holds. Then by Lemma 9.4(i), $E(G^+) = G^+ = L_1 * L_2$ is a central product of two quasisimple groups, and either (a) or (b) of Lemma 9.4(i) occurs. In either case, we see that L_1 admits an indecomposable module W of length 2 with composition factors A_1 and A_2, both of dimension $(p-1)/2$. By [Blau and Zhang 1993, Theorem A] applied to W, L_1 is of Lie type in characteristic p. Also, $\boldsymbol{Z}(L_1) \le \boldsymbol{Z}(G^+) \le \boldsymbol{O}_{p'}(G)$ is a p'-group. Hence $L_1 \cong \mathrm{SL}_2(p)$ (modulo a central subgroup) by Lemma 9.5 and $A_1 \cong A_2 \cong L((p-3)/2)$. In particular, $L_2 \cong \mathrm{SL}_2(p)$ in case (b), and (iii)(b) holds. In the case of (a), $B \in \mathrm{IBr}_p(L_2)$ has dimension 2. Since $p > 3$, by Theorem 2.1 we conclude that L_2 is of Lie type in characteristic p, and in fact that $L_2 \cong \mathrm{SL}_2(p^a)$ (modulo a central subgroup) and $B \cong L(1)^{(p^b)}$ for some $a \ge 1$ and $0 \le b < a$. Thus (iii)(a) holds. □

Proposition 9.7. *Let* $p > 3$ *and let* G *be a finite group with a faithful, reducible, indecomposable* kG*-module* V *of dimension* $\le 2p-3$. *Suppose in addition that* $\boldsymbol{O}_p(G) = 1$. *Then* $G^+ = E(G^+)$, G *has no composition factor isomorphic to* C_p, *and one of the following holds*:

(i) G^+ *is quasisimple.*

(ii) G^+ *is a central product of two quasisimple groups and* $\dim V = 2p-3$. *Furthermore,* V *has one composition factor of dimension* 1, *and either one of dimension* $2p-4$ *or two of dimension* $p-2$. *In either case,* $V \not\cong V^*$.

Proof. (a) Note that $\boldsymbol{O}_p(G^+) \le \boldsymbol{O}_p(G) = 1$. Next we show that $J := \boldsymbol{O}_{p'}(G^+) \le \boldsymbol{Z}(G^+)$. As in the proof of Lemma 9.3, it suffices to show that J acts by scalars on every G^+-composition factor of V. So assume that there is a G^+-composition factor X of V on which J does not act by scalars. Again as in the proof of Lemma 9.3, we see by Theorem 2.1 that $\dim X \ge p-1$. Since $\dim V \le 2p-3$, it follows that X is a G^+-composition factor of multiplicity 1, and, moreover, J acts by scalars on any other G^+-composition factor Y of V. Also, X extends to a G-composition factor (of multiplicity 1) of V. Now, by Lemma 7.8(i), there is an indecomposable subquotient of length 2 of V with G-composition factors X and $T \not\cong X$. In particular, by symmetry we may assume that $0 \ne \mathrm{Ext}^1_G(X, T) \hookrightarrow \mathrm{Ext}^1_{G^+}(X, T)$, and so $\mathrm{Ext}^1_{G^+}(X, Y) \ne 0$ for some simple G^+-summand Y of T. But this is impossible by Lemma 7.11(ii) (as J acts by scalars on Y but not on X).

Applying Lemma 9.1 to G^+, we see that

$$G^+ = (G^+)^+ = E(G^+) = L_1 * \cdots * L_t,$$

a central product of t quasisimple subgroups. Note that $t \geq 1$ as otherwise G is a p'-group and so V does not exist. Furthermore, G has no composition factors isomorphic to C_p.

(b) Assume now that $t \geq 2$. Suppose in addition that , for every composition factor V_i of V, at most one of the components L_j of G^+ acts nontrivially on V_i. For $1 \leq j \leq t$, let $\mathscr{X}_j$ denote the set of isomorphism classes of composition factors V_i of V on which L_j acts nontrivially. Also let $\mathscr{X}_0$ denote the set of isomorphism classes of composition factors V_i of V on which G^+ acts trivially. By the faithfulness of V, $\mathscr{X}_j \neq \varnothing$ for $j > 0$. Consider for instance $X \in \mathscr{X}_1$. By Lemma 7.8(i), there is some $X' \in \mathscr{X}_j$ (for some j) and some indecomposable subquotient W of length 2 of V with composition factors X, X'. Note that the p-radical of the group induced by the action of G on W is trivial, as C_p is not a composition factor of G. Applying Lemma 9.4(ii) to W, we see that $j = 0$ or 1. Moreover, if for *all* $X \in \mathscr{X}_1$ there is no such W with $X' \in \mathscr{X}_0$, then Lemma 7.10 applied to $\big(\mathscr{X} := \mathscr{X}_1, \mathscr{Y} := \bigcup_{i \neq 1} \mathscr{X}_i\big)$ implies that V is decomposable, a contradiction. Thus for some $X \in \mathscr{X}_1$, such a W exists with $X' \in \mathscr{X}_0$. Note that in this case $\dim X \geq p-2$. Indeed, G^+ acts trivially on X', and by symmetry we may assume that

$$0 < \dim \operatorname{Ext}^1_G(X', X) \leq \dim \operatorname{Ext}^1_{G^+}(X', X).$$

Therefore, for some simple summand X_1 of the G^+-module X we have that $0 \neq \operatorname{Ext}^1_{G^+}(k, X_1) \cong H^1(G^+, X_1)$. Note that C_p is not a composition factor of G^+, so by Lemma 7.3 we may assume here that G^+ acts faithfully on X_1. Applying Lemma 9.2 to G^+, we get $\dim X \geq \dim X_1 \geq p-2$.

Similarly, for some $Y \in \mathscr{X}_2$, we get an indecomposable subquotient T of length 2 of V with composition factors Y and $Y' \in \mathscr{X}_0$, and moreover $\dim Y \geq p-2$. Since $\dim V \leq 2p-3$ and $\mathscr{X}_0 \ni X', Y'$, we conclude that $\dim V = 2p-3$, $\dim X = \dim Y = p-2$, $t = 2$, and $X' \cong Y'$ has dimension 1. Suppose in addition that $V \cong V^*$. Observe that $X^* \ncong Y, X'$, so $X \cong X^*$. Similarly, Y and X' are self-dual. Thus all three composition factors of V have multiplicity 1 each and are self-dual. At least one of them occurs in soc V, and then also in head V by duality. It follows by Lemma 7.9 that V is decomposable, a contradiction. Thus we arrive at (ii).

(c) Finally, we consider the case where at least two of the L_i act nontrivially on some composition factor V_i of V. By Lemma 7.8(i), there is some indecomposable subquotient W of length 2 of V with composition factors V_i and V_j. By Lemma 9.4(ii) applied to W, $\dim V_j = 1$. In turn this implies by Lemma 9.2 that $\dim V_i \geq 2p-4$. Since $\dim V \leq 2p-3$, we must have that $\dim V_i = 2p-4$, $V = W$, $t = 2$ and

$\dim V = 2p-3$. Applying Lemma 7.9 and using the indecomposability of V as above, we see that $V \not\cong V^*$, and again arrive at (ii). □

10. Extensions and self-extensions, II

Let q be any odd prime power. It is well known (see, e.g., [Tiep and Zalesskii 1997] and [Guralnick et al. 2002]) that the finite symplectic group $\mathrm{Sp}_{2n}(q)$ has two complex irreducible *Weil* characters ξ_1, ξ_2 of degree $(q^n+1)/2$, and two such characters η_1, η_2 of degree $(q^n-1)/2$, whose reductions modulo any *odd* prime $p \nmid q$ are absolutely irreducible and distinct and are called (*p-modular*) *Weil characters* of $\mathrm{Sp}_{2n}(q)$.

Lemma 10.1. *Let q be an odd prime power and p an odd prime divisor of q^n+1 which does not divide $\prod_{i=1}^{2n-1}(q^i-1)$. Let $S := \mathrm{Sp}_{2n}(q)$ and let W_1 and W_2 denote the irreducible kS-modules affording the two irreducible p-modular Weil characters of S of degree $(q^n-1)/2$. Then for $1 \le i, j \le 2$ we have that* $\mathrm{Ext}^1_S(W_i, W_j) = 0$, *unless $i \neq j$ and $n = 1$, in which case* $\dim(\mathrm{Ext}^1_S(W_i, W_j)) = 1$.

Proof. The conditions on (n, q) imply that $(n, q) \neq (1, 3)$. In this case, [Tiep and Zalesskii 1996, Theorem 1.1] implies that each W_i has a unique complex lift (a complex module affording some η_i). Also, the Sylow p-subgroups of S are cyclic of order $(q^n+1)_p$. Hence $\mathrm{Ext}^1_S(W_i, W_i) = 0$ by Lemma 7.1.

Note that an involutory diagonal automorphism σ of S fuses η_1 with η_2 and W_1 with W_2. Consider the semidirect product $H := S \rtimes \langle\sigma\rangle$ and the irreducible kH-module $V := \mathrm{Ind}_S^H(W_1)$ of dimension q^n-1. Certainly, $\mathrm{Ind}_S^H(\eta_1)$ is a complex lift of V.

Assume that $n > 1$. Now if $(n, q) \neq (2, 3)$, then by [Tiep and Zalesskii 1996, Theorem 5.2], S has exactly five irreducible complex characters of degree $\le (q^n-1)$: 1_S, η_1, η_2, ξ_1, and ξ_2. When $(n, q) = (2, 3)$, there is one extra complex character of degree 6 [Conway et al. 1985]. It follows that if χ is any complex lift of V, then $\chi_S = \eta_1 + \eta_2$. Since σ fuses η_1 and η_2, we see that $\chi = \mathrm{Ind}_S^H(\eta_1)$. Thus V has a unique complex lift, and so by Lemma 7.1 and Frobenius reciprocity we have

$$\begin{aligned} 0 = \mathrm{Ext}^1_H(V, V) = \mathrm{Ext}^1_H(\mathrm{Ind}_S^H(W_1), V) &\cong \mathrm{Ext}^1_S(W_1, V_S) \\ &\cong \mathrm{Ext}^1_S(W_1, W_1) \oplus \mathrm{Ext}^1_S(W_1, W_2). \end{aligned}$$

In particular, $\mathrm{Ext}^1_S(W_1, W_2) = 0$.

Next suppose that $n = 1$. Inspecting the character table of $\mathrm{SL}_2(q)$ as given in [Digne and Michel 1991, Table 2], we see that S has a σ-invariant complex irreducible character χ of degree $q-1$ such that the restriction of χ to p'-elements of S is the Brauer character of V_S. Since H/S is cyclic and generated by σ, it follows that χ extends to a complex irreducible character $\tilde{\chi}$ of H. Now $\tilde{\chi} \neq \mathrm{Ind}_S^H(\eta_1)$ (since the latter is reducible over S), but both of them are complex lifts of V (by Clifford's theorem). Applying Lemma 7.1 and Frobenius reciprocity as above, we see that $\dim \mathrm{Ext}^1_H(V, V) = \dim \mathrm{Ext}^1_S(W_1, W_2) = 1$. □

Lemma 10.2. *Let H be a quasisimple group with $\mathbf{Z}(H)$ a p'-group. Let W and W' be absolutely irreducible kH-modules in characteristic p of dimension d, where (H, p, d) is one of the following triples:*

$$(2\mathsf{A}_7, 5, 4),\ (3J_3, 19, 18),\ (2Ru, 29, 28),\ (6_1 \cdot \mathrm{PSL}_3(4), 7, 6),$$
$$(6_1 \cdot \mathrm{PSU}_4(3), 7, 6),\ (2J_2, 7, 6),\ (3\mathsf{A}_7, 7, 6),\ (6\mathsf{A}_7, 7, 6),\ (M_{11}, 11, 10),$$
$$(2M_{12}, 11, 10),\ (2M_{22}, 11, 10),\ (6Suz, 13, 12),\ (2\mathrm{G}_2(4), 13, 12),\ (3\mathsf{A}_6, 5, 3),$$
$$(3\mathsf{A}_7, 5, 3),\ (M_{11}, 11, 9),\ (M_{23}, 23, 21),\ (2\mathsf{A}_7, 7, 4),\ (J_1, 11, 7).$$

If $\mathbf{Z}(H)$ acts the same way on W and W', assume in addition that there is an automorphism of H which sends W to W'. Then $\mathrm{Ext}^1_H(W, W') = 0$, with the following two exceptions: $(H, p, d) = (3\mathsf{A}_6, 5, 3)$ and $(2\mathsf{A}_7, 7, 4)$, where $\dim \mathrm{Ext}^1_H(W, W) = 1$.

Proof. Note that the Sylow p-subgroups of H have order p. Hence, in the case $W \cong W'$ we can apply Lemma 7.1; in particular, we arrive at the two exceptions listed above. This argument settles the cases of $(M_{11}, 11, 9)$, $(M_{23}, 23, 21)$, $(J_1, 11, 7)$, and $(2\mathrm{G}_2(4), 13, 12)$.

If $W \not\cong W'$ and $\mathbf{Z}(H)$ acts differently on W and W', then we also get that $\mathrm{Ext}^1_H(W, W') = 0$ since $\mathbf{Z}(H)$ is a central p'-group. So it remains to consider the case where $W \not\cong W'$ and $\mathbf{Z}(H)$ acts the same way on both of them. Suppose in addition that there is an involutory automorphism σ of H that swaps W and W' and that the module $\mathrm{Ind}^J_H(W)$ of $J := H \rtimes \langle\sigma\rangle$ has at most one complex lift. Then we can apply Lemma 7.1 to J as in the proof of Lemma 10.1 to conclude that $\mathrm{Ext}^1(W, W') = 0$. These arguments are used to handle the cases of $(2\mathsf{A}_7, 5, 4)$, $(3\mathsf{A}_7, 5, 3)$, $(3\mathsf{A}_7, 7, 6)$, $(2J_2, 7, 6)$, $(6Suz, 13, 12)$, $(6_1 \cdot \mathrm{PSL}_3(4), 7, 6)$, and $(6_1 \cdot \mathrm{PSU}_4(3), 7, 6)$.

In the six remaining cases of $(6\mathsf{A}_7, 7, 6)$, $(3J_3, 19, 18)$, $(2Ru, 29, 28)$, $(M_{11}, 11, 10)$, $(2M_{12}, 11, 10)$, and $(2M_{22}, 11, 10)$, we note (using [Jansen et al. 1995] or [GAP 2004]) that the nonisomorphic H-modules W and W' with the same action of $\mathbf{Z}(H)$ are *not* $\mathrm{Aut}(H)$-conjugate. □

Corollary 10.3. *Suppose that $q > 3$ is an odd prime power such that $p = (q+1)/2$ prime. Then there is a finite absolutely irreducible linear group $G < \mathrm{GL}(V) = \mathrm{GL}_{q-1}(k)$ of degree $q - 1$ over k such that $G^+ \cong \mathrm{SL}_2(q)$, all irreducible G^+-submodules in V are Weil modules of dimension $(q-1)/2$, and $\dim \mathrm{Ext}^1_G(V, V) = 1$. In particular, (G, V) is not adequate.*

Proof. Our conditions on p, q imply that $q \equiv 1 \pmod 4$. Now we can just appeal to the proof of Lemma 10.1, taking $H = \mathrm{GU}_2(q)/C$, where C is the unique subgroup of order $(q+1)/2$ in $\mathbf{Z}(\mathrm{GU}_2(q))$. □

Proposition 10.4. *Suppose* (G, V) *is as in the extraspecial case* (ii) *of Theorem 2.4. Then* $\mathrm{Ext}^1_G(V, V) = 0$.

Proof. Write $V|_{G^+} = e\sum_{i=1}^t W_i$ as usual and let K_i be the kernel of the action of G^+ on W_i. By Lemma 7.2, it suffices to show that $\mathrm{Ext}^1_{G^+}(W_i, W_j) = 0$ for all i, j. Recall that $R := \boldsymbol{O}_{p'}(G^+)$ acts irreducibly on W_i. By Theorem 2.4, K_i has no composition factor $\cong C_p$, whence $\mathrm{Ext}^1_{G^+}(W_i, W_i) = \mathrm{Ext}^1_{G^+/K_i}(W_i, W_i)$ by Lemma 7.3(ii). Next, G^+/K_i has cyclic Sylow p-subgroups (of order p) by Theorem 2.1(e), and we have shown in the proof of Proposition 5.6 that the G^+/K_i-module W_i has a unique complex lift. Hence $\mathrm{Ext}^1_{G^+/K_i}(W_i, W_i) = 0$ by Lemma 7.1.

Suppose now that $i \neq j$ and let M be any extension of the G^+-module W_i by the G^+-module W_j. Recall that the R-modules W_i and W_j are irreducible and nonisomorphic, as shown in the proof of Proposition 5.6. But R is a p'-group, so by Maschke's theorem $M = M_1 \oplus M_2$ with $M_i \cong W_i$ as R-modules. Now for any $g \in G^+$, $g(M_i) \cong (W_i)^g \cong W_i$ as R-modules, and so $g(M_i) = M_i$. Thus $M = M_1 \oplus M_2$ as a G^+-module. We have shown that $\mathrm{Ext}^1_{G^+}(W_i, W_j) = 0$. □

Proposition 10.5. *Suppose that* (G, V) *is as in case* (i) *of Theorem 2.4. Then* $\mathrm{Ext}^1_G(V, V) = 0$, *unless one of the following possibilities occurs for the group* $H < \mathrm{GL}(W)$ *induced by the action of* G^+ *on any irreducible* G^+*-submodule* W *of* V:

(i) $p = (q + 1)/2$, $\dim W = p - 1$, *and* $H \cong \mathrm{SL}_2(q)$.

(ii) $p = 2^f + 1$ *is a Fermat prime*, $\dim W = p - 2$, *and* $H \cong \mathrm{SL}_2(2^f)$.

(iii) $(H, p, d) = (3\mathsf{A}_6, 5, 3)$ *and* $(2\mathsf{A}_7, 7, 4)$.

Proof. Write $V|_{G^+} = e\sum_{i=1}^t W_i$ as usual and let K_i be the kernel of the action of G^+ on W_i. By Lemma 7.2, it suffices to show that $\mathrm{Ext}^1_{G^+}(W_i, W_j) = 0$ for all i, j. Note that neither G^+ nor K_i can have C_p as a composition factor, according to Theorem 2.4. Furthermore, if $K_i \neq K_j$ then we are done by Corollary 7.6. So we may assume that $K_i = K_j$ and then by Lemma 7.3 replace G^+ by $H = G^+/K_i = G^+/K_j$. Now we will go over the possibilities for (H, W_i) listed in Theorem 2.1(b)–(d).

Suppose we are in the case (b1) of Theorem 2.1. Assume first that $(p, H) = ((q^n + 1)/2, \mathrm{Sp}_{2n}(q))$. It is well known (see [Guralnick et al. 2002, Theorem 2.1]) that H has exactly two irreducible modules of dimension $(q^n - 1)/2$, namely the two Weil modules of that dimension. Hence we can apply Lemma 10.1 and arrive at the exception (i).

Next, assume that $(p, H) = ((q^n + 1)/(q + 1), \mathrm{PSU}_n(q))$; in particular, $n \geq 3$ is odd. Applying [Guralnick et al. 2002, Theorem 2.7 and Proposition 11.3], we see that there is a unique irreducible kH-module of dimension $p - 1 = (q^n - q)/(q + 1)$, and, furthermore, that this module has a unique complex lift. Hence we are done by Lemma 7.1.

Suppose now that we are in the case (c) of Theorem 2.1. If $H = \mathsf{A}_p$, then using [Guralnick and Tiep 2005, Lemma 6.1] for $p \geq 17$ and [Conway et al. 1985] for $p \leq 13$, we see that H has a unique irreducible kH-module of dimension $p-2$, and, furthermore, that this module has no complex lift unless $p = 5$, whence we are done by Lemma 7.1. Note that the exception $p = 5$ is recorded in (ii) (with $f = 2$).

Next, assume that $(p, H) = ((q^n - 1)/(q - 1), \mathrm{PSL}_n(q))$. If $n = 2$, then $p = q + 1 = 2^f + 1$ is a Fermat prime, in which case $H = \mathrm{SL}_2(2^f)$ has a unique irreducible kH-module W of dimension $p-2$, with 2^{f-1} complex lifts, whence $\dim \mathrm{Ext}^1_H(W, W) = 1$ by Lemma 7.1. This exception is recorded in (ii). If $n \geq 3$, then by [Guralnick and Tiep 1999, Theorem 1.1], H has a unique irreducible kH-module W of dimension $p-2$ with no complex lifts, whence $\dim \mathrm{Ext}^1_H(W, W) = 0$ by Lemma 7.1.

It remains to consider the 19 cases listed in Lemma 10.2. Furthermore, by Corollary 7.6, we need only consider the case where G^+ acts on W_i and W_j with the same kernel. Since G^+ has no composition factor isomorphic to C_p, by Lemma 7.3(ii) we may view W_i and W_j as modules over the same quasisimple group H, with the same kernel. The irreducibility of G on V further implies that $W_j \cong W_i^g$ for some $g \in G$, whence the H-modules W_i and W_j are $\mathrm{Aut}(H)$-conjugate. Now we are done by applying Lemma 10.2. □

Corollary 10.6. *Suppose that $p = 2^f + 1$ is a Fermat prime. Then there is a finite absolutely irreducible linear group $G < \mathrm{GL}(V) = \mathrm{GL}_{p-2}(k)$ of degree $p-2$ over k such that $G = G^+ \cong \mathrm{SL}_2(2^f)$ and $\dim \mathrm{Ext}^1_G(V, V) = 1$. In particular, (G, V) is not adequate.*

Proof. See the proof of Proposition 10.5 and the exception (ii) listed therein. □

Proof of Theorem 1.3. (a) Assume first that G is not p-solvable. Then G^+ has no composition factor isomorphic to C_p, and $H^1(G, k) = 0$ by Theorem 2.4. By Lemma 7.2, we need to verify that $\mathrm{Ext}^1_{G^+}(W_i, W_j) = 0$ for any two simple G^+-submodules W_i and W_j of V, of dimension $1 < d < p$. Suppose for instance that $\mathrm{Ext}^1_{G^+}(W_1, W_2) \neq 0$.

Suppose in addition that $p > 3$. Then the perfect group G^+ admits a reducible indecomposable module U with two composition factors W_1 and W_2, of dimension $2d$, say with kernel K. Since G^+ has no composition factor isomorphic to C_p, $\mathbf{O}_p(X) = 1$ for the group $X := G^+/K$ induced by the action of G^+ on U. Suppose that X is not quasisimple. By Proposition 9.7, we have $d = p - 1$. Then by Lemma 9.6, either we arrive at the exception (b)(ii) listed in Theorem 1.3, or else Lemma 9.3 applies. In the latter case, we see that $H^1(X, k) \neq 0$, whence X and G^+ admit C_p as a composition factor, a contradiction. Thus X is quasisimple and $\mathbf{Z}(X)$ is a p'-group. If X is of Lie type in characteristic $p > 3$, then we must have $d = (p \pm 1)/2$ and arrive (using Lemma 9.5) at the exception (b)(i). Otherwise we are in the case (i) of Theorem 2.4, and so by Proposition 10.5 we arrive at the exceptions (b)(iii)–(v).

(b) Now we consider the case where $p = 3$ and G is not p-solvable. Then the perfect group G^+ acts nontrivially on W_1 and W_2, which are of dimension 2. Applying Theorem 2.4, we see that $G^+ = L_1 * \cdots * L_n$ is a central product of quasisimple groups; moreover, for all j we have that $L_j = \mathrm{SL}_2(q)$ with $q = 3^a > 3$ or $q = 5$. Also, for each i, there is a unique k_i such that L_j acts nontrivially on W_i precisely when $j = k_i$. Since $\mathrm{Ext}^1_X(k, k) = 0$ for any perfect group X, by Lemma 7.7 we may assume that $k_1 = k_2 = 1$ and $\mathrm{Ext}^1_{L_1}(W_1, W_2) \neq 0$. If $q = 5$, then the case (b)(iii) holds. Otherwise we arrive at (b)(vi) — indeed, $\mathrm{Ext}^1_{L_1}(L(3^{a-2}), L(3^{a-1})) \neq 0$ by [Andersen et al. 1983, Corollary 4.5].

(c) We may now assume that G^+ is p-solvable (and so is G). In particular, the subgroup $H < \mathrm{GL}(W_i)$ induced by the action of G^+ on W_i is p-solvable, whence p is a Fermat prime, and $H = \boldsymbol{O}_{p'}(H)P$ with $P \cong C_p$. Since G^+ projects onto H, G^+ also has C_p as a composition factor, and so $H^1(G^+, k) \neq 0$; in particular, $\mathrm{Ext}^1_{G^+}(V, V) \neq 0$. We arrive at the exception (a) of Theorem 1.3. □

Proof of Corollary 1.4. Suppose that (G, V) is *not* adequate, and let $\overline{V} := V \otimes_k \bar{k}$. By the assumptions, $\dim W < p$. Since $\dim \overline{V}/\dim W$ divides $|G/G^+|$ by [Navarro 1998, Theorem 8.30], $p \nmid \dim_{\bar{k}} \overline{V} = \dim_k V$. Next, (G, V) is weakly adequate by Theorem 1.2. It follows that $\mathrm{Ext}^1_G(V, V) \neq 0$ and so $\mathrm{Ext}^1_G(\overline{V}, \overline{V}) \neq 0$. Now we can apply Theorem 1.3. □

References

[Alperin 1986] J. L. Alperin, *Local representation theory*, Cambridge Studies in Advanced Mathematics **11**, Cambridge University Press, 1986. MR 87i:20002 Zbl 0593.20003

[Andersen et al. 1983] H. H. Andersen, J. Jørgensen, and P. Landrock, "The projective indecomposable modules of SL(2, p^n)", *Proc. London Math. Soc.* (3) **46**:1 (1983), 38–52. MR 84f:20044 Zbl 0503.20013

[Barnet-Lamb et al. 2013] T. Barnet-Lamb, T. Gee, and D. Geraghty, "Serre weights for rank two unitary groups", *Math. Ann.* **356**:4 (2013), 1551–1598. MR 3072811 Zbl 06194417

[Barnet-Lamb et al. 2014] T. Barnet-Lamb, T. Gee, D. Geraghty, and R. Taylor, "Potential automorphy and change of weight", *Ann. of Math.* (2) **179**:2 (2014), 501–609. MR 3152941 Zbl 06284344

[Benson 1998] D. J. Benson, *Representations and cohomology, I: Basic representation theory of finite groups and associative algebras*, 2nd ed., Cambridge Studies in Advanced Mathematics **30**, Cambridge University Press, 1998. MR 99f:20001a Zbl 0908.20001

[Blau and Zhang 1993] H. I. Blau and J. P. Zhang, "Linear groups of small degree over fields of finite characteristic", *J. Algebra* **159**:2 (1993), 358–386. MR 94i:20082 Zbl 0857.20029

[Breuer et al.] T. Breuer et al., "Decomposition matrices", database, http://www.math.rwth-aachen.de/homes/MOC/decomposition/.

[Breuil et al. 2001] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, "On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises", *J. Amer. Math. Soc.* **14**:4 (2001), 843–939. MR 2002d:11058 Zbl 0982.11033

[Burkhardt 1976] R. Burkhardt, "Die Zerlegungsmatrizen der Gruppen PSL(2, p^f)", *J. Algebra* **40**:1 (1976), 75–96. MR 58 #864 Zbl 0334.20008

[Calegari 2012] F. Calegari, "Even Galois representations and the Fontaine–Mazur conjecture, II", *J. Amer. Math. Soc.* **25**:2 (2012), 533–554. MR 2869026 Zbl 1282.11051

[Clozel et al. 2008] L. Clozel, M. Harris, and R. Taylor, "Automorphy for some l-adic lifts of automorphic mod l Galois representations", *Publ. Math. Inst. Hautes Études Sci.* **108** (2008), 1–181. MR 2010j:11082 Zbl 1169.11020

[Conway et al. 1985] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of finite groups*, Oxford University Press, Eynsham, 1985. MR 88g:20025 Zbl 0568.20001

[Dieulefait 2014] L. Dieulefait, "Automorphy of Symm^5(GL(2)) and base change", preprint, 2014. To appear in *J. Math. Pures Appl.* arXiv 1208.3946

[Dieulefait and Gee 2012] L. Dieulefait and T. Gee, "Automorphy lifting for small l", Appendix B to [Dieulefait 2014], 2012. arXiv 1209.5105

[Digne and Michel 1991] F. Digne and 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

[Doty and Henke 2005] S. Doty and A. Henke, "Decomposition of tensor products of modular irreducibles for SL$_2$", *Q. J. Math.* **56**:2 (2005), 189–207. MR 2005m:20107 Zbl 1108.20043

[GAP 2004] *GAP – Groups, Algorithms, and Programming*, Version 4.4, The GAP Group, 2004, http://www.gap-system.org.

[Geck 1990] M. Geck, "Irreducible Brauer characters of the 3-dimensional special unitary groups in nondefining characteristic", *Comm. Algebra* **18**:2 (1990), 563–584. MR 91b:20016 Zbl 0696.20011

[Guralnick 1999] R. M. Guralnick, "Small representations are completely reducible", *J. Algebra* **220**:2 (1999), 531–541. MR 2000m:20018 Zbl 0941.20001

[Guralnick 2012a] R. Guralnick, "Adequacy of representations of finite groups of Lie type", Appendix A to [Dieulefait 2014], 2012. arXiv 1208.4128

[Guralnick 2012b] R. Guralnick, "Adequate subgroups, II", *Bull. Math. Sci.* **2**:1 (2012), 193–203. MR 2942677 Zbl 06073629

[Guralnick and Tiep 1999] R. M. Guralnick and P. H. Tiep, "Low-dimensional representations of special linear groups in cross characteristics", *Proc. London Math. Soc.* (3) **78**:1 (1999), 116–138. MR 2000a:20016 Zbl 0974.20014

[Guralnick and Tiep 2005] R. M. Guralnick and P. H. Tiep, "The non-coprime $k(GV)$ problem", *J. Algebra* **293**:1 (2005), 185–242. MR 2006g:20018 Zbl 1083.20006

[Guralnick et al. 2002] R. M. Guralnick, K. Magaard, J. Saxl, and P. H. Tiep, "Cross characteristic representations of symplectic and unitary groups", *J. Algebra* **257**:2 (2002), 291–347. MR 2004b:20022 Zbl 1025.20002

[Guralnick et al. 2007] R. Guralnick, W. M. Kantor, M. Kassabov, and A. Lubotzky, "Presentations of finite simple groups: profinite and cohomological approaches", *Groups Geom. Dyn.* **1**:4 (2007), 469–523. MR 2008j:20089 Zbl 1135.20024

[Guralnick et al. 2012] R. Guralnick, F. Herzig, R. Taylor, and J. Thorne, "Adequate subgroups", Appendix to [Thorne 2012], 2012.

[Guralnick et al. 2014] R. Guralnick, F. Herzig, and P. H. Tiep, "Adequate subgroups and indecomposable modules", preprint, 2014. To appear in *J. Europ. Math. Soc.* arXiv 1405.0043

[Holt 1980] D. F. Holt, "Exact sequences in cohomology and an application", *J. Pure Appl. Algebra* **18**:2 (1980), 143–147. MR 82h:20063 Zbl 0439.18016

[James 1986] G. James, "The irreducible representations of the finite general linear groups", *Proc. London Math. Soc.* (3) **52**:2 (1986), 236–268. MR 87h:20028 Zbl 0587.20022

[Jansen et al. 1995] C. Jansen, K. Lux, R. Parker, and R. Wilson, *An atlas of Brauer characters*, London Mathematical Society Monographs. New Series **11**, Oxford University Press, New York, 1995. MR 96k:20016 Zbl 0831.20001

[Jantzen 1997] J. C. Jantzen, "Low-dimensional representations of reductive groups are semisimple", pp. 255–266 in *Algebraic groups and Lie groups*, edited by G. Lehrer et al., Austral. Math. Soc. Lect. Ser. **9**, Cambridge University Press, 1997. MR 99g:20079 Zbl 0877.20029

[Jantzen 2003] J. C. Jantzen, *Representations of algebraic groups*, 2nd ed., Mathematical Surveys and Monographs **107**, American Mathematical Society, Providence, RI, 2003. MR 2004h:20061 Zbl 1034.20041

[Janusz 1969] G. J. Janusz, "Indecomposable modules for finite groups", *Ann. of Math.* **89** (1969), 209–241. MR 39 #5622 Zbl 0197.02302

[Khare and Wintenberger 2009] C. Khare and J.-P. Wintenberger, "Serre's modularity conjecture, I", *Invent. Math.* **178**:3 (2009), 485–504. MR 2010k:11087 Zbl 05636295

[Kleidman and Liebeck 1990] P. Kleidman and M. Liebeck, *The subgroup structure of the finite classical groups*, London Mathematical Society Lecture Note Series **129**, Cambridge University Press, 1990. MR 91g:20001 Zbl 0697.20004

[Kleshchev and Tiep 2009] A. S. Kleshchev and P. H. Tiep, "Representations of finite special linear groups in non-defining characteristic", *Adv. Math.* **220**:2 (2009), 478–504. MR 2009j:20022 Zbl 1165.20009

[Kleshchev and Tiep 2010] A. S. Kleshchev and P. H. Tiep, "Representations of the general linear groups which are irreducible over subgroups", *Amer. J. Math.* **132** (2010), 425–473. MR 2011k:20091 Zbl 1211.20017

[McNinch 1999] G. J. McNinch, "Semisimple modules for finite groups of Lie type", *J. London Math. Soc.* **60**:3 (1999), 771–792. MR 2001k:20096 Zbl 0961.20014

[Navarro 1998] G. Navarro, *Characters and blocks of finite groups*, London Mathematical Society Lecture Note Series **250**, Cambridge University Press, 1998. MR 2000a:20018 Zbl 0903.20004

[Navarro and Tiep 2010] G. Navarro and P. H. Tiep, "Degrees of rational characters of finite groups", *Adv. Math.* **224**:3 (2010), 1121–1142. MR 2011h:20015 Zbl 1200.20006

[Serre 1994] J.-P. Serre, "Sur la semi-simplicité des produits tensoriels de représentations de groupes", *Invent. Math.* **116**:1-3 (1994), 513–530. MR 94m:20091 Zbl 0816.20014

[Thorne 2012] J. Thorne, "On the automorphy of l-adic Galois representations with small residual image", *J. Inst. Math. Jussieu* **11**:4 (2012), 855–920. MR 2979825 Zbl 1269.11054

[Thorne 2015] J. Thorne, "A 2-adic automorphy lifting theorem for unitary groups over CM fields", preprint, 2015, http://math.harvard.edu/~thorne/p_equals_2.pdf.

[Tiep and Zalesskii 1996] P. H. Tiep and A. E. Zalesskii, "Minimal characters of the finite classical groups", *Comm. Algebra* **24**:6 (1996), 2093–2167. MR 97f:20018 Zbl 0901.20031

[Tiep and Zalesskii 1997] P. H. Tiep and A. E. Zalesskii, "Some characterizations of the Weil representations of the symplectic and unitary groups", *J. Algebra* **192**:1 (1997), 130–165. MR 99d:20074 Zbl 0877.20030

[Wilson et al.] R. A. Wilson, P. Walsh, J. Tripp, I. Suleiman, R. A. Parker, S. P. Norton, S. Nickerson, S. Linton, J. Bray, and R. Abbott, "ATLAS of finite group representations", online database, http://brauer.maths.qmul.ac.uk/Atlas/v3.

Communicated by Barry Mazur
Received 2014-04-13 Accepted 2014-12-14

guralnic@usc.edu *Department of Mathematics, University of Southern California, 3620 South Vermont Ave, Los Angeles, CA 90089-2532, United States*

herzig@math.toronto.edu *Department of Mathematics, University of Toronto, 40 Saint George Street, Room 6290, Toronto, ON M5S 2E4, Canada*

tiep@math.arizona.edu *Department of Mathematics, University of Arizona, 617 North Santa Rita Avenue, Tucson, AZ 85721-0089, United States*

ALGEBRA AND NUMBER THEORY 9:1 (2015)
dx.doi.org/10.2140/ant.2015.9.149

Random matrices, the Cohen–Lenstra heuristics, and roots of unity

Derek Garton

The Cohen–Lenstra–Martinet heuristics predict the frequency with which a fixed finite abelian group appears as an ideal class group of an extension of number fields, for certain sets of extensions of a base field. Recently, Malle found numerical evidence suggesting that their proposed frequency is incorrect when there are unexpected roots of unity in the base field of these extensions. Moreover, Malle proposed a new frequency, which is a much better match for his data. We present a random matrix heuristic (coming from function fields) that leads to a function field version of Malle's conjecture (as well as generalizations of it).

1. Introduction

1.1. ***Cohen–Lenstra–Martinet and Malle.*** We start with Cohen and Lenstra's famous heuristic principle concerning the distribution of ideal class groups of quadratic number fields. We fix an odd prime ℓ, to be used throughout the paper.

Heuristic 1.1.1 [Cohen and Lenstra 1984]. A finite abelian ℓ-group should appear as the ℓ-Sylow subgroup of the ideal class group of an imaginary quadratic extension of $\mathbb{Q}$ with frequency inversely proportional to the order of its automorphism group.

With a bit more notation, we can reframe this heuristic. Let $\mathscr{G}$ be the poset of isomorphism classes of finite abelian ℓ-groups and for any number field K, let $\operatorname{cl}(K)$ denote the ideal class group of K. For any group G, let $G[\ell^\infty]$ denote its ℓ-Sylow subgroup. Now, since $\sum_{A\in\mathscr{G}} 1/|\operatorname{Aut} A| = \prod_{i=1}^{\infty}(1-\ell^{-i})^{-1}$ (a fact first proved by Hall [1938]), the map $\mathscr{G}\to\mathbb{R}$ given by $A\mapsto|\operatorname{Aut} A|^{-1}\prod_{i=1}^{\infty}(1-\ell^{-i})$ defines a discrete probability distribution on $\mathscr{G}$. Heuristic 1.1.1 is the claim that the statistics of this distribution match the statistics of ℓ-Sylow subgroups of imaginary quadratic extensions (when ordered by fundamental discriminant). In other words,

MSC2010: primary 11R29; secondary 11R58, 15B52.

Keywords: random matrices, function fields, roots of unity, ideal class groups, Cohen–Lenstra heuristics.

Heuristic 1.1.1 is equivalent to the following assertion: for any $A \in \mathcal{G}$,

$$\lim_{X\to\infty} \frac{\bigl|\{0 \le D \le X \mid -D \text{ a fundamental discriminant, } \operatorname{cl}(\mathbb{Q}(\sqrt{-D}))[\ell^\infty] \simeq A\}\bigr|}{\bigl|\{0 \le D \le X \mid -D \text{ a fundamental discriminant}\}\bigr|} = \frac{1}{|\operatorname{Aut} A|}\prod_{i=1}^{\infty}(1-\ell^{-i}).$$

(This assertion remains unproven; in fact, this limit is not even known to exist.) This heuristic explains many previously observed tendencies of class groups of imaginary quadratic fields; for example that their orders seem to be divisible by three with probability

$$1-\prod_{i=1}^{\infty}(1-3^{-i}) = \tfrac{1}{3}+\tfrac{1}{9}+\cdots \approx .44.$$

Cohen and Martinet [1990] extended their heuristics to include relative class groups of finite extensions of arbitrary number fields, placing different distributions on $\mathcal{G}$ depending on properties of the family of extensions they study. Once again, they proved that these distributions imply many numerical observations, thereby obtaining a new family of conjectures. (Recall that relative ideal class groups are defined as follows: if K/K_0 is an extension of number fields, the relative class group $\operatorname{cl}(K/K_0)$ is the kernel of the norm map $\mathrm{N}_{K/K_0} : \operatorname{cl}(K) \to \operatorname{cl}(K_0)$.)

However, Malle [2008] presented new computational data that called into question some of the Cohen–Lenstra–Martinet conjectures. For example, he studied the 3-parts of the relative class groups of quadratic extensions of $\mathbb{Q}(\sqrt{-3})$, which has third roots of unity. Cohen, Lenstra and Martinet predicted that the class numbers of such extensions should be coprime to 3 with probability

$$\prod_{i=2}^{\infty}(1-3^{-i}) \approx .840.$$

On the other hand, when Malle computed the class numbers of the first million of these extensions with discriminant at least 10^{20}, he discovered that the proportion of them with class number coprime to 3 was about .852. He conjectured that the proportion of all such class groups that have class number coprime to 3 should be exactly

$$\frac{4}{3}\prod_{i=1}^{\infty}(1+3^{-i})^{-1} \approx .852,$$

which is in much better agreement with his data. In a subsequent paper, Malle [2010] presented more computational evidence calling into question more of the Cohen–Lenstra–Martinet conjectures, once again when there are ℓth roots of unity in the base field. In that paper, he also presented a new family of distributions on $\mathcal{G}$ to describe relative class groups when the base field of the extension has ℓth roots of unity but not ℓ^2th roots of unity (see Conjecture 2.1 in [ibid.]). These distributions on $\mathcal{G}$ imply rank statistics that seem to be a much better fit for his new data. A special case of his conjecture is the following:

Conjecture 1.1.2 [Malle 2010]. Suppose that $A \in \mathcal{G}$ and that A has ℓ-rank r. Let K_0 be a number field with ℓth but not ℓ^2th roots of unity. Let $\mathcal{S}$ be the set of quadratic extensions K/K_0 with a fixed signature (with fixed relative unit rank u). Then

$$\lim_{X\to\infty} \frac{|\{K \in \mathcal{S} \mid |\mathrm{Disc}\, K| \le X, \mathrm{cl}(K/K_0)[\ell^\infty] \simeq A\}|}{|\{K \in \mathcal{S} \mid |\mathrm{Disc}\, K| \le X\}|}$$
$$= \frac{\prod_{i=u+1}^{u+r} (\ell^i - 1)}{\ell^{r(u+1)}|A|^u|\mathrm{Aut}\, A|} \cdot \prod_{i=u+1}^{\infty} (1+\ell^{-i})^{-1}.$$

In this paper, we study a random matrix model of ideal class groups of function fields when the base field has ℓth roots of unity (i.e., the function field analog of the situation Malle studies in Conjecture 1.1.2). We compute the distributions on $\mathcal{G}$ given by this matrix model in two cases (see Theorem 5.1.4): in the case when the base field has ℓth roots of unity but not ℓ^2th roots of unity, and in the case when the base field has ℓ^2th roots of unity but not ℓ^3th roots of unity. In the former case, our distribution matches the distribution proposed by Malle. Moreover, we compute all the moments of the distribution given by this matrix model in the general case when the base case has ℓ^ξth but not $\ell^{\xi+1}$th roots of unity for any $\xi \in \mathbb{Z}^{>0}$ (see Corollary 3.2.7).

The work in this paper is based on my Ph.D. dissertation [Garton 2012]. The matrix distributions were computed independently in the Ph.D. dissertation of M. Adam [2014b] as well as in [Adam 2014a]. They are also used in [Adam and Malle 2015].

1.2. ***The function field case.*** Complementing the work described in Section 1.1, investigators have been studying analogous phenomena in function fields defined over finite fields. Friedman and Washington [1989] addressed the case of quadratic extensions of the field $\mathbb{F}_{p^n}(t)$ for a prime $p \neq 2$ and $n \in \mathbb{Z}^{>0}$. More precisely, if $f(t) \in \mathbb{F}_{p^n}[t]$ is monic of degree $2g+1$ with distinct roots, let C_f be the hyperelliptic curve (defined over $\mathbb{F}_{p^n}$) of genus g given by $y^2 = f(t)$. Note that the curve C_f has exactly one point at infinity, just as imaginary quadratic extensions of $\mathbb{Q}$ have exactly one place at infinity. Thus, $\mathrm{Pic}^0_{\mathbb{F}_{p^n}}(C_f)$ is isomorphic to the ideal class group of the field extension

$$\mathbb{F}_{p^n}(t)\big[\sqrt{f(t)}\,\big]/\mathbb{F}_{p^n}(t).$$

To study these groups, Friedman and Washington introduced a new heuristic principle, one that comes from the geometry of hyperelliptic curves over finite fields. Specifically, for $f(t) \in \mathbb{F}_{p^n}[t]$ monic of degree $2g+1$ with distinct roots, let $T_\ell(C_f)$ be the ℓ-adic Tate module of C_f, which is a free $2g$-dimensional $\mathbb{Z}_\ell$-module. In addition, let Frob_{p^n} be the p^n-power Frobenius map acting on $T_\ell(C_f)$. Thinking of Frob_{p^n} as a matrix over $\mathbb{Z}_\ell$, it is well known that $\mathrm{coker}(\mathrm{Id} - \mathrm{Frob}_{p^n})$ is isomorphic to the ℓ-Sylow subgroup of $\mathrm{Pic}^0_{\mathbb{F}_{p^n}}(C_f)$ (see the appendix of [Friedman and Washington 1989] for a proof of this fact). The same authors conjectured that the statistics of ℓ-Sylow subgroups of ideal class groups of quadratic extensions of $\mathbb{F}_{p^n}(t)$ match the statistics of ℓ-adic matrices. Specifically, if we let

$$F(g, p^n, \ell, A) := \frac{\left|\{f \in \mathbb{F}_{p^n}[t] \mid f \text{ monic with distinct roots, } \deg f = 2g+1,\ \mathrm{Pic}^0_{\mathbb{F}_{p^n}}(C_f)[\ell^\infty] \simeq A\}\right|}{\left|\{f \in \mathbb{F}_{p^n}[t] \mid f \text{ monic with distinct roots, } \deg f = 2g+1\}\right|},$$

then they proposed the following:

Heuristic 1.2.1 [Friedman and Washington 1989]. If $A \in \mathcal{G}$, then

$$\lim_{g\to\infty} F(g, p^n, \ell, A) = \lim_{g\to\infty} \alpha_{2g}(\{\phi \in \mathrm{Mat}_{2g}(\mathbb{Z}_\ell) \mid \mathrm{coker}(\mathrm{Id} - \phi) \simeq A\}),$$

where α_{2g} is the normalized Haar measure on $\mathrm{Mat}_{2g}(\mathbb{Z}_\ell)$.

(See Sections 2.1 and 2.2 for more details on Haar measures.) Katz and Sarnak [1999] vastly extended the philosophy of considering the action of Frobenius as a random matrix, especially when the size of the base field is large. Friedman and Washington show that the limit on the right-hand side of Heuristic 1.2.1 exists, and that it defines exactly the same distribution on $\mathcal{G}$ as Cohen and Lenstra's original heuristic for imaginary quadratic extensions of $\mathbb{Q}$. However, just as the work of Malle calls into question the appropriateness of certain Cohen–Lenstra–Martinet distributions, it also calls into question the appropriateness of Friedman and Washington's proposed distribution. Indeed, the Friedman–Washington heuristic does not depend at all on the presence of ℓth roots of unity in the base field $\mathbb{F}_{p^n}(t)$, while Malle's work suggests that distributions modeling ℓ-Sylow subgroups of class groups ought to change in the presence of ℓth roots of unity. Thus, the new data of Malle suggests that Heuristic 1.2.1 might be flawed when $\mathbb{F}_{p^n}(t)$ has ℓth roots of unity.

A possible explanation for this flaw is that Frob_{p^n} is a symplectic similitude with respect to the Weil pairing on $T_\ell(C_f)$. Indeed, it scales the Weil pairing by p^n, so when considered as a matrix, $\mathrm{Frob}_{p^n} \in \mathrm{GSp}_{2g}^{(p^n)}(\mathbb{Z}_\ell)$. (See Section 2.1 for more details on this notation.) Since the presence of ℓth roots of unity in

$\mathbb{F}_{p^n}(t)$ depends on the congruence class of $p^n \pmod{\ell}$, the set of symplectic similitudes that scale the Weil pairing by p^n does indeed change when $\mathbb{F}_{p^n}(t)$ has ℓth roots of unity. These facts led Friedman and Washington (and Achter [2008]) to suggest:

Heuristic 1.2.2. If $A \in \mathcal{G}$, then

$$\lim_{g\to\infty} F(g, p^n, \ell, A) = \lim_{g\to\infty} \mu_{2g}^{(p^n)}(\{\phi \in \mathrm{GSp}_{2g}^{(p^n)}(\mathbb{Z}_\ell) \mid \operatorname{coker}(\mathrm{Id} - \phi) \simeq A\}),$$

where $\mu_{2g}^{(p^n)}$ is the unique normalized multiplicative Haar measure on $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ translated to $\mathrm{GSp}_{2g}^{(p^n)}(\mathbb{Z}_\ell)$.

(Again, see Sections 2.1 and 2.2 for more details on Haar measures.) Friedman and Washington hoped that this new heuristic would turn out to describe the same distribution as Heuristic 1.2.1, but Achter [2006] proved that

$$\lim_{g\to\infty} \mu_{2g}^{(p^n)}\big(\{\phi \in \mathrm{GSp}_{2g}^{(1)}(\mathbb{Z}_\ell) \mid \operatorname{coker}(\mathrm{Id} - \phi) \simeq \{0\}\}\big) \neq \lim_{g\to\infty} \alpha_{2g}\big(\{\phi \in \mathrm{Mat}_{2g}(\mathbb{Z}_\ell) \mid \operatorname{coker}(\mathrm{Id} - \phi) \simeq \{0\}\}\big),$$

revealing that this was not the case, providing an early indication of the importance of the presence of ℓth roots of unity in the base field. Achter used work of Katz and Sarnak [1999] to prove a revised version of Heuristic 1.2.1:

Theorem 1.2.3 [Achter 2008]. *If $A \in \mathcal{G}$, then*

$$\lim_{p^n\to\infty} \big| F(g, p^n, \ell, A) - \mu_{2g}^{(p^n)}\big(\{\phi \in \mathrm{GSp}_{2g}^{(p^n)}(\mathbb{Z}_\ell) \mid \operatorname{coker}(\mathrm{Id} - \phi) \simeq A\}\big)\big| = 0.$$

We remark that this limit in Theorem 1.2.3 leaves g fixed while letting p^n increase, whereas the limit in Heuristic 1.2.2 does the opposite.

The work of Ellenberg, Venkatesh and Westerland [Ellenberg et al. 2009] uses the topology of Hurwitz spaces to study Heuristic 1.2.2. One consequence of their work is that

$$\lim_{g\to\infty} \lim_{\substack{p^n\to\infty \\ p^n \not\equiv 1 \pmod{\ell}}} F(g, p^n, \ell, A) = \frac{1}{|\mathrm{Aut}\, A|} \prod_{i=1}^{\infty} (1 - \ell^{-i}).$$

Since $p^n \equiv 1 \pmod{\ell}$ exactly when $\mathbb{F}_{p^n}(t)$ has ℓth roots of unity, this result only addresses the case when the base field does not have ℓth roots of unity (and only when $p^n \to \infty$). The remaining case is when $p^n \equiv 1 \pmod{\ell}$; that is, the case where there are ℓth roots of unity in the base field. Conjecture 1.1.2 suggests that a different distribution is needed to describe this case. In fact, Corollary 5.2.2 gives such a distribution. Using Achter's result (Theorem 1.2.3), Corollary 5.2.2 implies the following theorem:

Theorem 1.2.4. *If A is a finite abelian ℓ-group with ℓ-rank r and ℓ^2-rank s, then*

$$\lim_{g\to\infty} \lim_{\substack{p^n\to\infty \\ p^n\equiv 1 \pmod{\ell^\xi}, \\ p^n\not\equiv 1 \pmod{\ell^{\xi+1}}}} F(g, p^n, \ell, A) = \begin{cases} \ell^{\frac{r(r-1)}{2}} \cdot (\ell^{-1}; \ell^{-1})_r \cdot \dfrac{\prod_{i=1}^{\infty} (1+\ell^{-i})^{-1}}{|\operatorname{Aut} A|^{-1}} & \textit{if } \xi = 1, \\ \ell^{\frac{r(r-1)}{2}+\frac{s(s-1)}{2}} \cdot (\ell^{-1}; \ell^{-1})_s \cdot (\ell^{-1}; \ell^{-2})_{\lceil\frac{r-s}{2}\rceil} \cdot \dfrac{\prod_{i=1}^{\infty} (1+\ell^{-i})^{-1}}{|\operatorname{Aut} A|^{-1}} & \textit{if } \xi = 2, \end{cases}$$

where $(\ell^{-1}; \ell^{-j})_k$ is the ℓ^{-j}-Pochhammer symbol, defined for any $j \in \mathbb{Z}^{>0}$ and $k \in \mathbb{Z}^{\geq 0}$ (see Notation 5.1.1).

Theorem 1.2.4 extends Conjecture 1.1.2 by including the case where $\mathbb{F}_{p^n}(t)$ has ℓ^2th roots of unity but not ℓ^3th roots of unity. Since imaginary hyperelliptic curves have only one place at infinity, the function field version of Conjecture 1.1.2 should set $u = 0$; making this substitution in Conjecture 1.1.2 yields the $\xi = 1$ case of Theorem 1.2.4.

2. Preliminaries

2.1. ***Notation and definitions.*** As above, let ℓ be an odd prime and let $\mathcal{G}$ be the poset of isomorphism classes of finite abelian ℓ-groups, with the relation $[A] \leq [B]$ if and only if there exists an injection $A \hookrightarrow B$. (For notational simplicity, we will conflate finite abelian ℓ-groups and the equivalence classes containing them.) For any $A \in \mathcal{G}$, we denote the exponent of A by $\exp A$. If $i \in \mathbb{Z}^{>0}$, let

$$\operatorname{rank}_{\ell^i} A := \dim_{\mathbb{F}_\ell}(\ell^{i-1}A/\ell^i A).$$

We will abbreviate $\operatorname{rank}_\ell A$ by $\operatorname{rank} A$. If $r_1, \dots, r_{i-1} \in \mathbb{Z}^{>0}$ and $r_i \in \mathbb{Z}^{\geq 0}$, let $\mathcal{G}(r_1, \dots, r_i)$ be the following subposet of $\mathcal{G}$:

$$\mathcal{G}(r_1, \dots, r_i) := \{A \in \mathcal{G} \mid \operatorname{rank}_{\ell^j} A = r_j \text{ for all } j \in \{1, \dots, i\}\}.$$

Next, for any $\rho \in \mathbb{Z}^{>0}$, set $R_\rho = \mathbb{Z}_\ell/\ell^\rho\mathbb{Z}_\ell \simeq \mathbb{Z}/\ell^\rho\mathbb{Z}$. For any $g, \rho \in \mathbb{Z}^{>0}$, let $\langle\,\cdot\,,\cdot\,\rangle_{2g,\rho}$ be the symplectic form on $(R_\rho)^{2g}$ given by

$$\Omega_g := \begin{pmatrix} 0 & \mathrm{Id}_g \\ -\mathrm{Id}_g & 0 \end{pmatrix}$$

with respect to the standard basis; note that $\langle\,\cdot\,,\cdot\,\rangle_{2g,a} : (R_\rho)^{2g} \times (R_\rho)^{2g} \to (R_\rho)$ is R_ρ-bilinear, alternating and nondegenerate. (See Theorem III.2 of [McDonald 1976] for more details on symplectic spaces.) Let $\langle\,\cdot\,,\cdot\,\rangle_{2g}$ be the analogous choice of symplectic form on $(\mathbb{Z}_\ell)^{2g}$. For any ring R and any $g \in \mathbb{Z}^{>0}$, if R^{2g} has a symplectic form $\langle\,\cdot\,,\,\cdot\,\rangle$, then the *symplectic group of R* is

$$\begin{aligned}\mathrm{Sp}_{2g}(R) &\simeq \mathrm{Sp}(R^{2g}, \langle\,\cdot\,,\,\cdot\,\rangle)\\ &= \{\phi \in \mathrm{GL}(R^{2g}) \mid \langle\phi(\boldsymbol{x}), \phi(\boldsymbol{y})\rangle = \langle\boldsymbol{x}, \boldsymbol{y}\rangle \text{ for all } \boldsymbol{x}, \boldsymbol{y} \in R^{2g}\}.\end{aligned}$$

Note that a different choice of symplectic form on R^{2g} yields an isometric space, so the choice is immaterial (see p. 188 of [McDonald 1976] for more details). Similarly, the *group of symplectic similitudes of R* is

$$\begin{aligned}\mathrm{GSp}_{2g}(R) \simeq \mathrm{GSp}(R^{2g}, \langle\,\cdot\,,\,\cdot\,\rangle) = \big\{\phi \in \mathrm{GL}(R^{2g}) \mid &\text{ there exists } m(\phi) \in R^{\times}\\ &\text{such that } \langle\phi(\boldsymbol{x}), \phi(\boldsymbol{y})\rangle = m(\phi)\cdot\langle\boldsymbol{x}, \boldsymbol{y}\rangle \text{ for all } \boldsymbol{x}, \boldsymbol{y} \in R^{2g}\big\}.\end{aligned}$$

For concreteness, we will always assume that the rings $(R_\rho)^{2g}$ and $(\mathbb{Z}_\ell)^{2g}$ are equipped with the forms $\langle\,\cdot\,,\,\cdot\,\rangle_{2g,\rho}$ and $\langle\,\cdot\,,\,\cdot\,\rangle_{2g}$ fixed above. The map

$$m : \mathrm{GSp}_{2g}\,(R) \to R^{\times} : \phi \mapsto m(\phi)$$

described above is a homomorphism called the *multiplier map*, and the element $m(\phi) \in R^{\times}$ is called the *multiplier* of ϕ. For any $g \in \mathbb{Z}^{>0}$, let μ_{2g} be the unique Haar measure on $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ satisfying $\mu_{2g}(\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)) = 1$. (We say a Haar measure satisfying this last condition is *normalized*.) Note that μ_{2g} is invariant under both left and right multiplication since $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ is a unimodular group. Finally, for any $g \in \mathbb{Z}^{>0}$ and any unit x in a ring R, let $\mathrm{GSp}_{2g}^{(x)}(R) = m^{-1}(x)$.

