COMPOSITIO MATHEMATICA

Explicit Serre weights for two-dimensional Galois representations

Frank Calegari, Matthew Emerton, Toby Gee and Lambros Mavrides

Compositio Math. **153** (2017), 1893–1907.

doi:10.1112/S0010437X17007254

FOUNDATION COMPOSITIO MATHEMATICA

LONDON MATHEMATICAL SOCIETY
EST. 1865

Compositio Math. 153 (2017) 1893–1907
doi:10.1112/S0010437X17007254

Explicit Serre weights for two-dimensional Galois representations

Frank Calegari, Matthew Emerton, Toby Gee and Lambros Mavrides

Abstract

We prove the explicit version of the Buzzard–Diamond–Jarvis conjecture formulated by Dembele *et al.* (*Serre weights and wild ramification in two-dimensional Galois representations*, Preprint (2016), arXiv:1603.07708 [math.NT]). More precisely, we prove that it is equivalent to the original Buzzard–Diamond–Jarvis conjecture, which was proved for odd primes (under a mild Taylor–Wiles hypothesis) in earlier work of the third author and coauthors.

1. Introduction

The weight part of Serre's conjecture Hilbert modular forms predicts the weights of the Hilbert modular forms giving rise to a particular modular mod p Galois representation, in terms of the restrictions of this Galois representation to decomposition groups above p. The conjecture was originally formulated in [BDJ10] in the case that p is unramified in the totally real field. Under a mild Taylor–Wiles hypothesis on the image of the global Galois representation, this conjecture has been proved for $p > 2$ in a series of papers of the third author and coauthors, culminating in the paper [GLS15], which proves a generalization allowing p to be arbitrarily ramified. We refer the reader to the introduction to [GLS15] for a discussion of these results.

Let $K/\mathbb{Q}_p$ be an unramified extension and let $\overline{\rho} : G_K \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ be a (continuous) representation. If $\overline{\rho}$ is irreducible, then the recipe for predicted weights in [BDJ10] is completely explicit, but in the case where it is a non-split extension of characters, the recipe is in terms of the reduction modulo p of certain crystalline extensions of characters. This description is not useful for practical computations and the recent paper [DDR16] proposed an alternative recipe in terms of local class field theory, along with the Artin–Hasse exponential, which can be made completely explicit in concrete examples (indeed, [DDR16, §§ 9–10] gives substantial numerical evidence for their conjecture).

In this paper, we prove [DDR16, Conjecture 7.2], which says that the recipes of [BDJ10] and [DDR16] agree. This is a purely local conjecture and our proof is purely local. Our main input is the results of [GLS14] (and their generalization to $p = 2$ in [Wan16]). We briefly sketch our approach. Suppose that $\overline{\rho} \cong \left(\begin{smallmatrix}\chi_1 & * \\ 0 & \chi_2\end{smallmatrix}\right)$, and set $\chi = \chi_1\chi_2^{-1}$. For a given Serre weight, the recipes of [BDJ10] and [DDR16] determine subspaces L_{BDJ} and L_{DDR} of $H^1(G_K, \chi)$, and we have to prove that $L_{\mathrm{BDJ}} = L_{\mathrm{DDR}}$.

Received 22 August 2016, accepted in final form 31 March 2017, published online 20 June 2017.
2010 Mathematics Subject Classification 11F80, 11F41 (primary).
Keywords: Galois representations, Hilbert modular forms.
The first author is supported in part by NSF grant DMS-1648702. The second author is supported in part by the NSF grant DMS-1303450. The third author is supported in part by a Leverhulme Prize, EPSRC grant EP/L025485/1, Marie Curie Career Integration Grant 303605, and ERC Starting Grant 306326.

Let K_∞/K be the (non-Galois) extension obtained by adjoining a compatible system of p^nth roots of a fixed uniformizer of K for all n. The restriction map $H^1(G_K,\chi)\to H^1(G_{K_\infty},\chi)$ is injective unless χ is the mod p cyclotomic character, and [GLS14, Theorem 7.9] allows us to give an explicit description of the image of L_{BDJ} in $H^1(G_{K_\infty},\chi)$ in terms of Kisin modules. The theory of the field of norms gives a natural isomorphism of G_{K_∞} with $G_{k((u))}$, where k is the residue field of K, and we obtain a description of the image of L_{BDJ} in $H^1(G_{k((u))},\chi)$ in terms of Artin–Schreier theory. On the other hand, we prove a compatibility of the Artin–Hasse exponential with the field of norms construction that allows us to compute the image of L_{DDR} in $H^1(G_{k((u))},\chi)$. We then use an explicit reciprocity law of Schmid [Sch36] to reduce the comparison of L_{BDJ} and L_{DDR} to a purely combinatorial problem, which we solve.

It is possible that the conjecture of [DDR16] could be extended to the case that p ramifies in K; we have not tried to do this, but we expect that if such a generalization exists, it could be proved by the methods of this paper, using the results of [GLS15].

The fourth author's PhD thesis [Mav16] proved [DDR16, Conjecture 7.2] in generic cases using similar techniques to those of this paper in the setting of (φ,Γ)-modules (using the results of [CD11] where we appeal to [GLS14]), while the first three authors arrived separately at the strategy presented here for resolving the general case.

2. Notation

We follow the conventions of [GLS15], which are the same as those in the arXiv version of [GLS14] (see [GLS15, Appendix A] for a correction to some of the indices in the published version of [GLS14]). Let p be prime, and let $K/\mathbb{Q}_p$ be a finite unramified extension of degree f, with residue field k. Embeddings $\sigma : k\hookrightarrow\overline{\mathbb{F}}_p$ biject with $\mathbb{Q}_p$-linear embeddings $K\hookrightarrow\overline{\mathbb{Q}}_p$, and we choose one such embedding $\sigma_0 : k\hookrightarrow\overline{\mathbb{F}}_p$, and recursively require that $\sigma_{i+1}^p=\sigma_i$. Note that $\sigma_{i+f}=\sigma_i$. Note also that this convention is opposite to that of [DDR16], so that their σ_i is our σ_{-i}; consequently, to compare our formulae to those of [DDR16], one has to negate the indices throughout.

If π is a root of $x^{p^f-1}+p=0$ then we have the fundamental character $\omega_f : G_K\to k^\times$ defined by

$$\omega_f(g)=g(\pi)/\pi \pmod{\pi\mathcal{O}_{K(\pi)}}.$$

The composite of ω_f with the Artin map Art_K (which we normalize so that a uniformizer corresponds to a geometric Frobenius element) is the homomorphism $K^\times\to k^\times$ sending p to 1 and sending elements of $\mathcal{O}_K^\times$ to their reductions modulo p. For each $\sigma : k\hookrightarrow\overline{\mathbb{F}}_p$, we set $\omega_\sigma := \sigma\circ\omega|_{I_K}$ and $\omega_i := \omega_{\sigma_i}$ so that, in particular, we have $\omega_{i+1}^p=\omega_i$.

If l/k is a finite extension, we choose an embedding $\widetilde{\sigma}_0 : l\hookrightarrow\overline{\mathbb{F}}_p$ extending σ_0, and again set $\widetilde{\sigma}_i=\widetilde{\sigma}_{i+1}^p$. We have an isomorphism

$$l\otimes_{\mathbb{F}_p}\overline{\mathbb{F}}_p \xrightarrow{\sim} \prod_{\widetilde{\sigma}_i}\overline{\mathbb{F}}_p, \tag{2.0.1}$$

with the projection onto the factor labelled by $\widetilde{\sigma}_i$ being given by $x\otimes y\mapsto\widetilde{\sigma}_i(x)y$. Under this isomorphism, the automorphism $\varphi\otimes\mathrm{id}$ on $l\otimes_{\mathbb{F}_p}\overline{\mathbb{F}}_p$ becomes identified with the automorphism on $\prod\overline{\mathbb{F}}_p$ given by $(y_i)\mapsto(y_{i-1})$.

