COMPOSITIO MATHEMATICA

Extensions of rank one (φ, Γ)-modules and crystalline representations

Seunghwan Chang and Fred Diamond

Compositio Math. **147** (2011), 375–427.

doi:10.1112/S0010437X1000504X

FOUNDATION COMPOSITIO MATHEMATICA

The London Mathematical Society

Compositio Math. 147 (2011) 375–427
doi:10.1112/S0010437X1000504X

Extensions of rank one (φ, Γ)-modules and crystalline representations

Seunghwan Chang and Fred Diamond

Abstract

Let K be a finite unramified extension of $\mathbf{Q}_p$. We parametrize the (φ, Γ)-modules corresponding to reducible two-dimensional $\overline{\mathbf{F}}_p$-representations of G_K and characterize those which have reducible crystalline lifts with certain Hodge–Tate weights.

Contents

Received 10 September 2009, accepted in final form 26 April 2010, published online 13 December 2010.
2000 Mathematics Subject Classification 11S25 (primary).
Keywords: p-adic representations, crystalline representations, (φ, Γ)-modules, Wach modules.

1. Introduction

Buzzard, Jarvis and one of the authors [BDJ10] have formulated a generalization of Serre's conjecture for mod p Galois representations over totally real fields unramified at p. To give a recipe for weights, certain distinguished subspaces of local Galois cohomology groups in characteristic p are defined in terms of the existence of 'crystalline lifts' to characteristic zero. More precisely, let K be a finite unramified extension of $\mathbf{Q}_p$ with residue field k, $\mathbf{F}$ a finite extension of $\mathbf{F}_p$ containing k, $\psi: G_K \to \mathbf{F}^\times$ a character, and denote by S the set of embeddings of k in $\mathbf{F}$. For each $J \subset S$, they define a subspace (or in certain cases two subspaces) of $H^1(G_K, \mathbf{F}(\psi))$, which we denote L_J (or $L_J^\pm$); with certain exceptions these subspaces have dimension $|J|$ (see Remark 7.7 below for the relation between our notation and that of [BDJ10]). The definition of these subspaces in terms of crystalline lifts is somewhat indirect, making it hard for example to compare the spaces L_J for different J. Viewing the specification of the weights in terms of a conjectural mod p Langlands correspondence as in [BDJ10, § 4], such a comparison provides information about possible local factors at primes over p of mod p automorphic representations (see [Bre09]).

The aim of this paper is to describe them more explicitly using Fontaine's theory of (φ, Γ)-modules. In particular, we prove that, if ψ is *generic*, as defined in § 5.2, then the subspaces are well-behaved with respect to J in the following sense.

Theorem 1.1. *If ψ is generic and $\psi|_{I_K} \neq \chi^{\pm 1}$ where χ is the* mod p *cyclotomic character, then* $L_J = \bigoplus_{\tau \in J} L_{\{\tau\}}$.

We remark that Theorem 1.1 has been proved independently by Breuil [Bre09, Proposition A.3] using different methods. We also treat the case where $\psi|_{I_K} = \chi^{\pm 1}$; see Theorem 7.8 below for the statement.

We also give a complete description of the spaces L_J (and $L_J^\pm$) in terms of (φ, Γ)-modules when K is quadratic, without the assumption that ψ is generic. In particular, we prove the following theorem, which exhibits cases where the spaces L_J are not well-behaved as in Theorem 1.1.

Theorem 1.2. *Suppose that $[K : \mathbf{Q}_p] = 2$ and that ψ is ramified. Writing $S = \{\tau, \tau'\}$, we have $L_{\{\tau\}} = L_{\{\tau'\}}$ if and only if $\psi|_{I_K} = \omega_2^i$ for some fundamental character ω_2 of niveau 2 and some integer $i \in \{1, \dots, p-1\}$.*

This is part of Theorem 7.12 below; see also Theorem 7.15 for the case when ψ is unramified.

The paper is organized as follows. In § 2 we review preliminary facts on p-adic representations and (φ, Γ)-modules, and set up the category of étale (φ, Γ)-modules (corresponding to $\mathbf{F}[G_K]$-modules) in which we will be working. In § 3 we give a parametrization of rank one objects in the category, and identify them as reductions of crystalline characters of G_K using results of Dousmanis [Dou08]. In § 4 we construct bases for the space of extensions of rank one objects. (In a different but related direction, see [Her98, Her01, Liu08] for computation of p-adic Galois cohomology via (φ, Γ)-modules.) In § 5 we introduce the notion of bounded extensions, motivated by the theory of Wach modules, which characterizes those (φ, Γ)-modules corresponding to crystalline representations (see [Ber02, Ber04b, Wac96, Wac97]), and use this to define subspaces $V_J^{(\pm)}$, which we compute in the generic and quadratic cases. In § 6 we treat certain exceptional cases excluded from §§ 4 and 5. In § 7 we relate the spaces $L_J^{(\pm)}$ and $V_J^{(\pm)}$ in the generic and quadratic cases and prove our main results. We remark that a difficulty arises from the fact that the integral Wach module functor is not right exact; to overcome this we derive sufficient conditions for exactness that may be of independent interest.

2. Generalities on p-adic representations

In this section we summarize (and expand a bit upon) basic facts on p-adic representations, crystalline representations, (φ, Γ)-modules and Wach modules. We will give references for details and proofs along the way. For an excellent general introduction to the theory, see [Ber04a].

Let p be a rational prime and fix an algebraic closure $\overline{\mathbf{Q}}_p$ of $\mathbf{Q}_p$. If K is a finite extension of $\mathbf{Q}_p$ contained in $\overline{\mathbf{Q}}_p$, G_K denotes the Galois group $\mathrm{Gal}(\overline{\mathbf{Q}}_p/K)$ and K_0 denotes the absolutely unramified subfield of K. Let $\chi : G_K \to \mathbf{Z}_p^\times$ be the cyclotomic character and let $\bar{\cdot} : \mathbf{Z}_p \to \mathbf{F}_p$ be the reduction modulo p, so that $\overline{\chi} = \bar{\cdot} \circ \chi : G_K \to \mathbf{F}_p^\times$ is the mod p cyclotomic character. We set $K_n = K(\mu_{p^n}) \subset \overline{\mathbf{Q}}_p$ for $n \geqslant 1$, and get a tower of fields

$$K = K_0 \subset K_1 \subset \cdots \subset K_n \subset \cdots \subset K_\infty \subset \overline{\mathbf{Q}}_p,$$

where $K_\infty = \bigcup_{n \geqslant 1} K_n$. We define H_K to be the kernel of χ, i.e., $H_K = \mathrm{Gal}(\overline{\mathbf{Q}}_p/K_\infty)$, and set $\Gamma_K = G_K/H_K = \mathrm{Gal}(K_\infty/K)$. In many cases where there is no possibility of confusion, we will simply write Γ for Γ_K, suppressing K. We set $\Gamma_n = \Gamma_{K,n} = \mathrm{Gal}(K_\infty/K_n)$ for $n \geqslant 1$.

2.1 Fontaine's rings

Here we give a summary of the constructions of some of the rings introduced by Fontaine that we will be using. See [CC98, Col99, Fon94a] for more details. Let $\mathbf{C}_p$ denote the p-adic completion of $\overline{\mathbf{Q}}_p$ and v_p the p-adic valuation normalized by $v_p(p) = 1$. The set

$$\widetilde{\mathbf{E}} = \varprojlim_{x \mapsto x^p} \mathbf{C}_p = \{x = (x^{(0)}, x^{(1)}, \ldots) \mid x^{(i)} \in \mathbf{C}_p, (x^{(i+1)})^p = x^{(i)}\},$$

together with the addition and the multiplication defined by

$$(x+y)^{(i)} = \lim_{j \to \infty} (x^{(i+j)} + y^{(i+j)})^{p^j} \quad \text{and} \quad (xy)^{(i)} = x^{(i)} y^{(i)},$$

is an algebraically closed field of characteristic p, complete for the valuation $v_{\mathbf{E}}$ defined by $v_{\mathbf{E}}(x) = v_p(x^{(0)})$. We endow $\widetilde{\mathbf{E}}$ a Frobenius φ and the action of $G_{\mathbf{Q}_p}$ by

$$\varphi((x^{(i)})) = ((x^{(i)})^p) \quad \text{and} \quad g((x^{(i)})) = (g(x^{(i)}))$$

if $g \in G_{\mathbf{Q}_p}$. We denote the ring of integers of $\widetilde{\mathbf{E}}$ by $\widetilde{\mathbf{E}}^+$; it is stable under the actions of φ and $G_{\mathbf{Q}_p}$. Let $\varepsilon = (1, \varepsilon^{(1)}, \ldots, \varepsilon^{(i)}, \ldots)$ be an element of $\widetilde{\mathbf{E}}$ such that $\varepsilon^{(1)} \neq 1$, so that $\varepsilon^{(i)}$ is a primitive p^ith root of unity for all $i \geqslant 1$. Then $v_{\mathbf{E}}(\varepsilon - 1) = p/(p-1)$ and $\mathbf{E}_{\mathbf{Q}_p}$ is defined to be the subfield $\mathbf{F}_p((\varepsilon - 1))$ of $\widetilde{\mathbf{E}}$. We define $\mathbf{E}$ to be the separable closure of $\mathbf{E}_{\mathbf{Q}_p}$ in $\widetilde{\mathbf{E}}$, and $\widetilde{\mathbf{E}}^+$ (respectively $\mathfrak{m}_{\mathbf{E}}$) to be the ring of integers (respectively the maximal ideal) of $\mathbf{E}^+$. The field $\mathbf{E}$ is stable under the action of $G_{\mathbf{Q}_p}$ and we have $\mathbf{E}^{H_{\mathbf{Q}_p}} = \mathbf{E}_{\mathbf{Q}_p}$. The theory of the field of norms shows that $\mathbf{E}_K := \mathbf{E}^{H_K}$ is a finite separable extension of $\mathbf{E}_{\mathbf{Q}_p}$ of degree $|H_{\mathbf{Q}_p}/H_K| = [K_\infty : \mathbf{Q}_p(\mu_{p^\infty})]$ and allows one to identify $\mathrm{Gal}(\mathbf{E}/\mathbf{E}_K)$ with H_K. The ring of integers of $\mathbf{E}_K$ is denoted by $\mathbf{E}_K^+$.

Let $\widetilde{\mathbf{A}} = W(\widetilde{\mathbf{E}})$ be the ring of Witt vectors with coefficients in $\widetilde{\mathbf{E}}$ and let $\widetilde{\mathbf{B}} = \widetilde{\mathbf{A}}[1/p] = \mathrm{Fr}(\widetilde{\mathbf{A}})$. Then $\widetilde{\mathbf{B}}$ is a complete discrete valuation field with ring of valuation $\widetilde{\mathbf{A}}$ and residue field $\widetilde{\mathbf{E}}$. If $x \in \widetilde{\mathbf{E}}$, $[x]$ denotes Teichmüller representative of x in $\widetilde{\mathbf{A}}$. Then every element of $\widetilde{\mathbf{A}}$ can be written uniquely in the form $\sum_{i \geqslant 0} p^i [x_i]$ and that of $\widetilde{\mathbf{B}}$ in the form $\sum_{i \gg \infty} p^i [x_i]$. We endow $\widetilde{\mathbf{A}}$ with the topology that makes the map $x \mapsto (x_i)_{i \in \mathbf{N}}$ a homeomorphism $\widetilde{\mathbf{A}} \to \widetilde{\mathbf{E}}^{\mathbf{N}}$, where $\widetilde{\mathbf{E}}^{\mathbf{N}}$ is endowed with the product topology ($\widetilde{\mathbf{E}}$ is endowed with the topology defined by the valuation $v_{\mathbf{E}}$). We endow $\widetilde{\mathbf{B}} = \bigcup_{i \in \mathbf{N}} p^{-i} \widetilde{\mathbf{A}}$ with the topology of inductive limit. The action of $G_{\mathbf{Q}_p}$ on $\widetilde{\mathbf{E}}$ induces continuous actions on $\widetilde{\mathbf{A}}$ and $\widetilde{\mathbf{B}}$ that commute with the Frobenius φ. Let $\pi = [\varepsilon] - 1$. Define $\mathbf{A}_{\mathbf{Q}_p}$

to be the closure of $\mathbf{Z}_p[\pi, \pi^{-1}]$ in $\widetilde{\mathbf{A}}$. Then

$$\mathbf{A}_{\mathbf{Q}_p} = \left\{ \sum_{i \in \mathbf{Z}} a_n \pi^i \,\middle|\, a_i \in \mathbf{Z}_p,\ a_i \to 0 \text{ as } i \to -\infty \right\}$$

and $\mathbf{A}_{\mathbf{Q}_p}$ is a complete discrete valuation ring with residue field $\mathbf{E}_{\mathbf{Q}_p}$. As

$$\varphi(\pi) = (1+\pi)^p - 1 \quad \text{and} \quad \gamma(\pi) = (1+\pi)^{\chi(g)} - 1 \quad \text{if } g \in G_{\mathbf{Q}_p},$$

the ring $\mathbf{A}_{\mathbf{Q}_p}$ and its field of fractions $\mathbf{B}_{\mathbf{Q}_p} = \mathbf{A}_{\mathbf{Q}_p}[1/p]$ are stable under φ and the action of $G_{\mathbf{Q}_p}$. Let $\mathbf{B}$ be the closure of the maximal unramified extension of $\mathbf{B}_{\mathbf{Q}_p}$ contained in $\widetilde{\mathbf{B}}$, and set $\mathbf{A} = \mathbf{B} \cap \widetilde{\mathbf{A}}$, so that we have $\mathbf{B} = \mathbf{A}[1/p]$. Then $\mathbf{A}$ is a complete discrete valuation ring with field of fractions $\mathbf{B}$ and residue field $\mathbf{E}$. The ring $\mathbf{A}$ and the field $\mathbf{B}$ are stable under φ and $G_{\mathbf{Q}_p}$. If K is a finite extension of $\mathbf{Q}_p$, we define $\mathbf{A}_K = \mathbf{A}^{H_K}$ and $\mathbf{B}_K = \mathbf{B}^{H_K}$, which makes $\mathbf{A}_K$ a complete discrete valuation ring with residue field $\mathbf{E}_K$ and the field of fractions $\mathbf{B}_K = \mathbf{A}_K[1/p]$. When $K = \mathbf{Q}_p$, the two definitions of $\mathbf{A}_K$ and $\mathbf{B}_K$ coincide. If F is a finite extension of K, then $\mathbf{B}_F$ is an unramified extension of $\mathbf{B}_K$ of degree $[F_\infty : K_\infty]$. If the extension F/K is Galois, then the extensions $\widetilde{\mathbf{B}}_F/\widetilde{\mathbf{B}}_K$ and $\mathbf{B}_F/\mathbf{B}_K$ are also Galois with Galois group

$$\mathrm{Gal}(\widetilde{\mathbf{B}}_F/\widetilde{\mathbf{B}}_K) = \mathrm{Gal}(\mathbf{B}_F/\mathbf{B}_K) = \mathrm{Gal}(\mathbf{E}_F/\mathbf{E}_K) = \mathrm{Gal}(F_\infty/K_\infty) = H_K/H_F.$$

In particular, if K is a finite unramified extension of $\mathbf{Q}_p$, we have

$$\mathbf{A}_K = \left\{ \sum_{n \in \mathbf{Z}} a_n \pi^n \,\middle|\, a_n \in \mathcal{O}_K, a_n \to 0 \text{ as } n \to -\infty \right\},$$

with φ acting as the Frobenius and Γ acting trivially on $\mathcal{O}_K$.

The homomorphism $\theta : \widetilde{\mathbf{A}}^+ \to \mathcal{O}_{\mathbf{C}_p}$, $\sum_{n \geqslant 0} p^n [x_n] \mapsto \sum_{n \geqslant 0} p^n x_n^{(0)}$ is surjective and its kernel is a principal ideal generated by $\omega = \pi/\varphi^{-1}(\pi)$. We extend θ to a homomorphism $\widetilde{\mathbf{B}}^+ = \widetilde{\mathbf{A}}^+[1/p] \to \mathbf{C}_p$ and we set $\mathbf{B}^+_{\mathrm{dR}}$ to be the ring $\varprojlim \widetilde{\mathbf{B}}^+/(\ker\theta)^n$. Then θ extends by continuity to a homomorphism $\mathbf{B}^+_{\mathrm{dR}} \to \mathbf{C}_p$. This makes $\mathbf{B}^+_{\mathrm{dR}}$ a discrete valuation ring with maximal ideal $\ker\theta$ and residue field $\mathbf{C}_p$. The action of $G_{\mathbf{Q}_p}$ on $\widetilde{\mathbf{B}}^+$ extends by continuity to a continuous action of $G_{\mathbf{Q}_p}$ on $\mathbf{B}^+_{\mathrm{dR}}$. The series $\log[\varepsilon] = \sum_{n \geqslant 1} (-1)^{n-1} \pi^n/n$ converges in $\mathbf{B}^+_{\mathrm{dR}}$ to an element t, which is a generator of $\ker\theta$ on which $\sigma \in G_{\mathbf{Q}_p}$ act via the formula $\sigma(t) = \chi(\sigma)t$. We set $\mathbf{B}_{\mathrm{dR}} = \mathbf{B}^+_{\mathrm{dR}}[t^{-1}] = \mathrm{Fr}\,\mathbf{B}^+_{\mathrm{dR}}$, and $\mathbf{B}_{\mathrm{dR}}$ comes with a decreasing, separated and exhaustive filtration $\mathrm{Fil}^i\mathbf{B}_{\mathrm{dR}} := t^i \mathbf{B}^+_{\mathrm{dR}}$ for $i \in \mathbf{Z}$. Let $\mathbf{A}_{\mathrm{cris}} = \{x = \sum_{n \geqslant 0} a_n(\omega^n/n!) \in \mathbf{B}^+_{\mathrm{dR}} \mid a_n \in \widetilde{\mathbf{A}}^+, a_n \to 0\}$. Then $\mathbf{B}^+_{\mathrm{cris}} = \mathbf{A}_{\mathrm{cris}}[1/p]$ is a subring of $\mathbf{B}^+_{\mathrm{dR}}$ stable by $G_{\mathbf{Q}_p}$ and contains t, and the action of φ on $\widetilde{\mathbf{B}}^+$ extends by continuity to an action of $\mathbf{B}^+_{\mathrm{cris}}$. We have $\varphi(t) = pt$ and we define $\mathbf{B}_{\mathrm{cris}}$ to be the subring $\mathbf{B}^+_{\mathrm{cris}}[1/t]$ of $\mathbf{B}_{\mathrm{dR}}$, and define the filtration $\mathrm{Fil}^i\mathbf{B}_{\mathrm{cris}} := \mathrm{Fil}^i\mathbf{B}_{\mathrm{dR}} \cap \mathbf{B}_{\mathrm{cris}}$.

2.2 Crystalline representations

Let K be a finite extension of $\mathbf{Q}_p$, and let K_0 denote its maximal absolutely unramified subfield.

Definition 2.1. A *p-adic representation of G_K* is a finite dimensional $\mathbf{Q}_p$-vector space together with a linear and continuous action of G_K. A *$\mathbf{Z}_p$-representation of G_K* is a $\mathbf{Z}_p$-module of finite type with a $\mathbf{Z}_p$-linear and continuous action of G_K. A *mod p representation of G_K* is a finite dimensional $\mathbf{F}_p$-vector space with a linear and continuous action of G_K.

Remark 2.2. A $\mathbf{Z}_p$-representation T of G_K that is torsion-free over $\mathbf{Z}_p$ is naturally identified with a (*G_K-stable*) *lattice* of the p-adic representation $V := \mathbf{Q}_p \otimes_{\mathbf{Z}_p} T$ of G_K.

If B is a topological $\mathbf{Q}_p$-algebra endowed with a continuous action of G_K and if V is a p-adic representation of G_K, we define $\mathbf{D}_B(V) := (B \otimes_{\mathbf{Q}_p} V)^{G_K}$, which is naturally a module over B^{G_K}. If, in addition, B is G_K-regular (i.e., B is a domain, $(\mathrm{Fr}\, B)^{G_K} = B^{G_K}$, and every $b \in B - \{0\}$ such that $\mathbf{Q}_p b$ is stable under G_K-action is a unit), then the map

$$\alpha_V : B \otimes_{B^{G_K}} \mathbf{D}_B(V) \to B \otimes_{\mathbf{Q}_p} V$$

induced by the inclusion $D_B(V) \to B \oplus_{Q_p} V$ is an injection (see [Fon94b, § 1.3]). In particular, we have

$$\dim_{B^{G_K}} \mathbf{D}_B(V) \leqslant \dim_{\mathbf{Q}_p} V.$$

(If B is G_K-regular, B^{G_K} is forced to be a field.)

Definition 2.3. If B is G_K-regular, we say that a p-adic representation V of G_K is B*-admissible* if $\dim_{B^{G_K}} \mathbf{D}_B(V) = \dim_{\mathbf{Q}_p} V$. We say that V is *crystalline* if it is $\mathbf{B}_{\mathrm{cris}}$-admissible and that V is *de Rham* if $\mathbf{B}_{\mathrm{dR}}$-admissible.

Remark 2.4. We have the following equivalent conditions (cf. [Fon94b, § 1.4]):

(i) $\dim_{B^{G_K}} \mathbf{D}_B(V) = \dim_{\mathbf{Q}_p} V$;

(ii) α_V is an isomorphism; and

(iii) $B \otimes_{\mathbf{Q}_p} V \simeq B^{\dim_{\mathbf{Q}_p} V}$ as $B[G_K]$-modules.

If V is a p-adic representation of G_K, $\mathbf{D}_{\mathrm{dR}}(V) := (\mathbf{B}_{\mathrm{dR}} \otimes_{\mathbf{Q}_p} V)^{G_K}$ is naturally a filtered K-vector space. More precisely, it is a finite dimensional K-vector space with a decreasing, separated and exhaustive filtration $\mathrm{Fil}^i \mathbf{D}_{\mathrm{dR}}(V) := (\mathrm{Fil}^i \mathbf{B}_{\mathrm{dR}} \otimes_{\mathbf{Q}_p} V)^{G_K}$ of K-subspaces for $i \in \mathbf{Z}$. If V is de Rham, a *Hodge–Tate weight* of V is defined to be an integer $h \in \mathbf{Z}$ such that $\mathrm{Fil}^h \mathbf{D}_{\mathrm{dR}}(V) \neq \mathrm{Fil}^{h+1} \mathbf{D}_{\mathrm{dR}}(V)$ with multiplicity $\dim_K \mathrm{Fil}^h \mathbf{D}_{\mathrm{dR}}(V)/\mathrm{Fil}^{h+1} \mathbf{D}_{\mathrm{dR}}(V)$. So there are $\dim_{\mathbf{Q}_p} V$ Hodge–Tate weights of V counting multiplicities. We remark that this differs from the more standard convention (e.g., [Ber04a]) of defining $-h$ to be a Hodge–Tate weight of V for h as above.

Definition 2.5. A *filtered φ-module over K* is a finite dimensional K_0-vector space D together with a σ-semilinear bijection $\varphi : D \to D$ and a $\mathbf{Z}$-indexed filtration on $D_K := D \otimes_{K_0} K$ of K-subspaces that is decreasing, separated and exhaustive.

If V is a p-adic representation of G_K, then $\mathbf{D}_{\mathrm{cris}}(V) := (\mathbf{B}_{\mathrm{cris}} \otimes_{\mathbf{Q}_p} V)^{G_K}$ is a filtered φ-module over K. More precisely, the Frobenius on $\mathbf{B}_{\mathrm{cris}}$ induces a Frobenius map $\varphi : \mathbf{D}_{\mathrm{cris}}(V) \to \mathbf{D}_{\mathrm{cris}}(V)$ and the filtration on $\mathbf{B}_{\mathrm{dR}}$ induces a filtration $\mathrm{Fil}^i \mathbf{D}_{\mathrm{cris}}(V) := D_K \cap (\mathrm{Fil}^i \mathbf{B}_{\mathrm{dR}} \otimes_{\mathbf{Q}_p} V)^{G_K}$ on $\mathbf{D}_{\mathrm{cris}}(V)$. Moreover, $\mathbf{D}_{\mathrm{cris}}(V)$ has finite dimension over K_0 and φ is bijective on $\mathbf{D}_{\mathrm{cris}}(V)$. We get a functor

$$\mathbf{D}_{\mathrm{cris}} : \mathrm{Rep}_{\mathbf{Q}_p} G_K \to \mathrm{MF}_K^{\varphi}$$

from the category of p-adic representations of G_K to the category of filtered φ-modules over K.

If D is a filtered φ-module over K of finite dimension $d \geqslant 1$, then $\wedge^d D$ is a filtered φ-module of dimension one. If $e \in \wedge^d_{K_0} D - \{0\}$ and $\varphi(e) = \lambda e$ then $\mathrm{val}(\lambda)$ is independent of choice of e and we define $t_N(D) := v_p(\lambda)$. Also, we define $t_H(D) = t_H(D_K)$ to be the largest integer such that $\mathrm{Fil}^{t_H(D)}(\wedge^d_K D_K)$ is non-zero, i.e. $\mathrm{Fil}^i(\wedge^d_K D_K) = \wedge^d_K D_K$ for $i \leqslant t_H(D)$ and $\mathrm{Fil}^i(\wedge^d_K D_K) = 0$ for $i > t_H(D)$.

Definition 2.6. Let D be a filtered φ-module over K. We say that D is *weakly admissible* if $t_H(D) = t_N(D)$ and $t_H(D') \leqslant t_N(D')$ for every subobject D' of D. We say that D is *admissible* if $D \simeq \mathbf{D}_{\mathrm{cris}}(V)$ for some p-adic representation V of dimension $\dim_{K_0} D$.

https://doi.org/10.1112/S0010437X1000504X Published online by Cambridge University Press

One can show that, if V is a crystalline representation of G_K, then $\mathbf{D}_{\text{cris}}(V)$ is weakly admissible. The converse was conjectured by Fontaine, and proved by Colmez and Fontaine.

Theorem 2.7 [CF00]. *Every weakly admissible filtered φ-module over K is admissible.*

In sum, we have an equivalence of categories

$$\mathbf{D}_{\text{cris}} : \mathrm{Rep}^{\text{cris}}_{\mathbf{Q}_p} G_K \to \mathrm{MF}_K^{\varphi,\text{w.a.}}$$

between crystalline representations of G_K and weakly admissible filtered φ-modules over K with a quasi-inverse given by $\mathbf{V}_{\text{cris}}(\cdot) := (\mathrm{Fil}^0(\cdot))^{\varphi=1}$.

2.3 (φ, Γ)-modules

Definition 2.8. A (φ, Γ)-*module over* $\mathbf{A}_K$ (respectively $\mathbf{B}_K$, $\mathbf{E}_K$) is an $\mathbf{A}_K$-module of finite type (respectively finite dimensional vector space over $\mathbf{B}_K$, $\mathbf{E}_K$) endowed with a semilinear and continuous action of Γ_K and with a semilinear map φ that commutes with the action of Γ_K. We say that a (φ, Γ)-module M over $\mathbf{A}_K$ (respectively $\mathbf{E}_K$) is *étale* if $\varphi(M)$ generates M over $\mathbf{A}_K$ (respectively $\mathbf{E}_K$). A (φ, Γ)-module M over $\mathbf{B}_K$ is *étale* if M contains an $\mathbf{A}_K$-lattice that is stable under φ and is étale.

Remark 2.9. We identify a (étale) (φ, Γ)-module over $\mathbf{A}_K$ killed by p with the corresponding (étale) (φ, Γ)-modules over $\mathbf{E}_K$.

If T is a $\mathbf{Z}_p$-representation of G_K, we define $\mathbf{D}(T) = (\mathbf{A} \otimes_{\mathbf{Z}_p} T)^{H_K}$. Then $\mathbf{D}(T)$ is naturally a module over $\mathbf{A}_K$ of finite type. The Frobenius φ on $\mathbf{A}$ induces a Frobenius map $\varphi : \mathbf{D}(T) \to \mathbf{D}(T)$ and the residual action of Γ_K on $\mathbf{D}(T)$ commutes with φ. One can also check that $\mathbf{D}(T)$ is étale over $\mathbf{A}_K$. Conversely, if M is an étale (φ, Γ)-module over $\mathbf{A}_K$ we define $\mathbf{T}(M) = (\mathbf{A} \otimes_{\mathbf{A}_K} M)^{\varphi=1}$, which is a $\mathbf{Z}_p$-representation of G_K.

Theorem 2.10 [Fon90]. *The functor $T \mapsto \mathbf{D}(T)$ defines an equivalence of categories*

$$\mathbf{D} : \mathrm{Rep}_{\mathbf{Z}_p} G_K \to \mathrm{M}^{\varphi,\Gamma,\text{et}}_{\mathbf{A}_K}$$

between $\mathbf{Z}_p$-representations and étale (φ, Γ)-modules over $\mathbf{A}_K$ with $\mathbf{T}$ as a quasi-inverse. It induces, by inverting p, an equivalence of categories

$$\mathbf{D} : \mathrm{Rep}_{\mathbf{Q}_p} G_K \to \mathrm{M}^{\varphi,\Gamma,\text{et}}_{\mathbf{B}_K}$$

between p-adic representations and étale (φ, Γ)-modules over $\mathbf{B}_K$ with

$$M \mapsto \mathbf{V}(M) := (\mathbf{B} \otimes_{\mathbf{B}_K} D)^{\varphi=1}$$

as a quasi-inverse. Moreover, if T is a $\mathbf{Z}_p$-representation and V a p-adic representation of G_K, then

$$\mathrm{rank}_{\mathbf{Z}_p} T = \mathrm{rank}_{\mathbf{A}_K} \mathbf{D}(T),$$
$$\dim_{\mathbf{Q}_p} V = \dim_{\mathbf{B}_K} \mathbf{D}(V).$$

When we restrict the equivalence to the p-torsion objects we get the following corollary.

Corollary 2.11. *The functor $T \mapsto \mathbf{D}(T)$ defines an equivalence of categories between* $\bmod p$ *representations of G_K and étale (φ, Γ_K)-modules over $\mathbf{E}_K$.*

https://doi.org/10.1112/S0010437X1000504X Published online by Cambridge University Press

Now we introduce coefficients to representations of G_K and (φ,Γ)-modules to extend Theorem 2.10 and Corollary 2.11. We assume that K is absolutely unramified (of degree f over $\mathbf{Q}_p$) and let F be a finite extension of $\mathbf{Q}_p$ with ring of integers $\mathcal{O}_F$, uniformizer ϖ_F and residue field $\mathbf{F}$. Consider the ring $\mathbf{A}_{K,F} := \mathcal{O}_F \otimes_{\mathbf{Z}_p} \mathbf{A}_K$ with the actions of φ and Γ_K extended to $\mathbf{A}_{K,F}$ by linearity, i.e., φ acts as $1\otimes\varphi$ and $\gamma\in\Gamma_K$ as $1\otimes\gamma$. We assume there is an embedding $\tau_0 : K \hookrightarrow F$, which we fix once and for all, and put $\tau_i = \tau_0\circ\varphi^i$, where φ is the Frobenius on K. We denote by S the set of all embeddings $K\hookrightarrow F$ and fix the identification $S = \mathbf{Z}/f\mathbf{Z}$ via the map $\tau_i \mapsto i$. We can then identify $\mathbf{A}_{K,F}$ with $\mathbf{A}^S_{\mathbf{Q}_p,F}$ via the isomorphism defined by $a\otimes b\pi^n \mapsto (a\tau(b)\otimes\pi^n)_\tau$. Note that

$$\mathbf{A}_{\mathbf{Q}_p,F} = \left\{ \sum_{n\in\mathbf{Z}} a_n\pi^n \;\middle|\; a_n\in\mathcal{O}_F,\, a_n\to 0 \text{ as } n\to-\infty \right\},$$

and the actions of φ and $\gamma\in\Gamma_K$ on $\mathbf{A}^S_{\mathbf{Q}_p,F}$ become

$$\varphi(g_0(\pi), g_1(\pi),\dots,g_{f-1}(\pi)) = (g_1(\varphi(\pi)),\dots,g_{f-1}(\varphi(\pi)), g_0(\varphi(\pi))),$$
$$\gamma(g_0(\pi), g_1(\pi),\dots,g_{f-1}(\pi)) = (g_0(\gamma(\pi)), g_1(\gamma(\pi)),\dots,g_{f-1}(\gamma(\pi))).$$

We similarly define $\mathbf{B}_{K,F} = F\otimes_{\mathbf{Q}_p}\mathbf{B}_K$ and $\mathbf{E}_{K,F} = \mathbf{F}\otimes_{\mathbf{F}_p}\mathbf{E}_K$ and endow them with actions of φ and Γ. Note that $\mathbf{B}_{K,F} = \mathbf{A}_{K,F}[1/p]$ and $\mathbf{E}_{K,F} = \mathbf{A}_{K,F}/\varpi_F\mathbf{A}_{K,F}$. Again identifying S with the set of embeddings $k\to\mathbf{F}$, we have the isomorphism $\mathbf{E}_{K,F} = \mathbf{F}((\pi))^S$ with the actions of φ and Γ_K given by the same formulas as above.

DEFINITION 2.12. An $\mathcal{O}_F$*-representation* of G_K is a finitely generated $\mathcal{O}_F$-module with a continuous $\mathcal{O}_F$-linear action of G_K. A (φ,Γ_K)*-module over* $\mathbf{A}_{K,F}$ is a finitely generated $\mathbf{A}_{K,F}$-module M endowed with commuting semilinear actions of Γ_K and φ. A (φ,Γ_K)-module M over $\mathbf{A}_{K,F}$ is *étale* if $\varphi(M)$ generates M over $\mathbf{A}_K$, or equivalently over $\mathbf{A}_{K,F}$.

We write $\mathrm{Rep}_{\mathcal{O}_F}G_K$ for the category of $\mathcal{O}_F$-representations of G_K, and $\mathrm{M}^{\varphi,\Gamma,\mathrm{et}}_{\mathbf{A}_{K,F}}$ for that of étale (φ,Γ_K)-modules over $\mathbf{A}_{K,F}$. We use analogous definitions and notation for representations of G_K over F and $\mathbf{F}$, and (φ,Γ_K)-modules over $\mathbf{B}_{K,F}$ and $\mathbf{E}_{K,F}$. The category of étale (φ,Γ_K)-modules over $\mathbf{E}_{K,F}$ is the main category we will be working in. Theorem 2.10 and Corollary 2.11 immediately yield the following corollary.

COROLLARY 2.13. *The functor* $\mathbf{D}$ *induces equivalences of categories* $\mathrm{Rep}_{\mathcal{O}_F}G_K\to\mathrm{M}^{\varphi,\Gamma,\mathrm{et}}_{\mathbf{A}_{K,F}}$, $\mathrm{Rep}_F G_K\to\mathrm{M}^{\varphi,\Gamma,\mathrm{et}}_{\mathbf{B}_{K,F}}$ *and* $\mathrm{Rep}_{\mathbf{F}}G_K\to\mathrm{M}^{\varphi,\Gamma,\mathrm{et}}_{\mathbf{E}_{K,F}}$.