For any $x \in (\mathbb{Z}_\ell)^{\times}$ and $\phi \in \mathrm{GSp}_{2g}^{(x)}(\mathbb{Z}_\ell)$ we define a measure $\mu_{2g}^{(x)}$ on $\mathrm{GSp}_{2g}^{(x)}(\mathbb{Z}_\ell)$ as follows: for any μ_{2g}-measurable subset $S \subseteq \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$, define

$$\mu_{2g}^{(x)}(S\phi) := \mu_{2g}(S).$$

This measure is independent of the choice $\phi \in \mathrm{GSp}_{2g}^{(x)}(\mathbb{Z}_\ell)$. Indeed, given some other $\psi \in \mathrm{GSp}_{2g}^{(x)}(\mathbb{Z}_\ell)$, there exists a unique $\phi_\psi \in \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$ such that $\phi_\psi\phi = \psi$; i.e., $S\psi = S\phi_\psi\phi$. Since μ_{2g} is translation-invariant, we know that

$$\mu_{2g}(S) = \mu_{2g}(S\phi_\psi),$$

as desired. Moreover, since μ_{2g} is translation-invariant (by $\mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$) and normalized, so is $\mu_{2g}^{(x)}$. Similarly, for any $\rho \in \mathbb{Z}^{>0}$, let $\nu_{2g,\rho}$ be the unique normalized Haar measure on $\mathrm{Sp}_{2g}(R_\rho)$, and for any $x \in R_\rho^{\times}$, define $\nu_{2g,\rho}^{(x)}$ on $\mathrm{GSp}_{2g}^{(x)}(R_\rho)$ as above. For any $\rho \in \mathbb{Z}^{>0}$, $x \in R_\rho^{\times}$ and $S \subseteq \mathrm{GSp}_{2g}^{(x)}(R_\rho)$, we know $\nu_{2g,\rho}^{(x)}(S) = |S|\cdot|\mathrm{Sp}_{2g}(R_\rho)|^{-1}$, since $\mathrm{Sp}_{2g}(R_\rho)$ is a finite group. To ease notation, for any $A \in \mathcal{G}$, $g \in \mathbb{Z}^{>0}$ and $x \in (\mathbb{Z}_\ell)^{\times}$, we set

$$\mu_{2g}^{(x)}(A) := \mu_{2g}^{(x)}(\{\phi \in \mathrm{GSp}_{2g}^{(x)}(\mathbb{Z}_\ell) \mid \operatorname{coker}(\mathrm{Id} - \phi) \simeq A\}).$$

Furthermore, if $\rho \in \mathbb{Z}^{>0}$ and $x \in R_\rho^\times$, set

$$\nu_{2g,\rho}^{(x)}(A) := \nu_{2g,\rho}^{(x)}(\{\gamma \in \mathrm{GSp}_{2g}^{(x)}(R_\rho) \mid \mathrm{coker}(\mathrm{Id} - \gamma) \simeq A\}).$$

2.2. ***The Haar measures.*** The measures defined in Section 2.1 have an important relationship, given in the following lemma.

Lemma 2.2.1. *Suppose $A \in \mathcal{G}$, $g \in \mathbb{Z}^{>0}$, $x \in (\mathbb{Z}_\ell)^\times$ and $\rho \in \mathbb{Z}^{>0}$. Let $\overline{\cdot} : \mathbb{Z}_\ell \to R_\rho$ denote reduction mod ℓ^ρ. If $\ell^\rho > \exp A$, then*

$$\mu_{2g}^{(x)}(A) = \nu_{2g,\rho}^{(\bar{x})}(A).$$

Proof. Choose any $\phi \in \mathrm{GSp}_{2g}^{(x)}(\mathbb{Z}_\ell)$. Then for any measurable $S \subseteq \mathrm{GSp}_{2g}^{(x)}(\mathbb{Z}_\ell)$, we know that

$$\mu_{2g}^{(x)}(S) = \mu_{2g}^{(x)}(S\phi^{-1}\phi) = \mu_{2g}(S\phi^{-1})$$

by the definition of $\mu_{2g}^{(x)}$. Since μ_{2g} is invariant under translation, every coset of the kernel of the reduction map $\overline{\cdot} : \mathrm{Sp}_{2g}(\mathbb{Z}_\ell) \to R_\rho$ has the same measure; namely,

$$[\mathrm{Sp}_{2g}(\mathbb{Z}_\ell) : \ker(\overline{\cdot})]^{-1} = |\mathrm{Sp}_{2g}(R_\rho)|^{-1}.$$

Moreover, note that if $\psi \in \mathrm{GSp}_{2g}^{(x)}(\mathbb{Z}_\ell)$, then $m(\overline{\psi}) = \overline{m(\psi)}$ and $\mathrm{coker}(\mathrm{Id} - \psi) \simeq A$ if and only if $\mathrm{coker}(\mathrm{Id} - \overline{\psi}) \simeq A$, since $\ell^\rho > \exp A$. The result follows. □

Notation 2.2.2. Suppose that $g \in \mathbb{Z}^{>0}$ and $\xi \in \mathbb{Z}^{\geq 0}$. For $\rho \in \mathbb{Z}^{>0}$ satisfying $\rho \geq \xi$, we define an important subgroup of $\mathrm{GSp}_{2g}(R_\rho)$:

$$\mathrm{GSp}_{2g}^{\langle\xi\rangle}(R_\rho) := \{\gamma \in \mathrm{GSp}_{2g}(R_\rho) \mid m(\gamma) \in \ell^\xi R_\rho + 1\}.$$

Note that $\mathrm{GSp}_{2g}^{\langle\rho\rangle}(R_\rho) = \mathrm{Sp}_{2g}(R_\rho)$ and $\mathrm{GSp}_{2g}^{\langle 0\rangle}(R_\rho) = \mathrm{GSp}_{2g}(R_\rho)$. For any $A \in \mathcal{G}$, we adopt the suggestive notation

$$N_{2g,\rho}^{\langle\xi\rangle}(A) := |\{\gamma \in \mathrm{GSp}_{2g}^{\langle\xi\rangle}(R_\rho) \mid \mathrm{coker}(\mathrm{Id} - \gamma) \simeq A\}|$$

and, if $\rho > \xi$,

$$\nu_{2g,\rho}^{\langle\xi\rangle}(A) := \frac{N_{2g,\rho}^{\langle\xi\rangle}(A) - N_{2g,\rho}^{\langle\xi+1\rangle}(A)}{|\mathrm{GSp}_{2g}^{\langle\xi\rangle}(R_\rho)| - |\mathrm{GSp}_{2g}^{\langle\xi+1\rangle}(R_\rho)|}.$$

Goal 2.2.3. We can now state the matrix-theoretic analog of the situation about which Malle made his Conjecture 2.1. Following Heuristic 1.2.2, for $A \in \mathcal{G}$, $x \in (\mathbb{Z}_\ell)^\times$ and $\xi \in \mathbb{Z}^{>0}$, with $x \equiv 1 \pmod{\ell^\xi}$ but $x \not\equiv 1 \pmod{\ell^{\xi+1}}$, we must evaluate

$$\mu_x(A) := \lim_{g\to\infty} \mu_{2g}^{(x)}(A).$$

If we let $\bar{\cdot} : \mathbb{Z}_\ell \to R_\rho$ denote reduction mod ℓ^ρ, then we know by Lemma 2.2.1 that this amounts to calculating

$$\lim_{g\to\infty} \nu_{2g,\rho}^{(\bar{x})}(A)$$

for any $\rho \in \mathbb{Z}^{>0}$ satisfying both $\ell^\rho > \exp A$ and $\rho > \xi$. In Note 3.1.5 we will see that, for all such ρ,

$$\nu_{2g,\rho}^{(\bar{x})}(A) = \nu_{2g,\rho}^{\langle\xi\rangle}(A),$$

so we will turn our attention to computing

$$\lim_{g\to\infty} \nu_{2g,\rho}^{\langle\xi\rangle}(A),$$

which we compute explicitly for $\xi = 1, 2$ in Corollary 5.2.2. Using Achter's result, Theorem 1.2.3, we then obtain Theorem 1.2.4 as a corollary.

Remark 2.2.4. Suppose that $x \in \mathbb{Z}_\ell$. In addition to explicitly computing the distribution $\mu_x : \mathcal{G} \to \mathbb{R}$ if $x \equiv 1 \pmod{\ell^\xi}$ but $x \not\equiv 1 \pmod{\ell^{\xi+1}}$ for $\xi = 1, 2$, we also compute the moments of this distribution for any $\xi \in \mathbb{Z}^{>0}$. Specifically, in Corollary 3.2.7 we find that if $A \in \mathcal{G}$ then

$$\sum_{B\in\mathcal{G}} |\mathrm{Surj}(B, A)|\,\mu_x(B) = |\Lambda(A/\ell^\xi)|.$$

(See Notation 3.2.1 for the definition of Λ.) For any $A \in \mathcal{G}$, we call the quantity $\sum_{B\in\mathcal{G}}|\mathrm{Surj}(B, A)|\mu_x(B)$ the "Ath moment" of the distribution μ_x by analogy. Just as the kth moment of a real-valued random variable X is the expected value of X^k, the Ath moment of μ_x is the expected value of $|\mathrm{Surj}(B, A)|$, where B is a $\mathcal{G}$-valued random variable. Moreover, under certain favorable conditions, the set of Ath moments of a distribution on $\mathcal{G}$ determines the distribution, making the analogy even stronger. The term "Ath moment" is becoming standard in the literature related to the Cohen–Lenstra heuristics (see, for example, [Ellenberg et al. 2009; Matchett Wood 2014]).

3. The symplectic action

3.1. *Basic properties.*

Notation 3.1.1. For any $A, B \in \mathcal{G}$, let $\mathrm{Inj}(A, B)$ and $\mathrm{Surj}(A, B)$ be the sets of injective homomorphisms and surjective homomorphisms from A to B.

In what follows, we will consider either injections or surjections (as well as either kernels or cokernels) depending on which is more convenient at the time. The next two lemmas justify this shifting point of view.

Lemma 3.1.2. *Suppose that $A \in \mathcal{G}$, $g, \rho \in \mathbb{Z}^{>0}$ and $\xi \in \mathbb{Z}^{\geq 0}$. If $\rho \geq \xi$, then $\mathrm{GSp}_{2g}^{\langle \xi \rangle}(R_\rho)$ acts on $\mathrm{Inj}(A, (R_\rho)^{2g})$ and $\mathrm{Surj}((R_\rho)^{2g}, A)$ by postcomposition and precomposition, respectively. These actions have the same number of orbits.*

Proof. If $\ell^\rho < \exp A$, the result is trivial, so suppose $\ell^\rho \geq \exp A$. In this case, we can think of A as an R_ρ-module. Moreover, we know that R_ρ is an injective R_ρ-module by Baer's criterion, so the functor

$$(\,\cdot\,)^\vee := \mathrm{Hom}(\,\cdot\,, R_\rho) : R_\rho\mathtt{-mod} \to R_\rho\mathtt{-mod}$$

is exact. Thus, for any $\gamma \in \mathrm{GSp}_{2g}^{\langle \xi \rangle}(R_\rho)$,

$$f, h \in \mathrm{Inj}(A, (R_\rho)^{2g}) \quad \text{with } \gamma \circ f = h$$

if and only if

$$f^\vee, h^\vee \in \mathrm{Surj}(((R_\rho)^{2g})^\vee, A^\vee) \quad \text{with } f^\vee \circ \gamma^\vee = h^\vee.$$

After choosing R_ρ-bases for $(R_\rho)^{2g}$ and A, it is easy to see that $((R_\rho)^{2g})^\vee \simeq (R_\rho)^{2g}$, $A^\vee \simeq A$ and $\gamma^\vee = \gamma^\top \in \mathrm{GSp}_{2g}^{\langle \xi \rangle}(R_\rho)$, giving the result. □

The number orbits of the action described above turn out to be very important, so we bestow a name upon them:

Definition 3.1.3. Suppose that $A \in \mathcal{G}$, $g, \rho \in \mathbb{Z}^{>0}$ and $\xi \in \mathbb{Z}^{\geq 0}$. If $\rho \geq \xi$, let $o_{2g,\rho}^{A,\langle \xi \rangle}$ be the number of orbits of $\mathrm{GSp}_{2g}^{\langle \xi \rangle}(R_\rho)$ acting on $\mathrm{Inj}(A, (R_\rho)^{2g})$ or $\mathrm{Surj}((R_\rho)^{2g}, A)$.

Lemma 3.1.4. *For A, g, ρ, ξ as above,*

$$N_{2g,\rho}^{\langle \xi \rangle}(A) = \left|\{\gamma \in \mathrm{GSp}_{2g}^{\langle \xi \rangle}(R_\rho) \mid \ker(\mathrm{Id} - \gamma) \simeq A\}\right|.$$

Proof. As in Lemma 3.1.2, this follows from the exactness of $(\,\cdot\,)^\vee$. Note that, for any $\gamma \in \mathrm{GSp}_{2g}^{\langle \xi \rangle}(R_\rho)$,

$$(\mathrm{coker}(\mathrm{Id} - \gamma))^\vee = \ker((\mathrm{Id} - \gamma)^\vee) = \ker(\mathrm{Id} - \gamma^\top),$$

giving the result. □

In Goal 2.2.3, we turned our attention from the measures of cosets of the symplectic group to subgroups of the group of symplectic similitudes. The following note justifies this turn.

Note 3.1.5. Suppose that $A \in \mathcal{G}$, $g \in \mathbb{Z}^{>0}$, $x \in \mathbb{Z}_\ell$ and $\xi \in \mathbb{Z}^{>0}$, with $x \equiv 1 \pmod{\ell^\xi}$ but $x \not\equiv 1 \pmod{\ell^{\xi+1}}$. If $\rho \in \mathbb{Z}^{>0}$ satisfies $\rho > \xi$, then

$$\nu_{2g,\rho}^{(\bar{x})}(A) = \nu_{2g,\rho}^{\langle \xi \rangle}(A).$$

Proof. This amounts to showing that if $x, y \in R_\rho$ such that $x \equiv y \equiv 1 \pmod{\ell^\xi}$ but neither x nor y is equivalent to $1 \pmod{\ell^{\xi+1}}$, then

$$\nu_{2g,\rho}^{(\bar{x})}(A) = \nu_{2g,\rho}^{(\bar{y})}(A).$$

By our assumptions on x and y, there exists some m_0 such that $\ell \nmid m_0$ and $\bar{x}^{m_0} = \bar{y}$. Choose some m in the arithmetic progression $\{m_0 + \ell^{\rho-\xi} j\}_{j=0}^{\infty}$ such that

$$\gcd(m, |\mathrm{GSp}_{2g}(R_\rho)|) = 1,$$

and choose k such that $mk \equiv 1 \pmod{|\mathrm{GSp}_{2g}(R_\rho)|}$. Now, the map

$$\begin{gathered}(\,\cdot\,)^m : \mathrm{GSp}_{2g}^{(\bar{x})}(R_\rho) \to \mathrm{GSp}_{2g}^{(\bar{y})}(R_\rho)\\ \gamma \mapsto \gamma^m\end{gathered}$$

is bijective with inverse $(\,\cdot\,)^k$. Moreover, for any $z \in (R_\rho)^{2g}$ and any $\gamma \in \mathrm{GSp}_{2g}^{(\bar{x})}(R_\rho)$, it is clear that $\gamma z = z$ if and only if $\gamma^m z = z$. Thus, we obtain

$$\left|\{\gamma \in \mathrm{GSp}_{2g}^{(\bar{x})}(R_\rho) \mid \ker(\mathrm{Id} - \gamma) \simeq A\}\right| = \left|\{\gamma \in \mathrm{GSp}_{2g}^{(\bar{y})}(R_\rho) \mid \ker(\mathrm{Id} - \gamma) \simeq A\}\right|,$$

and we conclude by Lemma 3.1.4. □

3.2. *Orbit counting.*

Notation 3.2.1. For any $A \in \mathscr{G}$, let $\Lambda(A)$ be the set of alternating bilinear forms on A thought of as a $(\mathbb{Z}/\exp A)$-module.

Note 3.2.2. Suppose that $A = \mathbb{Z}/\ell^{\alpha_1} \oplus \cdots \oplus \mathbb{Z}/\ell^{\alpha_r}$ with $\alpha_1 \geq \cdots \geq \alpha_r > 0$. Then

$$|\Lambda(A)| = \ell^{\sum_{i=2}^{r} (i-1)\alpha_i}$$

Proof. Let $\{\boldsymbol{e}_i\}_{i=1}^r$ be a $(\mathbb{Z}/\exp A)$-basis for A such that $\boldsymbol{e}_i$ has order ℓ^{α_i} for all $i \in \{1, \dots, r\}$. Every alternating bilinear form $\langle\,\cdot\,,\cdot\,\rangle$ on A corresponds to an antisymmetric matrix $(\langle \boldsymbol{e}_i, \boldsymbol{e}_j\rangle) \in \mathrm{Mat}_{r\times r}\,(\mathbb{Z}/\exp A)$. Moreover, $\ell^{\alpha_j}\langle \boldsymbol{e}_i, \boldsymbol{e}_j\rangle = \langle \boldsymbol{e}_i, \ell^{\alpha_j}\boldsymbol{e}_j\rangle = 0$ for all $i < j$ since $\boldsymbol{e}_i$ has order ℓ^{α_i} for all $i \in \{1, \dots, r\}$. Conversely, any antisymmetric matrix $(a_{ij}) \in \mathrm{Mat}_{r\times r}\,(\mathbb{Z}/\exp A)$ corresponds to an alternating bilinear form on A, as long it has 0s along its main diagonal and $\ell^{\alpha_j} a_{ij} = 0$ whenever $i < j$ (this requirement encodes the fact that any bilinear form $\langle\,\cdot\,,\cdot\,\rangle$ on A must satisfy $\ell^{\alpha_j}\langle \boldsymbol{e}_i, \boldsymbol{e}_j\rangle = 0$ for all $i < j$). There are ℓ^{α_j} such elements of $\mathbb{Z}/\exp A$, so the result follows. □

Lemma 3.2.3. *Suppose that $r \in \mathbb{Z}^{\geq 0}$, $A \in \mathscr{G}(r)$, $g, \rho \in \mathbb{Z}^{>0}$ and $\xi \in \mathbb{Z}^{\geq 0}$. If $\ell^\rho \geq \exp A$, $\rho \geq \xi$ and $2g \geq r$, then*

$$o_{2g,\rho}^{A,\langle\xi\rangle} \leq \ell^{-(\rho-\xi)}|\Lambda(A)| + (\ell - 1) \sum_{i=0}^{\rho-\xi-1} \ell^{-(i+1)}|\Lambda(A/\ell^{\xi+i})|.$$

Furthermore, when $g \geq r$, the upper bound above is an equality. (*In particular, $o_{2g,\rho}^{A,\langle\xi\rangle}$ is independent of g for large enough g.*)

As pointed out in Goal 2.2.3, we need only calculate

$$\lim_{g\to\infty} \nu_{2g,\rho}^{\langle\xi\rangle}(A).$$

Despite this fact, the inequality for small g in Lemma 3.2.3 does indeed turn out to be useful. This is due to the fact that $\nu_{2g,\rho}^{\langle\xi\rangle}(A)$ can be expressed as a sum of orbit data for finite abelian groups of rank up to $2g$. (See Corollary 4.2.4.)

Proof of the lemma. The result is obviously true when $r = 0$, so suppose that $r > 0$. Theorem 2.14 of [Michael 2006] shows that the set of orbit representatives of $\mathrm{GSp}_{2g}^{\langle\rho\rangle}(R_\rho) = \mathrm{Sp}_{2g}(R_\rho)$ acting on $\mathrm{Surj}((R_\rho)^{2g}, A)$ injects into $\Lambda(A)$; there, this injection is denoted s', and when $g \geq r$, the map s' is a bijection.

We can define an action of $(R_\rho)^\times = \mathrm{GSp}_{2g}(R_\rho)/\mathrm{Sp}_{2g}(R_\rho)$ on $\mathrm{Surj}((R_\rho)^{2g}, A)$ as follows. For any $x \in (R_\rho)^\times$ and $f \in \mathrm{Surj}((R_\rho)^{2g}, A)$, note that

$$\begin{pmatrix} 0 & x\cdot \mathrm{Id}_g \\ -\mathrm{Id}_g & 0 \end{pmatrix} \in \mathrm{GSp}_{2g}(R_\rho), \quad \text{and define} \quad x\cdot f = f\circ \begin{pmatrix} 0 & x\cdot \mathrm{Id}_g \\ -\mathrm{Id}_g & 0 \end{pmatrix}.$$

We can also define an action of $(R_\rho)^\times$ on $\Lambda(A)$ by $x\cdot\langle\cdot,\cdot\rangle = x\langle\cdot,\cdot\rangle$ for any $x \in (R_\rho)^\times$ and $\langle\cdot,\cdot\rangle \in \Lambda(A)$. Again referring to the notation of [ibid.], the map s' is equivariant with respect to these two actions. (This follows from the definition of the map s' and the comment immediately preceding Lemma 2.2 from [ibid.].)

Thus, computing the number of orbits of $\mathrm{GSp}_{2g}^{\langle\xi\rangle}(R_\rho)$ acting on $\mathrm{Surj}((R_\rho)^{2g}, A)$ is a straightforward application of Burnside's counting theorem. Indeed, suppose that $A = \mathbb{Z}/\ell^{\alpha_1} \oplus\cdots\oplus \mathbb{Z}/\ell^{\alpha_r}$ with $\alpha_1 \geq \cdots \geq \alpha_r > 0$, then use Note 3.2.2 to see that

$$\begin{aligned} o_{2g,\rho}^{A,\langle\xi\rangle} &\leq \frac{1}{|\ell^\xi R_\rho + 1|}\cdot \sum_{\upsilon\in\ell^\xi R_\rho+1} |\mathrm{Fix}\,(\upsilon)| \\ &= \frac{1}{|\ell^\xi R_\rho + 1|}\Biggl(\Biggl(\sum_{i=0}^{\rho-\xi-1} \sum_{\upsilon\in(\ell^{\xi+i}R_\rho+1)\setminus(\ell^{\xi+i+1}R_\rho+1)} |\mathrm{Fix}(\upsilon)|\Biggr) + \sum_{\upsilon\in\ell^\rho R_\rho+1=\{1\}} |\mathrm{Fix}(\upsilon)|\Biggr) \\ &= \frac{1}{\ell^{\rho-\xi}}\Biggl(\sum_{i=0}^{\rho-\xi-1} (\ell^{\rho-\xi-i} - \ell^{\rho-\xi-i-1})\ell^{\sum_{j=2}^r (j-1)\min\{\xi+i,\alpha_j\}} + \ell^{\alpha_2+2\alpha_3+\cdots+(r-1)\alpha_r}\Biggr) \\ &= \frac{1}{\ell^{\rho-\xi}}|\Lambda(A)| + (\ell-1)\sum_{i=0}^{\rho-\xi-1} \ell^{-(i+1)}|\Lambda(A/\ell^{\xi+i})|, \end{aligned}$$

with equality when $g \geq r$. □

Notation 3.2.4. Suppose that $A \in \mathcal{G}$, $\rho \in \mathbb{Z}^{>0}$ and $\xi \in \mathbb{Z}^{\geq 0}$. If $\ell^\rho \geq \exp A$ and $\rho \geq \xi$, use Lemma 3.2.3 to define $o_\rho^{A,\langle\xi\rangle} := o_{2g,\rho}^{A,\langle\xi\rangle}$ for any $g \in \mathbb{Z}^{>0}$ such that $g \geq \operatorname{rank} A$.

We now mention an identity which will be useful later. (See Corollary 3.2.7 and Note 4.2.5.)

Note 3.2.5. Suppose $A \in \mathcal{G}$ and $\rho, \xi \in \mathbb{Z}^{>0}$. If $\ell^\rho \geq \exp A$ and $\rho > \xi$, then by Lemma 3.2.3 and Note 3.2.2, we see that

$$\ell o_\rho^{A,\langle \xi \rangle} - o_\rho^{A,\langle \xi+1 \rangle} = (\ell - 1)|\Lambda(A/\ell^\xi)|.$$

Below is a simple observation, which has Corollary 3.2.7 as an important consequence. This corollary gives the moments of the probability distributions $\mu_x : \mathcal{G} \to \mathbb{R}$ for any $x \in \mathbb{Z}_\ell$, as promised in Section 2.2.

Lemma 3.2.6. *Suppose that $A \in \mathcal{G}$, $g, \rho \in \mathbb{Z}^{>0}$ and $\xi \in \mathbb{Z}^{\geq 0}$. Furthermore, suppose $\rho \geq \xi$, let $\gamma \in \mathrm{GSp}_{2g}^{\langle \xi \rangle}(R_\rho)$, and consider $\mathrm{Inj}(A, \ker(\mathrm{Id} - \gamma)) \subseteq \mathrm{Inj}(A, (R_\rho)^{2g})$. There is a one-to-one correspondence between $\mathrm{Inj}(A, \ker(\mathrm{Id} - \gamma))$ and $\mathrm{Fix}(\gamma)$. Dually, there is a one-to-one correspondence between $\mathrm{Surj}(\mathrm{coker}(\mathrm{Id} - \gamma), A)$ and $\mathrm{Fix}(\gamma)$.*

Proof. Suppose that $f \in \mathrm{Inj}(A, (R_\rho)^{2g})$. Note that $f \in \mathrm{Inj}(A, \ker(\mathrm{Id} - \gamma))$ if and only if $(\mathrm{Id} - \gamma) f = 0$ if and only if $f = \gamma f$. The dual proof is similar. □

Corollary 3.2.7. *Let $x \in \mathbb{Z}_\ell$ and suppose that $x \equiv 1 \pmod{\ell^\xi}$ but $x \not\equiv 1 \pmod{\ell^{\xi+1}}$ for some $\xi \in \mathbb{Z}^{>0}$. If $A \in \mathcal{G}$, then*

$$\sum_{B \in \mathcal{G}} |\mathrm{Surj}(B, A)| \mu_x(B) = |\Lambda(A/\ell^\xi)|.$$

Proof. Choose any $g, \rho \in \mathbb{Z}^{>0}$ such that $g \geq \operatorname{rank} A$, $\ell^\rho \geq \exp A$, and $\rho > \xi$. To begin with, note that

$$\begin{aligned}
&\sum_{B \in \mathcal{G}} |\mathrm{Surj}(B, A)| \nu_{2g,\rho}^{(x)}(B) \\
&\quad = |\mathrm{GSp}_{2g}^{(x)}(R_\rho)|^{-1} \cdot \sum_{B \in \mathcal{G}} |\mathrm{Surj}(B, A)| \cdot \left|\{\gamma \in \mathrm{GSp}_{2g}^{(x)}(R_\rho) \mid \mathrm{coker}(\mathrm{Id} - \gamma) \simeq B\}\right| \\
&\quad = |\mathrm{GSp}_{2g}^{(x)}(R_\rho)|^{-1} \cdot \sum_{\gamma \in \mathrm{GSp}_{2g}^{(x)}(R_\rho)} |\mathrm{Surj}(\mathrm{coker}(\mathrm{Id} - \gamma), A)|.
\end{aligned}$$

Now, thanks to Note 3.1.5, we can turn our attention to the quantity

$$|\mathrm{GSp}_{2g}^{\langle \xi \rangle}(R_\rho) \setminus \mathrm{GSp}_{2g}^{\langle \xi+1 \rangle}(R_\rho)|^{-1} \cdot \sum_{\gamma \in \mathrm{GSp}_{2g}^{\langle \xi \rangle}(R_\rho) \setminus \mathrm{GSp}_{2g}^{\langle \xi+1 \rangle}(R_\rho)} |\mathrm{Surj}(\mathrm{coker}(\mathrm{Id} - \gamma), A)|.$$

Using the fact that $|\mathrm{GSp}_{2g}^{\langle \xi \rangle}(R_\rho)| = \ell |\mathrm{GSp}_{2g}^{\langle \xi+1 \rangle}(R_\rho)|$ and applying Lemma 3.2.6 to $\mathrm{GSp}_{2g}^{\langle \xi \rangle}(R_\rho)$ acting on $\mathrm{Surj}((R_\rho)^{2g}, A)$, then using Burnside's counting theorem and Notation 3.2.4, we see that

$$
\begin{aligned}
&|\mathrm{GSp}_{2g}^{\langle\xi\rangle}(R_\rho)\setminus\mathrm{GSp}_{2g}^{\langle\xi+1\rangle}(R_\rho)|^{-1}\cdot\sum_{\gamma\in\mathrm{GSp}_{2g}^{\langle\xi\rangle}(R_\rho)\setminus\mathrm{GSp}_{2g}^{\langle\xi+1\rangle}(R_\rho)}|\mathrm{Surj}(\mathrm{coker}(\mathrm{Id}-\gamma),A)|\\
&=\frac{\ell}{(\ell-1)\,|\mathrm{GSp}_{2g}^{\langle\xi\rangle}(R_\rho)|}\Bigg(\sum_{\gamma\in\mathrm{GSp}_{2g}^{\langle\xi\rangle}(R_\rho)}|\mathrm{Fix}\,\gamma|-\sum_{\gamma\in\mathrm{GSp}_{2g}^{\langle\xi+1\rangle}(R_\rho)}|\mathrm{Fix}\,\gamma|\Bigg)\\
&=\frac{\ell}{\ell-1}\Bigg(\sum_{\gamma\in\mathrm{GSp}_{2g}^{\langle\xi\rangle}(R_\rho)}\frac{|\mathrm{Fix}\,\gamma|}{|\mathrm{GSp}_{2g}^{\langle\xi\rangle}(R_\rho)|}-\sum_{\gamma\in\mathrm{GSp}_{2g}^{\langle\xi+1\rangle}(R_\rho)}\frac{|\mathrm{Fix}\,\gamma|}{\ell\,|\mathrm{GSp}_{2g}^{\langle\xi+1\rangle}(R_\rho)|}\Bigg)\\
&=\frac{\ell}{\ell-1}\Big(o_{2g,\rho}^{A,\langle\xi\rangle}-\frac{1}{\ell}o_{2g,\rho}^{A,\langle\xi+1\rangle}\Big)\\
&=\frac{1}{\ell-1}\big(\ell o_\rho^{A,\langle\xi\rangle}-o_\rho^{A,\langle\xi+1\rangle}\big),
\end{aligned}
$$

so we can conclude by applying Note 3.2.5 and Lemma 2.2.1. □

4. A weighted Möbius function

4.1. ***First observations.*** Let $\mathcal{P}$ be a locally finite poset. The *Möbius function* on $\mathcal{P}$, denoted by $\mu_{\mathcal{P}}$, is defined by the following criteria: for any $x, z\in\mathcal{P}$,

$$
\begin{aligned}
\mu_{\mathcal{P}}(x,z)&=0 &&\text{if } x\not\leq z,\\
\mu_{\mathcal{P}}(x,z)&=1 &&\text{if } x=z,\\
\textstyle\sum_{x\leq y\leq z}\mu_{\mathcal{P}}(x,y)&=0 &&\text{if } x<z.
\end{aligned}
$$

A classic reference for Möbius functions is [Rota 1964]. In this section, we need to study a variant of the Möbius function on the poset of subgroups of a finite group (ordered by inclusion). For a history of the work on the Möbius function on this poset, see [Hawkes et al. 1989]. Now, for any finite group G, let $\mathcal{P}_G$ be the poset of subgroups of G ordered by inclusion. For $A\in\mathcal{G}$, we study an amalgam of the Möbius functions on $\mathcal{P}_A$ and $\mathcal{G}$, which we define below.

Notation 4.1.1. For any $A, B\in\mathcal{G}$, let $\mathrm{sub}(A,B)$ be the number of subgroups of B that are isomorphic to A. If $A\in\mathcal{G}$, an A-*chain* is a finite (possibly empty) linearly ordered subset of $\{B\in\mathcal{G}\mid B>A\}$. Now, given an A-chain $\mathfrak{C}=\{A_j\}_{j=1}^{i}$, with $A_j<A_{j+1}$ for all $j\in\{1,\dots,i-1\}$, define

$$\mathrm{sub}(\mathfrak{C}):=(-1)^i\,\mathrm{sub}(A,A_1)\prod_{j=1}^{i-1}\mathrm{sub}(A_j,A_{j+1}).$$

(We set $\operatorname{sub}(\mathfrak{C}) = 1$ if $\mathfrak{C}$ is empty.) Finally, for any $A, B \in \mathcal{G}$, let

$$S(A, B) = \begin{cases} 0 & \text{if } A \not\leq B, \\ 1 & \text{if } A = B, \\ \displaystyle\sum_{\substack{A\text{-chains } \mathfrak{C}, \\ \max \mathfrak{C} = B}} \operatorname{sub}(\mathfrak{C}) & \text{if } A < B. \end{cases}$$

Remark 4.1.2. Though S is defined on the poset $\mathcal{G}$, it is closely related to the classical work on the Möbius function on the subgroup lattice of a fixed group. Indeed, by applying Lemma 2.2 of [Hawkes et al. 1989], we see that if $A, B \in \mathcal{G}$, then

$$S(A, B) = \sum_{\substack{C \leq B \\ C \simeq A}} \mu_B(C, B).$$

Given $x \in (\mathbb{Z}_\ell)^\times$, we can use the function S defined in Notation 4.1.1 to begin our analysis of the measure μ_x, following the outline in Goal 2.2.3.

Lemma 4.1.3. *Suppose $A \in \mathcal{G}$, $g, \rho \in \mathbb{Z}^{>0}$ and $\xi \in \mathbb{Z}^{\geq 0}$, with $\rho \geq \xi$ and $\ell^\rho \geq \exp A$. Then*

$$o_{2g,\rho}^{A,\langle\xi\rangle} |\mathrm{GSp}_{2g}^{\langle\xi\rangle}(R_\rho)| = \sum_{\substack{B \in \mathcal{G} \\ B \leq (R_\rho)^{2g}}} N_{2g,\rho}^{\langle\xi\rangle}(B)\, |\mathrm{Inj}(A, B)|.$$

Proof. Applying Lemma 3.2.6 and Burnside's counting theorem, we see that

$$\begin{aligned} o_{2g,\rho}^{A,\langle\xi\rangle} |\mathrm{GSp}_{2g}^{\langle\xi\rangle}(R_\rho)| &= \sum_{\gamma \in \mathrm{GSp}_{2g}^{\langle\xi\rangle}(R_\rho)} |\mathrm{Fix}(\gamma)| = \sum_{\gamma \in \mathrm{GSp}_{2g}^{\langle\xi\rangle}(R_\rho)} |\mathrm{Inj}(A, \ker(\mathrm{Id} - \gamma))| \\ &= \sum_{\substack{B \in \mathcal{G} \\ B \leq (R_\rho)^{2g}}} N_{2g,\rho}^{\langle\xi\rangle}(B)\, |\mathrm{Inj}(A, B)|, \end{aligned}$$

where the last step follows from Lemma 3.1.4. □

For A, g, ρ, ξ as above, Lemma 4.1.3 gives us an "upper triangular" system of equations, which we will solve for $N_{2g,\rho}^{\langle\xi\rangle}(A)$. (The quotes indicate that the system is indexed by the poset $\mathcal{P}_{(R_\rho)^{2g}}$.) Proposition 4.1.4 is the first step along this path.

Proposition 4.1.4. *Suppose A, g, ρ, ξ are as above. Then*

$$\frac{N_{2g,\rho}^{\langle\xi\rangle}(A)}{|\mathrm{GSp}_{2g}^{\langle\xi\rangle}(R_\rho)|} = \sum_{\substack{B \in \mathcal{G} \\ B \leq (R_\rho)^{2g}}} o_{2g,\rho}^{B,\langle\xi\rangle} \cdot \frac{S(A, B)}{|\mathrm{Aut}\, B|}.$$

Proof. We use strong induction on $|(R_\rho)^{2g}|/|A|$. In light of Lemma 4.1.3, the base case $A = (R_\rho)^{2g}$ is trivial. Now suppose the result is true for all $B \in \mathcal{G}$ with

$B \le (R_\rho)^{2g}$ and $|(R_\rho)^{2g}|/|B| < |(R_\rho)^{2g}|/|A|$. Using Lemma 4.1.3, we see that

$$\begin{aligned}\frac{N^{\langle\xi\rangle}_{2g,\rho}(A)}{|\mathrm{GSp}^{\langle\xi\rangle}_{2g}(R_\rho)|} &= \frac{1}{|\mathrm{Aut}\,A|}\cdot\Biggl(o^{A,\langle\xi\rangle}_{2g,\rho} - \frac{1}{|\mathrm{GSp}^{\langle\xi\rangle}_{2g}(R_\rho)|}\cdot\sum_{\substack{B\in\mathcal{G}\\ B\le(R_\rho)^{2g}\\ B\ne A}} N^{\langle\xi\rangle}_{2g,\rho}(B)\,|\mathrm{Inj}(A,B)|\Biggr)\\ &= \frac{o^{A,\langle\xi\rangle}_{2g,\rho}}{|\mathrm{Aut}\,A|} - \sum_{\substack{B\in\mathcal{G}\\ B\le(R_\rho)^{2g}\\ B\ne A}} \frac{N^{\langle\xi\rangle}_{2g,\rho}(B)}{|\mathrm{GSp}^{\langle\xi\rangle}_{2g}(R_\rho)|}\cdot\mathrm{sub}(A,B),\end{aligned}$$

so the result follows by the induction hypothesis. □

4.2. *Vanishing of the Möbius function.* Before proceeding, we need a bit more notation, and two results from [Garton 2014b].

Notation 4.2.1. For any $A\in\mathcal{G}$ and any $i\in\mathbb{Z}^{\ge 0}$, let

$$A_{\oplus i} := A\oplus\overbrace{(\mathbb{Z}/\ell)\oplus\cdots\oplus(\mathbb{Z}/\ell)}^{i\text{ times}}.$$

Hall [1934] proved that if G is an ℓ-group of order ℓ^n, then $\mu_G(1,G)=0$ unless G is elementary abelian, in which case $\mu_G(1,G)=(-1)^n\ell^{\binom{n}{2}}$. There is an analogous result for the function S:

Theorem 4.2.2 [Garton 2014b]. *If $A, B\in\mathcal{G}$, then $S(A,B)=0$ unless there exists an injection $\iota : A\hookrightarrow B$ with* coker(ι) *elementary abelian.*

Additionally, this property of S will prove helpful:

Theorem 4.2.3 [ibid.]. *If $A, B\in\mathcal{G}$ and $B=C_{\oplus i}$ for some $C\in\mathcal{G}$ with* $\operatorname{rank} C = \operatorname{rank} A$ *and $i\in\mathbb{Z}^{\ge 0}$, then $S(A,B)=S(A,C)\cdot S(C,B)$.*

Theorem 4.2.2 and Theorem 4.2.3 have the following corollary:

Corollary 4.2.4. *Suppose A, g, ρ, ξ are as above, and let $r=\operatorname{rank} A$. If in addition we know $\xi\in\mathbb{Z}^{>0}$ and ρ satisfies $\rho>\xi$ and $\ell^\rho>\exp A$, then*

$$\nu^{\langle\xi\rangle}_{2g,\rho}(A)=\sum_{B\in\mathcal{G}(r)} S(A,B)\cdot\sum_{i=0}^{2g-r}\frac{\ell o^{B_{\oplus i},\langle\xi\rangle}_{2g,\rho}-o^{B_{\oplus i},\langle\xi+1\rangle}_{2g,\rho}}{\ell-1}\cdot\frac{S(B,B_{\oplus i})}{|\mathrm{Aut}\,B_{\oplus i}|}.$$

Proof. Using the fact that $|\mathrm{GSp}^{\langle\xi\rangle}_{2g}(R_\rho)|=\ell\,|\mathrm{GSp}^{\langle\xi+1\rangle}_{2g}(R_\rho)|$, note that

$$\begin{aligned}\nu^{\langle\xi\rangle}_{2g,\rho}(A) &= \frac{N^{\langle\xi\rangle}_{2g,\rho}(A)-N^{\langle\xi+1\rangle}_{2g,\rho}(A)}{|\mathrm{GSp}^{\langle\xi\rangle}_{2g}(R_\rho)|-|\mathrm{GSp}^{\langle\xi+1\rangle}_{2g}(R_\rho)|}\\ &= \frac{\ell N^{\langle\xi\rangle}_{2g,\rho}(A)}{(\ell-1)\,|\mathrm{GSp}^{\langle\xi\rangle}_{2g}(R_\rho)|}-\frac{N^{\langle\xi+1\rangle}_{2g,\rho}(A)}{(\ell-1)\,|\mathrm{GSp}^{\langle\xi+1\rangle}_{2g}(R_\rho)|}.\end{aligned}$$

Applying Proposition 4.1.4, we obtain

$$\nu_{2g,\rho}^{\langle\xi\rangle}(A) = \sum_{\substack{B\in\mathcal{G}\\ B\leq(R_\rho)^{2g}}} \frac{\ell o_{2g,\rho}^{B,\langle\xi\rangle} - o_{2g,\rho}^{B,\langle\xi+1\rangle}}{\ell-1}\cdot\frac{S(A,B)}{|\mathrm{Aut}\,B|}.$$

Now, by Theorem 4.2.2 we know that if $B\in\mathcal{G}$ is not of the form $B=C_{\oplus i}$ for some $C\in\mathcal{G}(r)$ and some $i\in\mathbb{Z}^{\geq 0}$, then $S(A,B)$ vanishes. Thus, by Theorem 4.2.3, we conclude that

$$\nu_{2g,\rho}^{\langle\xi\rangle}(A) = \sum_{B\in\mathcal{G}(r)} S(A,B)\cdot\sum_{i=0}^{2g-r} \frac{\ell o_{2g,\rho}^{B_{\oplus i},\langle\xi\rangle} - o_{2g,\rho}^{B_{\oplus i},\langle\xi+1\rangle}}{\ell-1}\cdot\frac{S(B,B_{\oplus i})}{|\mathrm{Aut}\,B_{\oplus i}|},$$

as desired. □

Note 4.2.5. Suppose A, g, ρ, ξ, r are as in Corollary 4.2.4, and suppose that $g\geq r$. Then for any $B\in\mathcal{G}(r)$ and $i\in\{0\ldots,g-r\}$, we know by Note 3.2.5 and Note 3.2.2 that

$$\frac{\ell o_{2g,\rho}^{B_{\oplus i},\langle\xi\rangle} - o_{2g,\rho}^{B_{\oplus i},\langle\xi+1\rangle}}{\ell-1} = |\Lambda(B_{\oplus i}/\ell^\xi)| = \ell^{ir+\frac{i(i-1)}{2}}|\Lambda(B/\ell^\xi B)|,$$

and for any $i\in\{g-r+1,\ldots,2g-r\}$, we can use the proof of Lemma 3.2.3 to note that

$$\frac{\ell o_{2g,\rho}^{B_{\oplus i},\langle\xi\rangle} - o_{2g,\rho}^{B_{\oplus i},\langle\xi+1\rangle}}{\ell-1} \leq \ell o_{2g,\rho}^{B_{\oplus i},\langle\xi\rangle} \leq \ell|\Lambda(B_{\oplus i})| = \ell^{ir+\frac{i(i-1)}{2}+1}|\Lambda(B)|.$$

Thus, if

$$\sum_{i=0}^{\infty}\ell^{ir+\frac{i(i-1)}{2}}\frac{S(B,B_{\oplus i})}{|\mathrm{Aut}\,B_{\oplus i}|}$$

converges absolutely (and it does; see Lemmas 5.1.2 and 5.1.3 and Theorem 5.1.4), then so does

$$\sum_{i=0}^{\infty}\frac{\ell o_{2g,\rho}^{B_{\oplus i},\langle\xi\rangle} - o_{2g,\rho}^{B_{\oplus i},\langle\xi+1\rangle}}{\ell-1}\cdot\frac{S(B,B_{\oplus i})}{|\mathrm{Aut}\,B_{\oplus i}|},$$

and

$$\lim_{g\to\infty}\nu_{2g,\rho}^{\langle\xi\rangle}(A) = \sum_{B\in\mathcal{G}(r)} S(A,B)|\Lambda(B/\ell^\xi B)|\cdot\sum_{i=0}^{\infty}\ell^{ir+\frac{i(i-1)}{2}}\frac{S(B,B_{\oplus i})}{|\mathrm{Aut}\,B_{\oplus i}|}.$$

Analyzing the inner series is the subject of the next section. (Note that this limit does not depend on ρ, once ρ is large enough; this is consistent with Lemma 2.2.1.)

5. q-series and convergence

5.1. *q-series.* Before continuing, we make a small foray into some q-series notation and calculations.

Notation 5.1.1. For $z, q \in \mathbb{C}$ with $|q| < 1$ and $i \in \mathbb{Z}^{\geq 0}$, let

$$(z; q)_i := \prod_{j=0}^{i-1} (1 - q^j z).$$

To ease notation, set $(q)_i := (q; q)_i$. Recall the definition of the q-binomial coefficients: for any $k, m \in \mathbb{Z}^{\geq 0}$, let

$$\binom{k}{m}_q := \frac{(q)_k}{(q)_m (q)_{k-m}},$$

with $\binom{k}{m}_q := 0$ if $k < m$.

For $i \in \mathbb{Z}^{\geq 0}$, let $r_i = -1/(\ell^{\frac{i(i+1)}{2}} (\ell^{-1})_i)$. We define the next object in terms of any finite set of nonnegative integers S and any $i \in \mathbb{Z}$ satisfying $i > \max S$. If $S \cup \{0\} = \{s_0, \dots, s_j\}$, where $0 = s_0 < s_1 < \cdots < s_{j+1} := i$, define $r_S^i = \prod_{i=0}^{j} r_{s_{i+1} - s_i}$.

Finally, let $t_0 = 1$, let $t_1 = r_{\varnothing}^1$, and for $i > 1$, let

$$t_i = \sum_{S \subseteq \{1, \dots i-1\}} r_S^i.$$

Lemma 5.1.2.
$$\sum_{i=0}^{\infty} t_i = \prod_{i=1}^{\infty} (1 + \ell^{-i})^{-1}.$$

Proof. Let $R = r_1 + r_2 + \cdots$ and, to get into the spirit of a q-series calculation, let $q = \ell^{-1}$. Using a product formula of Euler (see [Andrews 1976, p. 19]), we note that

$$R = -\sum_{i=1}^{\infty} \frac{q^{\frac{i(i+1)}{2}}}{(1 - q^i) \cdots (1 - q)} = -\sum_{i=1}^{\infty} \frac{q^i q^{\frac{i(i-1)}{2}}}{(1 - q^i) \cdots (1 - q)} = 1 - \prod_{i=1}^{\infty} (1 + q^i).$$

Now, by the definition of t_i (and by using Lemma 5.1.3 to rearrange the terms of the sum), we know

$$\sum_{i=0}^{\infty} t_i = 1 + R + R^2 + R^3 + \cdots = \frac{1}{1 - R} = \prod_{i=1}^{\infty} (1 + \ell^{-i})^{-1},$$

as desired. □

Next, we justify the reordering of the summands in Lemma 5.1.2:

Lemma 5.1.3. *For any finite set of nonnegative integers S and $i \in \mathbb{Z}$ satisfying $i > \max S$, let $\rho_S^i := |r_S^i|$. Next, let $\tau_0 = 1$, let $\tau_1 = \rho_\varnothing^1$, and for any $i > 1$, let*

$$\tau_i := \sum_{S \subseteq \{1,\ldots i-1\}} \rho_S^i.$$

Then $\sum_{i=0}^\infty \tau_i$ converges.

Proof. For fun, we will give two proofs: a simple proof that holds for any $\ell > 3$, and a more complicated one that holds for $\ell \geq 3$. Note that the sum clearly diverges for $\ell = 2$ since it includes infinitely many 1s.

For the simple proof, note that for any finite set S of nonnegative integers and any $i > \max S$, we know $\rho_S^i \leq (\ell - 1)^{-i}$. It follows that for any $i \in \mathbb{Z}^{\geq 0}$, we have that $\tau_i \leq 2^{i-1}(\ell-1)^{-i}$, so $\sum_{i=0}^\infty \tau_i$ converges for $\ell > 3$.

Of course, this argument fails for $\ell = 3$. In this case, for a finite set S of nonnegative integers and an $i > \max S$, we must use a (slightly) better bound than $\rho_S^i \leq (\ell-1)^{-i}$. Let $\lambda = (\ell-1)^{-1}$. Since $(\ell^m - 1)^{-1} \leq (\ell-1)^{-m}$ for any $m \in \mathbb{Z}^{\geq 0}$, if we let $S \cup \{0\} = \{s_0, \ldots, s_j\}$, where $0 = s_0 < s_1 < \cdots < s_{j+1} := i$, then

$$\rho_S^i = \prod_{k=0}^{j} |r_{s_{k+1}-s_k}| \leq \prod_{k=0}^{j} \lambda^{\frac{1}{2}(s_{k+1}-s_k)(s_{k+1}-s_k+1)}. \tag{1}$$

Let T_i be the number of compositions of i by triangular numbers. By rearranging the terms of $\sum_{i=0}^\infty \tau_i$ to order them by the exponent of λ appearing in the bound (1), we see that if $\sum_{i=1}^\infty T_i \lambda^i$ converges, then so does $\sum_{i=0}^\infty \tau_i$. Since the generating function for the number of compositions of positive triangular numbers is

$$\sum_{i=0}^\infty T_i x^i = \frac{1}{1 - \sum_{j=1}^\infty x^{\frac{1}{2}j(j+1)}}, \tag{2}$$

we need only show that the radius of convergence of (2) is at least λ. Since $\ell \geq 3$, we know that $\lambda \leq \frac{1}{2}$, and

$$1 > \tfrac{1}{2} + (\tfrac{1}{2})^3 + (\tfrac{1}{2})^6 + (\tfrac{1}{2})^{10} + \cdots,$$

so the lemma is true. □

We can now finish proving the result mentioned in Note 4.2.5.

Theorem 5.1.4. *Suppose $A \in \mathcal{G}$, $\rho, \xi \in \mathbb{Z}^{>0}$, and let $r = \operatorname{rank} A$. If $\rho > \xi$ and $\ell^\rho > \exp A$, then*

$$\lim_{g\to\infty} \nu_{2g,\rho}^{\langle\xi\rangle}(A) = \prod_{i=1}^\infty (1+\ell^{-i})^{-1} \cdot \sum_{B \in \mathcal{G}(r)} |\Lambda(B/\ell^\xi B)| \cdot \frac{S(A,B)}{|\operatorname{Aut} B|}.$$

Proof. Let $B \in \mathscr{G}(r, s)$, let S be a finite set of nonnegative integers, and let i be a positive integer with $i > \max S$. Suppose $S \cup \{0\} = \{s_0, \dots, s_j\}$, where $0 = s_0 < \cdots < s_{j+1} := i$. Now, we know by [Garton 2014a] that, for any $k, m \in \mathbb{Z}^{\geq 0}$ with $k \leq m$,

$$\operatorname{sub}(B_{\oplus k}, B_{\oplus m}) = \frac{\ell^{(r+k)(m-k)}(\ell^{-1})_{r-s+m}}{(\ell^{-1})_{r-s+i}(\ell^{-1})_{m-k}}$$

and

$$|\operatorname{Aut} B_{\oplus i}| = \frac{\ell^{2ir+i^2}(\ell^{-1})_{r-s+i}}{(\ell^{-1})_{r-s}}|\operatorname{Aut} B|,$$

so

$$\begin{aligned}
&(-1)^{j+1} \cdot \frac{\ell^{ir+\frac{i(i-1)}{2}}}{|\operatorname{Aut} B_{\oplus i}|} \cdot \prod_{k=0}^{j} \operatorname{sub}(B_{\oplus s_k}, B_{\oplus s_{k+1}}) \\
&= (-1)^{j+1} \cdot \frac{\ell^{-ir-\frac{i(i+1)}{2}}}{|\operatorname{Aut} B|} \cdot \frac{(\ell^{-1})_{r-s}}{(\ell^{-1})_{r-s+i}} \cdot \prod_{k=0}^{j} \frac{\ell^{(r+s_k)(s_{k+1}-s_k)}(\ell^{-1})_{r-s+s_{k+1}}}{(\ell^{-1})_{r-s+s_k}(\ell^{-1})_{s_{k+1}-s_k}} \\
&= (-1)^{j+1} \cdot \frac{\ell^{-ir-\frac{i(i+1)}{2}}}{|\operatorname{Aut} B|} \cdot \prod_{k=0}^{j} \frac{\ell^{(r+s_k)(s_{k+1}-s_k)}}{(\ell^{-1})_{s_{k+1}-s_k}} \\
&= (-1)^{j+1} \cdot \frac{1}{|\operatorname{Aut} B|} \cdot \prod_{k=0}^{j} \frac{\ell^{-\frac{1}{2}(s_{k+1}-s_k)(s_{k+1}-s_k+1)}}{(\ell^{-1})_{s_{k+1}-s_k}}.
\end{aligned}$$

But by Lemma 5.1.2, this means that

$$\sum_{i=0}^{\infty} \ell^{ir+\frac{i(i-1)}{2}} \frac{S(B, B_{\oplus i})}{|\operatorname{Aut} B_{\oplus i}|} = \frac{1}{|\operatorname{Aut} B|} \cdot \sum_{i=0}^{\infty} t_i = \frac{1}{|\operatorname{Aut} B|} \cdot \prod_{i=1}^{\infty} (1 + \ell^{-i})^{-1},$$

so we conclude by Note 4.2.5. □

5.2. *The main results.* To conclude we mention two corollaries of Theorem 5.1.4, one trivial and one nontrivial.

Corollary 5.2.1. *If* $x \in (\mathbb{Z}_\ell)^\times$ *satisfies* $x \equiv 1 \pmod{\ell}$, *then*

$$\lim_{g\to\infty} \mu_{2g}^{(x)}(\{0\}) = \prod_{i=1}^{\infty} (1 + \ell^{-i})^{-1}.$$

Friedman and Washington [1989] proved the analog of Corollary 5.2.1 for the groups $\mathrm{GL}_n(\mathbb{Z}_\ell)$; namely, they proved that

$$\lim_{g\to\infty} \mu_{\mathrm{GL}_n(\mathbb{Z}_\ell)}(\{\phi \in \mathrm{GL}_n(\mathbb{Z}_\ell) \mid \operatorname{coker}(\mathrm{Id} - \phi) \simeq \{0\}\}) = \prod_{i=1}^{\infty} (1 - \ell^{-i}),$$

where $\mu_{\mathrm{GL}_n(\mathbb{Z}_\ell)}$ is the normalized Haar measure on $\mathrm{GL}_n(\mathbb{Z}_\ell)$. Friedman and Washington expressed the hope that the statistics of $\mathrm{GL}_n(\mathbb{Z}_\ell)$ (as $n \to \infty$) would match those of $\mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$ (as $2g \to \infty$). Achter [2006] proved that this was not the case. Corollary 5.2.1 calculates a particular statistic for $\mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$ (as $2g \to \infty$). It is noteworthy that the quantity in Corollary 5.2.1 matches Malle's conjectured probability that the class numbers of relative class groups are coprime to ℓ (when the base field of the extension has ℓth roots of unity but not ℓ^2th roots of unity; see Conjecture 2.1 in [Malle 2010]). Furthermore, Corollary 5.2.2 shows that the distribution on $\mathcal{G}$ proposed by Malle matches the distribution on $\mathcal{G}$ given by $\mu_{2g}^{(x)}$ for any $x \in (\mathbb{Z}_\ell)^\times$ with $x \equiv 1 \pmod{\ell}$ but $x \not\equiv 1 \pmod{\ell^2}$. Moreover, Corollary 5.2.2 also computes the distribution on $\mathcal{G}$ given by $\mu_{2g}^{(x)}$ when $x \equiv 2 \pmod{\ell}$ but $x \not\equiv 1 \pmod{\ell^3}$; this is analogous to the number field case when the base field has ℓ^2th roots of unity but not ℓ^3th roots of unity. The proof of Corollary 5.2.2 relies heavily on calculations from [Garton 2014a].