If $\mathcal{M}$ is an $l\otimes_{\mathbb{F}_p}\overline{\mathbb{F}}_p$-module equipped with a φ-linear endomorphism φ, then the isomorphism (2.0.1) induces a corresponding decomposition $\mathcal{M}\xrightarrow{\sim}\prod_i\mathcal{M}_i$, and the endomorphism φ of $\mathcal{M}$ induces $\overline{\mathbb{F}}_p$-linear morphisms $\varphi : \mathcal{M}_{i-1}\to\mathcal{M}_i$.

3. Results

3.1 Fields of norms

We briefly recall (following [Kis09, § 1.1.12]) the theory of the field of norms and of étale φ-modules, adapted to the case at hand. For each n, let $(-p)^{1/p^n}$ be a choice of the p^nth root of $-p$, chosen so that $((-p)^{1/p^{n+1}})^p = (-p)^{1/p^n}$, and let $K_n = K((-p)^{1/p^n})$. Write $K_\infty = \bigcup_n K_n$. Then, by the theory of the field of norms,

$$\varprojlim_{N_{K_{n+1}/K_n}} K_n$$

(the transition maps being the norm maps) can be identified with $k((u))$, with $((-p)^{1/p^n})_n$ corresponding to u. If F is a finite extension of K (inside some given algebraic closure of K containing K_∞), then $F_\infty := FK_\infty$ is a finite extension of K_∞, and applying the field of norms construction to F_∞, we obtain a finite separable extension

$$\mathcal{F} := \varprojlim_{N_{FK_n/FK_{n-1}}} FK_n,$$

of $k((u))$. If F is Galois over K, then F_∞ is Galois over K_∞, and $\mathcal{F}$ is also Galois over $k((u))$, and there is a natural isomorphism of Galois groups

$$\mathrm{Gal}(\mathcal{F}/k((u))) \xrightarrow{\sim} \mathrm{Gal}(F_\infty/K_\infty), \tag{3.1.1}$$

and, composing with the canonical homomorphism $\mathrm{Gal}(F_\infty/K_\infty) \to \mathrm{Gal}(F/K)$, a natural homomorphism of Galois groups

$$\mathrm{Gal}(\mathcal{F}/k((u))) \to \mathrm{Gal}(F/K). \tag{3.1.2}$$

Every finite extension of K_∞ arises as such an F_∞ and, in this manner, we obtain a functorial bijection between finite extensions of K_∞ and finite separable extensions $\mathcal{F}$ of $k((u))$. In particular, the various isomorphisms (3.1.1) piece together to induce a natural isomorphism of absolute Galois groups

$$G_{K_\infty} = G_{k((u))}. \tag{3.1.3}$$

The utility of the isomorphism (3.1.3) arises from the fact that there is an equivalence of abelian categories between the category of finite-dimensional $\overline{\mathbb{F}}_p$-representations V of $G_{k((u))}$ and the category of *étale φ-modules*. The latter are, by definition, finite $k((u)) \otimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p$-modules $\mathcal{M}$ equipped with a φ-semilinear map $\varphi : \mathcal{M} \to \mathcal{M}$, with the property that the induced $k((u)) \otimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p$-linear map $\varphi^*\mathcal{M} \to \mathcal{M}$ is an isomorphism. This equivalence of categories preserves lengths in the obvious sense, and is given by the functors

$$T : \mathcal{M} \to (k((u))^{\mathrm{sep}} \otimes_{k((u))} \mathcal{M})^{\varphi=1}$$

(where $k((u))^{\mathrm{sep}}$ is a separable closure of $k((u))$) and

$$V \mapsto (k((u))^{\mathrm{sep}} \otimes_{\mathbb{F}_p} V)^{G_{k((u))}}.$$

The isomorphism (3.1.3) then allows us to describe finite-dimensional representations of G_{K_∞} over $\overline{\mathbb{F}}_p$ via étale φ-modules. In the § 3.3 we make this description completely explicit in the context of (the restriction to K_∞ of) the crystalline extensions of characters that arise in the conjecture of [BDJ10].

The above isomorphisms of Galois groups are compatible with local class field theory in a natural way. Namely, if F/K and $\mathcal{F}/k((u))$ are as above, then the projection map $k((u)) = \varprojlim_{N_{K_{n+1}/K_n}} K_n \to K$ induces a natural map

$$k((u))^\times / N_{\mathcal{F}/k((u))^\times} \mathcal{F}^\times \to K^\times / N_{F/K} F^\times, \tag{3.1.4}$$

and we have the following result.

Lemma 3.1.5. *If F/K is a finite abelian extension, then the following diagram commutes.*

$$\begin{array}{ccc} \mathrm{Gal}(\mathcal{F}/k((u))) & \xrightarrow{\mathrm{Art}_{k((u))}^{-1}} & k((u))^\times / N_{\mathcal{F}/k((u))^\times} \mathcal{F}^\times \\ \Big\downarrow{\scriptstyle (3.1.2)} & & \Big\downarrow{\scriptstyle (3.1.4)} \\ \mathrm{Gal}(F/K) & \xrightarrow{\mathrm{Art}_K^{-1}} & K^\times / N_{F/K} F^\times \end{array}$$

Proof. This is easily checked directly, and is a special case of [AJ12, Proposition 5.2], which proves a generalization to higher-dimensional local fields; see also [Lau88], where the analogous result is proved for general APF extensions (strictly speaking, the result of [Lau88] does not apply as written in our situation, as the extension K_∞/K is not Galois; but, in fact, the argument still works). In brief, it is enough to check separately the cases that F/K is either unramified or totally ramified; in the former case the result is immediate, while the latter case follows from Dwork's description of Artin's reciprocity map for totally ramified abelian extensions [Ser79, XIII § 5 Corollary to Theorem 2]. □

3.2 Compatibility of pairings

It will be convenient to establish a further compatibility between various natural pairings. For a field M, let $M^{(p)}/M$ denote the maximal exponent p abelian extension (inside some fixed algebraic closure). If M_∞/M is an extension, then we have a diagram as follows (where pr is the natural map given by restriction of automorphisms of $M_\infty^{(p)}$ to $M^{(p)}$).

$$\begin{array}{ccccc} \mathrm{Gal}(M_\infty^{(p)}/M_\infty) & \times & H^1(G_{M_\infty}, \overline{\mathbb{F}}_p) & \longrightarrow & \overline{\mathbb{F}}_p \\ \Big\downarrow{\scriptstyle \mathrm{pr}} & & \Big\uparrow{\scriptstyle \iota} & & \\ \mathrm{Gal}(M^{(p)}/M) & \times & H^1(G_M, \overline{\mathbb{F}}_p) & \longrightarrow & \overline{\mathbb{F}}_p \end{array}$$

Lemma 3.2.1. *The diagram commutes, in the sense that $\langle \mathrm{pr}\, \alpha, \beta \rangle = \langle \alpha, \iota\beta \rangle$.*

Proof. Since $H^1(G_M, \overline{\mathbb{F}}_p) = \mathrm{Hom}(G_M, \overline{\mathbb{F}}_p)$ (and similarly for M_∞), since the pairings are given by evaluation, and since ι is the natural restriction map, this is clear. □

Suppose now that M is a finite extension of $\mathbb{Q}_p$ with residue field l, and that π is a uniformizer of M. If M_∞/M is the extension given by a compatible choice of p-power roots of π, then

$$\mathrm{Gal}(M_\infty^{(p)}/M_\infty) \simeq l((u))^\times \otimes \mathbb{F}_p$$

via the field of norms construction together with local class field theory (applied to $l((u))$).