For each embedding $\tau : K\hookrightarrow\mathbf{F}$, let $e_\tau : \mathbf{A}_{K,F}\to\mathbf{A}_{\mathbf{Q}_p,F}$ denote the projection to the τ-component, defined by $a\otimes b\pi^i\mapsto a\tau(b)\pi^i$. If M is a (φ,Γ)-module over $\mathbf{A}_{K,F}$, then $M = \prod_{\tau\in S} e_\tau M$, each $e_\tau M$ inherits an action of Γ, and φ induces semilinear morphisms $e_{\tau\circ\varphi}M\to e_\tau M$ compatible with the action of Γ. We use the same notation for (φ,Γ)-modules over $\mathbf{B}_{K,F}$ and $\mathbf{E}_{K,F}$.

LEMMA 2.14. *If* M *is an étale* (φ,Γ)*-module over* $\mathbf{A}_{K,F}$*, then the following are equivalent:*

(i) $\mathbf{T}(M)$ *is free over* $\mathcal{O}_F$ *of rank* d*;*

(ii) M *is free over* $\mathbf{A}_K$ *of rank* $d[F:\mathbf{Q}_p]$*; and*

(iii) M *is free over* $\mathbf{A}_{K,F}$ *of rank* d*.*

If M *is an étale* (φ,Γ)*-module over* $\mathbf{B}_{K,F}$ *(respectively* $\mathbf{E}_{K,F}$*), then* M *is free over* $\mathbf{B}_{K,F}$ *(respectively* $\mathbf{E}_{K,F}$*) of rank* $\dim_F\mathbf{T}(M)$ *(respectively* $\dim_{\mathbf{F}}\mathbf{T}(M)$*).*

Proof. Suppose that M is étale over $\mathbf{A}_{K,F}$. Then multiplication by p is injective on M if and only if it is injective on $\mathbf{T}(M)$. Thus M is torsion-free, and hence free, over $\mathbf{A}_K$ if and only if $\mathbf{T}(M)$ is free over $\mathcal{O}_F$. Since the $\mathbf{A}_K$-rank of M coincides with the $\mathbf{Z}_p$-rank of $\mathbf{T}(M)$, the first two conditions are equivalent.

If M is free of rank d over $\mathbf{A}_{K,F}$, then it is clearly free of rank $d[F:\mathbf{Q}_p]$ over $\mathbf{A}_K$. Conversely suppose that M is free over $\mathbf{A}_K$. Then each $e_\tau M$ is torsion-free, hence free, over the discrete valuation ring $\mathbf{A}_{\mathbf{Q}_p,F}$. We need only show that each $e_\tau M$ has the same rank. Since M is étale, the maps

$$e_{\tau\circ\varphi}M \otimes_{\mathbf{A}_{\mathbf{Q}_p,F},\varphi} \mathbf{A}_{\mathbf{Q}_p,F} \to e_\tau M$$

are surjective, so we have $\operatorname{rank}(e_{\tau_i}M) \leqslant \operatorname{rank}(e_{\tau_{i+1}}M)$ for all $i \in \mathbf{Z}/f\mathbf{Z}$. The equivalence between the last two conditions follows.

The assertions for étale (φ,Γ)-modules over $\mathbf{B}_{K,F}$ and $\mathbf{E}_{K,F}$ are similar, but simpler since $\mathbf{B}_K$ and $\mathbf{E}_K$ are fields. □

Finally, there are tensor products and exact sequences in the various categories of étale (φ,Γ)-modules, compatible via $\mathbf{D}$ with tensor products and exact sequences in the corresponding categories of representations of G_K.

2.4 Wach modules

It is very useful to be able to characterize whether a p-adic representation is crystalline in terms of the corresponding (φ,Γ)-module. This can be done via the theory of Wach modules if K is unramified over $\mathbf{Q}_p$.

Let $\mathbf{A}^+ = \mathbf{A} \cap \widetilde{\mathbf{A}}^+ = \mathbf{B} \cap \widetilde{\mathbf{A}}^+$ and $\mathbf{B}^+ = \mathbf{A}^+[1/p]$. If K is a finite unramified extension of $\mathbf{Q}_p$, we set $\mathbf{A}_K^+ = (\mathbf{A}^+)^{H_K} = \mathcal{O}_K[[\pi]] \subset \mathbf{A}_K$ and $\mathbf{B}_K^+ = (\mathbf{B}^+)^{H_K} = \mathbf{A}_K^+[p^{-1}] \subset \mathbf{B}_K$.

Definition 2.15. Let K be a finite unramified extension of $\mathbf{Q}_p$. We say that a $\mathbf{Z}_p$-representation T (respectively p-adic representation V) of G_K is *of finite height* if there exists a basis of $\mathbf{D}(T)$ (respectively $\mathbf{D}(V)$) such that the matrices describing the action of φ and the action of Γ_K are defined over $\mathbf{A}_K^+$ (respectively $\mathbf{B}_K^+$).

Colmez [Col99] proved that every crystalline representation is necessarily of finite height. The converse is not true in general and there are representations of finite height that are not crystalline. However, Wach [Wac96, Wac97] proved that finiteness of height together with a certain condition (existence of a certain $\mathbf{A}_K^+$-submodule of the corresponding (φ,Γ)-module) implies crystallinity. Berger [Ber02, Ber04b] then refined the results of Wach and Colmez as summarized below.

Definition 2.16. Suppose $a \leqslant b \in \mathbf{Z}$. A *Wach module* over $\mathbf{A}_K^+$ (respectively $\mathbf{B}_K^+$) with weights in $[a,b]$ is a free $\mathbf{A}_K^+$-module (respectively $\mathbf{B}_K^+$-module) N of finite rank, endowed with an action of Γ_K that becomes trivial modulo π, and also with a Frobenius map $\varphi: N[1/\pi] \to N[1/\pi]$ that commutes with the action of Γ_K and such that $\varphi(\pi^{-a}N) \subset \pi^{-a}N$ and $\pi^{-a}N/\varphi(\pi^{-a}N)$ is killed by q^{b-a}, where we define $q := \varphi(\pi)/\pi$.

Theorem 2.17 [Ber04b]. (i) *A p-adic representation V is crystalline with Hodge–Tate weights in $[a,b]$ if and only if $\mathbf{D}(V)$ contains a Wach module $\mathbf{N}(V)$ of rank $\dim_{\mathbf{Q}_p} V$ with weights in $[a,b]$. The association $V \mapsto \mathbf{N}(V)$ induces an equivalence of categories between crystalline representations of G_K and Wach modules over $\mathbf{B}_K^+$, compatible with tensor products, duality and exact sequences.*

https://doi.org/10.1112/S0010437X1000504X Published online by Cambridge University Press

(ii) *For a given crystalline representation V, the map $T \mapsto \mathbf{N}(T) := \mathbf{N}(V) \cap \mathbf{D}(T)$ induces a bijection between G_K-stable lattices of V and Wach modules over $\mathbf{A}_K^+$ that are $\mathbf{A}_K^+$-lattices contained in $\mathbf{N}(V)$. Moreover $\mathbf{D}(T) = \mathbf{A}_K \otimes_{\mathbf{A}_K^+} \mathbf{N}(T)$.*

(iii) *If V is a crystalline representation of G_K, and if we endow $\mathbf{N}(V)$ with the filtration $\mathrm{Fil}^i\mathbf{N}(V) = \{x \in \mathbf{N}(V) \mid \varphi(x) \in q^i\mathbf{N}(V)\}$, then we have an isomorphism $\mathbf{D}_{\mathrm{cris}}(V) \to \mathbf{N}(V)/\pi\mathbf{N}(V)$ of filtered φ-modules (with the induced filtration on $\mathbf{N}(V)/\pi\mathbf{N}(V)$).*

Remark 2.18. If $0 \to V_1 \to V \to V_2 \to 0$ is an exact sequence of crystalline representations of G_K, then

$$0 \to \mathbf{N}(V_1) \to \mathbf{N}(V) \to \mathbf{N}(V_2) \to 0$$

is an exact sequence of $\mathbf{B}_K^+$-modules. However, $\mathbf{N}$ does not define an exact functor from G_K-stable lattices to $\mathbf{A}_K^+$-modules; indeed it fails to be right exact. We return to this point in more detail in § 7.

Again by introducing an action of F to the categories, we get an analogous equivalence of categories between crystalline F-representations and Wach modules over $\mathbf{B}_{K,F}^+ := F \otimes_{\mathbf{Q}_p} \mathbf{B}_K^+$. Here, by a crystalline F-representation we mean a finite dimensional F-vector space with a continuous action of G_K which is crystalline considered as a $\mathbf{Q}_p$-linear representation (i.e., forgetting F-structure). Similarly, for a fixed crystalline F-representation of G_K, we have a corresponding equivalence of categories between G_K-stable $\mathcal{O}_F$-lattices and Wach modules over $\mathbf{A}_{K,F}^+ := \mathcal{O}_F \otimes_{\mathbf{Z}_p} \mathbf{A}_K^+$.

Corollary 2.19. *Let $k \in \mathbf{Z}_{\geqslant 0}$. An F-representation V of G_K is crystalline with Hodge–Tate weights in $[0, k]$ (i.e., positive crystalline) if and only if there exists a $\mathbf{B}_{K,F}^+$-module N free of rank $d := \dim_F(V)$ contained in $\mathbf{D}(V)$ such that:*

(i) *the Γ-action preserves N and is trivial on $N/\pi N$; and*

(ii) *$\varphi(N) \subset N$ and $N/\varphi^*(N)$ is killed by q^k.*

Moreover, if N is given a filtration by

$$\mathrm{Fil}^i(N) := \{x \in N \mid \varphi(x) \in q^i N\}$$

for $i \geqslant 0$, then we have an isomorphism

$$\mathbf{D}_{\mathrm{cris}}(V) \simeq N/\pi N$$

of filtered φ-modules over $F \otimes_{\mathbf{Q}_p} K$, where $N/\pi N$ is endowed with induced filtration.

A standard argument (cf. Lemma 2.14) shows that an F-representation V of G_K is crystalline if and only if the filtered φ-module $\mathbf{D}_{\mathrm{cris}}(V) = (\mathbf{B}_{\mathrm{cris}} \otimes_{\mathbf{Q}_p} V)^{G_K}$ is free of rank $\dim_F V$ over $F \otimes_{\mathbf{Q}_p} K$. We have a decomposition $\mathbf{D}_{\mathrm{cris}}(V) = \bigoplus_{\tau : K \hookrightarrow F} e_\tau \mathbf{D}_{\mathrm{cris}}(V)$, where $e_\tau \mathbf{D}_{\mathrm{cris}}(V)$ is the filtered F-vector space $\mathbf{D}_{\mathrm{cris}}(V) \otimes_{K \otimes_{\mathbf{Q}_p} F, e_\tau} F$ with the filtration given by $\mathrm{Fil}^i e_\tau \mathbf{D}_{\mathrm{cris}}(V) := e_\tau \mathrm{Fil}^i \mathbf{D}_{\mathrm{cris}}(V)$. A *labeled Hodge–Tate weight* with respect to the embedding $\tau : K \hookrightarrow F$ is an integer $h \in \mathbf{Z}$ such that $\mathrm{Fil}^h e_\tau \mathbf{D}_{\mathrm{cris}}(V) \neq \mathrm{Fil}^{h+1} e_\tau \mathbf{D}_{\mathrm{cris}}(V)$, counted with multiplicity

$$\dim_F \mathrm{Fil}^h e_\tau \mathbf{D}_{\mathrm{cris}}(V)/\mathrm{Fil}^{h+1} e_\tau \mathbf{D}_{\mathrm{cris}}(V).$$

Lemma 2.20. *If N is a Wach module over $\mathbf{A}_{K,F}^+$ (respectively $\mathbf{B}_{K,F}^+$), then N is free over $\mathbf{A}_{K,F}^+$ (respectively $\mathbf{B}_{K,F}^+$).*

https://doi.org/10.1112/S0010437X1000504X Published online by Cambridge University Press

Proof. We just give the proof for Wach modules over $\mathbf{A}^+_{K,F}$; the case of $\mathbf{B}^+_{K,F}$ can be deduced from this or proved similarly.

Let T denote the $\mathcal{O}_F$-representation corresponding to T, and let d denote its rank. The $\mathcal{O}_F \otimes_{\mathbf{Z}_p} \mathcal{O}_K$-module $N/\pi N$ is a lattice in $D_{\mathrm{crys}}(\mathbf{Q}_p \otimes_{\mathbf{Z}_p} T)$, which is free of rank d over $F \otimes_{\mathbf{Q}_p} K$. It follows that $N/\pi N$ is free of rank d over $\mathcal{O}_F \otimes_{\mathbf{Z}_p} \mathcal{O}_K$. Since π is in the Jacobson radical of $\mathbf{A}^+_{K,F}$, Nakayama's lemma shows that N is generated by d elements over $\mathbf{A}^+_{K,F}$. By Lemma 2.14, we know that $\mathbf{A}_{K,F} \otimes_{\mathbf{A}^+_{K,F}} N$ is free of rank d over $\mathbf{A}_{K,F}$, so it follows that N is free of rank d over $\mathbf{A}^+_{K,F}$. □

3. Rank one modules

In this section we give a parametrization of rank one étale (φ, Γ)-modules over $\mathbf{E}_{K,F}$ (with a view toward parametrizing their extensions) and then identify them with the reduction modulo p of Wach modules of rank one over $\mathbf{A}^+_{K,F}$.

3.1 A parametrization

Denote by $\mathrm{val}_\pi : \mathbf{F}((\pi)) \to \mathbf{Z}$ the valuation normalized by $\mathrm{val}_\pi(\pi) = 1$, and let $\lambda_\gamma \in \mathbf{F}_p[[\pi]]$ be the unique $(p^f - 1)/(p-1)$th root of $\gamma(\pi)/\overline{\chi}(\gamma)\pi$, that is congruent to 1 mod π, if $\gamma \in \Gamma$.

Proposition 3.1. *For any $C \in \mathbf{F}^\times$ and any $\vec{c} = (c_0, \ldots, c_{f-1}) \in \mathbf{Z}^S$, letting $M = \mathbf{E}_{K,f} e$ with*

$$\varphi(e) = Pe = (C\pi^{(p-1)c_0}, \pi^{(p-1)c_1}, \ldots, \pi^{(p-1)c_{f-1}})\, e,$$
$$\gamma(e) = G_\gamma e = (\lambda_\gamma^{\sum_0 \vec{c}}, \lambda_\gamma^{\sum_1 \vec{c}}, \ldots, \lambda_\gamma^{\sum_{f-1} \vec{c}})\, e,$$

where $\Sigma_l = \Sigma_l \vec{c} = \sum c_i p^j$ summing over $0 \leqslant i, j \leqslant f-1$, $i - j \equiv l \bmod f$, defines an étale (φ, Γ)-module of rank one over $\mathbf{E}_{K,F}$. Conversely, for any rank one étale (φ, Γ)-module M over $\mathbf{E}_{K,F}$ we can choose a basis e so that $M = \mathbf{E}_{K,F} e$ with the action of φ and Γ given as above for some C and some $\vec{c}$. Two such modules M and M' are isomorphic if and only if $C = C'$ and $\Sigma_0 \vec{c} \equiv \Sigma_0 \vec{c'} \bmod p^f - 1$. In particular, every rank one (φ, Γ)-module over $\mathbf{E}_{K,F}$ can be written uniquely in this form with $0 \leqslant c_i \leqslant p-1$ and at least one $c_i < p-1$.

Proof. To show that the given formula actually defines an étale (φ, Γ)-module we need to verify that $P\varphi(G_\gamma) = G_\gamma \gamma(P)$ and $G_{\gamma\gamma'} = G_\gamma \gamma(G_{\gamma'})$. The first identity holds as

$$\begin{aligned}
\varphi(G_\gamma)/G_\gamma &= (\lambda_\gamma^{p\Sigma_1 - \Sigma_0}, \ldots, \lambda_\gamma^{p\Sigma_0 - \Sigma_{f-1}}) \\
&= (\lambda_\gamma^{c_0(p^f-1)}, \ldots, \lambda_\gamma^{c_{f-1}(p^f-1)}) \\
&= \left(\left(\frac{\gamma(\pi)}{\pi}\right)^{c_0(p-1)}, \ldots, \left(\frac{\gamma(\pi)}{\pi}\right)^{c_{f-1}(p-1)} \right) = \gamma(P)/P.
\end{aligned}$$

To prove the second identity, as Γ acts componentwise, we need to show that $\lambda_{\gamma\gamma'} = \lambda\gamma(\lambda)$. But note that

$$(\lambda_\gamma \gamma(\lambda_{\gamma'}))^{(p^f-1)/(p-1)} = \frac{\gamma(\pi)}{\pi}\overline{\chi}(\gamma)\gamma\left(\frac{\gamma'(\pi)}{\pi}\overline{\chi}(\gamma')\right) = \frac{\gamma\gamma'(\pi)}{\pi}\overline{\chi}(\gamma\gamma')$$

and $\lambda_\gamma \gamma(\lambda_{\gamma'}) \equiv 1 \bmod \pi$. The claim follows from the uniqueness of the λ_γ. Note also that the function $\gamma \mapsto \lambda_\gamma$ is continuous since it is the composite of $\gamma(\pi)/\overline{\chi}(\gamma)\pi$ with the inverse of the continuous bijective function $x \mapsto x^{(p^f-1)/(p-1)}$ on the compact Hausdorff space $1 + \pi\mathbf{F}_p[[\pi]]$; it follows that the Γ-action we have just defined is continuous.

We now prove that any rank one module can be written in this form. Suppose we are given a rank one module $M = \mathbf{E}_{K,F}e$ such that $\varphi(e) = (h_0(\pi), \dots, h_{f-1}(\pi))e$ and $\gamma(e) = (g_0(\pi), \dots, g_{f-1}(\pi))e$. Note that, if $u \in \mathbf{E}_{K,F}^\times$, by a change of basis $e' = ue$ we get $P' = (\varphi(u)/u)P$ and $G'_\gamma = (\gamma(u)/u)G_\gamma$, where $\varphi(e') = P'e'$ and $\gamma(e') = G'_\gamma e'$. If $u = (\pi^j, \dots, \pi^j)$, then $\varphi(u)/u = (\pi^{(p-1)j}, \dots, \pi^{(p-1)j})$. So we can assume that $h_i(\pi) \in \mathbf{F}[[\pi]]$ by choosing a large enough $j > 0$. We can 'shift' between components by appropriate change of basis: if $u = (1, \dots, 1, u_i(\pi), 1, \dots, 1)$, then $\varphi(u)/u = (1, \dots, 1, u_{i-1}(\pi^p), u_i(\pi)^{-1}, 1, \dots, 1)$. By successive changes of basis we can make it into a form where $\varphi(e) = (h(\pi), 1, \dots, 1)e$ with $h(\pi) \in \mathbf{F}[[\pi]]$. Moreover, for some choice of e, $\varphi(e) = (C\pi^v, 1, \dots, 1)e$ for $C \in \mathbf{F}^\times$ and $v \geqslant 0$ as

$$\frac{\varphi(u(\pi), u(\pi^{p^{f-1}}), \dots, u(\pi^p))}{(u(\pi), u(\pi^{p^{f-1}}), \dots, u(\pi^p))} = (u(\pi^{p^f})/u(\pi), 1 \dots, 1)$$

and the map $1 + \pi\mathbf{F}[[\pi]] \to 1 + \pi\mathbf{F}[[\pi]]$, $u(\pi) \mapsto u(\pi^{p^f})/u(\pi)$, is surjective: as the map is multiplicative and $1 + \pi\mathbf{F}[[\pi]]$ is complete π-adically, it suffices to prove that, for any $s \geqslant 1$ and $\alpha \in \mathbf{F}^\times$, $1 + \alpha\pi^s t(\pi)$ is in the image for some $t(\pi) \in \mathbf{F}[[\pi]]^\times$, and indeed $1 - \alpha\pi^s \mapsto (1 - \alpha\pi^{sp^f})/(1 - \alpha\pi^s) \equiv 1 + \alpha\pi^s \bmod \pi^{s+1}$.

To show that $(p-1)|v$, we note that $\varphi\gamma(e) = \gamma\varphi(e)$ if and only if

$$\frac{\varphi(g_0, \dots, g_{f-1})}{(g_0, \dots, g_{f-1})} = \frac{\gamma(C\pi^v, 1, \dots, 1)}{(C\pi^v, 1, \dots, 1)},$$

where $G_\gamma = (g_0, \dots, g_{f-1})$. This is equivalent to

$$\left(\frac{g_1(\pi^p)}{g_0(\pi)}, \dots, \frac{g_0(\pi^p)}{g_{f-1}(\pi)}\right) = \left(\left(\frac{\gamma(\pi)}{\pi}\right)^v, 1, \dots, 1\right),$$

which implies that $(\gamma(\pi)/\pi)^v = g_0(\pi^{p^f})/g_0(\pi) \equiv 1 \bmod \pi$. If $\delta \in \Gamma$ is such that $\delta\Gamma_1$ generates $\Gamma/\Gamma_1 \simeq \mu_{p-1}$, then $\delta(\pi)/\pi \equiv \chi(\delta) \bmod \pi$. Thus $\delta(\pi)/\pi$ has order $p-1$ modulo π so that $p-1|v$ and $\varphi(e) = (C\pi^{(p-1)w}, 1, \dots, 1)$, where $(p-1)w = v$.

To determine the corresponding action of $\gamma \in \Gamma$, we note that $\varphi\gamma(e) = \gamma\varphi(e)$ if and only if

$$\left(\frac{g_1(\pi^p)}{g_0(\pi)}, \dots, \frac{g_0(\pi^p)}{g_{f-1}(\pi)}\right) = \left(\left(\frac{\gamma(\pi)}{\pi}\right)^{(p-1)w}, 1, \dots, 1\right)$$

if and only if $g_0(\pi^{p^f})/g_0(\pi) = (\gamma(\pi)/\pi)^{(p-1)w} = (\gamma(\pi)/\pi\overline{\chi}(\gamma))^{(p-1)w}$ (the order of $\overline{\chi}$ being $p-1$) and $g_1(\pi) = g_2(\pi^p), \dots, g_{f-2}(\pi) = g_{f-1}(\pi^p), g_{f-1}(\pi) = g_0(\pi^p)$. Thus, to get g_i that satisfy the above identity, we just need to define $g_0(\pi)$ such that $g_0(\pi^{p^f})/g_0(\pi) = (\gamma(\pi)/\pi\overline{\chi}(\gamma))^{(p-1)w}$. If we set $g_0(\pi) = \alpha_\gamma\lambda_\gamma(\pi)^w$ with $\alpha_\gamma \in \mathbf{F}^\times$, we have $g_0(\pi^{p^f})/g_0(\pi) = \lambda_\gamma(\pi^{p^f})^w/\lambda_\gamma(\pi)^w = \lambda_\gamma(\pi)^{w(p^f-1)} = (\gamma(\pi)/\pi\overline{\chi}(\gamma))^{(p-1)w}$. Conversely if $g'_0(\pi) \in \mathbf{E}_{K,F}^\times$ satisfies

$$g'_0(\pi^{p^f})/g'_0(\pi) = (\gamma(\pi)/\pi\overline{\chi}(\gamma))^{(p-1)w} = g'_0(\pi^{p^f})/g'_0(\pi),$$

then $h(\pi) = g'_0(\pi)g_0^{-1}(\pi)$ satisfies $h(\pi^{p^f}) = h(\pi)$ and is therefore constant. Thus we see that the identity implies that $g_0(\pi)$ has the required form.

Since $G_{\gamma\gamma'} = G_\gamma \gamma(G'_\gamma)$, the map $\gamma \mapsto \alpha_\gamma$ must define a character $\Gamma \to \mathbf{F}^\times$, from which we conclude that $\alpha_\gamma = \overline{\chi}(\gamma)^{j_0}$ for some $0 \leqslant j_0 < p-1$. Letting $u = (\pi, \pi^{p^{f-1}}, \pi^{p^{f-2}}, \ldots, \pi^p)$, we have

$$\begin{aligned}\frac{\varphi(u)}{u} &= (\pi^{p^f-1}, 1, \ldots, 1),\\ \frac{\gamma(u)}{u} &= \left(\frac{\gamma(\pi)}{\pi}, \left(\frac{\gamma(\pi)}{\pi}\right)^{p^{f-1}}, \left(\frac{\gamma(\pi)}{\pi}\right)^{p^{f-2}}, \ldots, \left(\frac{\gamma(\pi)}{\pi}\right)^{p}\right)\\ &\equiv (\overline{\chi}(\gamma), \ldots, \overline{\chi}(\gamma)) \mod \pi,\end{aligned}$$

so replacing e by $u^{-j}e$ for some $j \equiv j_0 \bmod p-1$ gives $M = \mathbf{E}_{K,F}e$ with

$$\begin{aligned}\varphi(e) &= (C\pi^{(p-1)w}, 1, \ldots, 1)e,\\ \gamma(e) &= (\lambda_\gamma(\pi)^w, \lambda_\gamma(\pi^{p^{f-1}})^w, \ldots, \lambda_\gamma(\pi^p)^w)e,\end{aligned}$$

where $0 \leqslant w < p^f - 1$. Write $w = c_0 + c_1 p + \cdots + c_{f-1}p^{f-1}$ with $0 \leqslant c_i \leqslant p-1$. Taking $e' = ue$ with $u = (1, \pi^{(p-1)(c_1 + c_2 p + \cdots + c_{f-1}p^{p-2})}, 1, \ldots, 1)$ yields

$$\varphi(e') = (C\pi^{(p-1)c_0}, \pi^{(p-1)(c_1+c_2p+\cdots+c_{f-1}p^{p-2})}, 1, \ldots, 1)e.$$

Doing this successively gives $\varphi(e) = (C\pi^{(p-1)c_0}, \pi^{(p-1)c_1}, \ldots, \pi^{(p-1)c_{f-1}})e$ for some basis e. It is easily checked that those changes of basis that maintain $G_\gamma \equiv (1, \ldots, 1) \bmod \pi$ are $e' = ue$ such that $u = (u_0, \ldots, u_{f-1})$ with $(p-1)|\mathrm{val}_\pi(u_i)$ and that the corresponding action of $\gamma \in \Gamma$ is given by $\gamma(e) = (\lambda_\gamma^{\sum_0 \vec{c}}, \lambda_\gamma^{\sum_1 \vec{c}}, \ldots, \lambda_\gamma^{\sum_{f-1}\vec{c}})e$.

Finally, we suppose that M is isomorphic to $M' = \mathbf{E}_{K,F}e'$ with

$$\begin{aligned}\varphi(e') &= P'e' = (C'\pi^{(p-1)c'_0}, \pi^{(p-1)c'_1}, \ldots, \pi^{(p-1)c'_{f-1}})e',\\ \gamma(e') &= G'_\gamma e' = (\lambda_\gamma^{\sum_0 \vec{c'}}, \lambda_\gamma^{\sum_1 \vec{c'}}, \ldots, \lambda_\gamma^{\sum_{f-1}\vec{c'}})e',\end{aligned}$$

and determine when the two are isomorphic. After appropriate changes of bases we can assume that

$$\begin{aligned}\varphi(e) &= Pe = (C\pi^{(p-1)w}, 1, \ldots, 1)e,\\ \varphi(e') &= P'e' = (C'\pi^{(p-1)w'}, 1, \ldots, 1)e',\end{aligned}$$

where $w = \sum_0 \vec{c}$ and $w' = \sum_0 \vec{c'}$ satisfy $0 \leqslant w, w' < p^f - 1$.

Suppose that $u = (u_0, \ldots, u_{f-1}) \in \mathbf{E}_{K,F}^\times$ is such that $P' = (\varphi(u)/u)P$ and $G'_\gamma = (\gamma(u)/u)G_\gamma$ for all $\gamma \in \Gamma$. Then $\gamma(u_0)/u_0 \equiv 1 \bmod \pi\mathbf{F}[[\pi]]$, so $(p-1)|\mathrm{val}_\pi(u_0)$. It follows that $u = (u_0(\pi), u_0(\pi^{p^{f-1}}), \ldots, u_0(\pi^p))$ with $u_0(\pi) = u'_0(\pi)\pi^{(p-1)j}$ for some $u'_0(\pi) \in \mathbf{F}[[\pi]]^\times$ and $j \in \mathbf{Z}$, in which case we have

$$\varphi(u)/u = (\pi^{(p-1)(p^f-1)j}u'_0(\pi)^{p^f-1}, 1, \ldots, 1).$$

Thus, we conclude that M and M' are isomorphic if and only if $C = C'$ and $\sum c_i p^i \equiv \sum c'_i p^i \bmod p^f - 1$.

The last assertion is clear. □

We denote the module defined in the proposition by $M_{C\vec{c}} = M_{C(c_0,\ldots,c_{f-1})}$. We simply write $M_{\vec{c}}$ for $M_{C\vec{c}}$ if $C = 1$. We also put

$$\begin{aligned}\kappa_\varphi(M_{C\vec{c}}) &= \kappa_\varphi(C, \vec{c}\,) = (C\pi^{(p-1)c_0}, \pi^{(p-1)c_1}, \ldots, \pi^{(p-1)c_{f-1}}),\\ \kappa_\gamma(M_{C\vec{c}}) &= \kappa_\gamma(C, \vec{c}\,) = (\lambda_\gamma^{\sum_0 \vec{c}}, \lambda_\gamma^{\sum_1 \vec{c}}, \ldots, \lambda_\gamma^{\sum_{f-1}\vec{c}}),\end{aligned}$$

and write Σ_l for $\Sigma_l \vec{c}$, where the c_i are understood.

3.2 Lifts in characteristic zero

We now construct rank one Wach modules over $\mathbf{A}^+_{K,F}$ following Dousmanis [Dou08, § 2] and check that these reduce modulo ϖ_F to the (φ, Γ)-modules $M_{C\vec{c}}$ over $\mathbf{E}_{K,F}$.

Let $q_1 = q = \varphi(\pi)/\pi$, $q_n = \varphi^{n-1}(q) \in \mathbf{Z}_p[[\pi]]$ and let $\Lambda_f = \prod_{j\geqslant 0} q_{1+jf}/p$, $\Lambda_\gamma = \Lambda_f/\gamma(\Lambda_f) \in \mathbf{Q}[[\pi]]$. One then has that $\Lambda_f \in 1 + \pi\mathbf{Q}_p[[\pi]]$ and $\Lambda_\gamma \in 1 + \pi\mathbf{Z}_p[[\pi]]$.

Suppose we want to construct a rank one Wach module $N = \mathbf{A}^+_{K,F} e$ such that

$$\varphi(e) = (\tilde{C}q^{c_0}, q^{c_1}, \dots, q^{c_{f-1}})e,$$
$$\gamma(e) = (g_0(\pi), \dots, g_{f-1}(\pi))e$$

if $\gamma \in \Gamma$, where $\tilde{C} \in \mathcal{O}_F^\times$ is any lift of $C \in \mathbf{F}^\times$ and each $g_i(\pi) = g_{\gamma,i}(\pi) \in \mathcal{O}_F[[\pi]]$ depends on $\gamma \in \Gamma$. Commutativity of the actions of φ and Γ amounts to the following identities:

$$\begin{aligned}
\gamma(q)^{c_0} g_0(\pi) &= q^{c_0}\varphi(g_1(\pi)),\\
\gamma(q)^{c_1} g_1(\pi) &= q^{c_1}\varphi(g_2(\pi)),\\
&\vdots\\
\gamma(q)^{c_{f-2}} g_{f-2}(\pi) &= q^{c_{f-2}}\varphi(g_{f-1}(\pi)),\\
\gamma(q)^{c_{f-1}} g_{f-1}(\pi) &= q^{c_{f-1}}\varphi(g_0(\pi)).
\end{aligned}$$

Thus, we are looking for a solution $g_i(\pi)$ for each γ of the equation

$$g_0(\pi) = \left(\frac{q}{\gamma(q)}\right)^{c_0} \varphi\left(\frac{q}{\gamma(q)}\right)^{c_1} \varphi^2\left(\frac{q}{\gamma(q)}\right)^{c_2} \cdots \varphi^{f-1}\left(\frac{q}{\gamma(q)}\right)^{c_{f-1}} \varphi^f(g_0(\pi)).$$

It is straightforward to check that

$$g_0(\pi) = \Lambda_\gamma^{c_0}\varphi(\Lambda_\gamma)^{c_1}\varphi^2(\Lambda_\gamma)^{c_2}\cdots\varphi^{f-1}(\Lambda_\gamma)^{c_{f-1}}$$

gives the unique solution, that is congruent to 1 modulo π, and that the remaining $g_i(\pi)$ are uniquely determined by

$$\begin{aligned}
g_1(\pi) &= \left(\frac{q}{\gamma(q)}\right)^{c_1} \varphi\left(\frac{q}{\gamma(q)}\right)^{c_2} \cdots \varphi^{f-1}\left(\frac{q}{\gamma(q)}\right)^{c_{f-1}} \varphi^{f-1}(g_0(\pi)),\\
&\vdots\\
g_{f-2}(\pi) &= \left(\frac{q}{\gamma(q)}\right)^{c_{f-2}} \varphi\left(\frac{q}{\gamma(q)}\right)^{c_{f-1}} \varphi^2(g_0(\pi)),\\
g_{f-1}(\pi) &= \left(\frac{q}{\gamma(q)}\right)^{c_{f-1}} \varphi(g_0(\pi)).
\end{aligned}$$

Dousmanis [Dou08, § 6] shows that $N = \mathbf{A}^+_{K,F} e$ endowed with the actions of φ and Γ described above defines a Wach module over $\mathbf{A}^+_{K,F}$, which we denote by $N_{\tilde{C}\vec{c}}$. Furthermore, $(N_{\tilde{C}\vec{c}}/\pi N_{\tilde{C}\vec{c}}) \otimes_{\mathbf{A}^+_{K,F}} \mathbf{B}^+_{K,F}$ is a filtered φ-module corresponding to a positive character $G_K \to \mathbf{F}^\times$ with labeled Hodge–Tate weights $(c_{f-1}, c_0, c_1, \dots, c_{f-2})$. One can check the following by direct computation.

Proposition 3.2. *We have an isomorphism $M_{C\vec{c}} \simeq N_{\tilde{C}\vec{c}} \otimes_{\mathbf{A}^+_{K,F}} \mathbf{E}_{K,F}$ of (φ, Γ)-modules over $\mathbf{E}_{K,F}$.*

Combined with [BDJ10, Lemma 3.8], we obtain the following corollary, where ω_τ denotes the fundamental character associated to τ (i.e., $\omega_\tau : I_K \to \mathbf{F}^\times$ is defined by composing τ with the homomorphism $I_K \to k^\times$ obtained from local class field theory, with the convention that uniformizers correspond to geometric Frobenius elements).

COROLLARY 3.3. *If $\psi : G_K \to \mathbf{F}^\times$ is the character defined by the action on $\mathbf{V}(M_{C\vec{c}})$, then $\psi|_{I_K} = \prod_{\tau \in S} \omega_\tau^{-c_{\tau\circ\varphi^{-1}}}$.*

4. Bases for the space of extensions

We will assume $p > 2$ for the rest of the paper except in §§ 6.3 and 7. We fix a topological generator η of the pro-cyclic group $\Gamma = \Gamma_K$, and set $\xi = \eta^{p-1}$, so that ξ topologically generates Γ_1.