Corollary 5.2.2. *Suppose $r, s \in \mathbb{Z}^{\geq 0}$ with $r \geq s$. Furthermore, suppose that $x \in \mathbb{Z}_\ell$ and $\xi \in \mathbb{Z}^{>0}$ with $x \equiv 1 \pmod{\ell^\xi}$ but $x \not\equiv 1 \pmod{\ell^{\xi+1}}$. If $A \in \mathcal{G}(r, s)$, then*

$$\lim_{g\to\infty} \mu_{2g}^{(x)}(A) = \begin{cases} \ell^{\frac{r(r-1)}{2}} \cdot (\ell^{-1})_r \cdot \dfrac{\prod_{i=1}^{\infty}(1+\ell^{-i})^{-1}}{|\mathrm{Aut}\,A|} & \text{if } \xi = 1, \\ \ell^{\frac{r(r-1)}{2}+\frac{s(s-1)}{2}} \cdot (\ell^{-1})_s (\ell^{-1}; \ell^{-2})_{\lceil\frac{r-s}{2}\rceil} \cdot \dfrac{\prod_{i=1}^{\infty}(1+\ell^{-i})^{-1}}{|\mathrm{Aut}\,A|} & \text{if } \xi = 2. \end{cases}$$

Proof. Choose any $\rho \in \mathbb{Z}^{>0}$ with $\rho > \xi$ and $\ell^\rho > \exp A$. Then by Lemma 2.2.1 we know

$$\mu_{2g}^{(x)}(A) = \nu_{2g,\rho}^{\langle\xi\rangle}(A).$$

Now, we know from [Garton 2014a] that

$$\sum_{B\in\mathcal{G}(r)} \frac{S(A, B)}{|\mathrm{Aut}\,B|} = \frac{(\ell^{-1})_r}{|\mathrm{Aut}\,A|},$$

and, for any $i \in \{s, \ldots, r\}$,

$$\sum_{B\in\mathcal{G}(r,i)} \frac{S(A, B)}{|\mathrm{Aut}\,B|} = (-1)^{i-s} \cdot \ell^{\frac{s(s+1)}{2}-\frac{i(i+1)}{2}} \cdot \binom{r-s}{r-i}_{\ell^{-1}} \cdot \frac{(\ell^{-1})_s}{|\mathrm{Aut}\,A|}.$$

The $\xi = 1$ case follows from Note 3.2.2. For $\xi = 2$, use Note 3.2.2 again to see that

$$\begin{aligned}\sum_{B\in\mathscr{G}(r)} |\Lambda(B/\ell^2 B)|\cdot\frac{S(A,B)}{|\mathrm{Aut}\,B|} &= \sum_{i=s}^{r}\sum_{B\in\mathscr{G}(r,i)} |\Lambda(B/\ell^2 B)|\cdot\frac{S(A,B)}{|\mathrm{Aut}\,B|}\\ &= \sum_{i=s}^{r}(-1)^{i-s}\cdot\ell^{\frac{r(r-1)}{2}+\frac{s(s+1)}{2}-i}\cdot\binom{r-s}{r-i}_{\ell^{-1}}\cdot\frac{(\ell^{-1})_s}{|\mathrm{Aut}\,A|}\\ &= \frac{\ell^{\frac{r(r-1)}{2}+\frac{s(s+1)}{2}}(\ell^{-1})_s}{|\mathrm{Aut}\,A|}\cdot\sum_{i=s}^{r}(-1)^{i-s}\cdot\binom{r-s}{r-i}_{\ell^{-1}}\cdot\ell^{-i}.\end{aligned}$$

Letting $k = r - s$ and $q = 1/\ell$, we apply formula (1.10) from [Kupershmidt 2000], which is a corollary of formula (1.12), to obtain

$$\begin{aligned}\sum_{B\in\mathscr{G}(r)} |\Lambda(B/\ell^2 B)|\cdot\frac{S(A,B)}{|\mathrm{Aut}\,B|} &= \frac{\ell^{\frac{r(r-1)}{2}+\frac{s(s-1)}{2}}(\ell^{-1})_s}{|\mathrm{Aut}\,A|}\cdot\sum_{i=0}^{k}(-1)^i\binom{k}{i}_q q^i\\ &= \frac{\ell^{\frac{r(r-1)}{2}+\frac{s(s-1)}{2}}(\ell^{-1})_s}{|\mathrm{Aut}\,A|}\cdot(q;q^2)_{\lceil\frac{k}{2}\rceil},\end{aligned}$$

as desired. □

References

[Achter 2006] J. D. Achter, "The distribution of class groups of function fields", *J. Pure Appl. Algebra* **204**:2 (2006), 316–333. MR 2006h:11132 Zbl 1134.11042

[Achter 2008] J. D. Achter, "Results of Cohen–Lenstra type for quadratic function fields", pp. 1–7 in *Computational arithmetic geometry* (San Francisco, 2006), edited by K. E. Lauter and K. A. Ribet, Contemp. Math. **463**, Amer. Math. Soc., Providence, RI, 2008. MR 2009j:11101 Zbl 1166.11018

[Adam 2014a] M. Adam, "On the distribution of eigenspaces in classical groups over finite rings", *Linear Algebra Appl.* **443** (2014), 50–65. MR 3148893 Zbl 1292.20076

[Adam 2014b] M. Adam, *On the distribution of eigenspaces in classical groups over finite rings and the Cohen–Lenstra heuristic*, Ph.D. thesis, Technischen Universität Kaiserslautern, 2014, https://kluedo.ub.uni-kl.de/files/3732/Diss_Adam86.pdf.

[Adam and Malle 2015] M. Adam and G. Malle, "A class group heuristic based on the distribution of 1-eigenspaces in matrix groups", *J. Number Theory* **149** (2015), 225–235. MR 3296009

[Andrews 1976] G. E. Andrews, *The theory of partitions*, Encyclopedia of Mathematics and its Applications **2**, Addison-Wesley, Reading, MA, 1976. MR 58 #27738

[Cohen and Lenstra 1984] H. Cohen and H. W. Lenstra, Jr., "Heuristics on class groups of number fields", pp. 33–62 in *Number theory* (Noordwijkerhout, Netherlands, 1983), edited by H. Jager, Lecture Notes in Math. **1068**, Springer, Berlin, 1984. MR 85j:11144 Zbl 0558.12002

[Cohen and Martinet 1990] H. Cohen and J. Martinet, "Étude heuristique des groupes de classes des corps de nombres", *J. Reine Angew. Math.* **404** (1990), 39–76. MR 91k:11097 Zbl 0699.12016

[Ellenberg et al. 2009] J. S. Ellenberg, A. Venkatesh, and C. Westerland, "Homological stability for Hurwitz spaces and the Cohen–Lenstra conjecture over function fields", preprint, 2009. arXiv 0912.0325

[Friedman and Washington 1989] E. Friedman and L. C. Washington, “On the distribution of divisor class groups of curves over a finite field”, pp. 227–239 in *Théorie des nombres* (Université Laval, Quebec City, 1987), edited by J.-M. De Koninck and C. Levesque, de Gruyter, Berlin, 1989. MR 91e:11138 Zbl 0693.12013

[Garton 2012] D. Garton, *Random matrices and Cohen–Lenstra statistics for global fields with roots of unity*, Ph.D. thesis, University of Wisconsin, Madison, 2012, http://search.proquest.com/docview/1039288336.

[Garton 2014a] D. Garton, “Some finite abelian group theory and some q-series identities”, preprint, 2014. To appear in *Ann. Comb.* arXiv 1405.5824

[Garton 2014b] D. Garton, “A weighted Möbius function”, preprint, 2014. arXiv 1405.5818

[Hall 1934] P. Hall, “A Contribution to the Theory of Groups of Prime-Power Order”, *Proc. London Math. Soc.* **S2-36**:1 (1934), 29–95. MR 1575964 Zbl 59.0147.02

[Hall 1938] P. Hall, “A partition formula connected with Abelian groups”, *Comment. Math. Helv.* **11**:1 (1938), 126–129. MR 1509594 Zbl 0019.39705

[Hawkes et al. 1989] T. Hawkes, I. M. Isaacs, and M. Özaydin, “On the Möbius function of a finite group”, *Rocky Mountain J. Math.* **19**:4 (1989), 1003–1034. MR 90k:20046 Zbl 0708.20005

[Katz and Sarnak 1999] N. M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications **45**, American Mathematical Society, Providence, RI, 1999. MR 2000b:11070 Zbl 0958.11004

[Kupershmidt 2000] B. A. Kupershmidt, “q-Newton binomial: from Euler to Gauss”, *J. Nonlinear Math. Phys.* **7**:2 (2000), 244–262. MR 2002e:33024 Zbl 0955.33012

[Malle 2008] G. Malle, “Cohen–Lenstra heuristic and roots of unity”, *J. Number Theory* **128**:10 (2008), 2823–2835. MR 2009j:11179 Zbl 1225.11143

[Malle 2010] G. Malle, “On the distribution of class groups of number fields”, *Experiment. Math.* **19**:4 (2010), 465–474. MR 2011m:11224 Zbl 1297.11139

[Matchett Wood 2014] M. Matchett Wood, “The distribution of sandpile groups of random graphs”, preprint, 2014. arXiv 1402.5149

[McDonald 1976] B. R. McDonald, *Geometric algebra over local rings*, Pure and Applied Mathematics **36**, Marcel Dekker, New York, 1976. MR 57 #16198 Zbl 0346.20027

[Michael 2006] A. A. G. Michael, “Finite abelian actions on surfaces”, *Topology Appl.* **153**:14 (2006), 2591–2612. MR 2007c:57026 Zbl 1103.57023

[Rota 1964] G.-C. Rota, “On the foundations of combinatorial theory, I: Theory of Möbius functions”, *Z. Wahrscheinlichkeitstheorie und Verw. Gebiete* **2** (1964), 340–368. MR 30 #4688 Zbl 0121.02406

Communicated by Bjorn Poonen
Received 2014-05-26 Revised 2014-11-18 Accepted 2014-12-25

gartondw@pdx.edu
*Fariborz Maseeh Department of Mathematics and Statistics,
Portland State University, PO Box 751,
Portland, OR 97207-0751, United States*

ALGEBRA AND NUMBER THEORY 9:1 (2015)
dx.doi.org/10.2140/ant.2015.9.173

Local Beilinson–Tate operators

Amnon Yekutieli

In 1968 Tate introduced a new approach to residues on algebraic curves, based on a certain ring of operators that acts on the completion at a point of the function field of the curve. This approach was generalized to higher-dimensional algebraic varieties by Beilinson in 1980. However, Beilinson's paper had very few details, and his operator-theoretic construction remained cryptic for many years. Currently there is a renewed interest in the Beilinson–Tate approach to residues in higher dimensions.

Our paper presents a variant of Beilinson's operator-theoretic construction. We consider an n-dimensional topological local field K, and define a ring of operators $\mathrm{E}(K)$ that acts on K, which we call the ring of *local Beilinson–Tate operators*. Our definition is of an analytic nature (as opposed to the original geometric definition of Beilinson). We study various properties of the ring $\mathrm{E}(K)$. In particular we show that $\mathrm{E}(K)$ has an *n-dimensional cubical decomposition*, and this gives rise to a *residue functional* in the style of Beilinson and Tate. Presumably this residue functional coincides with the residue functional that we had constructed in 1992; but we leave this as a conjecture.

Introduction

Let X be a smooth curve over a perfect base field $\Bbbk$, with function field $\boldsymbol{k}(X)$, and let $x \in X$ be a closed point. The completion $K := \boldsymbol{k}(X)_{(x)}$ of $\boldsymbol{k}(X)$ at x is a local field. Tate [1968] introduced a ring $\mathrm{E}(K) \subset \mathrm{End}_{\Bbbk}(K)$, and two-sided ideals

MSC2010: primary 12J25; secondary 32A27, 13J05, 11R56, 46A13, 46H30.
Keywords: topological local fields, residues, Tate residue, Beilinson adeles.

$\mathrm{E}(K)_1, \mathrm{E}(K)_2 \subset \mathrm{E}(K)$. These new objects were defined using the valuation ring of K. Let us call the elements of $\mathrm{E}(K)$ *local Tate operators*. Heuristically, elements of $\mathrm{E}(K)_1$ are "compact operators", and elements of $\mathrm{E}(K)_2$ are "discrete operators". An operator $\phi \in \mathrm{End}_{\Bbbk}(K)$ is called *finite potent* if for some positive integer m the operator ϕ^m has finite rank. Tate proved that each $\phi \in \mathrm{E}(K)_1 \cap \mathrm{E}(K)_2$ is finite potent, and that $\mathrm{E}(K)_1 + \mathrm{E}(K)_2 = \mathrm{E}(K)$. Using some algebraic manipulations of the structure $(\mathrm{E}(K), \{\mathrm{E}(K)_j\})$, Tate constructed a *residue functional*

$$\mathrm{Res}^{\mathrm{T}}_{\boldsymbol{k}(X)/\Bbbk, x} : \Omega^1_{\boldsymbol{k}(X)/\Bbbk} \to \Bbbk.$$

Here $\Omega^1_{\boldsymbol{k}(X)/\Bbbk}$ is the module of Kähler 1-forms of $\boldsymbol{k}(X)$. Then he showed that his residue functional is the same as the one gotten by Laurent series expansion at x.

Finally, Tate gave a global variant of this residue functional, using the adeles of X instead of the completion $\boldsymbol{k}(X)_{(x)}$. He related the local and global residues, and proved that, when the curve X is proper, the sum of the local residues of any form $\alpha \in \Omega^1_{\boldsymbol{k}(X)/\Bbbk}$ is zero. The Tate construction gave a totally new way of looking at residues and duality for curves.

This circle of ideas was extended by Beilinson [1980] to higher dimensions in his extremely brief paper (that did not contain any proofs). Actually Beilinson's paper had in it several important innovations, related to a finite type $\Bbbk$-scheme X. By a chain of points in X of length n we mean a sequence $\xi = (x_0, \dots, x_n)$ of points such that x_i is a specialization of x_{i-1}. The chain ξ is *saturated* if each x_i is an immediate specialization of x_{i-1}. Beilinson said that:

(1) For a chain ξ of length n and a quasi-coherent sheaf $\mathcal{M}$ there is an $\mathcal{O}_X$-module $\mathcal{M}_\xi$, gotten by an n-fold zigzag inverse and direct limit process. When $\mathcal{M}$ is coherent and $n = 0$, this is the $\mathfrak{m}_{x_0}$-adic completion $\widehat{\mathcal{M}}_{x_0}$ of the stalk $\mathcal{M}_{x_0}$. (Let us call $\mathcal{M}_\xi$ the *Beilinson completion* of $\mathcal{M}$ along ξ.)

(2) For every $n \in \mathbb{N}$ and quasi-coherent sheaf $\mathcal{M}$, there is a sheaf $\mathbb{A}^n(\mathcal{M})$ called the *sheaf of adeles of degree n with values in* $\mathcal{M}$. It is a restricted product of the Beilinson completions $\mathcal{M}_\xi$ along length n chains. The sheaves $\mathbb{A}^n(\mathcal{M})$ assemble into a flasque resolution of $\mathcal{M}$. When X is a curve, $\mathbb{A}^1(\mathcal{O}_X)$ is the usual sheaf of adeles of X.

(3) For a saturated chain $\xi = (x_0, \dots, x_n)$, the completion $\boldsymbol{k}(x_0)_\xi$ of the residue field $\boldsymbol{k}(x_0)$ is a finite product of n-dimensional local fields.

(4) Let $A := \boldsymbol{k}(x_0)_\xi$ as in (3). Then there is a ring $\mathrm{E}(A) \subset \mathrm{End}_{\Bbbk}(A)$, with an *n-dimensional cubical decomposition* (see Definition 0.3 below), from which a Tate-style residue functional can be obtained.

(5) The higher adeles in (2) and the cubically decomposed ring of operators $\mathrm{E}(A)$ in (4) can be combined to prove a global residue theorem when X is proper.

The adelic resolution (2) was clarified, and all claims proved (for any noetherian scheme X), by Huber [1991]. The assertion about higher local fields (3) was proved in [Yekutieli 1992] (for any excellent noetherian scheme X); see Theorem 6.1.

For a long time assertions (4) and (5) were essentially neglected and remained cryptic. Very recently we heard about renewed interest in the work of Beilinson, mainly by Braunling, Groechenig and Wolfson [Braunling 2014a; 2014b; Braunling et al. 2014]. Item (4) above is discussed in [Braunling 2014a; 2014b]. A long-term goal of this team is to understand and make precise the global aspect (5) of Beilinson's construction, and then to apply this construction in various directions. Independently, Osipov [2005; 2007] has been studying higher adeles and higher local fields.

Discussions with Wolfson and Braunling led us to the realization that the topological aspects of higher local fields, and their implications on item (4) above, are not sufficiently understood. *The purpose of this paper is to present an analytic variant of the Beilinson–Tate construction for topological local fields and to study its properties.* Presumably our analytic construction agrees with the geometric construction of [Beilinson 1980; Braunling 2014b], and the resulting residue functional is the same as the residue functional from [Yekutieli 1992] — see Conjectures 0.9 and 0.12 below.

Throughout the introduction we keep the assumption that $\mathbb{k}$ is a perfect base field. An *n-dimensional topological local field* over $\mathbb{k}$ is — roughly speaking — a field extension K of $\mathbb{k}$, with a rank n valuation, and with a topology compatible with the valuation. An example is the field of iterated Laurent series $K = \mathbb{k}((t_2))((t_1))$, which is of dimension 2. See Definitions 3.1 and 3.8 for details. It is important to mention that a topological local field K of dimension $n \geq 2$ is not a topological ring, but only a *semi-topological ring*: multiplication is continuous only in one argument. We abbreviate "topological local field" to "TLF" and "semi-topological" to "ST". The theory of ST rings and modules is reviewed in Section 1.

A TLF K of dimension n has discrete valuation rings $\mathcal{O}_i(K)$ and residue fields $\boldsymbol{k}_i(K)$ for $i = 1, \dots, n$. They are related as follows: $\boldsymbol{k}_i(K)$ is the residue field of $\mathcal{O}_i(K)$ and the fraction field of $\mathcal{O}_{i+1}(K)$; and K is the fraction field of $\mathcal{O}_1(K)$. By a *system of liftings* for K we mean a sequence $\boldsymbol{\sigma} = (\sigma_1, \dots, \sigma_n)$, where each $\sigma_i : \boldsymbol{k}_i(K) \to \mathcal{O}_i(K)$ is a continuous lifting of the canonical surjection $\mathcal{O}_i(K) \twoheadrightarrow \boldsymbol{k}_i(K)$. Such systems of liftings always exist; see Proposition 3.19.

Consider a TLF K equipped with a system of liftings $\boldsymbol{\sigma}$. We define a ring of operators $\mathrm{E}_{\boldsymbol{\sigma}}(K) \subset \mathrm{End}_{\mathbb{k}}(K)$, and ideals $\mathrm{E}_{\boldsymbol{\sigma}}(K)_{i,j} \subset \mathrm{E}_{\boldsymbol{\sigma}}(K)$. Our definition (Definitions 4.5 and 4.14 in the body of the paper) is a modification of Beilinson's original definition from [Beilinson 1980]. But whereas Beilinson's original definition was geometric in nature (and pertained only to a TLF arising as a factor of a completion $\boldsymbol{k}(x_0)_\xi$), our definition is of an analytic nature. (We saw a similar definition in a private communication from Braunling.)

Here is our first main result. It is repeated as Corollary 4.22.

Theorem 0.1. *Let K be an n-dimensional TLF over $\mathbb{k}$, and let $\boldsymbol{\sigma}$ and $\boldsymbol{\sigma}'$ be two systems of liftings for K.*

(1) *There is equality $\mathrm{E}_{\boldsymbol{\sigma}}(K) = \mathrm{E}_{\boldsymbol{\sigma}'}(K)$ of these subrings of $\mathrm{End}_{\mathbb{k}}(K)$.*

(2) *For any $i = 1, \dots, n$ and $j = 1, 2$ there is equality $\mathrm{E}_{\boldsymbol{\sigma}}(K)_{i,j} = \mathrm{E}_{\boldsymbol{\sigma}'}(K)_{i,j}$ of these ideals of $\mathrm{E}_{\boldsymbol{\sigma}}(K)$.*

The theorem justifies the next definition.

Definition 0.2. Let K be an n-dimensional TLF over $\mathbb{k}$. Define $\mathrm{E}(K) := \mathrm{E}_{\boldsymbol{\sigma}}(K)$ and $\mathrm{E}(K)_{i,j} := \mathrm{E}_{\boldsymbol{\sigma}}(K)_{i,j}$, where $\boldsymbol{\sigma}$ is any system of liftings for K. We call $\mathrm{E}(K)$ the ring of *local Beilinson–Tate operators* on K.

Here is a definition from [Braunling 2014b], which distills Beilinson's definition [1980]. The notation we use is closer to the original notation of Tate.

Definition 0.3. Let A be a commutative $\mathbb{k}$-ring. An *n-dimensional cubically decomposed ring of operators on A* is data $(E, \{E_{i,j}\})$ consisting of:

- A $\mathbb{k}$-subring $E \subset \mathrm{End}_{\mathbb{k}}(A)$ containing A.
- Two-sided ideals $E_{i,j} \subset E$, indexed by $i \in \{1, \dots, n\}$ and $j \in \{1, 2\}$.

These are the conditions:

(i) For every $i \in \{1, \dots, n\}$ we have $E = E_{i,1} + E_{i,2}$.

(ii) Every operator $\phi \in \bigcap_{i=1}^{n} \bigcap_{j=1}^{2} E_{i,j}$ is finite potent.

The next result is Theorem 4.24(1) in the body of the paper.

Theorem 0.4. *Let K be an n-dimensional TLF over $\mathbb{k}$. The data*

$$(\mathrm{E}(K), \{\mathrm{E}(K)_{i,j}\})$$

of local Beilinson–Tate operators is an n-dimensional cubically decomposed ring of operators on K.

Let A be any commutative ST $\mathbb{k}$-ring. We can talk about the ring $\mathrm{End}_{\mathbb{k}}^{\mathrm{cont}}(A)$ of continuous $\mathbb{k}$-linear operators on A. There is also the ring $\mathcal{D}_{A/\mathbb{k}}^{\mathrm{cont}}$ of *continuous differential operators*; see the review in Section 2. There are inclusions of $\mathbb{k}$-rings

$$A \subset \mathcal{D}_{A/\mathbb{k}}^{\mathrm{cont}} \subset \mathrm{End}_{\mathbb{k}}^{\mathrm{cont}}(A) \subset \mathrm{End}_{\mathbb{k}}(A).$$

Theorem 0.5. *Let K be an n-dimensional TLF over $\mathbb{k}$. The ring $\mathrm{E}(K)$ of local Beilinson–Tate operators satisfies*

$$\mathcal{D}_{K/\mathbb{k}}^{\mathrm{cont}} \subset \mathrm{E}(K) \subset \mathrm{End}_{\mathbb{k}}^{\mathrm{cont}}(K).$$

This is repeated as Theorem 4.24(2). Actually Theorem 0.5 is used in the proofs of Theorems 0.1 and 0.4.

In [Yekutieli 1992] we developed a theory of residues for TLFs. For every n-dimensional TLF K, we consider the module of top-degree separated differential forms $\Omega^{n,\mathrm{sep}}_{K/\Bbbk}$. It is a rank 1 free K-module, and it has the fine K-module topology. This means that, for any nonzero form $\alpha \in \Omega^{n,\mathrm{sep}}_{K/\Bbbk}$, the corresponding homomorphism $K \to \Omega^{n,\mathrm{sep}}_{K/\Bbbk}$ is a topological isomorphism. (We will say more about the fine topology later in the introduction.) The residue functional

$$\mathrm{Res}^{\mathrm{TLF}}_{K/\Bbbk} : \Omega^{n,\mathrm{sep}}_{K/\Bbbk} \to \Bbbk \tag{0-6}$$

constructed in [Yekutieli 1992] is a continuous $\Bbbk$-linear homomorphism, enjoying several important properties. See Theorem 5.4 for details.

Beilinson [1980] claimed that an n-dimensional cubically decomposed ring of operators $(E, \{E_{i,j}\})$ on a commutative $\Bbbk$-ring A determines a residue functional

$$\mathrm{Res}^{\mathrm{BT}}_{A/\Bbbk;E} : \Omega^{n}_{A/\Bbbk} \to \Bbbk. \tag{0-7}$$

For $n = 1$ this is the original abstract residue of [Tate 1968]. For $n \geq 2$ this was worked out in [Braunling 2014b], using Lie algebra homology and Hochschild homology.

Now consider an n-dimensional TLF K over $\Bbbk$. By Theorem 0.4, K is equipped with an n-dimensional cubically decomposed ring of operators $\mathrm{E}(K)$; and we let

$$\mathrm{Res}^{\mathrm{BT}}_{K/\Bbbk} : \Omega^{n}_{K/\Bbbk} \to \Bbbk \tag{0-8}$$

denote the corresponding residue functional.

Let A be any commutative ST $\Bbbk$-ring. For any q the module of Kähler differentials $\Omega^{q}_{A/\Bbbk}$ has a canonical topology (this is recalled at the end of Section 2). There is a canonical continuous surjection $\Omega^{q}_{A/\Bbbk} \twoheadrightarrow \Omega^{q,\mathrm{sep}}_{A/\Bbbk}$ to the separated module of differentials. Often (e.g., when $A = K$ is a TLF of dimension at least 1 and $\mathrm{char}(\Bbbk) = 0$) the kernel of this canonical surjection is very big.

Conjecture 0.9. Let K be an n-dimensional TLF over $\Bbbk$. The following diagram of $\Bbbk$-linear homomorphisms is commutative:

$$\begin{tikzcd}
\Omega^{n}_{K/\Bbbk} \arrow[r, two heads, "\mathrm{can}"] \arrow[dr, "\mathrm{Res}^{\mathrm{BT}}_{K/\Bbbk}"'] & \Omega^{n,\mathrm{sep}}_{K/\Bbbk} \arrow[d, "\mathrm{Res}^{\mathrm{TLF}}_{K/\Bbbk}"] \\
 & \Bbbk
\end{tikzcd}$$

When $n \leq 1$ we know the conjecture is true. For $n = 0$ it is trivial, and for $n = 1$ it is proved in [Tate 1968]. In order to help in proving this conjecture in higher dimensions we have included a review of the residue functional $\mathrm{Res}^{\mathrm{TLF}}_{K/\Bbbk}$ and its properties. This is Section 5 of the paper. We also state Conjecture 5.7, which is closely related to Conjecture 0.9.

Suppose A is a finite product of n-dimensional TLFs over $\Bbbk$; say $A = \prod_{l=1}^{r} K_l$. Let us define $\mathrm{E}(A) := \prod_l \mathrm{E}(K_l)$ and $\mathrm{E}(A)_{i,j} := \prod_l \mathrm{E}(K_l)_{i,j}$. It is not hard to see that the data

$$(\mathrm{E}(A), \{\mathrm{E}(A)_{i,j}\}) \tag{0-10}$$

is an n-dimensional cubically decomposed ring of operators on A.

Let X be a finite type $\Bbbk$-scheme, let $\xi = (x_0, \dots, x_n)$ be a saturated chain of points in X such that x_n is a closed point, and let $K := \boldsymbol{k}(x_0)$. According to [Yekutieli 1992] (see Theorem 6.1), the Beilinson completion $A := K_\xi$ is a finite product of n-dimensional TLFs over $\Bbbk$. Beilinson's construction [1980], worked out in detail in [Braunling 2014b], gives rise to an n-dimensional cubically decomposed ring of operators

$$(\mathrm{E}_{X,\xi}(K), \{\mathrm{E}_{X,\xi}(K)_{i,j}\}) \tag{0-11}$$

on K_ξ. (This is our notation.) Note that by definition both $\mathrm{E}_{X,\xi}(K)$ and $\mathrm{E}(K_\xi)$ are subrings of $\mathrm{End}_{\Bbbk}(K_\xi)$.

Conjecture 0.12. Let X be a finite type $\Bbbk$-scheme, let $\xi = (x_0, \dots, x_n)$ be a saturated chain of points in X such that x_n is a closed point, and let $K := \boldsymbol{k}(x_0)$. Then the n-dimensional cubically decomposed rings of operators $\mathrm{E}(K_\xi)$ and $\mathrm{E}_{X,\xi}(K)$ are equal.

To help in proving this conjecture we have included Section 6, in which we recall some facts from [Yekutieli 1992] about the Beilinson completions $\boldsymbol{k}(x_0)_\xi$, and provide our interpretation of the geometric definition of $\mathrm{E}_{X,\xi}(K)$. In Remark 6.11 we explain the geometric significance of these conjectures.

To finish the introduction we wish to discuss a technical result that is used in the proof of Theorem 0.1. This result is of a very general nature, and could possibly find other applications.

We work in the category $\mathsf{STRing_c}\,\Bbbk$ of commutative ST $\Bbbk$-rings. The morphisms are continuous $\Bbbk$-ring homomorphisms. Let $A \in \mathsf{STRing_c}\,\Bbbk$. The *fine A-module topology* on an A-module M is the finest topology that makes M into a ST A-module. For example, if $M \cong A^r$ for $r \in \mathbb{N}$, then the product topology is the fine A-module topology on M. For more see Section 1.

Consider an artinian local ring A in $\mathsf{STRing_c}\,\Bbbk$, with residue field K. Give K the fine A-module topology relative to the canonical surjection $\pi : A \to K$; so π becomes a homomorphism in $\mathsf{STRing_c}\,\Bbbk$. Suppose $\sigma : K \to A$ is a homomorphism in $\mathsf{STRing_c}\,\Bbbk$ such that $\pi \circ \sigma$ is the identity of K. We call σ a lifting of K in $\mathsf{STRing_c}\,\Bbbk$. The lifting σ is called a *precise lifting* if the topology on A coincides with the fine K-module topology on it (via σ). The ring A is called a *precise artinian local* *ring* if it admits some precise lifting. There are examples of artinian local rings in $\mathsf{STRing_c}\,\Bbbk$ that are not precise, like in Example 1.27. However, the rings that we are interested in (such as quotients of $\mathcal{O}_1(K)$ for a TLF K — see Lemma 3.14, and Beilinson completions of artinian local rings — see Example 1.26) are precise. The reader might wonder if all continuous liftings $\sigma : K \to A$ for a precise artinian local ring A are precise. This is answered affirmatively in Corollary 0.14 below. It is a consequence of the following technical result:

Given a lifting $\sigma : K \to A$ and an A-module M, we denote by $\operatorname{rest}_\sigma(M)$ the K-module whose underlying $\Bbbk$-module is M, and K acts via σ.

Theorem 0.13. *Let A be a precise artinian local ring in* $\mathsf{STRing_c}\,\Bbbk$, *with residue field K. Put on K the fine A-module topology. Let $\sigma_1, \sigma_2 : K \to A$ be liftings in* $\mathsf{STRing_c}\,\Bbbk$ *of the canonical surjection $\pi : A \to K$, and assume that σ_2 is a precise lifting.*

Let M_1 and M_2 be finite A-modules, and let $\phi : M_1 \to M_2$ be an A-linear homomorphism. For $l = 1, 2$ choose K-linear isomorphisms $\psi_l : K^{r_l} \xrightarrow{\simeq} \operatorname{rest}_{\sigma_l}(M_l)$. Let $\bar{\phi} \in \operatorname{Mat}_{r_2\times r_1}(\operatorname{End}_\Bbbk(K))$ be the matrix representing the $\Bbbk$-linear homomorphism

$$\psi_2^{-1} \circ \phi \circ \psi_1 : K^{r_1} \to K^{r_2}.$$

Then:

(1) *The matrix $\bar{\phi}$ belongs to* $\operatorname{Mat}_{r_2\times r_1}(\mathcal{D}^{\text{cont}}_{K/\Bbbk})$.

(2) *Assume that $M_1 = M_2$ and ϕ is the identity automorphism. Write $r := r_1$. Then the matrix $\bar{\phi}$ belongs to* $\operatorname{GL}_r(\mathcal{D}^{\text{cont}}_{K/\Bbbk})$.

This is repeated as Theorem 2.8 in the body of the paper. From it we deduce the next result, which is Corollary 2.12.

Corollary 0.14. *Let A be a precise artinian local ring in* $\mathsf{STRing_c}\,\Bbbk$, *with residue field K. Give K the fine A-module topology. Then any lifting $\sigma : K \to A$ in* $\mathsf{STRing_c}\,\Bbbk$ *is a precise lifting.*

1. Semi-topological rings and modules

We begin with a general discussion of various categories of rings. The notation introduced here will make some of our more delicate definitions possible.

Let Ring be the category of rings (not necessarily commutative). The morphisms are unit-preserving ring homomorphisms. Inside it there is the full subcategory $\mathsf{Ring_c}$ of commutative rings.

Now let us fix a nonzero commutative base ring $\Bbbk$. A ring homomorphism $f : \Bbbk \to A$ is called *central* if $f(\Bbbk)$ is contained in the center of A. In this case we call A a *central* $\Bbbk$*-ring*. (A more common name for A is an associative unital $\Bbbk$-algebra.) The central $\Bbbk$-rings form a category $\mathsf{Ring}\,\Bbbk$, in which a morphism is a ring homomorphism $A \to B$ that respects the given central homomorphisms $\Bbbk \to A$ and $\Bbbk \to B$. Inside $\mathsf{Ring}\,\Bbbk$ there is the full subcategory $\mathsf{Ring_c}\,\Bbbk$ of commutative $\Bbbk$-rings. Of course, if $\Bbbk = \mathbb{Z}$ then $\mathsf{Ring}\,\mathbb{Z} = \mathsf{Ring}$.

Let A be a local ring in $\mathsf{Ring_c}\,\Bbbk$, with maximal ideal $\mathfrak{m}$ and residue field $K = A/\mathfrak{m}$. Recall that A is called a complete local ring if the canonical homomorphism $A \to \lim_{\leftarrow i} A/\mathfrak{m}^i$ is bijective. The canonical surjection $\pi : A \twoheadrightarrow K$ makes K into an object of $\mathsf{Ring_c}\,\Bbbk$. A *lifting* of the canonical surjection $\pi : A \twoheadrightarrow K$ in $\mathsf{Ring_c}\,\Bbbk$, or a *coefficient field* for A in $\mathsf{Ring_c}\,\Bbbk$, is a homomorphism $\sigma : K \to A$ in $\mathsf{Ring_c}\,\Bbbk$ such that the composition $\pi \circ \sigma$ is the identity of K.

The next result is part of the Cohen structure theorem. We will repeat its proof, because the proof itself will feature in some of our constructions.

Theorem 1.1 (Cohen). *Assume $\Bbbk$ is a perfect field. Let A be a complete local ring in $\mathsf{Ring_c}\,\Bbbk$, with residue field K. Then there exists a lifting $\sigma : K \to A$ in $\mathsf{Ring_c}\,\Bbbk$ of the canonical surjection $\pi : A \twoheadrightarrow K$. Moreover, if $\Bbbk \to K$ is finite, then this lifting σ is unique.*

Proof. Consider the K-module $\Omega^1_{K/\Bbbk}$ of Kähler differential forms. Choose a collection $\{b_x\}_{x \in X}$ of elements of K so that the collection of forms $\{\mathrm{d}(b_x)\}_{x \in X}$ is a basis of the K-module $\Omega^1_{K/\Bbbk}$. According to [Matsumura 1986, Theorems 26.5 and 26.8], the collection of elements $\{b_x\}_{x \in X}$ is algebraically independent over $\Bbbk$, and K is formally étale over the subfield $\Bbbk(\{b_x\})$ generated by this collection. (Actually, if either $\operatorname{char} \Bbbk = 0$ or K is finitely generated over $\Bbbk$, then the field K is separable algebraic over $\Bbbk(\{b_x\})$. See [Matsumura 1986, Theorem 26.2].)

For any $x \in X$ choose an arbitrary lifting $\sigma_{\mathrm{b}}(b_x) \in A$ of the element b_x; thus $\pi(\sigma_{\mathrm{b}}(b_x)) = b_x$. Since the collection $\{b_x\}_{x \in X}$ is algebraically independent over $\Bbbk$, the subring $\Bbbk[\{b_x\}]$ of K is a polynomial ring. Therefore the function $\sigma_{\mathrm{b}} : X \to A$ extends uniquely to a homomorphism $\sigma_{\mathrm{p}} : \Bbbk[\{b_x\}] \to A$ in $\mathsf{Ring_c}\,\Bbbk$. Because A is a local ring, for any nonzero element $b \in \Bbbk[\{b_x\}]$ its lift $\sigma_{\mathrm{p}}(b)$ is invertible in A. Thus σ_{p} extends uniquely to a homomorphism $\sigma_{\mathrm{r}} : \Bbbk(\{b_x\}) \to A$. (The subscripts b, p, r refer to “basis”, “polynomial” and “rational”.)

Let $A_i := A/\mathfrak{m}^{i+1}$, with surjection $\pi_i : A \to A_i$. Because $\Bbbk(\{b_x\}) \to K$ is formally étale, the homomorphism $\pi_i \circ \sigma_{\mathrm{r}} : \Bbbk(\{b_x\}) \to A_i$ extends uniquely to a homomorphism $\sigma_i : K \to A_i$, which lifts $A_i \twoheadrightarrow K = A_0$. We get an inverse system of liftings, and thus a lifting $\sigma : K \to \lim_{\leftarrow i} A/\mathfrak{m}^i = A$, $\sigma := \lim_{\leftarrow i} \sigma_i$. The restriction of σ to $\Bbbk(\{b_x\})$ equals σ_{r}, and in particular we see that σ is a homomorphism in $\mathsf{Ring_c}\,\Bbbk$.

If $\Bbbk \to K$ is finite then $X = \varnothing$, and hence σ is unique. □

Remark 1.2. Liftings exist whenever they can exist, namely if and only if A contains a field. This is called the equal characteristics case. Indeed, if A contains a field then it contains some perfect field $\Bbbk$ (e.g., $\mathbb{Q}$ or F_p). Now Theorem 1.1 can be applied. Note that, if the residue field K contains $\mathbb{Q}$, then A also contains $\mathbb{Q}$.

The complication arises when the residue field $K = A/\mathfrak{m}$ contains F_p, but A does not contain it (i.e., $p \neq 0$ in A). This is called the mixed characteristics case. In this case the notion of lifting has to be modified. First the base ring $\Bbbk$ is replaced by two rings: a perfect field $\Bbbk$ of characteristic p, and a complete DVR $\widetilde{\Bbbk}$ whose maximal ideal is generated by p and whose residue field is $\Bbbk$. The ring $\widetilde{\Bbbk}$ is called the ring of Witt vectors of $\Bbbk$. (e.g., when $\Bbbk = \mathbb{F}_p$, its ring of Witt vectors is $\widetilde{\Bbbk} = \widehat{\mathbb{Z}}_{(p)}$, the p-adic integers.) A homomorphism $\Bbbk \to K$ lifts canonically to a homomorphism $\widetilde{\Bbbk} \to A$. Next there is a complete DVR $\widetilde{K}$, whose maximal ideal is generated by p and whose residue field is K, and $\widetilde{\Bbbk} \to \widetilde{K}$ is p-adically formally smooth. Therefore there exists a lifting $\sigma : \widetilde{K} \to A$ over $\widetilde{\Bbbk}$. Moreover, all such liftings are controlled by $\Omega^1_{K/\Bbbk}$, just as in the proof of Theorem 1.1.

In this paper we shall deal exclusively with the equal characteristics case.

We are going to look at a more subtle lifting situation, involving topologies on A and K.

We consider the base ring $\Bbbk$ as a topological ring with the discrete topology. Recall that a topological $\Bbbk$-module is a $\Bbbk$-module M endowed with a topology such that addition and multiplication are continuous functions $M \times M \to M$ and $\Bbbk \times M \to M$ respectively. We say that the topology on M is *$\Bbbk$-linear*, and that M is a *linearly topologized $\Bbbk$-module*, if the element $0 \in M$ has a basis of open neighborhoods consisting of open $\Bbbk$-submodules.

In order to define a $\Bbbk$-linear topology on a $\Bbbk$-module M, all we have to do is to provide a collection $\{U_i\}_{i\in I}$ of $\Bbbk$-submodules of M that is cofiltered under inclusion; namely, for any $i, j \in I$, there exists $k \in I$ such that $U_k \subset U_i \cap U_j$. The resulting topology on M, in which the collection $\{U_i\}_{i\in I}$ is a basis of open neighborhoods of $0 \in M$, is called the $\Bbbk$-linear topology generated by this collection.

Definition 1.3. Let $M_1, \dots, M_p$, N be linearly topologized $\Bbbk$-modules, and let $\mu : \prod_{i=1}^{p} M_i \to N$ be a $\Bbbk$-multilinear function. We say that μ is *semi-continuous* if, for every $\boldsymbol{m} = (m_1, \dots, m_p) \in \prod_{i=1}^{p} M_i$ and every $i \in \{1, \dots, p\}$, the homomorphism

$$\mu_{\boldsymbol{m},i} : M_i \to N, \quad \mu_{\boldsymbol{m},i}(m'_i) := \mu(m_1, \dots, m_{i-1}, m'_i, m_{i+1}, \dots, m_p),$$

is continuous.

Definition 1.4 [Yekutieli 1992]. A *semi-topological $\Bbbk$-ring* is a $\Bbbk$-ring A with a $\Bbbk$-linear topology on it (so the underlying $\Bbbk$-module of A is a linearly topologized $\Bbbk$-module) such that multiplication $\mu : A \times A \to A$ is a semi-continuous bilinear function.

The semi-topological $\Bbbk$-rings form a category $\mathsf{STRing}\,\Bbbk$, in which the morphisms are the continuous $\Bbbk$-ring homomorphisms.

We use the abbreviation "ST" for "semi-topological". The ring $\Bbbk$ with its discrete topology is the initial object of $\mathsf{STRing}\,\Bbbk$. Inside $\mathsf{STRing}\,\Bbbk$ there is the full subcategory $\mathsf{STRing_c}\,\Bbbk$ of commutative ST $\Bbbk$-rings.

Example 1.5. Suppose A is a commutative $\Bbbk$-ring, and $\mathfrak{a} \subset A$ is an ideal. Give A the $\mathfrak{a}$-adic topology. Then A is a ST $\Bbbk$-ring. (The ring A is actually a topological ring, because multiplication $A \times A \to A$ is continuous.) The ring of Laurent series $A((t))$ — see Definition 1.17 — is a ST $\Bbbk$-ring, but it is usually not a topological ring.

Definition 1.6. Let A be a ST $\Bbbk$-ring. A *left ST A-module* is a left A-module M endowed with a $\Bbbk$-linear topology on it (so M is a linearly topologized $\Bbbk$-module) such that the bilinear function $\mu : A \times M \to M$, $\mu(a, m) := a \cdot m$, is semi-continuous.

The ST left A-modules form a category, in which the morphisms are the continuous A-linear homomorphisms. We denote this category by $\mathsf{STMod}\,A$.

There is a similar right module version, denoted by $\mathsf{STMod}\,A^{\mathrm{op}}$.

Remark 1.7. If A is a discrete ST $\Bbbk$-ring (e.g., $A = \Bbbk$), then a ST A-module M is also a topological A-module, because the multiplication function $A \times M \to M$ is continuous. We will usually ignore this fact.

Proposition 1.8. *Let A be a ST $\Bbbk$-ring. The category* $\mathsf{STMod}\,A$ *has these properties*:

(1) *It is a $\Bbbk$-linear additive category.*

(2) *It has limits and colimits* (*of arbitrary cardinality*)*. In particular there are coproducts*, *products*, *kernels and cokernels.*

Proof. This is all essentially in [Yekutieli 1992, Section 1.2]. The fact that $\mathsf{STMod}\,A$ is $\Bbbk$-linear is clear.

Given a collection $\{M_x\}_{x \in X}$ of ST A-modules, indexed by a set X, let $M := \bigoplus_{x \in X} M_x$ be the direct sum in $\mathsf{Mod}\,A$. Given any collection $\{U_x\}_{x \in X}$, where $U_x \subset M_x$ is an open $\Bbbk$-submodule, let $U := \bigoplus_{x \in X} U_x$, which is a $\Bbbk$-submodule of M. Give M the $\Bbbk$-linear topology generated by these $\Bbbk$-submodules U. This makes M into a ST A-module, and together with the embeddings $M_x \hookrightarrow M$ it becomes a coproduct in $\mathsf{STMod}\,A$. Likewise, the product $\prod_{x \in X} M_x$ in $\mathsf{Mod}\,A$, with the product topology, becomes a product in $\mathsf{STMod}\,A$.

Let $\phi : M \to N$ be a homomorphism in $\mathsf{STMod}\,A$. Then $\operatorname{Ker}(\phi)$, with the topology induced on it from M (the subspace topology), is a kernel of ϕ. The module $\operatorname{Coker}(\phi)$, with the topology induced on it from N (the quotient topology), is a cokernel of ϕ.

Now that we have coproducts, products, kernels and cokernels, any limit and colimit can be produced in $\mathsf{STMod}\,A$. □

Let $A \in \mathsf{STRing}\,\Bbbk$. We often use the notation $\mathrm{Hom}_A^{\mathrm{cont}}(M, N)$ to denote the $\Bbbk$-module of continuous A-linear homomorphism between two ST left A-modules M and N. This is just another way to refer to the $\Bbbk$-module $\mathrm{Hom}_{\mathsf{STMod}\,A}(M, N)$.

Remark 1.9. The concept of ST module is very close to the concept of *smooth representation* from the theory of representations of topological groups. Perhaps some of our work here can be used in that area.

Definition 1.10. Let A be a ST ring, and let M be a left A-module. The *fine A-module topology* on M is the finest linear topology on M that makes it into a ST A-module.

It is not clear at first whether such a topology exists; but it does — see [Yekutieli 1992, Section 1.2]. The fine topology can be characterized as follows: a ST A-module M has the fine A-module topology if and only if, for any $N \in \mathsf{STMod}\,A$, the canonical function

$$\mathrm{Hom}_A^{\mathrm{cont}}(M, N) \to \mathrm{Hom}_A(M, N)$$

is bijective [Yekutieli 1992, Proposition 1.2.4]. (So we get a left adjoint to the forgetful functor $\mathsf{STMod}\,A \to \mathsf{Mod}\,A$.)

The fine A-module topology can be described quite explicitly. First consider a free module $F = \bigoplus_{x \in X} A$. The direct sum (i.e., coproduct) topology on it is the fine topology. Now take any A-module M, and let $F \twoheadrightarrow M$ be some A-linear surjection from a free module F. Then the quotient topology on M coincides with its fine topology.

Definition 1.11. Let $\phi : M \to N$ be a homomorphism in $\mathsf{STMod}\,A$.

(1) ϕ is called a *strict monomorphism* if it is injective and the topology on M equals the subspace topology on it induced by ϕ and N.

(2) ϕ is called a *strict epimorphism* if it is surjective and the topology on N equals the quotient topology on it induced by ϕ and M.

Example 1.12. Let $\phi : M \to N$ be a homomorphism in $\mathsf{STMod}\,A$, and assume both modules have the fine A-module topologies. If ϕ is a surjection, then it is a strict epimorphism. If $\phi : M \to N$ a split injection in $\mathsf{STMod}\,A$, then it is a strict monomorphism.

Definition 1.13. Let $f : A \to B$ be a homomorphism in $\mathsf{STRing}\,\Bbbk$. We say that f is a *strict monomorphism* (resp. *strict epimorphism*) in $\mathsf{STRing}\,\Bbbk$ if it is so in $\mathsf{STMod}\,\Bbbk$.

Definition 1.14. Let $A \in \mathsf{STRing}_{\mathrm{c}}\,\Bbbk$, let $f : A \to B$ be a homomorphism in $\mathsf{Ring}_{\mathrm{c}}\,\Bbbk$, and let $M \in \mathsf{Mod}\,B$. We view M as an A-module via f. The fine A-module topology on M is called the *fine (A, f)-module topology*.

Lemma 1.15. *In the situation of Definition 1.14*:

(1) *The ring B, with the fine (A, f)-module topology, becomes an object of* $\mathsf{STRing_c}\,\Bbbk$; *and $f : A \to B$ becomes a morphism in* $\mathsf{STRing_c}\,\Bbbk$.

(2) *Give B the fine (A, f)-module topology. Then the fine B-module topology on M coincides with the fine (A, f)-module topology on it. Therefore M, endowed with the fine (A, f)-module topology, is an object of* $\mathsf{STMod}\,B$.

Proof. This is easy using [Yekutieli 1992, Proposition 1.2.4]. □

Lemma 1.16. *Let $\{B_i\}_{i \in \mathbb{N}}$ be an inverse system in* $\mathsf{STRing}\,\Bbbk$. *The ring $B := \varprojlim_i B_i$, with its inverse limit topology* (see Proposition 1.8(2)), *is a ST $\Bbbk$-ring.*

Proof. This follows almost immediately from the definitions. □

Here is the most important construction of ST rings in our context. This is [Yekutieli 1992, Definition 1.3.3]. Lemmas 1.15 and 1.16 justify it.

Definition 1.17. Let A be a commutative ST $\Bbbk$-ring.

(1) Let t be a variable.

  (a) For any $i \in \mathbb{N}$ put on the truncated polynomial ring $A[t]/(t^{i+1})$ the fine A-module topology. This makes $A[t]/(t^{i+1})$ a ST $\Bbbk$-ring.

  (b) Give the ring of formal power series $A[[t]] := \lim_{\leftarrow i} A[t]/(t^{i+1})$ the inverse limit topology. In this way $A[[t]]$ is a ST $\Bbbk$-ring.

  (c) Give the ring of formal Laurent series $A((t)) := A[[t]][t^{-1}]$ the fine $A[[t]]$-module topology. In this way $A((t))$ is a ST $\Bbbk$-ring.

(2) Let $\boldsymbol{t} = (t_1, \dots, t_n)$ be a sequence of variables. The *ring of iterated Laurent series*

$$A((\boldsymbol{t})) = A((t_1, \dots, t_n))$$

is the commutative ST $\Bbbk$-ring defined recursively on n by

$$A((t_1, \dots, t_n)) := A((t_2, \dots, t_n))((t_1)),$$

using part (1).

Note that as ST A-modules there is an isomorphism

$$A((t)) = \Bigl(\prod_{i \geq 0} A \cdot t^i\Bigr) \oplus \Bigl(\bigoplus_{i<0} A \cdot t^i\Bigr) \cong \Bigl(\prod_{i \in \mathbb{N}} A\Bigr) \oplus \Bigl(\bigoplus_{i \in \mathbb{N}} A\Bigr).$$

Remark 1.18. Strangely, for $n \geq 2$ (and when A is nonzero), the ring $B := A((t_1, \dots, t_n))$ is *not topological*; namely, multiplication is not a continuous function $B \times B \to B$. This is the reason for introducing the semi-topological apparatus.

Furthermore, the topology on B is *not metrizable*. Still, B is *complete*, in the sense that the canonical homomorphism $B \to \lim_{\leftarrow U} B/U$, where U runs over all open $\Bbbk$-submodules of B, is bijective.

Exercise 1.19. Let $K := \Bbbk((\boldsymbol{t}))$, the ring of Laurent series in the sequence of variables $\boldsymbol{t} = (t_1, \dots, t_n)$, with its topology from Definition 1.17. Let $\mathrm{F}(\mathbb{Z}^n, \Bbbk)$ be the set of functions $a : \mathbb{Z}^n \to \Bbbk$, written in subscript notation; namely for $\boldsymbol{i} = (i_1, \dots, i_n) \in \mathbb{Z}^n$ the value of a is $a_{\boldsymbol{i}} \in \Bbbk$. The notation for monomials in $\boldsymbol{t}$ is $\boldsymbol{t}^{\boldsymbol{i}} := t_1^{i_1} \cdots t_n^{i_n}$. We say that a collection $\{a_{\boldsymbol{i}} \boldsymbol{t}^{\boldsymbol{i}}\}_{\boldsymbol{i} \in \mathbb{Z}^n}$ of elements of K is a *Cauchy collection* if, for every open $\Bbbk$-submodule $U \subset K$, there is a finite subset $I \subset \mathbb{Z}^n$ such that $a_{\boldsymbol{i}} \boldsymbol{t}^{\boldsymbol{i}} \in U$ for all $\boldsymbol{i} \notin I$. A function $a \in \mathrm{F}(\mathbb{Z}^n, \Bbbk)$ is called Cauchy if the collection $\{a_{\boldsymbol{i}} \boldsymbol{t}^{\boldsymbol{i}}\}_{\boldsymbol{i} \in \mathbb{Z}^n}$ is Cauchy. The set of Cauchy functions is denoted by $\mathrm{F_c}(\mathbb{Z}^n, \Bbbk)$. The exercise is to show that for any $a \in \mathrm{F_c}(\mathbb{Z}^n, \Bbbk)$ the series $\sum_{\boldsymbol{i} \in \mathbb{Z}^n} a_{\boldsymbol{i}} \boldsymbol{t}^{\boldsymbol{i}}$ converges in K, and that the resulting function $\mathrm{F_c}(\mathbb{Z}^n, \Bbbk) \to K$ is a $\Bbbk$-linear bijection. (For a slightly more general assertion see the end of [Yekutieli 1992, Section 1.3].)

Definition 1.20. Let $f : A \to B$ be a homomorphism in $\mathsf{STRing}\, \Bbbk$. Given M in $\mathsf{STMod}\, B$, we denote by $\mathrm{rest}_f(M)$ the ST A-module whose underlying ST $\Bbbk$-module is M, and A acts via f.

In this way we get a functor

$$\mathrm{rest}_f : \mathsf{STMod}\, B \to \mathsf{STMod}\, A.$$

We now return to liftings.

Definition 1.21. Let A be a local ring in $\mathsf{STRing_c}\, \Bbbk$, with residue field K. We put on K the fine A-module topology, so that the canonical surjection $\pi : A \twoheadrightarrow K$ is a morphism in $\mathsf{STRing_c}\, \Bbbk$. A *lifting of* K in $\mathsf{STRing_c}\, \Bbbk$ is a homomorphism $\sigma : K \to A$ in $\mathsf{STRing_c}\, \Bbbk$ such that the composition $\pi \circ \sigma$ is the identity of K.

The important thing to remember is that $\sigma : K \to A$ has to be continuous.

Example 1.22. Assume $\Bbbk$ is a field of characteristic 0. Let $K := \Bbbk((t_2))$ and $A := K[[t_1]]$, with topologies from Definition 1.17. So we are in the situation of Definition 1.21. Consider the lifting $\sigma : K \to A$ from Example 3.13. If at least one of the elements c_i is nonzero, the lifting σ is not continuous.

Remark 1.23. Let A be a local ring in $\mathsf{STRing_c}\, \Bbbk$, with maximal ideal $\mathfrak{m}$. We do not assume any relation between the given topology of A and its $\mathfrak{m}$-adic topology. For instance, A could have the discrete topology, which is finer than any other topology.

On the other hand, in Example 1.22 above, where $A = \Bbbk((t_2))[[t_1]]$ and $\mathfrak{m} = (t_1)$, the $\mathfrak{m}$-adic topology on A is finer than the given topology on it (since the discrete topology on $K = \Bbbk((t_2))$ is finer than its t_2-adic topology).

The next definition is a generalization of [Yekutieli 1992, Definition 2.2.1].