On the other hand, taking Galois cohomology of the short exact sequence

$$0 \to \overline{\mathbb{F}}_p \to l((u))^{\mathrm{sep}} \otimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p \xrightarrow{\psi\otimes\mathrm{id}} l((u))^{\mathrm{sep}} \otimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p \to 0,$$

where $\psi : l((u))^{\mathrm{sep}} \to l((u))^{\mathrm{sep}}$ is the Artin–Schreier map defined by $\psi(x) = x^p - x$, yields an isomorphism

$$H^1(G_{M_\infty}, \overline{\mathbb{F}}_p) = H^1(G_{l((u))}, \overline{\mathbb{F}}_p) = \mathrm{Hom}(G_{l((u))}, \overline{\mathbb{F}}_p) \simeq (l((u))/\psi l((u))) \otimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p;$$

concretely, the element $a \in l((u))$ corresponds to the homomorphism $f_a : G_{l((u))} \to \mathbb{F}_p$ given by $f_a(g) = g(x) - x$, where $x \in l((u))^{\mathrm{sep}}$ is chosen so that $\psi(x) = a$. (See e.g. [Ser79, X § 3(a)] for more details.)

Theorem 3.2.2. *Let $\sigma_b \in \mathrm{Gal}(M_\infty^{(p)}/M_\infty)$ be the Galois element corresponding via the local Artin map to an element $b \in l((u))^\times \otimes \mathbb{F}_p$, and let f_a be the element of $H^1(G_{M_\infty}, \overline{\mathbb{F}}_p)$ corresponding to an element $a \in (l((u))/\psi l((u))) \otimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p$. Then*

$$\langle f_a, \sigma_b \rangle = \mathrm{Tr}_{l\otimes_{\mathbb{F}_p}\overline{\mathbb{F}}_p/\overline{\mathbb{F}}_p}\left(\mathrm{Res}\, a \cdot \frac{db}{b}\right).$$

Proof. This was first proved in [Sch36]; for a more modern proof, see [Ser79, XIV Corollary to Proposition 15]. □

3.3 Crystalline extension classes and L_{BDJ}

We begin by briefly recalling some of the main results of [GLS14]. For each $0 \leqslant i \leqslant f-1$ we fix an integer $r_i \in [1, p]$; we then define r_i for all integers i by demanding that $r_{i+f} = r_i$. We let J be a subset of $\{0, \ldots, f-1\}$, and we assume that J is maximal in the sense of [DDR16, § 7.2]; in other words, we assume that:

(i) if for some $i > j$ we have $(r_j, \ldots, r_i) = (1, p-1, \ldots, p-1, p)$, and $j+1, \ldots, i \notin J$, then $j \notin J$; and

(ii) if all the r_i are equal to $p-1$, or if $p = 2$ and all of the r_i are equal to 2, then J is non-empty.

We let $\chi : G_K \to \overline{\mathbb{F}}_p^\times$ be a character with the property that

$$\chi|_{I_K} = \prod_{j\in J} \omega_j^{r_j} \prod_{j\notin J} \omega_j^{-r_j}.$$

We let L_{BDJ} denote the subset of $H^1(G_K, \chi)$ consisting of those classes corresponding to extensions of the trivial character by χ that arise as the reductions of crystalline representation whose σ_i-labelled Hodge–Tate weights are $\{0, (-1)^{i\notin J} r_i\}$, where $(-1)^{i\notin J}$ is 1 if $i \in J$ and -1 otherwise. The subsequent points follow from the proof of [GLS14, Theorem 9.1], together with [GLS14, Lemmas 9.3 and 9.4] and (in the case that $p = 2$) the results of [Wan16].

(i) The subset L_{BDJ} is an $\overline{\mathbb{F}}_p$-subspace of $H^1(G_K, \chi)$.

(ii) An extension class is in L_{BDJ} if and only if it admits a *reducible* crystalline lift whose σ_i-labelled Hodge–Tate weights are $\{0, (-1)^{i\notin J} r_i\}$.

(iii) If $J = \{0, \ldots, f-1\}$ and all $r_i = p$, then $L_{\mathrm{BDJ}} = H^1(G_K, \chi)$.

(iv) Assume that we are not in the case of the previous point. Then $\dim_{\overline{\mathbb{F}}_p} L_{\mathrm{BDJ}} = |J|$, unless $\chi = 1$, in which case $\dim_{\overline{\mathbb{F}}_p} L_{\mathrm{BDJ}} = |J| + 1$.

We recall below from [DDR16] the definition of another subspace of $H^1(G_K, \chi)$, denoted by L_{DDR}; our main result, then, is that $L_{\mathrm{BDJ}} = L_{\mathrm{DDR}}$. We begin with an easy special case.

LEMMA 3.3.1. *If $J = \{0, \dots, f-1\}$ and every $r_i = p$, then $L_{\mathrm{BDJ}} = L_{\mathrm{DDR}}$.*

Proof. In this case we have $L_{\mathrm{DDR}} = H^1(G_K, \chi)$ by definition (see Definition 3.4.1 below), and we already noted above that $L_{\mathrm{BDJ}} = H^1(G_K, \chi)$. □

We can and do exclude the case covered by Lemma 3.3.1 from now on; that is, in addition to the assumptions made above, we assume that:

- if every r_i is equal to p, then $J \neq \{0, \dots, f-1\}$.

If $\chi = \bar{\epsilon}$, then the peu ramifié subspace of $H^1(G_K, \bar{\epsilon})$ is, by definition, the codimension one subspace spanned by the classes corresponding via Kummer theory to elements of $\mathcal{O}_K^\times$. Since we have excluded the cases covered by Lemma 3.3.1, L_{BDJ} is contained in the peu ramifié subspace of $H^1(G_K, \bar{\epsilon})$ by [DS15, Theorem 4.9].

By [GLS15, Lemma 5.4.2], for any $\chi \neq \bar{\epsilon}$ the natural restriction map $H^1(G_K, \chi) \to H^1(G_{K_\infty}, \chi)$ is injective, while if $\chi = \bar{\epsilon}$, then the kernel is spanned by the tres ramifié class corresponding to $-p$; in particular, the restriction of this map to L_{BDJ} is injective. The following theorem describes the image of L_{BDJ}; before stating it, we introduce some notation that we will use throughout the paper.

Write χ as a power of ω_0 times an unramified character $\mu : \mathrm{Gal}(L/K) \to \overline{\mathbb{F}}_p^\times$, and write $\mu(\mathrm{Frob}_K) = a$, so that $a^{[l:k]} = 1$; here $\mathrm{Frob}_K \in \mathrm{Gal}(L/K)$ denotes the arithmetic Frobenius. For each $\sigma : k \hookrightarrow \overline{\mathbb{F}}_p$, we let $\lambda_{\sigma,\mu}$ be the element $(1, a^{-1}, \dots, a^{1-[l:k]}) \in l \otimes_{k,\sigma} \overline{\mathbb{F}}_p$, so that $\lambda_{\sigma,\mu}$ is a basis of the one-dimensional $\overline{\mathbb{F}}_p$-vector space $(l \otimes_{k,\sigma} \overline{\mathbb{F}}_p)^{\mathrm{Gal}(L/K)=\mu}$. Similarly, we let $\lambda_{\sigma,\mu^{-1}}$ be the element $(1, a, \dots, a^{[l:k]-1}) \in l \otimes_{k,\sigma} \overline{\mathbb{F}}_p$.