Given $C \in \mathbf{F}^\times$ and $\vec{c} = (c_0, \ldots, c_{f-1}) \in \{0, 1, \ldots, p-1\}^S$ with some $c_i < p-1$, we are going to parametrize the space of extension classes $\mathrm{Ext}^1(M_0, M_{C\vec{c}})$ in the category of étale (φ, Γ)-modules over $\mathbf{E}_{K,F}$. Here M_0 denotes the étale (φ, Γ)-module $\mathbf{E}_{K,F}$ with the usual action of φ and Γ, so $M_0 = M_{1,\vec{0}}$ corresponds to the trivial character $G_K \to \mathbf{F}^\times$. Recall that $M_{C\vec{c}}$, $\kappa_\varphi(M_{C\vec{c}})$ and $\kappa_\gamma(M_{C\vec{c}})$ were defined at the end of § 3.1; since $M_{C\vec{c}}$ will be fixed in this section, we denote these simply κ_φ and κ_γ.

We start by noticing that there is an $\mathbf{F}$-linear isomorphism

$$\beta : H/H_0 \to \mathrm{Ext}^1(M_0, M_{C\vec{c}}),$$

where H is the subgroup of $\mathbf{E}_{K,F} \times \{\Gamma \to \mathbf{E}_{K,F}\}$ consisting of elements $(\mu_\varphi, (\mu_\gamma)_{\gamma\in\Gamma})$ such that $\gamma \mapsto \mu_\gamma$ is continuous and satisfies:[1]

$$(\dagger) \qquad (\kappa_\varphi\varphi - 1)(\mu_\gamma) = (\kappa_\gamma\gamma - 1)(\mu_\varphi) \quad \forall \gamma \in \Gamma,$$

$$(\ddagger) \qquad \mu_{\gamma\gamma'} = \kappa_\gamma\gamma(\mu_{\gamma'}) + \mu_\gamma \quad \forall \gamma, \gamma' \in \Gamma,$$

and $H_0 = \{(\kappa_\varphi\varphi(b) - b, (\kappa_\gamma\gamma(b) - b)_{\gamma\in\Gamma}) \mid b \in \mathbf{F}((\pi))^S\} \subset H$.

We call elements of H *cocyles* and those of H_0 *coboundaries*. The map β is defined as follows: given a cocycle $\mu = (\mu_\varphi, (\mu_\gamma)_{\gamma\in\Gamma}) \in H$, we define an extension

$$0 \to M_{C\vec{c}} \to E \to M_0 \to 0$$

basis $\{e, e'\}$ such that the action φ and $\gamma \in \Gamma$ are given by the matrices $P = \left(\begin{smallmatrix} \kappa_\varphi & \mu_\varphi \\ 0 & 1 \end{smallmatrix}\right)$ and $G_\gamma = \left(\begin{smallmatrix} \kappa_\gamma & \mu_\gamma \\ 0 & 1 \end{smallmatrix}\right)$. It is straightforward to check that the matrices P and G_γ define an extension if and only if $\mu \in H$, that every extension arises this way, and that a change of basis for an extension E corresponds to adding an element of H_0 to μ. If $\mu \in H$, then we write $[\mu]$ for the corresponding extension class $\beta(\mu)$.

By Corollary 2.13, we get an isomorphism $\mathrm{Ext}^1(M_{\vec{0}}, M_{C\vec{c}}) \simeq H^1(K, \mathbf{F}(\psi))$ where $\psi : G_K \to \mathbf{F}^\times$ is the character defined by the action on $\mathbf{V}(M_{C\vec{c}})$.

LEMMA 4.1. *Via Corollary 2.13, $M_{\vec{0}}$ corresponds to the trivial character and $M_{\overrightarrow{p-2}}$ to the $\bmod p$ cyclotomic character.*

Proof. The assertion is clear for the trivial character. The $\bmod p$ cyclotomic character factors as $G_K \to \mathbf{Z}_p^\times \to \mathbf{F}_p^\times \hookrightarrow \mathbf{F}^\times$, where the arrow in the middle is the reduction $\bmod p$. If $T = \mathbf{Z}_p(1)$, its Wach module is given by $\mathbf{N}(\mathbf{Z}_p(1)) = \mathbf{A}_K^+ e$, where $\varphi(e) = (\pi/\varphi(\pi))e$ and $\gamma(e) = (\chi(\gamma)\pi/\gamma(\pi))e$ if $\gamma \in \Gamma$ (cf. [Ber04b, Appendice A]). Working modulo p and extending

[1] We will frequently use the following notation: for an element κ and a ring endomorphism ψ of $\mathbf{E}_{K,F}$, we denote by $\kappa\psi - 1$ the $\mathbf{F}$-linear endomorphism of $\mathbf{E}_{K,F}$ defined by $(\kappa\psi - 1)(x) = \kappa\psi(x) - x$. We do the same for $\mathbf{F}((\pi))$ in place of $\mathbf{E}_{K,F}$. Thus, for example, if $\Sigma, s \in \mathbf{Z}$, then $(\lambda_\gamma^\Sigma\gamma - 1)(\pi^s)$ denotes $\lambda_\gamma(\pi)^\Sigma \cdot \gamma(\pi^s) - \pi^s$.

scalars to $\mathbf{F}$ we see that the étale (φ, Γ)-module over $\mathbf{E}_{K,F}$ corresponding to the mod p cyclotomic character is given by $M = \mathbf{E}_{K,F}e$ with $\varphi(e) = \pi^{1-p}e = (\pi^{1-p}, \ldots, \pi^{1-p})e$. By a change of basis $e' = ue$ with $u = (\pi^{p-1}, \ldots, \pi^{p-1})$, we get $M \simeq M_{\overrightarrow{p-2}}$. □

Since

$$\dim_{\mathbf{F}} H^1(K, \mathbf{F}(\psi)) = \begin{cases} f+1 & \text{if } \psi = 1 \text{ or } \overline{\chi}, \\ f & \text{if } \psi \notin \{1, \overline{\chi}\}, \end{cases}$$

we have

$$\dim_{\mathbf{F}} \operatorname{Ext}^1(M_{\vec{0}}, M_{C\vec{c}}) = \begin{cases} f+1 & \text{if } C = 1, \text{ and } \vec{c} = \vec{0} \text{ or } \vec{c} = \overrightarrow{p-2}, \\ f & \text{otherwise.} \end{cases}$$

We are about to define elements $B_0, \ldots, B_{f-1} \in H$ such that the associated extension classes form a basis for $\operatorname{Ext}^1(M_{\vec{0}}, M_{C\vec{c}})$ except for the two cases where $C = 1, \vec{c} = \vec{0}$ or $C = 1, \vec{c} = \overrightarrow{p-2}$, for which a separate treatment will be given in § 6. Thanks to the isomorphism β, we only need to define μ_φ and the μ_γ satisfying the desired properties (†) and (‡). According to whether the parameter c_i is equal to $p-1$ or not, the extension B_i is constructed in a slightly different manner.

4.1 Construction of B_i when $c_i < p-1$

Recall that we have fixed a topological generator η for Γ, and we let $\xi = \eta^{p-1}$, a topological generator for Γ_1.

Lemma 4.2. *Suppose that $\Sigma, s \in \mathbf{Z}$, and $v = v_p(\Sigma + s(p^f-1)/(p-1)) < \infty$. Then*

$$(\lambda_\eta^\Sigma \eta - 1)(\pi^s) \in (\overline{\chi}(\eta)^s - 1)\pi^s + \overline{s_v} \frac{\overline{\chi}(\eta)^s(\overline{\chi}(\eta) - 1)}{2} \pi^{s+p^v} + \pi^{s+2p^v} \mathbf{F}_p[[\pi^{p^v}]],$$

where $\Sigma + s(p^f-1)/(p-1) = \sum_{j \geqslant v} s_j p^j$.

Proof. It is easy to see that in $\mathbf{F}_p[[\pi]]/\pi^{p-1}$ we have

$$\lambda_\eta = \lambda_\eta^{(p^f-1)/(p-1)} = \frac{\eta(\pi)}{\overline{\chi}(\eta)\pi} = \overline{\chi}(\eta)^{-1} \sum_{j=1}^{d_0-1} \overline{\frac{d_0!}{j!(d_0-j)!}} \pi^{j-1} = 1 + \sum_{j=2}^{d_0-1} \overline{\frac{d_0!}{d_0 j!(d_0-j)!}} \pi^{j-1},$$

where $\chi(\eta) = \sum_{j \geqslant 0} d_j p^j \in \mathbf{Z}_p^\times$. Noting that, if $s \in \mathbf{Z}$, then

$$(\lambda_\eta^\Sigma \eta - 1)(\pi^s) = \left(\overline{\chi}(\eta)^s \lambda_\eta^\Sigma \cdot \left(\frac{\eta(\pi)}{\overline{\chi}(\eta)\pi} \right)^s - 1 \right) \pi^s,$$

the result follows as

$$\begin{aligned}
\overline{\chi}(\eta)^s \lambda_\eta^\Sigma \cdot \left(\frac{\eta(\pi)}{\overline{\chi}(\eta)\pi} \right)^s - 1 &= \overline{\chi}(\eta)^s \lambda_\eta^{\Sigma + s(p^f-1)/(p-1)} - 1 \\
&= \overline{\chi}(\eta)^s \lambda_\eta^{\sum_{j \geqslant v} s_j p^j} - 1 \\
&= \overline{\chi}(\eta)^s \lambda_\eta(\pi^{p^v})^{s_v} \lambda_\eta(\pi^{p^{v+1}})^{s_{v+1}} \cdots - 1 \\
&\equiv (\overline{\chi}(\eta)^s - 1) + \overline{\chi}(\eta)^s \left(\left(1 + \frac{\overline{\chi}(\eta) - 1}{2} \pi^{p^v} \right)^{s_v} - 1 \right) \\
&\equiv (\overline{\chi}(\eta)^s - 1) + \overline{s_v} \frac{\overline{\chi}(\eta)^s(\overline{\chi}(\eta) - 1)}{2} \pi^{p^v} \mod \pi^{2p^v}
\end{aligned}$$

and

$$\overline{\chi}(\eta)^s\lambda_\eta^\Sigma\cdot\left(\frac{\eta(\pi)}{\overline{\chi}(\eta)\pi}\right)^s-1-\left((\overline{\chi}(\eta)^s-1)+\overline{s_v}\frac{\overline{\chi}(\eta)^s(\overline{\chi}(\eta)-1)}{2}\pi^{p^v}\right)\in\pi^{2p^v}\mathbf{F}_p[[\pi^{p^v}]].\qquad\square$$

We note the following lemma, whose straightforward proof we omit.

Lemma 4.3. *If $n\geqslant 1$, $\gamma\in\Gamma_n$ and $\chi(\gamma)\equiv 1+zp^n \bmod p^{n+1}$, then $\lambda_\gamma\equiv 1+z\pi^{p^n-1}+z\pi^{p^n} \bmod \pi^{2p^n-2}$.*

Lemma 4.4. *Let $\chi(\xi)\equiv 1+zp \mod p^2$ with $0<z\leqslant p-1$ and let $\Sigma, s\in\mathbf{Z}$. If $v=v_p(\Sigma+s(p^f-1)/(p-1))<\infty$, then*

$$(\lambda_\xi^\Sigma\xi-1)(\pi^s)\in\overline{s_v z}(\pi^{s+(p-1)p^v}+\pi^{s+p^{v+1}})+\pi^{s+2p^v(p-1)}\mathbf{F}_p[[\pi^{p^v}]],$$

where $\Sigma+s(p^f-1)/(p-1)=\sum_{j\geqslant v}s_jp^j$.

Proof. By Lemma 4.3, we have

$$\lambda_\xi\equiv\frac{\xi(\pi)}{\pi\overline{\chi}(\xi)}\equiv 1+z\pi^{p-1}+z\pi^p\mod \pi^{2p-2}.$$

Noting that, if $s\in\mathbf{Z}$, then

$$(\lambda_\xi^\Sigma\xi-1)(\pi^s)=\left(\lambda_\xi^\Sigma\cdot\left(\frac{\xi(\pi)}{\pi\overline{\chi}(\xi)}\right)^s-1\right)\pi^s,$$

the result follows as

$$\begin{aligned}\lambda_\xi^\Sigma\cdot\left(\frac{\xi(\pi)}{\pi\overline{\chi}(\xi)}\right)^s-1&=\lambda_\xi^{\Sigma+s(p^f-1)/(p-1)}-1\\&=\lambda_\xi(\pi^{p^v})^{s_v}\lambda_\xi(\pi^{p^{v+1}})^{s_{v+1}}\cdots-1\\&\equiv\lambda_\xi(\pi^{p^v})^{s_v}-1\mod \pi^{(p-1)p^{v+1}}\\&\equiv\overline{s_v z}(\pi^{(p-1)p^v}+\pi^{p^{v+1}})\mod \pi^{2(p-1)p^v}\end{aligned}$$

and

$$\lambda_\xi^\Sigma\cdot\left(\frac{\xi(\pi)}{\pi\overline{\chi}(\xi)}\right)^s-1-\overline{s_v z}(\pi^{(p-1)p^v}+\pi^{p^{v+1}})\in\pi^{2(p-1)p^v}\mathbf{F}_p[[\pi^{p^v}]].\qquad\square$$

We now assume $c_i<p-1$ and construct an element $B_i\in H$. (For the case $c_i=p-1$, we will need to use a modified construction described in § 4.2.)

Suppose for the moment that we have successfully defined B_i with $\mu_\varphi(B_i)$ of the form $(0,\dots,0,H_i(\pi),0,\dots,0)$, $H_i(\pi)$ being the ith component. For each $\gamma\in\Gamma$, by the condition (†) there should exist $\mu_\gamma(B_i)=(G_0(\pi),\dots,G_{f-1}(\pi))$ such that

$$(\kappa_\varphi\varphi-1)(\mu_\gamma(B_i))=(\kappa_\gamma\gamma-1)(\mu_\varphi(B_i)),$$

i.e.,

$$\begin{aligned}&(C\pi^{(p-1)c_0}G_1(\pi^p)-G_0(\pi),\pi^{(p-1)c_1}G_2(\pi^p)-G_1(\pi),\dots,\pi^{(p-1)c_{f-1}}G_0(\pi^p)-G_{f-1}(\pi))\\&\quad=(0,\dots,0,(\lambda_\gamma^{\Sigma_i}\gamma-1)(H_i(\pi)),0,\dots,0).\end{aligned}$$

https://doi.org/10.1112/S0010437X1000504X Published online by Cambridge University Press

This is true if and only if

$$\begin{aligned}(C\pi^{(p-1)\Sigma_i}\Phi - 1)(G_i(\pi)) &= (\lambda_\gamma^{\Sigma_i}\gamma - 1)(H_i(\pi)),\\ G_{i+1}(\pi) &= \pi^{(p-1)c_{i+1}}G_{i+2}(\pi^p),\\ &\vdots\\ G_{f-1}(\pi) &= \pi^{(p-1)c_{f-1}}G_0(\pi^p),\\ G_0(\pi) &= C\pi^{(p-1)c_0}G_1(\pi^p),\\ G_1(\pi) &= \pi^{(p-1)c_1}G_2(\pi^p),\\ &\vdots\\ G_{i-1}(\pi) &= \pi^{(p-1)c_{i-1}}G_i(\pi^p),\end{aligned}$$

where $\Phi(G(\pi)) = G(\pi^{p^f})$. Except for the case $C = 1$, $\vec{c} = \vec{0}$, the map $C\pi^{(p-1)\Sigma_i}\Phi - 1$ defines a bijection $\mathbf{F}[[\pi]] \to \mathbf{F}[[\pi]]$. So the trick is to find $H_i(\pi)$ so that we have $(\lambda_\gamma^{\Sigma_i}\gamma - 1)(H_i(\pi)) \in \mathbf{F}[[\pi]]$. The corresponding $G_i(\pi)$ and so the $\mu_\gamma(B_i)$ are automatically and uniquely determined by the bijectivity. Moreover, since the bijection $C\pi^{(p-1)\Sigma_i}\Phi - 1$ on the compact Hausdorff space $\mathbf{F}[[\pi]]$ is continuous, so is its inverse, and it follows that $\gamma \mapsto \mu_\gamma(B_i)$ is continuous.

To find such $H_i(\pi)$, we observe via Lemma 4.2 that[2]

$$\mathrm{val}_\pi(\lambda_\eta^{\Sigma_i}\eta - 1)(\pi^{1-p}) = 2 - p \quad \text{and} \quad \mathrm{val}_\pi(\lambda_\eta^{\Sigma_i}\eta - 1)(\pi^s) = s \quad \text{if } 2 - p \leqslant s \leqslant -1.$$

Then there exist unique $\epsilon_{2-p}, \ldots, \epsilon_{-1} \in \mathbf{F}_p$ such that

$$(\lambda_\eta^{\Sigma_i}\eta - 1)(\pi^{1-p} + \epsilon_{2-p}\pi^{2-p} + \cdots + \epsilon_{-1}\pi^{-1}) \in \mathbf{F}[[\pi]].$$

We set

$$H_i(\pi) = \pi^{1-p} + h_i(\pi) = \pi^{1-p} + \epsilon_{2-p}\pi^{2-p} + \cdots + \epsilon_{-1}\pi^{-1}$$

and claim that

$$(\lambda_\gamma^{\Sigma_i}\gamma - 1)(H_i(\pi)) \in \mathbf{F}[[\pi]]$$

for all $\gamma \in \Gamma$. Note that by Lemma 4.3 we have $\lambda_{\gamma_1} \equiv 1 \bmod \pi^{p-1}$, so that $(\lambda_{\gamma_1}\gamma_1 - 1)(\pi^s) \equiv 0 \bmod \pi^{p-1}$ for all $1 - p \leqslant s \leqslant -1$ if $\gamma_1 \in \Gamma_1$. Since any given $\gamma \in \Gamma$ can be written as $\gamma = \eta^m\gamma_1$, where $m \in \mathbf{N}_{\geqslant 0}$ and $\gamma_1 \in \Gamma_1$, we have

$$(\lambda_\gamma^{\Sigma_i}\gamma - 1)(H_i(\pi)) \in \mathbf{F}[[\pi]]$$

by the following lemma.

Lemma 4.5. *Let Σ and v be integers and $H(\pi) \in \mathbf{F}((\pi))$. For any $\gamma, \gamma' \in \Gamma$, if the valuations (in π) of $(\lambda_\gamma^\Sigma\gamma - 1)(H(\pi))$ and $(\lambda_{\gamma'}^\Sigma\gamma' - 1)(H(\pi))$ are at least v, so is that of $(\lambda_{\gamma\gamma'}^\Sigma\gamma\gamma' - 1)(H(\pi))$.*

Proof. If both $\lambda_\gamma^\Sigma\gamma(H(\pi)) - H(\pi)$ and $\lambda_{\gamma'}^\Sigma\gamma'(H(\pi)) - H(\pi)$ are in $\pi^v\mathbf{F}[[\pi]]$, then

$$\begin{aligned}(\lambda_{\gamma\gamma'}^\Sigma\gamma\gamma' - 1)(H(\pi)) &= \left(\frac{\gamma\gamma'(\pi)}{\pi\overline{\chi}(\gamma\gamma')}\right)^{(p-1)\Sigma/(p^f-1)}\gamma\gamma'(H(\pi)) - H(\pi)\\ &= \left(\gamma\left(\frac{\gamma'(\pi)}{\pi\overline{\chi}(\gamma')}\right)\frac{\gamma(\pi)}{\pi\overline{\chi}(\gamma)}\right)^{(p-1)\Sigma/(p^f-1)}\gamma(\gamma'(H(\pi))) - H(\pi)\\ &= \lambda_\gamma^\Sigma\gamma(\lambda_{\gamma'}^\Sigma\gamma'(H(\pi)) - H(\pi)) + \lambda_\gamma^\Sigma\gamma(H(\pi)) - H(\pi) \in \pi^v\mathbf{F}[[\pi]].\end{aligned}$$ □

[2] Note that, if $c_i = p - 1$, then $\Sigma_i \equiv -1 \bmod p$ and $v \geqslant 1$ in the notation of Lemma 4.2, which is why we need to modify the construction in that case.

So far we have defined $\mu_\varphi = \mu_\varphi(B_i)$ and $\mu_\gamma = \mu_\gamma(B_i)$ satisfying the condition (†), and need to verify the condition (‡). It is easily checked that, if $\gamma, \gamma' \in \Gamma$, both $\mu_{\gamma\gamma'}$ and $\mu'_{\gamma\gamma'} = \kappa_\gamma \gamma(\mu_{\gamma'}) + \mu_\gamma$ satisfy (†). Since when we fix μ_φ the solution of (†) for $\gamma\gamma'$ is unique (by the bijectivity of the map $C\pi^{\Sigma_i}\Phi - 1$), we must have (‡) $\mu_{\gamma\gamma'} = \kappa_\gamma\gamma(\mu_{\gamma'}) + \mu_\gamma$.

4.2 Construction of B_i when $c_i = p - 1$

Proposition 4.6. *If $c_i = p-1$ and $c_{i+1} \neq p-2$, we have*

$$(\lambda_\eta^{\Sigma_i}\eta - 1)(\pi^{1-p^2} + h''_i(\pi) + \epsilon(\pi^{2-2p} + h'_i(\pi) + h_i(\pi))) \in \mathbf{F}[[\pi]]$$

for some unique $\epsilon \in \mathbf{F}^\times$ and some unique Laurent polynomials $h''_i(\pi) = \sum_{s=1}^{p-2} \epsilon''_s \pi^{1-p^2+sp}$, $h'_i(\pi) = \sum_{s=1}^{p-2} \epsilon'_s \pi^{2-2p+s}$ and $h_i(\pi) = \sum_{s=1}^{p-2} \epsilon_s \pi^{1-p+s} \in \mathbf{F}[\pi][1/\pi]$.

Proof. By Lemma 4.2 we have,

$$(\lambda_\eta^{\Sigma_i}\eta - 1)(\pi^{1-p^2}) \in \mathbf{F}^\times \pi^{1-p^2+p} + \pi^{1-p^2+2p}\mathbf{F}[[\pi^p]]$$

and

$$(\lambda_\eta^{\Sigma_i}\eta - 1)(\pi^{1-p^2+sp}) \in \mathbf{F}^\times \pi^{1-p^2+sp} + \sum_{j=1}^{p-s} \mathbf{F}\pi^{1-p^2+(s+j)p} + \mathbf{F}[[\pi]]$$

for $1 \leqslant s \leqslant p-2$. Thus there exist unique $\epsilon''_s, \nu' \in \mathbf{F}$ such that

$$(\lambda_\eta^{\Sigma_i}\eta - 1)\left(\pi^{1-p^2} + \sum_{s=1}^{p-2} \epsilon''_s \pi^{1-p^2+sp}\right) \in \nu'\pi^{1-p} + \mathbf{F}[[\pi]].$$

Similarly, there exist unique $\epsilon'_s, \epsilon_s, \nu \in F$ such that

$$(\lambda_\eta^{\Sigma_i}\eta - 1)\left(\pi^{2-2p} + \sum_{s=1}^{p-2} \epsilon'_s \pi^{2-2p+s} + \sum_{s=1}^{p-2} \epsilon_s \pi^{1-p+s}\right) \in \nu\pi^{1-p} + \mathbf{F}[[\pi]].$$

Put $h''_i(\pi) = \sum_{s=1}^{p-2} \epsilon''_s \pi^{2-p^2+sp}$, $h'_i(\pi) = \sum_{s=1}^{p-2} \epsilon'_s \pi^{2-2p+s}$ and $h_i(\pi) = \sum_{s=1}^{p-2} \epsilon_s \pi^{1-p+s}$.

The point then is to show that both ν and ν' are non-zero so that

$$(\lambda_\eta^{\Sigma_i}\eta - 1)(\pi^{1-p^2} + h''_i(\pi)) + \epsilon\,(\lambda_\eta^{\Sigma_i}\eta - 1)(\pi^{2-2p} + h'_i(\pi) + h_i(\pi)) \in \mathbf{F}[[\pi]],$$

where $\epsilon = -\nu'/\nu \in \mathbf{F} - \{0\}$. So let us prove the non-vanishing of ν' and ν. Suppose $\nu' = 0$, so that $\mathrm{val}_\pi(\lambda_\eta^{\Sigma_i}\eta - 1)(\pi^{1-p^2} + h''_i(\pi)) \geqslant 0$. By Lemma 4.5, recalling that $\xi = \eta^{p-1}$, it follows that $\mathrm{val}_\pi(\lambda_\xi^{\Sigma_i}\xi - 1)(\pi^{1-p^2} + h''_i(\pi)) \geqslant 0$, However, by Lemma 4.4 we have $\mathrm{val}_\pi(\lambda_\eta^{\Sigma_i}\eta - 1)(\pi^{1-p^2} + h''_i(\pi)) = 1 - p$. Thus ν' cannot be zero. Similarly, we get $\nu \neq 0$. □

Proposition 4.7. *If $c_i = p-1$, and $r \in \{0, \ldots, f-1\}$ is such that $c_{i+1} = \cdots = c_{i+r} = p-2$ and $c_{i+r+1} \neq p-2$, we have*

$$(\lambda_\eta^{\Sigma_i}\eta - 1)\left(\pi^{1-p^{r+2}} + \sum_{j=0}^{r+1} h_i^{(j)} + \sum_{j=0}^{r} \epsilon^{(j)} h_i'^{(j)}\right) \in \mathbf{F}[[\pi]]$$

https://doi.org/10.1112/S0010437X1000504X Published online by Cambridge University Press

for some unique Laurent polynomials

$$h_i^{(j)}(\pi)=\sum_{s=1}^{p-2}\epsilon_s^{(j)}\pi^{1-p^{j+1}+sp^j}\quad (0\leqslant j\leqslant r+1),$$

$$h_i'^{(j)}(\pi)=\pi^{1+p^j-2p^{j+1}}+\sum_{s=1}^{p-2}\epsilon_s'^{(j)}\pi^{1+p^j-2p^{j+1}+sp^j}\quad (0\leqslant j\leqslant r)$$

in $\mathbf{F}[\pi][1/\pi]$ *with* $\epsilon_1^{(r+1)},\epsilon^{(r)}\neq 0$.

Proof. By Lemma 4.2 (with $v=r+1$, $s_v=c_{i+r+1}+2$) we get

$$(\lambda_\eta^{\Sigma_i}\eta-1)\pi^{1-p^{r+2}}\in\mathbf{F}^\times\pi^{1-p^{r+2}+p^{r+1}}+\pi^{1-p^{r+2}+2p^{r+1}}\mathbf{F}[[\pi^{p^{r+1}}]]$$

and

$$(\lambda_\eta^{\Sigma_i}\eta-1)\pi^{1-p^{r+2}+sp^{r+1}}\in\mathbf{F}^\times\pi^{1-p^{r+2}+sp^{r+1}}+\sum_{t=1}^{p-s-1}\mathbf{F}\pi^{1-p^{r+2}+(s+t)p^{r+1}}+\mathbf{F}[[\pi]]$$

for $1\leqslant s\leqslant p-2$, so that there exist unique $\epsilon_1^{(r+1)},\dots,\epsilon_{p-2}^{(r+1)},\nu^{(r+1)}\in\mathbf{F}$ such that

$$(\lambda_\eta^{\Sigma_i}\eta-1)\left(\pi^{1-p^{r+2}}+\sum_{s=1}^{p-2}\epsilon_s^{(r+1)}\pi^{1-p^{r+2}+sp^{r+1}}\right)\in\nu^{(r+1)}\pi^{1-p^{r+1}}+\mathbf{F}[[\pi]].$$

We set $h_i^{(r+1)}=\sum_{s=1}^{p-2}\epsilon_s^{(r+1)}\pi^{1-p^{r+2}+sp^{r+1}}$.

Again by Lemma 4.2 we get

$$(\lambda_\eta^{\Sigma_i}\eta-1)\pi^{1-2p^{r+1}+p^r}\in\ \mathbf{F}^\times\pi^{1-2p^{r+1}+2p^r}+\pi^{1-2p^{r+1}+3p^r}\mathbf{F}[[\pi^{p^r}]]$$

and

$$(\lambda_\eta^{\Sigma_i}\eta-1)\pi^{1-2p^{r+1}+(1+s)p^r}\in\mathbf{F}^\times\pi^{1-2p^{j+1}+(1+s)p^j}+\sum_{t=1}^{p-s-2}\mathbf{F}\pi^{1-2p^{r+1}+(1+s+t)p^r}+\pi^{1-p^{r+1}}\mathbf{F}[[\pi^{p^r}]]$$

for $1\leqslant s\leqslant p-2$, so that there exist unique $\epsilon_1'^{(r)},\dots,\epsilon_{p-2}'^{(r)},\nu'^{(r)}\in\mathbf{F}$ such that

$$(\lambda_\eta^{\Sigma_i}\eta-1)\left(\sum_{s=0}^{p-2}\epsilon_s'^{(r)}\pi^{1+p^r-2p^{r+1}+sp^r}\right)\in\nu'^{(r)}\pi^{1-p^{r+1}}+\pi^{1-p^{r+1}+p^r}\mathbf{F}[[\pi^{p^r}]],$$

where we have set $\epsilon_0'^{(r)}=1$.

As in the proof of Proposition 4.6, one can show that both $\nu^{(r+1)}$ and $\nu'^{(r)}$ are not zero, so that

$$(\lambda_\eta^{\Sigma_i}\eta-1)(\pi^{1-p^{r+2}}+h_i^{(r+1)}+\epsilon^{(r)}h_i'^{(r)})\in\pi^{1-p^{r+1}+p^r}\mathbf{F}[[\pi^{p^r}]],$$

where $\epsilon^{(r)}=-\nu^{(r+1)}/\nu'^{(r)}\neq 0$. Then again

$$(\lambda_\eta^{\Sigma_i}\eta-1)(\pi^{1-p^{r+2}}+h_i^{(r+1)}+\epsilon^{(r)}h_i'^{(r)}+h_i^{(r)})\in\mathbf{F}\pi^{1-p^r}+\mathbf{F}[[\pi]]$$

for some $h_i^{(r)}=\sum_{s=1}^{p-2}\epsilon_s^{(r)}\pi^{1-p^{r+1}+sp^r}$. Iterating the process proves the proposition. ∎

When $c_i=p-1$, $c_{i+1}=\cdots=c_{i+r}=p-2$, $c_{i+r+1}\neq p-2$, we define

$$\mu_\varphi(B_i)=(0,\dots,0,H_i(\pi),0,\dots,0),$$

https://doi.org/10.1112/S0010437X1000504X Published online by Cambridge University Press

where

$$H_i(\pi) = \pi^{1-p^{r+2}} + \sum_{j=1}^{r+1} h_i^{(j)}(\pi) + \sum_{j=0}^{r} \epsilon^{(j)} h_i'^{(j)}(\pi)$$

is the ith component. By Proposition 4.7, we get $(\lambda_\gamma^{\Sigma_i}\gamma - 1)(\mu_\varphi(B_i)) \in \mathbf{F}[[\pi]]$ and then $\mu_\gamma(B_i)$ is determined by bijectivity of the map $C\pi^{(p-1)\Sigma_i}\Phi - 1 : \mathbf{F}[[\pi]] \to \mathbf{F}[[\pi]]$. The condition (‡) is checked in an analogous fashion as in § 4.1.

Remark 4.8. The cocycle B_i for the case $c_i = p-1$, $c_{i+1} = \cdots = c_{i+r} = p-2$, $c_{i+r+1} \neq p-2$ is cohomologous to a cocycle B_i' defined by

$$\begin{aligned}
\mu_\varphi(B_i') = &\left(\epsilon^{(0)}\pi^{2-2p} \sum_{s=0}^{p-2} \epsilon_s'^{(0)}\pi^s + \pi^{1-p}\sum_{s=1}^{p-2}\epsilon_s^{(0)}\pi^s\right)e_i \\
&+ \left(\epsilon^{(1)}\pi^{3-3p} \sum_{s=0}^{p-2} \epsilon_s'^{(1)}\pi^s + \pi^{2-2p}\sum_{s=1}^{p-2}\epsilon_s^{(1)}\pi^s\right)e_{i+1} \\
&\vdots \\
&+ \left(\epsilon^{(r)}\pi^{3-3p} \sum_{s=0}^{p-2} \epsilon_s'^{(r)}\pi^s + \pi^{2-2p}\sum_{s=1}^{p-2}\epsilon_s^{(r)}\pi^s\right)e_{i+r} \\
&+ \left(\pi^{2-2p}\sum_{s=0}^{p-2}\epsilon_s^{(r+1)}\pi^s\right)e_{i+r+1},
\end{aligned}$$

where $\epsilon_0'^{(0)} = \epsilon_0'^{(1)} = \cdots = \epsilon_0'^{(r)} = \epsilon_0^{(r+1)} = 1$ and $\epsilon^{(r)} \neq 0$. See Lemma 5.7 for the proof in the case $f = 2$.

4.3 Linear independence of the $[B_i]$

Throughout this subsection we assume $C \neq 1$ if $\vec{c} = \vec{0}$, so that $C\pi^{(p-1)\Sigma_i}\Phi - 1 : \mathbf{F}[[\pi]] \to \mathbf{F}[[\pi]]$ defines a valuation-preserving bijection for all $i \in S$. From the constructions in §§ 4.1 and 4.2 we have at hand the extensions $[B_0], \ldots, [B_{f-1}] \in \mathrm{Ext}^1(M_0, M_{C\vec{c}})$ such that, if $i \in S$,

$$\mu_\varphi(B_i) = (0, \ldots, 0, H_i(\pi), \ldots, 0)$$

has ith component

$$H_i(\pi) = \pi^{1-p^{r+2}} + \sum_{j=0}^{r+1} h_i^{(j)}(\pi) + \sum_{j=0}^{r} \epsilon^{(j)} h_i'^{(j)}(\pi),$$

where, if $c_i \neq p-1$, then we set $r = -1$ and $h_i^{(0)}(\pi) = h_i(\pi)$ was defined in § 4.1, and, if $c_i = p-1$, then r is the least non-negative integer such that $c_{i+r+1} \neq p-2$ and $h_i^{(j)}$, $h_i^{(j)}$ and $\epsilon'^{(j)}$ were defined in § 4.2.