Definition 1.24. Let A be an artinian local ring in $\mathsf{STRing_c}\, \Bbbk$, with residue field K. We put on K the fine A-module topology, so that the canonical surjection $\pi : A \twoheadrightarrow K$ is a strict epimorphism in $\mathsf{STRing_c}\, \Bbbk$.

(1) A lifting $\sigma : K \to A$ in $\mathsf{STRing_c}\,\Bbbk$ is called a *precise lifting* if the original topology of A equals the fine (K,σ)-module topology on it.

(2) The topology on A is called a *precise topology*, and A is called a *precise artinian local ring in* $\mathsf{STRing_c}\,\Bbbk$, if there exists some precise lifting $\sigma : K \to A$ in $\mathsf{STRing_c}\,\Bbbk$.

Here are examples:

Example 1.25. Start with an artinian local ring A in $\mathsf{Ring_c}\,\Bbbk$, and with a given lifting $\sigma : K \to A$ of the residue field. Put any topology on K that makes it into an object of $\mathsf{STRing_c}\,\Bbbk$. Next give A the fine (K,σ)-module topology. According to Lemma 1.15(2), the fine A-module topology on K equals its original topology. We see that $\sigma : K \to A$ is a precise lifting, and hence A is a precise artinian local ring in $\mathsf{STRing_c}\,\Bbbk$.

Definition 1.24 makes sense also for an artinian *semi-local* ring A, with Jacobson radical $\mathfrak{r}$ and residue ring $K := A/\mathfrak{r}$. Of course, here K is a finite product of fields. This is used in the next example.

Example 1.26. We use the Beilinson completion that is explained in Section 6. Assume $\Bbbk$ is a perfect field, and let X be a finite type $\Bbbk$-scheme. Take a saturated chain of points $\xi = (x_0, \dots, x_n)$ in X, and let $A := \mathcal{O}_{X,x_0}/\mathfrak{m}_{x_0}^{l+1}$ for some $l \in \mathbb{N}$. So A is an artinian local ring, and its residue field is $K := \boldsymbol{k}(x_0)$. Let $\sigma : K \to A$ be a lifting in $\mathsf{Ring_c}\,\Bbbk$.

We view A and K as quasi-coherent sheaves on X, constant on the closed set $\overline{\{x_0\}}$. The lifting σ is a differential operator of $\mathcal{O}_X$-modules, and hence, according to [Yekutieli 1992, Propositions 3.1.10 and 3.2.2], there is a homomorphism $\sigma_\xi : K_\xi \to A_\xi$ in $\mathsf{STRing_c}\,\Bbbk$ that lifts the canonical surjection $\pi_\xi : A_\xi \to K_\xi$. The arguments in the proof of [Yekutieli 1992, Proposition 3.2.5] show that K_ξ has the fine A_ξ-module topology, and vice versa.

By Theorem 6.1 the ring K_ξ is a finite product of fields. Therefore A_ξ is an artinian semi-local ring, with residue ring K_ξ. We see that the lifting $\sigma_\xi : K_\xi \to A_\xi$ is a precise lifting, and A_ξ is a precise artinian semi-local ring in $\mathsf{STRing_c}\,\Bbbk$.

Example 1.27. Assume $\Bbbk$ is a field. Let $K := \Bbbk((t))$ with the discrete topology, and let $\mathfrak{m} := \Bbbk((t))$ with the t-adic topology. We view $\mathfrak{m}$ as a ST K-module. Define $A := K \oplus \mathfrak{m}$, the trivial extension of K by $\mathfrak{m}$ (so $\mathfrak{m}^2 = 0$). For any lifting $\sigma : K \to A$, the (K,σ)-module topology on A is the discrete topology. Therefore there is no precise lifting, and A is not a precise artinian local ring in $\mathsf{STRing_c}\,\Bbbk$.

A question that immediately comes to mind is this: If A is a precise artinian local ring in $\mathsf{STRing_c}\,\Bbbk$, are all liftings $\sigma : K \to A$ in $\mathsf{STRing_c}\,\Bbbk$ precise? This is answered affirmatively in Corollary 2.12 in the next section.

Let A be a ST $\Bbbk$-ring and let M be a ST A-module. The closure $\overline{\{0\}}$ of the zero submodule $\{0\}$ is an A-submodule of M.

Definition 1.28. Let A be a ST $\Bbbk$-ring and let M be a ST A-module.

(1) If $\{0\}$ is closed in M, then M is called a *separated ST module*.

(2) Define $M^{\text{sep}} := M/\overline{\{0\}}$. This is a ST A-module with the quotient topology from M, and we call it *the separated ST module associated to M*.

Of course, M is a separated ST module if and only if it is a Hausdorff topological space.

The assignment $M \mapsto M^{\text{sep}}$ is a $\Bbbk$-linear functor from $\mathsf{STMod}\, A$ to itself. There is a functorial strict epimorphism $\tau_M : M \to M^{\text{sep}}$. The ST module M^{sep} is separated, and it is easy to see that for any separated ST A-module N the homomorphism

$$\operatorname{Hom}_A^{\text{cont}}(M^{\text{sep}}, N) \to \operatorname{Hom}_A^{\text{cont}}(M, N)$$

induced by τ_M is bijective.

Remark 1.29. The reader might wonder why we work with separated modules and not with complete modules. The reason is that, for a ST A-module M, its completion $\widehat{M} := \lim_{\leftarrow U} M/U$, where U runs over all open subgroups of M, could fail to be an A-module!

However, in many important instances (such as the module of differentials of a topological local field), the ST A-module M^{sep} turns out to be complete.

We end this section with a discussion of ST tensor products.

Definition 1.30 [Yekutieli 1992, Definition 1.2.11]. Suppose A is a commutative ST $\Bbbk$-ring, and $M_1, \dots, M_p$ are ST A-modules. The tensor product topology on the A-module

$$\bigotimes_{i=1}^{p} M_i := M_1 \otimes_A \cdots \otimes_A M_p$$

is the finest linear topology such that the canonical multilinear function

$$\prod_{i=1}^{p} M_i \to \bigotimes_{i=1}^{p} M_i$$

is semi-continuous.

With this topology, $\bigotimes_{i=1}^{p} M_i$ is a ST A-module. Given any semi-continuous A-multilinear function $\beta : \prod_{i=1}^{p} M_i \to N$, where N is a ST A-module, the corresponding A-linear homomorphism $\bigotimes_{i=1}^{p} M_i \to N$ is continuous. For more details see [Yekutieli 1992, Section 1.2].

Example 1.31. Let $f : A \to B$ be a homomorphism in $\mathsf{STRing_c}\,\Bbbk$, and let M be in $\mathsf{STMod}\,A$. Then $B \otimes_A M$, with the tensor product topology, is a ST B-module. We get an adjoint to the forgetful functor rest_f. If M has the fine A-module topology, then $B \otimes_A M$ has the fine B-module topology. See [Yekutieli 1992, Proposition 1.2.14 and Corollary 1.2.15].

Remark 1.32. Assume the base ring $\Bbbk$ is a field. Let M and N be ST $\Bbbk$-modules (i.e., linearly topologized $\Bbbk$-modules). Beilinson [2008] talks about three topologies on the tensor product $M \otimes_{\Bbbk} N$.

In our paper we encounter two topologies on $M \otimes_{\Bbbk} N$. The first is the tensor product topology from Definition 1.30. It is symmetric: the automorphism $m_1 \otimes m_2 \mapsto m_2 \otimes m_1$ of $M \otimes_{\Bbbk} M$ is a homeomorphism.

For the second kind of tensor product topology consider $M := \Bbbk(t_2)$ with the t_2-adic topology, and $N := \Bbbk(t_1)$ the t_1-adic topology. So $M \cong N$ in $\mathsf{STMod}\,\Bbbk$. Let $K := \Bbbk((t_1, t_2))$ be the field of iterated Laurent series, with the topology of Definition 1.17, starting from the discrete topology on $\Bbbk$. The embedding $M \otimes_{\Bbbk} N \subset K$ induces a topology on it, making it into a ST $\Bbbk$-module. Presumably this topology on $M \otimes_{\Bbbk} N$ can be described in terms of the topologies of M and N. Now K is complete, and $M \otimes_{\Bbbk} N$ is dense in it. Since the roles of the two variables in K are different (e.g., the series $\sum_{i \in \mathbb{N}} t_1^i \cdot t_2^{-i}$ is summable, but the series $\sum_{i \in \mathbb{N}} t_1^{-i} \cdot t_2^i$ is not summable), we see that this topology on $M \otimes_{\Bbbk} N$ is not symmetric.

It should be interesting to compare our two tensor product topologies to the three discussed in [Beilinson 2008].

2. Continuous differential operators

Our approach to continuous differential operators is an adaptation to the ST context of the definitions from [EGA IV 1967]. We are following [Yekutieli 1992; 1995]. Recall that the base ring $\Bbbk$ is a nonzero commutative ring, and it has the discrete topology.

Let A be a commutative $\Bbbk$-ring. Any $\Bbbk$-central A-bimodule P has an increasing filtration $\{F_i(P)\}_{i \in \mathbb{Z}}$ by A-sub-bimodules, called the differential filtration. This filtration is defined inductively. For $i \leq -1$ we define $F_i(P) := 0$. For $i \geq 0$ the elements of $F_i(P)$ are the elements $p \in P$ such that $a \cdot p - p \cdot a \in F_{i-1}(P)$ for every $a \in A$.

Now assume A is a commutative ST $\Bbbk$-ring, and let M, N be ST A-modules. The set $\mathrm{Hom}^{\mathrm{cont}}_{\Bbbk}(M, N)$ of continuous $\Bbbk$-linear homomorphisms is a $\Bbbk$-central A-bimodule, so it has a differential filtration. We define

$$\mathrm{Diff}^{\mathrm{cont}}_{A/\Bbbk}(M, N) := \bigcup_i F_i(\mathrm{Hom}^{\mathrm{cont}}_{\Bbbk}(M, N)) \subset \mathrm{Hom}^{\mathrm{cont}}_{\Bbbk}(M, N).$$

The elements of

$$F_i(\mathrm{Diff}^{\mathrm{cont}}_{A/\Bbbk}(M, N)) := F_i(\mathrm{Hom}^{\mathrm{cont}}_{\Bbbk}(M, N))$$

are by definition continuous differential operators of order at most i. Note that

$$F_0(\mathrm{Diff}^{\mathrm{cont}}_{A/\Bbbk}(M, N)) = \mathrm{Hom}^{\mathrm{cont}}_{A}(M, N).$$

When $N = M$ we write

$$\mathrm{Diff}^{\mathrm{cont}}_{A/\Bbbk}(M) := \mathrm{Diff}^{\mathrm{cont}}_{A/\Bbbk}(M, M).$$

This is a subring of $\mathrm{End}^{\mathrm{cont}}_{\Bbbk}(M)$. Let $\mathrm{Der}^{\mathrm{cont}}_{A/\Bbbk}(M)$ be the A-module of continuous $\Bbbk$-linear derivations $A \to M$. Then

$$F_1(\mathrm{Diff}^{\mathrm{cont}}_{A/\Bbbk}(A, M)) = M \oplus \mathrm{Der}^{\mathrm{cont}}_{A/\Bbbk}(M)$$

as left A-modules.

If $M = A$ then we write

$$\mathcal{D}^{\mathrm{cont}}_{A/\Bbbk} := \mathrm{Diff}^{\mathrm{cont}}_{A/\Bbbk}(A). \tag{2-1}$$

This is the ring of continuous differential operators of A (relative to $\Bbbk$). Let us write $\mathcal{T}^{\mathrm{cont}}_{A/\Bbbk} := \mathrm{Der}^{\mathrm{cont}}_{A/\Bbbk}(A)$, the Lie algebra of continuous derivations of A. Then

$$F_1(\mathcal{D}^{\mathrm{cont}}_{A/\Bbbk}) = A \oplus \mathcal{T}^{\mathrm{cont}}_{A/\Bbbk}$$

as left A-modules.

If A is discrete, then $\mathcal{D}^{\mathrm{cont}}_{A/\Bbbk} = \mathcal{D}_{A/\Bbbk}$, the usual ring of differential operators from [EGA IV 1967]; and $\mathcal{T}^{\mathrm{cont}}_{A/\Bbbk} = \mathcal{T}_{A/\Bbbk}$, the usual Lie algebra of derivations.

Remark 2.2. There is a canonical topology on $\mathrm{Hom}^{\mathrm{cont}}_{\Bbbk}(M, N)$, called the *Hom topology*, making it a ST A-module; see [Yekutieli 1995, Definition 1.1]. However, in this paper we shall not need this topology, and hence we consider $\mathrm{Hom}^{\mathrm{cont}}_{\Bbbk}(M, N)$ as an untopologized object (or as a discrete ST $\Bbbk$-module).

Example 2.3. Let $\boldsymbol{t} = (t_1, \dots, t_n)$ be a sequence of variables of length $n \geq 1$. In Definition 1.17 we saw how to make the ring of iterated Laurent series $\Bbbk((\boldsymbol{t})) := \Bbbk((t_1, \dots, t_n))$ into a ST $\Bbbk$-ring. This is a separated ST ring, i.e., $\Bbbk((\boldsymbol{t})) = \Bbbk((\boldsymbol{t}))^{\mathrm{sep}}$. Let $\Bbbk[\boldsymbol{t}]$ be the polynomial ring, with discrete topology. According to [Yekutieli 1992, Corollary 1.5.19] the ring homomorphism $\Bbbk[\boldsymbol{t}] \to \Bbbk((\boldsymbol{t}))$ is *topologically étale relative to* $\Bbbk$. This implies that any $\Bbbk$-linear differential operator ϕ on $\Bbbk[\boldsymbol{t}]$ extends uniquely to a continuous $\Bbbk$-linear differential operator $\widehat{\phi}$ on $\Bbbk((\boldsymbol{t}))$. This gives us a ring homomorphism $\mathcal{D}_{\Bbbk[\boldsymbol{t}]/\Bbbk} \to \mathcal{D}^{\mathrm{cont}}_{\Bbbk((\boldsymbol{t}))/\Bbbk}$ that respects the differential filtrations, and such that the induced homomorphism

$$\Bbbk((\boldsymbol{t})) \otimes_{\Bbbk[\boldsymbol{t}]} \mathcal{D}_{\Bbbk[\boldsymbol{t}]/\Bbbk} \to \mathcal{D}^{\mathrm{cont}}_{\Bbbk((\boldsymbol{t}))/\Bbbk} \tag{2-4}$$

is bijective.

If $\Bbbk$ has characteristic 0 (i.e., $\mathbb{Q} \subset \Bbbk$), then by (2-4) any $\hat{\phi} \in F_l(\mathcal{D}^{\mathrm{cont}}_{\Bbbk((\boldsymbol{t}))/\Bbbk})$ can be expressed uniquely as a finite sum

$$\hat{\phi} = \sum_{(i_1,\dots,i_n)} a_{(i_1,\dots,i_n)} \cdot \partial_1^{i_1} \cdots \partial_n^{i_n}, \tag{2-5}$$

where $i_k \in \mathbb{N}$, $\sum_k i_k \leq l$, $a_{(i_1,\dots,i_n)} \in \Bbbk((\boldsymbol{t}))$ and $\partial_i := \partial / \partial t_i$.

On the other hand, if $\Bbbk$ has characteristic $p > 0$ (i.e., $\mathrm{F}_p \subset \Bbbk$), then the structure of $\mathcal{D}^{\mathrm{cont}}_{\Bbbk((\boldsymbol{t}))/\Bbbk}$ is totally different. For every $m \geq 0$ let $\Bbbk((\boldsymbol{t}^{p^m})) := \Bbbk((t_1^{p^m}, \dots, t_n^{p^m}))$, which is a subring of $\Bbbk((\boldsymbol{t}))$. The ring $\Bbbk((\boldsymbol{t}))$ is a free module over $\Bbbk((\boldsymbol{t}^{p^m}))$ of rank p^{nm}, and the topology on $\Bbbk((\boldsymbol{t}))$ is the fine $\Bbbk((\boldsymbol{t}^{p^m}))$-module topology. According to [Yekutieli 1992, Theorem 1.4.9 and Corollary 2.1.18] we have

$$\mathcal{D}^{\mathrm{cont}}_{\Bbbk((\boldsymbol{t}))/\Bbbk} = \mathcal{D}_{\Bbbk((\boldsymbol{t}))/\Bbbk} = \bigcup_{m \geq 0} \mathrm{End}_{\Bbbk((\boldsymbol{t}^{p^m}))}\big(\Bbbk((\boldsymbol{t}))\big).$$

Let B be a $\Bbbk$-ring (not necessarily commutative). For any r_1, $r_2 \in \mathbb{N}$ let $\mathrm{Mat}_{r_2 \times r_1}(B)$ be the set of $r_2 \times r_1$ matrices with entries in B. The set of matrices $\mathrm{Mat}_r(B) := \mathrm{Mat}_{r \times r}(B)$ is a $\Bbbk$-ring with matrix multiplication, and $\mathrm{Mat}_{r_2 \times r_1}(B)$ is a $\Bbbk$-central $\mathrm{Mat}_{r_2}(B)$-$\mathrm{Mat}_{r_1}(B)$-bimodule. The group of invertible elements of $\mathrm{Mat}_r(B)$ is denoted by $\mathrm{GL}_r(B)$.

Now consider some $M \in \mathsf{Mod}\,\Bbbk$. The $\Bbbk$-ring $B := \mathrm{End}_{\Bbbk}(M)$ acts on M from the left. We view M^{r_1} as a column module, namely we make the identification $M^{r_1} = \mathrm{Mat}_{r_1 \times 1}(M)$. Then, for any $\phi \in \mathrm{Mat}_{r_2 \times r_1}(B)$ and $m \in M^{r_1}$, the matrix product $\phi \cdot m$ is an element of M^{r_2}. In this way we obtain a canonical isomorphism

$$\mathrm{Hom}_{\Bbbk}(M^{r_1}, M^{r_2}) \cong \mathrm{Mat}_{r_2 \times r_1}(\mathrm{End}_{\Bbbk}(M)) = \mathrm{Mat}_{r_2 \times r_1}(B) \tag{2-6}$$

of left $\mathrm{Mat}_{r_2}(B)$-modules and right $\mathrm{Mat}_{r_1}(B)$-modules.

The next lemma shows that this also happens in the topological and differential contexts.

Lemma 2.7. *Let $A \in \mathsf{STRing}_{\mathrm{c}}\,\Bbbk$ and $M \in \mathsf{STMod}\,A$. For any natural numbers r_1 and r_2, matrix multiplication gives rise to bijections*

$$\mathrm{Mat}_{r_2 \times r_1}(\mathrm{End}^{\mathrm{cont}}_{\Bbbk}(M)) \cong \mathrm{Hom}^{\mathrm{cont}}_{\Bbbk}(M^{r_1}, M^{r_2})$$

and

$$\mathrm{Mat}_{r_2 \times r_1}(\mathrm{Diff}^{\mathrm{cont}}_{A/\Bbbk}(M)) \cong \mathrm{Diff}^{\mathrm{cont}}_{A/\Bbbk}(M^{r_1}, M^{r_2}).$$

In particular, a homomorphism $\phi : M^r \to M^r$ in $\mathsf{STMod}\,\Bbbk$ is an isomorphism if and only if the corresponding matrix belongs to $\mathrm{GL}_r(\mathrm{End}^{\mathrm{cont}}_{\Bbbk}(M))$.

Proof. This is a straightforward consequence of the definitions. □

Lifting, precise liftings and precise artinian local rings in $\mathsf{STRing_c}\,\Bbbk$ were introduced in Definitions 1.21 and 1.24. The main result of this section is the next theorem.

Theorem 2.8. *Let A be a precise artinian local ring in* $\mathsf{STRing_c}\,\Bbbk$, *with residue field K. Give K the fine A-module topology. Let $\sigma_1, \sigma_2 : K \to A$ be liftings in* $\mathsf{STRing_c}\,\Bbbk$ *of the canonical surjection $A \twoheadrightarrow K$, and assume that σ_2 is a precise lifting.*

Let M_1 and M_2 be finite A-modules, and let $\phi : M_1 \to M_2$ be an A-linear homomorphism. For $l = 1, 2$ choose K-linear isomorphisms $\psi_l : K^{r_l} \xrightarrow{\simeq} \operatorname{rest}_{\sigma_l}(M_l)$. Let $\bar{\phi} \in \operatorname{Mat}_{r_2 \times r_1}(\operatorname{End}_{\Bbbk}(K))$ be the matrix such that the diagram

$$\begin{tikzcd} M_1 \arrow[r, "\phi"] & M_2 \\ K^{r_1} \arrow[u, "\psi_1"] \arrow[r, "\bar{\phi}"] & K^{r_2} \arrow[u, "\psi_2"'] \end{tikzcd}$$

in $\mathsf{Mod}\,\Bbbk$ *is commutative. Then the following hold*:

(1) *The matrix $\bar{\phi}$ belongs to* $\operatorname{Mat}_{r_2 \times r_1}(\mathcal{D}^{\mathrm{cont}}_{K/\Bbbk})$.

(2) *Assume that $M_1 = M_2$ and ϕ is the identity automorphism. Write $r := r_1$. Then the matrix $\bar{\phi}$ belongs to* $\mathrm{GL}_r(\mathcal{D}^{\mathrm{cont}}_{K/\Bbbk})$.

Proof. (1) Give M_1 and M_2 the fine A-module topologies. Let us write $\bar{M}_l := K^{r_l}$; these are ST K-modules with the fine K-module topologies. Since $\sigma_1, \sigma_2 : K \to A$ are continuous, it follows that both $\psi_l : \bar{M}_l \to M_l$ are continuous, namely are homomorphisms in $\mathsf{STMod}\,\Bbbk$. Furthermore, because σ_2 is a precise lifting, it follows that $\psi_2 : \bar{M}_2 \to M_2$ is a homeomorphism, so it is an isomorphism in $\mathsf{STMod}\,\Bbbk$. We conclude that $\bar{\phi} = \psi_2^{-1} \circ \phi \circ \psi_1$ is a homomorphism in $\mathsf{STMod}\,\Bbbk$, namely it is continuous.

Next, let us view A as a K-ring via σ_1. (There is no topology in this paragraph.) The canonical surjection $A \twoheadrightarrow K$ makes A into an augmented K-ring. Let us view $\bar{M}_1$ as an A-module via this augmentation. Now both $\bar{M}_1$ and M_1 are finite length A-modules, and $\psi_1 : \bar{M}_1 \to M_1$ is K-linear. According to [Yekutieli 1992, Proposition 1.4.4], ψ_1 is a differential operator over A. (The order of this operator is bounded by $r_1 - 1$.)

Similarly, we can view A as an augmented K-ring via σ_2. (There is no topology in this paragraph either.) Now both $\psi_2 : \bar{M}_2 \to M_2$ and its inverse $\psi_2^{-1} : M_2 \to \bar{M}_2$ are K-linear, and therefore they are differential operators over A. We conclude that the composition

$$\bar{\phi} = \psi_2^{-1} \circ \phi \circ \psi_1 : \bar{M}_1 \to \bar{M}_2$$

is a differential operator over A. Here the liftings σ_1, σ_2 stop playing a role. Now A acts on $\bar{M}_1$ and $\bar{M}_2$ via the canonical surjection $A \twoheadrightarrow K$, and this implies that $\bar{\phi}$ is a differential operator over K.

Combining the two results above we conclude that $\bar{\phi} : \bar{M}_1 \to \bar{M}_2$ is a continuous differential operator over K. Using Lemma 2.7 we see that the matrix $\bar{\phi}$ belongs to $\mathrm{Mat}_{r_2 \times r_1}(\mathcal{D}^{\mathrm{cont}}_{K/\Bbbk})$. This establishes (1).

(2) The proof of this part is very similar to that of [Yekutieli 1995, Lemma 6.6]

Let $\mathfrak{m}$ be the maximal ideal of A, and write $M := M_1$. Consider the $\mathfrak{m}$-adic filtration on M. The associated graded module $\mathrm{gr}_{\mathfrak{m}}(M)$ is a K-module of length r (regardless of any lifting). By a *filtered K-basis* of M we mean a collection $\{m_i\}_{1=1}^{r}$ of elements of M such that the collection of symbols $\{\bar{m}_i\}_{1=1}^{r}$ is a K-basis of $\mathrm{gr}_{\mathfrak{m}}(M)$ and such that $\deg(\bar{m}_i) \leq \deg(\bar{m}_{i+1})$. Such bases exist: simply choose a graded basis of $\mathrm{gr}_{\mathfrak{m}}(M)$, suitably ordered, and lift it to M.

Choose a filtered K-basis $\{m_i\}_{1=1}^{r}$ of M. For $l = 1, 2$ let $\chi_l : \bar{M} \to \mathrm{rest}_{\sigma_l}(M)$ be the K-linear isomorphism corresponding to this filtered basis. We get a commutative diagram

$$\begin{tikzcd}
M \arrow[r, "\phi=\mathbf{1}_M"] & M \arrow[r, "\phi=\mathbf{1}_M"] & M \arrow[r, "\phi=\mathbf{1}_M"] & M \\
\bar{M} \arrow[u, "\psi_1"] \arrow[r, "\bar{\phi}_1"] \arrow[rrr, bend right, "\bar{\phi}"'] & \bar{M} \arrow[u, "\chi_1"'] \arrow[r, "\bar{\phi}'"] & \bar{M} \arrow[u, "\chi_2"'] \arrow[r, "\bar{\phi}_2"] & \bar{M} \arrow[u, "\psi_2"']
\end{tikzcd}$$

in $\mathsf{Mod}\,\Bbbk$. By what we already know from (1), the matrices in the bottom row belong to $\mathrm{Mat}_r(\mathcal{D}^{\mathrm{cont}}_{K/\Bbbk})$; and they satisfy $\bar{\phi} = \bar{\phi}_2 \circ \bar{\phi}' \circ \bar{\phi}_1$. Moreover $\bar{\phi}_1, \bar{\phi}_2$ are in $\mathrm{GL}_r(K) \subset \mathrm{GL}_r(\mathcal{D}^{\mathrm{cont}}_{K/\Bbbk})$. Thus it suffices to prove that $\bar{\phi}' \in \mathrm{GL}_r(\mathcal{D}^{\mathrm{cont}}_{K/\Bbbk})$.

Write $\bar{\phi}' = [\gamma_{i,j}]$ with $\gamma_{i,j} \in \mathcal{D}^{\mathrm{cont}}_{K/\Bbbk}$. These operators satisfy

$$\sum_{i=1}^{r} \sigma_1(a_i) \cdot m_i = \sum_{i,j=1}^{r} \sigma_2(\gamma_{i,j}(a_i)) \cdot m_j \tag{2-9}$$

for any column $[a_i] \in K^r$. Therefore, for any i and any $a \in K$, taking $a_i := a$ and $a_j := 0$ for $j \neq i$, formula (2-9) gives

$$\sigma_1(a) \cdot m_i = \sum_{j=1}^{r} \sigma_2(\gamma_{i,j}(a)) \cdot m_j .$$

But the basis $\{m_i\}_{1=1}^{r}$ is filtered, and this implies that $\gamma_{i,j}(a) = 0$ for $j < i$ and $\gamma_{i,i}(a) = a$. As elements of the ring $\mathcal{D}^{\mathrm{cont}}_{K/\Bbbk}$ we get $\gamma_{i,j} = 0$ for $j < i$ and $\gamma_{i,i} = 1$.

So the matrix $\bar{\phi}'$ is upper triangular with 1 on the diagonal:

$$\bar{\phi}' = [\gamma_{i,j}] = \begin{bmatrix} 1 & * & \cdots & * \\ 0 & 1 & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} \in \mathrm{Mat}_r(\mathcal{D}^{\mathrm{cont}}_{K/\Bbbk}).$$

The matrix $\epsilon := 1 - \bar{\phi}' \in \mathrm{Mat}_r(\mathcal{D}^{\mathrm{cont}}_{K/\Bbbk})$ is nilpotent, and hence the matrix

$$\theta := \sum_{i=0}^{r} \epsilon^i \in \mathrm{Mat}_r(\mathcal{D}^{\mathrm{cont}}_{K/\Bbbk})$$

satisfies $\theta \circ \bar{\phi}' = \bar{\phi}' \circ \theta = 1$. We conclude that $\bar{\phi}' \in \mathrm{GL}_r(\mathcal{D}^{\mathrm{cont}}_{K/\Bbbk})$. □

Remark 2.10. An attempt to deduce assertion (2) of the theorem from assertion (1) by functoriality will not work. This is because (a priori) there is no symmetry between the two liftings σ_1 and σ_2: only the lifting σ_2 is assumed to be precise.

Eventually we show (Corollary 2.12) that the lifting σ_1 is also precise. But this relies on Theorem 2.8!

Corollary 2.11. *In the situation of part* (2) *of the theorem, the fine* (K, σ_1)*-module topology on* $M_1 = M_2$ *equals the fine* (K, σ_2)*-module topology on it.*

Proof. For $l = 1, 2$ let us denote by M_l^{st} the $\Bbbk$-module M_l endowed with the fine (K, σ_l)-module topology. We want to prove that $M_1^{\mathrm{st}} = M_2^{\mathrm{st}}$; or, equivalently, we want to prove that the identity automorphism $\phi : M_1 \to M_2$ in $\mathsf{Mod}\,\Bbbk$ becomes an isomorphism $\phi^{\mathrm{st}} : M_1^{\mathrm{st}} \to M_2^{\mathrm{st}}$ in $\mathsf{STMod}\,\Bbbk$.

We have equality $\phi = \psi_2 \circ \bar{\phi} \circ \psi_1^{-1}$ of isomorphisms $M_1 \to M_2$ in $\mathsf{Mod}\,\Bbbk$. By definition of the fine topology, $\psi_l : K^{r_l} \xrightarrow{\simeq} M_l^{\mathrm{st}}$ are isomorphisms in $\mathsf{STMod}\,\Bbbk$. Therefore it suffices to prove that $\bar{\phi} : K^{r_1} \to K^{r_2}$ is an isomorphism in $\mathsf{STMod}\,\Bbbk$. This is true by Lemma 2.7 and part (2) of the theorem. □

The next corollary is a generalization of [Yekutieli 1992, Proposition 2.2.2(a)].

Corollary 2.12. *Let A be a precise artinian local ring in* $\mathsf{STRing_c}\,\Bbbk$, *with residue field K. Give K the fine A-module topology. Then any lifting $\sigma : K \to A$ in* $\mathsf{STRing_c}\,\Bbbk$ *is a precise lifting.*

Proof. Write $\sigma_1 := \sigma$. By definition there exists some precise lifting $\sigma_2 : K \to A$; so the topology on A equals the fine (K, σ_2)-module topology. Now apply Corollary 2.11 with $M := A$. □

Here is another corollary, pointed out to us by Wolfson:

Corollary 2.13. *Let A be a precise artinian local ring in* $\mathsf{STRing_c}\,\Bbbk$, *with residue field K, and let $\sigma : K \to A$ be a precise lifting. Let M be a finite A-module,* *and choose a K-linear isomorphism $K^r \xrightarrow{\simeq} \operatorname{rest}_\sigma(M)$. Then A acts on $M \cong K^r$ via* $\operatorname{Mat}_r(\mathcal{D}^{\text{cont}}_{K/\Bbbk})$.

Proof. In the theorem, take $M_l := M$. For $a \in A$ we get an A-linear homomorphism $\phi : M \to M$, $\phi(m) := a \cdot m$. □

Remark 2.14. If we only wanted to know that $\bar{\phi} \in \operatorname{Mat}_{r_2 \times r_1}(\operatorname{End}^{\text{cont}}_{\Bbbk}(K))$ in Theorem 2.8(1), and that in part (2) $\bar{\phi} \in \operatorname{GL}_r(\operatorname{End}^{\text{cont}}_{\Bbbk}(K))$, then we did not have to talk about differential operators at all, and the proof could have been included in Section 1. The reason for placing the proof here is twofold. First, it is more economical to prove the full result at once.

The second reason is more delicate. Sometimes in characteristic $p > 0$, differential operators are automatically continuous. See Example 2.3. In such cases all liftings $\sigma : K \to A$ are continuous. This says that Theorem 2.8 could hold without assuming a priori that the liftings $\sigma_1, \sigma_2 : K \to A$ are continuous.

We finish this section with a discussion of differential forms. This will be needed in Section 5. Recall that for $A \in \mathsf{Ring}_{\mathrm{c}}\, \Bbbk$ we have the de Rham complex, or the DG ring of Kähler differentials, $\Omega_{A/\Bbbk} = \bigoplus_{i \geq 0} \Omega^i_{A/\Bbbk}$, with its differential d. In degree 0 we have $\Omega^0_{A/\Bbbk} = A$, and the $\Bbbk$-linear derivation $\mathrm{d} : A \to \Omega^1_{A/\Bbbk}$ is universal, in the sense that for any $\Bbbk$-linear derivation $\partial : A \to M$ there is a unique A-linear homomorphism $\phi : \Omega^1_{A/\Bbbk} \to M$ such that $\partial = \phi \circ \mathrm{d}$. The A-module $\Omega^i_{A/\Bbbk}$ is the i-th exterior power of the A-module $\Omega^1_{A/\Bbbk}$, and the operator d on $\Omega_{A/\Bbbk}$ is the unique extension of $\mathrm{d} : \Omega^0_{A/\Bbbk} \to \Omega^1_{A/\Bbbk}$ to an odd derivation.

Now consider $A \in \mathsf{STRing}_{\mathrm{c}}\, \Bbbk$. The abstract DG ring $\Omega_{A/\Bbbk}$ is too big (at least in characteristic 0). However the DG ring $\Omega_{A/\Bbbk}$ has a canonical ST structure. For every i consider the $(i+1)$-st tensor power $\mathrm{T}^{i+1}_{\Bbbk}(A) := A \otimes_{\Bbbk} \cdots \otimes_{\Bbbk} A$, with its tensor product topology (Definition 1.30). There is a surjection $\mathrm{T}^{i+1}_{\Bbbk}(A) \twoheadrightarrow \Omega^i_{A/\Bbbk}$,

$$a_0 \otimes a_1 \otimes \cdots \otimes a_i \mapsto a_0 \cdot \mathrm{d}(a_1) \cdots \mathrm{d}(a_i),$$

and we use it to give $\Omega^i_{A/\Bbbk}$ the quotient topology. Then $\Omega_{A/\Bbbk} = \bigoplus_{i \geq 0} \Omega^i_{A/\Bbbk}$ gets the direct sum topology. It turns out that $\Omega_{A/\Bbbk}$ becomes a DG ST ring. In particular the differential d is continuous. For any i let $\Omega^{i,\text{sep}}_{A/\Bbbk} := (\Omega^i_{A/\Bbbk})^{\text{sep}}$, the associated separated ST module. Let $\Omega^{\text{sep}}_{A/\Bbbk} := \bigoplus_{i \geq 0} \Omega^{i,\text{sep}}_{A/\Bbbk}$, with the direct sum topology. Note that $\Omega^{0,\text{sep}}_{A/\Bbbk} = A^{\text{sep}}$.

Proposition 2.15 [Yekutieli 1992]. *Let A be a commutative ST $\Bbbk$-ring.*

1. *The ST $\Bbbk$-module $\Omega^{\text{sep}}_{A/\Bbbk}$ has a DG ST $\Bbbk$-ring structure such the canonical surjection $\tau_A : \Omega_{A/\Bbbk} \twoheadrightarrow \Omega^{\text{sep}}_{A/\Bbbk}$ is a homomorphism of DG ST $\Bbbk$-rings.*
2. *Let M be a separated ST A-module. The derivation $\mathrm{d} : A \to \Omega^{1,\text{sep}}_{A/\Bbbk}$ induces a bijection*

$$\operatorname{Hom}^{\text{cont}}_A(\Omega^{1,\text{sep}}_{A/\Bbbk}, M) \xrightarrow{\simeq} \operatorname{Der}^{\text{cont}}_{A/\Bbbk}(M).$$

For a proof and full details see [Yekutieli 1992, Section 1.5].

Example 2.16. Let $K := \Bbbk((t_1, \dots, t_n))$ be as in Example 2.3, and let $\Bbbk[\boldsymbol{t}] := \Bbbk[t_1, \dots, t_n]$. Since K is a separated ST $\Bbbk$-ring, we see that $\Omega^{0,\mathrm{sep}}_{K/\Bbbk} = K$. Because the homomorphism $\Bbbk[\boldsymbol{t}] \to K$ is topologically étale in $\mathsf{STRing}_{\mathrm{c}}\, \Bbbk$, it follows that $\Omega^{1,\mathrm{sep}}_{K/\Bbbk}$ is a free K-module with basis the sequence $(\mathrm{d}(t_1), \dots, \mathrm{d}(t_n))$. For every i we have

$$\Omega^{i,\mathrm{sep}}_{K/\Bbbk} = \textstyle\bigwedge^i_K \Omega^{1,\mathrm{sep}}_{K/\Bbbk},$$

a free K-module of rank $\binom{n}{i}$, with the fine K-module topology. For proofs see [Yekutieli 1992, Corollaries 1.5.19 and 1.5.13].

Note that if $\Bbbk$ is a field of characteristic 0, then the K-module $\Omega^1_{K/\Bbbk}$ is a free K-module of rank equal to $\mathrm{tr.deg}_{\Bbbk}(K)$, which is uncountably infinite. Thus the kernel of the canonical surjection $\tau_K : \Omega^1_{K/\Bbbk} \twoheadrightarrow \Omega^{1,\mathrm{sep}}_{K/\Bbbk}$ is gigantic.

3. Topological local fields

In this section we review definitions and results from [Yekutieli 1992, Section 2.1]. We start with a definition due to Parshin [1976; 1983] and Kato [1979]. See also [Fesenko and Kurihara 2000].

Definition 3.1. Let K be a field. An *n-dimensional local field structure* on K, for $n \geq 1$, is a sequence $\mathcal{O}_1(K), \dots, \mathcal{O}_n(K)$ of complete discrete valuation rings, such that:

- K is the fraction field of $\mathcal{O}_1(K)$.
- For $1 \leq i \leq n-1$, the residue field of $\mathcal{O}_i(K)$ is the fraction field of $\mathcal{O}_{i+1}(K)$.

The data $(K, \{\mathcal{O}_i(K)\}_{i=1}^n)$ is an *n-dimensional local field*. We refer to $\mathcal{O}_i(K)$ as the i-th valuation ring of K. The residue field of $\mathcal{O}_i(K)$ is denoted by $\boldsymbol{k}_i(K)$, and its maximal ideal is denoted by $\mathfrak{m}_i(K)$. We also write $\boldsymbol{k}_0(K) := K$.

Let K be an n-dimensional local field. A *system of uniformizers* in K (called a regular system of parameters in [Yekutieli 1992]) is a sequence $(a_1, \dots, a_n)$ of elements of $\mathcal{O}_1(K)$ such that a_1 generates the maximal ideal $\mathfrak{m}_1(K)$ of $\mathcal{O}_1(K)$ and, if $n \geq 2$, the sequence $(\bar{a}_2, \dots, \bar{a}_n)$, which is the image of $(a_2, \dots, a_n)$ under the canonical surjection $\mathcal{O}_1(K) \twoheadrightarrow \boldsymbol{k}_1(K)$, is a system of uniformizers in $\boldsymbol{k}_1(K)$. A system of uniformizers $\boldsymbol{a} = (a_1, \dots, a_n)$ in K determines a valuation on K, with values in the group $\mathbb{Z}^n$ ordered lexicographically.

It is easy to find a system of uniformizers in an n-dimensional local field K. Say $(\bar{a}_2, \dots, \bar{a}_n)$ is a system of uniformizers in $\boldsymbol{k}_1(K)$. Choose an arbitrary lifting to a sequence $(a_2, \dots, a_n)$ in $\mathcal{O}_1(K)$, and append to it any uniformizer a_1 of $\mathcal{O}_1(K)$.

Let $\mathcal{O}(K)$ be the subring of K defined by

$$\mathcal{O}(K) := \mathcal{O}_1(K) \times_{\boldsymbol{k}_1(K)} \mathcal{O}_2(K) \cdots \times_{\boldsymbol{k}_{n-1}(K)} \mathcal{O}_n(K). \tag{3-2}$$

This is a local ring, whose residue field is $\boldsymbol{k}_n(K)$. We call $\mathcal{O}(K)$ the ring of integers of K. The ring $\mathcal{O}(K)$ is integrally closed in its field of fractions K; but unless $n = 1$ (in which case $\mathcal{O}(K) = \mathcal{O}_1(K)$), $\mathcal{O}(K)$ is not noetherian.

A 0-dimensional local field is just a field; there are no valuations. Its ring of integers is $\mathcal{O}(K) := K$, and $\boldsymbol{k}_0(K) := K$ too.

Definition 3.3. Let $\mathbb{k}$ be a nonzero commutative ring. An *n-dimensional local field over* $\mathbb{k}$, for $n \in \mathbb{N}$, is an n-dimensional local field $(K, \{\mathcal{O}_i(K)\}_{i=1}^n)$ together with a ring homomorphism $\mathbb{k} \to \mathcal{O}(K)$ such that the induced ring homomorphism $\mathbb{k} \to \boldsymbol{k}_n(K)$ is finite.

In other words, the n-dimensional local field structure of K lives in the category $\mathsf{Ring_c}\,\mathbb{k}$ of commutative $\mathbb{k}$-rings. If $\mathbb{k}$ is a field, then $\boldsymbol{k}_n(K)$ is a finite field extension of $\mathbb{k}$.

By abuse of notation, we usually call K an n-dimensional local field over $\mathbb{k}$, and keep the data $\{\mathcal{O}_i(K)\}_{i=1}^n$ implicit.

Remark 3.4. Some authors insist that the base ring be $\mathbb{k} = \mathbb{Z}$; this forces $\boldsymbol{k}_n(K)$ to be a finite field. We do not impose such a restriction.

Definition 3.5. Let K and L be n-dimensional local fields over $\mathbb{k}$, for $n \geq 0$. A *morphism of n-dimensional local fields over* $\mathbb{k}$ is a $\mathbb{k}$-ring homomorphism $f : K \to L$ such that the following conditions hold when $n \geq 1$:

- $f(\mathcal{O}_1(K)) \subset \mathcal{O}_1(L)$.
- The induced $\mathbb{k}$-ring homomorphism $f : \mathcal{O}_1(K) \to \mathcal{O}_1(L)$ is a local homomorphism.
- The induced $\mathbb{k}$-ring homomorphism $\bar{f} : \boldsymbol{k}_1(K) \to \boldsymbol{k}_1(L)$ is a morphism of $(n-1)$-dimensional local fields over $\mathbb{k}$.

The category of n-dimensional local fields over $\mathbb{k}$ is denoted by $\mathsf{LF}^n\,\mathbb{k}$. Note that any morphism in $\mathsf{LF}^n\,\mathbb{k}$ is finite. Cf. Remark 3.11 below regarding more general morphisms between local fields.

Remark 3.6. It can be shown that a field K in $\mathsf{Ring_c}\,\mathbb{k}$ admits at most one structure of an n-dimensional local field (see, e.g., [Morrow 2013, Remark 2.3]). This implies that the forgetful functor $\mathsf{LF}^n\,\mathbb{k} \to \mathsf{Ring_c}\,\mathbb{k}$ is fully faithful.

From here on we assume that the base ring $\mathbb{k}$ is a *perfect field*. This implies that all our local fields are of equal characteristic.

Definition 3.7. Let $\mathbb{k}$ be a perfect field. Given a finite field extension $\mathbb{k}'$ of $\mathbb{k}$, the *standard n-dimensional topological local field* over $\mathbb{k}$ with last residue field $\mathbb{k}'$ is the field of iterated Laurent series

$$\mathbb{k}'((t_1, \ldots, t_n)) := \mathbb{k}'((t_n)) \cdots ((t_1)).$$

Let us write $K := \Bbbk'((t_1, \dots, t_n))$. The field K comes equipped with these two structures:

(1) A structure of an n-dimensional local field, in which the valuation rings are

$$\mathcal{O}_i(K) := \Bbbk'((t_{i+1}, \dots, t_n))[\![t_i]\!],$$

and the residue fields are

$$\boldsymbol{k}_i(K) := \Bbbk'((t_{i+1}, \dots, t_n)).$$

(2) A structure of an ST $\Bbbk$-ring, with the topology from Definition 1.17, starting from the discrete topology on $\Bbbk'$.

For $n = 0$ we have $K = \Bbbk'$, a finite extension of $\Bbbk$ with the discrete topology.

Definition 3.8 [Yekutieli 1992, Section 2.1]. Let $\Bbbk$ be a perfect field. An *n-dimensional topological local field over* $\Bbbk$, for $n \geq 0$, is a field K together with:

(a) A structure $\{\mathcal{O}_i(K)\}_{i=1}^{n}$ of an n-dimensional local field on K.

(b) A ring homomorphism $\Bbbk \to \mathcal{O}(K)$ such that $\Bbbk \to \boldsymbol{k}_n(K)$ is finite.

(c) A topology on K, making it a semi-topological $\Bbbk$-ring.

The condition is this:

(P) There is a bijection

$$f : \Bbbk'((t_1, \dots, t_n)) \xrightarrow{\simeq} K$$

from the standard n-dimensional topological local field with last residue field $\Bbbk' := \boldsymbol{k}_n(K)$. The bijection f must have these two properties:

(i) f is an isomorphism in $\mathsf{LF}^n\,/\Bbbk$ (i.e., it respects the valuations).

(ii) f is an isomorphism in $\mathsf{STRing}_\mathsf{c}\,\Bbbk$ (i.e., it respects the topologies).

Such a bijection f is called a *parametrization* of K.

The parametrization f is not part of the structure of K; it is required to exist, but (as we shall see) there are many distinct parametrizations. We use the abbreviation "TLF" for "topological local field".

Definition 3.9. Let K and L be n-dimensional TLFs over $\Bbbk$. A *morphism of TLFs* $f : K \to L$ is a homomorphism of $\Bbbk$-rings satisfying these two conditions:

(i) f is a morphism of n-dimensional local fields (i.e., it respects the valuations; see Definition 3.5).

(ii) f is a homomorphism of ST $\Bbbk$-rings (i.e., it is continuous).

The category of n-dimensional TLFs over $\Bbbk$ is denoted by $\mathsf{TLF}^n\,/\Bbbk$.

There are forgetful functors $\mathsf{TLF}^n\,\Bbbk \to \mathsf{LF}^n\,\Bbbk$ and $\mathsf{TLF}^n\,\Bbbk \to \mathsf{STRing}_\mathsf{c}\,\Bbbk$.

Remark 3.10. The conditions of Definition 3.3 and 3.8 are more restrictive than those of [Yekutieli 1992, Definition 2.1.10], in this respect: here we require that the last residue field $\mathbb{k}' := \boldsymbol{k}_n(K)$ is finite over the base field $\mathbb{k}$, whereas in [loc. cit.] we only required that $\Omega^1_{\mathbb{k}'/\mathbb{k}}$ should be a finite $\mathbb{k}'$-module (which allows $\mathbb{k}'$ to be a finitely generated extension field of $\mathbb{k}$ with transcendence degree greater than 0).

If the TLF K arises as a local factor of a Beilinson completion $\boldsymbol{k}(x_0)_{\xi}$, as in Theorem 6.1, then the last residue field $\boldsymbol{k}_n(K)$ is finite over $\mathbb{k}$. So this fits into Definition 3.8.

Remark 3.11. In [Yekutieli 1992, Section 2.1] we also allow the much more general possibility of a morphism of TLFs $f : K \to L$ where $\dim(K) < \dim(L)$. For instance, the inclusions $\mathbb{k} \to \mathbb{k}((t_2)) \to \mathbb{k}((t_1, t_2))$ are morphisms. In this way we get a category $\mathsf{TLF}\, \mathbb{k}$, which contains each $\mathsf{TLF}^n\, \mathbb{k}$ as a full subcategory.

Remark 3.12. The papers on higher local fields from the Parshin school (prior to 1992) did not have a correct treatment of the topology on higher local fields. Some papers (e.g., [Parshin 1976; 1983; Beilinson 1980]) ignored it. Others — most notably [Lomadze 1981] — erroneously claimed that the topology of a local field is intrinsic, namely that it is determined by the valuations. This is correct in dimension 1; but it is *false* when $\operatorname{char}(\mathbb{k}) = 0$ and the dimension is 2 or higher. We gave a counterexample in [Yekutieli 1992, Example 2.1.22] that we reproduce in an expanded form as Example 3.13 below.

It is a deep fact, also proved in [Yekutieli 1992], that in characteristic $p > 0$ the topology is determined by the valuation, so that the forgetful functor $\mathsf{TLF}^n\, \mathbb{k} \to \mathsf{LF}^n\, \mathbb{k}$ is an equivalence. The proof relies on the structure of the ring of differential operators $\mathcal{D}_{K/\mathbb{k}}$ in characteristic $p > 0$ (see [Yekutieli 1992, Theorem 2.1.14 and Proposition 2.1.21]).

Example 3.13. This is a slightly expanded version of [Yekutieli 1992, Example 2.1.22]. Let $\mathbb{k}$ be a field of characteristic 0, and let $K := \mathbb{k}((t_1, t_2))$, the standard TLF of dimension 2. We choose a collection $\{b_i\}_{i \in I}$ of elements in $\boldsymbol{k}_1(K) = \mathbb{k}((t_2))$ that is a transcendence basis over the subfield $\mathbb{k}(t_2)$. For any $i \in I$ we choose some element $c_i \in \mathcal{O}_1(K)$. As explained in the proof of Theorem 1.1, there is a unique lifting

$$\sigma : \mathbb{k}((t_2)) \to \mathcal{O}_1(K) = \mathbb{k}((t_2))[[t_1]]$$

in $\mathsf{Ring}_{\mathsf{c}}\, \mathbb{k}$ such that $\sigma(t_2) = t_2$ and $\sigma(b_i) = b_i + t_1 c_i$ for all $i \in I$. Next we extend σ to a $\mathbb{k}$-ring automorphism $f : \mathcal{O}_1(K) \to \mathcal{O}_1(K)$ by setting $f(t_1) := t_1$. By localization this extends to a $\mathbb{k}$-ring automorphism $f : K \to K$.

It easy to check that f is an automorphism of K in the category $\mathsf{LF}^2\, \mathbb{k}$ of local fields. However, since f is the identity on the subfield $\mathbb{k}(t_1, t_2) \subset K$, and this subfield is a dense subset of K, it follows that f is continuous if and only if it is the identity automorphism of K, which occurs if and only if $c_i = 0$ for all i. Thus, if we choose at least one $c_i \neq 0$, f is not a morphism in $\mathsf{TLF}^2\,\Bbbk$.

Let K be a TLF of dimension $n \geq 1$ over $\Bbbk$. The inclusion $\mathcal{O}_1(K) \hookrightarrow K$ gives $\mathcal{O}_1(K)$ an induced structure of ST $\Bbbk$-ring (it is the subspace topology). Then the surjection $\mathcal{O}_1(K) \twoheadrightarrow \boldsymbol{k}_1(K)$ gives $\boldsymbol{k}_1(K)$ an induced structure of ST $\Bbbk$-ring (it is the quotient topology). And so on all the way to $\boldsymbol{k}_n(K)$. In other words, the topologies are such that each $\mathcal{O}_i(K) \hookrightarrow \boldsymbol{k}_{i-1}(K)$ is a strict monomorphism in $\mathsf{STRing_c}\,\Bbbk$, and each $\mathcal{O}_i(K) \twoheadrightarrow \boldsymbol{k}_i(K)$ is a strict epimorphism.

If we choose a parametrization $K \cong \Bbbk'((t_1, \dots, t_n))$, then the induced ring isomorphisms

$$\Bbbk'((t_{i+1}, \dots, t_n))[[t_i]] \cong \mathcal{O}_i(K)$$

and

$$\Bbbk'((t_{i+1}, \dots, t_n)) \cong \boldsymbol{k}_i(K)$$

are also isomorphisms of ST $\Bbbk$-rings. This follows from [Yekutieli 1992, Proposition 1.3.5]. In particular, each $\boldsymbol{k}_i(K)$ is an $(n-i)$-dimensional TLF over $\Bbbk$.

Recall the notions of precise lifting and precise artinian local ring from Definition 1.24.

Lemma 3.14. *Let K be a TLF of dimension $n \geq 1$ over $\Bbbk$; let $l \geq 0$. Then the ST ring $A_l := \mathcal{O}_1(K)/\mathfrak{m}_1(K)^{l+1}$, with the quotient topology from $\mathcal{O}_1(K)$, is a precise artinian local ring in* $\mathsf{STRing_c}\,\Bbbk$.

Proof. Choose a parametrization $K \cong \Bbbk'((t_1, \dots, t_n))$, and let $\bar{K} := \Bbbk'((t_2, \dots, t_n))$. Then $\bar{K} \cong \boldsymbol{k}_1(K)$ and $\bar{K}[[t_1]] \cong \mathcal{O}_1(K)$ as ST $\Bbbk$-rings; and the inclusion $\bar{K} \to \bar{K}[[t_1]]$ represents a lifting $\sigma_1 : \boldsymbol{k}_1(K) \to \mathcal{O}_1(K)$. As ST $\bar{K}$-modules, $\mathcal{O}_1(K) \cong \prod_{i=0}^{\infty} \bar{K}$ and $A_l \cong \prod_{i=0}^{l} \bar{K}$. This shows that the quotient topology on A_l coincides with the fine $\bar{K}$-module topology on it. So σ_1 is a precise lifting. □

Lemma 3.15. *Let $K \in \mathsf{TLF}^n\,\Bbbk$, with last residue field $\Bbbk' := \boldsymbol{k}_n(K)$. There is a unique lifting $\sigma : \Bbbk' \to \mathcal{O}(K)$ in $\mathsf{STRing_c}\,\Bbbk$ of the canonical surjection $\mathcal{O}(K) \twoheadrightarrow \Bbbk'$.*

Proof. Since $\Bbbk'$ is discrete, we do not have to worry about continuity. We use induction on n. Let $\bar{\sigma} : \Bbbk' \to \mathcal{O}(\boldsymbol{k}_1(K)) \subset \boldsymbol{k}_1(K)$ be the unique lifting for this $(n-1)$-dimensional TLF. Consider the canonical surjection $\pi : \mathcal{O}_1(K) \to \boldsymbol{k}_1(K)$. By Theorem 1.1 there is a unique $\Bbbk$-ring homomorphism $\sigma : \Bbbk' \to \mathcal{O}_1(K)$ such that $\pi \circ \sigma = \bar{\sigma}$. It is trivial to see that $\sigma(\Bbbk')$ is inside $\mathcal{O}(K)$. □

The construction and classification of parametrizations of a TLF (condition (P) in Definition 3.8) is made clear by the next theorem (which is a special case of [Yekutieli 1992, Corollary 2.1.19]).

Theorem 3.16 [Yekutieli 1992]. *Let K be an n-dimensional TLF over $\Bbbk$, let $(a_1, \dots, a_n)$ be a system of uniformizers in K, let $\Bbbk' := \boldsymbol{k}_n(K)$, and let $\sigma : \Bbbk' \to$*

$\mathcal{O}(K)$ be the unique lifting over $\Bbbk$. Then σ extends uniquely to an isomorphism of TLFs

$$f : \Bbbk'((t_1, \ldots, t_n)) \to K$$

such that $f(t_i) = a_i$.

Definition 3.17. Let K be an n-dimensional TLF over $\Bbbk$. By a *system of liftings* for K we mean a sequence $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_n)$, where for each i

$$\sigma_i : \boldsymbol{k}_i(K) \to \mathcal{O}_i(K)$$

is a homomorphism of ST $\Bbbk$-rings that lifts the canonical surjection $\mathcal{O}_i(K) \twoheadrightarrow \boldsymbol{k}_i(K)$.

The important thing to remember is that each lifting $\sigma_i : \boldsymbol{k}_i(K) \to \mathcal{O}_i(K)$ is continuous. When $n = 0$ the only system of liftings is the empty system $\boldsymbol{\sigma} = ()$.

Example 3.18. Take a standard TLF $K := \Bbbk'((t_1, \ldots, t_n))$. It comes equipped with a standard system of liftings

$$\sigma_i : \boldsymbol{k}_i(K) \to \mathcal{O}_i(K),$$

namely the inclusions

$$\sigma_i : \Bbbk'((t_{i+1}, \ldots, t_n)) \to \Bbbk'((t_{i+1}, \ldots, t_n))[[t_i]].$$

Proposition 3.19. *Any n-dimensional TLF K over $\Bbbk$ admits a system of liftings.*

Proof. Take a parametrization $f : \Bbbk'((t_1, \ldots, t_n)) \to K$. The standard system of liftings of $\Bbbk'((t_1, \ldots, t_n))$ induces a system of liftings on K. □

4. Lattices and BT operators

As before, $\Bbbk$ is a perfect base field.