THEOREM 3.3.2. *The subspace L_{BDJ} of $H^1(G_K, \chi)$ consists of precisely those classes whose restrictions to $H^1(G_{K_\infty}, \chi)$ can be represented by étale φ-modules $\mathcal{M}$ of the following form.*

Set $h_i = r_i$ if $i \in J$ and $h_i = 0$ if $i \notin J$. Then we can choose bases e_i, f_i of the $\mathcal{M}_i$ so that φ has the form

$$\varphi(e_{i-1}) = u^{r_i - h_i} e_i,$$
$$\varphi(f_{i-1}) = (a)_i u^{h_i} f_i + x_i e_i.$$

Here $(a)_i = 1$ for $i \neq 0$, and equals $a = \mu(\mathrm{Frob}_K)$ for $i = 0$; and we have $x_i = 0$ if $i \notin J$ and $x_i \in \overline{\mathbb{F}}_p$ if $i \in J$, except in the case that $\chi = 1$.

If $\chi = 1$ then $a = 1$, and if we fix some $i_0 \in J$, then x_{i_0} is allowed to be of the form $x'_{i_0} + x''_{i_0} u^p$ with $x'_{i_0}, x''_{i_0} \in \overline{\mathbb{F}}_p$ (while the other x_i are in $\overline{\mathbb{F}}_p$).

In every case, the x_i are uniquely determined by $\mathcal{M}$.

Proof. In the case $p > 2$, this is an immediate consequence of [GLS14, Theorem 7.9] (which describes the corresponding Kisin modules, which are just lattices in $\mathcal{M}$; the set J' appearing there can be taken to be our J by [GLS14, Proposition 8.8] and our assumption that J is maximal) and the proof of [GLS14, Theorem 9.1] (which shows that the different x_i give rise to different Galois representations), while if $p = 2$, then the result follows from the results of [Wan16]. □

As in § 2, we let π be a choice of (p^f-1)th root of $-p$. Write $M := L(\pi)$, where L/K is an unramified extension of degree prime to p, chosen so that $\chi|_{G_M}$ is trivial (in [DDR16] a slightly more general choice of M is permitted, but it is shown there that their constructions are independent of this choice, and this choice is convenient for us). Then M/K is an abelian extension of degree prime to p. Since (p^f-1) is prime to p, for each $n \geqslant 1$ there is a unique p^nth root π^{1/p^n} of π such that $(\pi^{1/p^n})^{(p^f-1)} = (-p)^{1/p^n}$, and we set $M_n = M(\pi^{1/p^n})$, $M_\infty = \bigcup_n M_n$.

If $\mathcal{M}$ is an étale φ-module with corresponding G_{K_∞}-representation $T(\mathcal{M})$, then it is easy to check that the étale φ-module corresponding to $T(\mathcal{M})|_{G_{M_\infty}}$ is

$$\mathcal{M}_M := l((u)) \otimes_{k((u)),u\mapsto u^{p^f-1}} \mathcal{M}.$$

Applying this to one of the étale φ-modules arising in the statement of Theorem 3.3.2, it follows that (with the obvious choice of basis e_i, f_i for $\mathcal{M}_M$) the matrix of $\varphi : \mathcal{M}_{M,i-1} \to \mathcal{M}_{M,i}$ is

$$\begin{pmatrix} u^{(r_i-h_i)(p^f-1)} & x_i \\ 0 & (a)_i u^{h_i(p^f-1)} \end{pmatrix}$$

whereas above $h_i = r_i$ if $i \in J$ and $h_i = 0$ if $i \notin J$, and x_i is zero if $i \notin J$. Furthermore, $x_i \in \overline{\mathbb{F}}_p$, except that if $\chi = 1$, we have fixed a choice of $i_0 \in J$, and x_{i_0} is allowed to be of the form $x'_{i_0} + x''_{i_0} u^{p(p^f-1)}$ with $x'_{i_0}, x''_{i_0} \in \overline{\mathbb{F}}_p$. (Here the $\mathcal{M}_{M,i}$ are periodic with period $f[l:k]$, but of course the r_i, h_i and x_i depend only on i modulo f.)

We now make a change of basis, setting $e'_i = u^{\alpha_i} e_i$ and $f'_i = a^{\lfloor i/f \rfloor} u^{\beta_i} f_i$ (where $0 \leqslant i \leqslant f[l:k]-1$), so that the matrix of $\varphi : \mathcal{M}_{M,i-1} \to \mathcal{M}_{M,i}$ becomes

$$\begin{pmatrix} u^{(r_i-h_i)(p^f-1)+p\alpha_{i-1}-\alpha_i} & a^{\lfloor i-1/f \rfloor} x_i u^{p\beta_{i-1}-\alpha_i} \\ 0 & u^{h_i(p^f-1)+p\beta_{i-1}-\beta_i} \end{pmatrix}.$$

We choose the α_i, β_i so that the entries on the diagonal become trivial; concretely, this means that we set

$$\alpha_i = -\sum_{j=0}^{f-1} (r_{i+j+1} - h_{i+j+1}) p^{f-1-j}, \quad \beta_i = -\sum_{j=0}^{f-1} h_{i+j+1} p^{f-1-j}.$$

Write $\xi_i := \alpha_i - p\beta_{i-1}$, so that we have

$$\xi_i = \sum_{j=0}^{f-1} (-1)^{i+j+1 \notin J} r_{i+j+1} p^{f-1-j} + \delta_{i\in J} r_i (p^f - 1),$$

where $\delta_{i\in J} = 1$ if $i \in J$ and 0 otherwise.

With the obvious basis for $\mathcal{M}_M$ as an $l((u)) \otimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p$-module, $\phi_{\mathcal{M}_M}$ is given by the matrix

$$\begin{pmatrix} 1 & (x_i a^{-1} \lambda_{\sigma_i,\mu^{-1}} u^{-\xi_i})_{i=0,\dots,f-1} \\ 0 & 1 \end{pmatrix}$$

where $\lambda_{\sigma_i,\mu^{-1}}$ is the element of $l \otimes_{k,\sigma_i} \overline{\mathbb{F}}_p$ that we defined above. Then $T(\mathcal{M}_M)$ is an extension of the trivial representation by itself, and thus corresponds to an element of $\mathrm{Hom}(G_{l((u))}, \overline{\mathbb{F}}_p)$. By the definition of T, the kernel of this homomorphism corresponds to the Artin–Schreier extension of $l((u))$ determined by $(x_i \lambda_{\sigma_i,\mu^{-1}} u^{-\xi_i})_{i=0,\dots,f-1}$. We have therefore proved the following result.

https://doi.org/10.1112/S0010437X17007254 Published online by Cambridge University Press

COROLLARY 3.3.3. *The image of* L_{BDJ} *in* $H^1(G_{M_\infty}, \overline{\mathbb{F}}_p) = \mathrm{Hom}(G_{l((u))}, \overline{\mathbb{F}}_p)$ *is spanned by the classes* $f_{\lambda_{\sigma_i,\mu^{-1}}u^{-\xi_i}}$ *corresponding via Artin–Schreier theory to the elements*

$$\lambda_{\sigma_i,\mu^{-1}}u^{-\xi_i} \in l \otimes_{k,\sigma_i} \overline{\mathbb{F}}_p \subseteq l \otimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p,$$

for $i \in J$*, together with the class* $f_{\lambda_{\sigma_{i_0},\mu^{-1}}u^{p(p^f-1)-\xi_{i_0}}}$ *if* $\chi = 1$.