To prove linear independence of the $[B_i]$, suppose that $\beta_0 B_0 + \cdots + \beta_{f-1}B_{f-1}$ is a coboundary for some $\beta_0, \ldots, \beta_{f-1} \in \mathbf{F}$. We want to show that $\beta_0 = \cdots = \beta_{f-1} = 0$. By the cyclic nature of the indexing, it is enough to show that $\beta_{f-1} = 0$. Since $\beta_0\mu_\varphi(B_0) + \cdots + \beta_{f-1}\mu_\varphi(B_{f-1}) = (\beta_0 H_0(\pi), \ldots, \beta_{f-1}H_{f-1}(\pi))$, by adding another coboundary, we see that

$$\begin{aligned}
&(\beta_0 H_0(\pi) + \beta_1 C\pi^{(p-1)c_0} H_1(\pi^p) + \cdots + \beta_{f-1} C\pi^{(p-1)\sum_{j=0}^{f-2} c_j p^j} H_{f-1}(\pi^{p^{f-1}}), 0, \ldots, 0) \\
&\quad = (C\pi^{(p-1)c_0} b_1(\pi^p) - b_0(\pi), \pi^{(p-1)c_1} b_2(\pi) - b_1(\pi), \ldots, \pi^{(p-1)c_{f-1}} b_0(\pi^p) - b_{f-1}(\pi))
\end{aligned}$$

for some $(b_0(\pi), \ldots, b_{f-1}(\pi)) \in \mathbf{F}((\pi))^S$. It follows that

$$\begin{aligned}&\beta_0 H_0(\pi) + \beta_1 C\pi^{(p-1)c_0} H_1(\pi^p) + \cdots + \beta_{f-1} C\pi^{(p-1)\sum_{j=0}^{f-2} c_j p^j} H_{f-1}(\pi^{p^{f-1}})\\ &\quad = (C\pi^{(p-1)\Sigma_0}\Phi - 1)(b_0(\pi))\end{aligned}$$

and

$$\begin{aligned} b_1(\pi) &= \pi^{(p-1)c_1} b_2(\pi^p),\\ b_2(\pi) &= \pi^{(p-1)c_2} b_3(\pi^p),\\ &\vdots\\ b_{f-2}(\pi) &= \pi^{(p-1)c_{f-2}} b_{f-1}(\pi^p),\\ b_{f-1}(\pi) &= \pi^{(p-1)c_{f-1}} b_0(\pi^p).\end{aligned}$$

As the map $C\pi^{(p-1)\Sigma_0}\Phi - 1 : \mathbf{F}[[\pi]] \to \mathbf{F}[[\pi]]$ is a bijection, we get a congruence

$$\begin{aligned}&\beta_0 H_0(\pi) + \beta_1 C\pi^{(p-1)c_0} H_1(\pi^p) + \cdots + \beta_{f-1} C\pi^{(p-1)\sum_{j=0}^{f-2} c_j p^j} H_{f-1}(\pi^{p^{f-1}})\\ &\quad \equiv (C\pi^{(p-1)\Sigma_0}\Phi - 1)(b(\pi)) \mod \mathbf{F}[[\pi]]\end{aligned}$$

for some $b(\pi) = b_{-s}\pi^{-s} + \sum_{j=1}^{s-1} b_{-s+j}\pi^{-s+j} \in \mathbf{F}[1/\pi]$ with $s > 0$ and $b_{-s} \neq 0$. Suppose $\beta_{f-1} \neq 0$ and we will get contradictions.

First assume $c_{f-1} = p-1, c_f = \cdots = c_{f-1+r} = p-2, c_{f+r} \neq p-2$ with $r > 0$, in which case we have

$$H_{f-1}(\pi) = \pi^{1-p^{r+2}} + \sum_{j=0}^{r+1} h_i^{(j)}(\pi) + \sum_{j=0}^{r} \epsilon^{(j)} h_i'^{(j)}(\pi).$$

One can check that the lowest degree term (in π) of the left-hand side of the congruence is

$$\beta_{f-1} C\pi^{(p-1)\sum_{j=0}^{f-2} c_j p^j} \pi^{(1-p^{r+2})p^{f-1}},$$

so that the valuation of the left-hand side is $(p-1)(\sum_{j=0}^{f-2} c_j p^j - (1 + p + \cdots + p^{r+1})p^{f-1})$. On the other hand, we have three possibilities for the right-hand side: $(p-1)\Sigma_0 - sp^f < -s$, $-s < (p-1)\Sigma_0 - sp^f$ and $(p-1)\Sigma_0 - sp^f = -s$.

If $(p-1)\Sigma_0 - sp^f < -s$, the leading term of the right-hand side is $b_{-s}C\pi^{(p-1)\Sigma_0}\pi^{-sp^f}$ and we have $s = (p-1)(2 + p + \cdots + p^r)$ and $\beta_{f-1} = b_{-s}$. Now the term

$$\beta_{f-1} C\pi^{(p-1)\sum_{j=0}^{f-2} c_j p^j} \epsilon^{(r)} \pi^{(1+p^r-2p^{r+1})p^{f-1}}$$

survives on the left-hand side and must match a term on the right-hand side. Considering possible matching valuations on the right-hand side we get either

$$(p-1)\sum_{j=0}^{f-2} c_j p^j + (1 + p^r - 2p^{r+1})p^{f-1} = -t$$

or

$$(p-1)\sum_{j=0}^{f-2} c_j p^j + (1 + p^r - 2p^{r+1})p^{f-1} = (p-1)\Sigma_0 - tp^f$$

for some $0 < t < s = (p-1)(2 + p + \cdots + p^r)$. The former equation contradicts the inequality $t < s$ and the latter implies that $t = 2p^r - p^{r-1} + p - 2$. Since $p^f \nmid t + (p-1)\Sigma_0$, there must be a term of degree $-t$ on the left-hand side. However, if $m < r$, then the leading term

https://doi.org/10.1112/S0010437X1000504X Published online by Cambridge University Press

of $\pi^{(p-1)\sum_{j=0}^{m-1} c_j p^j} H_m(\pi^{p^m})$ has degree greater than $-t$, and, if $m \geqslant r$, then its terms cannot be congruent to $-t \bmod p^r$, and we again arrive at a contradiction.

If $-s < (p-1)\Sigma_0 - sp^f$, the leading term of the right-hand side is $-b_{-s}\pi^{-s}$. Then $(p-1)|s$ and $s(p^f-1)/(p-1) < \Sigma_0 < p^f - 1$, so that $s < 1$, which is impossible.

Lastly, if $(p-1)\Sigma_0 - sp^f = -s$, working modulo powers of p, we get $s = c_0 = \cdots = c_{f-1} = p-1$, a contradiction.

Now we may assume that $\beta_j = 0$ for all $j \in S$ such that $c_j = p-1$ and $c_{j+1} = p-2$. Suppose now that $c_{f-1} = p-1$ and $c_0 \neq p-2$. We then proceed to show that $\beta_{f-1} = 0$ by induction on m, where $m \geqslant 1$ is such that $c_{f-m-1} \neq p-1$ and $c_{f-m} = c_{f-m+1} = \cdots c_{f-1} = p-1$. We may thus assume that $\beta_{f-m} = \cdots = \beta_{f-2} = 0$ if $m \geqslant 2$. The argument used in the case $r > 0$ then goes through with the following two changes: (1) the induction hypothesis is used to show that the term

$$\beta_{f-1} C \pi^{(p-1)\sum_{j=0}^{f-2} c_j p^j} \epsilon^{(0)} \pi^{(2-2p)p^{f-1}}$$

is alive on the left-hand side, and (2) the equality

$$(p-1)\sum_{j=0}^{f-2} c_j p^j + (2-2p)p^{f-1} = (p-1)\Sigma_0 - tp^f$$

immediately gives a contradiction without considering more terms.

Now we may assume that $\beta_j = 0$ for all $j \in S$ such that $c_j = p-1$, and suppose $c_{f-1} < p-1$. The leading term of the left-hand side then is

$$\beta_{f-1} C \pi^{(p-1)\sum_{j=0}^{f-2} c_j p^j} \pi^{(1-p)p^{f-1}}.$$

If $(p-1)\Sigma_0 - sp^f < -s$, $sp^f = (p-1)(\Sigma_0 - \sum_{j=0}^{f-2} c_j p^j + p^{f-1}) = (p-1)(c_{f-1}+1)p^{f-1}$, and so $p|(c_{f-1}+1)$, which is impossible as $0 \leqslant c_{f-1} < p-1$. If $(p-1)\Sigma_0 - sp^f \geqslant -s$, then

$$-s \leqslant (p-1)\left(\sum_{j=0}^{f-2} c_j p^j - p^{f-1}\right) \leqslant 1 - p,$$

contradicting that $s(p^f-1)/(p-1) \leqslant \Sigma_0 < p^f - 1$.

This completes the proof that the $[B_i]$ are linearly independent, hence form a basis for $\mathrm{Ext}^1(M_0, M_{C\vec{c}})$ (unless $C = 1, \vec{c} = \vec{0}$ or $C = 1, \vec{c} = \overline{p-2}$).

5. The space of bounded extensions

In this section we define bounded extensions, which we will later relate to extensions arising from crystalline representations.

5.1 Bounded extensions

Definition 5.1. Suppose $A, B \in \mathbf{F}^\times$ and $0 \leqslant a_i, b_i \leqslant p$ with exactly one of a_i or b_i being zero for each $i \in S$. We say that an extension (class) $E \in \mathrm{Ext}^1(M_{A\vec{a}}, M_{B\vec{b}})$ is *bounded* if there exists a basis for E such that the defining matrices P and G_γ satisfy the following:

(i) $P = \begin{pmatrix} \kappa_\varphi(B,\vec{b}) & * \\ 0 & \kappa_\varphi(A,\vec{a}) \end{pmatrix}$ and $G_\gamma = \begin{pmatrix} \kappa_\gamma(B,\vec{b}) & * \\ 0 & \kappa_\gamma(A,\vec{a}) \end{pmatrix}$ if $\gamma \in \Gamma$;

(ii) $P \in \mathrm{M}_2(\mathbf{F}[[\pi]]^S)$; and

(iii) $G_\gamma - I_2 \in \pi\mathrm{M}_2(\mathbf{F}[[\pi]]^S)$ if $\gamma \in \Gamma_1$.

https://doi.org/10.1112/S0010437X1000504X Published online by Cambridge University Press

Bounded extensions form a subspace, denoted by $\mathrm{Ext}^1_{\mathrm{bdd}}(M_{A\vec{a}}, M_{B\vec{b}})$, of the full space $\mathrm{Ext}^1(M_{A\vec{a}}, M_{B\vec{b}})$ of extensions.

Remark 5.2. Note that the space $\mathrm{Ext}^1_{\mathrm{bdd}}(M_{A\vec{a}}, M_{B\vec{b}})$ depends on $\vec{a}$ and $\vec{b}$ and not just on the isomorphism classes of the (φ, Γ)-modules $M_{A\vec{a}}$ and $M_{B\vec{b}}$.

LEMMA 5.3. *The condition (iii) in Definition 5.1 can be replaced by a weaker condition (iii′) $G_\xi - I_2 \in \pi\mathrm{M}_2(\mathbf{F}[[\pi]]^S)$. (Recall that ξ is a topological generator of Γ_1.)*

Proof. If $\gamma, \gamma' \in \Gamma_1$, then

$$G_{\gamma\gamma'} = G_\gamma \gamma G_{\gamma'} \equiv \begin{pmatrix} 1 & \mu_\gamma(E) + \gamma\mu_{\gamma'}(E) \\ 0 & 1 \end{pmatrix} \mod \pi$$

by Lemma 4.3. So, if $G_\xi = I_2 \bmod \pi$, we have by induction that $G_{\xi^n} \equiv I_2$ for all $n \geqslant 1$. Since $\langle \xi \rangle$ is dense in Γ_1, continuity of the action gives that $G_\gamma - I_2 \in \pi\mathrm{M}_2(\mathbf{F}[[\pi]]^S)$ for all $\gamma \in \Gamma_1$. □

We now describe a way to analyze extensions systematically and to check for boundedness. Given $J \subset S$ and $n \in \mathbf{Z}/(p^f - 1)\mathbf{Z}$, we can always find a_i, b_j for $i \in J,\ j \in S - J$ with $1 \leqslant a_i, b_j \leqslant p$ such that

$$n \equiv \sum_{j \notin J} b_j p^j - \sum_{i \in J} a_i p^i \mod p^f - 1.$$

The congruence has a unique solution if $n \not\equiv n_J \bmod p^f - 1$, and has two solutions if $n \equiv n_J \bmod p^f - 1$, where $n_J := \sum_{i \in J} p^{i+1} - \sum_{i \notin J} p^i$ (cf. [BDJ10, § 3]). To compute the solutions explicitly in the double solution case, suppose $n \equiv n_J \bmod p^f - 1$ and we have two solutions a_i, b_j and a'_i, b'_j. Then $\Sigma := \sum_{j \notin J}(b_j - b'_j)p^j - \sum_{i \in J}(a_i - a'_i)p^i \equiv 0 \bmod p^f - 1$. Note that $|\Sigma| \leqslant p^f - 1$, as $|a_i - a'_i|, |b_j - b'_j| \leqslant p - 1$, so that $\Sigma = 0$ or $\pm(p^f - 1)$, and in the latter case we can exchange $\vec{a}, \vec{b}$ and $\vec{a}', \vec{b}'$ if necessary in order to assume $\Sigma = p^f - 1$. If $\Sigma = 0$, then reducing modulo powers of p shows that $\vec{a} = \vec{a}'$ and $\vec{b} = \vec{b}'$. If $\Sigma = p^f - 1$, then we have solutions $a_i = 1, b_j = p$ and $a'_i = p, b'_j = 1$ $(i \in J,\ j \in S - J)$.

Now fix $J \subset S$, $C \in \mathbf{F}^\times$ and $\vec{c} \in \{0, 1, \ldots, p-1\}^S$ with some $c_i < p - 1$. If $\Sigma_0\vec{c} \not\equiv n_J \bmod p^f - 1$, we can solve the congruence $\Sigma_0\vec{c} \equiv \sum_{i \notin J} b_i p^i - \sum_{i \in J} a_i p^i \bmod p^f - 1$ with unique solution, and get an isomorphism

$$\mathrm{Ext}^1(M_{\vec{0}}, M_{C\vec{c}}) \simeq \mathrm{Ext}^1(M_{\vec{0}}, M_{C\vec{d}}),$$

where $d_i = -a_i$ if $i \in J$ and $d_j = b_j$ if $j \notin J$. The isomorphism is (not canonical but) well-defined up to $\mathrm{Aut}\, M_{C\vec{c}} = \mathbf{F}^\times$ and the valuations of entries of the matrices defining the (φ, Γ)-module extensions are invariant, which suffices for our purposes. Tensoring $M_{A\vec{a}}$ with the subobject and the quotient of the extension gives an isomorphism

$$\iota : \mathrm{Ext}^1(M_{\vec{0}}, M_{C\vec{c}}) \to \mathrm{Ext}^1(M_{A\vec{a}}, M_{B\vec{b}}),$$

where $CA = B$ and $a_i = 0$ if $i \notin J$ and $b_i = 0$ if $i \in J$. Note that, if $J = \emptyset$, $A = 1$ and $c_i > 0$ for all i, then $M_{A\vec{a}} = M_0$, $M_{B\vec{b}} = M_{C\vec{c}} = M_{C\vec{d}}$ and ι is the identity. In general, we have the following commutative diagram.

$$\begin{tikzcd} H/H_0 \arrow[r] \arrow[d] & H'/H'_0 \arrow[d] \\ \mathrm{Ext}^1(M_{\vec{0}}, M_{C\vec{c}}) \arrow[r] & \mathrm{Ext}^1(M_{A\vec{a}}, M_{B\vec{b}}) \end{tikzcd}$$

https://doi.org/10.1112/S0010437X1000504X Published online by Cambridge University Press

The vertical arrows are the isomorphisms β defined at the beginning of § 4, and the bottom arrow, which we also denote ι, is induced by

$$(\mu_\varphi, (\mu_\gamma)_{\gamma\in\Gamma}) \mapsto (\kappa_\varphi(A,\vec{a})\langle\vec{c}\,\rangle_J\mu_\varphi, (\kappa_\gamma(A,\vec{a})\langle\vec{c}\,\rangle_J\mu_\gamma)_{\gamma\in\Gamma}),$$

where the isomorphism $\mathbf{E}_{K,F}e = M_{C\vec{c}} \simeq M_{C\vec{d}} = \mathbf{E}_{K,F}e'$ is defined by the change of basis $e = \langle\vec{c}\,\rangle_J e'$ with $\langle\vec{c}\,\rangle_J \in \mathbf{E}_{K,F}^\times$. It is straighforward to check the following formula for $\langle\vec{c}\,\rangle_J$, which we will need in order to compute spaces of bounded extensions:

$$\langle\vec{c}\,\rangle_J = (\pi^{(p-1)\varepsilon_0}, \dots, \pi^{(p-1)\varepsilon_{f-1}}),$$

where $(p^f-1)\varepsilon_i = \Sigma_i(\vec{c}-\vec{d})$.

We define

$$V_J = \iota^{-1}(\mathrm{Ext}^1_{\mathrm{bdd}}(M_{A\vec{a}}, M_{B\vec{b}})) \subset \mathrm{Ext}^1(M_{\vec{0}}, M_{C\vec{c}}),$$

so that $\dim_{\mathbf{F}} V_J = \dim_{\mathbf{F}} \mathrm{Ext}^1_{\mathrm{bdd}}(M_{A\vec{a}}, M_{B\vec{b}})$.

If $\Sigma_0\vec{c} \equiv n_J \bmod p^f-1$, we can assume that $n_J = \sum_{i\notin J} b_ip^i - \sum_{i\in J} a_ip^i$ and $n_J + 1 - p^f = \sum_{i\notin J} b'_ip^i - \sum_{i\in J} a'_ip^i$ where a_i, b_j and a'_i, b'_j are two solutions. Then we have $a_i = p,\ b_j = 1$ and $a'_i = 1,\ b'_j = p$ (for $i\in J$ and $j \in S-J$).

As in the case of a unique solution, we have isomorphisms (but now there are two)

$$\iota_+ : \mathrm{Ext}^1(M_{\vec{0}}, M_{C\vec{c}}) \to \mathrm{Ext}^1(M_{A\vec{a}}, M_{B\vec{b}}),$$
$$\iota_- : \mathrm{Ext}^1(M_{\vec{0}}, M_{C\vec{c}}) \to \mathrm{Ext}^1(M_{A\vec{a}'}, M_{B\vec{b}'})$$

and define

$$V_J^+ = \iota_+^{-1}(\mathrm{Ext}^1_{\mathrm{bdd}}(M_{A\vec{a}}, M_{B\vec{b}})) \subset \mathrm{Ext}^1(M_{\vec{0}}, M_{C\vec{c}}),$$
$$V_J^- = \iota_-^{-1}(\mathrm{Ext}^1_{\mathrm{bdd}}(M_{A\vec{a}'}, M_{B\vec{b}'})) \subset \mathrm{Ext}^1(M_{\vec{0}}, M_{C\vec{c}}).$$

Note that we always use $+$ to denote the case where all $a_i = p$, $b_j = 1$, and $-$ for the case where all $a_i = 1$ and $b_j = p$.

In the next two subsections we will compute explicitly the spaces of bounded extensions in the generic case and in the case $f = 2$.

5.2 Generic case

For each $i \in S$, let $e_i : \mathbf{E}_{K,F} = \mathbf{F}((\pi))^S \to \mathbf{F}((\pi))$ denote the projection $(g_0, \dots, g_{f-1}) \mapsto g_i$.

Proposition 5.4. *If $0 < c_i < p-1$ for all $i \in S$, then:*

(i) $V_{\{i\}} = \mathbf{F}[B_{i+1}]$ *for all $i \in S$;*

(ii) $V_J = \bigoplus_{i\in J} V_{\{i\}}$ *if $J \subset S$; and*

(iii) $V_S^+ = V_S^- = \mathrm{Ext}^1(M_{\vec{0}}, M_{C\overrightarrow{p-2}})$ *if $C \neq 1, \vec{c} = \overrightarrow{p-2}$.*

Remark 5.5. Proposition 5.4 does not say anything about the cyclotomic case $C = 1, \vec{c} = \overrightarrow{p-2}$, which will be treated in § 6.1.

Proof. First consider the case $J \neq \emptyset$. We may assume that $f-1 \in J$; even though we do not have complete symmetry due to the presence of the constant C, we will see that the argument goes through independently of which component C lies in. As $0 < c_i < p-1$ for all $i \in S$ we have $(p^f-1)/(p-1) \leqslant \Sigma_0\vec{c} \leqslant (p-2)(p^f-1)/(p-1)$. We claim that the congruence

$$\Sigma_0\vec{c} \equiv \sum_{i\notin J} b_ip^i - \sum_{i\in J} a_ip^i \mod p^f - 1$$

https://doi.org/10.1112/S0010437X1000504X Published online by Cambridge University Press

has a unique solution a_i, b_j $(i \in J,\ j \notin J)$ such that $1 \leqslant a_i, b_j \leqslant p$, except when $J = S$ and $\vec{c} = \overrightarrow{p-2}$. If there were another distinct solution, we have either $\Sigma_0\vec{c} = \sum_{j\notin J} p^{j+1} - \sum_{j\in J} p^j$ or $\Sigma_0\vec{c} = \sum_{j\notin J} p^{j+1} - \sum_{j\in J} p^j + p^f - 1$. The former is impossible since modulo p we have $c_0 \equiv -1$ if $0 \in J$ and $c_0 \equiv 0$ if $j \notin J$, and thus $c_0 = p-1$ or 0, contradicting the assumption. In the latter case, we have $0 \in J$ and $c_0 = p-2$. Computations modulo p^2 show that $1 \in J$ and $c_1 = p-2$. By induction we get $J = S$ and $c_i = p-2$ for all $i \in S$. Thus, unless $J = S$, $\vec{c} = \overrightarrow{p-2}$, we have unique a_i, b_j $(i \in J,\ j \notin J)$ satisfying the equation $\sum_{i=0}^{f-1} c_i p^i = \sum_{i\notin J} b_i p^i - \sum_{i\in J} a_i p^i + p^f - 1$. Letting $u = (\pi^{(p-1)\delta_{f-1J}}, \pi^{(p-1)\delta_{0J}}, \ldots, \pi^{(p-1)\delta_{f-2J}})$ with $\delta_{iJ} = 1$ if $i \in J$ and $\delta_{iJ} = 0$ otherwise, one can check that $\mathbf{E}_{K,F}e = M_{C\vec{c}} \simeq M_{C\vec{d}} = \mathbf{E}_{K,F}e'$ via the change of basis $e = ue'$, where $d_i = b_i$ if $i \notin J$ and $d_i = -a_i$ if $i \in J$, and that $\langle \vec{c}\,\rangle_J = u$. Note that

$$\begin{aligned}\frac{\varphi(\langle \vec{c}\,\rangle_J)}{\langle \vec{c}\,\rangle_J} &= \frac{(\pi^{(p-1)p\delta_{0J}}, \pi^{(p-1)p\delta_{1J}}, \ldots, \pi^{(p-1)p\delta_{f-1J}})}{(\pi^{(p-1)\delta_{f-1J}}, \pi^{(p-1)\delta_{0J}}, \ldots, \pi^{(p-1)\delta_{f-2J}})}\\ &= (\pi^{(p-1)(p\delta_{0J}-\delta_{f-1J})}, \pi^{(p-1)(p\delta_{1J}-\delta_{0J})}, \ldots, \pi^{(p-1)(p\delta_{f-1J}-\delta_{f-2J})})\end{aligned}$$

and that

$$(p\delta_{0J} - \delta_{f-1J}) + p(p\delta_{1J} - \delta_{0J}) + \cdots + p^{f-1}(p\delta_{f-1J} - \delta_{f-2J}) = (p^f - 1)\delta_{f-1J} = p^f - 1.$$

Recall that we have a basis $[B_0], \ldots, [B_{f-1}]$ for $\mathrm{Ext}^1(M_{\vec{0}}, M_{C\vec{c}})$ such that

$$\begin{aligned}\mu_\varphi(B_i) &= (0, \ldots, 0, \pi^{1-p} + h_i(\pi), 0, \ldots, 0),\\ \mu_\xi(B_i) &= (G_0^{(i)}, \ldots, G_{f-1}^{(i)}),\end{aligned}$$

where $h_i(\pi) \in \mathbf{F}\pi^{2-p} + \cdots + \mathbf{F}\pi^{-1}$ and

$$\begin{aligned}G_i^{(i)}(\pi) &= -\alpha_i + g_i(\pi),\\ G_{i-1}^{(i)}(\pi) &= \pi^{(p-1)c_{i-1}}(-\alpha_i + g_i(\pi^p)),\\ G_{i-2}^{(i)}(\pi) &= \pi^{(p-1)(c_{i-2}+c_{i-1}p)}(-\alpha_i + g_i(\pi^{p^2})),\\ &\vdots\\ G_0^{(i)}(\pi) &= \pi^{(p-1)(c_0+c_1p+\cdots+c_{i-1}p^{i-1})}(-\alpha_i + g_i(\pi^{p^i})),\\ G_{f-1}^{(i)}(\pi) &= \pi^{(p-1)(c_{f-1}+c_0p+c_1p^2+\cdots+c_{i-1}p^i)}(-\alpha_i + g_i(\pi^{p^{i+1}})),\\ &\vdots\\ G_{i+1}^{(i)}(\pi) &= \pi^{(p-1)(c_{i+1}+\cdots+c_{i-1}p^{f-2})}(-\alpha_i + g_i(\pi^{p^{f-1}})),\end{aligned}$$

with $\alpha_i = \overline{s_0 z} \in \mathbf{F}^\times$ as in Lemma 4.4.

To show that $\iota[B_{i+1}] \in \mathrm{Ext}^1(M_{A\vec{a}}, M_{B\vec{b}})$ is bounded if $i \in J$ is straightforward: as $\langle \vec{c}\,\rangle_J = (\pi^{(p-1)\delta_{f-1J}}, \pi^{(p-1)\delta_{0J}}, \ldots, \pi^{(p-1)\delta_{f-2J}})$ and $\delta_{iJ} = 1$, we have

$$\begin{aligned}\mu_\varphi(\iota B_{i+1}) &= \kappa_\varphi(A, \vec{a})\langle \vec{c}\,\rangle_J \mu_\varphi(B_{i+1})\\ &= (0, \ldots, 0, \pi^{(p-1)(a_{i+1}+1)}(\pi^{1-p} + h_{i+1}(\pi)), 0, \ldots, 0) \in \mathbf{F}[[\pi]]^S\end{aligned}$$

with the non-zero entry in the $(i+1)$th component, and

$$\mu_\xi(\iota B_{i+1}) = \kappa_\xi(A, \vec{a})\langle \vec{c}\,\rangle_J \mu_\xi(B_{i+1}) \in \pi\mathbf{F}[[\pi]]^S$$

as $e_{i+1}\mu_\xi(\iota B_{i+1}) = \lambda_\xi^{(p-1)\Sigma_{j+1}\vec{a}}\pi^{p-1}G_{i+1}^{(i)}$ and $e_{j+1}\mu_\xi(\iota B_{i+1}) = \lambda_\xi^{(p-1)\Sigma_{j+1}\vec{a}}\pi^{(p-1)\delta_{jJ}}G_{j+1}^{(i)}$ is divisible by $\pi^{(p-1)c_{j+1}}$ if $j \neq i$.

https://doi.org/10.1112/S0010437X1000504X Published online by Cambridge University Press

Next we need to show that, if $E=\sum_{j=0}^{f-1}\beta_j B_j$ and $[E]\in V_J$, then $\beta_{i+1}=0$ for all $i\notin J$. Suppose $\iota[E]$ is bounded, $i\notin J$ and $\beta_{i+1}\neq 0$. Then $\mu_\varphi\iota(E+B)\in \mathbf{F}[[\pi]]^S$ and $\mu_\xi\iota(E+B)\in \pi\mathbf{F}[[\pi]]^S$ for some coboundary B, for which we have

$$\mu_\varphi(B)=(C\pi^{(p-1)c_0}b_1(\pi^p)-b_0,\pi^{(p-1)c_1}b_2(\pi^p)-b_1,\ldots,\pi^{(p-1)c_{f-1}}b_0(\pi^p)-b_{f-1}),$$
$$\mu_\xi(B)=((\lambda_\xi^{\Sigma_0\vec{c}}\xi-1)b_0(\pi),(\lambda_\xi^{\Sigma_1\vec{c}}\xi-1)b_1(\pi)\ldots,(\lambda_\xi^{\Sigma_{f-1}\vec{c}}\xi-1)b_{f-1}(\pi)),$$

for some $(b_0(\pi),\ldots,b_{f-1}(\pi))\in\mathbf{E}_{K,F}$. Note that $\kappa_\xi(A,\vec{a})\equiv 1=(1,\ldots,1) \bmod \pi$ and $e_{i+1}\langle\vec{c}\,\rangle_J=\pi^{(p-1)\delta_{iJ}}=1$. As $\mathrm{val}_\pi e_{i+1}\mu_\xi(E+B)=\mathrm{val}_\pi e_{i+1}\mu_\xi\iota(E+B)\geqslant 1$ while $\mathrm{val}_\pi e_{i+1}\mu_\xi(E)=0$, the valuation of $e_{i+1}\mu_\xi(B)=(\lambda_\xi^{\Sigma_{i+1}}\xi-1)b_{i+1}(\pi)$ has to be zero. Letting $s=\mathrm{val}_\pi b_{i+1}(\pi)$, Lemma 4.4 implies that $(\lambda_\xi^{\Sigma_{i+1}\vec{c}}\xi-1)b_{i+1}(\pi)\in\pi\mathbf{F}[[\pi]]$ if $s\geqslant 0$, and $\mathrm{val}_\pi(\lambda_\xi^{\Sigma_{i+1}\vec{c}}\xi-1)b_{i+1}(\pi)=s+(p-1)p^v$ if $s<0$ and $\Sigma_{i+1}\vec{c}+s(p^f-1)/(p-1)$ is divisible by p^v but not p^{v+1}. Thus $\mathrm{val}_\pi b_{i+1}(\pi)$ must be negative and divisible by $p-1$. Looking at the ith component, we have

$$\begin{aligned}e_i\mu_\varphi(\iota(E+B))&=\pi^{(p-1)(a_i+\delta_{i-1J})}(e_i\mu_\varphi(E)+e_i\mu_\varphi(B))\\&=\pi^{(p-1)\delta_{i-1J}}(\pi^{1-p}+h_i(\pi)+\pi^{(p-1)c_i}b_{i+1}(\pi^p)-b_i(\pi)),\end{aligned}$$

whose valuation has to be non-negative. Since $(p-1)c_i+p\,\mathrm{val}_\pi b_{i+1}(\pi)<1-p=\mathrm{val}_\pi(\pi^{1-p}+h_i(\pi))$, we get $\mathrm{val}_\pi b_i(\pi)=(p-1)c_i+p\,\mathrm{val}_\pi b_{i+1}(\pi)$. Cycling this through all $j\in S$ leads to $\mathrm{val}_\pi b_{i+1}(\pi)=(p-1)\Sigma_i\vec{c}+p^f\mathrm{val}_\pi b_{i+1}(\pi)$, so that $\mathrm{val}_\pi b_{i+1}(\pi)=-(p-1)\Sigma_i\vec{c}/(p^f-1)>1-p$, which is a contradiction.

Now suppose $J=S$, $C\neq 1$, $\vec{c}=\overrightarrow{p-2}$. In this case we have two solutions $\vec{a}=\vec{p},\vec{b}=\vec{0}$ and $\vec{a}'=\vec{1},\vec{b}'=\vec{0}$ of the congruence and the corresponding isomorphisms

$$\begin{aligned}\iota_+&:\mathrm{Ext}^1(M_{\vec{0}},M_{C\overrightarrow{p-2}})\to\mathrm{Ext}^1(M_{A\vec{p}},M_{B\vec{0}}),\\ \iota_-&:\mathrm{Ext}^1(M_{\vec{0}},M_{C\overrightarrow{p-2}})\to\mathrm{Ext}^1(M_{A\vec{1}},M_{B\vec{0}}).\end{aligned}$$

One can show that $V_J^+=V_J^-=\mathrm{Ext}^1(M_{\vec{0}},M_{C\overrightarrow{p-2}})$ by straightforward computations.

If $J=\emptyset$, the congruence equation has a unique solution unless $\vec{c}=\vec{1}$, in which case we have two solutions $\vec{a}=\vec{0},\vec{b}=\vec{1}$ and $\vec{a}'=\vec{0},\vec{b}'=\vec{p}$. The proof that $V_\emptyset=0$ (when $\vec{c}\neq\vec{1}$) and $V_\emptyset^+=V_\emptyset^-=0$ (when $\vec{c}=\vec{1}$) is similar to the case $J\neq\emptyset$. □

5.3 Case $f=2$

Throughout this subsection we assume that $f=2$, $0\leqslant c_0,c_1\leqslant p-1$, not both $p-1$. If $\vec{c}=\vec{0}$ or $\overrightarrow{p-2}$, we further assume $C\neq 1$; the cases $\vec{c}=\vec{0}$ and $\vec{c}=\overrightarrow{p-2}$ when $C=1$ are dealt with in §§ 6.1 and 6.2. Before determining which extensions are bounded, we describe the basis elements in the form we will need. Recall that we defined a basis $\{[B_0],[B_1]\}$ for $\mathrm{Ext}^1(M_{\vec{0}},M_{C\vec{c}})$, where B_0 and B_1 are cocycles of the following form:

$$\begin{aligned}\mu_\varphi(B_0)&=(H_0(\pi),0),\\ \mu_\xi(B_0)&=(G_0^{(0)}(\pi),G_1^{(0)}(\pi))\\&=((C\pi^{(p-1)\Sigma_0}\Phi-1)^{-1}((\lambda_\xi^{\Sigma_0}\xi-1)H_0(\pi)),\pi^{(p-1)c_1}G_0^{(0)}(\pi^p)),\\ \mu_\varphi(B_1)&=(0,H_1(\pi)),\\ \mu_\xi(B_1)&=(G_0^{(1)}(\pi),G_1^{(1)}(\pi))\\&=(\pi^{(p-1)c_0}G_1^{(1)}(\pi^p),(C\pi^{(p-1)\Sigma_1}\Phi-1)^{-1}((\lambda_\xi^{\Sigma_1}\xi-1)H_1(\pi))),\end{aligned}$$

https://doi.org/10.1112/S0010437X1000504X Published online by Cambridge University Press

where

$$H_0(\pi)=\begin{cases}\pi^{1-p}+h_0 & \text{if } c_0<p-1,\\ \pi^{1-p^2}+h_0^{(1)}+\epsilon^{(0)}h_0'^{(0)}+h_0^{(0)} & \text{if } c_0=p-1,\, c_1\neq p-2,\\ \pi^{1-p^3}+h_0^{(2)}+\epsilon^{(1)}h_0'^{(1)}+h_0^{(1)}+\epsilon^{(0)}h_0'^{(0)}+h_0^{(0)} & \text{if } c_0=p-1,\, c_1=p-2,\end{cases}$$

$$H_1(\pi)=\begin{cases}\pi^{1-p}+h_1 & \text{if } c_1<p-1,\\ \pi^{1-p^2}+h_1^{(1)}+\epsilon^{(0)}h_1'^{(0)}+h_1^{(0)} & \text{if } c_1=p-1,\, c_0\neq p-2,\\ \pi^{1-p^3}+h_1^{(2)}+\epsilon^{(1)}h_1'^{(1)}+h_1^{(1)}+\epsilon^{(0)}h_1'^{(0)}+h_1^{(0)} & \text{if } c_1=p-1,\, c_0=p-2.\end{cases}$$

LEMMA 5.6. *Suppose that $i\in\{0,1\}$ is such that $0\leqslant c_i<p-1$. Then for some $\alpha_i\in F^\times$, $g_i(\pi)\in 1+\pi\mathbf{F}[[\pi]]$, we have*

$$\left.\begin{aligned}\mu_\varphi(B_0)&=(\pi^{1-p}+h_0(\pi),0),\\ \mu_\xi(B_0)&=(\alpha_0g_0(\pi),\pi^{(p-1)c_1}\alpha_0g_0(\pi^p))\end{aligned}\right\}\quad \textit{if } i=0,$$

$$\left.\begin{aligned}\mu_\varphi(B_1)&=(0,\pi^{1-p}+h_1(\pi)),\\ \mu_\xi(B_1)&=(C\pi^{(p-1)c_0}\alpha_1g_1(\pi^p),\alpha_1g_1(\pi))\end{aligned}\right\}\quad \textit{if } i=1.$$

Proof. We assume $i=0$; the case $i=1$ is similar. As in Lemma 4.4, we have

$$L_0(\pi):=(\lambda_\xi^{\Sigma_0}\xi-1)(\pi^{1-p}+h_0(\pi))\equiv\overline{s_0z}\mod \pi\mathbf{F}[[\pi]],$$

so that $e_0\mu_\xi(B_0)=(C\pi^{(p-1)\Sigma_0}\Phi-1)^{-1}(L_0(\pi))=\alpha_0g_0(\pi)$ for some $g_0(\pi)\in 1+\pi\mathbf{F}[[\pi]]$ with $\alpha_0=(C-1)^{-1}\overline{s_0z}$ if $c_0=c_1=0$, and $\alpha_0=-\overline{s_0z}$ otherwise. (Recall that we assume for now that $C\neq 1$ if $c_0=c_1=0$.) $\square$

If $c_i=p-1$, we introduce a cocycle B_i' cohomologous to B_i, which we will work with.