Definition 4.1. Let K be an n-dimensional TLF over $\Bbbk$, and let M be a finite K-module. An *$\mathcal{O}_1(K)$-lattice* in M is a finite $\mathcal{O}_1(K)$-submodule L of M such that $M = K \cdot L$. We denote by $\mathrm{Lat}(M)$ the set of $\mathcal{O}_1(K)$-lattices in M.

Let L be an $\mathcal{O}_1(K)$-lattice in M. Recall that $\mathcal{O}_1(K)$ is a DVR. This implies that L is a free $\mathcal{O}_1(K)$-module, of rank equal to that of M.

Example 4.2. Consider a TLF K, and take $M := K^r$. Choose a uniformizer $a \in \mathcal{O}_1(K)$. For any $i \in \mathbb{Z}$ there is a lattice $L_i := a^i \cdot \mathcal{O}_1(K)^r \subset K^r$. Let us call these standard lattices. They do not depend on the choice of uniformizer.

When $r = 1$, all the $\mathcal{O}_1(K)$-lattices in M are standard. When $r > 1$, M has many more lattices. However any $\mathcal{O}_1(K)$-lattice L in M can be sandwiched between two standard lattices: $L_i \subset L \subset L_{-j}$ for $i, j \gg 0$.

Suppose M is a finite K-module, and $L,\ L' \in \operatorname{Lat}(M)$ with $L \subset L'$. Then the quotient L'/L is a finite length $\mathcal{O}_1(K)$-module. If we are given a lifting $\sigma_1 : \boldsymbol{k}_1(K) \to \mathcal{O}_1(K)$, then L'/L becomes a finite module over the TLF $\boldsymbol{k}_1(K)$, which we denote by $\operatorname{rest}_{\sigma_1}(L'/L)$; see Definition 1.20.

Lemma 4.3. *Let M be a finite K-module, let L be an $\mathcal{O}_1(K)$-lattice in M, and let $a \in \mathcal{O}_1(K)$ be a uniformizer. Give M the fine K-module topology. For every $i \in \mathbb{Z}$ give the lattice $L_i := a^i \cdot L$ the fine $\mathcal{O}_1(K)$-module topology. For every $i \in \mathbb{N}$ give the quotient L/L_i the fine $\mathcal{O}_1(K)$-module topology.*

1. *The topology on M equals the fine $\mathcal{O}_1(K)$-module topology on it.*
2. *The inclusions $L_i \to M$, for $i \in \mathbb{Z}$, are strict monomorphisms in* $\mathsf{STMod}\,\Bbbk$.
3. *Consider the direct system $\{L_{-j}\}_{j\in\mathbb{N}}$ in* $\mathsf{STMod}\,\Bbbk$. *Give $\lim_{j\to} L_{-j}$ the direct limit topology. Then the canonical bijection $\lim_{j\to} L_{-j} \to M$ is an isomorphism in* $\mathsf{STMod}\,\Bbbk$.
4. *The canonical surjections $L \to L/L_i$, for $i \in \mathbb{N}$, are strict epimorphisms in* $\mathsf{STMod}\,\Bbbk$.
5. *Let $\sigma_1 : \boldsymbol{k}_1(K) \to \mathcal{O}_1(K)$ be a lifting in* $\mathsf{STRing_c}\,\Bbbk$ *of the canonical surjection. Then for every $i \in \mathbb{N}$ the topology on L/L_i equals the fine $(\boldsymbol{k}_1(K), \sigma_1)$-module topology on it.*
6. *Consider the inverse system $\{L/L_i\}_{i\in\mathbb{N}}$ in* $\mathsf{STMod}\,\Bbbk$. *Give $\lim_{\leftarrow i}(L/L_i)$ the inverse limit topology. Then the canonical bijection $L \to \lim_{\leftarrow i}(L/L_i)$ is an isomorphism in* $\mathsf{STMod}\,\Bbbk$.

Proof. All these assertions become clear after we choose an $\mathcal{O}_1(K)$-linear isomorphism $L \cong \mathcal{O}_1(K)^r$ and a ST $\Bbbk$-ring isomorphism $\mathcal{O}_1(K) \cong \boldsymbol{k}_1(K)[[t]]$. See [Yekutieli 1992, Proposition 1.3.5]. □

Let K be a TLF of dimension $n \geq 1$ over $\Bbbk$. If $\boldsymbol{\sigma} = (\sigma_1, \dots, \sigma_n)$ is a system of liftings for K, then we write $\mathrm{d}_1(\boldsymbol{\sigma}) := (\sigma_2, \dots, \sigma_n)$. This is a system of liftings for the TLF $\boldsymbol{k}_1(K)$.

Definition 4.4. Let K be an n-dimensional TLF over $\Bbbk$, and let (M_1, M_2) be a pair of finite K-modules.

1. By a pair of $\mathcal{O}_1(K)$-lattices in (M_1, M_2) we mean a pair (L_1, L_2), where $L_i \in \operatorname{Lat}(M_i)$. The set of such pairs is denoted by $\operatorname{Lat}(M_1, M_2)$.
2. Let $\phi : M_1 \to M_2$ be a $\Bbbk$-linear homomorphism, and let (L_1, L_2), (L'_1, L'_2) be in $\operatorname{Lat}(M_1, M_2)$. We say that (L'_1, L'_2) is a *ϕ-refinement* of (L_1, L_2) if $L'_1 \subset L_1$, $L_2 \subset L'_2$, $\phi(L'_1) \subset L_2$ and $\phi(L_1) \subset L'_2$. In this case we write
$$(L'_1, L'_2) \prec_\phi (L_1, L_2),$$
and refer to it as a *ϕ-refinement* in $\operatorname{Lat}(M_1, M_2)$.

The relation $\prec_\phi$ is a partial ordering on $\operatorname{Lat}(M_1, M_2)$. If $(L'_1, L'_2) \prec_\phi (L_1, L_2)$, then there is an induced $\Bbbk$-linear homomorphism $\bar{\phi} : L_1/L'_1 \to L'_2/L_2$.

The next two definitions are variations of the original definitions in [Beilinson 1980], which are themselves generalizations to $n \geq 2$ of the definitions in [Tate 1968]. We saw similar definitions in the more recent papers [Osipov 2005; 2007; Braunling 2014a; 2014b]. The notation we use is close to that of Tate.

Definition 4.5. Let K be an n-dimensional TLF over $\Bbbk$, let $\boldsymbol{\sigma} = (\sigma_1, \dots, \sigma_n)$ be a system of liftings for K, and let (M_1, M_2) be a pair of finite K-modules. We define the subset

$$\mathrm{E}^{K}_{\boldsymbol{\sigma}}(M_1, M_2) \subset \operatorname{Hom}_{\Bbbk}(M_1, M_2)$$

as follows:

(1) If $n = 0$, any $\Bbbk$-linear homomorphism $\phi : M_1 \to M_2$ belongs to $\mathrm{E}^{K}_{\boldsymbol{\sigma}}(M_1, M_2)$.

(2) If $n \geq 1$, then a $\Bbbk$-linear homomorphism $\phi : M_1 \to M_2$ belongs to $\mathrm{E}^{K}_{\boldsymbol{\sigma}}(M_1, M_2)$ if it satisfies these two conditions:

  (i) Every $(L_1, L_2) \in \operatorname{Lat}(M_1, M_2)$ has some ϕ-refinement (L'_1, L'_2).

  (ii) For every ϕ-refinement $(L'_1, L'_2) \prec_\phi (L_1, L_2)$ in $\operatorname{Lat}(M_1, M_2)$ the induced homomorphism
  $$\bar{\phi} : L_1/L'_1 \to L'_2/L_2$$
  belongs to
  $$\mathrm{E}^{\boldsymbol{k}_1(K)}_{\mathrm{d}_1(\boldsymbol{\sigma})}(\operatorname{rest}_{\sigma_1}(L_1/L'_1), \operatorname{rest}_{\sigma_1}(L'_2/L_2)).$$

A homomorphism $\phi : M_1 \to M_2$ that belongs to $\mathrm{E}^{K}_{\boldsymbol{\sigma}}(M_1, M_2)$ is called a *local Beilinson–Tate operator* relative to $\boldsymbol{\sigma}$, or a BT operator for short.

Let K be a TLF over $\Bbbk$ of dimension at least 1. We denote by $\mathcal{O}_1(K)\|_{\mathfrak{m}_1(K)}$ the ST $\Bbbk$-ring which is the ring $\mathcal{O}_1(K)$ with its $\mathfrak{m}_1(K)$-adic topology. Given an $\mathcal{O}_1(K)$-module M, the fine $\mathcal{O}_1(K)\|_{\mathfrak{m}_1(K)}$-module topology on M is called the fine $\mathfrak{m}_1(K)$-adic topology. Now suppose $\phi : M_1 \to M_2$ is a $\Bbbk$-linear homomorphism. We say that ϕ is $\mathfrak{m}_1(K)$*-adically continuous* if it is continuous for the fine $\mathfrak{m}_1(K)$-adic topologies on M_1 and M_2.

Example 4.6. If $n = 1$ then the usual topology on $\mathcal{O}_1(K)$ equals the $\mathfrak{m}_1(K)$-adic topology. Thus K has the fine $\mathfrak{m}_1(K)$-adic topology. If $n > 1$ then the fine $\mathfrak{m}_1(K)$-adic topology is finer than, and not equal to, the usual topology on $\mathcal{O}_1(K)$ and K.

Lemma 4.7. *In the situation of Definition 4.5, the homomorphism $\phi : M_1 \to M_2$ satisfies condition* (2.i) *if and only if it is $\mathfrak{m}_1(K)$-adically continuous.*

Proof. Let $\bar{K}$ be the field $\boldsymbol{k}_1(K)$, but with the discrete topology. The lifting σ_1 induces an isomorphism of ST rings $\bar{K}[[t]] \xrightarrow{\simeq} \mathcal{O}_1(K)\|_{\mathfrak{m}_1(K)}$. Thus the field K, with the fine $\mathfrak{m}_1(K)$-adic topology, is isomorphic to $\bar{K}((t))$ as ST $\Bbbk$-rings. But we know that

$$\bar{K}((t)) \cong \Bigl(\prod_{i \geq 0} \bar{K} \cdot t^i\Bigr) \oplus \Bigl(\bigoplus_{i<0} \bar{K} \cdot t^i\Bigr)$$

as ST $\Bbbk$-modules, where $\bar{K} \cdot t^i \cong \bar{K}$ is discrete; cf. the proof of [Yekutieli 1992, Proposition 1.3.5]. It is now an exercise in quantifiers to compare t-adic continuity to condition (2.i). Cf. [Braunling 2014b, Remark 1 in Section 1.1], where this is also mentioned. □

Lemma 4.8. *In the situation of Definition 4.5, give M_1 and M_2 the fine K-module topologies. Then every $\phi \in \mathrm{E}^{K}_{\boldsymbol{\sigma}}(M_1, M_2)$ is continuous.*

Proof. The proof is by induction on n. For $n = 0$ there is nothing to prove, since these are discrete modules. So assume $n \geq 1$. (Actually for $n = 1$ this was proved in Lemma 4.7.) In view of Lemma 4.3, it suffices to prove that, for every $(L'_1, L'_2) \prec_{\phi} (L_1, L_2)$ in $\mathrm{Lat}(M_1, M_2)$, the induced homomorphism $\bar{\phi} : L_1/L'_1 \to L'_2/L_2$ is continuous. But $\bar{\phi}$ is a BT operator in dimension $n-1$, so by induction it is continuous. □

Lemma 4.9. *Let K be an n-dimensional TLF over $\Bbbk$, and let $\boldsymbol{\sigma}$ be a system of liftings for K. For $l = 1, 2, 3, 4$ let M_l be a finite K-module, and for $l = 1, 2, 3$ let $\phi_l : M_l \to M_{l+1}$ be a $\Bbbk$-linear homomorphism.*

1. *If ϕ_1 is K-linear then it is a BT operator.*
2. *If ϕ_1 and ϕ_2 are BT operators, then $\phi_2 \circ \phi_1$ is a BT operator.*
3. *Assume that ϕ_1 is surjective and K-linear, ϕ_3 is injective and K-linear, and $\phi_3 \circ \phi_2 \circ \phi_1$ is a BT operator. Then ϕ_2 is a BT operator.*

Here is a diagram depicting the situation:

$$\begin{tikzcd} M_1 \arrow[r, "\phi_1"] & M_2 \arrow[r, "\phi_2"] & M_3 \arrow[r, "\phi_3"] & M_4. \end{tikzcd}$$

Proof. We prove all three assertions by induction on n and on their sequential order. For $n = 0$ all assertions are trivial, so let us assume that $n \geq 1$. The conditions mentioned below are those in Definition 4.5.

(1) For this we assume that assertion (1) is true in dimension $n-1$. Condition (2.i), namely the $\mathfrak{m}_1(K)$-adic continuity of ϕ_1, is clear. Consider any ϕ-refinement $(L'_1, L'_2) \prec_{\phi_1} (L_1, L_2)$ in $\mathrm{Lat}(M_1, M_2)$. Since the induced homomorphism $\bar{\phi} : L_1/L'_1 \to L'_2/L_2$ is $\mathcal{O}_1(K)$-linear, it is also $(\boldsymbol{k}_1(K), \sigma_1)$-linear. By induction on n, $\bar{\phi}$ is a BT operator. So condition (2.ii) holds.

(2) Here we assume that assertions (2) and (3) are true in dimension $n-1$. Write $\psi := \phi_2 \circ \phi_1$. The $\mathfrak{m}_1(K)$-adic continuity of ψ, that is, condition (2.i), is clear. Consider any ψ-refinement $(L'_1, L'_3) \prec_{\psi} (L_1, L_3)$ in $\operatorname{Lat}(M_1, M_3)$. To satisfy condition (2.ii) we have to prove that $\bar{\psi} : L_1/L'_1 \to L'_3/L_3$ is a BT operator in dimension $n-1$. Let $L_2^{\diamondsuit} \in \operatorname{Lat}(M_2)$ be a lattice that contains $\phi_1(L_1)$, and let $L_3^{\diamondsuit} \in \operatorname{Lat}(M_3)$ be a lattice that contains both L'_3 and $\phi_2(L_2^{\diamondsuit})$. Let $L_2^{\heartsuit} \in \operatorname{Lat}(M_2)$ be a lattice that is contained in $L_2^{\diamondsuit}$. Let $L_1^{\heartsuit} \in \operatorname{Lat}(M_1)$ be such that $L_1^{\heartsuit} \subset L'_1$ and $\phi_1(L_1^{\heartsuit}) \subset L_2^{\heartsuit}$. All these choices are possible because condition (2.i) is satisfied by ϕ_1 and ϕ_2. Consider the commutative diagram

$$\begin{tikzcd}
\frac{L_1}{L_1^{\heartsuit}} \arrow[r, two heads, "\alpha"] \arrow[dr, "\bar{\phi}_1"'] & \frac{L_1}{L'_1} \arrow[r, "\bar{\psi}"] & \frac{L'_3}{L_3} \arrow[r, tail, "\beta"] & \frac{L_3^{\diamondsuit}}{L_3} \\
& \frac{L_2^{\diamondsuit}}{L_2^{\heartsuit}} \arrow[urr, "\bar{\phi}_2"'] & &
\end{tikzcd}$$

in $\mathsf{Mod}\,\Bbbk$. Since ϕ_1 and ϕ_2 are BT operators, condition (2.ii) says that $\bar{\phi}_1$ and $\bar{\phi}_2$ are BT operators (in dimension $n-1$). By part (2) the composition $\bar{\phi}_2 \circ \bar{\phi}_1$ is a BT operator. The homomorphisms α and β are $\boldsymbol{k}_1(K)$-linear. Therefore by part (3) the homomorphism $\bar{\psi}$ is a BT operator.

(3) For this we assume that assertions (1) and (2) are true in dimension n. Let $\psi := \phi_3 \circ \phi_2 \circ \phi_1$. Choose K-linear homomorphisms $\psi_1 : M_2 \to M_1$ and $\psi_3 : M_4 \to M_3$ that split ϕ_1 and ϕ_3 respectively. Then $\phi_2 = \psi_3 \circ \psi \circ \psi_1$. By assertions (1) and (2), we see that ϕ_2 is a BT operator. □

Lemma 4.10. *In the situation of Definition 4.5, the set* $\mathrm{E}^{K}_{\boldsymbol{\sigma}}(M_1, M_2)$ *is a* $\Bbbk$*-submodule of* $\operatorname{Hom}_{\Bbbk}(M_1, M_2)$.

Proof. The proof is by induction on n, and we can assume that $n \geq 1$. Take any $\phi_1, \phi_2 \in \mathrm{E}^{K}_{\boldsymbol{\sigma}}(M_1, M_2)$ and any $a \in \Bbbk$. Let $\psi := a \cdot \phi_1 + \phi_2$; we have to show that $\psi \in \mathrm{E}^{K}_{\boldsymbol{\sigma}}(M_1, M_2)$. Since condition (2.i) of Definition 4.5 is about $\mathfrak{m}_1(K)$-adic continuity (by Lemma 4.7), we see that ψ satisfies it.

We need to check condition (2.ii) of that definition. So let (L'_1, L'_2) be a ψ-refinement of (L_1, L_2). By $\mathfrak{m}_1(K)$-adic continuity there are lattices $L_1^{\diamondsuit} \subset L'_1$ and $L'_2 \subset L_2^{\diamondsuit}$ such that $\phi_i(L_1^{\diamondsuit}) \subset L_2$ and $\phi_i(L_1) \subset L_2^{\diamondsuit}$. Consider the commutative diagram

$$\begin{tikzcd}
\frac{L_1}{L_1^{\diamondsuit}} \arrow[r, two heads, "\alpha"] \arrow[rrr, bend right, "a \cdot \bar{\phi}_1 + \bar{\phi}_2"'] & \frac{L_1}{L'_1} \arrow[r, "\bar{\psi}"] & \frac{L'_2}{L_2} \arrow[r, tail, "\beta"] & \frac{L_2^{\diamondsuit}}{L_2}
\end{tikzcd}$$

in $\operatorname{Mod} \mathbb{k}$. The induction hypothesis tells us that $a \cdot \bar{\phi}_1 + \bar{\phi}_2$ is a BT operator. The homomorphisms α and β are $\boldsymbol{k}_1(K)$-linear. Therefore, according to Lemma 4.9(3), the homomorphism $\bar{\psi}$ is a BT operator. □

Lemma 4.11. *Let K be an n-dimensional TLF over $\mathbb{k}$, let $\boldsymbol{\sigma}$ be a system of liftings for K, and let (M_1, M_2) be a pair of finite K-modules. Then*

$$\operatorname{Diff}^{\text{cont}}_{K/\mathbb{k}}(M_1, M_2) \subset \mathrm{E}^K_{\boldsymbol{\sigma}}(M_1, M_2).$$

Proof. We use induction on n. For $n = 0$ there is nothing to prove, so let's assume that $n \geq 1$. (Actually, for $n = 1$ there is nothing to prove either; see Example 4.12.)

Let $\phi : M_1 \to M_2$ be a continuous differential operator. Choose K-linear isomorphisms $M_l \cong K^{r_l}$ for $l = 1, 2$; so we may view ϕ as a matrix $[\phi_{i,j}]$ in $\operatorname{Mat}_{r_2 \times r_1}(\mathcal{D}^{\text{cont}}_{K/\mathbb{k}})$. According to (1) and (2) of Lemma 4.9, it suffices to prove that each $\phi_{i,j}$ is a BT operator. Therefore we can assume that $M_1 = M_2 = K$ and $\phi \in \mathcal{D}^{\text{cont}}_{K/\mathbb{k}}$.

Choose a uniformizer $a \in \mathcal{O}_1(K)$. If $\operatorname{char}(\mathbb{k}) = 0$ then by formula (2-5) there is an integer d, depending on the coefficients of the operator ϕ in that expansion, such that $\phi(a^i \cdot \mathcal{O}_1(K)) \subset a^{i-d} \cdot \mathcal{O}_1(K)$ for all i. Hence ϕ is $\mathfrak{m}_1(K)$-adically continuous.

If $\operatorname{char}(\mathbb{k}) = p > 0$, then by [Yekutieli 1992, Theorem 1.4.9] the operator ϕ is linear over the subfield $K' := \mathbb{k} \cdot K^{p^d} \subset K$ for a sufficiently large natural number d. The field K' is also an n-dimensional TLF, $K' \to K$ is a morphism of TLFs, and $\mathcal{O}_1(K') \to \mathcal{O}_1(K)$ is a finite homomorphism. So the $\mathfrak{m}_1(K)$-adic topology on $\mathcal{O}_1(K)$ coincides with its $\mathfrak{m}_1(K')$-adic topology. Since ϕ is $\mathcal{O}_1(K')$-linear, it follows that ϕ is $\mathfrak{m}_1(K')$-adically continuous. Using Lemma 4.7, we see that in both cases ($\operatorname{char}(\mathbb{k}) = 0$ and $\operatorname{char}(\mathbb{k}) > 0$) condition (2.i) of Definition 4.5 holds.

Now take a ϕ-refinement $(L'_1, L'_2) \prec_\phi (L_1, L_2)$ in $\operatorname{Lat}(M_1, M_2)$. Write $\bar{M}_1 := \operatorname{rest}_{\sigma_1}(L_1/L'_1)$ and $\bar{M}_2 := \operatorname{rest}_{\sigma_1}(L'_2/L_2)$. We must prove that $\bar{\phi} : \bar{M}_1 \to \bar{M}_2$ is a BT operator between these $\boldsymbol{k}_1(K)$-modules. We know that $\bar{\phi}$ is a differential operator over $\mathcal{O}_1(K)$, and therefore it is also a differential operator over $\boldsymbol{k}_1(K)$. Choose some $\boldsymbol{k}_1(K)$-linear isomorphisms $\psi_l : \boldsymbol{k}_1(K)^{r_l} \xrightarrow{\simeq} \bar{M}_l$. Then

$$\psi := \psi_2^{-1} \circ \bar{\phi} \circ \psi_1 : \boldsymbol{k}_1(K)^{r_1} \to \boldsymbol{k}_1(K)^{r_2}$$

is a differential operator over $\boldsymbol{k}_1(K)$. By the induction hypothesis, ψ is a BT operator. Finally, by (1) and (2) of Lemma 4.9, the homomorphism $\bar{\phi} = \psi_2 \circ \psi \circ \psi_1^{-1}$ is a BT operator. □

Example 4.12. If $n = 0$, then by definition

$$\mathrm{E}^K_{\boldsymbol{\sigma}}(M_1, M_2) = \operatorname{Hom}_{\mathbb{k}}(M_1, M_2).$$

This is a finite $\mathbb{k}$-module.

If $n = 1$ then condition (2.ii) of Definition 4.5 is trivially satisfied. Lemma 4.7 and Example 4.12 show that

$$\mathrm{E}_{\boldsymbol{\sigma}}^{K}(M_1, M_2) = \mathrm{Hom}_{\Bbbk}^{\mathrm{cont}}(M_1, M_2),$$

the module of continuous $\Bbbk$-linear homomorphisms. This was already noticed in [Osipov 2005; 2007; Braunling 2014b, Section 1.1].

The equalities above indicate that the choice of $\boldsymbol{\sigma}$ is irrelevant. However in dimensions 0 and 1 there is only one lifting, so in fact there is no news here. Later, in Theorem 4.20, we will prove that in any dimension the system of liftings $\boldsymbol{\sigma}$ is not relevant.

Example 4.13. For $n \geq 2$ the inclusion

$$\mathrm{E}_{\boldsymbol{\sigma}}^{K}(M_1, M_2) \subset \mathrm{Hom}_{\Bbbk}^{\mathrm{cont}}(M_1, M_2)$$

is usually proper (i.e., it is not an equality). Here is a calculation demonstrating this: Let $K := \Bbbk((t_1, t_2))$, the standard TLF with its standard system of liftings $\boldsymbol{\sigma}$. Take $M_1 = M_2 := K$. Any $a \in K$ is a series $a = \sum_{i \in \mathbb{Z}} a_i(t_2) \cdot t_1^i$, where $a_i(t_2) \in \Bbbk((t_2))$ and $a_i(t_2) = 0$ for $i \ll 0$. We let $\psi \in \mathrm{End}_{\Bbbk}(K)$ be

$$\psi\biggl(\sum_{i \in \mathbb{Z}} a_i(t_2) \cdot t_1^i\biggr) := a_0(t_1).$$

To see that this is continuous we use the continuous decomposition

$$K = \Bbbk((t_2))((t_1)) \cong \Bbbk((t_2))[[t_1]] \oplus \biggl(\bigoplus_{i<0} \Bbbk((t_2)) \cdot t_1^i\biggr).$$

This gives a continuous function $\psi_1 : K \to \Bbbk((t_2))$, sending $\sum_{i \in \mathbb{Z}} a_i(t_2) \cdot t_1^i$ to $a_0(t_2)$. Next there is an isomorphism $\psi_2 : \Bbbk((t_2)) \to \Bbbk((t_1))$, $a_0(t_2) \mapsto a_0(t_1)$. Finally the inclusion $\psi_3 : \Bbbk((t_1)) \to \Bbbk((t_2))((t_1))$ is continuous. The function ψ is $\psi = \psi_3 \circ \psi_2 \circ \psi_1$, so it is continuous.

Take the standard lattices $L_i = t_1^i \cdot \Bbbk((t_2))[[t_1]]$ in K. For every j the element $a_j := t_2^j$ belongs to L_0, yet the element $\psi(a_j) = t_1^j$ does not belong to L_{j+1}. Thus $\psi(L_0)$ is not contained in any lattice, and requirement (2.i) of Definition 4.5 is violated, so ψ does not belong to $\mathrm{E}_{\boldsymbol{\sigma}}^{K}(K, K)$.

Recall that for an n-dimensional TLF K, with $n \geq 2$, and a system of liftings $\boldsymbol{\sigma} = (\sigma_1, \dots, \sigma_n)$, the truncation $\mathrm{d}_1(\boldsymbol{\sigma}) = (\sigma_2, \dots, \sigma_n)$ is a system of liftings for the first residue field $\boldsymbol{k}_1(K)$.

Definition 4.14. Let K be a TLF over $\Bbbk$ of dimension $n \geq 1$, let $\boldsymbol{\sigma} = (\sigma_1, \dots, \sigma_n)$ be a system of liftings for K, and let (M_1, M_2) be a pair of finite K-modules. For integers $i \in \{1, \dots, n\}$ and $j \in \{1, 2\}$, we define the subset

$$\mathrm{E}^{K}_{\boldsymbol{\sigma}}(M_1, M_2)_{i,j} \subset \mathrm{E}^{K}_{\boldsymbol{\sigma}}(M_1, M_2)$$

to be the set of BT operators $\phi : M_1 \to M_2$ that satisfy the conditions:

(i) The operator ϕ belongs to $\mathrm{E}^{K}_{\boldsymbol{\sigma}}(M_1, M_2)_{1,1}$ if there exists some $L_2 \in \mathrm{Lat}(M_2)$ such that $\phi(M_1) \subset L_2$.

(ii) The operator ϕ belongs to $\mathrm{E}^{K}_{\boldsymbol{\sigma}}(M_1, M_2)_{1,2}$ if there exists some $L_1 \in \mathrm{Lat}(M_1)$ such that $\phi(L_1) = 0$.

(iii) Let $n \geq 2$. For $i \in \{2, \dots, n\}$ and $j \in \{1, 2\}$, the operator ϕ belongs to $\mathrm{E}^{K}_{\boldsymbol{\sigma}}(M_1, M_2)_{i,j}$ if for any ϕ-refinement $(L'_1, L'_2) \prec_{\phi} (L_1, L_2)$ in $\mathrm{Lat}(M_1, M_2)$ the induced homomorphism

$$\bar{\phi} : L_1/L'_1 \to L'_2/L_2$$

belongs to

$$\mathrm{E}^{\boldsymbol{k}_1(K)}_{\mathrm{d}_1(\boldsymbol{\sigma})}(\mathrm{rest}_{\sigma_1}(L_1/L'_1), \mathrm{rest}_{\sigma_1}(L'_2/L_2))_{i-1,j}.$$

Definition 4.15. Let K be an n-dimensional TLF over $\Bbbk$, and let $\boldsymbol{\sigma}$ be a system of liftings for K. We define

$$\mathrm{E}_{\boldsymbol{\sigma}}(K) := \mathrm{E}^{K}_{\boldsymbol{\sigma}}(K, K).$$

If $n \geq 1$ we define

$$\mathrm{E}_{\boldsymbol{\sigma}}(K)_{i,j} := \mathrm{E}^{K}_{\boldsymbol{\sigma}}(K, K)_{i,j}.$$

Lemma 4.16. *Let K be an n-dimensional TLF over $\Bbbk$, with $n \geq 1$, and let $\boldsymbol{\sigma}$ be a system of liftings for K. For $l = 1, 2, 3, 4$ let M_l be a finite K-module, and for $l = 1, 2, 3$ let $\phi_l \in \mathrm{E}^{K}_{\boldsymbol{\sigma}}(M_l, M_{l+1})$. Take any $j \in \{1, 2\}$ and $i \in \{1, \dots, n\}$.*

(1) *The set $\mathrm{E}^{K}_{\boldsymbol{\sigma}}(M_1, M_2)_{i,j}$ is a $\Bbbk$-submodule of $\mathrm{E}^{K}_{\boldsymbol{\sigma}}(M_1, M_2)$.*

(2) *If $\phi_2 \in \mathrm{E}^{K}_{\boldsymbol{\sigma}}(M_2, M_3)_{i,j}$, then $\phi_3 \circ \phi_2 \circ \phi_1 \in \mathrm{E}^{K}_{\boldsymbol{\sigma}}(M_1, M_4)_{i,j}$.*

(3) *Assume that ϕ_1 is surjective and K-linear, ϕ_3 is injective and K-linear, and $\phi_3 \circ \phi_2 \circ \phi_1 \in \mathrm{E}^{K}_{\boldsymbol{\sigma}}(M_1, M_4)_{i,j}$. Then $\phi_2 \in \mathrm{E}^{K}_{\boldsymbol{\sigma}}(M_2, M_3)_{i,j}$.*

Proof. We use induction on n and on the sequential order of the assertions.

(1) For $i = 1$ this is clear. Now assume $i \geq 2$ (and hence also $n \geq 2$). For this we use the same strategy as in the proof of Lemma 4.10. We are allowed to make use of assertion (3) in dimension $n - 1$.

(2) For $i = 1$ this is clear. Now assume $i \geq 2$ (and hence also $n \geq 2$). Here we use the same proof as of Lemma 4.9(2), relying on assertions (2) and (3) in dimension $n - 1$.

(3) Same as the proof of Lemma 4.9(3). We rely on assertion (2) in dimension n. □

Lemma 4.17. *Let K be an n-dimensional TLF over $\Bbbk$, with $n \geq 1$, and let $\boldsymbol{\sigma}$ be a system of liftings for K. Let M_1 and M_2 be finite K-modules. For any i there is the equality*

$$\mathrm{E}^K_{\boldsymbol{\sigma}}(M_1, M_2) = \mathrm{E}^K_{\boldsymbol{\sigma}}(M_1, M_2)_{i,1} + \mathrm{E}^K_{\boldsymbol{\sigma}}(M_1, M_2)_{i,2}.$$

Proof. For $i = 1$ this is clear. (It is Tate's original observation [1968].)

Assume $i \geq 2$ (and hence also $n \geq 2$). For this we use induction on n. Choose K-linear isomorphisms $K^{r_l} \cong M_l$ for $l = 1, 2$. According to Lemmas 4.9 and 4.16 there are $\Bbbk$-linear isomorphisms

$$\mathrm{E}^K_{\boldsymbol{\sigma}}(M_1, M_2) \cong \mathrm{Mat}_{r_2 \times r_1}(\mathrm{E}_{\boldsymbol{\sigma}}(K))$$

and

$$\mathrm{E}^K_{\boldsymbol{\sigma}}(M_1, M_2)_{i,j} \cong \mathrm{Mat}_{r_2 \times r_1}(\mathrm{E}_{\boldsymbol{\sigma}}(K)_{i,j}).$$

Therefore we can assume that $M_1 = M_2 = K$.

The induction hypothesis says that the identity automorphism $\mathbf{1}_{\boldsymbol{k}_1(K)}$ of the TLF $\boldsymbol{k}_1(K)$ is a sum $\mathbf{1}_{\boldsymbol{k}_1(K)} = \bar{\phi}_1 + \bar{\phi}_2$, where $\bar{\phi}_j \in \mathrm{E}_{\mathrm{d}_1(\boldsymbol{\sigma})}(\boldsymbol{k}_1(K))_{i-1,j}$. Choose a uniformizer $a \in \mathcal{O}_1(K)$. Any element of K has a unique expansion as a series $\sum_{q \in \mathbb{Z}} \sigma_1(b_q) \cdot a^q$, where $b_q \in \boldsymbol{k}_1(K)$ and $b_q = 0$ for $q \ll 0$. Define $\phi_j \in \mathrm{End}_{\Bbbk}(K)$ by the formula

$$\phi_j\Bigl(\sum_{q \in \mathbb{Z}} \sigma_1(b_q) \cdot a^q\Bigr) := \sum_{q \in \mathbb{Z}} \sigma_1(\bar{\phi}_j(b_q)) \cdot a^q.$$

A little calculation shows that $\phi_j \in \mathrm{E}_{\boldsymbol{\sigma}}(K)_{i,j}$; and clearly $\phi_1 + \phi_2 = \mathbf{1}_K$. □

Definition 4.18 [Tate 1968]. Let M be a $\Bbbk$-module. An operator $\phi \in \mathrm{End}_{\Bbbk}(M)$ is called *finite potent* if, for some positive integer q, the operator ϕ^q has finite rank, i.e., the $\Bbbk$-module $\phi^q(M)$ is finite.

Lemma 4.19. *Let K be a TLF over $\Bbbk$ of dimension $n \geq 1$, let $\boldsymbol{\sigma}$ be a system of liftings for K, and let M be a finite K-module. Then any operator*

$$\phi \in \bigcap_{\substack{i=1,\dots,n \\ j=1,2}} \mathrm{E}^K_{\boldsymbol{\sigma}}(M, M)_{i,j}$$

is finite potent.

Proof. The proof is by induction on n. (For $n = 1$ this is Tate's original observation.)

Since $\phi \in \mathrm{E}^K_{\boldsymbol{\sigma}}(M, M)_{1,1}$, there is a lattice $L_2 \in \mathrm{Lat}(M)$ such that $\phi(M) \subset L_2$. Since $\phi \in \mathrm{E}^K_{\boldsymbol{\sigma}}(M, M)_{1,2}$, there is a lattice $L_1 \in \mathrm{Lat}(M)$ such that $\phi(L_1) = 0$. After replacing L_1 by a smaller lattice, we can assume that $L_1 \subset L_2$. Consider the commutative diagram

$$\begin{tikzcd}
0 \arrow[r, "\subset"] \arrow[d, "\phi"'] & L_1 \arrow[r, "\subset"] \arrow[d, "\phi"'] \arrow[dl, "\phi"'] & L_2 \arrow[r, "\subset"] \arrow[d, "\phi"'] & M \arrow[d, "\phi"'] \arrow[dl, "\phi"'] \\
0 \arrow[r, "\subset"'] & L_1 \arrow[r, "\subset"'] & L_2 \arrow[r, "\subset"'] & M
\end{tikzcd}$$

in $\operatorname{Mod} \Bbbk$. Define $\bar{M} := L_2/L_1$. If we can prove that the induced homomorphism $\bar{\phi} : \bar{M} \to \bar{M}$ is finite potent, then it will follow, by a simple linear algebra argument based on the diagram above, that ϕ is finite potent.

If $n = 1$ then $\bar{M}$ is finite over $\Bbbk$, so we are done. If $n \geq 2$, then by definition

$$\bar{\phi} \in \bigcap_{\substack{i=1,\dots,n-1 \\ j=1,2}} \mathrm{E}^{K}_{\mathrm{d}_1(\boldsymbol{\sigma})}(\bar{M}, \bar{M})_{i,j}.$$

The induction hypothesis says that $\bar{\phi}$ is finite potent. □

Theorem 4.20. *Let K be an n-dimensional TLF over $\Bbbk$, and let (M_1, M_2) be a pair of finite K-modules. Suppose $\boldsymbol{\sigma}$ and $\boldsymbol{\sigma}'$ are two systems of liftings for K.*

(1) *There is equality*

$$\mathrm{E}^{K}_{\boldsymbol{\sigma}}(M_1, M_2) = \mathrm{E}^{K}_{\boldsymbol{\sigma}'}(M_1, M_2)$$

inside $\operatorname{Hom}_{\Bbbk}(M_1, M_2)$

(2) *If $n \geq 1$, there is equality*

$$\mathrm{E}^{K}_{\boldsymbol{\sigma}}(M_1, M_2)_{i,j} = \mathrm{E}^{K}_{\boldsymbol{\sigma}'}(M_1, M_2)_{i,j}$$

for all $i = 1, \dots, n$ and $j = 1, 2$.

Proof. (1) By symmetry it is enough to prove the inclusion "$\subset$". The proof is by induction on n. For $n = 0$ there is nothing to prove.

Now assume $n \geq 1$. Let $\phi \in \mathrm{E}^{K}_{\boldsymbol{\sigma}}(M_1, M_2)$. We have to prove that ϕ is in $\mathrm{E}^{K}_{\boldsymbol{\sigma}'}(M_1, M_2)$. Since condition (2.i) of Definition 4.5 does not involve the liftings, there is nothing to check.

Next we consider condition (2.ii). Take some ϕ-refinement $(L'_1, L'_2) \prec_{\phi} (L_1, L_2)$ in $\operatorname{Lat}(M_1, M_2)$. Define $\bar{M}_1 := L_1/L'_1$ and $\bar{M}_2 := L'_2/L_2$, and let $\bar{\phi} : \bar{M}_1 \to \bar{M}_2$ be the induced homomorphism. Let us write $\bar{K} := \boldsymbol{k}_1(K)$, $\bar{\boldsymbol{\sigma}} := \mathrm{d}_1(\boldsymbol{\sigma})$ and $\bar{\boldsymbol{\sigma}}' := \mathrm{d}_1(\boldsymbol{\sigma}')$. We know that

$$\bar{\phi} \in \mathrm{E}^{\bar{K}}_{\bar{\boldsymbol{\sigma}}}(\operatorname{rest}_{\sigma_1}(\bar{M}_1), \operatorname{rest}_{\sigma_1}(\bar{M}_2)). \tag{4-21}$$

The induction hypothesis says that $\mathrm{E}_{\bar{\boldsymbol{\sigma}}}(\bar{K}) = \mathrm{E}_{\bar{\boldsymbol{\sigma}}'}(\bar{K})$.

Choose $\bar{K}$-linear isomorphisms $\chi_l : \bar{K}^{r_l} \xrightarrow{\simeq} \operatorname{rest}_{\sigma_1}(\bar{M}_l)$ and $\chi'_l : \bar{K}^{r_l} \xrightarrow{\simeq} \operatorname{rest}_{\sigma'_1}(\bar{M}_l)$. This gives rise to a commutative diagram

$$\begin{tikzcd}
\bar{M}_1 \arrow[r, "="] & \bar{M}_1 \arrow[r, "\bar{\phi}"] & \bar{M}_2 \arrow[r, "="] & \bar{M}_2 \\
\bar{K}^{r_1} \arrow[u, "\chi'_1"'] \arrow[r, "\psi_1"] & \bar{K}^{r_1} \arrow[u, "\chi_1"'] \arrow[r, "\psi"] & \bar{K}^{r_2} \arrow[u, "\chi_2"'] \arrow[r, "\psi_2"] & \bar{K}^{r_2} \arrow[u, "\chi'_2"']
\end{tikzcd}$$

in Mod $\Bbbk$. According to formula (4-21) and Lemma 4.9, the operator ψ is in $\operatorname{Mat}_{r_2 \times r_1}(\mathrm{E}_{\bar{\sigma}}(\bar{K}))$. Combining Lemma 3.14 and Theorem 2.8 we see that the operators ψ_l belong to $\mathrm{GL}_{r_l}(\mathcal{D}^{\mathrm{cont}}_{\bar{K}/\Bbbk})$. Therefore, by Lemma 4.11, $\psi_l \in \mathrm{GL}_{r_l}(\mathrm{E}_{\bar{\sigma}}(\bar{K}))$. We conclude that $\psi' := \psi_2 \circ \psi \circ \psi_1$ is in

$$\operatorname{Mat}_{r_2 \times r_1}(\mathrm{E}_{\bar{\sigma}}(\bar{K})) = \operatorname{Mat}_{r_2 \times r_1}(\mathrm{E}_{\bar{\sigma}'}(\bar{K})).$$

So by Lemma 4.9 we have

$$\bar{\phi} = \chi'_2 \circ \psi' \circ \chi'^{-1}_1 \in \mathrm{E}^{\bar{K}}_{\bar{\sigma}'}(\operatorname{rest}_{\sigma'_1}(\bar{M}_1), \operatorname{rest}_{\sigma'_1}(\bar{M}_2)).$$

This is what we had to prove.

(2) Again we only prove the inclusion "$\subset$", and the proof is by induction on n. For $i = 1$ the conditions do not involve the liftings, so there is nothing to check. Now consider $i \geq 2$ (and hence $n \geq 2$). We assume that the theorem is true for dimension $n-1$. Take some $\phi \in \mathrm{E}^{K}_{\boldsymbol{\sigma}}(M_1, M_2)_{i,j}$, and let $(L'_1, L'_2) \prec_{\phi} (L_1, L_2)$ be a ϕ-refinement in $\operatorname{Lat}(M_1, M_2)$. In the notation of the proof of part (1) above, the operator ψ is inside $\operatorname{Mat}_{r_2 \times r_1}(\mathrm{E}_{\bar{\sigma}}(\bar{K})_{i,j})$. This is because

$$\bar{\phi} \in \mathrm{E}^{\bar{K}}_{\bar{\sigma}}(\operatorname{rest}_{\sigma_1}(\bar{M}_1), \operatorname{rest}_{\sigma_1}(\bar{M}_2))_{i,j},$$

and $\mathrm{E}_{\bar{\sigma}}(\bar{K})_{i,j}$ is a two-sided ideal in the ring $\mathrm{E}_{\bar{\sigma}}(\bar{K})$. The induction hypothesis tells us that $\mathrm{E}_{\bar{\sigma}}(\bar{K})_{i,j} = \mathrm{E}_{\bar{\sigma}'}(\bar{K})_{i,j}$. Therefore the same calculations as above yield

$$\bar{\phi} \in \mathrm{E}^{\bar{K}}_{\bar{\sigma}'}(\operatorname{rest}_{\sigma'_1}(\bar{M}_1), \operatorname{rest}_{\sigma'_1}(\bar{M}_2))_{i,j}$$

as required. □

Taking $M_1 = M_2 := K$ in the theorem we obtain:

Corollary 4.22. *Let K be an n-dimensional TLF over $\Bbbk$, and let $\boldsymbol{\sigma}$ and $\boldsymbol{\sigma}'$ be two systems of liftings for K. Then $\mathrm{E}_{\boldsymbol{\sigma}}(K) = \mathrm{E}_{\boldsymbol{\sigma}'}(K)$. If $n \geq 1$ then $\mathrm{E}_{\boldsymbol{\sigma}}(K)_{i,j} = \mathrm{E}_{\boldsymbol{\sigma}'}(K)_{i,j}$ for all i, j.*

The corollary justifies the next definition.

Definition 4.23. Let K be an n-dimensional TLF over $\Bbbk$.

(1) We define

$$\mathrm{E}(K) := \mathrm{E}_{\boldsymbol{\sigma}}(K),$$

where $\boldsymbol{\sigma}$ is any system of liftings for K. Elements of $\mathrm{E}(K)$ are called *local Beilinson–Tate operators* on K.

(2) Assume $n \geq 1$. For $i \in \{1, \dots, n\}$ and $j \in \{1, 2\}$ we define

$$\mathrm{E}(K)_{i,j} := \mathrm{E}^{K}_{\boldsymbol{\sigma}}(K, K)_{i,j},$$

where $\boldsymbol{\sigma}$ is any system of liftings for K.

Of course, when $n = 0$ we have $\mathrm{E}(K) = \mathrm{End}_{\Bbbk}(K)$, which is not interesting. The next theorem summarizes what we know about BT operators in dimensions 1 and above. Recall the notion of an n-dimensional cubically decomposed ring of operators on a commutative $\Bbbk$-ring A, from Definition 0.3.

Theorem 4.24. *Let K be an n-dimensional TLF over $\Bbbk$, with $n \geq 1$.*

(1) *The ring of BT operators $\mathrm{E}(K)$, with its collection of ideals $\{\mathrm{E}(K)_{i,j}\}$, is an n-dimensional cubically decomposed ring of operators on K.*

(2) *There are inclusions of rings*

$$K \subset \mathcal{D}^{\mathrm{cont}}_{K/\Bbbk} \subset \mathrm{E}(K) \subset \mathrm{End}^{\mathrm{cont}}_{\Bbbk}(K) \subset \mathrm{End}_{\Bbbk}(K).$$

Proof. Assertion (1) is a combination of Lemmas 4.16, 4.17 and 4.19. Assertion (2) is a combination of Lemmas 4.9, 4.10 and 4.11. □

Remark 4.25. It would be good to have a structural understanding of the objects $\mathrm{E}(K)$ and $\mathrm{E}(K)_{i,j}$ associated to a TLF K. For instance, does $\mathrm{E}(K)$ carry a canonical structure of an ST ring, or perhaps some "higher semi-topological structure"? Such a structure could help in proving Conjecture 5.7.

Remark 4.26. Osipov [2007] introduced the categories C_n, $n \in \mathbb{N}$, that fiber over $\mathsf{Mod}\,\Bbbk$. These categories are defined inductively, in a way that closely resembles Beilinson's definitions [1980]. The paper [Braunling et al. 2014] introduced the categories Tate_n of *n-Tate spaces*, also fibered over $\mathsf{Mod}\,\Bbbk$. Presumably these two concepts coincide.

Let K be an n-dimensional TLF over $\Bbbk$. It seems likely that K should have a canonical C_n-structure, or a canonical Tate_n-structure. Moreover, the subrings $\mathrm{End}_{\mathsf{C}_n}(K)$, $\mathrm{End}_{\mathsf{Tate}_n}(K)$ and $\mathrm{E}(K)$ of $\mathrm{End}_{\Bbbk}(K)$ should coincide.

If that is the case, then some of our statements above become similar or equivalent to some results in [Osipov 2007]. For instance, our Lemma 4.8 corresponds to [Osipov 2007, Proposition 3].

5. Residues

In this section we provide background for Conjecture 0.9 in the Introduction. The base ring $\Bbbk$ is a perfect field, and it has the discrete topology.

Recall the way the DG ring of separated differential forms $\Omega^{\mathrm{sep}}_{A/\Bbbk} = \bigoplus_{i \geq 0} \Omega^{i,\mathrm{sep}}_{A/\Bbbk}$ was defined in Section 2 for any commutative ST $\Bbbk$-ring A. The usual module of Kähler differentials $\Omega^{i}_{A/\Bbbk}$ is a ST $\Bbbk$-module, with topology induced from the surjection $\mathrm{T}^{i+1}_{\Bbbk}(A) \twoheadrightarrow \Omega^{i}_{A/\Bbbk}$. Then $\Omega^{i,\mathrm{sep}}_{A/\Bbbk} := (\Omega^{i}_{A/\Bbbk})^{\mathrm{sep}}$ is the associated separated ST module. In degree 0 we have $\Omega^{0,\mathrm{sep}}_{A/\Bbbk} = A^{\mathrm{sep}}$. There is a canonical surjection of DG ST $\Bbbk$-rings

$$\tau_A : \Omega_{A/\Bbbk} \twoheadrightarrow \Omega^{\mathrm{sep}}_{A/\Bbbk}, \tag{5-1}$$

which is a topological strict epimorphism. Given any homomorphism $f : A \to B$ in the category $\mathsf{STRing_c}\,\Bbbk$, there is an induced commutative diagram of DG ST $\Bbbk$-rings

$$\begin{tikzcd}
\Omega_{A/\Bbbk} \arrow[r, "\Omega(f)"] \arrow[d, two heads, "\tau_A"'] & \Omega_{B/\Bbbk} \arrow[d, two heads, "\tau_B"] \\
\Omega^{\mathrm{sep}}_{A/\Bbbk} \arrow[r, "\Omega^{\mathrm{sep}}(f)"] & \Omega^{\mathrm{sep}}_{B/\Bbbk}
\end{tikzcd}$$

Let K be an n-dimensional TLF over $\Bbbk$, with its DG ST ring of separated differential forms $\Omega^{\mathrm{sep}}_{K/\Bbbk} = \bigoplus_{i=0}^{n} \Omega^{i,\mathrm{sep}}_{K/\Bbbk}$. In degree 0 we have $\Omega^{0,\mathrm{sep}}_{K/\Bbbk} = K$, since K is separated (in fact it is a complete ST $\Bbbk$-module). In degree n the K-module $\Omega^{n,\mathrm{sep}}_{K/\Bbbk}$ is free of rank 1 with the fine K-module topology. If $\boldsymbol{a} = (a_1, \dots, a_n)$ is a system of uniformizers for K, then the element

$$\mathrm{dlog}(\boldsymbol{a}) := a_1^{-1} \cdot \mathrm{d}(a_1) \cdots a_n^{-1} \cdot \mathrm{d}(a_n) \tag{5-2}$$

is a basis of $\Omega^{n,\mathrm{sep}}_{K/\Bbbk}$. See Theorem 3.16 and Example 2.16.

There is a theory of trace homomorphisms for separated differential forms. For any morphism $f : K \to L$ in $\mathsf{TLF}^n\,\Bbbk$, there is a homomorphism

$$\mathrm{Tr}^{\mathrm{TLF}}_{L/K} : \Omega^{\mathrm{sep}}_{L/\Bbbk} \to \Omega^{\mathrm{sep}}_{K/\Bbbk}. \tag{5-3}$$

This is a degree 0 homomorphism of DG ST $\Omega^{\mathrm{sep}}_{K/\Bbbk}$-modules. It is uniquely characterized by these properties: it is functorial; in degree 0 it coincides with the usual trace $\mathrm{tr}_{L/K} : L \to K$; and

$$\mathrm{Tr}^{\mathrm{TLF}}_{L/K} \circ \mathrm{dlog} = \mathrm{dlog} \circ \mathrm{n}_{L/K}$$

as functions $L^{\times} \to \Omega^{1,\mathrm{sep}}_{K/\Bbbk}$, where $\mathrm{n}_{L/K} : L^{\times} \to K^{\times}$ is the usual norm. The homomorphism $\mathrm{Tr}^{\mathrm{TLF}}_{L/K}$ is nondegenerate in top degree, in the sense that the induced homomorphism

$$\Omega^{n,\mathrm{sep}}_{L/\Bbbk} \to \mathrm{Hom}_K(L, \Omega^{n,\mathrm{sep}}_{K/\Bbbk})$$

is bijective. See [Yekutieli 1992, Section 2.3].

In [Yekutieli 1992, Section 2.4] we introduced the residue functional for TLFs. Its properties are summarized in the following theorem:

Theorem 5.4 [Yekutieli 1992]. *Let K be an n-dimensional TLF over $\Bbbk$. There is a $\Bbbk$-linear homomorphism*

$$\mathrm{Res}^{\mathrm{TLF}}_{K/\Bbbk} : \Omega^{n,\mathrm{sep}}_{K/\Bbbk} \to \Bbbk$$

with these properties:

(1) *Continuity*: *the homomorphism* $\mathrm{Res}^{\mathrm{TLF}}_{K/\Bbbk}$ *is continuous.*

(2) *Uniformization*: *let $\boldsymbol{a} = (a_1, \dots, a_n)$ be a system of uniformizers for K, and let $\Bbbk' \to \mathcal{O}(K)$ be the unique $\Bbbk$-ring lifting of the last residue field $\Bbbk' := \boldsymbol{k}_n(K)$ into the ring of integers $\mathcal{O}(K)$ of K. Then, for any $b \in \Bbbk'$ and any $i_1, \dots, i_n \in \mathbb{Z}$, we have*

$$\mathrm{Res}^{\mathrm{TLF}}_{K/\Bbbk}(b \cdot a_1^{i_1} \cdots a_n^{i_n} \cdot \mathrm{dlog}(\boldsymbol{a})) = \begin{cases} \mathrm{tr}_{\Bbbk'/\Bbbk}(b) & \text{if } i_1 = \cdots = i_n = 0, \\ 0 & \text{otherwise.} \end{cases}$$

(3) *Functoriality*: *let $f : K \to L$ be a morphism in the category* $\mathsf{TLF}^n\,\Bbbk$. *Then*

$$\mathrm{Res}^{\mathrm{TLF}}_{L/\Bbbk} = \mathrm{Res}^{\mathrm{TLF}}_{K/\Bbbk} \circ \mathrm{Tr}^{\mathrm{TLF}}_{L/K}.$$

(4) *Nondegeneracy*: *the residue pairing*

$$\langle -, - \rangle_{\mathrm{res}} : K \times \Omega^{n,\mathrm{sep}}_{K/\Bbbk} \to \Bbbk, \quad \langle a, \alpha \rangle_{\mathrm{res}} := \mathrm{Res}^{\mathrm{TLF}}_{K/\Bbbk}(a \cdot \alpha)$$

is a topological perfect pairing.

Furthermore, the function $\mathrm{Res}^{\mathrm{TLF}}_{K/\Bbbk}$ *is the uniquely determined by properties* (1) *and* (2).

Remark 5.5. Actually the residue homomorphism $\mathrm{Res}^{\mathrm{TLF}}_{-/-}$ exists in much greater generality. Recall from Remark 3.11 that there is a category $\mathsf{TLF}\,\Bbbk$ whose objects are TLFs of all dimensions, and there are morphisms $f : K \to L$ for $\dim(K) < \dim(L)$. The category $\mathsf{TLF}^n\,\Bbbk$ is a full subcategory of $\mathsf{TLF}\,\Bbbk$. In [Yekutieli 1992, Section 2.4] we construct a residue homomorphism

$$\mathrm{Res}^{\mathrm{TLF}}_{L/K} : \Omega^{\mathrm{sep}}_{L/\Bbbk} \to \Omega^{\mathrm{sep}}_{K/\Bbbk}$$

for any morphism $K \to L$ in $\mathsf{TLF}\,\Bbbk$. This is a DG ST $\Omega^{\mathrm{sep}}_{K/\Bbbk}$-linear homomorphism of degree $-m$, where $m := \dim(L) - \dim(K)$, and it has properties like those in Theorem 5.4. When $K = \Bbbk$ this is the residue homomorphism $\mathrm{Res}^{\mathrm{TLF}}_{L/\Bbbk}$ above; and when $m = 0$ this is the trace homomorphism: $\mathrm{Res}^{\mathrm{TLF}}_{L/K} = \mathrm{Tr}^{\mathrm{TLF}}_{L/K}$.

Another remark is a sign change: the uniformization formula above differs from that of [Yekutieli 1992, Theorem 2.4.3] by a factor of $(-1)^{\binom{n}{2}}$. This is disguised as a permutation of the factors of the differential form $\operatorname{dlog}(t_1, \dots, t_n)$. Cf. also [Yekutieli 1992, Remark 2.4.4]. Our better acquaintance recently with DG conventions dictates the current formula.

Let K be a TLF over $\mathbb{k}$ of dimension $n \geq 1$. The homological algebra and Lie algebra construction of [Beilinson 1980], as explained in [Braunling 2014b, Section 3.1], takes as input the cubically decomposed ring of BT operators $\mathrm{E}(K)$ from Definition 4.23, and produces the *Beilinson–Tate residue functional*

$$\operatorname{Res}^{\mathrm{BT}}_{K/\mathbb{k}} : \Omega^n_{K/\mathbb{k}} \to \mathbb{k}. \tag{5-6}$$

Not much is known about this residue functional when $n \geq 2$. We have already posed Conjecture 0.9, comparing $\operatorname{Res}^{\mathrm{BT}}_{K/\mathbb{k}}$ to $\operatorname{Res}^{\mathrm{TLF}}_{K/\mathbb{k}}$. Here is another conjecture:

Conjecture 5.7. Let K be a TLF over $\mathbb{k}$. The $\mathbb{k}$-linear functional $\operatorname{Res}^{\mathrm{BT}}_{K/\mathbb{k}}$ is continuous.