As in [DDR16, § 3.2], we may write $\chi|_{I_K} = \omega_0^{n_0}$ for some unique n_0 of the form $n_0 = \sum_{j=1}^{f} a_j p^{f-j}$ with each $a_j \in [1, p]$ and at least one $a_j \neq p$. We set

$$n_i = \sum_{j=1}^{f} a_{i+j} p^{f-j},$$

so we have $\chi|_{I_K} = \omega_i^{n_i}$, and for all i, j we have

$$p^{-i} n_i \equiv p^{-j} n_j \pmod{p^f - 1}.$$

Note that we have

$$\begin{aligned}\chi|_{I_K} &= \prod_{j\in J} \omega_j^{r_j} \prod_{j\notin J} \omega_j^{-r_j} \\ &= \prod_{j=0}^{f-1} \omega_i^{-(-1)^{i+j+1\in J} r_{i+j+1} p^{f-1-j}} \\ &= \omega_i^{\alpha_i - p\beta_{i-1}} = \omega_i^{\xi_i},\end{aligned}$$

so that, in particular, we have

$$\xi_i \equiv n_i \pmod{p^f - 1}. \tag{3.3.4}$$

3.4 The Artin–Hasse exponential and L_{DDR}

We now recall some of the definitions made in [DDR16, § 5.1]. In particular, for each i we define an embedding σ_i' and an integer n_i' as follows. If $a_{i-1} \neq p$, then we set $\sigma_i' = \sigma_{i-1}$ and $n_i' = n_{i-1}$. If $a_{i-1} = p$, then we let j be the greatest integer less than i such that $a_{j-1} \neq p - 1$, and we set $\sigma_i' = \sigma_{j-1}$ and $n_i' = n_{j-1} - (p^f - 1)$. Note that we always have $n_i' > 0$.

We let $E(x) = \exp(\sum_{m\geqslant 0} x^{p^m}/p^m) \in \mathbb{Z}_p[[x]]$ denote the Artin–Hasse exponential. For any $\alpha \in \mathfrak{m}_M$, we define the homomorphism

$$\epsilon_\alpha : l \otimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p \to \mathcal{O}_M^\times \otimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p$$

by $\epsilon_\alpha(a \otimes b) := E([a]\alpha) \otimes b$, where $[\cdot] : l \to W(l)$ is the Teichmüller lift. Then we set

$$u_i := \epsilon_{\pi^{n_i'}}(\lambda_{\sigma_i',\mu}) \in \mathcal{O}_M^\times \otimes \overline{\mathbb{F}}_p.$$

In the case that $\chi = 1$, we also set $u_{\mathrm{triv}} := \pi \otimes 1 \in M^\times \otimes \overline{\mathbb{F}}_p$, and in the case that $\chi = \overline{\epsilon}$, the mod p cyclotomic character, we set $u_{\mathrm{cyc}} := \epsilon_{\pi^{p(p^f-1)/(p-1)}}(b \otimes 1)$, where $b \in l$ is any element with

https://doi.org/10.1112/S0010437X17007254 Published online by Cambridge University Press

$\mathrm{Tr}_{l/\mathbb{F}_p}(b) \neq 0$. It is shown in [DDR16, § 5] that the u_i, together with u_{triv} if $\chi = 1$, and u_{cyc} if $\chi = \overline{\epsilon}$, are a basis of the $\overline{\mathbb{F}}_p$-vector space

$$U_\chi := (M^\times \otimes \overline{\mathbb{F}}_p(\chi^{-1}))^{\mathrm{Gal}(M/K)}.$$

Via the Artin map Art_M, we may write

$$H^1(G_K, \chi) \cong \mathrm{Hom}_{\mathrm{Gal}(M/K)}(M^\times, \overline{\mathbb{F}}_p(\chi))$$

and, thus, identify $H^1(G_K, \chi)$ with the $\overline{\mathbb{F}}_p$-dual of U_χ. We then define a basis of $H^1(G_K, \chi)$ by letting c_i, c_{triv} (if $\chi = 1$) and c_{cyc} (if $\chi = \overline{\epsilon}$) denote the dual basis to that given by the u_i, u_{triv} and u_{cyc}.

Recall from [DDR16, § 7.1] the definition of the set $\mu(J)$. It is defined as follows: $\mu(J) = J$, unless there is some $i \notin J$ for which we have $a_{i-1} = p$, $a_{i-2} = p-1, \dots, a_{i-s} = p-1, a_{i-s-1} \neq p-1$, and at least one of $i-1, i-2, \dots, i-s$ is in J. If this is the case, we let x be minimal such that $i-x \in J$, and we consider the set obtained from J by replacing $i-x$ with i. Then $\mu(J)$ is the set obtained by simultaneously making all such replacements (that is, making these replacements for all possible i).

Definition 3.4.1. We define L_{DDR} to be the subspace of $H^1(G_K, \chi)$ spanned by the classes c_i for $i \in \mu(J)$, together with the class c_{triv} if $\chi = 1$, and the class c_{cyc} if $\chi = \overline{\epsilon}$, $J = \{0, \dots, f-1\}$ and every $r_i = p$.

3.5 The comparison of L_{BDJ} and L_{DDR}

In this section, we prove that the classes in L_{BDJ} are orthogonal to certain u_i. We begin with a computation that will allow us to compare the constructions underlying the definition of L_{DDR}, which involve the Artin–Hasse exponential, with the field of norms constructions underlying the description of L_{BDJ}.

Lemma 3.5.1. *For any $n \geqslant 1$, $a \in l$ and $r \geqslant 1$ with $(r,p) = 1$ we have $N_{K_n/K} E([a^{1/p^n}](\pi^{1/p^n})^r) = E([a]\pi^r)$.*

Proof. Let ζ be a primitive p^nth root of unity. Then

$$\begin{aligned}
N_{K_n/K} E([a^{1/p^n}](\pi^{1/p^n})^r) &= \prod_{k=0}^{p^n-1} E([a^{1/p^n}](\pi^{1/p^n})^r \zeta^k) \\
&= \prod_{k=0}^{p^n-1} \exp\biggl(\sum_{m \geqslant 0} \frac{[a^{1/p^n}]^{p^m} (\pi^{1/p^n})^{rp^m} \zeta^{kp^m}}{p^m}\biggr) \\
&= \exp\biggl(\sum_{k=0}^{p^n-1} \sum_{m \geqslant 0} \frac{[a^{1/p^n}]^{p^m} (\pi^{1/p^n})^{rp^m} \zeta^{kp^m}}{p^m}\biggr) \\
&= \exp\biggl(\sum_{m \geqslant 0} \frac{[a^{1/p^n}]^{p^m} (\pi^{1/p^n})^{rp^m}}{p^m} \sum_{k=0}^{p^n-1} \zeta^{kp^m}\biggr).
\end{aligned}$$

https://doi.org/10.1112/S0010437X17007254 Published online by Cambridge University Press

Now the sum over roots of unity is 0 if $\zeta^{p^m} \neq 1$ (equivalently, $m < n$) and p^n if $\zeta^{p^m} = 1$ (equivalently, $m \geqslant n$). Hence,

$$\begin{aligned} N_{K_n/K} E([a^{1/p^n}](\pi^{1/p^n})^r) &= \exp\biggl(\sum_{m \geqslant n} \frac{[a^{1/p^n}]^{p^m}(\pi^{1/p^n})^{rp^m} p^n}{p^m}\biggr) \\ &= \exp\biggl(\sum_{m \geqslant 0} \frac{[a^{1/p^n}]^{p^{n+m}}(\pi^{1/p^n})^{rp^{n+m}} p^n}{p^{m+n}}\biggr) \\ &= \exp\biggl(\sum_{m \geqslant 0} \frac{[a]^{p^m}(\pi^r)^{p^m}}{p^m}\biggr) = E([a]\pi^r). \end{aligned}$$