LEMMA 5.7. *Suppose that $\{i,j\}=\{0,1\}$ with $c_i=p-1$ and $c_j<p-2$. Then there is a cocycle B_i' such that $[B_i']=[B_i]$ and*

$$\operatorname{val}_\pi(e_i\mu_\varphi(B_i'))=\operatorname{val}_\pi(e_j\mu_\varphi(B_i'))=2-2p,$$
$$\operatorname{val}_\pi e_i\mu_\xi(B_i'))\geqslant 0\quad\textit{and}\quad\operatorname{val}_\pi(e_j\mu_\xi(B_i'))=1-p.$$

Proof. Again assume $i=0$, the case $i=1$ being similar. By the very construction of $H_0(\pi)$, we have $L_0(\pi):=(\lambda_\xi^{\Sigma_0}\xi-1)H_0(\pi)\in\mathbf{F}[[\pi]]$, so that

$$g_0'(\pi):=e_0\mu_\xi(B_0)=(C\pi^{(p-1)\Sigma_0}\Phi-1)^{-1}(L_0(\pi))\in\mathbf{F}[[\pi]]$$

and $\mu_\xi(B_0)=(g_0'(\pi),\pi^{(p-1)c_1}g_0'(\pi^p))$. Now let $B_0'=B_0-B$, where B is a coboundary such that

$$\begin{aligned}\mu_\varphi(B)&=(C\pi^{(p-1)c_0}b_1(\pi^p)-b_0(\pi),\pi^{(p-1)c_1}b_0(\pi^p)-b_1(\pi))\\ &=(\pi^{1-p^2}+h_0^{(1)},-C^{-1}(\pi^{2-2p}+\widetilde{h}_0^{(1)})),\\ \mu_\xi(B)&=(0,(\lambda_\xi^{\Sigma_1}\xi-1)b_1(\pi)),\end{aligned}$$

where $b_0(\pi)=0$, $b_1(\pi)=C^{-1}(\pi^{2-2p}+\widetilde{h}_0^{(1)})$ with $\widetilde{h}_0^{(1)}:=\sum_{s=1}^{p-2}\epsilon_s^{(1)}\pi^{2-2p+s}$. Then

$$\begin{aligned}\mu_\varphi(B_0')&=(\epsilon^{(0)}h_0'^{(0)}+h_0^{(0)},C^{-1}(\pi^{2-2p}+h_0^{(1)}))\\ \mu_\xi(B_0')&=(g_0'(\pi),\pi^{(p-1)c_1}g_0'(\pi^p)-(\lambda_\xi^{\Sigma_1}\xi-1)b_1(\pi)),\end{aligned}$$

so that B_0' has the required form. $\square$

Lemma 5.8. *Suppose that $\{i, j\} = \{0, 1\}$ with $c_i = p-1$ and $c_j = p-2$. Then there is a cocycle B'_i such that $[B'_i] = [B_i]$ and*

$$\mathrm{val}_\pi(e_i\mu_\varphi(B'_i)) \geqslant 2-2p, \quad \mathrm{val}_\pi(e_j\mu_\varphi(B'_i)) = 3-3p,$$
$$\mathrm{val}_\pi(e_i\mu_\xi(B'_i)) = 1-p \quad \textit{and} \quad \mathrm{val}_\pi(e_j\mu_\xi(B'_i)) \geqslant 2-2p.$$

Proof. This is similar to Lemma 5.7 but choose the coboundary B such that

$$\begin{aligned}\mu_\varphi(B) &= (C\pi^{(p-1)c_0}b_1(\pi^p) - b_0(\pi), \pi^{(p-1)c_1}b_0(\pi^p) - b_1(\pi))\\ &= (\pi^{1-p^3} + \epsilon^{(1)}h_0'^{(1)} + h_0^{(1)} + h_0^{(2)} - C^{-1}\widetilde{h}_0^{(2)}, -C^{-1}(\epsilon^{(1)}\widetilde{h}_0'^{(1)} + \widetilde{h}_0^{(1)})),\\ \mu_\xi(B) &= ((\lambda_\xi^{\Sigma_0}\xi - 1)b_0(\pi), (\lambda_\xi^{\Sigma_1}\xi - 1)b_1(\pi)),\end{aligned}$$

by taking $b_0(\pi) = C^{-1}\widetilde{h}_0^{(2)}$, $b_1(\pi) = C^{-1}(\epsilon^{(1)}\widetilde{h}_0'^{(1)} + \widetilde{h}_0^{(1)}) + \pi^{(p-1)(p-2)}b_0(\pi^p)$, where $\widetilde{h}_0^{(2)} := \sum_{s=0}^{p-2}\epsilon_s^{(2)}\pi^{2-2p+s}$ (with $\epsilon_0^{(2)} = 1$), $\widetilde{h}_0'^{(1)} := \sum_{s=0}^{p-2}\epsilon_s'^{(1)}\pi^{3-3p+s}$ (with $\epsilon'^{(1)} = 1$) and $\widetilde{h}_0^{(1)} := \sum_{s=1}^{p-2}\epsilon_s^{(1)}\pi^{2-2p+s}$. □

Proposition 5.9. *If $f = 2$, then*

$$V_S = V_S^{\pm} = \mathrm{Ext}^1(M_{\vec{0}}, M_{C\vec{c}}),$$

with $\pm$ occurring when $\vec{c} = \overrightarrow{p-2}$.

Proof. By straightforward calculations one can check that both $\iota[B_0]$ and $\iota[B_1]$ are bounded in each of the following cases that need to be considered:

- $0 \leqslant c_0, c_1 \leqslant p-2$, $1 \leqslant a_0, a_1 \leqslant p-1$, $\langle\vec{c}\,\rangle_S = (\pi^{p-1}, \pi^{p-1})$;
- $c_0 = p-1$, $0 \leqslant c_1 < p-2$, $a_0 = 1$, $1 \leqslant a_1 < p-1$, $\langle\vec{c}\,\rangle_S = (\pi^{p-1}, \pi^{2p-2})$;
- $0 \leqslant c_0 < p-2$, $c_1 = p-1$, $1 \leqslant a_0 < p-1$, $a_1 = 1$, $\langle\vec{c}\,\rangle_S = (\pi^{2p-2}, \pi^{p-1})$;
- $p-2 \leqslant c_0, c_1 \leqslant p-1$, $p-1 \leqslant a_0, a_1 \leqslant p$, $\langle\vec{c}\,\rangle_S = (\pi^{2p-2}, \pi^{2p-2})$;
- $c_0 = c_1 = p-2$, $a_0 = a_1 = p$, $\langle\vec{c}\,\rangle_S = (\pi^{2p-2}, \pi^{2p-2})$ (for V_S^+); and
- $c_0 = c_1 = p-2$, $a_0 = a_1 = 1$, $\langle\vec{c}\,\rangle_S = (\pi^{p-1}, \pi^{p-1})$ (for V_S^-). □

Proposition 5.10. *If $f = 2$, then*

$$V_\emptyset = V_\emptyset^{\pm} = 0,$$

with $\pm$ occurring when $\vec{c} = \vec{1}$.

Proof. We have the following cases to consider:

- $1 \leqslant c_0, c_1 \leqslant p-1$, $1 \leqslant b_0, b_1 \leqslant p-1$, $\langle\vec{c}\,\rangle_\emptyset = (1, 1)$;
- $c_0 = 0$, $2 \leqslant c_1 \leqslant p-1$, $b_0 = p$, $1 \leqslant b_1 \leqslant p-2$, $\langle\vec{c}\,\rangle_\emptyset = (1, \pi^{1-p})$;
- $2 \leqslant c_0 \leqslant p-1$, $c_1 = 0$, $1 \leqslant b_0 \leqslant p-2$, $b_1 = p$, $\langle\vec{c}\,\rangle_\emptyset = (\pi^{1-p}, 1)$; and
- $0 \leqslant c_0, c_1 \leqslant 1$, $p-1 \leqslant b_0, b_1 \leqslant p$, $\langle\vec{c}\,\rangle_\emptyset = (\pi^{1-p}, \pi^{1-p})$.

If E is a cocycle such that $\iota[E]$ is bounded, then there is a coboundary B associated to some $(b_0(\pi), b_1(\pi)) \in \mathbf{F}((\pi))^S$ such that $\iota(E+B)$ has $\mu_\varphi \in \mathbf{F}[[\pi]]^S$ and $\mu_\xi \in \pi\mathbf{F}[[\pi]]^S$. As $\kappa_\varphi(A, \vec{a}) \in (\mathbf{F}^\times)^S$ and $\langle\vec{c}\,\rangle_\emptyset = (\pi^{(1-p)\epsilon_0}, \pi^{(1-p)\epsilon_1})$ for some $\epsilon_j \in \{0, 1\}$, we get $\mu_\varphi(E+B) \in \mathbf{F}[[\pi]]^S$ and $\mu_\xi(E+B) \in \pi\mathbf{F}[[\pi]]^S$.

First consider the case $0 \leqslant c_0, c_1 < p-1$ and $E = B_0 + \beta B_1$ for some $\beta \in \mathbf{F}^\times$. As $\mathrm{val}_\pi e_0\mu_\varphi(E) = 1-p$ and $\mathrm{val}_\pi e_1\mu_\varphi(E) \geqslant 1-p$, we have $\mathrm{val}_\pi(C\pi^{(p-1)c_0}b_1(\pi^p) - b_0(\pi)) = 1-p$

and $\mathrm{val}_\pi(\pi^{(p-1)c_1} b_0(\pi^p) - b_1(\pi)) \geqslant 1-p$. If $\mathrm{val}_\pi b_0(\pi) > 1-p$, then $(p-1)c_0 + p\mathrm{val}_\pi b_1(\pi) = 1-p$, which implies $p|(c_0+1)$, contradicting $c_0 < p-1$. If $\mathrm{val}_\pi b_0(\pi) \leqslant 1-p$, then $(p-1)c_1 + p\mathrm{val}_\pi b_0(\pi) < 1-p$, which implies that $\mathrm{val}_\pi b_1(\pi) = (p-1)c_1 + p\mathrm{val}_\pi b_0(\pi) < 1-p$, which in turn implies $(p-1)c_0 + p\mathrm{val}_\pi b_1(\pi) < 1-p$, so that $\mathrm{val}_\pi b_0(\pi) = (p-1)c_0 + p\mathrm{val}_\pi b_1(\pi) = (p-1)\Sigma_0 + p^2 \mathrm{val}_\pi b_0(\pi)$, yielding a contradiction. The proof that $\iota[B_1]$ is not bounded is the same.

Next suppose $c_0 = p-1$ and $0 < c_1 < p-2$. First consider the case $E = B_0' + \beta B_1$. As $\mathrm{val}_\pi e_1 \mu_\xi(E) = 1-p$, we have $\mathrm{val}_\pi(\lambda_\xi^{\Sigma_1}\xi - 1) b_1(\pi) = 1-p$, so that $\mathrm{val}_\pi b_1(\pi) \leqslant 2-2p$. Then $\mathrm{val}_\pi \pi^{(p-1)c_0} b_1(\pi^p) = (p-1)c_0 + p\mathrm{val}_\pi b_1(\pi) < (1-p)(1+p) < 2-2p = \mathrm{val}_\pi e_0 \mu_\varphi(E)$, and so $\mathrm{val}_\pi b_0(\pi) = \mathrm{val}_\pi \pi^{(p-1)c_0} b_1(\pi^p) = (p-1)c_0 + p\mathrm{val}_\pi b_1(\pi)$. Then again $\mathrm{val}_\pi \pi^{(p-1)c_1} b_0(\pi^p) = (p-1)\Sigma_1 + p^2 \mathrm{val}_\pi b_1(\pi) < 2-2p = \mathrm{val}_\pi e_1 \mu_\varphi(E)$, so that $\mathrm{val}_\pi b_1(\pi) = \mathrm{val}_\pi \pi^{(p-1)c_1} b_0(\pi^p) = (p-1)\Sigma_1 + p^2 \mathrm{val}_\pi b_1(\pi)$, or $\mathrm{val}_\pi b_1(\pi) = -(p-1)\Sigma_1/(p^2-1) > 2-2p$, a contradiction. The proof that $\iota[B_1]$ is not bounded is the same as in the case $c_0 < p-1$.

If $c_0 = p-1,\ c_1 = p-2$, the proof is similar to the preceding case, except that we start by noting that $\mathrm{val}_\pi e_0 \mu_\xi(E) = 1-p$ if $E = B_0' + \beta B_1$.

The proof in the case that $c_1 = p-1$ is the same as the case $c_0 = p-1$. $\square$

Proposition 5.11. *If $f = 2$, then*

$$V_{\{1\}} = \begin{cases} \mathbf{F}[B_1] & \text{if } c_0 = p-1, \\ \mathbf{F}[\alpha_1 B_0 - \alpha_0 B_1] & \text{if } 0 < c_0 < p-1,\ c_1 = 0, \\ \mathbf{F}[B_0] & 0 \leqslant c_0 < p-1,\ 0 < c_1 \leqslant p-1, \end{cases}$$
$$V_{\{1\}}^+ = \mathbf{F}[\alpha_1 B_0 - \alpha_0 B_1],$$
$$V_{\{1\}}^- = 0,$$

with $\pm$ occurring when $\vec{c} = \vec{0}$. (See Lemma 5.6 for the definition of the α_i.)

Proof. Unless $\vec{c} = \vec{0}$, $\vec{c}$ gives rise to unique $\vec{a} = (0, a_1)$, $\vec{b} = (b_0, 0)$ with $1 \leqslant a_1, b_0 \leqslant p$. If $\vec{c} = \vec{0}$, we have $\vec{a} = (0, p), \vec{b} = (1, 0)$ (for V_J^+) or $\vec{a} = (0, 1), \vec{b} = (p, 0)$ (for V_J^-). We always have $\langle \vec{c}\,\rangle_{\{1\}} = (\pi^{p-1}, 1)$ except when $\vec{c} = \vec{0}$, $b_0 = p$, $a_0 = 1$, in which case we have $\langle \vec{c}\,\rangle_{\{1\}} = (1, \pi^{1-p})$.

(i) Assume $c_0 = p-1$. It is straightforward to check that $\iota[B_1 + \beta B]$ is bounded for some $\beta \in \mathbf{F}^\times$, where B is a coboundary such that

$$\mu_\varphi(B) = (C\pi^{(p-1)c_0}\pi^{(1-p)p}, -\pi^{1-p}) \quad \text{and} \quad \mu_\xi(B) = (0, (\lambda_\xi^{\Sigma_1}\xi - 1)(\pi^{1-p})).$$

Suppose $\iota[B_0']$ is bounded. There exists a coboundary B such that $\mu_\varphi \iota(B_0' + B) \in \mathbf{F}[[\pi]]^S$, $\mu_\xi \iota(B_0' + B) \in \pi\mathbf{F}[[\pi]]^S$, and so

$$\mu_\varphi(B_0') + (C\pi^{(p-1)c_0} b_1(\pi^p) - b_0(\pi), \pi^{(p-1)c_1} b_0(\pi^p) - b_1(\pi)) \in \pi^{1-p}\mathbf{F}[[\pi]] \times \pi^{(1-p)a_1}\mathbf{F}[[\pi]],$$
$$\mu_\xi(B_0') + ((\lambda_\xi^{\Sigma_0}\xi - 1) b_0(\pi), (\lambda_\xi^{\Sigma_1}\xi - 1) b_1(\pi)) \in \pi^{2-p}\mathbf{F}[[\pi]] \times \pi\mathbf{F}[[\pi]]$$

for some $b_0(\pi), b_1(\pi) \in \mathbf{F}((\pi))$.

If $c_1 < p-2$, we have $\mathrm{val}_\pi(\lambda_\xi^{\Sigma_1}\xi - 1) b_1(\pi) = 1-p$ as $\mathrm{val}_\pi e_1 \mu_\xi(B_0') = 1-p$, so that $\mathrm{val}_\pi b_1(\pi) \leqslant 2-2p$. Then

$$\mathrm{val}_\pi(\pi^{(p-1)c_0} b_1(\pi^p)) = (p-1)c_0 + p\mathrm{val}_\pi b_1(\pi) < (1-p)(1+p) < \mathrm{val}_\pi e_0 \mu_\varphi(B_0'),$$

and so $\mathrm{val}_\pi b_0(\pi) = (p-1)c_0 + p\mathrm{val}_\pi b_1(\pi)$. Then again

$$\begin{aligned} \mathrm{val}_\pi \pi^{(p-1)c_1} b_0(\pi^p) &= (p-1)c_1 + p\mathrm{val}_\pi b_0(\pi) = (p-1)\Sigma_1 + p^2 \mathrm{val}_\pi b_1(\pi) \\ &< (1-p)(1+p) < (1-p)a_1, \end{aligned}$$

https://doi.org/10.1112/S0010437X1000504X Published online by Cambridge University Press

so that $\mathrm{val}_\pi b_1(\pi) = (p-1)\Sigma_1 + p^2 \mathrm{val}_\pi b_1(\pi)$, or $\mathrm{val}_\pi b_1(\pi) = -(p-1)\Sigma_1/(p^2-1) > 1-p$, a contradiction.

If $c_1 = p-2$, start with $\mathrm{val}_\pi(\lambda_\xi^{\Sigma_0}\xi - 1)b_0(\pi) = 1-p$ and the same argument as above (for the case $c_1 < p-2$) goes through.

(ii) Assume $0 < c_0 < p-1, c_1 = 0$. Straightforward calculations show that $\mu_\varphi \iota B_0, \mu_\varphi \iota B_1 \in \mathbf{F}[[\pi]]^S$ but $\mu_\xi \iota B_0(\pi), \mu_\xi \iota B_1 \notin \pi\mathbf{F}[[\pi]]^S$. If, however, we take $\alpha_1 B_0 - \alpha_0 B_1$, it has μ_φ obviously in $\mathbf{F}[[\pi]]^S$ and $\mu_\xi = \kappa_\xi(A, \vec{a})(\pi^{p-1}\alpha_0\alpha_1(g_0(\pi) - C\pi^{(p-1)c_0}g_1(\pi^p)), \alpha_0\alpha_1(g_0(\pi^p) - g_1(\pi))) \in \pi\mathbf{F}[[\pi]]^S$.

Now suppose $\iota[B_1]$ is bounded, and so we have, for some coboundary B, that $\mu_\varphi\iota(B_1 + B) \in \mathbf{F}[[\pi]]^S$ and $\mu_\xi\iota(B_1 + B) \in \pi\mathbf{F}[[\pi]]^S$, which implies

$$\begin{gathered}\mu_\varphi(B_1) + (C\pi^{(p-1)c_0}b_1(\pi^p) - b_0(\pi), \pi^{(p-1)c_1}b_0(\pi^p) - b_1(\pi)) \in \pi^{1-p}\mathbf{F}[[\pi]] \times \pi^{(1-p)a_1}\mathbf{F}[[\pi]],\\ \mu_\xi(B_1) + ((\lambda_\xi^{\Sigma_0}\xi - 1)b_0(\pi), (\lambda_\xi^{\Sigma_1}\xi - 1)b_1(\pi)) \in \pi^{2-p}\mathbf{F}[[\pi]] \times \pi\mathbf{F}[[\pi]]\end{gathered}$$

for some $b_0(\pi), b_1(\pi) \in \mathbf{F}((\pi))$.

We have $\mathrm{val}_\pi(\lambda_\xi^{\Sigma_1}\xi - 1)b_1(\pi) = 0$ and so $\mathrm{val}_\pi b_1(\pi) \leqslant 1-p$, so that $\mathrm{val}_\pi \pi^{(p-1)c_0} b_1(\pi^p) = (p-1)c_0 + p\mathrm{val}_\pi b_1(\pi) < 1-p$. Then $\mathrm{val}_\pi b_0(\pi) = (p-1)c_0 + p\mathrm{val}_\pi b_1(\pi)$ and $\mathrm{val}_\pi \pi^{(p-1)c_1} b_0(\pi^p) = (p-1)\Sigma_1 + p^2\mathrm{val}_\pi b_1(\pi) < (1-p)a_1$, so that $\mathrm{val}_\pi b_1(\pi) = \Sigma_1 + p^2 \mathrm{val}_\pi b_1(\pi)$, or $\mathrm{val}_\pi b_1(\pi) = -(p-1)/(p^2-1)\Sigma_1 > 1-p$, a contradiction.

(iii) Assume $0 \leqslant c_0 < p-1,\ \ 0 < c_1 \leqslant p-1$. It is straightforward to check that $\iota[B_0]$ is bounded:

$$\begin{aligned}\mu_\varphi\iota(B_0) &= (A, \pi^{(p-1)a_1})(\pi^{p-1}, 1)(\pi^{1-p} + h_0(\pi)) \in \mathbf{F}[[\pi]]^S,\\ \mu_\xi\iota(B_0) &= \kappa_\xi(A, \vec{a})(\pi^{p-1}, 1)(\alpha_0 g(\pi), \pi^{(p-1)c_1}\alpha_0 g_0(\pi^p)) \in \pi\mathbf{F}[[\pi]]^S\end{aligned}$$

as $c_1 > 0$.

Now suppose $\iota[B_1]$ is bounded. Then there exists a coboundary B such that $\mu_\varphi\iota(B_1 + B) \in \mathbf{F}[[\pi]]^S$, $\mu_\xi\iota(B_1 + B) \in \pi\mathbf{F}[[\pi]]^S$, and so

$$\begin{gathered}\mu_\varphi(B_1 + B) + (C\pi^{(p-1)c_0}b_1(\pi^p) - b_0(\pi), \pi^{(p-1)c_1}b_0(\pi^p) - b_1(\pi)) \in \pi^{1-p}\mathbf{F}[[\pi]] \times \pi^{(1-p)a_1}\mathbf{F}[[\pi]],\\ \mu_\xi(B_1 + B) + ((\lambda_\xi^{\Sigma_0}\xi - 1)b_0(\pi), (\lambda_\xi^{\Sigma_1}\xi - 1)b_1(\pi)) \in \pi^{2-p}\mathbf{F}[[\pi]] \times \pi\mathbf{F}[[\pi]].\end{gathered}$$

If $c_1 < p-1$, then the argument is the same as in case (ii).

If $c_1 = p-1,\ c_0 < p-2$, then as $\mathrm{val}_\pi e_0\mu_\xi(B_1' + B) \geqslant 2-p$ and $\mathrm{val}_\pi e_0\mu_\xi(B_1') = 1-p$, we have $\mathrm{val}_\pi e_0\mu_\xi(B) = \mathrm{val}_\pi(\lambda_\xi^{\Sigma_0}\xi - 1)b_0(\pi) = 1-p$, so that $\mathrm{val}_\pi b_0(\pi) \leqslant 2-2p$. Then

$$\begin{aligned}\mathrm{val}_\pi \pi^{(p-1)c_1} b_0(\pi^p) &= (p-1)c_1 + p\mathrm{val}_\pi b_0(\pi)\\ &\leqslant (1-p)(1+p) < \min(\mathrm{val}_\pi e_1\mu_\varphi B_1', (1-p)a_1),\end{aligned}$$

so that $\mathrm{val}_\pi b_1(\pi) = (p-1)c_1 + p\mathrm{val}_\pi b_0(\pi)$. So

$$\mathrm{val}_\pi \pi^{(p-1)c_0} b_1(\pi^p) = (p-1)\Sigma_0 + p^2\mathrm{val}_\pi b_0(\pi) < (1-p)(1+p) < \mathrm{val}_\pi e_0\mu_\varphi(B_1'),$$

which implies $\mathrm{val}_\pi b_0(\pi) = (p-1)\Sigma_0 + p^2\mathrm{val}_\pi b_0(\pi)$, or $\mathrm{val}_\pi b_0(\pi) = -(p-1)\Sigma_0/(p^2-1) > 1-p$, a contradiction.

If $c_1 = p-1,\ \ c_0 = p-2$, then as $\mathrm{val}_\pi e_1\mu_\xi(B_1' + B) \geqslant 1$ and $\mathrm{val}_\pi e_1\mu_\xi(B_1') = 1-p$, we have $\mathrm{val}_\pi e_1\mu_\xi(B) = \mathrm{val}_\pi(\lambda_\xi^{\Sigma_1}\xi - 1)b_1(\pi) = 1-p$, so that $\mathrm{val}_\pi b_1(\pi) \leqslant 2-2p$. Then

$$\mathrm{val}_\pi \pi^{(p-1)c_0} b_1(\pi^p) = (p-1)c_0 + p\mathrm{val}_\pi b_1(\pi) \leqslant (1-p)(1+p) < \mathrm{val}_\pi e_0\mu_\varphi B_1',$$

so that $\mathrm{val}_\pi b_0(\pi) = (p-1)c_0 + p\mathrm{val}_\pi b_1(\pi)$. So

$$\mathrm{val}_\pi \pi^{(p-1)c_1} b_0(\pi^p) = (p-1)\Sigma_1 + p^2\mathrm{val}_\pi b_1(\pi) < (1-p)(1+p) < \mathrm{val}_\pi e_1\mu_\varphi(B_1'),$$

which implies $\mathrm{val}_\pi b_1(\pi) = (p-1)\Sigma_1 + p^2\mathrm{val}_\pi b_1(\pi)$, or $\mathrm{val}_\pi b_1(\pi) = -(p-1)\Sigma_1/(p^2-1) > 1-p$, a contradiction.

(iv) Assume $c_0 = c_1 = 0,\ b_0 = 1, a_1 = p$. Straightforward calculations show that $\mu_\varphi \iota B_0(\pi)$, $\mu_\varphi \iota B_1 \in \mathbf{F}[[\pi]]^S$ but $\mu_\xi \iota B_0(\pi), \mu_\xi \iota B_1 \notin \pi\mathbf{F}[[\pi]]^S$. If, however, we take $\alpha_1 B_0 - \alpha_0 B_1$, it has μ_φ obviously in $\mathbf{F}[[\pi]]^S$ and

$$\mu_\xi = (\pi^{p-1}\alpha_0\alpha_1(g_0(\pi) - Cg_1(\pi^p)), \alpha_0\alpha_1(g_0(\pi^p) - g_1(\pi))) \in \pi\mathbf{F}[[\pi]]^S.$$

Now suppose $\iota[B_1]$ is bounded, and so we have, for some coboundary B, that $\mu_\varphi\iota(B_1 + B) \in \mathbf{F}[[\pi]]^S$ and $\mu_\xi\iota(B_1 + B) \in \pi\mathbf{F}[[\pi]]^S$, which implies

$$\begin{gathered}\mu_\varphi(B_0) + (Cb_1(\pi^p) - b_0(\pi), b_0(\pi^p) - b_1(\pi)) \in \pi^{1-p}\mathbf{F}[[\pi]] \times \pi^{(1-p)p}\mathbf{F}[[\pi]],\\ \mu_\xi(B_0) + ((\xi-1)b_0(\pi), (\xi-1)b_1(\pi)) \in \pi^{2-p}\mathbf{F}[[\pi]] \times \pi\mathbf{F}[[\pi]]\end{gathered}$$

for some $b_0(\pi), b_1(\pi) \in \mathbf{F}((\pi))$. We have $\mathrm{val}_\pi(\xi-1)b_1(\pi) = 0$ and so $\mathrm{val}_\pi b_1(\pi) \leqslant 1-p$, so that $\mathrm{val}_\pi b_1(\pi^p) = p\mathrm{val}_\pi b_1(\pi) < 1-p$. Then $\mathrm{val}_\pi b_0(\pi) = p\mathrm{val}_\pi b_1(\pi)$ and $\mathrm{val}_\pi b_0(\pi^p) = p^2\mathrm{val}_\pi b_1(\pi) < (1-p)p < \mathrm{val}_\pi e_0\mu_\varphi(B_1)$, giving $\mathrm{val}_\pi b_1(\pi) = 0$ and a contradiction.

(v) Assume $c_0 = c_1 = 0,\ b_0 = p,\ \ a_1 = 1$. Suppose $\iota[B_0 + \beta B_1]$ is bounded for some $\beta \in \mathbf{F}$. There exists a coboundary B such that $\mu_\varphi\iota(B_0 + \beta B_1 + B) \in \mathbf{F}[[\pi]]^S$ and $\mu_\xi\iota(B_0 + \beta B_1 + B) \in \pi\mathbf{F}[[\pi]]^S$. As $\kappa_\varphi(A, \vec{a})\langle\vec{c}\,\rangle \in (\mathbf{F}^\times)^S$, we have

$$\begin{aligned}\mu_\varphi(B_0 + \beta B_1 + B) &= \mu_\varphi(B_0 + \beta B_1) + (Cb_1(\pi^p) - b_0(\pi), b_0(\pi^p) - b_1(\pi)) \in \mathbf{F}[[\pi]]^S,\\ \mu_\xi(B_0 + \beta B_1 + B) &= \mu_\xi(B_0 + \beta B_1) + ((\xi-1)b_0(\pi), (\xi-1)b_1(\pi)) \in \pi\mathbf{F}[[\pi]]^S\end{aligned}$$

for some $b_0(\pi), b_1(\pi) \in \mathbf{F}((\pi))$.

Note that

$$\begin{gathered}\mathrm{val}_\pi e_0\mu_\varphi(B_0 + \beta B_1) = 1 - p \leqslant \mathrm{val}_\pi e_1\mu_\varphi(B_0 + \beta B_1),\\ \mathrm{val}_\pi e_0\mu_\xi(B_0 + \beta B_1) \geqslant 0, \quad \mathrm{val}_\pi e_1\mu_\xi(B_0 + \beta B_1) \geqslant 0.\end{gathered}$$

Then $\mathrm{val}_\pi e_0\mu\varphi(B) = \mathrm{val}_\pi(Cb_1(\pi^p) - b_0(\pi)) = 1-p$, and we get either $\mathrm{val}_\pi b_0(\pi) = 1 - p < \mathrm{val}_\pi b_1(\pi^p)$ or $\mathrm{val}_\pi b_1(\pi^p) = \mathrm{val}_\pi b_0(\pi) < 1-p$. In either case, we have $\mathrm{val}_\pi b_0(\pi^p) < 1-p$, so $\mathrm{val}_\pi b_0(\pi^p) = \mathrm{val}_\pi b_1(\pi)$, giving a contradiction. The same argument proves that $\iota[B_1]$ is not bounded. $\square$

Similarly one proves the following proposition.

PROPOSITION 5.12. *If $f = 2$, then*

$$\begin{aligned}V_{\{0\}} &= \begin{cases}\mathbf{F}[B_0] & \text{if } c_1 = p-1,\\ \mathbf{F}[C\alpha_1 B_0 - \alpha_0 B_1] & \text{if } c_0 = 0,\ 0 < c_1 < p-1,\\ \mathbf{F}[B_1] & 0 < c_0 \leqslant p-1,\ 0 \leqslant c_1 < p-1,\end{cases}\\ V_{\{0\}}^+ &= \mathbf{F}[C\alpha_1 B_0 - \alpha_0 B_1],\\ V_{\{0\}}^- &= 0,\end{aligned}$$

with $\pm$ occurring when $\vec{c} = \vec{0}$. (See Lemma 5.6 for the definition of the α_i.)

In proving Propositions 5.11 and 5.12 we have shown the following, which exhibits instances of coincidence of the V_J for distinct J.

https://doi.org/10.1112/S0010437X1000504X Published online by Cambridge University Press

Corollary 5.13. *Suppose $f=2$ and recall $(c_0,c_1)\neq(p-1,p-1)$.*

(i) *If $c_0=p-1$, then $V_{\{1\}}=V_{\{0\}}=\mathbf{F}[B_1]$.*

(ii) *If $c_1=p-1$, then $V_{\{1\}}=V_{\{0\}}=\mathbf{F}[B_0]$.*

(iii) *If $c_0=c_1=0$, then $V^+_{\{1\}}$ and $V^+_{\{0\}}$ are distinct and one-dimensional, and $V^-_{\{1\}}=V^-_{\{0\}}=0$.*

(iv) *In all other cases, $V_{\{1\}}$ and $V_{\{0\}}$ are distinct and one-dimensional.*

6. Exceptional cases

6.1 Cyclotomic character

Assume $C=1$, $\vec{c}=\overrightarrow{p-2}$, so that

$$\kappa_\varphi(C,\vec{c}\,)=(\pi^{(p-1)(p-2)},\dots,\pi^{(p-1)(p-2)}),$$

$$\kappa_\gamma(C,\vec{c}\,)=\left(\left(\frac{\gamma(\pi)}{\pi\overline{\chi}(\gamma)}\right)^{p-2},\dots,\left(\frac{\gamma(\pi)}{\pi\overline{\chi}(\gamma)}\right)^{p-2}\right)$$

if $\gamma\in\Gamma$. Recall that the B_i for all $i\in S$ have already been constructed in § 4.1 and we just need to construct an additional basis element, which we will denote B_{tr} (for *très ramifié*). Before we do this for arbitrary $f\geqslant 1$, let us first consider the situation where $f=1$ (i.e., $K=\mathbf{Q}_p$) and $\mathbf{F}=\mathbf{F}_p$ as a foundation for the general construction. (We will go back to the general case $f\geqslant 1$ in the paragraph preceding Lemma 6.4.)

Lemma 6.1. *Let $\eta\in\Gamma$ be such that $\eta\Gamma_1$ generates $\Gamma/\Gamma_1\simeq\mathbf{F}_p^\times$ and let $\chi(\xi)\equiv 1+zp \bmod p^2$ with $0<z\leqslant p-1$. If $s\in\mathbf{Z}$ is divisible by p^v but not by p^{v+1} for some $v\in\mathbf{Z}$, then*

$$\overline{\chi}(\eta)\eta(\pi^s)-\pi^s\in(\overline{\chi}(\eta)^{s+1}-1)\pi^s+\overline{s_v}\frac{\overline{\chi}(\eta)^{s+1}(\overline{\chi}(\eta)-1)}{2}\pi^{s+p^v}+\pi^{s+2p^v}\mathbf{F}_p[[\pi^{p^v}]],$$

$$\overline{\chi}(\xi)\xi(\pi^s)-\pi^s\in\overline{s_vz}(\pi^{s+(p-1)p^v}+\pi^{s+p^{v+1}})+\pi^{s+p^{v+1}(p-1)}\mathbf{F}_p[[\pi^{p^v}]],$$

where $s=\sum_{j\geqslant v}s_jp^j$.