It is closely related to the first conjecture. Indeed:

Proposition 5.8. (1) *Conjecture 0.9 implies Conjecture 5.7.*

(2) *Conjectures 5.7 and 0.12 together imply Conjecture 0.9.*

Proof. (1) We know that $\tau_K : \Omega^n_{K/\mathbb{k}} \to \Omega^{n,\mathrm{sep}}_{K/\mathbb{k}}$ and $\operatorname{Res}^{\mathrm{TLF}}_{K/\mathbb{k}}$ are continuous; see Theorem 5.4(1).

(2) Assume $\operatorname{Res}^{\mathrm{BT}}_{K/\mathbb{k}}$ is continuous. Then, since $\mathbb{k}$ is separated, the homomorphism $\operatorname{Res}^{\mathrm{BT}}_{K/\mathbb{k}}$ factors via τ_K. It remains to compare the continuous functionals

$$\operatorname{Res}^{\mathrm{BT}}_{K/\mathbb{k}},\ \operatorname{Res}^{\mathrm{TLF}}_{K/\mathbb{k}} : \Omega^{n,\mathrm{sep}}_{K/\mathbb{k}} \to \mathbb{k}.$$

Conjecture 0.12 says that we can use the results of [Braunling 2014b]. Now according to [Braunling 2014b, Theorem 26(3)], the functional $\operatorname{Res}^{\mathrm{BT}}_{K/\mathbb{k}}$ satisfies the uniformization condition (2) of Theorem 5.4. Since the $\mathbb{k}$-module spanned by the forms

$$b \cdot a_1^{i_1} \cdots a_n^{i_n} \cdot \operatorname{dlog}(\boldsymbol{a})$$

is dense inside $\Omega^{n,\mathrm{sep}}_{K/\mathbb{k}}$, and both functionals $\operatorname{Res}^{\mathrm{BT}}_{K/\mathbb{k}}$ and $\operatorname{Res}^{\mathrm{TLF}}_{K/\mathbb{k}}$ agree on it, these functionals must be equal. □

To end this section here are some remarks and examples related to the TLF residue:

Remark 5.9. The uniqueness of the residue functional $\operatorname{Res}^{\mathrm{TLF}}_{K/\mathbb{k}}$ has several other expressions, besides properties (1)–(2) of Theorem 5.4. For simplicity let us assume that $\mathbb{k}$ is infinite and $\boldsymbol{k}_n(K) = \mathbb{k}$.

Here is one alternative characterization: Let G be the "Galois group" of $K/\Bbbk$, namely $G := \mathrm{Aut}_{\mathsf{TLF}^n\,\Bbbk}(K)$. The group G acts on $\Omega^{n,\mathrm{sep}}_{K/\Bbbk}$ by continuous $\Bbbk$-linear isomorphisms, and hence it acts on $\mathrm{Hom}^{\mathrm{cont}}_{\Bbbk}(\Omega^{n,\mathrm{sep}}_{K/\Bbbk}, \Bbbk)$. It is not hard to show that $\mathrm{Res}^{\mathrm{TLF}}_{K/\Bbbk}$ is the only G-invariant element $\rho \in \mathrm{Hom}^{\mathrm{cont}}_{\Bbbk}(\Omega^{n,\mathrm{sep}}_{K/\Bbbk}, \Bbbk)$ that also satisfies $\rho(\mathrm{dlog}(\boldsymbol{a})) = 1$, where $\boldsymbol{a}$ is any system of uniformizers of K.

For the second characterization of the residue functional, let us assume that $\mathrm{char}(\Bbbk) = 0$. (This also works in $\mathrm{char}(\Bbbk) = p > 0$, but in a more complicated way — see [Yekutieli 1992, Digression 2.4.28].) Define $\mathrm{H}^n_{\mathrm{DR}}(K) := \mathrm{H}^n(\Omega^{\mathrm{sep}}_{K/\Bbbk})$. This is a rank 1 $\Bbbk$-module generated by the cohomology class of $\mathrm{dlog}(\boldsymbol{a})$. A calculation shows that $\mathrm{Res}^{\mathrm{TLF}}_{K/\Bbbk}$ is the only $\Bbbk$-linear homomorphism $\rho : \Omega^{n,\mathrm{sep}}_{K/\Bbbk} \to \Bbbk$ that factors through $\mathrm{H}^n_{\mathrm{DR}}(K)$ (i.e., it vanishes on n-coboundaries) and also satisfies $\rho(\mathrm{dlog}(\boldsymbol{a})) = 1$.

Remark 5.10. In dimension 1 the residue functional on local fields (with its topological aspects) was understood a long time ago (see [Serre 1988]).

The first attempt to extend the residue functional to local fields of dimension $n \geq 2$ was by Parshin and his school [1976; 1978; 1983; Beilinson 1980; Lomadze 1981]. In [Parshin 1976] the case of a surface is discussed, without attempt to isolate the resulting 2-dimensional local field from its geometric origin. In [Parshin 1983] there is a brief mention of a residue functional on a standalone n-dimensional local field, but without any details whatsoever. Beilinson [1980], quoting [Parshin 1976; 1978], incorrectly states that the residue functional on an n-dimensional local field K is independent of the parametrization of K (which, according to Theorem 3.16, means independent of the topology on K).

Lomadze [1981] studied the setup of a standalone n-dimensional local field in great detail. However, since he misunderstood the role of the topology in local fields of dimension $n \geq 2$ (see Remark 3.12), the residue functional he proposed was not well defined. To be specific, [Lomadze 1981] claimed that for a local field $K \in \mathsf{LF}^n\,\Bbbk$ there is a $\Bbbk$-linear homomorphism, let us denote it by $\mathrm{res} : \Omega^n_{K/\Bbbk} \to \Bbbk$, which satisfies continuity, uniformization (property (2) of Theorem 5.4), and invariance under automorphisms of K in $\mathsf{LF}^n\,\Bbbk$. However this is false for $n \geq 2$ and $\mathrm{char}(\Bbbk) = 0$, as was shown by a counterexample in [Yekutieli 1992]. We reproduce this counterexample, in an expanded form, in Examples 5.11 and 5.12 below.

In characteristic $p > 0$ the residue functional is indeed well defined on the category $\mathsf{LF}^n\,\Bbbk$. But this is due to the fact, discovered in [Yekutieli 1992], that the forgetful functor $\mathsf{TLF}^n\,\Bbbk \to \mathsf{LF}^n\,\Bbbk$ is an equivalence when $\mathrm{char}(\Bbbk) = p > 0$. See Remark 3.12.

Example 5.11. This is an expanded version of [Yekutieli 1992, Example 2.1.24]. It shows that, when $\mathrm{char}(\Bbbk) = 0$ and $n \geq 2$, there cannot be a $\Bbbk$-linear homomorphism

$\operatorname{res} : \Omega^n_{K/\Bbbk} \to \Bbbk$ for a local field $K \in \mathsf{LF}^n\, \Bbbk$ which satisfies continuity, uniformization, and invariance under automorphisms of K in $\mathsf{LF}^n\, \Bbbk$.

Let A be any commutative ST $\Bbbk$-ring. In order to distinguish between an "abstract" differential form $\alpha \in \Omega^i_{A/\Bbbk}$ and the "separated" differential form $\tau_A(\alpha) \in \Omega^{i,\mathrm{sep}}_{A/\Bbbk}$, we shall write $\bar{\alpha} := \tau_A(\alpha)$. Also we denote by $\bar{\mathrm{d}}$ the differential operator in the DG ring $\Omega^{\mathrm{sep}}_{A/\Bbbk}$. So $\tau_A \circ \mathrm{d} = \bar{\mathrm{d}} \circ \tau_A$ as $\Bbbk$-linear homomorphisms $\Omega^i_{A/\Bbbk} \to \Omega^{i+1,\mathrm{sep}}_{A/\Bbbk}$. Note that when A itself is separated we have $\Omega^{0,\mathrm{sep}}_{A/\Bbbk} = \Omega^0_{A/\Bbbk} = A$.

Since the homomorphism $\operatorname{res} : \Omega^n_{K/\Bbbk} \to \Bbbk$ is assumed to be continuous, and $\Bbbk$ is separated (because it is discrete), it follows that res factors through $\Omega^{n,\mathrm{sep}}_{K/\Bbbk}$, and $\operatorname{res}(\alpha) = \operatorname{res}(\bar{\alpha})$ for any $\alpha \in \Omega^n_{K/\Bbbk}$.

We shall use the setup of Example 3.13. So $\operatorname{char}(\Bbbk) = 0$, $n = 2$, and $K = \Bbbk((t_1, t_2)) = \Bbbk((t_2))((t_1))$, the standard 2-dimensional TLF with last residue field $\Bbbk$. We choose a collection $\{b_i\}_{i \in I}$ in $\Bbbk((t_2))$ that is a transcendence basis over the subfield $\Bbbk(t_2)$. We single out one element of the indexing set, say $i_0 \in I$, and define $\sigma(b_{i_0}) := b_{i_0} + t_1$. For $i \neq i_0$ we let $\sigma(b_i) := b_i$. This determines an automorphism f of K in the category $\mathsf{LF}^2\, \Bbbk$. (We already observed in Example 3.13 that f is not continuous). Let us write $b := b_{i_0}$; so $f(t_1) = t_1$, $f(t_2) = t_2$ and $f(b) = b + t_1$.

Define the differential forms

$$\alpha := t_1^{-1} \cdot \mathrm{d}(b) \cdot t_2^{-1} \cdot \mathrm{d}(t_2), \quad \beta := t_1^{-1} \cdot \mathrm{d}(b + t_1) \cdot t_2^{-1} \cdot \mathrm{d}(t_2)$$

and

$$\gamma := t_1^{-1} \cdot \mathrm{d}(t_1) \cdot t_2^{-1} \cdot \mathrm{d}(t_2) = \operatorname{dlog}(t_1, t_2)$$

in $\Omega^2_{K/\Bbbk}$. Note that $\beta = \alpha + \gamma$ and $\beta = f(\alpha)$.

Consider the continuous $\Bbbk$-linear derivation $\partial/\partial t_2$ of $\Bbbk((t_2))$. It is dual to the differential form $\bar{\mathrm{d}}(t_2) \in \Omega^{1,\mathrm{sep}}_{\Bbbk((t_2))/\Bbbk}$. Hence, letting $b' := \partial(b)/\partial t_2 \in \Bbbk((t_2))$, we have $\bar{\mathrm{d}}(b) = b' \cdot \bar{\mathrm{d}}(t_2)$ in $\Omega^{1,\mathrm{sep}}_{\Bbbk((t_2))/\Bbbk}$. Since the inclusion $\Bbbk((t_2)) \to K$ is continuous, it follows that $\bar{\mathrm{d}}(b) = b' \cdot \bar{\mathrm{d}}(t_2)$ in $\Omega^{1,\mathrm{sep}}_{K/\Bbbk}$. But then $\bar{\mathrm{d}}(b) \cdot \bar{\mathrm{d}}(t_2) = 0$ in $\Omega^{2,\mathrm{sep}}_{K/\Bbbk}$, from which we deduce that $\bar{\alpha} = 0$ in $\Omega^{2,\mathrm{sep}}_{K/\Bbbk}$. Therefore $\operatorname{res}(\alpha) = \operatorname{res}(\bar{\alpha}) = 0$. On the other hand, $\bar{\beta} = \bar{\alpha} + \bar{\gamma} = \bar{\gamma}$. And hence

$$\operatorname{res}(\beta) = \operatorname{res}(\bar{\beta}) = \operatorname{res}(\bar{\gamma}) = \operatorname{res}(\gamma) = 1$$

by the uniformization property. We see that $\beta = f(\alpha)$, $\operatorname{res}(\alpha) = 0$ and $\operatorname{res}(\beta) = 1$.

Example 5.12. Here is another way to view the previous example. Again $\Bbbk$ has characteristic 0. Let K be the local field $\Bbbk((t_1, t_2))$. We consider various topologies on K that make it into a TLF; namely we are looking at the objects in the fiber above K of the forgetful functor $F : \mathsf{TLF}^n\, \Bbbk \to \mathsf{LF}^n\, \Bbbk$. Theorem 3.16 shows that the group $\operatorname{Aut}_{\mathsf{LF}^n\, \Bbbk}(K)$ acts transitively on the objects in this fiber.

The first topology on the local field K is the standard topology of $\Bbbk((t_1, t_2))$, and we denote the resulting TLF by K_{st}. For the second topology we use the automorphism f from Example 5.11. We take the fine $(K_{\mathrm{st}}, f^{-1})$-module topology on K, and call the resulting TLF K_{nt}. Thus $f : K_{\mathrm{nt}} \to K_{\mathrm{st}}$ is an isomorphism in $\mathsf{TLF}^n\, \Bbbk$, and $F(K_{\mathrm{nt}}) = F(K_{\mathrm{st}}) = K$ in $\mathsf{LF}^n\, \Bbbk$.

Let K_{t} be any TLF such that $F(K_{\mathrm{t}}) = K$ (for instance the standard TLF K_{st} and the nonstandard TLF K_{nt}). There is a surjection

$$\tau_{\mathrm{t}} = \tau_{K_{\mathrm{t}}} : \Omega^2_{K/\Bbbk} = \Omega^2_{K_{\mathrm{t}}/\Bbbk} \twoheadrightarrow \Omega^{2,\mathrm{sep}}_{K_{\mathrm{t}}/\Bbbk},$$

and thus a residue homomorphism $\mathrm{res}_{\mathrm{t}} : \Omega^2_{K/\Bbbk} \to \Bbbk$ defined by $\mathrm{res}_{\mathrm{t}} := \mathrm{Res}^{\mathrm{TLF}}_{K_{\mathrm{t}}/\Bbbk} \circ \tau_{\mathrm{t}}$.

Consider the differential forms α, β, $\gamma \in \Omega^2_{K/\Bbbk}$ from Example 5.11. The calculation there shows that $\tau_{\mathrm{st}}(\alpha) = 0$. On the other hand, since $f \circ \tau_{\mathrm{nt}} = \tau_{\mathrm{st}} \circ f$ and $f(\gamma) = \gamma$, we have $f(\tau_{\mathrm{nt}}(\alpha)) = \tau_{\mathrm{st}}(f(\alpha)) = \tau_{\mathrm{st}}(\beta) = \tau_{\mathrm{st}}(\alpha) + \tau_{\mathrm{st}}(\gamma) = \tau_{\mathrm{st}}(\gamma) = f(\tau_{\mathrm{nt}}(\gamma))$, and therefore $\tau_{\mathrm{nt}}(\alpha) = \tau_{\mathrm{nt}}(\gamma)$. We conclude that, for the differential form $\alpha \in \Omega^2_{K/\Bbbk}$, we have $\mathrm{res}_{\mathrm{st}}(\alpha) = 0$, but $\mathrm{res}_{\mathrm{nt}}(\alpha) = \mathrm{res}_{\mathrm{nt}}(\gamma) = 1$.

Question 5.13. Take any $n \geq 2$. Consider the local field $K := \Bbbk((t_1, \dots, t_n))$, and the various TLFs K_{t} lying above it in $\mathsf{TLF}^n\, \Bbbk$, as in the previous example. We know that the residue $\mathrm{res}_{\mathrm{t}}(\alpha)$, for $\alpha \in \Omega^n_{K/\Bbbk}$, could change as we change the topology. However our counterexample involved transcendentals (the element b).

What about the subfield $\Bbbk(t_1, \dots, t_n) \in K$? Is it true that for a form α in $\Omega^n_{\Bbbk(t_1,\dots,t_n)/\Bbbk}$ the residue $\mathrm{res}_{\mathrm{t}}(\alpha)$ is independent of the topology K_{t} on K?

6. Geometry: completions

In this section we give background for Conjecture 0.12 in the introduction. We recall some facts on the Beilinson completion operation, and reproduce Beilinson's geometric definition of the BT operators.

Throughout this section $\Bbbk$ is a noetherian commutative ring, and X is a finite type $\Bbbk$-scheme. By a chain of points of length n in X we mean a sequence $\xi = (x_0, \dots, x_n)$ of points in X such that x_i is a specialization of x_{i-1} for all i. The chain ξ is called a *saturated chain* if every x_i is an immediate specialization of x_{i-1}, namely the closed set $\overline{\{x_i\}}$ has codimension 1 in $\overline{\{x_{i-1}\}}$. If $n \geq 1$, we denote by $\mathrm{d}_0(\xi)$ the chain obtained from ξ by deleting the point x_0.

Let $\mathcal{M}$ be a quasi-coherent $\mathcal{O}_X$-module. Beilinson [1980] introduced the completion $\mathcal{M}_\xi$ of $\mathcal{M}$ along ξ, which we refer to as the *Beilinson completion*. This is a very special case of his higher adeles. The definition of $\mathcal{M}_\xi$ is inductive on n, by an n-fold zigzag of inverse and direct limits. For a detailed account see [Yekutieli 1992, Section 3] or [Morrow 2013]. A basic geometric fact used in the definition is that, for any coherent sheaf $\mathcal{M}$, point $x \in X$ and number $i \in \mathbb{N}$, the truncated localization $\mathcal{M}_x / \mathfrak{m}_x^{i+1} \mathcal{M}_x$, when viewed as an $\mathcal{O}_X$-module supported on the closed set $\overline{\{x\}}$, is quasi-coherent. An important instance of this is when $\mathcal{M} = \mathcal{O}_X$ and $i = 0$, which gives the residue field $\boldsymbol{k}(x) = \mathcal{O}_{X,x} / \mathfrak{m}_x$.

Here are some important properties of the Beilinson completion operation. Let $\mathcal{M}$ be some quasi-coherent $\mathcal{O}_X$-module and let $\xi = (x_0, \dots, x_n)$ be a chain in X. We can view the completion $\mathcal{M}_\xi$ either as a module over the local ring $\mathcal{O}_{X,x_n}$ or as a constant $\mathcal{O}_X$-module supported on the closed set $\overline{\{x_n\}}$. Warning: $\mathcal{M}_\xi$ is usually not quasi-coherent. For any subchain $\xi' \subset \xi$ there is a canonical homomorphism $\mathcal{M}_{\xi'} \to \mathcal{M}_\xi$. When $n = 0$, so $\xi = (x_0)$, there is a canonical homomorphism $\mathcal{M}_{x_0} \to \mathcal{M}_{(x_0)}$, where the former is the stalk at the point. If $\mathcal{M}$ is coherent, then the homomorphism $\widehat{\mathcal{M}}_{x_0} \to \mathcal{M}_{(x_0)}$ from the $\mathfrak{m}_{x_0}$-adic completion is an isomorphism.

The completion $\mathcal{O}_{X,\xi}$ of the structure sheaf $\mathcal{O}_X$ is a commutative ring, the canonical sheaf homomorphism $\mathcal{O}_X \to \mathcal{O}_{X,\xi}$ is flat, and $\mathcal{M}_\xi$ is an $\mathcal{O}_{X,\xi}$-module. The sheaf homomorphism $\mathcal{O}_{X,\xi} \otimes_{\mathcal{O}_X} \mathcal{M} \to \mathcal{M}_\xi$ is an isomorphism. Thus the functor $\mathcal{M} \mapsto \mathcal{M}_\xi$ is exact. If $\mathcal{M}$ is coherent, ξ is saturated, and $n \geq 1$, then the canonical homomorphism

$$\mathcal{O}_{X,x_0} \otimes_{\mathcal{O}_X} \mathcal{M}_{\mathrm{d}_0(\xi)} \to \mathcal{M}_\xi$$

is an isomorphism.

The zigzag completion operation endows $\mathcal{M}_\xi$ with a $\Bbbk$-linear topology, similar to the iterated Laurent series construction in Definition 1.17. The ring $\mathcal{O}_{X,\xi}$ becomes a ST $\Bbbk$-ring, and $\mathcal{M}_\xi$ is a ST $\mathcal{O}_{X,\xi}$-module.

Let A be a semi-local commutative ring, with Jacobson radical $\mathfrak{r}$. We say that A is a *complete semi-local ring* if the canonical homomorphism $A \to \lim_{\leftarrow i} A/\mathfrak{r}^i$ is bijective. The *residue ring* of A is the ring $A/\mathfrak{r}$, which is a finite product of fields.

Theorem 6.1 [Parshin 1976; Beilinson 1980; Yekutieli 1992]. *Let $\Bbbk$ be an excellent noetherian ring, let X be a finite type $\Bbbk$-scheme, and let $\xi = (x_0, \dots, x_n)$ be a saturated chain in X of length $n \geq 1$ such that x_n is a closed point. Then the Beilinson completions $\mathcal{O}_{X,\xi}$ and $\boldsymbol{k}(x_0)_\xi$ have these algebraic properties*:

(1) *The ring $\boldsymbol{k}(x_0)_\xi$ is a finite product of n-dimensional local fields over $\Bbbk$.*

(2) *The ring $\mathcal{O}_{X,\xi}$ is a complete semi-local commutative $\Bbbk$-ring, with Jacobson radical $\mathfrak{r} = \mathcal{O}_{X,\xi} \otimes_{\mathcal{O}_{X,x_0}} \mathfrak{m}_{x_0}$ and residue ring $\boldsymbol{k}(x_0)_\xi$.*

(3) *Let K be one of the factors of the reduced artinian semi-local ring $\boldsymbol{k}(x_0)_\xi$, which by* (1) *is an n-dimensional local field. The DVR $\mathcal{O}_1(K)$ is the integral closure in K of the ring $\mathcal{O}_{X,\mathrm{d}_0(\xi)}$.*

If the base ring $\Bbbk$ is a perfect field, then the completion $\boldsymbol{k}(x_0)_\xi$ also has these topological properties:

(4) *Let K be one of the factors of the ring $\boldsymbol{k}(x_0)_\xi$. Then K, with the induced topology from $\boldsymbol{k}(x_0)_\xi$, is an n-dimensional TLF over $\Bbbk$.*

(5) *The image of the field $\boldsymbol{k}(x_0)$ in the ST ring $\boldsymbol{k}(x_0)_\xi$ is dense.*

Proof. (1–3) For $n = 1$ this is classical. For $n = 2$ this is in [Parshin 1976]. For $n \geq 3$ these assertions appear in [Beilinson 1980] without a proof. The proofs are [Yekutieli 1992, Theorem 3.3.2 and Corollary 3.3.5].

(4–5) For $n = 1$ this is classical. For $n \geq 2$ these assertions are [Yekutieli 1992, Proposition 3.3.6 and Corollary 3.3.7]. □

Remark 6.2. The condition that x_n is a closed point is only important to ensure that the last residue fields $\boldsymbol{k}_n(K)$ are finite over $\Bbbk$. Cf. Remark 3.10. The results in [Yekutieli 1992] quoted in the proof above only require the chain ξ to be saturated.

Suppose $\xi = (x_0, \dots, x_n)$ is a saturated chain in X. We have seen that there is a commutative diagram of flat ring homomorphisms

$$\begin{tikzcd}
\mathcal{O}_{X,x_n} \arrow[r] \arrow[d] & \mathcal{O}_{X,(x_n)} \arrow[dr] & \\
\mathcal{O}_{X,x_0} \arrow[r] & \mathcal{O}_{X,(x_0)} \arrow[r] & \mathcal{O}_{X,\xi}
\end{tikzcd}$$

Definition 6.3. Let $\xi = (x_0, \dots, x_n)$ be a saturated chain in X of length $n \geq 1$, and let M be a finite length $\mathcal{O}_{X,x_0}$-module. An $\mathcal{O}_{X,x_1}$-lattice in M is a finite $\mathcal{O}_{X,x_1}$-submodule L of M such that $M = \mathcal{O}_{X,x_0} \cdot L$. We denote by $\operatorname{Lat}_{X,\xi}(M)$ the set of all such lattices.

Of course the points $x_2, \dots, x_n$ have no influence on $\operatorname{Lat}_{X,\xi}(M)$. Note that if ξ has length 0 then $M_\xi = M$ for any finite length $\mathcal{O}_{X,x_0}$-module M.

Lemma 6.4. *Let $\xi = (x_0, \dots, x_n)$ be a saturated chain in X, and let M be a finite length $\mathcal{O}_{X,x_0}$-module. If L, $L' \in \operatorname{Lat}_{X,\xi}(M)$ and $L \subset L'$, then L'/L is a finite length $\mathcal{O}_{X,x_1}$-module.*

Proof. We can assume that $M \neq 0$. Let Z be the support in $\operatorname{Spec} \mathcal{O}_{X,x_1}$ of L. Then Z is a 1-dimensional scheme, with only two points: the closed point x_1 and the generic point x_0. The finite $\mathcal{O}_{X,x_1}$-module L'/L satisfies

$$(L'/L)_{x_0} \cong \mathcal{O}_{X,x_0} \otimes_{\mathcal{O}_{X,x_1}} (L'/L) = 0,$$

and hence it is supported on $\{x_1\}$. □

Let $\xi = (x_0, \dots, x_n)$ be a saturated chain in X, and let M be a finite length $\mathcal{O}_{X,x_0}$-module. We can view M as a quasi-coherent sheaf on X, constant on the closed set $\overline{\{x_0\}}$. The canonical homomorphism $M_{\mathrm{d}_0(\xi)} \to M_\xi$ is bijective. (If $n = 0$ then $\mathrm{d}_0(\xi)$ is empty, and we define $M_{()} := M$.) Note that M_ξ is a finite length $\mathcal{O}_{X,\xi}$-module.

Suppose we are given $\mathcal{O}_{X,x_1}$-lattices $L \subset L'$ in M. By the exactness of completion there are inclusions

$$L_{\mathrm{d}_0(\xi)} \subset L'_{\mathrm{d}_0(\xi)} \subset M_{\mathrm{d}_0(\xi)} = M_\xi,$$

and there is a canonical isomorphism of finite length $\mathcal{O}_{X,\mathrm{d}_0(\xi)}$-modules

$$(L'/L)_{\mathrm{d}_0(\xi)} \cong L'_{\mathrm{d}_0(\xi)}/L_{\mathrm{d}_0(\xi)}.$$

Let (M_1, M_2) be a pair of finite length $\mathcal{O}_{X,x_0}$-modules. Let $\mathrm{Lat}_{X,\xi}(M_1, M_2)$ be the set of pairs (L_1, L_2), where $L_i \in \mathrm{Lat}_{X,\xi}(M_i)$. We write $M_{i,\xi} := (M_i)_\xi$. Suppose $\phi : M_{1,\xi} \to M_{2,\xi}$ is a $\Bbbk$-linear operator. Like in Definition 4.4, we say that (L'_1, L'_2) is a ϕ-refinement of (L_1, L_2), and that $(L'_1, L'_2) \prec_\phi (L_1, L_2)$ is a ϕ-refinement in $\mathrm{Lat}_{X,\xi}(M_1, M_2)$, if $L'_1 \subset L_1$, $L_2 \subset L'_2$, $\phi(L_{1,\mathrm{d}_0(\xi)}) \subset L'_{2,\mathrm{d}_0(\xi)}$ and $\phi(L'_{1,\mathrm{d}_0(\xi)}) \subset L_{2,\mathrm{d}_0(\xi)}$.

Suppose A is a semi-local ring, with residue ring K. Any finite length A-module M has a canonical decomposition $M = \bigoplus_{\mathfrak{n}} M_{\mathfrak{n}}$, where $\mathfrak{n}$ runs over the finite set of maximal ideals of A, which of course coincides with the set Spec K.

Definition 6.5. Let A be a semi-local ring in $\mathsf{Ring}_{\mathrm{c}}\, \Bbbk$, with residue ring K. Let M_1, M_2 be finite length A-modules, and let $\phi : M_1 \to M_2$ be a $\Bbbk$-linear homomorphism. We say that ϕ is *local on* Spec K if $\phi(M_{1,\mathfrak{n}}) \subset M_{2,\mathfrak{n}}$ for every $\mathfrak{n} \in \operatorname{Spec} K$.

Here is a slight enhancement of the original definition found in [Beilinson 1980]; see Remark 6.7 below and Definition 4.5.

Definition 6.6 [Beilinson 1980]. Let $\xi = (x_0, \ldots, x_n)$ be a saturated chain of points in X such that x_n is a closed point. Let (M_1, M_2) be a pair of finite length modules over the ring $\mathcal{O}_{X,x_0}$. We define the subset

$$\mathrm{E}_{X,\xi}(M_1, M_2) \subset \mathrm{Hom}_{\Bbbk}(M_{1,\xi}, M_{2,\xi})$$

as follows:

(1) If $n = 0$, then any $\Bbbk$-linear homomorphism $\phi : M_{1,\xi} \to M_{2,\xi}$ belongs to $\mathrm{E}_{X,\xi}(M_1, M_2)$.

(2) If $n \geq 1$, a $\Bbbk$-linear homomorphism $\phi : M_{1,\xi} \to M_{2,\xi}$ belongs to $\mathrm{E}_{X,\xi}(M_1, M_2)$ if it satisfies these three conditions:

(i) Every $(L_1, L_2) \in \mathrm{Lat}_{X,\xi}(M_1, M_2)$ has some ϕ-refinement (L'_1, L'_2).

(ii) For every ϕ-refinement $(L'_1, L'_2) \prec_\phi (L_1, L_2)$ in $\mathrm{Lat}_{X,\xi}(M_1, M_2)$ the induced homomorphism

$$\bar{\phi} : (L_1/L'_1)_{\mathrm{d}_0(\xi)} \to (L'_2/L_2)_{\mathrm{d}_0(\xi)}$$

belongs to

$$\mathrm{E}_{X,\mathrm{d}_0(\xi)}(L_1/L'_1, L'_2/L_2).$$

(iii) The homomorphism ϕ is local on $\operatorname{Spec} \boldsymbol{k}(x_0)_\xi$.

Remark 6.7. Condition (2.iii) of Definition 6.6 is not part of the original definition in [Beilinson 1980]. Note that Tate [1968] only considered smooth curves, for which the completion is always a single local field, and there is no issue of locality.

The same locality condition eventually appears in Braunling's treatment — see the definition of the ring E_j in [Braunling 2014b, Theorem 26(1)].

The next definition uses notation like that of Tate. It can of course be rewritten using the notations of [Beilinson 1980] or of [Braunling 2014a; 2014b]. Compare to Definition 4.14 above.

Definition 6.8 [Beilinson 1980]. Let $\xi = (x_0, \dots, x_n)$ be a saturated chain of points in X of length $n \geq 1$ such that x_n is a closed point. Let (M_1, M_2) be a pair of finite length modules over the ring $\mathcal{O}_{X,x_0}$. For any $i \in \{1, \dots, n\}$ and $j \in \{1, 2\}$ we define the subset

$$\mathrm{E}_{X,\xi}(M_1, M_2)_{i,j} \subset \mathrm{E}_{X,\xi}(M_1, M_2)$$

to be the set of operators $\phi : M_{1,\xi} \to M_{2,\xi}$ in $\mathrm{E}_{X,\xi}(M_1, M_2)$ that satisfy the conditions:

(i) ϕ belongs to $\mathrm{E}_{X,\xi}(M_1, M_2)_{1,1}$ if there exists some $L_2 \in \mathrm{Lat}_{X,\xi}(M_2)$ such that $\phi(M_{1,\xi}) \subset L_{2,\mathrm{d}_0(\xi)}$.

(ii) ϕ belongs to $\mathrm{E}_{X,\xi}(M_1, M_2)_{1,2}$ if there exists some $L_1 \in \mathrm{Lat}_{X,\xi}(M_1)$ such that $\phi(L_{1,\mathrm{d}_0(\xi)}) = 0$.

(iii) Let $n \geq 2$. For $i \in \{2, \dots, n\}$ and $j \in \{1, 2\}$, ϕ belongs to $\mathrm{E}_{X,\xi}(M_1, M_2)_{i,j}$ if, for any ϕ-refinement $(L_1', L_2') \prec_\phi (L_1, L_2)$ in $\mathrm{Lat}_{X,\xi}(M_1, M_2)$, the induced homomorphism

$$\bar{\phi} : (L_1/L_1')_{\mathrm{d}_0(\xi)} \to (L_2'/L_2)_{\mathrm{d}_0(\xi)}$$

belongs to

$$\mathrm{E}_{X,\mathrm{d}_0(\xi)}(L_1/L_1', L_2'/L_2)_{i-1,j}.$$

Definition 6.9. Let $\xi = (x_0, \dots, x_n)$ be a saturated chain of points in X, of length $n \geq 1$, such that x_n is a closed point. Consider the residue field $K := \boldsymbol{k}(x_0)$.

(1) We define $\mathrm{E}_{X,\xi}(K) := \mathrm{E}_{X,\xi}(K, K)$.

(2) If $n \geq 1$ we define $\mathrm{E}_{X,\xi}(K)_{i,j} := \mathrm{E}_{X,\xi}(K, K)_{i,j}$.

By definition there are inclusions

$$\mathrm{E}_{X,\xi}(K)_{i,j} \subset \mathrm{E}_{X,\xi}(K) \subset \mathrm{End}_{\Bbbk}(K_\xi).$$

Theorem 6.10 [Beilinson 1980; Braunling 2014b, Proposition 13]. *Assume* $\Bbbk$ *is a perfect field. The data*

$$(\mathrm{E}_{X,\xi}(K), \{\mathrm{E}_{X,\xi}(K)_{i,j}\})$$

from Definition 6.9 is an n-dimensional cubically decomposed ring of operators on K_{ξ}, in the sense of Definition 0.3.

Conjecture 0.12 asserts that this n-dimensional cubically decomposed ring of operators on K_{ξ} coincides with the cubically decomposed ring of operators

$$(\mathrm{E}(K_{\xi}), \{\mathrm{E}(K_{\xi})_{i,j}\})$$

from Definition 4.23, modified as in formula (0-10).

Remark 6.11. Consider an integral finite type $\mathbb{k}$-scheme X of dimension n. Let $\xi = (x_0, \dots, x_n)$ be a maximal chain in X; so x_0 is the generic point. Write $K := \boldsymbol{k}(X) = \boldsymbol{k}(x_0)$. According to Theorem 6.10 there is a cubically decomposed ring of operators $\mathrm{E}_{X,\xi}(K)$ on K_{ξ}. Applying the abstract BT residue of formula (0-7) with $E := \mathrm{E}_{X,\xi}(K)$, we obtain the functional

$$\mathrm{Res}^{\mathrm{BT}}_{X,\xi} := \mathrm{Res}^{\mathrm{BT}}_{K_{\xi}/\mathbb{k};E} : \Omega^{n}_{K/\mathbb{k}} \to \mathbb{k}.$$

This is the residue functional that Beilinson [1980] had.

Beilinson [1980] claimed that the functionals $\mathrm{Res}^{\mathrm{BT}}_{X,\xi}$ satisfy several geometric properties. Most notably, when X is a proper scheme, then for any $\alpha \in \Omega^{n}_{K/\mathbb{k}}$ there is a global residue formula:

$$\sum_{\xi} \mathrm{Res}^{\mathrm{BT}}_{X,\xi}(\alpha) = 0. \tag{6-12}$$

The sum is on all maximal chains ξ in X.

Conjectures 0.9 and 0.12, combined with our results in [Yekutieli 1992] regarding the residue functionals $\mathrm{Res}^{\mathrm{TLF}}_{K_{\xi}/\mathbb{k}}$, imply most of the geometric properties of the residue functionals $\mathrm{Res}^{\mathrm{BT}}_{X,\xi}$ stated in [Beilinson 1980], including formula (6-12).

Conversely, as noted by Beilinson (private communication), a direct proof of the geometric properties of the functionals $\mathrm{Res}^{\mathrm{BT}}_{X,\xi}$ (perhaps by generalizing Tate's original idea to higher dimensions), together with Conjecture 0.12, would imply Conjecture 0.9.

Acknowledgments

I wish to thank Jesse Wolfson and Oliver Braunling for bringing their work to my attention and for many illuminating discussions. Thanks also to Matthew Morrow, John Tate and Alexander Beilinson for their input. Lastly, I want to thank the three anonymous referees for reading my paper carefully and suggesting many improvements.

References

[Beilinson 1980] A. A. Beĭlinson, "Residues and adèles", *Funktsional. Anal. i Prilozhen.* **14**:1 (1980), 44–45. In Russian; translated in *Functional Anal. Appl.* **14**:1 (1980), 34–35. MR 81f:14010 Zbl 0509.14018

[Beilinson 2008] A. Beilinson, "Remarks on topological algebras", *Mosc. Math. J.* **8**:1 (2008), 1–20, 183. MR 2010a:17040 Zbl 1170.14002

[Braunling 2014a] O. Braunling, "Adèle residue symbol and Tate's central extension for multiloop Lie algebras", *Algebra Number Theory* **8**:1 (2014), 19–52. MR 3207578 Zbl 06322071

[Braunling 2014b] O. Braunling, "On the local residue symbol in the style of Tate and Beilinson", preprint, 2014. arXiv 1403.8142v2

[Braunling et al. 2014] O. Braunling, M. Groechenig, and J. Wolfson, "Tate objects in exact categories", preprint, 2014. arXiv 1402.4969

[EGA IV 1967] A. Grothendieck, "Éléments de géométrie algébrique, IV: Étude locale des schémas et des morphismes de schémas IV", *Inst. Hautes Études Sci. Publ. Math.* **32** (1967), 5–361. MR 39 #220 Zbl 0153.22301

[Fesenko and Kurihara 2000] I. Fesenko and M. Kurihara (editors), *Invitation to higher local fields*, Geometry & Topology Monographs **3**, Geometry & Topology Publications, Coventry, 2000. MR 2001h:11005 Zbl 0954.00026

[Huber 1991] A. Huber, "On the Parshin–Beĭlinson adèles for schemes", *Abh. Math. Sem. Univ. Hamburg* **61** (1991), 249–273. MR 92k:14024 Zbl 0763.14006

[Kato 1979] K. Kato, "A generalization of local class field theory by using K-groups, I", *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **26**:2 (1979), 303–376. MR 81b:12016 Zbl 0428.12013

[Lomadze 1981] V. G. Lomadze, "On residues in algebraic geometry", *Izv. Akad. Nauk SSSR Ser. Mat.* **45**:6 (1981), 1258–1287. In Russian; translated in *Math. USSR Izv.* **19**:3 (1982), 495–520. MR 83g:14021 Zbl 0528.14003

[Matsumura 1986] H. Matsumura, *Commutative ring theory*, Cambridge Studies in Advanced Mathematics **8**, Cambridge University Press, Cambridge, 1986. MR 88h:13001 Zbl 0603.13001

[Morrow 2013] M. Morrow, "An introduction to higher dimensional local fields and adeles", unpublished notes, 2013, Available at http://www.math.uni-bonn.de/people/morrow. Older version at arXiv:1204.0586v2.

[Osipov 2005] D. V. Osipov, "Central extensions and reciprocity laws on algebraic surfaces", *Mat. Sb.* **196**:10 (2005), 111–136. In Russian; translated in *Sb. Math.* **196** (2005), no. 9–10, 1503–1527. MR 2007f:11071 Zbl 1177.14083

[Osipov 2007] D. Osipov, "Adeles on n-dimensional schemes and categories C_n", *Internat. J. Math.* **18**:3 (2007), 269–279. MR 2008b:14005 Zbl 1126.14004

[Parshin 1976] A. N. Paršin, "On the arithmetic of two-dimensional schemes, I: Distributions and residues", *Izv. Akad. Nauk SSSR Ser. Mat.* **40**:4 (1976), 736–773, 949. In Russian; translated in *Math. USSR Izvestija* **10**:4 (1976). MR 54 #7479 Zbl 0366.14003

[Parshin 1978] A. N. Paršin, "Abelian coverings of arithmetic schemes", *Dokl. Akad. Nauk SSSR* **243**:4 (1978), 855–858. In Russian; translated in *Sov. Math., Dokl.* **19** (1978), 1438–1442. MR 80b:14014 Zbl 0443.12006

[Parshin 1983] A. N. Parshin, "Chern classes, adèles and L-functions", *J. Reine Angew. Math.* **341** (1983), 174–192. MR 85c:14015 Zbl 0518.14013

[Serre 1988] J.-P. Serre, *Algebraic groups and class fields*, Graduate Texts in Mathematics **117**, Springer, New York, 1988. MR 88i:14041 Zbl 0703.14001

[Tate 1968] J. Tate, "Residues of differentials on curves", *Ann. Sci. École Norm. Sup.* (4) **1** (1968), 149–159. MR 37 #2756 Zbl 0159.22702

[Yekutieli 1992] A. Yekutieli, *An explicit construction of the Grothendieck residue complex*, Astérisque **208**, Société Mathématique de France, Paris, 1992. MR 94e:14026 Zbl 0788.14011

[Yekutieli 1995] A. Yekutieli, "Traces and differential operators over Beĭlinson completion algebras", *Compositio Math.* **99**:1 (1995), 59–97. MR 96g:14014 Zbl 0856.13019

Communicated by Edward Frenkel
Received 2014-06-25 Revised 2014-10-20 Accepted 2014-12-25

amyekut@math.bgu.ac.il *Department of Mathematics, Ben Gurion University,*
Be'er Sheva 84105, 62381 Beersheva, Israel

ALGEBRA AND NUMBER THEORY 9:1 (2015)
dx.doi.org/10.2140/ant.2015.9.225

Categories of abelian varieties over finite fields, I: Abelian varieties over $\mathbb{F}_p$

Tommaso Giorgio Centeleghe and Jakob Stix

We assign functorially a $\mathbb{Z}$-lattice with semisimple Frobenius action to each abelian variety over $\mathbb{F}_p$. This establishes an equivalence of categories that describes abelian varieties over $\mathbb{F}_p$ avoiding $\sqrt{p}$ as an eigenvalue of the Frobenius in terms of simple commutative algebra. This result extends the isomorphism classification of Waterhouse and Deligne's equivalence for ordinary abelian varieties.

1. Introduction

1.1. Let p be a prime number, $\bar{\mathbb{F}}_p$ an algebraic closure of the prime field $\mathbb{F}_p$ with p elements, and $\mathbb{F}_q \subset \bar{\mathbb{F}}_p$ the subfield with q elements, where $q = p^e$ is a power of p. The category

$$\mathsf{AV}_q$$

of abelian varieties over $\mathbb{F}_q$ is an additive category, where for any two objects A, B the abelian group $\mathrm{Hom}_{\mathbb{F}_q}(A, B)$ is free of finite rank. Even though the main result of this paper concerns abelian varieties over the prime field $\mathbb{F}_p$, the general theme of our work is describing suitable subcategories C of AV_q by means of lattices $T(A)$

Centeleghe was supported by a project jointly funded by the DFG Priority Program SPP 1489 and the Luxembourg FNR.
MSC2010: 11-02.
Keywords: abelian varieties, finite fields, Gorenstein rings, reflexive modules.

functorially attached to abelian varieties A of C. In contrast to the characteristic-zero case, if we insist that

$$\operatorname{rk}_{\mathbb{Z}}(T(A)) = 2\dim(A), \tag{1-1}$$

then it is *not* possible to construct $T(A)$ on the whole category AV_q (see Section 1.6). However, if we take C to be the full subcategory

$$\mathsf{AV}_q^{\mathrm{ord}}$$

of ordinary abelian varieties, Deligne [1969, §7] showed that a functor $A \mapsto T(A)$ satisfying (1-1) exists and gives an equivalence between $\mathsf{AV}_q^{\mathrm{ord}}$ and the category of finite free $\mathbb{Z}$-modules T equipped with a linear map $F : T \to T$ satisfying a list of easy-to-state axioms.

Inspired by Waterhouse [1969, Theorem 6.1], in the present work we show that a description in the style of Deligne can in fact be obtained, when $q = p$, for a considerably larger subcategory C of AV_p, which excludes only a single isogeny class of simple objects of AV_p from occurring as an isogeny factor (see Theorem 1). Deligne's method is an elegant application of the Serre–Tate theory of canonical liftings of ordinary abelian varieties, whereas our method, closer to that used by Waterhouse, does not involve lifting abelian varieties to characteristic zero. Even if the main result of this paper generalizes the $q = p$ case of Deligne's theorem, it is unlikely that a proof generalizing Deligne's lifting strategy is possible.

1.2. A *Weil q-number π* is an algebraic integer, lying in some unspecified field of characteristic zero, such that for any embedding $\iota : \mathbb{Q}(\pi) \hookrightarrow \mathbb{C}$ we have

$$|\iota(\pi)| = q^{1/2},$$

where $|-|$ is the ordinary absolute value of $\mathbb{C}$. Two Weil q-numbers π and π' are *conjugate* to each other if there exists an isomorphism $\mathbb{Q}(\pi) \xrightarrow{\sim} \mathbb{Q}(\pi')$ carrying π to π', in which case we write $\pi \sim \pi'$. We will denote by W_q the set of conjugacy classes of Weil q-numbers. A Weil q-number is either totally real or totally imaginary, hence it makes sense to speak of a *nonreal* element of W_q.

Let A be an object of AV_q, and denote by $\pi_A : A \to A$ the Frobenius isogeny of A relative to $\mathbb{F}_q$. If A is $\mathbb{F}_q$-simple then $\operatorname{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ is a division ring, and a well-known result of Weil says that π_A is a Weil q-number inside the number field $\mathbb{Q}(\pi_A)$. Let

$$A \sim \prod_{1 \le i \le r} A_i^{e_i} \tag{1-2}$$

be the decomposition of A up to $\mathbb{F}_q$-isogeny into powers of simple, pairwise nonisogenous factors A_i. The *Weil support* of A is defined as the subset

$$w(A) = \{\pi_{A_1}, \dots, \pi_{A_r}\} \subseteq W_q$$

given by the conjugacy classes of the Weil numbers π_{A_i} attached to the simple factors A_i. By Honda–Tate theory, the conjugacy classes of the π_{A_i} are pairwise distinct; moreover, any class in W_q arises as π_A, for some $\mathbb{F}_q$-simple abelian variety A, uniquely determined up to $\mathbb{F}_q$-isogeny [Tate 1971, Théorème 1].

1.3. Consider now the case $q = p$. Using Honda–Tate theory, it is easy to see that for a simple object A of AV_p the ring $\mathrm{End}_{\mathbb{F}_p}(A)$ is commutative if and only if $\pi_A \not\sim \sqrt{p}$, i.e., if and only if the Frobenius isogeny $\pi_A : A \to A$ defines a nonreal Weil p-number [Waterhouse 1969, Theorem 6.1]. Let

$$\mathsf{AV}_p^{\mathrm{com}}$$

be the full subcategory of AV_p given by all objects A such that $w(A)$ does not contain the conjugacy class of $\sqrt{p}$. Equivalently, $\mathsf{AV}_p^{\mathrm{com}}$ is the largest full subcategory of AV_p closed under taking cokernels containing all simple objects whose endomorphism ring is commutative. Since the Weil p-number $\sqrt{p}$ is associated to an $\mathbb{F}_p$-isogeny class of simple, supersingular abelian surfaces [Tate 1971, Exemple (b), p. 97], we have a natural inclusion $\mathsf{AV}_p^{\mathrm{ord}} \subset \mathsf{AV}_p^{\mathrm{com}}$.

The main result of this paper, proven at the end of Section 5.3, is the following:

Theorem 1. *There is an ind-representable contravariant functor*

$$A \mapsto (T(A), F)$$

which induces an antiequivalence between $\mathsf{AV}_p^{\mathrm{com}}$ *and the category of pairs* (T, F) *given by a finite, free* $\mathbb{Z}$*-module* T *and an endomorphism* $F : T \to T$ *satisfying the following properties*:

(i) $F \otimes \mathbb{Q}$ *is semisimple, and its eigenvalues are nonreal Weil* p*-numbers.*

(ii) *There exists a linear map* $V : T \to T$ *such that* $FV = p$.

Moreover, the lattice $T(A)$ *has rank* $2\dim(A)$ *for all* A *in* $\mathsf{AV}_p^{\mathrm{com}}$, *and* F *is equal to* $T(\pi_A)$.

To prove the theorem, we consider in Section 2 a family of Gorenstein rings

$$R_w = \mathbb{Z}[F, V]/(FV - p, h_w(F, V))$$

indexed by the finite subsets $w \subseteq W_p$, where $h_w(F, V)$ is a certain symmetric polynomial built out of the minimal polynomials over $\mathbb{Q}$ of the elements of w. An object (T, F) in the target category of the functor $T(-)$ of Theorem 1 is nothing but an R_w-module, for $w \subset W_p$ large enough, that is free of finite rank as a $\mathbb{Z}$-module. In this translation, the linear map $F : T \to T$ is given by the action of the image of F in R_w, and the relation $h_w(F, V)$ in R_w encodes precisely that $F \otimes \mathbb{Q}$ acts semisimply and with eigenvalues given by Weil p-numbers lying in w (see Sections 2.4, 2.5 and 3.2). Thanks to the Gorenstein property, these R_w-modules are precisely the reflexive R_w-modules; the category that they form will be denoted by (see Section 3)

$$\mathsf{Refl}(R_w).$$

For $v \subseteq w$, the corresponding rings are linked by natural surjective maps $\mathrm{pr}_{v,w} : R_w \to R_v$. We denote by $\mathcal{R}_p^{\mathrm{com}}$ the pro-system $(R_w, \mathrm{pr}_{v,w})$ with $w \subseteq W_p$ ranging over the finite subsets avoiding the conjugacy class of $\sqrt{p}$. We further set

$$\mathsf{Refl}(\mathcal{R}_p^{\mathrm{com}}) = \varinjlim_{w \subseteq W_p \setminus \{\sqrt{p}\}} \mathsf{Refl}(R_w),$$

and refer to Section 3.2 for details.

In this language, Theorem 1 can be stated as saying that

$$T : \mathsf{AV}_p^{\mathrm{com}} \to \mathsf{Refl}(\mathcal{R}_p^{\mathrm{com}})$$

is an antiequivalence of categories. While this formulation of the main result is closer to the perspective we adopted in its proof, the more concrete statement we chose to give above allows an immediate comparison to Deligne's result [1969].

1.4. The rings R_w studied in Section 2 are in fact defined for any finite subset $w \subseteq W_q$. They appear naturally in connection to abelian varieties, in that for any A in AV_q the natural map

$$\mathbb{Z}[F, V]/(FV - q) \to \mathrm{End}_{\mathbb{F}_q}(A) \tag{1-3}$$

sending F to π_A and V to the Verschiebung isogeny q/π_A induces an identification between $R_{w(A)}$ and the subring $\mathbb{Z}[\pi_A, q/\pi_A]$ of $\mathrm{End}_{\mathbb{F}_q}(A)$, which has finite index in the center (see Section 2.1). The rings R_w have been already considered in [Waterhouse 1969] and [Howe 1995], for example. The Gorenstein property of R_w in the ordinary cases is implicitly contained in [Howe 1995] and explicitly used in a special case in [Howe 2004]. However, to the best of our knowledge, a systematic investigation of the occurrence of Gorensteinness among the rings R_w has not been carried out previously (see Theorems 11 and 12).

An $\mathcal{R}_p^{\mathrm{com}}$-linear structure on $\mathsf{AV}_p^{\mathrm{com}}$ can be deduced from the map (1-3) (see Section 2.3). The requirement that $F = T(\pi_A)$ means precisely that the functor $T(-)$ is an $\mathcal{R}_p^{\mathrm{com}}$-linear functor (see Section 3.2).

1.5. The proof of the theorem consists of two steps. First, for any finite subset $w \subseteq W_p$ not containing the conjugacy class of $\sqrt{p}$, we construct a certain abelian variety A_w isogenous to the product of all simple objects attached to the elements of w via Honda–Tate theory. The object A_w is chosen in its isogeny class with the smallest possible endomorphism ring, i.e., such that the natural map

$$R_w \to \mathrm{End}_{\mathbb{F}_p}(A_w)$$

is an isomorphism (see Proposition 21). In order to show the existence of such an A_w, which already appears in [Waterhouse 1969, Theorem 6.1] if w consists of a single element, the assumption $q = p$ plays an important role. Exploiting the Gorenstein property of R_w, in Theorem 25 we show that the functor $\mathrm{Hom}_{\mathbb{F}_p}(-, A_w)$ gives a contravariant equivalence

$$\mathrm{Hom}_{\mathbb{F}_p}(-, A_w) : \mathsf{AV}_w \xrightarrow{\sim} \mathsf{Refl}(R_w),$$

where AV_w is the full subcategory of AV_p given by all abelian varieties A with $w(A) \subseteq w$.

The second step consists in showing that the abelian varieties A_w previously constructed can be chosen in such a way that the functors $\mathrm{Hom}_{\mathbb{F}_p}(-, A_w)$ interpolate well and define a functor on $\mathsf{AV}_p^{\mathrm{com}}$. More precisely we show the existence of an ind-system

$$\mathscr{A} = (A_w, \varphi_{w,v}), \tag{1-4}$$

indexed by finite subsets $w \subseteq W_p$ not containing the conjugacy class of $\sqrt{p}$, such that the corresponding direct limit of finite free $\mathbb{Z}$-modules

$$T(A) = \varinjlim_{w} \mathrm{Hom}_{\mathbb{F}_p}(A, A_w)$$

stabilizes for any A in $\mathsf{AV}_p^{\mathrm{com}}$. The contravariant functor $T(-)$ ind-represented by $\mathscr{A}$ will produce the required antiequivalence.

1.6. As Serre has observed, it is *not* possible to functorially construct a lattice $T(A)$ satisfying the expected $\mathrm{rk}_{\mathbb{Z}}(T(A)) = 2\dim(A)$ on the category of abelian varieties over $\overline{\mathbb{F}}_p$. This is due to the existence of objects like supersingular elliptic curves E over $\overline{\mathbb{F}}_p$. As is well known, the division ring $\mathrm{End}_{\overline{\mathbb{F}}_p}(E) \otimes \mathbb{Q}$ is a nonsplit quaternion algebra over $\mathbb{Q}$ and has no 2-dimensional $\mathbb{Q}$-linear representation that can serve as $T(E) \otimes \mathbb{Q}$. The issue just described is the same obstruction that prevents the existence of a Weil cohomology for varieties over finite fields with rational coefficients.

Using the same argument, one can show the nonexistence of a lattice $T(A)$ as above on the category AV_q, where q is a square. When q is not a square, the correct instance of Serre's observation preventing Theorem 1 from extending to all of AV_p is given by the isogeny class of $\mathbb{F}_q$-simple, supersingular abelian surfaces associated via Honda–Tate theory to the real, nonrational, Weil q-number $\sqrt{q}$. The endomorphism ring of any such surface A is an order of a quaternion algebra over $\mathbb{Q}(\sqrt{q}) = \mathbb{Q}(\sqrt{p})$ which is ramified at the two real places [Waterhouse 1969, p. 528]. It follows that $\mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{R} \simeq \mathbb{H} \times \mathbb{H}$ is a product of two copies of the Hamilton quaternions $\mathbb{H}$. Thus it admits no faithful representation on a 4-dimensional real vector space, which $T(A) \otimes \mathbb{R}$ would give rise to.

1.7. The dual abelian variety establishes an antiequivalence $A \mapsto A^t$ of AV_q which preserves Weil supports and has the effect of switching the roles of Frobenius and Verschiebung endomorphisms relative to $\mathbb{F}_q$. That is,

$$(\pi_A)^t = q/\pi_{A^t}$$

as isogenies from A^t to itself. On the module side, we define a covariant involution of $\mathsf{Refl}(\mathcal{R}_p^{\mathrm{com}})$, denoted by $M \mapsto M^\tau$, which interchanges the roles of F and V, i.e., such that

$$(T, F)^\tau = (T, p/F).$$

Using these two dualities we can exhibit a covariant version of the functor $T(-)$ of Theorem 1. More precisely, define

$$T_*(A) = T(A^t)^\tau$$

as the pair given by the $\mathbb{Z}$-module $T(A^t)$ equipped with the linear map $p/T(\pi_{A^t})$. In the notation as pairs, $T_*(A)$ takes the form

$$(T(A^t), p/T(\pi_{A^t})) = (T(A^t), T((\pi_A)^t)) = (T_*(A), T_*(\pi_A)).$$

The functor $T_*(-)$ gives a covariant, $\mathcal{R}_p^{\mathrm{com}}$-linear equivalence

$$T_* : \mathsf{AV}_p^{\mathrm{com}} \to \mathsf{Refl}(\mathcal{R}_p^{\mathrm{com}}) \tag{1-5}$$

which is pro-represented by the system $\mathcal{A}^t = (A_w^t, \varphi_{w',w}^t)$ dual to (1-4). In the definition of $T_*(-)$ it is necessary to apply the involution τ to $T(A^t)$ in order to guarantee that T_* be $\mathcal{R}_p^{\mathrm{com}}$-linear.