□

For each $r \geqslant 1$ have a homomorphism

$$\epsilon_{u^r} : l \otimes \overline{\mathbb{F}}_p \to l((u))^\times \otimes \mathbb{F}_p$$

defined by $\epsilon_{u^r}(a \otimes b) = E(au^r) \otimes b$. Then, for each i, we set

$$\tilde{u}_i := \epsilon_{u^{n'_i}}(\lambda_{\sigma'_i,\mu}) \in l((u))^\times \otimes \mathbb{F}_p.$$

Lemma 3.5.2. *Let $r \geqslant 1$ be coprime to p. Then under the homomorphism (3.1.4) (with M in place of K), the image of $E([a]u^r)$ is equal to $E([a]\pi^r)$; consequently, for each i, the image of $\tilde{u}_i$ is u_i.*

Proof. This is an immediate consequence of Lemma 3.5.1, taking into account Lemma 3.6.1 below, which shows that n'_i is coprime to p. □

We now state and prove our main result, which establishes [DDR16, Conjecture 7.2], by reducing the equality $L_{\mathrm{DDR}} = L_{\mathrm{BDJ}}$ to a purely combinatorial problem that is solved in § 3.6.

Theorem 3.5.3. *We have $L_{\mathrm{BDJ}} = L_{\mathrm{DDR}}$.*

Proof. Since we have $\dim_{\overline{\mathbb{F}}_p} L_{\mathrm{BDJ}} = \dim_{\overline{\mathbb{F}}_p} L_{\mathrm{DDR}} = |J| + \delta_{\chi=1}$, it is enough to prove that $L_{\mathrm{BDJ}} \subseteq L_{\mathrm{DDR}}$. By the definition of L_{DDR}, it is equivalent to prove that the image of every class in L_{BDJ} in $H^1(G_M, \overline{\mathbb{F}}_p)$ is orthogonal under the pairing of § 3.2 to the elements $u_j \in U_\chi$, $j \notin \mu(J)$.

In the case that $\chi = \overline{\epsilon}$, we also need to show that the classes are orthogonal to u_{cyc}; to see this, note that, as explained in [DDR16, § 6.4] the classes c_i (together with c_{triv} if $p = 2$) span the space of classes which are (equivalently) flatly or typically ramified in the sense of [DDR16, § 3.3], which are exactly the peu ramifié classes; in other words, the classes orthogonal to u_{cyc} are exactly the peu ramifié classes. As we recalled in § 3.3, it follows from [DS15, Theorem 4.9] that every class in L_{BDJ} is peu ramifié.

Combining Lemmas 3.1.5 and 3.2.1, Theorem 3.2.2, Lemma 3.5.2 and Corollary 3.3.3, we see that we must show that for all $i \in J$, $j \notin \mu(J)$, the residue

$$\mathrm{Tr}_{l \otimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p / \overline{\mathbb{F}}_p} \mathrm{Res}(\mathrm{dlog}(\tilde{u}_j) \cdot \lambda_{\sigma_i,\mu^{-1}} u^{-\xi_i}) \tag{3.5.4}$$

vanishes. (If $\chi = 1$, then we must also show that the pairing with $\lambda_{\sigma_{i_0},\mu^{-1}} u^{p(p^f-1)-\xi_{i_0}}$ vanishes.)

Since

$$\operatorname{dlog} E(X) = (X + X^p + X^{p^2} + \cdots) \operatorname{dlog} X$$

and $\operatorname{dlog}(\lambda u^n) = n \cdot u^{-1}$, the pairing (3.5.4) evaluates to

$$\operatorname{Tr}_{l\otimes_{\mathbb{F}_p}\overline{\mathbb{F}}_p/\overline{\mathbb{F}}_p} \operatorname{Res}\biggl(\sum_{m\geqslant 0} n'_j (\varphi\otimes 1)^m(\lambda_{\sigma'_j,\mu}) u^{n'_j p^m - 1} \cdot \lambda_{\sigma_i,\mu^{-1}} u^{-\xi_i}\biggr).$$

(Here $\varphi \otimes 1 : l \otimes \overline{\mathbb{F}}_p \to l \otimes \overline{\mathbb{F}}_p$ is the pth power map on l.)

This residue is given by the coefficient of u^{-1}, so we see that this pairing can be non-zero only when $\xi_i = p^m n'_j$ for some $m \geqslant 0$ (if $\chi = 1$, then we must also consider the possibility that $\xi_i - p(p^f - 1) = p^m n'_j$, but this is excluded by Lemma 3.6.6 below). If this holds, then the pairing evaluates to

$$n'_j \operatorname{Tr}_{l\otimes_{\mathbb{F}_p}\overline{\mathbb{F}}_p/\overline{\mathbb{F}}_p} (\varphi\otimes 1)^m(\lambda_{\sigma'_j,\mu}) \cdot \lambda_{\sigma_i,\mu^{-1}}.$$

Now, we have

$$(\varphi\otimes 1)^m(\lambda_{\sigma'_j,\mu}) \cdot \lambda_{\sigma_i,\mu^{-1}} = (\varphi\otimes 1)^m(\lambda_{\sigma'_j,\mu}\lambda_{\sigma_{i-m},\mu^{-1}})$$

which is non-zero if and only if $\sigma'_j = \sigma_{i-m}$, in which case its trace to $\overline{\mathbb{F}}_p$ is equal to $[l : k]$.

In conclusion, we have seen that in order for the pairing to be non-zero, we require:

(i) $\sigma'_j = \sigma_{i-m}$; and
(ii) $\xi_i = p^m n'_j$.

(In fact, although we do not need this stronger statement, we observe that the pairing is non-zero if and only if these conditions hold, because n'_j is always a unit by Lemma 3.6.1, while $[l : k]$ is prime to p.) By Proposition 3.6.7 below, these conditions imply that $j \in \mu(J)$, as required. □

Remark 3.5.5. It is clear that the method of the proof of Theorem 3.5.3 could be used to compare the bases of L_{BDJ} and L_{DDR} that we have been working with. We have checked that in suitably generic cases the bases are the same (up to scalars), but that in exceptional cases they may differ.

3.6 Combinatorics

Our main aim in this section is to prove Proposition 3.6.7, which was used in the proof of Theorem 3.5.3. We begin with some simple observations; the following three lemmas give us some control on the quantities ξ_i and n'_i which will be important in the proof of Proposition 3.6.7.

LEMMA 3.6.1. *The quantity n'_i is not divisible by p.*

Proof. This is automatic if $a_{i-1} \neq p$ because then $n'_i = n_{i-1} \equiv a_{i-1} \pmod p$. Assume that $a_{i-1} = p$, and write that $(a_{i-1}, a_{i-2}, \ldots, a_j) = (p, p-1, \ldots, p-1)$, with $a_{j-1} \neq p-1$. Now

$$n'_i := n_{j-1} - (p^f - 1) \equiv n_{j-1} + 1 \equiv a_{j-1} + 1 \pmod p.$$

However, since $a_{j-1} \neq p-1$ and lies in $[1, p]$, we have $a_{j-1} \not\equiv -1 \mod p$, and so $n'_i \not\equiv 0 \pmod p$. □

LEMMA 3.6.2. *If $i \in J$, then $0 < \xi_i < p^2(p^f - 1)/(p - 1)$.*

https://doi.org/10.1112/S0010437X17007254 Published online by Cambridge University Press

Proof. Since $i \in J$, we have

$$\xi_i = p^f r_i + (-1)^{i+1\notin J} p^{f-1} r_{i+1} + (-1)^{i+2\notin J} p^{f-2} r_{i+2} + \cdots + (-1)^{i-1\notin J} p r_{i-1}. \tag{3.6.3}$$