Proof. This is similar to the proofs of Lemmas 4.2 and 4.4. □

Lemma 6.2. *There exists $h'(\pi)\in\pi^{1-2p}+\pi^{2-2p}\mathbf{F}[[\pi]]$ such that*

$$(\overline{\chi}(\eta)\eta-1)(h'(\pi))\in\mathbf{F}(\pi^{-p}-\pi^{-1})+\pi\mathbf{F}[[\pi]].$$

(Recall that η is a topological generator of Γ.)

Proof. By Lemma 6.1, there exist $\epsilon_{2-2p},\dots,\epsilon_{-1},\epsilon_0\in\mathbf{F}$ (unique if we set $\epsilon_{-p}=\epsilon_{-1}=0$) such that

$$(\overline{\chi}(\eta)\eta-1)(\pi^{1-2p}+\epsilon_{2-2p}\pi^{2-2p}+\cdots+\epsilon_{-1}\pi^{-1}+\epsilon_0)\in\mathbf{F}\pi^{-p}+\mathbf{F}\pi^{-1}+\pi\mathbf{F}[[\pi]].$$

Set $h'(\pi)=\pi^{1-2p}+\epsilon_{2-2p}\pi^{2-2p}+\cdots+\epsilon_{-1}\pi^{-1}+\epsilon_0$, so

$$(\overline{\chi}(\eta)\eta-1)(h'(\pi))\in\alpha\pi^{-p}+\beta\pi^{-1}+\pi\mathbf{F}[[\pi]]$$

for some $\alpha,\beta\in\mathbf{F}$. Writing $(\overline{\chi}(\xi)\xi-1)=(\sum_{i=0}^{p-2}\overline{\chi}(\eta)^i\eta^i)(\overline{\chi}(\eta)\eta-1)$ we find that

$$(\overline{\chi}(\xi)\xi-1)(h'(\pi))\in-(\alpha\pi^{-p}+\beta\pi^{-1})+\mathbf{F}[[\pi]].$$

On the other hand, a direct computation shows that

$$(\overline{\chi}(\xi)\xi-1)(h'(\pi))\in z(\pi^{-p}-\pi^{-1})+\mathbf{F}[[\pi]],$$

where $z\in\mathbf{F}^\times$, so that $\alpha=\beta=-z$ and the lemma follows. □

https://doi.org/10.1112/S0010437X1000504X Published online by Cambridge University Press

Let $h'(\pi)$ be as in the lemma. Since $\varphi - 1$ is bijective on $\pi\mathbf{F}[[\pi]]$, it follows that

$$(\overline{\chi}(\eta)\eta - 1)(h'(\pi)) \in (\varphi - 1)(g'_\eta(\pi))$$

for a unique $g'_\eta \in -z^{-1}\pi^{-1} + \pi\mathbf{F}[[\pi]]$. We now extend the definition to construct elements $g'_\gamma(\pi) \in \pi^{-1}\mathbf{F}[[\pi]]$ for all $\gamma \in \Gamma$. We let

$$g'_{\eta^n}(\pi) = \sum_{i=0}^{n-1} \overline{\chi}(\eta)^i \eta^i (g'_\eta(\pi))$$

for $n \in \mathbf{N}$. If $\gamma' \in \Gamma_2$, then $(\overline{\chi}(\gamma')\gamma' - 1)(h'(\pi))$ is in $\pi\mathbf{F}[[\pi]]$ and can therefore be written as $(\varphi - 1)(g'_{\gamma'}(\pi))$ for a unique $g'_{\gamma'}(\pi) \in \pi\mathbf{F}[[\pi]]$. If $\eta^n \in \Gamma_2$, then $p(p-1)|n$ and the definitions coincide. Moreover, an arbitrary $\gamma \in \Gamma$ can be written as $\gamma'\eta^n$ for some $\gamma' \in \Gamma_2$ and $n \in \mathbf{N}$, and

$$g'_\gamma(\pi) := g'_{\gamma'}(\pi) + \gamma'(g'_{\eta^n}(\pi))$$

is independent of the choice of γ' and n.

One can then check that $\mu = (h'(\pi), (g'_\gamma(\pi))_{\gamma' \in \Gamma})$ satisfies conditions (†) and (‡), giving an extension

$$0 \to M_{\text{cyc}} \to E' \to M_0 \to 0$$

in the category of étale (φ, Γ)-modules over $\mathbf{E}_K$, where $M_{\text{cyc}} = \mathbf{E}_K e_1$ is a rank one object defined by $\varphi(e'_1) = e'_1$ and $\gamma(e'_1) = \chi(\gamma)e'_1$ if $\gamma \in \Gamma$ (and, of course, $M_0 = \mathbf{E}_K e_0$ by $\varphi(e_0) = e_0$ and $\gamma(e_0) = e_0$). Using the isomorphism $M_{\text{cyc}} \simeq M_{p-2} = \mathbf{E}_K e_1$ defined by $e'_1 = \pi^{2-p} e_1$ we get an extension

$$0 \to M_{p-2} \to E \to M_0 \to 0$$

defined by the cocycle $\mu = (\pi^{3(1-p)}h(\pi), (\pi^{1-p}g_\gamma(\pi))_{\gamma \in \Gamma})$ with $h(\pi) = \pi^{2p-1}h'(\pi)$, $g_\gamma(\pi) = \pi g'_\gamma(\pi)$.

Now we go back to the context of arbitrary $f \geqslant 1$, and define $\mu_\varphi(B_{\text{tr}}) = (\pi^{3(1-p)}h(\pi), \ldots, \pi^{3(1-p)}h(\pi))$ and $\mu_\gamma(B_{\text{tr}}) = (\pi^{1-p}g_\gamma(\pi), \ldots, \pi^{1-p}g_\gamma(\pi))$ for all $\gamma \in \Gamma$. It is straightforward to check that $B_{\text{tr}} \in H$, so that $[B_{\text{tr}}] \in \operatorname{Ext}^1(M_{\vec{0}}, M_{\overrightarrow{p-2}})$.

Remark 6.3. The class $[B_{\text{tr}}]$ is not canonical. Choosing $\epsilon_{-p} = -\epsilon_{-1} \neq 0$ in the proof of Lemma 6.2 gives different extension classes $[B_{\text{tr}}]$ differing by a multiple of $[B_0] + [B_1] + \cdots + [B_{f-1}]$.

Lemma 6.4. *The extensions $[B_0], \ldots, [B_{f-1}], [B_{\text{tr}}] \in \operatorname{Ext}^1(M_{\vec{0}}, M_{\overrightarrow{p-2}})$ are linearly independent, and therefore form a basis.*

Proof. It suffices to show that $[B_{\text{tr}}]$ is not contained in the span of the $[B_i]$. Suppose that $B_{\text{tr}} = \beta_0 B_0 + \cdots + \beta_{f-1}B_{f-1}$ for some $\beta_i \in \mathbf{F}$. Then $E := B_{\text{tr}} - (\beta_0 B_0 + \cdots + \beta_{f-1}B_{f-1})$ is a coboundary, so that

$$\mu_\varphi(E) = (\pi^{(p-1)(p-2)}b_1(\pi^p) - b_0(\pi), \ldots, \pi^{(p-1)(p-2)}b_0(\pi^p) - b_{f-1}(\pi))$$

for some $b_i(\pi) \in \mathbf{F}((\pi))$. As

$$\mu_\varphi(B_{\text{tr}}) = (\pi^{3(1-p)}h(\pi), \ldots, \pi^{3(1-p)}h(\pi)),$$
$$\mu_\xi(B_{\text{tr}}) = (\pi^{1-p}g_\xi(\pi), \ldots, \pi^{1-p}g_\xi(\pi)),$$

where $h(\pi), g_\xi(\pi) \in \mathbf{F}[[\pi]]^\times$, we have $\operatorname{val}_\pi e_i \mu_\varphi(E) = \operatorname{val}_\pi(\pi^{(p-1)(p-2)}b_{i+1}(\pi^p) - b_i(\pi)) = 3(1-p)$ for all $i \in S$. For each $i \in S$, letting $s_i := \operatorname{val}_\pi(b_i(\pi))$, we have $s_i \leqslant 3(1-p)$ or $(p-1)(p-2) + s_{i+1}p = 3(1-p)$. The latter is impossible looking at divisibility by p, and so $s_i \leqslant 3(1-p)$ for all $i \in S$, which yields a contradiction after cycling. $\square$

https://doi.org/10.1112/S0010437X1000504X Published online by Cambridge University Press

The determination of which linear combinations of $[B_0], [B_1], \ldots, [B_{f-1}]$ are bounded is exactly as in the generic case. We now extend this to include $[B_{\mathrm{tr}}]$.

Proposition 6.5. *Suppose that $C = 1$, $\vec{c} = \overrightarrow{p-2}$ and $A \in \mathbf{F}^\times$;*

(i) *if $J = S$, then*

$$\iota[B_{\mathrm{tr}}] \in \mathrm{Ext}^1_{\mathrm{bdd}}(M_{A\vec{p}}, M_{A\vec{0}}),$$

so that $V_S^+ = \mathrm{Ext}^1(M_{\vec{0}}, M_{\overrightarrow{p-2}})$;

(ii) *$V_S^- = \bigoplus_{i\in S} \mathbf{F}[B_i]$, and if $J \neq S$, then $V_J = \bigoplus_{i\in J} \mathbf{F}[B_{i+1}]$.*

Proof. (i) This is straightforward: as $\vec{a} = \vec{p}$ and $\langle \vec{c}\,\rangle_S = (\pi^{2(p-1)}, \ldots, \pi^{2(p-1)})$, we have

$$\mu_\varphi(\iota B_{\mathrm{tr}}) = (A\pi^{(p-1)^2} h(\pi), \pi^{(p-1)^2} h(\pi), \ldots, \pi^{(p-1)^2} h(\pi)) \in \mathbf{F}[[\pi]]^S,$$
$$\mu_\xi(\iota B_{\mathrm{tr}}) = (\lambda_\xi^{(p-2)(p^f-1)/(p-1)}, \ldots, \lambda_\xi^{(p-2)(p^f-1)/(p-1)})(\pi^{p-1} g_\xi(\pi), \ldots, \pi^{p-1} g_\xi(\pi)) \in \pi\mathbf{F}[[\pi]]^S.$$

(ii) Let $E := \beta_0 B_0 + \cdots + \beta_{f-1} B_{f-1} + B_{\mathrm{tr}}$ for some $\beta_0, \ldots, \beta_{f-1} \in \mathbf{F}$. We must show that, in all other cases where $\iota : \mathrm{Ext}^1(M_{\vec{0}}, M_{\overrightarrow{p-2}}) \to \mathrm{Ext}^1(M_{A\vec{a}}, M_{A\vec{b}})$ was defined, we have that $\iota[E]$ is not bounded.

So suppose that $\iota[E]$ is bounded. Then there exists a coboundary B defined by $(b_0(\pi), \ldots, b_{f-1}(\pi))$ such that $\mu_\varphi(\iota(E + B)) \in \mathbf{F}[[\pi]]^S$ and $\mu_\xi(\iota(E + B)) \in \pi\mathbf{F}[[\pi]]^S$. We have $e_i\langle \vec{c}\,\rangle_J = 1$ or π^{p-1} and $\mathrm{val}_\pi e_i \mu_\xi(\iota E) \leqslant 0$. It follows that $\mathrm{val}_\pi e_i \mu_\xi(B) = \mathrm{val}_\pi e_i \mu_\xi(E) = 1 - p$, so by Lemma 4.4, we must have $s_i := \mathrm{val}_\pi(b_i(\pi)) \leqslant 2(1 - p)$. Then we have $\mathrm{val}_\pi(\pi^{(p-1)c_i} b_i(\pi^p)) = (p - 1)(p - 2) + s_i p \leqslant (1 - p)(p + 2)$, so that $s_{i-1} = (p - 1)(p - 2) + s_i p$. Cycling this through indices leads to a contradiction. □

6.2 Trivial character

In this subsection, we assume that $C = 1$, $\vec{c} = \vec{0}$, so that $\kappa_\varphi(C, \vec{c}\,) = \kappa_\gamma(C, \vec{c}\,) = (1, \ldots, 1) \in \mathbf{F}((\pi))^S$.

Using Lemma 4.2 we can find unique $\epsilon_{2-p}, \ldots, \epsilon_{-1} \in \mathbf{F}$ such that

$$(\eta - 1)(\pi^{1-p} + \epsilon_{2-p}\pi^{2-p} + \cdots + \epsilon_{-1}\pi^{-1}) \in \mathbf{F}[[\pi]].$$

Set $H(\pi) = \pi^{1-p} + \epsilon_{2-p}\pi^{2-p} + \cdots + \epsilon_{-1}\pi^{-1}$. By Lemma 4.4, we get

$$(\xi - 1)(H(\pi)) \in \mathbf{F}^\times + \pi\mathbf{F}[[\pi]],$$

which implies, via Proposition 4.6, that

$$(\eta - 1)(H(\pi)) \in \nu + \pi\mathbf{F}[[\pi]]$$

for some $\nu \in \mathbf{F} - \{0\}$. Likewise we have

$$(\eta - 1)(H(\pi^p)) \in \nu + \pi\mathbf{F}[[\pi]],$$

so that

$$(\eta - 1)(-H(\pi^p) + H(\pi)) \in \pi\mathbf{F}[[\pi]].$$

Note that, if $\gamma' \in \Gamma_2$, then $(\gamma' - 1)(H(\pi)) \in \pi\mathbf{F}[[\pi]]$, and it follows that $(\gamma' - 1)(-H(\pi^p) + H(\pi)) \in \pi\mathbf{F}[[\pi]]$. Now for each $\gamma \in \Gamma$, writing $\gamma = \eta^n\gamma'$ where $\gamma' \in \Gamma_2$, we get by Lemma 4.5 that

$$(\gamma - 1)(-H(\pi^p) + H(\pi)) \in \pi\mathbf{F}[[\pi]].$$

As the map $g(\pi) \mapsto g(\pi^{p^f}) - g(\pi)$ defines a bijection $\pi\mathbf{F}[[\pi]] \to \pi\mathbf{F}[[\pi]]$, for each $\gamma \in \Gamma$ there exists a unique $g_\gamma(\pi) \in \pi\mathbf{F}[[\pi]]$ such that

$$g_\gamma(\pi^{p^f}) - g_\gamma(\pi) = (\gamma - 1)(-H(\pi^p) + H(\pi))$$

or equivalently

$$(\varphi - 1)(g_\gamma(\pi), g_\gamma(\pi^{p^{f-1}}), \dots, g_\gamma(\pi^p)) = (\gamma - 1)(-H(\pi^p) + H(\pi), 0, \dots, 0).$$

If we set

$$\mu_\varphi(B_0) = (-H(\pi^p) + H(\pi), 0, \dots, 0),$$
$$\mu_\gamma(B_0) = (g_\gamma(\pi), g_\gamma(\pi^{p^{f-1}}), \dots, g_\gamma(\pi^p)),$$

$\mu(B_0) = (\mu_\varphi(B_0), (\mu_\gamma(B_0))_{\gamma\in\Gamma})$ satisfies the condition (†) by the considerations above. We note that $\mu_\gamma(B_0)$ are uniquely determined so that they satisfy (†). As both $\mu_{\gamma\gamma'}(B_0)$ and $\mu'_{\gamma\gamma'} := \gamma(\mu_{\gamma'}(B_0)) + \mu_\gamma(B_0)$ satisfy (†) for $\gamma\gamma'$, they must coincide, so that (‡) is satisfied.

For each $1 \leqslant i \leqslant f-1$, we construct $[B_i] \in \mathrm{Ext}^1(M_{\vec{0}}, M_{\vec{0}})$ in a similar way, i.e., by setting

$$\mu_\varphi(B_i) = (0, \dots, 0, -H(\pi^p) + H(\pi), 0, \dots, 0),$$
$$\mu_\gamma(B_i) = (g_\gamma(\pi^{p^i}), \dots, g_\gamma(\pi^p), g_\gamma(\pi), g_\gamma(\pi^{p^{f-1}}), \dots, g_\gamma(\pi^{p^{i+1}})).$$

Remark 6.6. For each $0 \leqslant i \leqslant f-1$, consider the coboundary B''_i by

$$\mu_\varphi(B''_i) = (0, \dots, 0, H(\pi^p), -H(\pi), 0, \dots, 0),$$
$$\mu_\gamma(B''_i) = (0, \dots, 0, 0, (\gamma - 1)(H(\pi)), 0, \dots, 0),$$

where $H(\pi)$ is the ith component and $-H(\pi)$ is the $(i+1)$th component of $\mu_\varphi(B''_i)$ and $(\gamma-1)(H(\pi))$ is the $(i+1)$th component of $\mu_\gamma(B''_i)$. Define $B'_i = B_i + B''_i$ for each $0 \leqslant i \leqslant f-1$. Then $\mathbf{F}[B_i] = \mathbf{F}[B'_i]$ in $\mathrm{Ext}^1(M_{\vec{0}}, M_{\vec{0}})$ for all $0 \leqslant i \leqslant f-1$, where we have

$$\mu_\varphi(B'_i) = (0, \dots, 0, H(\pi), -H(\pi), 0, \dots, 0),$$
$$\mu_\gamma(B'_i) = (g_\gamma(\pi^{p^i}), \dots, g_\gamma(\pi^p), g_\gamma(\pi), g_\gamma(\pi^{p^{f-1}}) + (\gamma-1)H(\pi), g_\gamma(\pi^{p^{f-2}}), \dots, g_\gamma(\pi^{p^{i+1}})).$$

Next, we define B_{nr} (for *non-ramifié*) by setting

$$\mu_\varphi(B_{\mathrm{nr}}) = (1, 0, \dots, 0),$$
$$\mu_\gamma(B_{\mathrm{nr}}) = (0, 0, \dots, 0)$$

for all $\gamma \in \Gamma$. It is straightforward to check that this defines an extension $[B_{\mathrm{nr}}] \in \mathrm{Ext}^1(M_{\vec{0}}, M_{\vec{0}})$. We can 'move' the 1 in μ_φ to any component, i.e., taking any of $(1, 0, \dots, 0)$, $(0, 1, 0, \dots, 0), \dots, (0, \dots, 0, 1)$ to be μ_φ defines the same cocycle class (up to coboundaries).

Set $B_{\mathrm{cyc}} = \sum_{i=0}^{f-1} B'_i$. Then we have

$$\mu_\varphi(B_{\mathrm{cyc}}) = (0, \dots, 0),$$
$$\mu_\gamma(B_{\mathrm{cyc}}) = (g'_\gamma(\pi), \dots, g'_\gamma(\pi))$$

for some $g'_\gamma \in \mathbf{F}[[\pi]]$. Since $(\varphi - 1)g'_\gamma(\pi) = 0$, we must have in fact $g'_\gamma(\pi) = g'_\gamma \in \mathbf{F}$. In particular, $g'_\eta = \nu$. Moreover, $\gamma \mapsto g'_\gamma$ defines a homomorphism $\Gamma \to \mathbf{F}$. Thus if $\gamma = \eta^{n_\gamma}$ modulo Γ_2, then

$$\mu_\gamma(B_{\mathrm{cyc}}) = \nu\overline{n}_\gamma(1, \dots, 1).$$

Lemma 6.7. *The extensions $[B_{\mathrm{nr}}], [B_0], \dots, [B_{f-1}] \in \mathrm{Ext}^1(M_{\vec{0}}, M_{\vec{0}})$ are linearly independent, and therefore form a basis.*

Proof. Suppose that $E=\beta B_{\mathrm{nr}}+\beta_0 B_0+\cdots+\beta_{f-1}B_{f-1}$ is a coboundary. By adding some coboundary B we have

$$\begin{aligned} e_0\mu_\varphi(E+B) &= \beta+\beta_0(-H(\pi^p)+H(\pi))+\beta_1(-H(\pi^{p^2})+H(\pi^p))+\cdots \\ &\quad +\beta_{f-2}(-H(\pi^{p^{f-1}})+H(\pi^{p^{f-2}}))+\beta_{f-1}(-H(\pi^{p^f})+H(\pi^{p^{f-1}})) \\ &= \beta+\beta_0 H(\pi)+(\beta_1-\beta_0)H(\pi^p)+\cdots \\ &\quad +(\beta_{f-1}-\beta_{f-2})H(\pi^{p^{f-1}})-\beta_{f-1}H(\pi^{p^f}) \\ &= (\Phi-1)\Bigg(\sum_{j\geqslant s} b_j\pi^j\Bigg) \end{aligned}$$

for some $\sum_{j\geqslant s} b_j\pi^j\in\mathbf{F}((\pi))$. Equating constant terms gives $\beta=0$. If $\beta_{f-1}\neq 0$, then $s=1-p$, $\beta_0 H(\pi)=-(b_{1-p}\pi^{1-p}+\cdots+b_{-1}\pi^{-1})$ and $\beta_0=\beta_1=\cdots=\beta_{f-1}$. It follows that $E=\beta_{f-1}\sum_{i=0}^{f-1}B_i$ is cohomologous to $\beta_{f-1}B_{\mathrm{cyc}}$, and therefore that B_{cyc} is a coboundary. Thus there exists $(b_0(\pi),\ldots,b_{f-1}(\pi))\in\mathbf{F}((\pi))^S$ such that

$$\begin{aligned} (\varphi-1)(b_0(\pi),\ldots,b_{f-1}(\pi)) &= (0,\ldots,0), \\ (\xi-1)(b_0(\pi),\ldots,b_{f-1}(\pi)) &= -\nu(1,\ldots,1), \end{aligned}$$

which is impossible, as the former implies that $b_0(\pi)=\cdots=b_{f-1}(\pi)\in\mathbf{F}$, so that we get $(\xi-1)(b_0(\pi),\ldots,b_{f-1}(\pi))=0$. Thus, $\beta_{f-1}=0$.

If $0\leqslant i\leqslant f-2$ is the largest such that $\beta_i\neq 0$, then $\mathrm{val}_\pi(e_0\mu_\varphi(E+B))=p^{i+1}(1-p)$, which leads to an easy contradiction. Thus, $\beta_i=0$ for all $0\leqslant i\leqslant f-2$. □

We now assume $f=2$ and compute the spaces of bounded extensions. We then have the following cases to consider:

- $J=S$, $a_0=a_1=p-1$;
- $J=\{1\}$, $b_0=1$, $a_1=p$ (for V_J^+);
- $J=\{1\}$, $b_0=p$, $a_1=1$ (for V_J^-);
- $J=\{0\}$, $a_0=p$, $b_1=1$ (for V_J^+);
- $J=\{0\}$, $a_0=1$, $b_1=p$ (for V_J^-);
- $J=\emptyset$, $b_0=b_1=p-1$.

Proposition 6.8. *If $f=2$, $C=1$, $\vec{c}=\vec{0}$ and $A\in\mathbf{F}^\times$ then:*

(i) *$V_S=\mathrm{Ext}^1(M_{\vec{0}},M_{\vec{0}})$;*

(ii) *$V^+_{\{i\}}=\langle[B_{\mathrm{nr}}],[B_i]\rangle$ for $i=0,1$;*

(iii) *$V^-_{\{i\}}=\langle[B_{\mathrm{nr}}]\rangle$ for $i=0,1$;*

(iv) *$V_\emptyset=\{0\}$.*

Proof. (i) We have $\langle\vec{c}\,\rangle_S=(\pi^{p-1},\pi^{p-1})$ and it is straightforward to check that $\iota[B_0]$, $\iota[B_1]$ and $\iota[B_{\mathrm{nr}}]$ are bounded.

(ii) Suppose $J=\{1\}$. Then $b_0=1$, $a_1=p$ and $\langle\vec{c}\,\rangle_{\{1\}}=(\pi^{p-1},1)$ and it is straightforward to check that $\iota[B_1]$ and $\iota[B_{\mathrm{nr}}]$ are bounded. Therefore, it suffices to prove that $\iota[B_{\mathrm{cyc}}]$ is not bounded. So suppose that B is a coboundary such that $\iota(B_{\mathrm{cyc}}+B)$ has $\mu_\varphi\in\mathbf{F}[[\pi]]^S$ and $\mu_\xi\in\pi\mathbf{F}[[\pi]]^S$. Then

$$\mu_\varphi(B_{\mathrm{cyc}}+B)=\mu_\varphi(B)=(b_1(\pi^p)-b_0(\pi),b_0(\pi^p)-b_1(\pi))$$

https://doi.org/10.1112/S0010437X1000504X Published online by Cambridge University Press

for some $b_0(\pi), b_1(\pi) \in \mathbf{F}((\pi))$, and $(A\pi^{p-1}, \pi^{p(p-1)})\mu_\varphi(B) \in \mathbf{F}[[\pi]]^S$. Letting $v_0 = \mathrm{val}_\pi(b_0(\pi))$ and $v_1 = \mathrm{val}_\pi(b_1(\pi))$, we see that $v_0 \geqslant 1-p$ and $v_1 \geqslant 0$. Therefore

$$\mu_\xi(B_{\mathrm{cyc}} + B) = (-\nu + (\xi - 1)b_0(\pi), -\nu + (\xi - 1)b_1(\pi)),$$

and since $-\nu + (\xi-1)b_1(\pi)$ has constant term $-\nu$, we arrive at a contradiction.

The case $J = \{0\}$ is the same.

(iii) Suppose again that $J = \{1\}$. Now we have $b_0 = p$, $a_1 = 1$ and $\langle \vec{c}\,\rangle_{\{1\}} = (1, \pi^{1-p})$ and it is clear that $\iota[B_{\mathrm{nr}}]$ is bounded. Therefore, it suffices to prove that, if $E = \beta_0 B_0 + \beta_1 B_1$ with β_0, β_1 such that $\iota[E]$ is bounded, then $\beta_0 = \beta_1 = 0$. The argument in the proof of Lemma 6.7 shows that $\beta_0 = \beta_1$, so we are reduced to proving that $\iota[B_{\mathrm{cyc}}]$ is not bounded. The proof of this is similar to the proof of part (ii).

The case $J = \{0\}$ is the same.

(iv) Now we have $\langle \vec{c}\,\rangle_\emptyset = (\pi^{1-p}, \pi^{1-p})$, and if $\iota[E]$ is bounded then $\mu_\varphi(E + B) \in \pi^{p-1}\mathbf{F}[[\pi]]^S$ for some coboundary B. The proof of Lemma 6.7 then shows that E is cohomologous to a multiple of B_{cyc}, and the boundedness of $\iota[B_{\mathrm{cyc}}]$ yields a contradiction as above. □

6.3 Case $p = 2$

We assume $p = 2$ throughout this section. Now Γ is not pro-cyclic; we write $\Gamma = \Delta \times \Gamma_2$, where $\Delta = \langle \eta \rangle$ with $\chi(\eta) = -1$, so Δ has order 2, and we choose a topological generator ξ of Γ_2.

Lemma 6.9. *We have $\lambda_\eta \equiv 1 + \pi \bmod \pi^{2^f}\mathbf{F}[[\pi]]$. If $\gamma \in \Gamma_2$, then $\lambda_\gamma \equiv 1 \bmod \pi^3\mathbf{F}[[\pi]]$.*

Proof. The first assertion follows from the fact that

$$\lambda_\eta^{2^f - 1} = \eta(\pi)/\pi = (1+\pi)^{-1}.$$

For the second assertion, note that, if $\gamma \in \Gamma_2$, then $\chi(\gamma) \equiv 1 \bmod 4$, so $\gamma(\pi)/\pi \equiv 1 \bmod \pi^3\mathbf{F}[[\pi]]$. □

Let $C \in \mathbf{F}^\times$ and $\vec{c} = (c_0, \ldots, c_{f-1}) \in \{0,1\}^S$ with some $c_j = 0$ be given. First assume that $C \neq 1$ if $\vec{c} = \vec{0}$, so that $C\pi^{\Sigma_j \vec{c}}\Phi - 1 : \mathbf{F}[[\pi]] \to \mathbf{F}[[\pi]]$ defines a valuation-preserving bijection for all $j \in S$. As in the case $p > 2$, we will define for each $i \in S$ an element $H_i(\pi) \in \mathbf{F}((\pi))$ such that

$$(\lambda_\gamma^{\Sigma_i \vec{c}}\gamma - 1)H_i(\pi) \in \mathbf{F}[[\pi]]$$

for all $\gamma \in \Gamma$. If $c_i = 0$, we let $H_i(\pi) = \pi^{-1}$; otherwise we use the following lemma.

Lemma 6.10. *Suppose that $c_i = 1$, and $r \in 0, \ldots, f-1$ is such that $c_{i+1} = \cdots = c_{i+r} = 0$ and $c_{i+r+1} = 1$. Let*

$$H_i(\pi) = \pi^{1-2^{r+2}} + \pi^{1+2^r-2^{r+2}}.$$

Then $(\lambda_\gamma^{\Sigma_i \vec{c}}\gamma - 1)H_i(\pi) \in \mathbf{F}[[\pi]]$ for all $\gamma \in \Gamma$.

Proof. Note that we can assume $f \geqslant 2$. We have

$$\lambda_\gamma^{\Sigma_i}\gamma\pi^{1-2^{r+2}} = \lambda_\gamma^{\Sigma_i}\left(\frac{\gamma(\pi)}{\pi}\right)^{1-2^{r+2}}\pi^{1-2^{r+2}} = \lambda_\gamma^{\Sigma_i + (2^f-1)(1-2^{r+2})}\pi^{1-2^{r+2}}.$$

Note that $\Sigma_i = 1$ if $r = f-1$ and $\Sigma_i \equiv 1 + 2^{r+1} \bmod 2^{r+2}$ otherwise. In either case we have $\Sigma_i + (2^f - 1)(1 - 2^{r+2}) \equiv 2^{r+1} \bmod 2^{r+2}$. It follows that

$$(\lambda_\gamma^{\Sigma_i}\gamma - 1)(\pi^{1-2^{r+2}}) \equiv (\lambda_\gamma^{2^{r+1}} - 1)\pi^{1-2^{r+2}} \mod \mathbf{F}[[\pi]].$$

https://doi.org/10.1112/S0010437X1000504X Published online by Cambridge University Press

Similarly we find that

$$(\lambda_\gamma^{\Sigma_i}\gamma - 1)(\pi^{1+2^r-2^{r+2}}) \equiv (\lambda_\gamma^{2^r} - 1)\pi^{1+2^r-2^{r+2}} \mod \mathbf{F}[[\pi]].$$

Lemma 6.9 gives $\lambda_\eta^{2^s} \equiv 1 + \pi^{2^s} \bmod \pi^{2^{s+f}}$ for $s \geqslant 0$, and it follows that

$$(\lambda_\eta^{2^{r+1}} - 1)\pi^{1-2^{r+2}} \equiv (\lambda_\eta^{2^r} - 1)\pi^{1+2^r-2^{r+2}} \equiv \pi^{1+2^{r+1}-2^{r+2}} \mod \mathbf{F}[[\pi]].$$

Therefore the lemma holds for $\gamma = \eta$. We also get that $\lambda_\gamma^{2^s} \equiv 1 \bmod \pi^{3\times 2^s}$ for $\gamma \in \Gamma_2$, from which it follows that $(\lambda_\gamma^{2^{r+1}} - 1)\pi^{1-2^{r+2}}$ and $(\lambda_\gamma^{2^r} - 1)\pi^{1+2^r-2^{r+2}}$ are in $\mathbf{F}[[\pi]]$. The lemma therefore holds for $\gamma \in \Gamma_2$ as well, and we deduce from Lemma 4.5 that it holds for all $\gamma \in \Gamma$. □

By the bijectivity of $C\pi^{\Sigma_0\vec{c}}\Phi - 1$, for each $\gamma \in \Gamma$ we have a unique $G_i(\pi) = G_{i,\gamma}(\pi) \in \mathbf{F}[[\pi]]$ such that $(C\pi^{\Sigma_0\vec{c}}\Phi - 1)(G_i(\pi)) = (\lambda_\gamma^{\Sigma_i\vec{c}}\gamma - 1)(H_i(\pi))$. Then letting

$$\begin{aligned}
\mu_\varphi(B_i) &= (0, \ldots, 0, H_i(\pi), 0, \ldots, 0),\\
\mu_\gamma(B_i) &= (G_0(\pi), \ldots, G_i(\pi), \ldots, G_{f-1}(\pi)),
\end{aligned}$$

where

$$\begin{aligned}
G_0(\pi) &= C\pi^{c_0+2c_1+\cdots+2^{i-1}c_{i-1}}G_i(\pi^{2^i}),\\
G_1(\pi) &= \pi^{c_1+2c_2+\cdots+2^{i-2}c_{i-1}}G_i(\pi^{2^{i-1}}),\\
&\vdots\\
G_{i-1}(\pi) &= \pi^{c_{i-1}}G_i(\pi^2),\\
G_{i+1}(\pi) &= C\pi^{c_{i+1}+2c_{i+2}\cdots+2^{f-2}c_{i-1}}G_i(\pi^{2^{f-1}}),\\
&\vdots\\
G_{f-1}(\pi) &= C\pi^{c_{f-1}+2c_0+\cdots+2^{i}c_{i-1}}G_i(\pi^{2^{i+1}}),
\end{aligned}$$

gives rise to an extension $[B_i] \in \mathrm{Ext}^1(M_{\vec{0}}, M_{C\vec{c}})$. By almost identical arguments to the case $p > 2$, one finds that $[B_0], \ldots, [B_{f-1}]$ are linearly independent, so that they form a basis.

Now suppose that $C = 1$ and $\vec{c} = \vec{0}$. We can define, similarly to the $p > 2$ case, $[B_0], \ldots, [B_{f-2}], [B_{f-1}]$ such that

$$\begin{aligned}
\mu_\varphi(B_0) &= (\pi^{-2} + \pi^{-1}, 0, \ldots, 0),\\
\mu_\varphi(B_1) &= (0, \pi^{-2} + \pi^{-1}, 0, \ldots, 0),\\
&\vdots\\
\mu_\varphi(B_{f-1}) &= (0, \ldots, 0, \pi^{-2} + \pi^{-1}).
\end{aligned}$$

As before, each B_i is cohomologous to B_i' with

$$\mu_\varphi(B_i) = (0, \ldots, 0, \pi^{-1}, \pi^{-1}, 0, \ldots, 0),$$

the non-zero entries being in the $i, i+1$ coordinates (unless $f = 1$, in which case $\mu_\varphi(B_0) = 0$). We again set $B_{\mathrm{cyc}} = \sum_{i=0}^{f-1} B_i'$, and define a cocycle B_{nr} by setting

$$\begin{aligned}
\mu_\varphi(B_{\mathrm{nr}}) &= (1, 0, \ldots, 0),\\
\mu_\gamma(B_{\mathrm{nr}}) &= (0, 0, \ldots, 0)
\end{aligned}$$

for all $\gamma \in \Gamma$.

https://doi.org/10.1112/S0010437X1000504X Published online by Cambridge University Press

The difference now is that, if $p=2$, then $\dim_{\mathbf{F}} \mathrm{Ext}^1(M_{\vec{0}}, M_{\vec{0}}) = f+2$, so we need one more basis element. We define B_{tr} by

$$\mu_{\varphi}(B_{\mathrm{nr}}) = (0, 0, \dots, 0),$$
$$\mu_{\gamma}(B_{\mathrm{nr}}) = n_{\gamma}(1, 1, \dots, 1),$$

where $n_\gamma = 0$ if $\gamma \in \Gamma_3 \cup \eta\Gamma_3$, and $n_\gamma = 1$ otherwise (so $\gamma \mapsto n_\gamma$ defines a homomorphism $\Gamma \to \mathbf{F}$). One can check as in the case $p>2$ that the elements $[B_{\mathrm{nr}}], [B_0], [B_1], \dots, [B_{f-1}], [B_{\mathrm{tr}}]$ are linearly independent, hence form a basis for $\mathrm{Ext}^1(M_{\vec{0}}, M_{\vec{0}})$.