In Section 7.4 we compare $T_*(-)$ restricted to $\mathsf{AV}_p^{\mathrm{ord}}$ with Deligne's functor [1969, §7], which we denote by $T_{\mathrm{Del},p}(-)$. The comparison makes use of a compatible pro-system of projective R_w-modules M_w of rank 1 for all finite subsets $w \subseteq W_p$ consisting only of conjugacy classes of ordinary Weil p-numbers. Proposition 44 then describes, for all abelian varieties A over $\mathbb{F}_p$ with $w(A) \subseteq w$, a natural isomorphism

$$T_{\mathrm{Del},p}(A) \otimes_{R_w} M_w \xrightarrow{\sim} T_*(A).$$

Furthermore, by choosing a suitable ind-representing system $\mathcal{A} = (A_w, \varphi_{v,w})$, we may assume that $M_w = R_w$ for all w, i.e., the antiequivalence of Theorem 1 may be chosen in its covariant version to extend Deligne's equivalence; see Proposition 45 for details.

1.8. Finally, we indicate how to recover the ℓ-adic Tate module $T_\ell(A)$, for a prime $\ell \neq p$, and the contravariant Dieudonné module $T_p(A)$ (see [Waterhouse 1969, §1.2]) from the module $T(A)$. This involves working with the formal Tate module $T_\ell(\mathcal{A})$ and the formal Dieudonné module $T_p(\mathcal{A})$ of the direct system $\mathcal{A}$, respectively defined as the direct limit of $T_\ell(A_w)$ and the inverse limit of the $T_p(A_w)$, with transition maps obtained via functoriality of T_ℓ and T_p. More concretely, we have natural isomorphisms

$$T_\ell(A) \simeq \operatorname{Hom}_{\mathcal{R}_\ell}(T(A) \otimes \mathbb{Z}_\ell, T_\ell(\mathcal{A})),$$
$$T_p(A) \simeq (T(A) \otimes \mathbb{Z}_p) \mathbin{\widehat{\otimes}}_{\mathcal{R}_p} T_p(\mathcal{A});$$

see Propositions 27 and 28 for notation and proofs. In this respect the functor $T(-)$ can be interpreted as an integral lifting of the Dieudonné module functor $T_p(-)$.

In a forthcoming paper, we will apply the method used here to study certain categories of abelian varieties over a finite field which is larger that $\mathbb{F}_p$. Therefore, although Theorem 1 deals with abelian varieties over $\mathbb{F}_p$, we only restrict to the case $q = p$ when it becomes necessary.

2. On the ubiquity of Gorenstein rings among minimal central orders

2.1. ***Minimal central orders.*** Let $w \subseteq W_q$ be any finite set of conjugacy classes of Weil q-numbers. Choose Weil q-numbers $\pi_1, \dots, \pi_r$ representing the elements of w, and consider the ring homomorphism

$$\mathbb{Z}[F, V]/(FV - q) \to \prod_{1 \le i \le r} \mathbb{Q}(\pi_i) \tag{2-1}$$

sending F to $(\pi_1, \dots, \pi_r)$ and V to $(q/\pi_1, \dots, q/\pi_r)$.

Definition 2. The *minimal central order* R_w is the quotient

$$\mathbb{Z}[F, V]/(FV - q) \to R_w \tag{2-2}$$

by the kernel of the homomorphism (2-1). The image of F in R_w will be denoted by F_w, and the image of V by V_w.

The construction of the ring R_w is independent of the chosen Weil q-numbers in their respective conjugacy classes. When w consists of a single conjugacy class of a Weil number π, the ring $R_{\{\pi\}}$, isomorphic to the order of $\mathbb{Q}(\pi)$ generated by π and q/π, will sometimes be denoted simply by R_π. Since the representatives $\pi_1, \dots, \pi_r$ are pairwise nonconjugate, there is a canonical finite index inclusion

$$R_w \subseteq \prod_{\pi \in w} R_\pi;$$

in particular,

$$R_w \otimes \mathbb{Q} = \prod_{\pi \in w} \mathbb{Q}(\pi). \tag{2-3}$$

Moreover, for finite subsets $v \subseteq w \subseteq W_q$ we have a natural surjection

$$\mathrm{pr}_{v,w} : R_w \to R_v.$$

Our main goal in this section is to show that, under a mild assumption on w, the ring R_w is a 1-dimensional Gorenstein ring. This will be proved in Section 2.5, where we obtain a description of R_w by identifying the relations between the generators F and V.

Example 3. The equality of closed subschemes

$$\operatorname{Spec}(R_w) = \bigcup_{\pi \in w} \operatorname{Spec}(R_\pi) \subseteq \operatorname{Spec}(\mathbb{Z}[F, V]/(FV - q))$$

shows that the spectrum of R_w is obtained by gluing the spectra of the rings R_π along their various intersections inside $\operatorname{Spec}(\mathbb{Z}[F, V]/(FV - q))$. This means, roughly, that congruences between Weil q-numbers are responsible for R_w differing from the product of the R_π for all $\pi \in w$.

We measure in a special situation the deviation of R_w from being isomorphic to $\prod_{\pi \in w} R_\pi$. For $i = 1, 2$, let π_i be a quadratic Weil q-number with minimal polynomial

$$x^2 - \beta_i x + q,$$

where $\beta_i \in \mathbb{Z}$, and set $\Delta = \beta_1 - \beta_2$. Since $q/\pi_i = \beta_i - \pi_i$, we have

$$R_{\pi_i} = \mathbb{Z}[\pi_i] \simeq \mathbb{Z}[x]/(x^2 - \beta_i x + q);$$

moreover, the subring $R_w \subseteq \mathbb{Z}[\pi_1] \times \mathbb{Z}[\pi_2]$ is generated as a $\mathbb{Z}$-algebra by

$$(0, \Delta), (\pi_1, \pi_2) \in \mathbb{Z}[\pi_1] \times \mathbb{Z}[\pi_2],$$

since it is generated by (π_1, π_2) and $(\beta_1 - \pi_1, \beta_2 - \pi_2)$. Because $\beta_1 \equiv \beta_2$ modulo Δ, there are isomorphisms of quotients

$$\mathbb{Z}[\pi_1]/\Delta\mathbb{Z}[\pi_1] \simeq \mathbb{Z}[\pi_2]/\Delta\mathbb{Z}[\pi_2] =: R_0,$$

and R_w becomes the fiber product

$$R_w = \mathbb{Z}[\pi_1] \times_{R_0} \mathbb{Z}[\pi_2],$$

which is an order of index Δ^2 in the product $R_{\pi_1} \times R_{\pi_2}$. The congruences between π_1 and π_2 are encoded by the closed subscheme of $\operatorname{Spec}(\mathbb{Z}[F, V]/(FV - q))$ given by

$$\operatorname{Spec}(R_0) = \operatorname{Spec}(R_{\pi_1}) \cap \operatorname{Spec}(R_{\pi_2}).$$

Note that the minimal polynomials $x^2 - \beta_i + q$ yield Weil q-numbers if and only if

$$\beta_i^2 < 4q.$$

In particular, by letting q range over the powers of the prime p, the Weil q-numbers π_i may be chosen so that Δ is divisible by an arbitrary integer.

2.2. ***Connection to abelian varieties.*** We proceed to link R_w to abelian varieties over $\mathbb{F}_q$. Any such A has two distinguished isogenies, given by the Frobenius π_A and the Verschiebung q/π_A relative to $\mathbb{F}_q$. The $\mathbb{Q}$-algebra $\mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ is semisimple, and its center is equal to the subalgebra $\mathbb{Q}(\pi_A)$ generated by π_A [Tate 1966, Theorem 2]. It follows that any isogeny decomposition of A, as in (1-2), induces the isomorphism

$$\mathbb{Q}(\pi_A) \simeq \prod_{\pi_{A_i} \in w(A)} \mathbb{Q}(\pi_{A_i}), \tag{2-4}$$

sending π_A to $(\pi_{A_1}, \dots, \pi_{A_r})$, where $\pi_{A_1}, \dots, \pi_{A_r}$ are the Weil q-numbers defined by the simple factors of A and $w(A)$ is the Weil support of A defined in the introduction.

From (2-4) we deduce that the ring homomorphism

$$r_A : \mathbb{Z}[F, V]/(FV - q) \to \mathrm{End}_{\mathbb{F}_q}(A)$$

sending F to π_A and V to q/π_A gives an identification between $R_{w(A)}$ and the image of r_A, namely the subring

$$\mathbb{Z}[\pi_A, q/\pi_A],$$

which sits inside the center of $\mathrm{End}_{\mathbb{F}_q}(A)$ with finite index. In this way we see that $R_{w(A)}$ plays the role of a lower bound for the center of $\mathrm{End}_{\mathbb{F}_q}(A)$. This justifies the terminology we chose in its definition.

Remark 4. One can ask whether there exists an abelian variety A with Weil support w such that the natural map $R_w \to \mathrm{End}_{\mathbb{F}_p}(A)$ induced by r_A gives an isomorphism between R_w and the center of $\mathrm{End}_{\mathbb{F}_p}(A)$. In Proposition 21 below, generalizing a result of Waterhouse, we obtain a partial result in this direction.

2.3. ***Linear structures over minimal central orders.*** For a finite subset $w \subseteq W_q$ the full subcategory

$$\mathsf{AV}_w \subseteq \mathsf{AV}_q$$

consists of all abelian varieties A such that $w(A) \subseteq w$ or, equivalently, such that r_A factors through the quotient $\mathbb{Z}[F, V]/(FV - q) \to R_w$. Since for any morphism $f : A \to B$ in AV_q and any $\eta \in \mathbb{Z}[F, V]/(FV - q)$ the diagram

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "r_A(\eta)"'] & B \arrow[d, "r_B(\eta)"] \\ A \arrow[r, "f"] & B \end{tikzcd} \tag{2-5}$$

is commutative, as follows from the naturality of the Frobenius and Verschiebung isogenies, we deduce an R_w-linear structure on the category AV_w. Furthermore, for finite subsets $v \subseteq w$ the R_w-linear structure on AV_v induced by the fully faithful inclusion $\mathsf{AV}_v \subseteq \mathsf{AV}_w$ is compatible, via the surjection $\mathrm{pr}_{v,w}$, with the R_v-linear structure on AV_v.

Remark 5. If $W \subseteq W_q$ is now any subset, denote by $\mathcal{R}_W$ the projective system $(R_w, \mathrm{pr}_{w,v})$ as w ranges through all finite subsets of W, and by AV_W the full subcategory of AV_q whose objects are all abelian varieties A with $w(A) \subseteq W$. We will treat AV_W as the direct 2-limit of the categories AV_w, for finite subsets w of W. The collection of R_w-linear structures on the subcategories $\mathsf{AV}_w \subseteq \mathsf{AV}_W$, which are linked by the compatibility conditions described above, form what we will refer to as the $\mathcal{R}_W$-linear structure on AV_W.

2.4. ***The symmetric polynomial.*** Let π be a Weil q-number. If $\mathbb{Q}(\pi)$ has a real place then $\pi^2 = q$, so that $\mathbb{Q}(\pi)$ is totally real, and $[\mathbb{Q}(\pi) : \mathbb{Q}]$ is either 2 or 1 according to whether the degree $e = [\mathbb{F}_q : \mathbb{F}_p]$ is odd or even, respectively. In the first case there is only one conjugacy class of real Weil q-numbers; in the second one there are two of them, given by the rational integers $q^{e/2}$ and $-q^{e/2}$. In the general case where π is not real, the field $\mathbb{Q}(\pi)$ is a nonreal CM field, with complex conjugation induced by $\pi \mapsto q/\pi$.

The degree $2d = [\mathbb{Q}(\pi) : \mathbb{Q}]$ is even, except for the two rational Weil q-numbers occurring for e even, in which case $d = 1/2$. Set

$$P_\pi(x) = x^{2d} + a_{2d-1}x^{2d-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

for the normalized minimal polynomial of π over $\mathbb{Q}$. The polynomial $P_\pi(x)$ depends only on the conjugacy class of π. The following lemma is well known (see [Howe 1995, Proposition 3.4]):

Lemma 6. *Let π be a nonreal Weil q-number. For $r \geq 0$, we have $a_{d-r} = q^r a_{d+r}$.*

Proof. We can arrange the roots $\alpha_1, \ldots, \alpha_{2d}$ of $P_\pi(x)$ so that α_i and α_{2d+1-i} are complex conjugates of each other, that is, $\alpha_i \alpha_{2d+1-i} = q$. For a subset $I \subseteq \{1, \ldots, 2d\}$ we set $I^c = \{1, \ldots, 2d\} \setminus I$ and $\bar{I} = \{i : 2d + 1 - i \in I\}$; we will use the multiindex notation $\alpha^I = \prod_{i \in I} \alpha_i$. Then, summing over subsets of $\{1, \ldots, 2d\}$, we compute

$$\begin{aligned}(-1)^{d+r} a_{d-r} &= \sum_{|I|=d+r} \alpha^I = \left(\prod_{i=1}^{2d} \alpha_i\right) \cdot \sum_{|I|=d+r} \frac{1}{\alpha^{I^c}} \\ &= q^r \cdot \sum_{|J|=d-r} \frac{q^{d-r}}{\alpha^J} = q^r \cdot \sum_{|J|=d-r} \alpha^{\bar{J}} = q^r (-1)^{d-r} a_{d+r}. \qquad \square\end{aligned}$$

We next construct a symmetric polynomial $h_\pi(F, V) \in \mathbb{Z}[F, V]$. The idea is to consider the rational function $P_\pi(F)/F^d \in \mathbb{Z}[F, q/F]$ (at least when $d \in \mathbb{Z}$), and then formally set $V = q/F$.

Definition 7. We define the *symmetric polynomial* $h_\pi(F, V)$ attached to a Weil q-number π as follows:

(1) If π is a nonreal Weil q-number, then we set

$$h_\pi(F, V) = F^d + a_{2d-1}F^{d-1} + \cdots + a_{d+1}F + a_d + a_{d+1}V + \cdots + a_{2d-1}V^{d-1} + V^d.$$

(2) If $\pi = \pm p^m\sqrt{p}$ is real but not rational, then we set

$$h_\pi(F, V) = F - V.$$

(3) If $\pi = \pm p^m$ is rational, then we set

$$h_{\pm p^m}(F, V) = F^{1/2} \mp V^{1/2}.$$

The polynomial $h_w(F, V)$ just defined belongs to $\mathbb{Z}[F, V]$ if π not rational, and to $\mathbb{Z}[F^{1/2}, V^{1/2}]$ otherwise. It appears already in [Howe 1995, §9].

Lemma 8. (1) *If π is a nonreal Weil q-number, then we have $h_\pi(\pi, q/\pi) = 0$.*

(2) *If π is a real, but not rational, Weil q-number, then $h_\pi(F, V) = F - V$ and $h_\pi(\pi, q/\pi) = 0$.*

(3) *If $\pi = \pm p^m$ is rational, then $h_{p^m}(F, V) \cdot h_{-p^m}(F, V) = F - V$ is again contained in $\mathbb{Z}[F, V]$, and vanishes for $F = \pi$ and $V = q/\pi$.*

Proof. Assertion (1) follows from $h_\pi(\pi, q/\pi) = P_\pi(\pi)/\pi^d = 0$ which is based on Lemma 6. Assertion (2) and (3) are trivial. □

Definition 9. An *ordinary* Weil q-number is a Weil q-number π such that exactly half of the roots of its minimal polynomial $P_\pi(x)$ in an algebraic closure of $\mathbb{Q}_p$ are p-adic units.

A Weil q-number is ordinary if and only if its associated isogeny class of simple abelian varieties over $\mathbb{F}_q$ is ordinary. Real Weil numbers are not ordinary.

Lemma 10. *Let $w \subseteq W_q$ be a finite subset of nonreal conjugacy classes of Weil q-numbers. Then w consists of ordinary conjugacy classes if and only if $h_w(0, 0)$ is not divisible by p.*

Proof. Let $\alpha_1, \dots, \alpha_d, q/\alpha_1, \dots, q/\alpha_d$ be the roots of $\prod_{\pi\in w} P_\pi(x)$. Then

$$h_w(F, V) \equiv \prod_{i=1}^{d}(F - (\alpha_i + q/\alpha_i) + V) \mod (FV - q)$$

so that

$$h_w(F, V) \equiv (-1)^d \prod_{i=1}^{d} (\alpha_i + q/\alpha_i) \mod p.$$

This integer is not divisible by p if and only if the algebraic integers $\alpha_i + q/\alpha_i$ are p-adic units for all i. This happens if and only if either α_i or q/α_i are p-adic units for all i, that is, if w consists of ordinary conjugacy classes. □

2.5. ***Structure of the minimal central orders.*** In what follows we will define the degree of a finite subset $w \subseteq W_q$ by

$$\deg(w) = \mathrm{rk}_{\mathbb{Z}}(R_w) = \sum_{\pi \in w} [\mathbb{Q}(\pi) : \mathbb{Q}].$$

So w is of even degree if and only if w either contains none or both rational Weil q-numbers $\pm q^{e/2}$, which only exist when $e = [\mathbb{F}_q : \mathbb{F}_p]$ is even. Extending this notion, we will say that an arbitrary subset $W \subseteq W_q$ is of even degree if either none or both rational conjugacy classes of Weil q-numbers belong to W.

If $w \subseteq W_q$ is any finite subset, we set

$$h_w(F, V) = \prod_{\pi \in w} h_\pi(F, V),$$

which is contained in $\mathbb{Z}[F, V]$ as soon as w is of even degree.

Theorem 11. *Let $w \subseteq W_q$ be a finite set of Weil q-numbers of even degree.*

(1) *We have $R_w = \mathbb{Z}[F, V]/(FV - q, h_w(F, V))$.*

(2) *The ring R_w is a 1-dimensional complete intersection; in particular, it is a Gorenstein ring.*

When w consists of ordinary Weil q-numbers, part (1) of Theorem 11 is [Howe 1995, Proposition 9.1].

Proof. The ring R_w is reduced as it injects into a product of number fields. Moreover, R_w is a finite $\mathbb{Z}$-algebra, because it is generated by F and V satisfying integral relations in R_w. Thus R_w is free of finite rank as a $\mathbb{Z}$-module and of Krull dimension 1. More precisely, by (2-3) we have

$$\mathrm{rk}_{\mathbb{Z}}(R_w) = \sum_{\pi \in w} [\mathbb{Q}(\pi) : \mathbb{Q}] =: 2D$$

The ring $\mathbb{Z}[F, V]/(FV - q)$ is a normal ring with at most one rational singularity in $\mathfrak{p} = (F, V, p)$. Hence, $h_w(F, V)$ is a nonzero divisor in $\mathbb{Z}[F, V]/(FV - q)$ and it remains to show (1) to conclude the proof of (2).

We now show assertion (1). By Lemma 8 the evaluation of $h_w(F, V)$ in R_π vanishes for all $\pi \in w$. Hence we obtain a surjection

$$\varphi : S = \mathbb{Z}[F, V]/(FV - q, h_w(F, V)) \twoheadrightarrow R_w.$$

We are done if we can show that S is generated by $2D$ elements as a $\mathbb{Z}$-module.

By construction, $h_w(F, V)$ is a product of polynomials of the form

$$f_\pi(F) + g_\pi(V)$$

with $f_\pi, g_\pi \in \mathbb{Z}[X]$ monic (or $-g_\pi$ monic). The degrees are $\deg(f_\pi) = \deg(g_\pi) = [\mathbb{Q}(\pi) : \mathbb{Q}]/2$ if π is nonrational, and 1 if π is rational. Having a representative of the form $f(F) + g(V)$ for monic polynomials f, g (or $-g$) of the same degree is preserved under taking products:

$$\begin{aligned}(f_1(F) + g_1(V))(f_2(F) + g_2(V))& \\ = f_1 f_2(F) + g_1 g_2(V) + &\text{ lower degree terms in } F, V,\end{aligned}$$

where the mixed terms are of lower degree, because $FV = q$ necessarily leads to cancellations.

Hence the same holds for the product: $h_w(F, V) = f(V) + g(V)$ with $\deg(f) = \deg(g) = D$. In particular,

$$F^D, F^{D-1}, \ldots, F, 1, V, \ldots, V^{D-1}$$

generate S as a $\mathbb{Z}$-module. □

Since Theorem 1 deals with abelian varieties over $\mathbb{F}_p$, our main concern in this paper are the commutative algebra properties of R_w for finite subsets of W_p. Here Theorem 11 covers all cases. In order to complete the picture, we answer what happens if $w \subseteq W_q$ contains exactly one rational conjugacy class of Weil q-numbers.

Theorem 12. *Let q be the square of a positive or negative integer $\sqrt{q} \in \mathbb{Z}$. Let $v \subseteq W_q$ be a finite set containing no rational conjugacy class, and set $w = v \cup \{\sqrt{q}\}$.*

(1) *We have $R_w = \mathbb{Z}[F, V]/\big(FV - q, h_v(F, V)(F - \sqrt{q}), h_v(F, V)(V - \sqrt{q})\big)$.*

(2) *The ring R_w is Gorenstein if and only if all conjugacy classes of Weil q-numbers in v are ordinary.*

Proof. Reasoning as in the proof of Lemma 8, we see that the defining quotient map $\mathbb{Z}[F, V]/(FV - q) \to R_w$ factors as a surjective map

$$S = \mathbb{Z}[F, V]/\big(FV - q, h_v(F, V)(F - \sqrt{q}), h_v(F, V)(V - \sqrt{q})\big) \twoheadrightarrow R_w.$$

As in Theorem 11, as a $\mathbb{Z}$-module, the ring R_w is free of rank

$$\mathrm{rk}_{\mathbb{Z}}(R_w) = 1 + \sum_{\pi \in v} [\mathbb{Q}(\pi) : \mathbb{Q}] =: 2D + 1.$$

It is easy to see that S is generated as a $\mathbb{Z}$-module by

$$F^D, F^{D-1}, \dots, F, 1, V, \dots, V^D.$$

This shows assertion (1) above.

For assertion (2), we first note that after inverting one of the elements p, F or V, the three relations can be reduced to two relations, so that outside of (p, F, V) the ring R_w is a local complete intersection and hence Gorenstein. It remains to discuss the local ring in $\mathfrak{p} = (p, F, V)$.

There is a unique polynomial $h \in \mathbb{Z}[X]$ such that

$$h_v(F, V) = h(F) - h(0) + h(V) \in \mathbb{Z}[F, V],$$

and for this h we have $h(0) = h_v(0, 0)$. Since $\mathbb{Z}$ is regular (hence Gorenstein) and R_w is a flat $\mathbb{Z}$-algebra, it follows from [Matsumura 1989, Theorem 23.4] that R_w is Gorenstein in $\mathfrak{p}$ if and only if

$$R_w/pR_w = \mathbb{F}_p[F, V]/(FV, h(F)F, h(V)V)$$

is Gorenstein in $\bar{\mathfrak{p}} = (F, V)$. The ring R_w/pR_w is Artinian, hence of dimension 0, so that by [Matsumura 1989, Theorem 18.1] the ring $(R_w/pR_w)_{\bar{\mathfrak{p}}}$ is Gorenstein if and only if

$$1 = \dim_{\mathbb{F}_p} \operatorname{Hom}(\kappa(\bar{\mathfrak{p}}), R_w/pR_w).$$

The space of homomorphisms has the same dimension as the socle, i.e., the maximal submodule annihilated by (F, V). The socle is the intersection of the kernels of F and V as $\mathbb{F}_p$-linear maps of R_w, which can be easily evaluated in the basis $F^D, F^{D-1}, \dots, F, 1, V, \dots, V^D$. The intersection is 1-dimensional if $p \nmid h(0)$, and it is 2-dimensional otherwise. By Lemma 10, this completes the proof. □

3. Remarks on reflexive modules

3.1. ***Reflexive versus $\mathbb{Z}$-free.*** Let S be a noetherian ring. Recall that a finitely generated S-module M is *reflexive* (resp. *torsionless*) if the natural map

$$M \to \operatorname{Hom}_S(\operatorname{Hom}_S(M, S), S)$$

is an isomorphism (resp. injective). We denote the category of finitely generated reflexive S-modules by $\mathsf{Refl}(S)$.

Lemma 13. *Let $w \subseteq W_q$ be a finite set of Weil q-numbers such that R_w is Gorenstein, and let ℓ be a prime number. Let M be a finitely generated R_w-module (resp. $R_w \otimes \mathbb{Z}_\ell$-module). The following are equivalent:*

(a) *M is reflexive.*

(b) *M is torsionless.*

(c) *M is free as a $\mathbb{Z}$-module (resp. $\mathbb{Z}_\ell$-module).*

Proof. Assertions (a) and (b) are equivalent by [Bass 1963, Theorem 6.2(4)], since R_w is Gorenstein and of dimension 1.

For a uniform treatment, we set $S = R_w \otimes \Lambda$ with $\Lambda = \mathbb{Z}$ (resp. $\Lambda = \mathbb{Z}_\ell$). Since S is finite flat over Λ, the dual module $\mathrm{Hom}_S(M, S)$ is free as a Λ-module. The same holds for every submodule of $\mathrm{Hom}_S(M, S)$, which shows assertion (b) implies (c).

For the converse direction we introduce the total ring of fractions $S \subset K = S \otimes_{\mathbb{Z}} \mathbb{Q}$, which is a product of fields. Therefore, assuming (c), the composite map

$$M \to M \otimes_{\mathbb{Z}} \mathbb{Q} = M \otimes_S K \to \mathrm{Hom}_S(\mathrm{Hom}_K(M \otimes_S K, K), K)$$

is injective. And since it factors over the natural map $M \to \mathrm{Hom}_S(\mathrm{Hom}_S(M, S), S)$, the latter is also injective and hence M is torsionless. □

3.2. *The main theorem with reflexive modules.* Let $w \subseteq W_q$ be a finite set of conjugacy classes of Weil q-numbers of even degree (see Section 2.5), so that, in particular, R_w is Gorenstein (see Theorem 11). For an object M of $\mathsf{Refl}(R_w)$, let (M_0, F_M) be the pair consisting of the $\mathbb{Z}$-module M_0 underlying M and of the linear map $F_M : M_0 \to M_0$ given by the action of $F_w \in R_w$ on M.

Proposition 14. *The functor $M \mapsto (M_0, F_M)$ gives an equivalence between* $\mathsf{Refl}(R_w)$ *and the category of pairs (T, F) consisting of a finite, free $\mathbb{Z}$-module T, and an endomorphism $F : T \to T$ satisfying the following conditions:*

(i) *$F \otimes \mathbb{Q}$ is semisimple with eigenvalues given by Weil q-numbers in w.*

(ii) *There exists $V : T \to T$ such that $FV = q$.*

A morphism between two such pairs (T, F) and (T', F') is a linear map $f : T \to T'$ such that $fF = F'f$.

Proof. Thanks to Lemma 13, an R_w-module belongs to $\mathsf{Refl}(R_w)$ if and only if it is finite and free as a $\mathbb{Z}$-module. Moreover, the linear map $F_M : M_0 \to M_0$ satisfies in the ring $\mathrm{End}_{\mathbb{Z}}(M_0)$ the polynomial

$$F^d \cdot h_w(F, q/F) = \prod_{\pi \in w} P_\pi(F),$$

which is squarefree. Therefore $F_M \otimes \mathbb{Q}$ is semisimple with eigenvalues given by Weil q-numbers whose conjugacy classes belong to w. The map $V_M : M_0 \to M_0$ induced by the action of $V_w \in R_w$ on M satisfies $V_M F_M = q$. Essential surjectivity of the functor follows easily from Lemma 13. □

Let now $v \subseteq w$ be a finite subset which is also of even degree. By Lemma 13, the natural projection $\mathrm{pr}_{v,w} : R_w \to R_v$ gives a fully faithful embedding

$$\mathsf{Refl}(R_v) \subseteq \mathsf{Refl}(R_w),$$

by means of which $\mathsf{Refl}(R_v)$ can be regarded as the full subcategory whose objects are those for which the R_w-action factors over $\mathrm{pr}_{v,w} : R_w \to R_v$. Using the description of Proposition 14, we easily see that an object M of $\mathsf{Refl}(R_w)$ lies in $\mathsf{Refl}(R_v)$ if and only if the eigenvalues of $F_M \otimes \mathbb{Q} : M_0 \otimes \mathbb{Q} \to M_0 \otimes \mathbb{Q}$ define conjugacy classes of Weil q-numbers in v.

Definition 15. Let $W \subseteq W_q$ be a subset of even degree, and $\mathcal{R}_W = (R_w)$ be the pro-ring with w ranging over all finite subsets of W of even degree. The category

$$\mathsf{Refl}(\mathcal{R}_W) := \varinjlim_{w \subseteq W} \mathsf{Refl}(R_w)$$

is the full subcategory of the category of $\mathbb{Z}[F, V]$-modules given by all M such that:

(1) There exists $w_M \subseteq W$ such that the structural action of $\mathbb{Z}[F, V]$ on M factors through $\mathbb{Z}[F, V] \to R_{w_M}$ (and hence through $\mathbb{Z}[F, V] \to R_w$ for all w containing w_M).

(2) For any finite $w \subseteq W$ of even degree containing w_M, the module M is reflexive as an R_w-module.

Notice that condition (2) is equivalent to asking that M be a reflexive module over R_w for some $w \subseteq W$ of even degree such that the action of R_w on M is defined (see Lemma 13).

Remark 16. For any finite $w \subseteq W$ of even degree, the category $\mathsf{Refl}(\mathcal{R}_W)$ contains the R_w-linear category $\mathsf{Refl}(R_w)$ as a full subcategory. Moreover, if $v \subseteq w$ are finite subsets of W of even degree, then the R_v-linear structure on $\mathsf{Refl}(R_v)$ induced from the fully faithful embedding $\mathsf{Refl}(R_v) \subseteq \mathsf{Refl}(R_w)$ is compatible, via the surjection $\mathrm{pr}_{v,w} : R_w \to R_v$, with the natural R_w-linear structure. Formally we are in a situation analogous to that described in Remark 5, where the category AV_W played the role of $\mathsf{Refl}(\mathcal{R}_W)$. We will then refer to this data as the $\mathcal{R}_W$-linear structure of $\mathsf{Refl}(\mathcal{R}_W)$.

The category $\mathsf{Refl}(\mathcal{R}_W)$ can be given a concrete description in terms of pairs (T, F) given by a finite free $\mathbb{Z}$-module T and a linear map $F : T \to T$ such that:

(i) $F \otimes \mathbb{Q}$ is semisimple and its eigenvalues are Weil q-numbers in W.

(ii) There exists $V : T \to T$ with $FV = q$.

The notion of morphism between two such pairs is clear. This can be seen reasoning as in Proposition 14, and using the compatibility of linear structures described in Remark 16.

Denote now the set $W_p \setminus \{\sqrt{p}\}$ of nonreal conjugacy classes of Weil p-numbers simply by W_p^{com}, and the corresponding pro-ring $\mathcal{R}_{W_p^{\mathrm{com}}}$ by $\mathcal{R}_p^{\mathrm{com}}$. Theorem 1 then claims the existence of a contravariant, $\mathcal{R}_{W_p^{\mathrm{com}}}$-linear, ind-representable equivalence

$$T : \mathsf{AV}_p^{\mathrm{com}} \to \mathsf{Refl}(\mathcal{R}_p^{\mathrm{com}})$$

such that $T(A)$ is a lattice of rank $2\dim(A)$. By definition, the $\mathcal{R}_{W_p^{\mathrm{com}}}$-linearity of $T(-)$ is the requirement that for any finite $w \subseteq W_p^{\mathrm{com}}$ the restriction of T to AV_w has values in $\mathsf{Refl}(R_w)$ and is R_w-linear. These conditions amount precisely to the equality $F = T(\pi_A)$ for all A in $\mathsf{AV}_p^{\mathrm{com}}$.

3.3. ***Further remarks.*** The following piece of homological algebra is used later:

Lemma 17. *Let S be a 1-dimensional Gorenstein ring. For any finitely generated reflexive S-module M, we have*

$$\mathrm{Ext}^1_S(M, S) = 0.$$

Proof. We use a free presentation of the dual $\mathrm{Hom}_S(M, S)$ and dualize again. This yields an embedding of M into a free S-module and then a short exact sequence

$$0 \longrightarrow M \longrightarrow S^n \longrightarrow M' \longrightarrow 0.$$

The Ext-sequence, and the fact that S has injective dimension 1 [Bass 1963, §1], yield

$$0 = \mathrm{Ext}^1_S(S^n, S) \longrightarrow \mathrm{Ext}^1_S(M, S) \longrightarrow \mathrm{Ext}^2_S(M', S) = 0$$

from which the lemma follows. □

Finally, here is a criterion for invertible reflexive modules in terms of their endomorphism algebras:

Proposition 18. *Let S be a reduced Gorenstein ring of dimension at most* 1, *and let M be a reflexive module. Then the following are equivalent*:

(a) *M is locally free of rank* 1.

(b) *The natural map $S \to \mathrm{End}_S(M)$ is an isomorphism.*

Proof. If M is locally free of rank 1, then $\mathrm{End}_S(M) \simeq M^\vee \otimes M \simeq S$, where $M^\vee = \mathrm{Hom}_S(M, S)$, and (b) holds.

For the converse, we may assume that S is a complete local ring by passing to the completion. Since $\mathrm{End}_S(M) = S$ we have $M \neq 0$, and, moreover, M cannot be a module (extending the S-module structure) for a strictly larger subring of the total ring of fractions of S. Now [Bass 1963, Proposition 7.2] shows that M has a nonzero projective direct summand M_0. With $M = M_0 \oplus M_1$, we find

$$S \times \mathrm{End}_S(M_1) = \mathrm{End}_S(M_0) \times \mathrm{End}_S(M_1) \subseteq \mathrm{End}_S(M) = S$$

and therefore $\mathrm{End}_S(M_1) = 0$. This forces $M_1 = 0$, and M is projective. Then $\mathrm{End}_S(M)$ is projective with rank equal to the square of the rank of M (as a locally constant function on $\mathrm{Spec}(S)$). Thus M is of rank 1 and the proof is complete. □

4. Abelian varieties with minimal endomorphism algebra

Before restricting to the case $q = p$, we recall the following classical result of Tate (see [Tate 1966, §1] for $\ell \neq p$, [Waterhouse and Milne 1971, Theorem 6] for any ℓ, also [Chai et al. 2014, §A.1]) which will be used frequently. For A an abelian variety over $\mathbb{F}_q$ and ℓ a prime number, denote by $A[\ell^\infty]$ the ℓ-divisible group corresponding to A.

Theorem 19 (Tate). *Let A, B be abelian varieties over $\mathbb{F}_q$, and ℓ a prime number. The natural map $f \mapsto f[\ell^\infty]$ induces an isomorphism*

$$\mathrm{Hom}_{\mathbb{F}_q}(A, B) \otimes \mathbb{Z}_\ell \xrightarrow{\sim} \mathrm{Hom}(A[\ell^\infty], B[\ell^\infty]).$$

As is well known, the isomorphism of Tate's theorem takes a more concrete form as follows. If $\ell \neq p$, it can be formulated in terms of Galois representations, and says that the functor ℓ-adic Tate module $T_\ell(-)$ induces an isomorphism

$$\mathrm{Hom}_{\mathbb{F}_q}(A, B) \otimes \mathbb{Z}_\ell \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}_\ell[\mathrm{Gal}_{\mathbb{F}_q}]}(T_\ell(A), T_\ell(B)).$$

If $\ell = p$, using the language of Dieudonné modules, Tate's theorem translates into the fact that the functor contravariant Dieudonné module $T_p(-)$ induces an isomorphism

$$\mathrm{Hom}_{\mathbb{F}_q}(A, B) \otimes \mathbb{Z}_p \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{D}_{\mathbb{F}_q}}(T_p(B), T_p(A)),$$

where $\mathcal{D}_{\mathbb{F}_q}$ is the Dieudonné ring of $\mathbb{F}_q$.

Remark 20. For any prime ℓ the R_w-linear structure on the category AV_w defined in Section 2.1 induces an enrichment of the functor $T_\ell(-)$ to left $R_w \otimes \mathbb{Z}_\ell$-modules for $\ell \neq p$, and to right[1] $R_w \otimes \mathbb{Z}_p$-modules for $\ell = p$.

For any $A \in \mathsf{AV}_w$ and any $\ell \neq p$, the action of the arithmetic Frobenius of $\mathbb{F}_q$ on $T_\ell(A)$ agrees with the action of $F_w \otimes 1 \in R_w \otimes \mathbb{Z}_\ell$, and we have a natural identification

$$\mathrm{Hom}_{\mathbb{Z}_\ell[\mathrm{Gal}_{\mathbb{F}_p}]}(T_\ell(A), T_\ell(B)) = \mathrm{Hom}_{R_w \otimes \mathbb{Z}_\ell}(T_\ell(A), T_\ell(B))$$

for $\ell \neq p$ and all $A, B \in \mathsf{AV}_w$. In the special case where $q = p$, and only in this case, the Dieudonné ring $\mathcal{D}_{\mathbb{F}_q}$ is commutative, and hence the theory of Dieudonné

[1] We employ the contravariant Dieudonné theory; therefore the left R_w-module structure of the Hom-groups in AV_w turns into a right $R_w \otimes \mathbb{Z}_p$-modules structure on the corresponding Dieudonné modules. However R_w is commutative, hence for A in AV_w we can safely treat $T_p(A)$ as a left $R_w \otimes \mathbb{Z}_p$-module.

modules of abelian varieties over the prime field $\mathbb{F}_p$ does not involve semilinearity aspects. For any $A \in \mathsf{AV}_w$ the action of $\mathcal{D}_{\mathbb{F}_p}$ on $T_p(A)$ factors through the quotient $\mathcal{D}_{\mathbb{F}_p} \twoheadrightarrow R_w \otimes \mathbb{Z}_p$, and Tate's theorem says that

$$\mathrm{Hom}_{\mathcal{D}_{\mathbb{F}_p}}(T_p(A), T_p(B)) = \mathrm{Hom}_{R_w \otimes \mathbb{Z}_p}(T_p(B), T_p(A))$$

for all $A, B \in \mathsf{AV}_w$. So, roughly speaking, the Dieudonné theory of abelian varieties over the prime field is analogous to the theory of Tate modules at primes $\ell \neq p$, up to replacing covariance with contravariance.

For any $\pi \in W_p$, we choose a simple abelian variety B_π over $\mathbb{F}_p$ whose associated Weil p-number represents π.

Proposition 21. *Let $w \subseteq W_p$ be a finite set of conjugacy classes of Weil p-numbers not containing $\sqrt{p}$. There exists an abelian variety A_w over $\mathbb{F}_p$ isogenous to $\prod_{\pi \in w} B_\pi$ such that $T_\ell(A_w)$ is free of rank 1 over $R_w \otimes \mathbb{Z}_\ell$ for all primes ℓ. Furthermore, for any such A_w, the natural map*

$$R_w \to \mathrm{End}_{\mathbb{F}_p}(A_w)$$

is an isomorphism.

Remark 22. In the case where w consists of just one Weil p-number, the abelian variety A_w in Proposition 21 was already considered by Waterhouse [1969, Theorem 6.1]. We observe that the product $\prod_{\pi \in w} A_{\{\pi\}}$ of the varieties constructed for each singleton $\{\pi\} \subset w$ may well fail to serve as the A_w satisfying the properties of Proposition 21. This failure is explained by a phenomenon analogous to congruences between Weil q-numbers, discussed in Example 3.

Proof. Let B be any abelian variety over $\mathbb{F}_p$ isogenous to $\prod_{\pi \in w} B_\pi$. For any $\pi \in W_p$ with $\pi \not\sim \sqrt{p}$, it is straightforward to verify using Honda–Tate theory [Tate 1971, Théorème 1(ii)] that

(i) all local invariants of the division ring $\mathrm{End}^0_{\mathbb{F}_p}(B_\pi)$ are trivial,

(ii) $[\mathbb{Q}(\pi) : \mathbb{Q}] = 2\dim(B_\pi)$.

In fact, each of these conditions is equivalent to the commutativity of $\mathrm{End}_{\mathbb{F}_p}(B_\pi)$.

Since the abelian varieties B_π, $\pi \in w$, are pairwise nonisogenous, we have that $\mathrm{End}_{\mathbb{F}_p}(B)$ is also commutative, and isomorphic to an order of the product of CM fields $\prod_{\pi \in w} \mathbb{Q}(\pi)$. We deduce the chain of equalities

$$\mathrm{rk}_{\mathbb{Z}}(\mathrm{End}_{\mathbb{F}_p}(B)) = \sum_{\pi \in w} [\mathbb{Q}(\pi) : \mathbb{Q}] = \sum_{\pi \in w} 2\dim(B_\pi) = 2\dim(B).$$

From the injectivity of the isomorphism of Theorem 19, and using the language of Dieudonné modules if $\ell = p$, it follows that the action of $R_w \otimes \mathbb{Q}_\ell = \prod_{\pi \in w} \mathbb{Q}(\pi) \otimes \mathbb{Q}_\ell$ on

$$V_\ell(B) = T_\ell(B) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$$

is faithful. Hence $V_\ell(B)$ has rank 1 over $\prod_{\pi\in w}\mathbb{Q}(\pi)\otimes\mathbb{Q}_\ell$, since they both have dimension $2\dim(B)$ over $\mathbb{Q}_\ell$ (notice that $\dim_{\mathbb{Q}_p}(V_p(B)) = 2\dim(B)$ because we work over $\mathbb{F}_p$).

Therefore, for every ℓ we can choose an $R_w\otimes\mathbb{Z}_\ell$-lattice

$$\Lambda_\ell \subset V_\ell(B)$$

which is free of rank 1, and which contains $T_\ell(B)$ if $\ell\neq p$ and is contained in $T_p(B)$ if $\ell = p$.

If $R_w\otimes\mathbb{Z}_\ell$ is the maximal order of $\prod_{\pi\in w}\mathbb{Q}(\pi)\otimes\mathbb{Q}_\ell$, as occurs for almost all ℓ, then $T_\ell(B)$ is necessarily free of rank 1 over $R_w\otimes\mathbb{Z}_\ell$ and we take $\Lambda_\ell = T_\ell(B)$.

Now, if $\ell\neq p$, then the finite subgroup

$$N_\ell = \Lambda_\ell/T_\ell(B) \subset B[\ell^\infty],$$

being an R_w-submodule, is stable under Frobenius and hence is defined over $\mathbb{F}_p$. The corresponding isogeny $\psi_\ell : B\to B/N_\ell$ induces an identification $\Lambda_\ell \simeq T_\ell(B/N_\ell)$ of $R_w\otimes\mathbb{Z}_\ell$-modules.

Similarly, the p-power degree isogeny $\psi_p : B\to B/N_p$, where N_p is the $\mathbb{F}_p$-subgroup-scheme of B corresponding to the Dieudonné module $T_p(B)/\Lambda_p$, induces an identification $T_p(B/N_p)\simeq\Lambda_p$ of $R_w\otimes\mathbb{Z}_p$-modules. Therefore, after applying a finite sequence of isogenies to B, we obtain the abelian variety A_w with the desired property.

Lastly, by Theorem 19, the natural map

$$R_w \to \mathrm{End}_{\mathbb{F}_p}(A_w)$$

is an isomorphism after $-\otimes\mathbb{Z}_\ell$ for all prime numbers ℓ, since $T_\ell(A_w)\simeq R_w\otimes\mathbb{Z}_\ell$. Therefore the last statement of the proposition follows. □

Remark 23. One can show that there is a free and transitive action of the Picard group $\mathrm{Pic}(R_w)$ on the set of isomorphism classes of abelian varieties A_w satisfying the conditions of Proposition 21 (see [Waterhouse 1969, Theorem 6.1.3] for the case of simple abelian varieties, i.e., $w = \{\pi\}$). We will discuss this below in Section 7.3.

The Gorenstein property of R_w allows the following useful characterization of the abelian varieties A_w satisfying the property of Proposition 21 (see also the end of §4 in [Serre and Tate 1968]).

Proposition 24. *Let $w\subseteq W_p$ be a finite set of conjugacy classes of Weil p-numbers not containing $\sqrt{p}$, and let A be an abelian variety over $\mathbb{F}_p$ isogenous to $\prod_{\pi\in w} B_\pi$. The following conditions are equivalent*:

(a) *$T_\ell(A)$ is free of rank 1 over $R_w\otimes\mathbb{Z}_\ell$, for all primes ℓ.*

(b) *$\mathrm{End}_{\mathbb{F}_p}(A)$ is equal to the minimal central order R_w.*

Proof. Thanks to Proposition 21, we only need to show that (b) implies (a). Since R_w is Gorenstein by Theorem 11, its completion $R_w \otimes \mathbb{Z}_\ell$ is also Gorenstein. It follows from [Bass 1963, Theorem 6.2] that the torsion-free $R_w \otimes \mathbb{Z}_\ell$-module $T_\ell(A)$ is reflexive.

By (b) and Theorem 19 we have $\mathrm{End}_{R_w \otimes \mathbb{Z}_\ell}(T_\ell(A)) = R_w \otimes \mathbb{Z}_\ell$, so Proposition 18 yields that $T_\ell(A)$ is projective of rank 1. Since $R_w \otimes \mathbb{Z}_\ell$ is a finite $\mathbb{Z}_\ell$-algebra, hence a product

$$R_w \otimes \mathbb{Z}_\ell = \prod_\lambda R_\lambda$$

of complete local rings R_λ, its Picard group is trivial and $T_\ell(A)$ is free of rank 1 as an $R_w \otimes \mathbb{Z}_\ell$-module. □

We conclude the section by observing that if A is an abelian variety over $\mathbb{F}_q$, for q arbitrary, the Dieudonné module $T_p(A)$ has rank $2\dim(A)$ over the Witt vectors $W(\mathbb{F}_q)$ of $\mathbb{F}_q$. It follows that the naive analogue of (a) can never be attained if $q > p$ for rank reasons, and the above proposition is peculiar to the $q = p$ case.

5. Construction of the antiequivalence

In this section we give a proof of Theorem 1. Recall from Remark 5 that for a subset $W \subseteq W_q$ of conjugacy classes of Weil q-numbers, the category AV_W is the full subcategory of AV_q consisting of all abelian varieties A over $\mathbb{F}_q$ whose support $w(A)$ is contained in W.

5.1. *Finite Weil support.*

We begin by defining the lattice $T(A)$ and its endomorphism F on the increasing family of subcategories

$$\mathsf{AV}_w \subseteq \mathsf{AV}_p^{\mathrm{com}}$$

for finite subsets $w \subseteq W_p^{\mathrm{com}}$.

Let us then assume that $\sqrt{p} \notin w$, and pick an abelian variety A_w satisfying the condition of Proposition 21 for w. For any object A of AV_w there is a natural $R_w = \mathrm{End}_{\mathbb{F}_p}(A_w)$-module structure on

$$\mathrm{M}_w(A) := \mathrm{Hom}_{\mathbb{F}_p}(A, A_w).$$

This is the same R_w-structure described in Remark 5.

Theorem 25. *Let $w \subseteq W_p$ be a finite set of nonreal conjugacy classes of Weil p-numbers. The functor $\mathrm{M}_w(-)$ induces an antiequivalence*

$$\mathsf{AV}_w \to \mathsf{Refl}(R_w).$$

The $\mathbb{Z}$-rank of $\mathrm{M}_w(A)$ *is* $2\dim(A)$.

Proof. We begin by showing that $\mathrm{M}_w(-)$ is fully faithful. The map

$$f : \mathrm{Hom}_{\mathbb{F}_p}(A', A'') \to \mathrm{Hom}_{R_\pi}(\mathrm{M}_w(A''), \mathrm{M}_w(A'))$$

is a homomorphism of finitely generated $\mathbb{Z}$-modules, and hence it is an isomorphism if and only if it is an isomorphism after scalar extension $- \otimes \mathbb{Z}_\ell$ for all primes ℓ.

We first treat the case $\ell \neq p$. For $N \in \mathsf{Refl}(R_w \otimes \mathbb{Z}_\ell)$, set

$$N^\vee = \mathrm{Hom}_{R_w \otimes \mathbb{Z}_\ell}(N, T_\ell(A_w)),$$

which is isomorphic to the $R_w \otimes \mathbb{Z}_\ell$-dual of N, in view of our choice of A_w. The isomorphism of Theorem 19 gives a natural isomorphism of contravariant functors

$$(T_\ell(-))^\vee = \mathrm{Hom}_{R_w \otimes \mathbb{Z}_\ell}(T_\ell(-), T_\ell(A_w)) \simeq \mathrm{M}_w(-) \otimes \mathbb{Z}_\ell \tag{5-1}$$

on AV_w (see Remark 20). This translates into the commutative diagram

$$\begin{tikzcd}
\mathrm{Hom}_{\mathbb{F}_p}(A', A'') \otimes \mathbb{Z}_\ell \arrow[r, "\simeq"] \arrow[d, "f \otimes \mathbb{Z}_\ell"] & \mathrm{Hom}_{R_w \otimes \mathbb{Z}_\ell}(T_\ell(A'), T_\ell(A'')) \arrow[d, "(-)^\vee"] \\
\mathrm{Hom}_{R_w}(\mathrm{M}_w(A''), \mathrm{M}_w(A')) \otimes \mathbb{Z}_\ell \arrow[r, "\simeq"] & \mathrm{Hom}_{R_w \otimes \mathbb{Z}_\ell}(T_\ell(A'')^\vee, T_\ell(A')^\vee)
\end{tikzcd}$$

where both horizontal maps are isomorphisms as a consequence of Theorem 19. Since $R_w \otimes \mathbb{Z}_\ell$ is a completion of a Gorenstein ring by Theorem 11, it is itself Gorenstein. Because $T_\ell(A_w)$ is free of rank 1, this implies that $N \mapsto N^\vee$ is an contravariant autoequivalence of $\mathsf{Refl}(R_w \otimes \mathbb{Z}_\ell)$ [Bass 1963, Theorem 6.2]. Therefore the right vertical map in the diagram is an isomorphism, and we conclude that $f \otimes \mathbb{Z}_\ell$ is an isomorphism as well.

Concerning the case $\ell = p$, for any $N \in \mathsf{Refl}(R_w \otimes \mathbb{Z}_p)$ we set

$$N_\vee = \mathrm{Hom}_{R_w \otimes \mathbb{Z}_p}(T_p(A_w), N).$$

The isomorphism of Theorem 19 then gives a natural isomorphism of contravariant functors

$$(T_p(-))_\vee = \mathrm{Hom}_{R_w \otimes \mathbb{Z}_p}(T_p(A_w), T_p(-)) \simeq \mathrm{M}_w(-) \otimes \mathbb{Z}_p \tag{5-2}$$

on AV_w, which translates into the commutative diagram

$$\begin{tikzcd}
\mathrm{Hom}_{\mathbb{F}_p}(A', A'') \otimes \mathbb{Z}_p \arrow[r, "\simeq"] \arrow[d, "f \otimes \mathbb{Z}_p"] & \mathrm{Hom}_{R_w \otimes \mathbb{Z}_p}(T_p(A''), T_p(A')) \arrow[d, "(-)_\vee"] \\
\mathrm{Hom}_{R_w}(\mathrm{M}_w(A''), \mathrm{M}_w(A')) \otimes \mathbb{Z}_p \arrow[r, "\simeq"] & \mathrm{Hom}_{R_w \otimes \mathbb{Z}_p}(T_p(A'')_\vee, T_p(A')_\vee)
\end{tikzcd}$$

The horizontal maps are isomorphisms by Theorem 19. Since $T_p(A_w)$ is free of rank 1 over $R_w \otimes \mathbb{Z}_p$, the right vertical map in the diagram is an isomorphism. We conclude that $f \otimes \mathbb{Z}_p$ is an isomorphism as well.

We have now established that the functor $A \mapsto \mathrm{M}_w(A)$ from AV_w to the category $\mathsf{Refl}(R_w)$ is fully faithful.

In order to show that $\mathrm{M}_w(-)$ is an equivalence, we must now show that this functor is essentially surjective. Let $M \in \mathsf{Refl}(R_w)$ be a reflexive module. Since R_w is Gorenstein, the natural map $M \to \mathrm{Hom}_{R_w}(\mathrm{Hom}_{R_w}(M, R_w), R_w)$ is an isomorphism. Dualizing a presentation of the dual $\mathrm{Hom}_{R_w}(M, R_w)$ leads to a copresentation

$$0 \longrightarrow M \longrightarrow (R_w)^n \xrightarrow{\psi} (R_w)^m.$$

Since $\mathrm{M}_w(A_w) = \mathrm{End}_{\mathbb{F}_p}(A_w) = R_w$, we find by full faithfulness of $\mathrm{M}_w(-)$ a homomorphism

$$\Psi : (A_w)^m \to (A_w)^n$$

with $\psi = \mathrm{M}_w(\Psi)$. The cokernel

$$B = \mathrm{coker}(\Psi)$$

exists and is an abelian variety $B \in \mathsf{AV}_w$. By definition of the cokernel, the functor $\mathrm{M}_w(-)$ is left-exact; hence

$$0 \longrightarrow \mathrm{M}_w(B) \longrightarrow \mathrm{M}_w((A_w)^n) \xrightarrow{\mathrm{M}_w(\Psi)} \mathrm{M}_w((A_w)^m),$$

and so

$$M \simeq \mathrm{M}_w(B)$$

as R_w-modules. This completes the proof of essential surjectivity.

We are only left with showing that $\mathrm{rk}_{\mathbb{Z}}(\mathrm{Hom}_{\mathbb{F}_p}(A, A_w)) = 2\dim(A)$ for all A in AV_w. The statement is additive in A and depends only on the isogeny class of A and A_w. Recall that for any $\pi \in W_p$ we have chosen a simple abelian variety B_π over $\mathbb{F}_p$ whose associated Weil p-number represents π. Because A_w is isogenous to $\prod_{\pi \in w} B_\pi$, it is enough to show that for any $\pi \in w$ we have

$$\mathrm{rk}_{\mathbb{Z}}\Bigg(\mathrm{Hom}_{\mathbb{F}_p}\Bigg(B_\pi, \prod_{\pi' \in w} B_{\pi'}\Bigg)\Bigg) = 2\dim(B_\pi).$$

This follows from the equality $\mathrm{rk}_{\mathbb{Z}}(\mathrm{End}_{\mathbb{F}_p}(B_\pi)) = 2\dim(B_\pi)$ for all Weil p-numbers $\pi \not\sim \sqrt{p}$ [Tate 1971, Théorème 1(ii)], and the proof of the theorem is complete. □

5.2. ***The direct system.*** In order to prove Theorem 1, we construct a direct system $\mathcal{A} = \varinjlim A_w$ consisting of abelian varieties A_w indexed by finite sets w of Weil p-numbers not containing $\sqrt{p}$, and having the property stated in Proposition 21.

Let $v \subseteq w$ be two finite sets of nonreal Weil p-numbers. By means of the canonical surjection

$$\mathrm{pr}_{v,w} : R_w \twoheadrightarrow R_v,$$

we may consider R_v-modules as R_w-modules such that the action factors over $\mathrm{pr}_{v,w}$. Lemma 13 shows that

$$\mathsf{Refl}(R_v) \subseteq \mathsf{Refl}(R_w)$$

is a full subcategory. After choosing abelian varieties A_v and A_w as in Proposition 21, associated to the sets v and w respectively, we obtain a diagram of functors

$$\begin{tikzcd} \mathsf{AV}_w \arrow[r, "\mathrm{Hom}_{\mathbb{F}_p}(-\,,A_w)"] & \mathsf{Refl}(R_w) \\ \mathsf{AV}_v \arrow[u, hook] \arrow[r, "\mathrm{Hom}_{\mathbb{F}_p}(-\,,A_v)"] & \mathsf{Refl}(R_v) \arrow[u, hook] \end{tikzcd} \tag{5-3}$$

where the vertical functors are natural full subcategories. This diagram need not commute for arbitrary unrelated choices A_w and A_v. The next proposition shows that for every A_w there is a canonical abelian subvariety $A_{v,w} \subseteq A_w$ that leads to a choice of A_v for which (5-3) commutes.