The upper bound is immediate, as we have $r_j \leqslant p$ for all j (and in the case that all r_j are equal to p, we are not allowing J^c to be empty). For the lower bound, if $r_i \geqslant 2$, then $\xi_i \geqslant 2p^f - (p^f + p^{f-1} + \cdots + p^2) > 0$, so we may assume that $r_i = 1$. Suppose that $J \neq \{i\}$, and let $x \geqslant 0$ be minimal so that $i + x + 1 \in J$. Since $r_i = 1$ and $i \in J$, it follows from the maximality condition on J that no initial segment of $(r_{i+1}, \ldots, r_{i+x})$ can be $(p-1, p-1, \ldots, p)$ (which also excludes the degenerate case consisting of a single initial p). Hence, either all the r_j for $j \in [i+1, i+x]$ are at most $p-1$, in which case

$$p^{f-1} r_{i+1} + \cdots + p^{f-x} r_{i+x} \leqslant (p^{f-1} + \cdots + p^{f-x})(p-1) = p^f - p^{f-x},$$

so that

$$\xi_i \geqslant p^{f-x} + p^{f-x-1} - (p^{f-x-2} + \cdots + p)p = p^{f-x} - p^{f-x-2} - \cdots - p^2 > 0,$$

or for some $y < x$ we have $r_{i+1}, \ldots, r_{i+y} = p-1$ and $r_{i+y+1} < p-1$, in which case

$$\begin{aligned} p^{f-1} r_{i+1} + \cdots + p^{f-x} r_{i+x} &\leqslant (p^{f-1} + \cdots + p^{f-y})(p-1) \\ &\quad + (p-2)p^{f-y-1} + p(p^{f-y-2} + \cdots p^{f-x}) \\ &= (p^{f-1} + \cdots + p^{f-x})(p-1) \\ &\quad - p^{f-y-1} + p^{f-y-2} + \cdots + p^{f-x} \\ &\leqslant (p^{f-1} + \cdots + p^{f-x})(p-1) \\ &= p^f - p^{f-x}, \end{aligned}$$

and one proceeds as above. Finally, if $J = \{i\}$, then arguing as above (and, again, using the maximality condition on J) we see (considering the two cases as above) that $\xi_i \geqslant p^f - (p^{f-1} + \cdots + p)(p-1) = p > 0$. □

LEMMA 3.6.4. *For any value of i, we have $(p^f - 1)/(p-1) \leqslant n_i < (p^f - 1) + (p^f - 1)/(p-1)$.*

Proof. This is immediate from the definition of n_i. □

Let $v_p(\xi_i)$ denote the p-adic valuation of ξ_i. The following lemma shows that ξ_i is in some sense a function of this valuation, and is crucial for our main argument.

LEMMA 3.6.5. *If $i \in J$, and if $m := v_p(\xi_i)$, then $m \geqslant 1$. If furthermore $m > 1$, then we have $\xi_i = p^m(n_{i-m} - (p^f - 1))$, while if $m = 1$, then either $\xi_i = p n_{i-1}$ or $\xi_i = p(n_{i-1} - (p^f - 1))$, depending on whether or not $\xi_i/p \geqslant (p^f - 1)/(p-1)$.*

Proof. Equation (3.6.3) shows that m is at least 1 if $i \in J$. From (3.3.4), we deduce that $\xi_i/p^m \equiv n_{i-m} \pmod{p^f - 1}$. By Lemma 3.6.2 we have

$$0 < \xi_i/p^m < p^{2-m}(p^f - 1)/(p-1),$$

so that if $m \geqslant 2$ it follows by Lemma 3.6.4 that

$$\xi_i/p^m < (p^f - 1)/(p-1) \leqslant n_{i-m} < (p^f - 1) + (p^f - 1)/(p-1).$$

Since $\xi_i > 0$ by Lemma 3.6.2, the congruence modulo $p^f - 1$ forces the equality $n_{i-m} - \xi_i/p^m = (p^f - 1)$. If $m = 1$, then we have

$$0 < \xi_i/p < (p^f - 1) + (p^f - 1)/(p - 1)$$

and the claim follows in the same way. □

The following simple lemma was used in the proof of Theorem 3.5.3 in the case $\chi = 1$.

Lemma 3.6.6. *Suppose that $\chi = 1$ and that $i \in J$. Then there are no solutions to the equation $\xi_i - p(p^f - 1) = p^m(p^f - 1)$, for any $m \geqslant 0$.*

Proof. Since $\chi = 1$, we have $n_j = p^f - 1$ for all j. From Lemma 3.6.5, we find that either $v_p(\xi_i) \geqslant 2$, in which case $\xi_i = 0$ (contradicting Lemma 3.6.2), or $v_p(\xi_i) = 1$, in which case either $\xi_i = 0$ or $\xi_i = p(p^f - 1)$. The first case again contradicts Lemma 3.6.2. The second case leads to the equation $0 = p^m(p^f - 1)$, which has no solutions, as required. □

We now prove our main combinatorial result.

Proposition 3.6.7. *Suppose that $i \in J$, and that for some integers j, m we have:*

(i) $\sigma'_j = \sigma_{i-m}$*; and*
(ii) $\xi_i = p^m n'_j$*;*

then $j \in \mu(J)$.

Proof. By Lemma 3.6.1, we must have $m = v_p(\xi_i)$. Suppose first that $m = 1$ and $\xi_i = pn_{i-1}$. We need to solve the equations $\sigma'_j = \sigma_{i-1}$ and $n'_j = n_{i-1}$.

If $a_{j-1} = p$, then we have $\sigma'_j = \sigma_{s-1}$ and $n'_j = n_{s-1} - (p^f - 1)$, where s is the greatest integer less than j for which $a_{s-1} \neq p - 1$. Since $\sigma'_j = \sigma_{i-1}$ by assumption, we find that $s = i$. However, then $n_{i-1} = n'_j = n_{i-1} - (p^f - 1)$, which is not possible.

Thus, $a_{j-1} \neq p$ and, hence, we have $\sigma'_j = \sigma_{j-1}$, so that $j = i$. We must show that $j = i \in \mu(J)$. By the definition of $\mu(J)$, this will be the case unless for some $s > i$ we have $i+1, \ldots, s \notin J$, and $(a_i, \ldots, a_{s-1}) = (p-1, \ldots, p-1, p)$. Suppose then that this holds; we must show that we cannot have $\xi_i = pn_{i-1}$ after all. Now, by definition and the assumption that $i+1, \ldots, s \notin J$, we have

$$\begin{aligned}\xi_i/p &= p^{f-1}r_i - p^{f-2}r_{i+1} - \cdots + (-1)^{s+1\notin J}p^{f+i-2-s}r_{s+1} + \cdots + (-1)^{i-1\notin J}r_{i-1}\\ &\leqslant p^f - (p^{f-2} + \cdots + p^{f+i-s-1}) + (p^{f+i-2-s} + \cdots + 1)p\\ &= p^f - (p^{f-2} + \cdots + p^{f+i-s}) + (p^{f+i-2-s} + \cdots + p)\end{aligned}$$

while

$$\begin{aligned}n_{i-1} &= p^{f-1}a_i + p^{f-2}a_{i+1} + \cdots + a_{i-1}\\ &\geqslant p^{f-1}(p-1) + \cdots + p^{f+i+1-s}(p-1) + p^{f+i-s}p + p^{f+i-1-s} + \cdots + 1\\ &= p^f + p^{f+i-1-s} + \cdots + 1,\end{aligned}$$

which gives the required contradiction.