Finally we assume $f=2$ and compute the spaces of bounded extensions. There are three possibilities to consider:

(i) $\vec{c} = (0,1)$ or $(1,0)$;
(ii) $\vec{c} = (0,0)$ and $C \neq 1$;
(iii) $\vec{c} = (0,0)$ and $C = 1$.

We omit the proofs of the following which are essentially the same as for $p>2$.

Proposition 6.11. *If $\vec{c} = (0,1)$ or $(1,0)$, then:*

- $V_S = \mathrm{Ext}^1(M_{\vec{0}}, M_{C\vec{c}})$;
- *if $\vec{c} = (0,1)$, then $V_{\{0\}} = V_{\{1\}} = \mathbf{F}[B_0]$;*
- *if $\vec{c} = (1,0)$, then $V_{\{0\}} = V_{\{1\}} = \mathbf{F}[B_1]$;*
- $V_{\emptyset} = 0$.

Proposition 6.12. *If $\vec{c} = (0,0)$ and $C \in \mathbf{F}^\times$ with $C \neq 1$, then:*

- $V_S^+ = V_S^- = \mathrm{Ext}^1(M_{\vec{0}}, M_{C\vec{0}})$;
- $V_{\{1\}}^+ = \mathbf{F}[B_0 + B_1]$;
- $V_{\{0\}}^+ = \mathbf{F}[CB_0 + B_1]$;
- $V_{\{1\}}^- = V_{\{0\}}^- = V_{\emptyset}^+ = V_{\emptyset}^- = 0$.

Proposition 6.13. *If $\vec{c} = (0,0)$ and $C = 1$, then:*

- $V_S^+ = V_S^- = \mathrm{Ext}^1(M_{\vec{0}}, M_{\vec{0}})$;
- *$V_{\{i\}}^+ = \mathbf{F}[B_{\mathrm{nr}}] \oplus \mathbf{F}[B_i]$ for $i = 0, 1$;*
- *$V_{\{i\}}^- = \mathbf{F}[B_{\mathrm{nr}}]$ for $i = 0, 1$;*
- $V_{\emptyset}^+ = V_{\emptyset}^- = 0$.

Remark 6.14. With a view towards relating bounded extensions to crystalline ones, we would have liked $V_S^- = \mathbf{F}[B_{\mathrm{nr}}] \oplus \mathbf{F}[B_0] \oplus \mathbf{F}[B_1]$ in the trivial case. This could have been achieved with a more restrictive definition of boundedness, requiring for example that $\mu_\gamma \in \pi^2 \mathbf{F}[[\pi]]^S$ for $\gamma \in \Gamma_2$ if $p=2$. However, we opted instead for the definition we found most uniform and easiest to work with.

7. Crystalline $\Rightarrow$ bounded

The paper [BDJ10] formulates conjectures concerning weights of mod p Hilbert modular forms in terms of the associated local Galois representations $G_K \to \mathrm{GL}_2(\mathbf{F})$. When the local representation is reducible, i.e., of the form $\left(\begin{smallmatrix} \chi_1 & * \\ 0 & \chi_2 \end{smallmatrix}\right)$, the set of weights is determined by the associated class in $H^1(G_K, \mathbf{F}(\chi_1\chi_2^{-1}))$, or more precisely whether the class lies in certain distinguished subspaces. These subspaces are defined in terms of reductions of crystalline extensions of crystalline characters. Our aim is to relate these to the spaces of bounded extensions we computed in the preceding sections. The idea is to show that Wach modules over $\mathbf{A}^+_{K,F}$ associated to crystalline extensions have bounded reductions. This is easily seen to be true when the Wach module itself is the extension of two Wach modules; the problem is that this is not always the case. Recall that Theorem 2.17 establishes an equivalence of categories between crystalline representations and Wach modules over $\mathbf{B}^+_K$. We note however that $\mathbf{N}$ does not define an exact functor from G_K-stable lattices to $\mathbf{A}^+_K$-modules.

Example 7.1. Let $K = \mathbf{Q}_p$ and $V = \mathbf{Q}_p(1-p) \oplus \mathbf{Q}_p$. The corresponding Wach module is $\mathbf{N}(V) = \mathbf{B}^+_{\mathbf{Q}_p} e_1 \oplus \mathbf{B}^+_{\mathbf{Q}_p} e_2$ with:

- $\varphi(e_1) = q^{p-1} e_1$ and $\gamma(e_1) = (\gamma(\pi)/\chi(\gamma)\pi)^{p-1} e_1$ for $\gamma \in \Gamma$;
- φ and Γ acting trivially on e_2.

Let $f_1 = p^{-1}(e_1 - \pi^{p-1} e_2)$ and consider the $\mathbf{A}^+_{\mathbf{Q}_p}$-lattice $N = \mathbf{A}^+_{\mathbf{Q}_p} f_1 \oplus \mathbf{A}^+_{\mathbf{Q}_p} e_2$ in $\mathbf{N}(V)$. Then it is straightforward to check that N is a Wach module over $\mathbf{A}^+_{\mathbf{Q}_p}$, hence corresponds to a $G_{\mathbf{Q}_p}$-stable lattice T in V. Such a lattice necessarily fits into an exact sequence

$$0 \to \mathbf{Z}_p(1-p) \to T \to \mathbf{Z}_p \to 0$$

of $\mathbf{Z}_p$-representations of $G_{\mathbf{Q}_p}$, but there is no surjective morphism $\alpha : N \to \mathbf{A}^+_{\mathbf{Q}_p}$. Indeed, the image would have to be generated over $\mathbf{A}^+_{\mathbf{Q}_p}$ by elements $\alpha(f_1)$ and $\alpha(e_2)$ satisfying $p\alpha(f_1) = -\pi^{p-1}\alpha(e_2)$, and hence could not be free over $\mathbf{A}^+_{\mathbf{Q}_p}$. This example is somewhat special since V is split and T can also be written as an extension

$$0 \to \mathbf{Z}_p \to T \to \mathbf{Z}_p(1-p) \to 0,$$

which does correspond to an extension of Wach modules. However, it illustrates the problem, which we shall see also occurs for lattices in non-split extensions of $\mathbf{Q}_p$-representations.

We will prove under certain hypotheses that the relevant extensions of $\mathbf{Z}_p$-representations do in fact correspond to extensions of Wach modules. In particular, we will show this holds in the generic case, and in all but a few special cases when $f = 2$. As a result, we will be able to give a complete description of the distinguished subspaces in [BDJ10] in terms of (φ, Γ)-modules in the generic case and the case $f = 2$.

7.1 The extension lemma

We first establish a general criterion for a Wach module over $\mathbf{A}^+_{K,F}$ to arise from an extension of two Wach modules. We consider extensions of crystalline representations of arbitrary dimension since it is no more difficult than the case of one-dimensional representations.

Suppose that we have an exact sequence

$$0 \to V_1 \to V \to V_2 \to 0$$

of crystalline $\mathbf{Q}_p$-representations of G_K with Hodge–Tate weights in $[0, b]$ for some $b \geqslant 0$. We shall identify V_1 with a subrepresentation of V. By Theorem 2.17, we have an exact sequence of corresponding Wach modules over $\mathbf{B}^+_K$:

$$0 \to M_1 \to M \to M_2 \to 0,$$

https://doi.org/10.1112/S0010437X1000504X Published online by Cambridge University Press

where $M = \mathbf{N}(V)$, $M_1 = \mathbf{N}(V_1) = \mathbf{N}(V) \cap \mathbf{D}(V_1)$ and M_2 is the image of $\mathbf{N}(V)$ in $\mathbf{D}(V_2)$. Now suppose that T is a G_K-stable lattice in V. Letting $T_1 = T \cap V_1$ and $T_2 = T/T_1$, we have an exact sequence

$$0 \to T_1 \to T \to T_2 \to 0$$

of $\mathbf{Z}_p$-representations of G_K. Letting $N = \mathbf{N}(T) = M \cap \mathbf{D}(T)$ be the Wach module in $M = \mathbf{N}(V)$ corresponding to T, we see that $N_1 := N \cap M_1 = \mathbf{N}(T_1)$ since

$$N \cap M_1 = \mathbf{N}(T) \cap \mathbf{D}(V_1) = \mathbf{D}(T) \cap \mathbf{N}(V) \cap \mathbf{D}(V_1) = \mathbf{D}(T) \cap \mathbf{N}(V_1) = \mathbf{D}(T_1) \cap \mathbf{N}(V_1).$$

The quotient $N_2 := N/N_1$ is a finitely generated torsion-free $\mathbf{A}_K^+$-module with an action of φ and Γ such that $q^b N_2 \subset \varphi^*(N_2)$ and Γ acts trivially on $N_2/\pi N_2$. (Note that N_2 is torsion-free since $N/N_1 \hookrightarrow M_2$, but N_2 is not necessarily free, as we will see below.) Furthermore $\mathbf{N}(T) \to \mathbf{N}(T_2)$ induces an injective homomorphism $N_2 \to \mathbf{N}(T_2)$, which becomes an isomorphism on tensoring with $\mathbf{B}_K^+$.

Letting $\mathbf{E}_K^+ = \mathbf{A}_K^+/p\mathbf{A}_K^+$, $\overline{N} = N/pN$ and $\overline{N}_i = N_i/pN_i$, we know also that

$$\overline{N}[1/\pi] = \mathbf{E}_K \otimes_{\mathbf{E}_K^+} \overline{N} \quad \text{and} \quad \overline{N}_i[1/\pi] = \mathbf{E}_K \otimes_{\mathbf{E}_K^+} \overline{N}_i$$

for $i = 1, 2$ are the (φ, Γ)-modules over $\mathbf{E}_K$ corresponding to the reductions $\bmod\, p$ of the corresponding G_K-stable lattices. Moreover $\overline{N}_1$ and $\overline{N}$ are free over $\mathbf{E}_K^+$ and the homomorphism $\overline{N}_1 \to \overline{N}$ is injective; we identify $\overline{N}_1$ with a submodule of $\overline{N}$.

Lemma 7.2. *The following are equivalent:*

(i) *the homomorphism* $\mathbf{N}(T) \to \mathbf{N}(T_2)$ *is surjective;*

(ii) $N_2 = \mathbf{N}(T)/\mathbf{N}(T_1)$ *is free over* $\mathbf{A}_K^+$*; and*

(iii) $\overline{N}_1 = \overline{N} \cap \mathbf{D}(T_1/pT_1)$.

Proof. If $\mathbf{N}(T) \to \mathbf{N}(T_2)$ is surjective, then $N_2 \cong \mathbf{N}(T_2)$ is free over $\mathbf{A}_K^+$. Conversely, if N_2 is free, then $\mathbf{N}(T)$ maps onto a Wach module over $\mathbf{A}_K^+$ in $\mathbf{N}(V_2)$, which by Theorem 2.17 is of the form $\mathbf{N}(T_2')$ for some G_K-stable lattice T_2' in V_2; moreover $\mathbf{N}(T_2') \subset \mathbf{N}(T_2)$ implies that $T_2' \subset T_2$. On the other hand, since $\mathbf{N}(T)$ maps to $\mathbf{N}(T_2')$, $\mathbf{D}(T)$ maps to $\mathbf{D}(T_2')$, hence T maps to T_2', and therefore $T_2 = T_2'$.

Since $\mathbf{B}_K^+ \otimes_{\mathbf{A}_K^+} N_2 \cong \mathbf{N}(V_2)$ is free of rank $d_2 := \dim_{\mathbf{Q}_p} V_2$ over B_K^+, it follows from Nakayama's lemma that N_2 is free over $\mathbf{A}_K^+$ if and only if $N_2/pN_2 = \overline{N}/\overline{N}_1$ is free of rank d_2 over $\mathbf{E}_K^+$. Since $\overline{N}$ and $\overline{N}_1$ are free over $\mathbf{E}_K^+$ and the difference of their ranks is d_2, this in turn is equivalent to $\overline{N}/\overline{N}_1$ being torsion-free over $\mathbf{E}_K^+$, which in turn is equivalent to $\overline{N}_1 = \overline{N} \cap \overline{N}_1[1/\pi]$. $\square$

Example 7.3. Returning to Example 7.1, note that, since $e_1 - \pi^{p-1}e_2 \in pN$, we have $\pi^{p-1}\overline{e}_2 = -\overline{e}_1 \in \overline{N}$, so $\overline{e}_2 = -\pi^{1-p}\overline{e}_1 \in \overline{N}_1'$, where $\overline{N}_1' = \overline{N} \cap \overline{N}_1[1/\pi]$. Thus we find in this case that $\overline{N}_1 = \mathbf{F}_p[[\pi]]\overline{e}_1$, but $\overline{N}_1' = \pi^{1-p}\mathbf{F}_p[[\pi]]\overline{e}_1$, so the criterion of the lemma is not satisfied.

We remark that everything above holds with coefficients; in particular, if

$$0 \to T_1 \to T \to T_2 \to 0$$

is an exact sequence of G_K-stable $\mathcal{O}_F$-lattices in crystalline representations, then the sequence

$$0 \to \mathbf{N}(T_1) \to \mathbf{N}(T) \to \mathbf{N}(T_2) \to 0$$

of $\mathbf{A}_{K,F}^+$-modules is exact if and only if

$$\mathbf{N}(T_1)/\varpi_F\mathbf{N}(T_1) = (\mathbf{N}(T)/\varpi_F\mathbf{N}(T)) \cap \mathbf{D}(T_1/\varpi_F T_1).$$

https://doi.org/10.1112/S0010437X1000504X Published online by Cambridge University Press

7.2 Extensions of rank one modules

We now specialize to the case where V_1 and V_2 are one-dimensional over F, with labeled Hodge–Tate weights $(b_{f-1}, b_0, \ldots, b_{f-2})$ and $(a_{f-1}, a_0, \ldots, a_{f-2})$ where each $a_i, b_i \geqslant 0$. Suppose that we have an exact sequence

$$0 \to V_1 \to V \to V_2 \to 0$$

of crystalline F-representations of G_K, and T is a G_K-stable $\mathcal{O}_F$-lattice in V. We thus have exact sequences

$$0 \to T_1 \to T \to T_2 \to 0 \quad \text{and} \quad 0 \to \overline{T}_1 \to \overline{T} \to \overline{T}_2 \to 0,$$

where each T_i is a G_K-stable $\mathcal{O}_F$-lattices in V_i and $\bar{\cdot}$ denotes reduction modulo ϖ_F. We let $N = \mathbf{N}(T)$ be the Wach module over $\mathbf{A}^+_{K,F}$ corresponding to T, and $\overline{N}$ its reduction modulo ϖ_F. Thus $\overline{N}$ is a free rank two $\mathbf{E}^+_{K,F}$-module with an action of φ and Γ such that Γ acts trivially modulo $\overline{N}/\pi\overline{N}$. Furthermore $\mathbf{E}_{K,F} \otimes_{\mathbf{E}^+_{K,F}} \overline{N} \cong \mathbf{D}(\overline{T})$ as (φ, Γ)-modules over $\mathbf{E}_{K,F}$. Letting $\overline{N}'_1 = \mathbf{D}(\overline{T}_1) \cap \overline{N}$ and $\overline{N}'_2 = \overline{N}/\overline{N}'_1$, we see that each $\overline{N}'_i$ is an $\mathbf{E}^+_{K,F}$-lattice in $\mathbf{D}(\overline{T}_i)$, stable under φ and Γ with Γ acting trivially modulo π.

From the classification of rank one (φ, Γ)-modules over $\mathbf{E}_{K,F}$, we know that $\mathbf{D}(\overline{T}_1) \cong M_{C\vec{c}} = \mathbf{E}_{K,F}e$ for some $C \in \mathbf{F}^\times$ and $\vec{c} \in \mathbf{Z}^S$. Under this isomorphism, $\overline{N}'_1$ corresponds to a submodule of the form $(\pi^{r_0}, \pi^{r_1}, \ldots, \pi^{r_{f-1}})\mathbf{E}^+_{K,F}e$. Since Γ acts trivially on $\mathbf{E}^+_{K,F}e/\pi\mathbf{E}^+_{K,F}e$ and on $\overline{N}'_1/\pi\overline{N}'_1$, we see that $(p-1)|r_i$ for $i = 0, \ldots, f-1$. Moreover,

$$\varphi^*(\overline{N}'_1) = (\pi^{(p-1)b'_0}, \ldots, \pi^{(p-1)b'_{f-1}})\overline{N}'_1$$

for some $b'_0, \ldots, b'_{f-1}$, all non-negative since $\overline{N}'_1$ is stable under φ. Similarly we have

$$\varphi^*(\overline{N}'_2) = (\pi^{(p-1)a'_0}, \ldots, \pi^{(p-1)a'_{f-1}})\overline{N}'_2$$

for some $a'_0, \ldots, a'_{f-1} \geqslant 0$.

For the following proposition, recall that $\Sigma_j(\vec{c}\,) = \sum_{i=0}^{f-1} c_{i+j}p^i$, where c_k is defined for $k \in \mathbf{Z}$ by setting $c_k = c_{k'}$ if $k \equiv k' \bmod f$. We also define a partial ordering on $\mathbf{Z}^S$ by $\vec{c} \leqslant \vec{c}'$ if $c_i \leqslant c'_i$ for all i.

Proposition 7.4. *With the above notation, we have:*

(i) $\min(a_i, b_i) \leqslant a'_i \leqslant \max(a_i, b_i)$, $\min(a_i, b_i) \leqslant b'_i \leqslant \max(a_i, b_i)$ *and* $a'_i + b'_i = a_i + b_i$ *for* $i = 0, \ldots, f-1$;

(ii) *if* $\vec{a} \leqslant \vec{b}$ *or* $\vec{b} \leqslant \vec{a}$, *then* $\{\vec{a}, \vec{b}\} = \{\vec{a}', \vec{b}'\}$;

(iii) $\Sigma_j(\vec{a}') \geqslant \Sigma_j(\vec{a})$, $\Sigma_j(\vec{b}') \leqslant \Sigma_j(\vec{b})$, $\Sigma_j(\vec{a}') \equiv \Sigma_j(\vec{a}) \bmod (p^f - 1)$ *and* $\Sigma_j(\vec{b}') \equiv \Sigma_j(\vec{b}) \bmod (p^f - 1)$ *for* $j = 0, \ldots, f-1$; *and*

(iv) $\vec{a} = \vec{a}'$ *if and only if* $\vec{b} = \vec{b}'$ *if and only if* $\mathbf{N}(T) \to \mathbf{N}(T_2)$ *is surjective.*

Proof. (i) We first prove that $a'_i + b'_i = a_i + b_i$ for $i = 0, \ldots, f-1$. The $\mathbf{A}^+_{K,F}$-module $\wedge^2_{\mathbf{A}^+_{K,F}} \mathbf{N}(T)$ inherits actions of φ and Γ, making it a Wach module in $\wedge^2_{\mathbf{B}^+_{K,F}} \mathbf{N}(V) \cong \mathbf{N}(\wedge^2_F V)$, hence it corresponds to an $\mathcal{O}_F$-lattice in $\wedge^2_F V$. The same is true of $\mathbf{N}(T_1) \otimes_{\mathbf{A}^+_{K,F}} \mathbf{N}(T_2)$; since any two such lattices are scalar multiples of each other, it follows that the corresponding Wach modules over $\mathbf{A}^+_{K,F}$ are isomorphic, and hence that

$$\overline{N}'_1 \otimes_{\mathbf{E}^+_{K,F}} \overline{N}'_2 \cong \wedge^2_{\mathbf{E}^+_{K,F}} \overline{N} \cong (\mathbf{N}(T_1)/\varpi_F\mathbf{N}(T_1)) \otimes_{\mathbf{E}^+_{K,F}} (\mathbf{N}(T_2)/\varpi_F\mathbf{N}(T_2))$$

https://doi.org/10.1112/S0010437X1000504X Published online by Cambridge University Press

as $\mathbf{E}^{+}_{K,F}$-modules. Moreover, the isomorphisms are compatible with the action of φ, so $a'_i + b'_i = a_i + b_i$ for all i.

For the inequalities, suppose first that $\min(a_i, b_i) = 0$ for each i. Since $a_i + b_i = a'_i + b'_i$, we know that $a'_i + b'_i \leqslant \max(a_i, b_i)$ for each i, and the result follows. The general case follows by twisting T by a character with the correct Hodge structure and $\mathbf{N}(T)$ by the corresponding Wach module.

(ii) By twisting we can again reduce to the case where $\min(a_i, b_i) = 0$ for each i. The condition $\vec{a} \leqslant \vec{b}$ or $\vec{b} \leqslant \vec{a}$ becomes $\vec{a}$ or $\vec{b} = \vec{0}$, and we must show that $\vec{a}'$ or $\vec{b}' = \vec{0}$. The result then follows from the equality $\vec{a} + \vec{b} = \vec{a}' + \vec{b}'$ proved in (i).

If $\vec{a}' \neq \vec{0}$ and $\vec{b}' \neq \vec{0}$, then $\varphi^f(\overline{N}'_i) \subset \pi \overline{N}'_i$ for $i = 1, 2$, so that $\varphi^{2f}(\overline{N}) \subset \pi \overline{N}$. This means that φ is topologically nilpotent on N in the sense that $\varphi(N) \subset (\pi, \varpi_F)N$ for some $n > 0$.

On the other hand, the F-representation V of G_K is *ordinary* in the sense that there is an exact sequence

$$0 \to V_0 \to V \to V/V_0 \to 0,$$

where V_0 is unramified, V/V_0 is positive crystalline and each is one-dimensional over F. (If $\vec{b} = \vec{0}$, then take $V_0 = V_1$; if $\vec{b} \neq \vec{0}$ and $\vec{a} = \vec{0}$, then the sequence $0 \to V_1 \to V \to V_2 \to 0$ splits and we can take V_0 to be the image of V_2.) Since $\mathbf{D}_{\mathrm{crys}}(V_0) \subset \mathbf{D}_{\mathrm{crys}}(V) \cong \mathbf{N}(V)/\pi\mathbf{N}(V)$ and $N/\pi N$ is a φ-stable lattice in $\mathbf{N}(V)/\pi\mathbf{N}(V)$, we see that there is an element $e_0 \in N/\pi N$ such that $e_0 \notin \varpi_F(N/\pi N)$ and $\phi(e_0) = ue_0$ for some $u \in (\mathcal{O}_F \otimes \mathcal{O}_K)^\times$. Choosing a lift $\tilde{e}_0 \in N$ of e_0, we have that $\varphi(\tilde{e}_0) \in u\tilde{e}_0 + (\pi, \varpi_F)N$, contradicting that φ is topologically nilpotent on N.

(iii) Since $\overline{N}_1 = \mathbf{N}(T_1)/\varpi_F\mathbf{N}(T_1)$ is contained in $\overline{N}'_1$, we can write $\overline{N}_1 = (\pi^{t_0}, \pi^{t_1}, \ldots, \pi^{t_{f-1}})\overline{N}'_1$ for some integers $t_0, t_1, \ldots, t_{f-1} \geqslant 0$. We therefore have

$$\begin{aligned}\phi^*(\overline{N_1}) &= (\pi^{pt_1}, \pi^{pt_2}, \ldots, \pi^{pt_{f-1}}, \pi^{pt_0})\phi^*(\overline{N}'_1)\\ &= (\pi^{b'_0+pt_1}, \pi^{b'_1+pt_2}, \ldots, \pi^{b'_{f-2}+pt_{f-1}}, \pi^{b'_{f-1}+pt_0})\overline{N}'_1.\end{aligned}$$

On the other hand, we also have

$$\begin{aligned}\phi^*(\overline{N_1}) &= (\pi^{b_0}, \pi^{b_1}, \ldots, \pi^{b_{f-1}})(\overline{N}_1)\\ &= (\pi^{b_0+t_0}, \pi^{b_1+t_1}, \ldots, \pi^{b_{f-1}+t_{f-1}})\overline{N}'_1.\end{aligned}$$

It follows that $b_j + t_j = b'_j + pt_{j+1}$ and thus $\Sigma_j(\vec{b}) + \sum_{i=0}^{f-1} t_{i+j}p^i = \Sigma_j(\vec{b}') + \sum_{i=0}^{f-1} t_{i+j+1}p^{i+1}$, and therefore that $\Sigma_j(\vec{b}) = t_j(p^f - 1) + \Sigma_j(\vec{b}')$. The assertions concerning $\Sigma_j(\vec{b}')$ follow, and those concerning $\Sigma_j(\vec{a}')$ then follow using (i).

(iv) We see from the proof of (iii) that the hypotheses of Lemma 7.2 are satisfied if and only if $\overline{N}_1 = \overline{N}'_1$ if and only if $\vec{t} = 0$. On the other hand, $\vec{b} = \vec{b}'$ if and only if $t_i = pt_{i+1}$ for $i = 0, \ldots, f-1$, which implies that $t_i = p^f t_i$ for $i = 0, \ldots, f-1$, hence is equivalent to $\vec{t} = \vec{0}$. That $\vec{a} = \vec{a}'$ if and only if $\vec{b} = \vec{b}'$ follows from (i). □

7.3 Generic case

In this subsection, we specialize to the generic case in the sense of § 5.2, namely $0 < c_i < p - 1$ for all i. Recall that if $J \subset S$, then there are integers a_i and b_i for $i \in S$ such that:

- $1 \leqslant a_i \leqslant p$ if $i \in J$, and $a_i = 0$ if $i \notin J$;
- $1 \leqslant b_i \leqslant p$ if $i \notin J$, and $b_i = 0$ if $i \in J$; and
- $\sum_{i\in S} b_i p^i - \sum_{i\in S} a_i p^i \equiv \sum_{i\in S} c_i p^i \bmod p^f - 1$.

Moreover, the a_i and b_i are uniquely determined by $\vec{c}$ and J except in the case where we can take either $a_i = p$ for $i \in J$ and $b_i = 1$ for $i \notin J$, or $a_i = 1$ for $i \in J$ and $b_i = p$ for $i \notin J$.

Lemma 7.5. *Suppose that $0 < c_i < p-1$ for all i. Then $a_i < p$ and $b_i < p$ for all i unless $\vec{c} = \vec{1}$, $J = \emptyset$ and $\vec{b} = \vec{p}$, or $\vec{c} = \overrightarrow{p-2}$, $J = S$ and $\vec{a} = \vec{p}$. In particular, $\vec{a}$ and $\vec{b}$ are uniquely determined by $\vec{c}$ and J except in the above two cases where we can also have $\vec{b}$ or $\vec{a} = \vec{1}$ instead of $\vec{p}$.*

Proof. Suppose that $b_i = p$ and consider $\Sigma_i(\vec{c})$. We have $\Sigma_i(\vec{c}) \equiv \Sigma_i(\vec{b}) - \Sigma_i(\vec{a}) \bmod (p^f - 1)$ and

$$1 + p + \cdots + p^{f-1} \leqslant \Sigma_i(\vec{c}) \leqslant (p^f - 1) - (1 + p + \cdots + p^{f-1}).$$

If $\Sigma_i(\vec{b}) - \Sigma_i(\vec{a}) \in [0, p^f - 1)$, then $\Sigma_i(\vec{c}) = \Sigma_i(\vec{b}) - \Sigma_i(\vec{a}) \equiv 0 \mod p$, so $c_i = 0$, giving a contradiction. If $\Sigma_i(\vec{b}) - \Sigma_i(\vec{a}) \in [1 - p^f, 0)$, then $\Sigma_i(\vec{c}) = p^f - 1 + \Sigma_i(\vec{b}) - \Sigma_i(\vec{a}) \equiv p - 1 \mod p$, so $c_i = p-1$, giving a contradiction. If $\Sigma_i(\vec{b}) - \Sigma_i(\vec{a}) \geqslant p^f - 1$, then $0 \leqslant \Sigma_i(\vec{b}) - \Sigma_i(\vec{a}) - (p^f - 1) \leqslant 1 + \cdots + p^{f-1}$, giving $\Sigma_i(\vec{c}) = 1 + \cdots + p^{f-1}$, so that $\vec{c} = \vec{1}$, $J = \emptyset$ and $\vec{b} = \vec{p}$. If $\Sigma_i(\vec{b}) - \Sigma_i(\vec{a}) \leqslant 1 - p^f$, then similar considerations give a contradiction. The proof in the case $a_i = p$ is similar (in fact, one can exchange $\vec{c}$ with $\overrightarrow{p-1} - \vec{c}$, J with its complement and $\vec{a}$ with $\vec{b}$), giving $\vec{c} = \overrightarrow{p-2}$, $J = S$ and $\vec{a} = \vec{p}$. □

Suppose that $V_1 = F(\chi_1)$ and $V_2 = F(\chi_2)$, where χ_1 and χ_2 are crystalline characters of G_K with labeled Hodge–Tate weights $(b_{f-1}, b_0, \ldots, b_{f-2})$ and $(a_{f-1}, a_0, \ldots, a_{f-2})$ respectively, V is an extension

$$0 \to V_1 \to V \to V_2 \to 0$$

of representations of G_K over F, and T is a G_K-stable $\mathcal{O}_F$-lattice in V. Letting $T_1 = T \cap V_1$ and $T_2 = T/T_1$, we have

$$0 \to T_1 \to T \to T_2 \to 0.$$

Lemma 7.6. *Suppose that $\vec{c} \in \mathbf{Z}^S$ is generic and $\vec{a}, \vec{b} \in \mathbf{Z}^S$ are as above. If V is crystalline, then*

$$0 \to \mathbf{N}(T_1) \to \mathbf{N}(T) \to \mathbf{N}(T_2) \to 0$$

is exact.

Proof. Since V is crystalline, there is a Wach module $N = \mathbf{N}(T)$ over $\mathbf{A}^+_{K,F}$ corresponding to T. Since $\vec{c}$ is generic, we have $\max(a_i, b_i) \leqslant p-1$ for all i, unless $\{\vec{a}, \vec{b}\} = \{\vec{0}, \vec{p}\}$. If $\max(a_i, b_i) \leqslant p - 1$ for all i, then by Proposition 7.4(i) and (iii), we have:

- $0 \leqslant a'_i \leqslant \max(a_i, b_i) \leqslant p-1$ for all i; and
- $\sum_{i=0}^{f-1} a'_i p^i \equiv \sum_{i=0}^{f-1} a_i p^i \bmod (p^f - 1)$.

These conditions imply that $\vec{a} = \vec{a}'$ (unless $\{\vec{a}, \vec{a}'\} = \{\vec{0}, \overrightarrow{p-1}\}$, which would give $\{\vec{a}, \vec{b}\} = \{\vec{0}, \overrightarrow{p-1}\}$ and hence that $\vec{c} = \vec{0}$ is not generic). If $\{\vec{a}, \vec{b}\} = \{\vec{0}, \vec{p}\}$, then we instead use parts (ii) and (iii) of Proposition 7.4 to conclude that $\vec{a} = \vec{a}'$. Thus in either case, we conclude from part (iv) of the proposition that $\mathbf{N}(T) \to \mathbf{N}(T_2)$ is surjective, and therefore the sequence of Wach modules is exact. □

Now consider a character $\psi : G_K \to \mathbf{F}^\times$. By the classification of rank one (φ, Γ)-modules over $\mathbf{E}_{K,F}$, there is a unique pair $C \in \mathbf{F}^\times$, $\vec{c} \in \mathbf{Z}^S$ with $0 \leqslant c_i \leqslant p-1$ and some $c_i < p-1$, such that $\mathbf{D}(\mathbf{F}(\psi)) \cong M_{C\vec{c}}$. Suppose that $J \subset S$ and $\vec{a}, \vec{b} \in \mathbf{Z}^S$ satisfying the usual conditions, and that $A, B \in \mathbf{F}^\times$ with $BA^{-1} = C$. Recall then that we have defined a subspace $\mathrm{Ext}^1_{\mathrm{bdd}}(M_{A\vec{a}}, M_{B\vec{b}})$

of $\mathrm{Ext}^1(M_{A\vec{a}}, M_{B\vec{b}})$ and an isomorphism

$$\iota : \mathrm{Ext}^1(M_{\vec{0}}, M_{C\vec{c}}) \to \mathrm{Ext}^1(M_{A\vec{a}}, M_{B\vec{b}}),$$

well-defined up to an element of $\mathbf{F}^\times$. We then define V_J as the preimage of $\mathrm{Ext}^1_{\mathrm{bdd}}(M_{A\vec{a}}, M_{B\vec{b}})$. This space is independent of the choices of A and B such that $BA^{-1} = C$, but for certain J there are two choices for the pair $\vec{a}, \vec{b}$; we denote by V_J^+ the space obtained by taking $a_i = p$ for all $i \in J$ and $b_i = 1$ for all $i \notin J$, and by V_J^- the one obtained by taking $a_i = 1$ for all $i \in J$ and $b_i = p$ for all $i \notin J$.

We now also recall the definition of the subspaces of $H^1(G_K, \mathbf{F}(\psi))$ used in [BDJ10], but we modify the notation from there to be more consistent with this paper. (For the translation between the notations, see the remark below.) For ψ, J, $\vec{a}$, $\vec{b}$ as above, we consider a crystalline lift $\tilde{\psi}_J : G_K \to F^\times$ of ψ with labeled Hodge–Tate weights $(h_{f-1}, h_0, \dots, h_{f-2})$, where $h_i = -a_i$ if $i \in J$ and $h_i = b_i$ if $i \notin J$. Such a character $\tilde{\psi}_J$ is uniquely determined up to an unramified twist, which we specify by requiring that $\tilde{\psi}_J(g)$ be the Teichmüller lift of $\psi(g)$ for $g \in G_K$ corresponding via local class field theory to the uniformizer $p \in K^\times$. When $(\vec{a}, \vec{b})$ is not uniquely determined by J, we adopt the notation $\tilde{\psi}_J^\pm$ as usual. Recall that $H^1_f(G_K, F(\tilde{\psi}_J))$ denotes the space of cohomology classes corresponding to crystalline extensions

$$0 \to F(\tilde{\psi}_J) \to V \to F \to 0.$$

We then define the space L'_J as the image in $H^1(G_K, \mathbf{F}(\psi))$ of the preimage in $H^1(G_K, \mathcal{O}_F(\tilde{\psi}_J))$ of $H^1_f(G_K, F(\tilde{\psi}_J))$. We set $L_J = L'_J$ except in the following two cases.

- If ψ is cyclotomic, $J = S$ and $\vec{a} = \vec{p}$, we let $L_J = H^1(G_K, \mathbf{F}(\psi))$.
- If ψ is trivial and $J \neq S$, we let L_J be the span of L'_J and the unramified class.