Proposition 26. *Let w be a set of nonreal conjugacy classes of Weil p-numbers, let A_w be an abelian variety over $\mathbb{F}_p$ such that $\mathrm{End}_{\mathbb{F}_p}(A_w) = R_w$, and let $v \subseteq w$ be any subset. Then the subgroup generated by all images*

$$A_{v,w} := \langle \mathrm{im}(f) : f : B \to A_w,\, B \in \mathsf{AV}_v \rangle \subseteq A_w$$

satisfies the following:

(1) *$A_{v,w}$ belongs to AV_v and is an abelian subvariety of A_w.*

(2) *$T_\ell(A_{v,w})$ is free of rank 1 over $R_v \otimes \mathbb{Z}_\ell$ for all primes ℓ.*

(3) *The diagram (5-3) commutes when A_w is chosen to be the abelian variety associated to w and $A_v = A_{v,w}$ as that associated to v.*

(4) *The abelian variety $A_{v,w}$ is the image of any map $f : B \to A_w$ such that $w(B) = v$ and $w(\mathrm{coker}(f)) = w \setminus v$.*

Proof. Assertion (1) is obvious and assertion (3) follows from the natural equality

$$\mathrm{Hom}_{\mathbb{F}_p}(B, A_{v,w}) = \mathrm{Hom}_{\mathbb{F}_p}(B, A_w)$$

for every $B \in \mathsf{AV}_v$, since every morphism $f : B \to A_w$ takes values in the subvariety $A_{v,w} \subseteq A_w$.

Assertion (4) is obvious once we pass to the semisimple category of abelian varieties up to isogeny. Therefore $f(B)$ and $A_{v,w}$ have the same dimension. Since by definition $f(B) \subseteq A_{v,w}$, we obtain the claimed equality.

It remains to verify assertion (2), which by Proposition 24 is equivalent to $\mathrm{End}_{\mathbb{F}_p}(A_{v,w}) = R_v$. The natural map

$$R_w = \mathrm{End}_{\mathbb{F}_p}(A_w) = \mathrm{M}_w(A_w) \to \mathrm{M}_w(A_{v,w}) = \mathrm{End}_{\mathbb{F}_p}(A_{v,w}) \tag{5-4}$$

factors through the quotient map $\mathrm{pr}_{v,w} : R_w \twoheadrightarrow R_v$. In order to prove (2), it is enough to show that (5-4) is surjective. It suffices to verify surjectivity after $- \otimes \mathbb{Z}_\ell$ for every prime number ℓ.

Assume first that $\ell \neq p$. Let C be the quotient abelian variety $C = A_w/A_{v,w}$. There is an exact sequence of reflexive $R_w \otimes \mathbb{Z}_\ell$-modules

$$0 \longrightarrow \mathrm{T}_\ell(A_{v,w}) \longrightarrow \mathrm{T}_\ell(A_w) \longrightarrow \mathrm{T}_\ell(C) \longrightarrow 0,$$

and its Ext-sequence contains

$$\begin{aligned} \mathrm{Hom}_{R_w\otimes\mathbb{Z}_\ell}(\mathrm{T}_\ell(A_w), \mathrm{T}_\ell(A_w)) \longrightarrow \mathrm{Hom}_{R_w\otimes\mathbb{Z}_\ell}(\mathrm{T}_\ell(A_{v,w}), \mathrm{T}_\ell(A_w)) \\ \longrightarrow \mathrm{Ext}^1_{R_w\otimes\mathbb{Z}_\ell}(\mathrm{T}_\ell(C), \mathrm{T}_\ell(A_w)). \end{aligned}$$

The Ext^1-term vanishes by Lemma 17. Thus Theorem 19 shows the surjectivity of

$$\begin{aligned} \mathrm{M}_w(A_w) \otimes \mathbb{Z}_\ell = \mathrm{Hom}_{R_w\otimes\mathbb{Z}_\ell}(\mathrm{T}_\ell(A_w), \mathrm{T}_\ell(A_w)) \\ \twoheadrightarrow \mathrm{Hom}_{R_w\otimes\mathbb{Z}_\ell}(\mathrm{T}_\ell(A_{v,w}), \mathrm{T}_\ell(A_w)) = \mathrm{M}_w(A_{v,w}) \otimes \mathbb{Z}_\ell. \end{aligned}$$

If $\ell = p$, then the inclusion $A_{v,w} \subseteq A_w$ gives a surjection of reflexive $R_w \otimes \mathbb{Z}_p$-modules

$$\mathrm{T}_p(A_w) \twoheadrightarrow \mathrm{T}_p(A_{v,w}).$$

Since $T_p(A_w)$ is free over $R_w \otimes \mathbb{Z}_p$, we obtain a surjection

$$\mathrm{Hom}_{R_w\otimes\mathbb{Z}_p}(T_p(A_w), T_p(A_w)) \twoheadrightarrow \mathrm{Hom}_{R_w\otimes\mathbb{Z}_p}(T_p(A_w), T_p(A_{v,w})),$$

which, by Theorem 19, says that $\mathrm{M}_w(A_w) \otimes \mathbb{Z}_p \to \mathrm{M}_w(A_{v,w}) \otimes \mathbb{Z}_p$ is surjective. This completes the proof of the proposition. □

5.3. ***Proof of the main result.*** We are now ready to prove our main result. We must show that the abelian varieties A_w that exist by Proposition 21 for each w, and which yield equivalences of the desired type on the respective full subcategories AV_w by Theorem 25, can be chosen in a compatible way for every $v \subseteq w$. This requires a two-step process. We use the notation of Proposition 26.

- First, we establish compatibility on the set-theoretic level: we must fix isomorphism classes for each A_w such that $A_v \simeq A_{v,w}$ for every $v \subseteq w$.

- Secondly, we categorize the first choice: we must choose isomorphisms $A_v \simeq A_{v,w}$ such that the inclusions $\varphi_{w,v} : A_v \simeq A_{v,w} \subseteq A_w$ obey the cocycle condition $\varphi_{w,v} \circ \varphi_{v,u} = \varphi_{w,u}$ for $u \subseteq v \subseteq w$, and thus construct an ind-system $\mathscr{A} = (A_w, \varphi_{w,v})$.

Proof of Theorem 1. For any finite set $w \subseteq W_p$ that avoids $\sqrt{p}$, let $Z(w)$ be the set of isomorphism classes $[A]$ of abelian varieties A in AV_w such that the natural map $R_w \to \operatorname{End}_{\mathbb{F}_p}(A)$ is an isomorphism. The elements of $Z(w)$ all belong to the same isogeny class, and so $Z(w)$ is finite, since there are only finitely many isomorphism classes of abelian varieties over a finite field lying in a given isogeny class (in fact, finiteness holds for isomorphism classes of abelian varieties of fixed dimension [Milne 1986, Corollary 18.9]). Moreover, the set $Z(w)$ is nonempty by Proposition 21.

For any pair $v \subseteq w$ of finite sets of nonreal Weil p-numbers, we construct a map

$$\zeta_{v,w} : Z(w) \to Z(v)$$

given by $\zeta_{v,w}([A]) = [B]$, where B is the abelian subvariety of A generated by the image of all $f : C \to A$ with $w(C) \subseteq v$. Proposition 26 states that $\zeta_{v,w}$ indeed takes values in $Z(v)$.

These maps satisfy the compatibility condition

$$\zeta_{u,w} = \zeta_{u,v}\zeta_{v,w}$$

for all tuples $u \subseteq v \subseteq w$, hence they define a projective system

$$(Z(w), \zeta_{v,w})$$

indexed by finite subsets $w \subseteq W_p$ with $\sqrt{p} \notin w$. Since the sets $Z(w)$ are finite and nonempty, a standard compactness argument shows that the inverse limit is not empty:

$$Z = \varprojlim_{w} Z(w) \neq \varnothing.$$

We choose a compatible[2] system $z = (z_w) \in Z$ of isomorphism classes of abelian varieties.

Now we would like to choose abelian varieties A_w in each class z_w, and inclusions

$$\varphi_{w,v} : A_v \to A_w$$

[2] We will see later in Remark 40 that $\zeta_{v,w}$ is always surjective. This extra piece of information simplifies the construction of the system marginally. However, we find it conceptually easier to deduce this fact from the antiequivalence of Theorem 1, hence the order of the assertions and proofs.

for every $v \subseteq w$ that are isomorphic to the inclusion from Proposition 26 in a compatible way: for $u \subseteq v \subseteq w$ we want

$$\varphi_{w,u} = \varphi_{w,v}\varphi_{v,u}.$$

Because the set of Weil numbers is countable, we may choose a cofinal totally ordered subsystem of finite subsets of W_p^{com}

$$w_1 \subseteq w_2 \subseteq \cdots \subseteq w_i \subseteq \cdots .$$

Working first with this totally ordered subsystem, we can construct a direct system

$$\mathscr{A}_0 = (A_{w_i}, \varphi_{w_j,w_i})$$

of abelian varieties, as desired, by induction. If A_{w_i} is already constructed, then we choose $A_{w_{i+1}}$ in $z_{w_{i+1}}$ and deduce from $\zeta_{w_i,w_{i+1}}(z_{w_{i+1}}) = z_{w_i}$ that there is an inclusion $\varphi_{w_{i+1},w_i} : A_{w_i} \to A_{w_{i+1}}$ as desired.

Once this is achieved, we may identify all transfer maps of the restricted system $\mathscr{A}_0$ with inclusions. Now we can extend the directed system $\mathscr{A}_0$ from the index set $\{w_i \; : \; i \in \mathbb{N}\}$ to an ind-object $\mathscr{A}$ on all finite subsets of W_p. For a general finite $w \subset W_p$ we choose i large enough such that $w \subseteq w_i$, and define

$$A_w := A_{w,w_i} \subseteq A_{w_i}$$

by means of the construction of Proposition 26. This choice is well defined, i.e., independent of $i \gg 0$. Furthermore, there are compatible transfer maps $\varphi_{v,w} : A_v \to A_w$ for all $v \subseteq w$ that lead to the desired direct system

$$\mathscr{A} = (A_w, \varphi_{w,v}).$$

In the sense of ind-objects we have $\mathscr{A}_0 \simeq \mathscr{A}$ and so $\mathscr{A}_0$ would suffice for Theorem 1, but we wanted to restore symmetry and have A_w for all finite subsets $w \subseteq W_p^{\mathrm{com}}$.

Let A be any element of $\mathsf{AV}_p^{\mathrm{com}}$, and set

$$T(A) = \mathrm{Hom}_{\mathbb{F}_p}(A, \mathscr{A}) = \varinjlim_{w} \mathrm{Hom}_{\mathbb{F}_p}(A, A_w) = \varinjlim_{w} \mathrm{M}_w(A).$$

The groups $\mathrm{Hom}_{\mathbb{F}_p}(A, A_w)$ are stable when w is large enough. More precisely, if w, w' are finite sets of Weil p-numbers with $w(A) \subseteq w \subseteq w'$, then the map

$$\varphi_{w',w} \circ - : \mathrm{Hom}_{\mathbb{F}_p}(A, A_w) \to \mathrm{Hom}_{\mathbb{F}_p}(A, A_{w'})$$

is an isomorphism (see Proposition 26). Moreover, $T(-)$ restricted to AV_w recovers the functor $\mathrm{M}_w(-)$ of Theorem 25 constructed using the object A_w of $\mathscr{A}$, and induces an antiequivalence between AV_w and $\mathsf{Refl}(R_w)$.

Observe that, by the naturality of the Frobenius isogeny, for any finite $w \subseteq W_p$ avoiding $\sqrt{p}$ and any $f \in \mathrm{Hom}_{\mathbb{F}_p}(A, A_w)$ the diagram

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "\pi_A"'] & A_w \arrow[d, "\pi_{A_w}"] \\ A \arrow[r, "f"] & A_w \end{tikzcd}$$

is commutative. This implies that, for w sufficiently large, the action of $F_w \in R_w$ on $T(A)$ is given by $T(\pi_A)$, the morphism induced by the Frobenius isogeny π_A via functoriality of T.

Compatibility in w shows that $T(-)$ induces an antiequivalence

$$T = \varinjlim M_w : \mathsf{AV}_p^{\mathrm{com}} = \varinjlim_w \mathsf{AV}_w \xrightarrow{\sim} \varinjlim_w \mathsf{Refl}(R_w) = \mathsf{Refl}(\mathcal{R}_p^{\mathrm{com}}).$$

Due to the remarks of Section 3.2, this is precisely the claim of Theorem 1, and so its proof is complete. □

6. Properties of the functor T

6.1. ***Recovering Tate and Dieudonné module.*** Let A be an abelian variety over $\mathbb{F}_p$, and set $w = w(A)$. We explain here how the $R_w \otimes \mathbb{Z}_\ell$-modules $T_\ell(A)$ can be recovered from the pair $(T(A), F)$ attached to A by Theorem 1. We set

$$\mathcal{R}_\ell = \varprojlim_w (R_w \otimes \mathbb{Z}_\ell)$$

for all prime numbers ℓ, where in the projective limit w ranges through all finite subsets of W_p^{com}, and define

$$T_\ell(\mathcal{A}) = \begin{cases} \varinjlim_w T_\ell(A_w) & \ell \neq p, \\ \varprojlim_w T_p(A_w) & \ell = p, \end{cases}$$

as the direct limit if $\ell \neq p$ and the projective limit if $\ell = p$ of the system obtained by applying $T_\ell(-)$ to the direct system $\mathcal{A} = (A_w)_w$ constructed in the proof of Theorem 1.

We first discuss the ℓ-adic Tate module, and assume $\ell \neq p$. Since for $v \subseteq w$ the map $A_v \to A_w$ is an inclusion of abelian varieties, the induced map $T_\ell(A_v) \to T_\ell(A_w)$ is the inclusion of a direct summand, at least as $\mathbb{Z}_\ell$-modules. Hence $T_\ell(\mathcal{A})$ is a free $\mathbb{Z}_\ell$-module of countable infinite rank.

Proposition 27. *Let A be an abelian variety over $\mathbb{F}_p$ with $\sqrt{p} \notin w(A)$. There is a natural isomorphism of $\mathcal{R}_\ell$-modules*

$$T_\ell(A) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{R}_\ell}(T(A) \otimes \mathbb{Z}_\ell, T_\ell(\mathcal{A})).$$

Proof. Let $w \subseteq W_p^{\mathrm{com}}$ be a finite set containing $w(A)$. Since $R_w \otimes \mathbb{Z}_\ell$ is Gorenstein, dualizing (5-1) yields the first equality in

$$T_\ell(A) = \mathrm{Hom}_{R_w \otimes \mathbb{Z}_\ell}(M_w(A) \otimes \mathbb{Z}_\ell, T_\ell(A_w)) = \mathrm{Hom}_{\mathcal{R}_\ell}(T(A) \otimes \mathbb{Z}_\ell, T_\ell(\mathcal{A})).$$

The second equality holds, because $T_\ell(A_w) \subseteq T_\ell(\mathcal{A})$ is the maximal submodule on which $\mathcal{R}_\ell$ acts through its quotient $\mathcal{R}_\ell \to R_w \otimes \mathbb{Z}_\ell$. □

Now we address the contravariant Dieudonné module $T_p(A)$. We endow $T_p(\mathcal{A})$ with the projective limit topology. If M is a topological $\mathcal{R}_p$-module which is finite and free over $\mathbb{Z}_p$, then the action of $\mathcal{R}_p$ on M factors through $\mathcal{R}_p \to R_w \otimes \mathbb{Z}_p$ for some large enough w, by compactness of M. We denote by

$$M \mathbin{\widehat{\otimes}_{\mathcal{R}_p}} T_p(\mathcal{A}) = \varprojlim_{w \gg \varnothing} M \otimes_{R_w \otimes \mathbb{Z}_p} T_p(A_w)$$

the continuous tensor product.

Proposition 28. *Let A be an abelian variety over $\mathbb{F}_p$ with $\sqrt{p} \notin w(A)$. There is a natural isomorphism of $\mathcal{R}_p$-modules*

$$T_p(A) = (T(A) \otimes \mathbb{Z}_p) \mathbin{\widehat{\otimes}_{\mathcal{R}_p}} T_p(\mathcal{A}).$$

Proof. Let $w \subseteq W_p^{\mathrm{com}}$ be a finite set containing $w(A)$. We deduce from (5-2) a natural identification

$$\begin{aligned} T_p(A) &= \mathrm{Hom}_{R_w \otimes \mathbb{Z}_p}(T_p(A_w), T_p(A)) \otimes_{R_w \otimes \mathbb{Z}_p} T_p(A_w) \\ &= \mathrm{M}_w(A) \otimes_{R_w} T_p(A_w) = (T(A) \otimes \mathbb{Z}_p) \mathbin{\widehat{\otimes}_{\mathcal{R}_p}} T_p(\mathcal{A}), \end{aligned}$$

because for $w(A) \subseteq w \subseteq w'$ the natural maps

$$(T(A) \otimes \mathbb{Z}_p) \otimes_{R_{w'} \otimes \mathbb{Z}_p} T_p(A_{w'}) \to (T(A) \otimes \mathbb{Z}_p) \otimes_{R_w \otimes \mathbb{Z}_p} T_p(A_w)$$

are isomorphisms. □

6.2. ***Isogenies and inclusions.*** We discuss how the functor $T(-)$ detects isogenies and inclusions.

Proposition 29. *Let A and B be abelian varieties in $\mathsf{AV}_p^{\mathrm{com}}$.*

(1) *The map $f : B \to A$ is an isogeny if and only if $T(f) \otimes \mathbb{Q}$ is an isomorphism.*

(2) *For an isogeny $f : B \to A$, the map $T(f)$ is injective and the image is of index*

$$\deg(f) = |\mathrm{coker}(T(f))|.$$

Proof. (1) An isogeny f has an inverse up to multiplication-by-n map for $n = \deg(f)$. Therefore $T(f)$ is an isomorphism after inverting $\deg(f)$.

Conversely, if f is not an isogeny, then either $\ker(f)$ or $\mathrm{coker}(f)$ have a nontrivial abelian variety as a direct summand up to isogeny. In the presence of such a direct summand the map $T(f) \otimes \mathbb{Q}$ cannot be an isomorphism.

(2) We indicate the ℓ-primary part by an index ℓ. Then using Proposition 27, for $\ell \neq p$ we have

$$|\mathrm{coker}(T(f))|_\ell = |\mathrm{coker}(T(f)) \otimes \mathbb{Z}_\ell| = |\mathrm{coker}(T_\ell(f)^\vee : T_\ell(A)^\vee \to T_\ell(B)^\vee)|.$$

The duals here are $\mathrm{Hom}(-, R_w \otimes \mathbb{Z}_\ell)$. Since $R_w \otimes \mathbb{Z}_\ell$ is reduced Gorenstein of dimension 1, we can use [Bass 1963, Theorem 6.3(4)] and induction on the length to see that

$$|\mathrm{coker}(T_\ell(f)^\vee : T_\ell(A)^\vee \to T_\ell(B)^\vee)| = |\mathrm{coker}(T_\ell(f) : T_\ell(B) \to T_\ell(A))| = |\ker(f)|_\ell.$$

If $\ell = p$, using Proposition 28 yields

$$\begin{aligned} |\mathrm{coker}(T(f))|_p = |\mathrm{coker}(T(f)) \otimes \mathbb{Z}_p| &= |\mathrm{coker}(T_p(f) : T_p(A) \to T_p(B))| \\ &= |\ker(f)|_p, \end{aligned}$$

where the last equality follows from Dieudonné theory. □

Proposition 30. *Let A and B be abelian varieties in $\mathsf{AV}_p^{\mathrm{com}}$. For a map $f : B \to A$, the following are equivalent*:

(a) *$T(f) : T(A) \twoheadrightarrow T(B)$ is surjective.*

(b) *The map f can be identified with the inclusion of an abelian subvariety.*

Proof. If $T(f)$ is surjective, Proposition 27 shows that the induced map $T_\ell(B) \to T_\ell(A)$ is injective. Therefore $\ker(f)$ is at most a finite group scheme. We may therefore replace A by the image A_0 of $B \to A$ and thus reduce to the case of the isogeny $f_0 : B \to A_0$. Here Proposition 29 implies that $\deg(f_0) = 1$, hence $B = A_0$ and f is indeed an inclusion of an abelian subvariety.

Conversely, if $f : B \to A$ is an inclusion, then there is a map $g : A \to B$ such that $gf : B \to B$ is an isogeny. Therefore $T(f)$ has at least an image of finite index. The image of $T(f)$ is a reflexive submodule in the image of the equivalence $T(-)$, so that there is an abelian variety C and a factorization $B \to C \to A$ with $T(A) \twoheadrightarrow T(C)$ surjective and $T(C) \subseteq T(B)$ an inclusion.

We have already proven that $C \to A$ is an abelian subvariety, and it is easy to see that $B \to C$ is an isogeny. Therefore $B \to C$ is an isomorphism. □

As an application, we prove a variant for objects of AV_p of Waterhouse's theorem on possible endomorphism rings of $\mathbb{F}_p$-simple abelian varieties over $\mathbb{F}_p$; see [Waterhouse 1969, Theorem 6.1.2]:

Theorem 31. *Let w be a set of conjugacy classes of nonreal Weil p-numbers. Then the following are equivalent*:

(a) *S is an order in $R_w \otimes \mathbb{Q}$ containing R_w.*

(b) *S is isomorphic as an R_w-algebra to $\mathrm{End}_{\mathbb{F}_p}(B)$ for an abelian variety B with $w(B) = w$ whose simple factors up to isogeny occur with multiplicity* 1.

Proof. Since R_w is the minimal central order for abelian varieties B with $w(B) = w$, it is clear that (b) implies (a).

Conversely, if S is an order containing R_w, then S is a reflexive R_w-module and thus corresponds to an abelian variety B. Let A_w be the abelian variety occurring in the ind-system pro-representing $T(-)$, so that $T(A_w) = R_w$. The inclusion $R_w \subseteq S$ corresponds to an isogeny $\varphi : B \to A_w$ by Proposition 29, so that B has the required Weil support and product structure up to isogeny. Moreover,

$$\mathrm{End}_{\mathbb{F}_p}(B) = \mathrm{End}_{R_w}(S) = \{\lambda \in R_w \otimes \mathbb{Q} : \lambda S \subseteq S\} = S$$

shows (a) implies (b). □

7. Ambiguity and comparison

The construction of the functor $T(-)$ in Section 5.3 depends on the choice of an ind-abelian variety $\mathscr{A}$. For the sake of distinguishing the different choices, we set in this section

$$T_{\mathscr{A}}(-) = \mathrm{Hom}_{\mathbb{F}_p}(-, \mathscr{A}).$$

7.1. *Continuous line bundles.*

Definition 32. Let $W \subseteq W_q$ be a subset. Let us denote by $\mathscr{R}_W$ the pro-ring (R_w), where w ranges over the finite subsets of W.

(1) An $\mathscr{R}_W$*-module* is a pro-system $\mathscr{M} = (M_w)$ with w ranging over the finite subsets of W, such that M_w is an R_w-module and the maps $M_w \to M_v$ for $v \subseteq w$ are R_w-module homomorphisms (where R_w acts on M_v via the projection $R_w \to R_v$). Homomorphisms of $\mathscr{M}$ are levelwise R_w-module homomorphisms.

(2) An $\mathscr{R}_W$-module $\mathscr{M}$ is *invertible* if for all $w \subseteq W$ the R_w-module M_w is invertible and for $v \subseteq w$ the maps $M_w \to M_v$ are surjective (equivalently, they induce a natural isomorphism $M_w \otimes_{R_w} R_v \simeq M_v$).

(3) The set of isomorphism classes of invertible $\mathscr{R}_W$-modules forms a group, denoted by $\mathrm{Pic}(\mathscr{R}_W)$, under levelwise tensor products, the *Picard group* of $\mathscr{R}_W$.

For a finite set w of conjugacy classes of Weil q-numbers, we set $X_w = \mathrm{Spec}(R_w)$ and consider the ind-schemes

$$\mathscr{X} = \varinjlim_{w} X_w,$$

and for a subset $W \subseteq W_q$ the ind-scheme

$$\mathscr{X}_W = \varinjlim_{w \subseteq W} X_w,$$

with closed immersions as transfer maps, all denoted i, induced by the projections $\mathrm{pr}_{v,w} : R_w \twoheadrightarrow R_v$. The invertible $\mathcal{R}_W$-modules are just line bundles on $\mathscr{X}_W$, and

$$\mathrm{Pic}(\mathcal{R}_W) = \mathrm{Pic}(\mathscr{X}_W) = \mathrm{H}^1(\mathscr{X}_W, \mathbb{O}^\times).$$

Since $\mathbb{O}^\times_{\mathscr{X}_W} = \varprojlim_{w \subseteq W} i_* \mathbb{O}^\times_{X_w}$, we find an exact sequence

$$0 \longrightarrow \varprojlim_{w \subseteq W}{}^1 R_w^\times \longrightarrow \mathrm{Pic}(\mathcal{R}_W) \longrightarrow \varprojlim_{w \subseteq W} \mathrm{Pic}(R_w) \longrightarrow 0.$$

The quotient of $\mathrm{Pic}(\mathcal{R}_W)$ given by $\varprojlim_w \mathrm{Pic}(R_w)$ parametrizes the choices of a compatible system of isomorphism classes of rank-1 R_w-modules M_w. The $\varprojlim^1$-term parametrizes all choices of transfer maps to obtain an invertible $\mathcal{R}_W$-module $\mathcal{M} = (M_w)$ from a given compatible choice of isomorphism classes of invertible R_w-modules at every level.

Proposition 33. *Let $V \subseteq W \subseteq W_q$ be subsets. Then the natural restriction map*

$$\mathrm{Pic}(\mathcal{R}_W) \twoheadrightarrow \mathrm{Pic}(\mathcal{R}_V)$$

is surjective.

Proof. For $v \subseteq w$, define Zariski sheaves $\mathcal{K}_{v,w}$ on $\mathscr{X}_W$ by the short exact sequence

$$0 \longrightarrow \mathcal{K}_{v,w} \longrightarrow i_* \mathbb{O}^\times_{X_w} \longrightarrow i_* \mathbb{O}^\times_{X_v} \longrightarrow 0.$$

Then $\mathcal{K}_{V,W} = \varprojlim_{w \subseteq W} \mathcal{K}_{w \cap V, w}$ is the kernel of $\mathbb{O}^\times_{\mathscr{X}_W} \twoheadrightarrow i_* \mathbb{O}^\times_{\mathscr{X}_V}$. The Zariski cohomology sequence yields an exact sequence

$$\mathrm{Pic}(\mathcal{R}_W) \longrightarrow \mathrm{Pic}(\mathcal{R}_V) \longrightarrow \mathrm{H}^2(\mathscr{X}_W, \mathcal{K}_{V,W}),$$

and it remains to show vanishing of $\mathrm{H}^2(\mathscr{X}_W, \mathcal{K}_{V,W})$. The pro-structure of $\mathcal{K}_{V,W}$ leads to a short exact sequence

$$0 \longrightarrow \varprojlim_{w \subseteq W}{}^1 \mathrm{H}^1(X_w, \mathcal{K}_{w \cap V, w}) \longrightarrow \mathrm{H}^2(\mathscr{X}_W, \mathscr{K}_{V,W}) \longrightarrow \varprojlim_{w \subseteq W} \mathrm{H}^2(X_w, \mathcal{K}_{w \cap V, w}) \longrightarrow 0.$$

The $\varprojlim$-term on the right vanishes by cohomological dimension because $\dim(X_w)$ is 1. The $\varprojlim^1$-term on the left vanishes, as we claim that $(\mathrm{H}^1(X_w, \mathcal{K}_{w \cap V, w}))_{w \subseteq W}$ is a surjective system, and hence a Mittag–Leffler system. Indeed, for finite subsets $w \subseteq w' \subseteq W$, the cokernel $\mathscr{C}_{w,w'}$ of

$$\mathcal{K}_{w' \cap V, w'} \to \mathcal{K}_{w \cap V, w}$$

is a sheaf with support in at most the finitely many points of $X_{w'}$ that are contained in more than one irreducible component, and so $\mathrm{H}^1(X_{w'}, \mathscr{C}_{w,w'}) = 0$. Since $\mathrm{H}^1(X_{w'}, -)$ is right exact, we have an exact sequence

$$\mathrm{H}^1(X_{w'}, \mathcal{K}_{w' \cap V, w'}) \to \mathrm{H}^1(X_w, \mathcal{K}_{w \cap V, w}) \to \mathrm{H}^1(X_{w'}, \mathscr{C}_{w,w'}) = 0,$$

from which we deduce the claim. □

7.2. ***Mixed tensor products.*** We recall Serre and Tate's well-known tensor product construction (see [Giraud 1968] for the parallel Hom-construction explaining a construction of Shimura and Taniyama). Let A be an abelian variety over $\mathbb{F}_q$ and M a finitely generated R_w-module for some $w(A) \subseteq w \subset W_q$. The R_w-action on A induces an R_w-module structure on the set of U-valued points for any $\mathbb{F}_q$-scheme U. The fppf-sheafification $(M \otimes_{R_w} A)^\#$ of the functor on $\mathbb{F}_q$-schemes

$$U \mapsto M \otimes_{R_w} A(U)$$

is representable by an abelian variety. Indeed, let

$$R_w^m \xrightarrow{\varphi} R_w^n \longrightarrow M \longrightarrow 0$$

be a finite presentation. The $m \times n$-matrix φ also defines a map $\varphi_A : A^m \to A^n$, and

$$M \otimes_{R_w} A(U) = \operatorname{coker}(\varphi \otimes \mathrm{id}_{A(U)}) = \operatorname{coker}(\varphi_A : A(U)^m \to A(U)^n) = \operatorname{coker}(\varphi_A(U)),$$

so that

$$(M \otimes_{R_w} A)^\# = \operatorname{coker}(\varphi_A),$$

and this is representable by an abelian variety. We denote the representing object by

$$M \otimes_{R_w} A.$$

If $w \subseteq w'$ and M' is a finitely presented $R_{w'}$-module with $M = M' \otimes_{R_{w'}} R_w$, then there is an obvious identification

$$M' \otimes_{R_{w'}} A = M \otimes_{R_w} A.$$

In particular, if $W \subseteq W_q$ is a subset and $w(A) \subseteq W$, then for any invertible $\mathcal{R}_W$-module $\mathcal{M} = (M_w)$ we have a well-defined tensor product given by

$$\mathcal{M} \otimes_{\mathcal{R}_W} A := M_w \otimes_{R_w} A$$

for all sufficiently large finite $w(A) \subseteq w \subseteq W$.

7.3. ***Choices of ind-representing objects.*** Before we describe our choices, we need three propositions of independent interest.

Proposition 34. *Let $W \subseteq W_q$ be a subset, A an abelian variety with $w(A) \subseteq W$, and $\mathcal{M} = (M_w)$ an invertible $\mathcal{R}_W$-module. Then there is a natural isomorphism*

$$\operatorname{Hom}_{\mathbb{F}_q}(-, \mathcal{M} \otimes_{\mathcal{R}_W} A) \simeq \mathcal{M} \otimes_{\mathcal{R}_W} \operatorname{Hom}_{\mathbb{F}_q}(-, A)$$

of functors $\mathsf{AV}_W \to \mathsf{Refl}(\mathcal{R}_W)$.

Proof. We set $w = w(A)$, and must show that naturally in X

$$\mathrm{Hom}_{\mathbb{F}_q}(X, M_w \otimes_{R_w} A) \simeq M_w \otimes_{R_w} \mathrm{Hom}_{\mathbb{F}_q}(X, A)$$

for any abelian variety X over $\mathbb{F}_q$. We extend this claim to projective R_w-modules M of finite rank. Since the tensor construction is compatible with direct sums, clearly the claim is additive in M in the sense that it holds for M' and M'' if and only if it holds for $M = M' \oplus M''$. This reduces the claim to free modules $M = R_w^n$, and by the same argument to $M = R_w$. Now the claim trivially holds. □

Proposition 35. *Let $W \subseteq W_q$ be a subset containing no rational Weil q-number. Any $\mathcal{R}_W$-linear contravariant equivalence*

$$S : \mathsf{AV}_W \to \mathsf{Refl}(\mathcal{R}_W)$$

is ind-representable, i.e., of the form

$$S(-) = \mathrm{Hom}_{\mathbb{F}_p}(-, \mathcal{B})$$

for an ind-system $\mathcal{B} = (B_w, \varphi_{w,v})$ such that the following holds for all finite subsets $v \subseteq w \subseteq W$:

(i) $w(B_w) = w$.

(ii) *The natural map $R_w \to \mathrm{End}_{\mathbb{F}_q}(B_w)$ is an isomorphism.*

(iii) *B_w is isogenous to the product of its simple factors with multiplicity* 1.

(iv) *The maps $\varphi_{w,v} : B_v \to B_w$ are inclusions.*

Proof. The pro-system $\mathcal{R}_W = (R_w, \mathrm{pr}_{v,w})$ can be considered as the pro-system of the free rank-1 modules $R_w \in \mathsf{Refl}(R_w) \subseteq \mathsf{Refl}(\mathcal{R}_W)$. As such there is a unique ind-system $\mathcal{B} = (B_w, \varphi_{w,v})$ with $S(\mathcal{B}) = (S(B_w)) = \mathcal{R}_W$. Yoneda's lemma assigns to the compatible elements $1 \in R_w = S(B_w)$ a natural transformation

$$\Phi : \mathrm{Hom}_{\mathbb{F}_q}(-, \mathcal{B}) = \varinjlim_w \mathrm{Hom}_{\mathbb{F}_q}(-, B_w) \to S(-).$$

For every $A \in \mathsf{AV}_W$ the map Φ is the composition of the two isomorphisms

$$\varinjlim_w \mathrm{Hom}(A, B_w) \xrightarrow{S} \varinjlim_w \mathrm{Hom}_{R_w}(R_w, S(A)) \xrightarrow{\mathrm{ev}_1} S(A),$$

where ev_1 denotes the evaluation map at 1. It remains to prove the finer claims on the ind-representing system $\mathcal{B}$.

Since S is an $\mathcal{R}_W$-linear equivalence, $\mathcal{R}_W$ acts on B_w through R_w as on $S(B_w) = R_w$. Here we use that R_w is commutative, and so we can forget to pass to the opposite ring due to S being contravariant. Since F_w acts on B_w by the Frobenius isogeny π_{B_w}, and on $R_w = S(B_w)$ by $F_w \in R_w$, it follows that $w(B_w) = w$.

The natural map $R_w \to \mathrm{End}_{\mathbb{F}_w}(B_w)$ is an isomorphism, because applying the $\mathcal{R}_W$-linear $S(-)$ transforms it to the map $R_w \to \mathrm{End}_{\mathcal{R}_w}(R_w)$, which is indeed an isomorphism. We deduce assertion (iii) from this as well.

It remains to show that $\varphi_{w,v} : B_v \to B_w$ is isomorphic to an inclusion for all $v \subseteq w$. We denote the image of $\varphi_{w,v}$ by C. Since S is ind-representable, the surjection $B_v \to C$ becomes an inclusion

$$S(C) \hookrightarrow S(B_v).$$

Since by construction $S(B_w) \to S(B_v)$ is the surjective map $\mathrm{pr}_{v,w} : R_w \to R_v$, we conclude that $S(C) \simeq S(B_v)$ is an isomorphism. Consequently, because S is an equivalence, we have $C \simeq B_v$ and assertion (iv) holds. □

The third proposition is related to Proposition 24.

Proposition 36. *Let $W \subseteq W_q$ be a subset containing no rational Weil q-number, and let*

$$S : \mathsf{AV}_W \to \mathsf{Refl}(\mathcal{R}_W)$$

be an $\mathcal{R}_W$-linear contravariant equivalence.

Let $w \subseteq W$ be a finite set of conjugacy classes of Weil q-numbers, and let A be an abelian variety over $\mathbb{F}_q$ with $w = w(A)$. The following are equivalent:

(a) *The natural map $R_w \to \mathrm{End}_{\mathbb{F}_q}(A)$ is an isomorphism.*

(b) *$S(A)$ is a projective R_w-module of rank* 1.

Proof. Since $S(-)$ is an equivalence of categories, the map $R_w \to \mathrm{End}_{\mathbb{F}_p}(A)$ is an isomorphism if and only if the map

$$R_w \to \mathrm{End}_{R_w}(S(A))$$

is an isomorphism (S is contravariant but the rings are commutative here). Since R_w is a reduced Gorenstein ring of dimension 1 by Theorem 11, this is equivalent by Proposition 18 to $S(A)$ being a projective R_w-module of rank 1. □

We define the tensor product of an invertible $\mathcal{R}_W$-module $\mathcal{M} = (M_w)$ and an ind-system $\mathcal{A} = (A_w, \varphi_{w,v})$ of abelian varieties indexed by finite subsets of W and with $w(A_w) = w$ by

$$\mathcal{M} \otimes \mathcal{A} := (M_w \otimes_{R_w} A_w).$$

Theorem 37. *Let $W \subseteq W_q$ be a subset containing no rational Weil q-number.*

Let $\mathcal{A} = (A_w, \varphi_{w,v})$ be an ind-system of abelian varieties over $\mathbb{F}_q$ indexed by finite subsets of W such that:

(i) $w(A_w) = w$.

(ii) *The natural map $R_w \to \mathrm{End}_{\mathbb{F}_q}(A_w)$ is an isomorphism.*

(iii) *A_w is isogenous to the product of its simple factors with multiplicity* 1.

(iv) *The maps $\varphi_{w,v} : A_v \to A_w$ are inclusions.*

For an invertible $\mathcal{R}_W$-module $\mathcal{M}$, the ind-system $\mathcal{M} \otimes_{\mathcal{R}_W} \mathcal{A}$ has the same properties (i)–(iv), *and the group* $\operatorname{Pic}(\mathcal{R}_W)$ *acts freely and transitively by*

$$\mathcal{A} \mapsto \mathcal{M} \otimes_{\mathcal{R}_W} \mathcal{A}$$

on the set of isomorphism classes of such ind-systems.

Remark 38. When $q = p$ and $W = \{\pi\}$ consists of a single Weil p-number, Theorem 37 is a special case of [Waterhouse 1969, Theorem 6.1.3], which inspired the above result.

Proof of Theorem 37. By a W-version of the proof of Theorem 1 for any ind-system $\mathcal{A}$ satisfying (i)–(iv), the functor

$$T_{\mathcal{A}} = \operatorname{Hom}_{\mathbb{F}_q}(-, \mathcal{A}) : \mathsf{AV}_W \to \mathsf{Refl}(\mathcal{R}_W)$$

is a contravariant $\mathcal{R}_W$-linear antiequivalence $\mathsf{AV}_W \to \mathsf{Refl}(\mathcal{R}_W)$. The effect of the action by $\mathcal{M} \in \operatorname{Pic}(\mathcal{R}_W)$ on the represented functors is described by Proposition 34 as

$$T_{\mathcal{M} \otimes_{\mathcal{R}_W} \mathcal{A}}(-) = \mathcal{M} \otimes_{\mathcal{R}_W} T_{\mathcal{A}}(-).$$

Since $\mathcal{M} = (M_w)$ is invertible, the functor $\mathcal{M} \otimes_{\mathcal{R}_W} -$ is an autoequivalence of AV_W. We thus have natural isomorphisms

$$R_w = \operatorname{End}_{\mathbb{F}_q}(A_w) = \operatorname{End}_{\mathbb{F}_q}(\mathcal{M} \otimes_{\mathcal{R}_W} A_w) = T_{\mathcal{M} \otimes_{\mathcal{R}_W} \mathcal{A}}(\mathcal{M} \otimes_{\mathcal{R}_W} A_w).$$

Moreover, since $\mathcal{M} = (M_w)$ is invertible, the functor $T_{\mathcal{M} \otimes_{\mathcal{R}_W} \mathcal{A}}(-)$ is an antiequivalence as well, and

$$T_{\mathcal{M} \otimes_{\mathcal{R}_W} \mathcal{A}}(\mathcal{M} \otimes_{\mathcal{R}_W} \mathcal{A}) = \mathcal{R}_W$$

as pro-systems. It follows from the proof of Proposition 35 that $\mathcal{M} \otimes_{\mathcal{R}_W} \mathcal{A}$ also satisfies properties (i)–(iv). This shows that $\operatorname{Pic}(\mathcal{R}_W)$ indeed acts on isomorphism classes of such $\mathcal{A}$.

Let $\mathcal{M}$ be an invertible $\mathcal{R}_W$-module, and let $\mathcal{A}$ be a pro-system as above such that there is an isomorphism $\mathcal{M} \otimes_{\mathcal{R}_W} \mathcal{A} \simeq \mathcal{A}$. Evaluating the resulting natural isomorphism

$$\mathcal{M} \otimes_{\mathcal{R}_W} T_{\mathcal{A}}(-) \simeq T_{\mathcal{A}}(-)$$

in $\mathcal{A}$ itself yields an isomorphism $\mathcal{M} \otimes_{\mathcal{R}_W} \mathcal{R}_W \simeq \mathcal{R}_W$, and hence $\mathcal{M}$ must be trivial in $\operatorname{Pic}(\mathcal{R}_W)$. This shows that the action is free.

Let now $\mathcal{A}$ and $\mathcal{B}$ be two pro-systems of the type considered. The $\mathcal{R}_W$-module

$$\mathcal{M} = T_{\mathcal{B}}(\mathcal{A}) = (\operatorname{Hom}_{\mathbb{F}_p}(A_w, B_w))$$

(note that all maps of pro-objects $\mathcal{A} \to \mathcal{B}$ are levelwise maps since $w(A_w) = w = w(B_w)$) is levelwise an invertible R_w-module $\mathcal{M}_w = T_{\mathcal{B}}(A_w)$ by Proposition 36. The transfer maps $\mathcal{M}_w \to \mathcal{M}_v$ agree with $T_{\mathcal{B}}(\varphi_{w,v})$, which is surjective. Indeed, the image corresponds to an abelian variety C such that $\varphi_{w,v}$ factors as

$$A_v \longrightarrow C \longrightarrow A_w.$$

Now the same argument as in the proof of Proposition 35 shows that $w(C) \subseteq w$ and $C \to A_w$ is an inclusion. Since $\varphi_{w,v}$ is an inclusion, we necessarily have $A_v = C$ and $T_{\mathcal{B}}(\varphi_{w,v})$ is indeed surjective. Consequently, the $\mathcal{R}_W$-module $\mathcal{M} = (\mathcal{M}_w)$ is invertible.

There is a natural map defined by composition of maps

$$\mathcal{M} \otimes_{\mathcal{R}_W} T_{\mathcal{A}}(-) = \mathrm{Hom}(\mathcal{A}, \mathcal{B}) \otimes \mathrm{Hom}(-, \mathcal{A}) \to \mathrm{Hom}(-, \mathcal{B}) = T_{\mathcal{B}}(-).$$

This is an isomorphism, because for every X in AV_W and large enough w we have

$$\begin{aligned}\mathcal{M} \otimes_{\mathcal{R}_W} T_{\mathcal{A}}(X) &= \mathrm{Hom}_{\mathbb{F}_p}(A_w, B_w) \otimes_{R_w} \mathrm{Hom}_{\mathbb{F}_p}(X, A_w)\\ &= T_{\mathcal{B}}(A_w) \otimes_{R_w} \mathrm{Hom}_{R_w}(T_{\mathcal{B}}(A_w), T_{\mathcal{B}}(X))\\ &= T_{\mathcal{B}}(X).\end{aligned}$$

Here we have used again the assumption that $T_{\mathcal{B}}(-)$ is an equivalence and the fact that $T_{\mathcal{B}}(A_w)$ is invertible as an R_w-module by Proposition 36. □

Corollary 39. *The action of* $\mathrm{Pic}(\mathcal{R}_p^{\mathrm{com}})$ *on the isomorphism classes of ind-systems* $\mathcal{A}$ *that represent* $\mathcal{R}_p^{\mathrm{com}}$*-linear antiequivalences* $\mathcal{A}_p^{\mathrm{com}} \to \mathsf{Refl}(\mathcal{R}_p^{\mathrm{com}})$ *is free and transitive.*

Proof. This follows immediately from Theorem 37, the proof of Theorem 1 and Proposition 35. □

Remark 40. With the notation of Section 5.3, for finite sets $v \subseteq w \subseteq W_p$ avoiding $\sqrt{p}$ the transfer map

$$\zeta_{v,w} : Z(w) \to Z(v)$$

in the pro-system of isomorphism classes occurring in the proof of Theorem 1 is in fact surjective. This follows immediately from Theorem 37 and the surjectivity of $\mathrm{Pic}(R_w) \to \mathrm{Pic}(R_v)$ from Proposition 33.

Corollary 41. *Let* $V \subseteq W \subseteq W_p$ *be subsets avoiding* $\sqrt{p}$*, and let* $\mathcal{A}_V = (A_v, \varphi_{w,v})$ *be an ind-system of abelian varieties over* $\mathbb{F}_p$ *indexed by finite subsets of* V *as in Theorem 37 such that*

$$T_{\mathcal{A}_V} = \mathrm{Hom}_{\mathbb{F}_p}(-, \mathcal{A}_V) : \mathsf{AV}_V \to \mathsf{Refl}(\mathcal{R}_V)$$

is an $\mathcal{R}_V$-linear antiequivalence of categories. Then $\mathcal{A}_V$ can be extended to an ind-system $\mathcal{A}_W = (A_w, \varphi_{v,w})$ of abelian varieties over $\mathbb{F}_p$ indexed by finite subsets of W as in Theorem 37. In particular the antiequivalence

$$T_{\mathcal{A}_W} = \mathrm{Hom}_{\mathbb{F}_p}(-, \mathcal{A}_W) : \mathsf{AV}_W \to \mathsf{Refl}(\mathcal{R}_W)$$

naturally extends $T_{\mathcal{A}_V}$.

Proof. We start by choosing an auxiliary ind-system $\mathcal{B}_W$ indexed by finite subsets of W as in Theorem 37. The restriction

$$\mathrm{Hom}_{\mathbb{F}_p}(-, \mathcal{B}_W) : \mathsf{AV}_V \to \mathsf{Refl}(\mathcal{R}_V)$$

is an $\mathcal{R}_V$-linear antiequivalence and is ind-represented by the restriction $\mathcal{B}_V = \mathcal{B}_W|_V$ of the indices to finite subsets of V. By Theorem 37 there is an $\mathcal{M}_V \in \mathrm{Pic}(\mathcal{R}_V)$ such that

$$\mathcal{A}_V = \mathcal{M}_V \otimes_{\mathcal{R}_V} \mathcal{B}_V.$$

By Proposition 33 we can find $\mathcal{M}_W \in \mathrm{Pic}(\mathcal{R}_W)$ such that $\mathcal{M}_V = \mathcal{M}_W \otimes_{\mathcal{R}_W} \mathcal{R}_V$. Then

$$\mathcal{A}_W = \mathcal{M}_W \otimes_{\mathcal{R}_w} \mathcal{B}_W$$

obviously extends $\mathcal{A}_V$ in the desired manner. □

7.4. ***Comparison with Deligne's functor for ordinary abelian varieties over $\mathbb{F}_p$.*** Let $w \subseteq W_p^{\mathrm{com}}$ be a finite subset, and let $\tau : R_w \to R_w$ be the automorphism interchanging F_w and V_w. Denote by R_w^τ the R_w-module obtained by letting R_w operate onto itself via τ. Similarly, for an object M of $\mathsf{Refl}(R_w)$, denote by M^τ the R_w-module $M \otimes_{R_w} R_w^\tau$.

We fix a contravariant equivalence T as in Theorem 1, and an ind-representing system $\mathcal{A} = (A_w, \varphi_{w',w})$ for $T = T_{\mathcal{A}}$. The covariant functor on $\mathsf{AV}_p^{\mathrm{com}}$

$$T_*(A) = T(A^t)^\tau = \varinjlim_w \mathrm{Hom}(A_w^t, A),$$

is pro-representable by the dual system $\mathcal{A}^t = (A_w^t, \varphi_{w',w}^t)$ and a version of Theorem 1 with a covariant equivalence

$$T_* : \mathsf{AV}_p^{\mathrm{com}} \to \mathsf{Refl}(\mathcal{R}_p^{\mathrm{com}})$$

holds. Notice that T_* is $\mathcal{R}_p^{\mathrm{com}}$-linear, since the dual of the Frobenius isogeny $\pi_A : A \to A$ is the Verschiebung isogeny $p/\pi_{A^t} : A^t \to A^t$.

We recall that Deligne's functor T_{Del} on $\mathsf{AV}_q^{\mathrm{ord}}$ is defined as

$$T_{\mathrm{Del}}(A) = \mathrm{H}_1(\widetilde{A}(\mathbb{C}), \mathbb{Z}),$$

where $\widetilde{A}/W(\overline{\mathbb{F}}_p)$ is the Serre–Tate canonical lift of $A \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_p$ to characteristic 0 over the Witt-vectors $W(\overline{\mathbb{F}}_p)$, and where the $\mathbb{C}$-valued points are taken with respect to an a priori fixed embedding $W(\bar{\mathbb{F}}_p) \hookrightarrow \mathbb{C}$. The lattice $T_{\mathrm{Del}}(A)$ comes equipped with a natural Frobenius action by $F = T_{\mathrm{Del}}(\pi_A)$.

Note that the functor depends on the chosen embedding $W(\bar{\mathbb{F}}_p) \hookrightarrow \mathbb{C}$.

We denote by W_q^{ord} the set of conjugacy classes of ordinary Weil q-numbers, i.e., of Weil q-numbers such that at least half of the roots of the characteristic polynomial are p-adic units, when regarded inside an algebraic closure of $\mathbb{Q}_p$. With the abbreviation $\mathcal{R}_q^{\mathrm{ord}} = \mathcal{R}_{W_q^{\mathrm{ord}}}$, the main result of [Deligne 1969, §7] can be stated as:

Theorem 42. *The covariant functor T_{Del} induces an $\mathcal{R}_q^{\mathrm{ord}}$-linear equivalence of categories*

$$T_{\mathrm{Del}} : \mathsf{AV}_q^{\mathrm{ord}} \to \mathsf{Refl}(\mathcal{R}_q^{\mathrm{ord}}).$$

We now compare $T_*(-)$ with T_{Del} when both are restricted to $\mathsf{AV}_p^{\mathrm{ord}}$:

Proposition 43. *The functor $T_{\mathrm{Del}}(-)$ is pro-representable by a pro-system $\mathcal{A}_{\mathrm{Del}}$ and*

$$T_{\mathrm{Del}}(\mathcal{A}_{\mathrm{Del}}) = \mathcal{R}_q^{\mathrm{ord}}.$$

The dual ind-system $\mathcal{A}_{\mathrm{Del}}^t$ satisfies (i)–(iv) *of Proposition 35.*

Proof. This follows from Proposition 35 applied to the functor $X \mapsto T_{\mathrm{Del}}(X^t)$. □

Let T_*^{ord} and $T_{\mathrm{Del},p}$ denote the restriction of T_* and T_{Del} to $\mathsf{AV}_p^{\mathrm{ord}}$, respectively. The functor T_*^{ord} is pro-represented by the dual $\mathcal{A}^{\mathrm{ord},t}$ of the ind-system $\mathcal{A}^{\mathrm{ord}}$ which is defined as $\mathcal{A}$ restricted to indices in W_p^{ord}.

Proposition 44. *There is an invertible $\mathcal{R}_p^{\mathrm{ord}}$-module $\mathcal{M} = (M_w)_{w \in W_p^{\mathrm{ord}}}$ and a natural isomorphism*

$$\mathcal{M} \otimes_{\mathcal{R}_p^{\mathrm{ord}}} T_{\mathrm{Del},p}(-) \xrightarrow{\sim} T_*^{\mathrm{ord}}(-)$$

of covariant equivalences $\mathsf{AV}_p^{\mathrm{ord}} \to \mathsf{Refl}(\mathcal{R}_p^{\mathrm{ord}})$, and a natural isomorphism of ind-systems

$$\mathcal{M} \otimes_{\mathcal{R}_q^{\mathrm{ord}}} \mathcal{A}_{\mathrm{Del}}^t \simeq \mathcal{A}^{\mathrm{ord}}.$$

Proof. This follows from Theorem 37 applied to $W = W_q^{\mathrm{ord}}$. □

Proposition 45. *For an appropriate choice of ind-system $\mathcal{A} = (A_w, \varphi_{v,w})$, the covariant functor T_* associated to the functor $T = T_{\mathcal{A}}$ of Theorem 1 extends a given choice of Deligne's functor*

$$T_{\mathrm{Del},p} \simeq T_*|_{\mathcal{A}_p^{\mathrm{ord}}} : \mathsf{AV}_p^{\mathrm{ord}} \to \mathsf{Refl}(\mathcal{R}_p^{\mathrm{ord}}).$$

Proof. This follows from Proposition 44 together with the argument of Corollary 41 based on the surjectivity $\mathrm{Pic}(\mathcal{R}_p^{\mathrm{com}}) \to \mathrm{Pic}(\mathcal{R}_p^{\mathrm{ord}})$ of Proposition 33. □

Acknowledgments

The authors would like to thank Gebhard Böckle for stimulating discussions and for his suggestion of the symmetric polynomial $h_\pi(F, V)$. We thank Filippo Nuccio for valuable comments on an earlier version of the manuscript, and Hendrik Lenstra for his interesting observations on local complete intersections. Special thanks go to Brian Conrad and Frans Oort for their attentive reading of a preliminary version of our work, and for the prompt and interesting feedback they gave us. Finally we thank the anonymous referees for their quick work in reviewing the paper.

References

[Bass 1963] H. Bass, "On the ubiquity of Gorenstein rings", *Math. Z.* **82** (1963), 8–28. MR 27 #3669 Zbl 0112.26604

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

[Deligne 1969] P. Deligne, "Variétés abéliennes ordinaires sur un corps fini", *Invent. Math.* **8** (1969), 238–243. MR 40 #7270 Zbl 0179.26201

[Giraud 1968] J. Giraud, "Remarque sur une formule de Shimura–Taniyama", *Invent. Math.* **5** (1968), 231–236. MR 37 #2757 Zbl 0165.54801

[Howe 1995] E. W. Howe, "Principally polarized ordinary abelian varieties over finite fields", *Trans. Amer. Math. Soc.* **347**:7 (1995), 2361–2401. MR 96i:11065 Zbl 0859.14016

[Howe 2004] E. W. Howe, "On the non-existence of certain curves of genus two", *Compos. Math.* **140**:3 (2004), 581–592. MR 2005a:11088 Zbl 1067.11035

[Matsumura 1989] H. Matsumura, *Commutative ring theory*, 2nd ed., Cambridge Studies in Advanced Mathematics **8**, Cambridge University Press, 1989. MR 90i:13001 Zbl 0666.13002

[Milne 1986] J. S. Milne, "Abelian varieties", pp. 103–150 in *Arithmetic geometry* (Storrs, CT, 1984), edited by G. Cornell and J. H. Silverman, Springer, New York, 1986. MR 861974 Zbl 0604.14028

[Serre and Tate 1968] J.-P. Serre and J. Tate, "Good reduction of abelian varieties", *Ann. of Math.* (2) **88** (1968), 492–517. MR 38 #4488 Zbl 0172.46101

[Tate 1966] J. Tate, "Endomorphisms of abelian varieties over finite fields", *Invent. Math.* **2** (1966), 134–144. MR 34 #5829 Zbl 0147.20303

[Tate 1971] J. Tate, "Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)", exposé no. 352, 95–110 in *Séminaire Bourbaki,* 1968/69, Lecture Notes in Math. **175**, Springer, Berlin, 1971. MR 3077121 Zbl 0212.25702

[Waterhouse 1969] W. C. Waterhouse, "Abelian varieties over finite fields", *Ann. Sci. École Norm. Sup.* (4) **2** (1969), 521–560. MR 42 #279 Zbl 0188.53001

[Waterhouse and Milne 1971] W. C. Waterhouse and J. S. Milne, "Abelian varieties over finite fields", pp. 53–64 in *1969 Number Theory Institute* (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, NY., 1969), edited by D. Lewis, Amer. Math. Soc., Providence, R.I., 1971. MR 47 #3397 Zbl 0216.33102

Communicated by Brian Conrad
Received 2014-07-21 Revised 2014-12-05 Accepted 2015-01-06

tommaso.centeleghe@iwr.uni-heidelberg.de
IWR, Universität Heidelberg, Im Neuenheimer Feld 368,
D-69120 Heidelberg, Germany

stix@math.uni-heidelberg.de
Institut für Mathematik, Goethe-Universität Frankfurt,
Robert-Mayer-Straße 6–8, D-60325 Frankfurt am Main,
Germany

mathematical sciences publishers msp

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. 1 2015

1937-0652(2015)9:1;1-8