Having disposed of the case that $m = 1$ and $\xi_i = pn_{i-1}$, it follows from Lemma 3.6.5 that we may assume that $\xi_i = p^m(n_{i-m} - (p^f - 1))$. We show first that we cannot have $a_{j-1} \neq p$. Indeed, if this occurs, then by definition we have $n'_j = n_{j-1}$ and $\sigma'_j = \sigma_{i-1}$, so that the equations we need to solve are $i-m=j-1$, and $n_{i-m}-(p^f-1)=n_{j-1}$, which are mutually inconsistent, since together they imply that $n_{j-1}-(p^f-1)=n_{j-1}$.

We are thus reduced to the case when $a_{j-1}=p$ and, by the definition of n'_j, we see (since $\sigma'_j=\sigma_{i-m}$) that $i-m$ must be congruent to the greatest integer i' less than $j-1$ with $a_{i'}\neq p-1$. Replacing i by something congruent to its modulo f, we may assume that $i-m=i'$, so that $a_{i-m}\neq p-1$, $a_{i-m+1}=\cdots=a_{j-2}=p-1$ and $a_{j-1}=p$. Again, we must show that this implies that $j\in\mu(J)$. By the definition of $\mu(J)$, this will be the case unless $i-m+1,\ldots,j-2,j-1,j\notin J$. Since we are assuming that $i\in J$, this implies, in particular, that j is contained in the interval $[i-m,i)$. We now show that this leads to a contradiction. Consider the equation $\xi_i/p^m=n_{i-m}-(p^f-1)$. From the definitions and the assumptions we are making, we have

$$\begin{aligned} n_{i-m} &= p^{f-1}a_{i-m+1}+\cdots+p^{f-x}a_{i-m+x}+\cdots+a_{i-m} \\ &= p^f+p^{f-m+i-j}a_j+\cdots+a_{i-m}, \end{aligned}$$

so that

$$\begin{aligned} n_{i-m}-(p^f-1) &= 1+p^{f-m+i-j}a_j+\cdots+a_{i-m} \\ &> p^{f-m+i-j}+p^{f-m+i-j-1}+\cdots+1. \end{aligned}$$

Thus,

$$\xi_i=p^m(n_{i-m}-(p^f-1))>p^{f+i-j}+p^{f+i-j-1}+\cdots+p^m. \tag{3.6.8}$$

Since $\xi_i\leqslant p^2(p^f-1)/(p-1)$ by Lemma 3.6.2, we conclude that, in particular,

$$(p^f-1)/(p-1)>\xi_i/p^2>p^{f+i-j-2}=p^{(f-1)+(i-j-1)},$$

which is only possible if $i=j+1$. Assume now that this is the case. Then we may rewrite (3.6.8) in the form

$$\xi_i=p^m(n_{i-m}-(p^f-1))>p^{f+1}+p^f+\cdots+p^m. \tag{3.6.9}$$

We also find that $i-m+1,\ldots,i-1\notin J$, so that, from the definition of ξ_i (and taking into account the fact that $i\in J$), we compute

$$\begin{aligned} \xi_i &= p^f r_i+\cdots+(-1)^{i-m\notin J}p^m r_{i-m}-(p^{m-1}r_{i-m+1}+\cdots+pr_{i-1}) \\ &\leqslant p^f r_i+\cdots+(-1)^{i-m\notin J}p^m r_{i-m} \\ &\leqslant (p^f+\cdots+p^m)p=p^{f+1}+p^f+\cdots+p^{m+1}. \end{aligned}$$

This contradicts (3.6.9), and completes the argument. □

ACKNOWLEDGEMENTS

We would all like to thank Fred Diamond for many helpful conversations over the last decade about the weight part of Serre's conjecture, and for his key role in formulating the various generalisations of it to Hilbert modular forms. The fourth author is particularly grateful for his support and guidance over the course of his graduate studies. We would also like to thank him for suggesting that the four of us write this joint paper. We are grateful to Ehud de Shalit for sending us a copy of his paper [Sha92], which led us to Schmid's explicit reciprocity law. We would also like to thank David Savitt for informing us of the forthcoming paper [Wan16] of Xiyuan Wang, and Victor Abrashkin for informing us of his paper [Abr97], which extends the results of [Sha92], and much as in the present paper relates these results to the Artin–Hasse exponential. Finally, we would like to thank the anonymous referee for their careful reading of the paper.

References

Abr97 V. A. Abrashkin, *The field of norms functor and the Brückner–Vostokov formula*, Math. Ann. **308** (1997), 5–19.

AJ12 V. Abrashkin and R. Jenni, *The field-of-norms functor and the Hilbert symbol for higher local fields*, J. Théor. Nombres Bordeaux **24** (2012), 1–39.

BDJ10 K. Buzzard, F. Diamond and F. Jarvis, *On Serre's conjecture for mod l Galois representations over totally real fields*, Duke Math. J. **155** (2010), 105–161.

CD11 S. Chang and F. Diamond, *Extensions of rank one* (ϕ, Γ)*-modules and crystalline representations*, Compositio Math. **147** (2011), 375–427.

DDR16 L. Dembele, F. Diamond and D. P. Roberts, *Serre weights and wild ramification in two-dimensional Galois representations*, Preprint (2016), arXiv:1603.07708 [math.NT].

DS15 F. Diamond and D. Savitt, *Serre weights for locally reducible two-dimensional Galois representations*, J. Inst. Math. Jussieu **14** (2015), 639–672.

GLS14 T. Gee, T. Liu and D. Savitt, *The Buzzard–Diamond–Jarvis conjecture for unitary groups*, J. Amer. Math. Soc. **27** (2014), 389–435.

GLS15 T. Gee, T. Liu and D. Savitt, *The weight part of Serre's conjecture for* GL(2), Forum Math. Pi **e2** (2015), 52pp.

Kis09 M. Kisin, *Moduli of finite flat group schemes, and modularity*, Ann. of Math. (2) **170** (2009), 1085–1180.

Lau88 F. Laubie, *Extensions de Lie et groupes d'automorphismes de corps locaux*, Compositio Math. **67** (1988), 165–189.

Mav16 L. Mavrides, *On wild ramification in reductions of two-dimensional crystalline Galois representations*, PhD thesis, KCL, 2016.

Sch36 H. L. Schmid, *Zyklische algebraische Funktionenkörper vom Grade* p^n *über endlichem Konstantenkörper der Charakteristik* p, J. Reine Angew. Math. **175** (1936), 108–123.

Ser79 J.-P. Serre, *Local fields*, in *Translated from the French by Marvin Jay Greenberg*, Graduate Texts in Mathematics, vol. 67 (Springer, New York, 1979), viii+241.

Sha92 E. de Shalit, *Artin–Schreier-Witt extensions as limits of Kummer–Lubin–Tate extensions, and the explicit reciprocity law*, in *The arithmetic of function fields (Columbus, OH, 1991)*, Mathematical Sciences Research Institute Publications, vol. 2 (Springer, Berlin, 1992), 413–420.

Wan16 X. Wang, 2016, in preparation.

Frank Calegari fcale@math.uchicago.edu
Department of Mathematics, University of Chicago, 5734 South University Avenue, Chicago, IL 60637, USA

Matthew Emerton emerton@math.uchicago.edu
Department of Mathematics, University of Chicago, 5734 South University Avenue, Chicago, IL 60637, USA

Toby Gee toby.gee@imperial.ac.uk
Department of Mathematics, Imperial College London, London SW7 2AZ, UK

Lambros Mavrides lambros.mavrides@kcl.ac.uk
Department of Mathematics, King's College London, London WC2R 2LS, UK