As usual we disambiguate using the notation $L_J^\pm$. More precisely, we define $\tilde{\psi}_J^\pm$ as above, taking all $a_i = p$ and $b_j = 1$ for $\tilde{\psi}_J^+$, and all $a_i = 1$ and $b_j = p$ for $\tilde{\psi}_J^-$. We then define $(L'_J)^\pm$ as the image in $H^1(G_K, \mathbf{F}(\psi))$ of the preimage in $H^1(G_K, \mathcal{O}_F(\tilde{\psi}_J^\pm))$ of $H^1_f(G_K, F(\tilde{\psi}_J)^\pm)$. We then make the same modifications as above in the same exceptional cases to obtain the space $L_J^\pm$. In particular, the first exceptional case above actually only applies to L_J^+. We identify L_J (or $L_J^\pm$) with subspaces of $\mathrm{Ext}^1(M_{\vec{0}}, M_{C\vec{c}})$ via the isomorphisms

$$H^1(G_K, \mathbf{F}(\psi)) \cong \mathrm{Ext}^1_{\mathbf{F}[G_K]}(\mathbf{F}, \mathbf{F}(\psi)) \cong \mathrm{Ext}^1(\mathbf{D}(\mathbf{F}), \mathbf{D}(\mathbf{F}(\psi))) \cong \mathrm{Ext}^1(M_{\vec{0}}, M_{C\vec{c}}),$$

the last of these given by an isomorphism $\mathbf{D}(\mathbf{F}(\psi)) \cong M_{C\vec{c}}$ that is unique up to an element of $\mathbf{F}^\times$.

Remark 7.7. The article [BDJ10] (after Lemma 3.9) defines spaces $L_\alpha \subset H^1(G_K, \overline{\mathbf{F}}_p(\psi))$ for certain pairs (V, J) where $J \subset S$ and V is an irreducible representation of $\mathrm{GL}_2(k)$. The relation between the spaces is that $L_{(V,J')} = L_J \otimes_{\mathbf{F}} \overline{\mathbf{F}}_p$, where $J = \{i \mid i-1 \in J'\}$ and if $V \cong \bigotimes_{i \in S}(\det^{m_i} \otimes_k \mathrm{Sym}^{n_i - 1} k^2 \otimes_{k,\tau_i} \overline{\mathbf{F}}_p)$, then we take $a_i = n_{i-1}$ if $i \in J$ and $b_i = n_{i-1}$ if $i \notin J$. (The space $L_{(V,J')}$ is in fact independent of $\vec{m}$, and when there are two choices of $\vec{n}$ compatible with ψ and J', the resulting spaces $L_{(V,J')}$ are obtained from $L_J^\pm$ in the evident way.)

We now prove our main result in the generic case.

Theorem 7.8. *Suppose that $\vec{c}$ is generic.*

(i) *Suppose that $J \neq S$ (respectively $J \neq \emptyset$) if $\vec{c} = \overrightarrow{p-2}$ (respectively $\vec{c} = \vec{1}$). Then $V_J = L_J$, so $L_J = \bigoplus_{i \in J} L_{\{i\}}$.*

https://doi.org/10.1112/S0010437X1000504X Published online by Cambridge University Press

(ii) *If* $\vec{c} = \overrightarrow{p-2}$ *and* $J = S$, *then* $V_J^{\pm} = L_J^{\pm}$, *so* $L_J^- = \bigoplus_{i \in J} L_{\{i\}}$ *if* $f > 1$.

(iii) *If* $\vec{c} = \vec{1}$ *and* $J = \emptyset$, *then* $V_J^{\pm} = L_J^{\pm} = \{0\}$.

Proof. We first prove part (i). Suppose that $x \in L_J$, so x is a class of extensions

$$0 \to M_{C\vec{c}} \to E \to M_{\vec{0}} \to 0$$

corresponding via $\mathbf{D}$ to a class of extensions of Galois representations

$$0 \to \mathbf{F}(\psi) \to \overline{T} \to \mathbf{F} \to 0.$$

The assumption that $x \in L_J$ means that there is an extension

$$0 \to \mathcal{O}_F(\tilde{\psi}_J) \to T \to \mathcal{O}_F \to 0$$

whose reduction mod ϖ_F is $\overline{T}$ and such that $F \otimes_{\mathcal{O}_F} T$ is crystalline. Let $\psi_2 : G_K \to F^\times$ be a crystalline character with labeled Hodge–Tate weights $(a_{f-1}, a_0, \ldots, a_{f-2})$ and let $\psi_1 = \tilde{\psi}_J \psi_2$. (Recall that $a_i = 0$ if $i \notin J$ and $b_i = 0$ if $i \in J$.) Then ψ_1 is crystalline with Hodge–Tate weights $(b_{f-1}, b_0, \ldots, b_{f-2})$ and we have an exact sequence

$$0 \to T_1 \to T(\psi_2) \to T_2 \to 0,$$

where $T_i = \mathcal{O}_F(\psi_i)$ and $F \otimes_{\mathcal{O}_F} T(\psi_2)$ is crystalline. By Lemma 7.6, the corresponding sequence of Wach modules over $\mathbf{A}_{K,F}^+$,

$$0 \to \mathbf{N}(T_1) \to N \to \mathbf{N}(T_2) \to 0,$$

is exact. Reducing mod ϖ_F, we obtain an exact sequence of free $\mathbf{E}_{K,F}^+$-modules with commuting φ and Γ actions such that Γ acts trivially mod π. Tensoring with $\mathbf{E}_{K,F}$ yields an exact sequence

$$0 \to M_{B\vec{b}} \to E' \to M_{A\vec{a}} \to 0$$

of (φ, Γ)-modules, bounded with respect to a basis for $\overline{N}$. It follows that E' defines an element of $\mathrm{Ext}^1_{\mathrm{bdd}}(M_{A\vec{a}}, M_{B\vec{b}})$. Moreover, this exact sequence is obtained from the one defining x by twisting with $M_{A\vec{a}}$, so we have shown that $\iota(x)$ is bounded, and hence that $x \in V_J$. Thus $L_J \subset V_J$.

By Proposition 5.4 of this paper and Lemma 3.10 of [BDJ10], we have that $\dim_{\mathbf{F}} V_J = |J| = \dim_{\mathbf{F}} L_J = |J|$; therefore $L_J = V_J$. The assertion that $L_J = \bigoplus_{i \in J} L_{\{i\}}$ then also follows from Proposition 5.4.

The proofs of parts (ii) and (iii) are exactly the same as that for part (i), except that for part (ii) in the cyclotomic case one uses Proposition 6.5. ◻

Remark 7.9. We see from the proof of the theorem that, in the definition of L_J, $\tilde{\psi}_J$ can be replaced by its twist by any unramified character $G_K \to \mathcal{O}_F^\times$ with trivial reduction mod ϖ_F. This can also be proved using Fontaine–Laffaille theory.

However, in the case where ψ is cyclotomic, $J = S$ and $\vec{a} = \vec{p}$, we defined L_J as $H^1(G_K, \mathbf{F}(\psi))$ rather than L'_J. In fact L'_J has codimension one and depends on the unramified twist, as the next proof shows.

As a further application, we show that, in the generic case, bounded extensions 'lift' to extensions of Wach modules.

Corollary 7.10. *Suppose that* $\vec{c} \in \mathbf{Z}^S$ *is generic and* $\vec{a}, \vec{b} \in \mathbf{Z}^S$ *are as above and that*

$$0 \to M_{B\vec{b}} \to E \to M_{A\vec{a}} \to 0$$

https://doi.org/10.1112/S0010437X1000504X Published online by Cambridge University Press

is a bounded extension of (φ, Γ)-modules over $\mathbf{E}_{K,F}$. In the case $A = B$, $\vec{c} = \overrightarrow{p-2}$ and $\vec{a} = \vec{p}$, assume F is ramified. Then the extension E arises by applying $\mathbf{E}_{K,F} \otimes_{\mathbf{A}^+_{K,F}}$ to an exact sequence over $\mathbf{A}^+_{K,F}$ of Wach modules of the form

$$0 \to \mathbf{N}(\psi_1) \to N \to \mathbf{N}(\psi_2) \to 0,$$

where ψ_1 (respectively ψ_2) is a crystalline character with labeled Hodge–Tate weights $(b_{f-1}, b_0, \ldots, b_{f-2})$ (respectively $(a_{f-1}, a_0, \ldots, a_{f-2})$).

Proof. First assume we are not in the exceptional case where $A = B$, $\vec{c} = \overrightarrow{p-2}$ and $\vec{a} = \vec{p}$. Since the extension class defined by E is bounded, the equality $V_J = L_J$ of the preceding theorem shows that E arises by applying $\mathbf{D}$ to the reduction mod ϖ_F of a crystalline extension

$$0 \to \mathcal{O}_F(\psi_1) \to T \to \mathcal{O}_F(\psi_2) \to 0,$$

where ψ_1 and ψ_2 have the required Hodge–Tate weights. Lemma 7.6 then gives the desired extension of Wach modules over $\mathbf{A}^+_{K,F}$.

Suppose now that $A = B$, $\vec{c} = \overrightarrow{p-2}$ and $\vec{a} = \vec{p}$. Consider the class $x := \iota(E) \in \mathrm{Ext}^1(M_{\vec{0}}, M_{\overrightarrow{p-2}}) \cong H^1(G_K, \mathbf{F}(\chi))$, where χ denotes the cyclotomic character. We claim that there is an unramified character $\mu : G_K \to \mathcal{O}_F^\times$ with trivial reduction mod ϖ_F so that x is in the image of $H^1(G_K, \mathcal{O}_F(\chi^p\mu))$. (This is essentially proved in [KW09a, Proposition 3.5] or [KW09b, § 3.2.7], but there it is assumed that x is *très ramifié*, so we recall the argument here.) The long exact sequence associated to

$$0 \to \mathcal{O}_F(\chi^p\mu) \xrightarrow{\varpi_F} \mathcal{O}_F(\chi^p\mu) \to \mathbf{F}(\chi) \to 0$$

shows that the image of $H^1(G_K, \mathcal{O}_F(\chi^p\mu))$ is the kernel of the connecting homomorphism

$$H^1(G_K, \mathbf{F}(\chi)) \to H^2(G_K, \mathcal{O}_F(\chi^p\mu)).$$

By Tate duality, this is the space orthogonal to the image of the connecting homomorphism

$$H^0(G_K, (F/\mathcal{O}_F)(\chi^{1-p}\mu^{-1})) \to H^1(G_K, \mathbf{F})$$

arising from the dual short exact sequence. Letting α denote the homomorphism $G_K \to \mathbf{F}$ defined by $(\chi^{1-p} - 1)/p$, and β the unramified homomorphism sending Frob_K to 1, we find that the image of the connecting homomorphism is spanned by β if $\mu \not\equiv 1 \bmod p\mathcal{O}_F$ (which is possible as F is ramified over $\mathbf{Q}_p$) and by $\alpha + \lambda\beta$ if $\mu(\mathrm{Frob}_K) \equiv 1 + p\lambda \bmod p\varpi_F\mathcal{O}_F$. If $x \cup \beta = 0$ then we can take $\mu \not\equiv 1 \bmod p\mathcal{O}_F$, and if $x \cup \beta \neq 0$ then there is a unique λ so that $\lambda(x \cup \beta) = -x \cup \alpha$ and we choose μ accordingly. Now since $H^1(G_K, F(\chi^p\mu)) = H^1_f(G_K, F(\chi^p\mu))$, we see that E arises from the reduction of a crystalline extension of the required form, and the result again follows from Lemma 7.6. □

7.4 Case $f = 2$

In this subsection we will show that, if $f = 2$, then $L_J = V_J$ (or $L_J^\pm = V_J^\pm$) unless $\vec{c} = \vec{0}$; in other words, the space of bounded extensions coincides with the one obtained from reductions of crystalline extensions of the corresponding weights unless the ratio of the characters is unramified. Furthermore, we give a complete description in this exceptional case.

Before treating the case $f = 1$, we note what happens in the case $f = 1$. The case $\vec{c} \neq \vec{0}$ is already treated by the results of the preceding section. Assume for the moment that $p > 2$. Then the proof goes through just the same if $\vec{c} = \vec{0}$ and $J = S = \{0\}$. Suppose then that $\vec{c} = \vec{0}$ and $J = \emptyset$.

https://doi.org/10.1112/S0010437X1000504X Published online by Cambridge University Press

If $C \neq 1$, then $V_\emptyset = L_\emptyset = \{0\}$, so there is nothing to prove. If $C = 1$, then we have $V_\emptyset = \{0\}$, but $L_\emptyset = H^1(G_{\mathbf{Q}_p}, \mathbf{F})$. Indeed, all such classes arise as reductions of lattices in representations of the form $\mathbf{Q}_p \oplus \mathbf{Q}_p(\chi^{1-p}\mu)$ with μ unramified; the corresponding Wach module is described just as in Example 7.1 and so does not give rise to a bounded extension. If $p = 2$, there are differences in the case $C = 1$ (see Remark 6.14). In that case

$$V_S^+ = V_S^- = L_S^+ = H^1(G_{\mathbf{Q}_2}, \mathbf{F}) = \langle B_{\mathrm{nr}}, B_{\mathrm{cyc}}, B_{\mathrm{tr}}\rangle$$

and $V_\emptyset^+ = V_\emptyset^- = \{0\}$, but $L_S^- = L_\emptyset^- = \langle B_{\mathrm{nr}}, B_{\mathrm{cyc}}\rangle$ and $L_\emptyset^+ = \langle B_{\mathrm{nr}}, B_{\mathrm{tr}}\rangle$. (For the explicit descriptions, note that the extensions of Galois representations are unramified twists of ones on which H_K acts trivially, and if H_K acts trivially on T, then $\mathbf{D}(T) = \mathbf{E}_K \otimes T$.)

We now turn our attention to $f = 2$. We maintain the notation of the preceding section, without the assumption that $\vec{c}$ is generic. In particular, $J \subset S$ and $\vec{a}, \vec{b}$ satisfy the usual conditions, V_1 and V_2 are one-dimensional crystalline representations with labeled Hodge–Tate weights (b_1, b_0) and (a_1, a_0), V is an extension of V_2 by V_1, T is a G_K-stable $\mathcal{O}_F$-lattice in V, $T_1 = T \cap V_1$ and $T_2 = T/T_1$. The refinement of Lemma 7.6 is the following lemma.

Lemma 7.11. *Suppose that $f = 2$ and $\vec{c} \neq \vec{0}$. If V is crystalline, then*

$$0 \to \mathbf{N}(T_1) \to \mathbf{N}(T) \to \mathbf{N}(T_2) \to 0$$

is exact.

Proof. Since the generic case is covered by Lemma 7.6, we can assume (interchanging embeddings if necessary) that $\vec{c} = (i, 0)$ for some $i \in \{1, \dots, p-2\}$ or that $\vec{c} = (i, p-1)$ for some $i \in \{0, \dots, p-2\}$. The cases where $J = \emptyset$ or $J = S$ are covered by the same argument (using parts (ii), (iii) and (iv) of Proposition 7.4), as are the cases where $\vec{c} = (i, 0)$ or $J = \{1\}$ (using parts (i), (iii) and (iv) of the proposition). We are thus left with the case where $\vec{c} = (i, p-1)$ for some $i \in \{0, \dots, p-2\}$ and $J = \{0\}$, in which case $\vec{a} = (p-i, 0)$ and $\vec{b} = (0, p)$. In the notation of Proposition 7.4, the possible values of $\vec{b}'$ are $(0, p)$ and $(1, 0)$. To complete the proof, we must rule out the latter possibility, which we accomplish by considering the reduction of $\mathbf{N}(T)$ modulo p^2. From the exact sequence

$$0 \to \mathbf{D}(T_1) \to \mathbf{D}(T) \to \mathbf{D}(T_2) \to 0$$

and the description in [Dou08] of rank one (φ, Γ)-modules recalled in § 3, we see that there is a basis $\{e_1, e_2\}$ for $\mathbf{D}(T)$ over $\mathbf{A}_{K,F}$ in terms of which the matrices describing the actions of φ and $\gamma \in \Gamma$ are

$$P = \begin{pmatrix} (\tilde{B}, q^p) & * \\ 0 & (\tilde{A}q^{p-i}, 1) \end{pmatrix} \quad \text{and} \quad G_\gamma = \begin{pmatrix} (\varphi(\Lambda_\gamma^p), \Lambda_\gamma^p) & * \\ 0 & (\Lambda_\gamma^{p-i}, \varphi(\Lambda_\gamma)^{p-i}) \end{pmatrix}$$

for some $\tilde{A}, \tilde{B} \in \mathcal{O}_F^\times$. On the other hand, since V is crystalline, there is a basis $\{e_1', e_2'\}$ for $\mathbf{D}(T)$ over $\mathbf{A}_{K,F}$ in terms of which the matrices P' and G_γ' describing these actions lie in $\mathrm{GL}_2(\mathbf{A}_{K,F}^+)$, with $G_\gamma' \equiv I \bmod \pi \mathrm{M}_2(A_{K,F}^+)$. If we assume further that $\vec{b}' = (1, 0)$ (and so $\vec{a}' = (p-i-1, p)$), then we can choose e_1', e_2' such that

$$\overline{P}' \equiv \begin{pmatrix} (B\pi^{p-1}, 1) & * \\ 0 & (A\pi^{(p-i-1)(p-1)}, \pi^{p(p-1)}) \end{pmatrix} \quad \text{and} \quad \overline{G}_\gamma' = \begin{pmatrix} (\lambda_\gamma, \lambda_\gamma^p) & * \\ 0 & (\lambda_\gamma^{p^2+p-i-1}, \lambda_\gamma^{p^2-ip}) \end{pmatrix},$$

https://doi.org/10.1112/S0010437X1000504X Published online by Cambridge University Press

where $\bar{\cdot}$ denotes reduction modulo ϖ_F. Since $\mathbf{D}(T) \cong \mathbf{A}_{K,F} \otimes_{\mathbf{A}^+_{K,F}} \mathbf{N}(T)$, we can write $(e'_1, e'_2) = (e_1, e_2)Q$ for some $Q \in \mathrm{GL}_2(A_{K,F})$, and then we have

$$P' = Q^{-1}P\varphi(T) \quad \text{and} \quad G'_\gamma = Q^{-1}G_\gamma\gamma(Q) \quad \text{for all } \gamma \in \Gamma.$$

CLAIM. We have $Q \equiv RS \bmod p\mathbf{A}_{K,F}$ for some matrices $R = \begin{pmatrix} \alpha(q^{-1},1) & * \\ 0 & \beta(q,1) \end{pmatrix} \in \mathrm{GL}_2(\mathbf{A}_{K,F})$ with $\alpha, \beta \in \mathcal{O}_F^\times$ and $S \in I + \varpi_F \mathrm{M}_2(A^+_{K,F})$.

Since F may be ramified over $\mathbf{Q}_p$, we prove the claim by showing inductively that $Q \equiv R_m S_m \bmod \varpi_F^m \mathbf{A}_{K,F}$ for some matrices R_m, S_m of the prescribed form for $m = 1, \ldots, e$ where $e = e(F/\mathbf{Q}_p)$.

To prove the statement for $m = 1$, note that setting $R_0 = \begin{pmatrix} (q^{-1},1) & 0 \\ 0 & (q,1) \end{pmatrix}$ gives

$$\overline{R}_0^{-1}\overline{P}\varphi(\overline{R}_0) = \begin{pmatrix} (B\pi^{p-1}, 1) & * \\ 0 & (A\pi^{(p-i)(p-1)}, \pi^{p(p-1)}) \end{pmatrix}.$$

So if we write $R = R_0 S_0$, then

$$\overline{S}_0 \begin{pmatrix} (B\pi^{p-1}, 1) & * \\ 0 & (A\pi^{(p-i)(p-1)}, \pi^{p(p-1)}) \end{pmatrix} = \begin{pmatrix} (B\pi^{p-1}, 1) & * \\ 0 & (A\pi^{(p-i)(p-1)}, \pi^{p(p-1)}) \end{pmatrix} \varphi(\overline{S}_0).$$

It follows easily that $\overline{S}_0 = \left(\begin{smallmatrix} \bar{\alpha} & \bar{\delta} \\ 0 & \bar{\beta} \end{smallmatrix}\right)$ for some $\bar{\alpha}, \bar{\beta} \in \mathbf{F}^\times$, $\bar{\delta} \in \mathbf{E}_{K,F}$. Choosing lifts $\alpha, \beta \in \mathcal{O}_F^\times$ and $\delta \in \mathbf{A}_{K,F}$ and setting $R_1 = R_0\left(\begin{smallmatrix} \alpha & \delta \\ 0 & \beta \end{smallmatrix}\right)$ gives the result for $m = 1$.

Suppose now that $m \in \{1, \ldots, e-1\}$ and that $Q \equiv R_m S_m \bmod \varpi_F^m \mathbf{A}_{K,F}$ with R_m, S_m of the prescribed form. Setting $Q_m = R_m^{-1} Q S_m^{-1}$, we have $Q_m = I + \varpi_F^m Q'_m$ for some $Q'_m \in \mathrm{M}_2(\mathbf{A}_{K,F})$. Define

$$\begin{gathered} P_m = R_m^{-1}P\varphi(R_m), \quad G_{\gamma,m} = R_m^{-1}G_\gamma\gamma(R_m), \\ P'_m = S_m^{-1}P'\varphi(S_m) \quad \text{and} \quad G'_{\gamma,m} = S_m^{-1}G'_\gamma\gamma(S_m), \end{gathered}$$

so that

$$P'_m = Q_m^{-1}P_m\varphi(Q_m) \quad \text{and} \quad G'_{\gamma,m} = Q_m^{-1}G'_{\gamma,m}\gamma(Q_m).$$

Note that $P'_m \in \mathrm{M}_2(\mathbf{A}^+_{K,F})$, $G'_{\gamma,m} \in I + \pi\mathrm{M}_2(\mathbf{A}^+_{K,F})$, $P_m \equiv P'_m \bmod \varpi_F^m \mathrm{M}_2(\mathbf{A}_{K,F})$, $G_{\gamma,m} \equiv G'_{\gamma,m} \bmod \varpi_F^m \mathrm{M}_2(\mathbf{A}_{K,F})$,

$$P_m \equiv \begin{pmatrix} (\tilde{B}\pi^{p-1}, 1) & * \\ 0 & (\tilde{A}\pi^{(p-i-1)(p-1)}, \pi^{p(p-1)}) \end{pmatrix} \mod p\mathrm{M}_2(\mathbf{A}_{K,F})$$

and

$$G_{\gamma,m} \equiv \begin{pmatrix} (\lambda_\gamma, \lambda_\gamma^p) & * \\ 0 & (\lambda_\gamma^{p^2+p-i-1}, \lambda_\gamma^{p^2-ip}) \end{pmatrix} \mod p\mathrm{M}_2(\mathbf{A}_{K,F}).$$

Note that, since $m+1 \leqslant e$, the last two congruences hold mod ϖ_F^{m+1}, and that $Q_m^{-1} \equiv I - \varpi_F^m Q'_m \bmod \varpi_F^{m+1}\mathrm{M}_2(\mathbf{A}_{K,F})$. It follows that

$$\begin{aligned} P'_m &\equiv (I - \varpi_F^m Q'_m)P_m(I + \varpi_F^m \varphi(Q'_m)) \\ &\equiv P_m + \varpi_F^m(P_m\varphi(Q'_m) - Q'_m P_m) \bmod \varpi_F^{m+1}\mathrm{M}_2(\mathbf{A}_{K,F}), \end{aligned}$$

and therefore that

$$\varpi_F^m(P_m\varphi(Q'_m) - Q'_m P_m) \equiv P'_m - P_m \equiv \varpi_F^m \begin{pmatrix} x & y \\ z & w \end{pmatrix} \mod \varpi_F^{m+1}\mathrm{M}_2(\mathbf{A}_{K,F})$$

with $x, z, w \in \mathbf{A}^+_{K,F}$. Note that $\overline{P}_m = \overline{P}'$, so we have $\overline{P}'\varphi(\overline{Q}'_m) - \overline{Q}'_m\overline{P}' = \left(\begin{smallmatrix} \bar{x} & \bar{y} \\ \bar{z} & \bar{w} \end{smallmatrix}\right)$ for some $\bar{x}, \bar{z}, \bar{w} \in \mathbf{E}^+_{K,F}$, $\bar{y} \in \mathbf{E}_{K,F}$. Similarly we find that $\overline{G}'_\gamma\gamma(\overline{Q}'_m) - \overline{Q}'_m\overline{G}'_\gamma = \left(\begin{smallmatrix} \bar{x}_\gamma & \bar{y}_\gamma \\ \bar{z}_\gamma & \bar{w}_\gamma \end{smallmatrix}\right)$ for some $\bar{x}_\gamma, \bar{z}_\gamma, \bar{w}_\gamma \in \pi\mathbf{E}^+_{K,F}$, $\bar{y}_\gamma \in \mathbf{E}_{K,F}$.

Writing

$$\overline{Q}'_m = \begin{pmatrix} (r_0, r_1) & (s_0, s_1) \\ (t_0, t_1) & (u_0, u_1) \end{pmatrix}$$

with $r_0, r_1, \ldots, u_0, u_1 \in \mathbf{F}((\pi))$, the condition that $\bar{z} \in \mathbf{E}^+_{K,F}$ becomes $\pi^{p(p-1)}t_0(\pi)^p - t_1(\pi)$, $A\pi^{(p-i-1)(p-1)}t_1(\pi^p) - B\pi^{p-1}t_0(\pi) \in \mathbf{F}[[\pi]]$, from which one deduces that $\mathrm{val}_\pi(t_0) \geqslant 1-p$ and $\mathrm{val}_\pi(t_1) \geqslant 0$. The condition that $\bar{z}_\gamma \in \pi\mathbf{E}^+_{K,F}$ then becomes that $\gamma(t_0)\lambda_\gamma^{p^2+p-i-2} - t_0 \in \pi\mathbf{F}[[\pi]]$. Lemma 4.2 rules out the possibility that $1-p < \mathrm{val}_\pi(t_0) < 0$, and Lemma 4.4 rules out the possibility that $\mathrm{val}_\pi(t_0) = 1-p$. Therefore $(t_0, t_1) \in \mathbf{E}^+_{K,F}$. Since $\overline{P}' \in \mathrm{M}_2(\mathbf{E}^+_{K,F})$, the condition that $\bar{x} \in \mathbf{E}^+_{K,F}$ then becomes that $\pi^{p-1}(r_1(\pi^p) - r_0(\pi)), r_0(\pi^p) - r_1(\pi) \in \mathbf{F}[[\pi]]$, which implies that $(r_0, r_1) \in \mathbf{E}^+_{K,F}$. The condition that $\bar{w} \in \mathbf{E}^+_{K,F}$ becomes that $\pi^{(p-i-1)(p-1)}(u_1(\pi^p) - u_0(\pi)), \pi^{p(p-1)}u_0(\pi^p) - u_1(\pi) \in \mathbf{F}[[\pi]]$, which implies that $\mathrm{val}_\pi(u_0) \geqslant 1-p$ and $\mathrm{val}_\pi(u_1) \geqslant i+2-p$. Since $(t_0, t_1) \in \mathbf{E}^+_{K,F}$ and $\overline{G}'_\gamma \equiv I \bmod \pi\mathrm{M}_2(\mathbf{E}^+_{K,F})$, the condition that $\overline{w}_\gamma \in \pi\mathbf{E}^+_{K,F}$ becomes that $\gamma(u_i) - u_i \in \pi\mathbf{E}^+_{K,F}$ for $i = 0, 1$, so that Lemmas 4.2 and 4.4 again imply that $(u_0, u_1) \in \mathbf{E}^+_{K,F}$. We can thus lift $\overline{Q}'_m$ to a matrix $\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \in \mathrm{M}_2(\mathbf{A}_{K,F})$ with $r, t, u \in \mathbf{A}^+_{K,F}$. Setting $R_{m+1} = R_m \left(\begin{smallmatrix} 1 & \varpi_F^m s \\ 0 & 1 \end{smallmatrix}\right)$ and $S_{m+1} = \left(\begin{smallmatrix} 1+\varpi_F^m r & 0 \\ \varpi_F^m t & 1+\varpi_F^m u \end{smallmatrix}\right) S_m$ then gives $Q \equiv R_{m+1}S_{m+1} \bmod \varpi_F^{m+1}\mathrm{M}_2(\mathbf{A}_{K,F})$ with R_{m+1}, S_{m+1} of the prescribed form, and completes the proof of the claim.

To derive a contradiction from the claim, we proceed as in the proof of the induction step above, but with $m = e$ and working modulo ϖ_F^{m+1}. More precisely, we define Q_e, Q'_e, P_e, $G_{\gamma,e}$, P'_e and $G'_{\gamma,e}$ as above; the difference now is that the congruences satisfied by P_e and $G_{\gamma,e}$ modulo p are not satisfied modulo $p\varpi_F$. In particular, the upper left-hand entry of P_e is $(\tilde{A}q, q^p/\varphi(q))$, and a straightforward calculation shows that

$$\frac{q^p}{\varphi(q)} \equiv 1 + p(g(\pi^{-p}) - g(\pi^{-1}) + f(\pi)) \mod p^2\mathbf{A}_{\mathbf{Q}_p},$$

where $g(X) = \sum_{i=1}^{p-1}(-X)^i/i$ and $f(\pi) \in \mathbf{A}^+_{\mathbf{Q}_p}$. As before, we have $\overline{P}'\varphi(\overline{Q}'_e) - \overline{Q}'_e\overline{P}' = \left(\begin{smallmatrix} \bar{x} & \bar{y} \\ \bar{z} & \bar{w} \end{smallmatrix}\right)$ with $\bar{z} \in \mathbf{E}^+_{K,F}$ since P_e is upper-triangular, but now $\bar{x} \in (0, c(\bar{g}(\pi^{-p}) - \bar{g}(\pi^{-1}))) + \mathbf{E}^+_{K,F}$ for some $c \in \mathbf{F}^\times$ (the reduction of p/ϖ_F^e). Similarly we have $\overline{G}'_\gamma\gamma(\overline{Q}'_e) - \overline{Q}'_e\overline{G}'_\gamma = \left(\begin{smallmatrix} \bar{x}_\gamma & \bar{y}_\gamma \\ \bar{z}_\gamma & \bar{w}_\gamma \end{smallmatrix}\right)$ with $\bar{z}_\gamma \in \pi\mathbf{E}^+_{K,F}$. So just as before we get $(t_0, t_1) \in \mathbf{E}^+_{K,F}$, but this implies that $\pi^{p-1}(r_1(\pi^p) - r_0(\pi)) \in \mathbf{F}[[\pi]]$ and $r_0(\pi^p) - r_1(\pi) \in c(\bar{g}(\pi^{-p}) - \bar{g}(\pi^{-1})) + \mathbf{F}[[\pi]]$, which leads to a contradiction and completes the proof of the lemma. □

Theorem 7.12. *Suppose that $f = 2$ and $\vec{c} \neq \vec{0}$. Then $V_J = L_J$ (or $V_J^\pm = L_J^\pm$) for all $J \subset S$. In particular, $L_{\{0\}} = L_{\{1\}}$ if and only if $\vec{c} = (i, p-1)$ or $(p-1, i)$ for some $i \in \{1, \ldots, p-2\}$.*

Proof. The proof of the first assertion is exactly the same as for Theorem 7.8. The second then follows from the corresponding result for V_J in § 5.3. □

Theorem 1.2 of the introduction now follows in view of Corollary 3.3.

Remark 7.13. Again we see that, in the definition of L_J, $\tilde{\psi}_J$ can be replaced by its twist by any unramified character with trivial reduction; the cases where some a_i or b_i is p (with $J = \{0\}$ or $\{1\}$) are outside the range of Fontaine–Laffaille theory.

Note also that the case where we had to work the hardest in the proof of Lemma 7.11 is precisely the one where $L_{\{0\}} = L_{\{1\}}$.

By the same proof as Corollary 7.10, we obtain the following corollary.

Corollary 7.14. *Suppose that $f = 2$, that $\vec{c} \neq \vec{0}$ and $\vec{a}, \vec{b} \in \mathbf{Z}^S$ are as above and that*

$$0 \to M_{B\vec{b}} \to E \to M_{A\vec{a}} \to 0$$

is a bounded extension of (φ, Γ)-modules over $\mathbf{E}_{K,F}$. In the case $A = B$, $\vec{c} = \overrightarrow{p-2}$ and $\vec{a} = \vec{p}$, assume F is ramified. Then the extension E arises by applying $\mathbf{E}_{K,F} \otimes_{\mathbf{A}^+_{K,F}}$ to an exact sequence over $\mathbf{A}^+_{K,F}$ of Wach modules of the form

$$0 \to \mathbf{N}(\psi_1) \to N \to \mathbf{N}(\psi_2) \to 0,$$

where ψ_1 (respectively ψ_2) is a crystalline character with labeled Hodge–Tate weights (b_1, b_0) (respectively (a_1, a_0)).

We now say what we can in the case $\vec{c} = \vec{0}$. First note that the proof of Lemma 7.11 goes through in the following cases:

- $J = S$, in which case $\vec{a} = \overrightarrow{p-1}$ (or $\vec{2}$ if $p = 2$);
- $J = \{0\}$, $\vec{a} = (p, 0)$, $\vec{b} = (0, 1)$ (the + case);
- $J = \{1\}$, $\vec{a} = (0, p)$, $\vec{b} = (1, 0)$ (the + case).

The proof of Theorem 7.12 goes through in these cases unless $J = S$, $p = 2$, $\vec{a} = 1$, $C = 1$, where we get $L^-_S \subset V^-_S$, but $\dim L^-_S = 3 \neq \dim V^-_S = 4$ (see Remark 6.14). In this case, however, we know that L^-_S consists of the *peu ramifiée* extensions. To compute the corresponding (φ, Γ)-modules, note that $V^+_{\{0\}} = L^+_{\{0\}}$ contains the classes arising from reductions of Galois stable lattices in $F(\mu\psi^2) \oplus F(\psi^\sigma)$, where $\psi : G_K \to \mathcal{O}_F^\times$ is a crystalline character with labeled Hodge–Tate weights $(0, 1)$, σ is the non-trivial element of $\mathrm{Gal}(K/\mathbf{Q}_2)$, and $\mu : G_K \to \mathcal{O}_F^\times$ is an unramified character with trivial reduction $\bmod\, \varpi_F$. These classes correspond to homomorphisms $G_K \to \mathbf{F}$ whose restriction to inertia is a multiple of the reduction of $1/2(\psi^\sigma\psi^{-2} - 1)|_{I_K}$. One can compute these explicitly using class field theory and check that they are *peu ramifiée*. It follows that $L^+_{\{0\}} \subset L^-_S$, and similarly $L^+_{\{1\}} \subset L^-_S$, so that $L^-_S = \langle B_{\mathrm{nr}}, B_0, B_1 \rangle$.

If $J = \emptyset$, we have $V_\emptyset = \{0\}$, and $L_\emptyset = \{0\}$ unless $C = 1$. If $C = 1$, one can compute the extensions and associated (φ, Γ)-modules explicitly since they are unramified twists of representations on which H_K acts trivially. If $p \neq 2$, one gets $L_\emptyset = \langle B_{\mathrm{nr}}, B_{\mathrm{cyc}} \rangle$. If $p = 2$, one gets $L^+_\emptyset = \langle B_{\mathrm{nr}}, B_{\mathrm{cyc}} \rangle$ (with $\vec{b} = \vec{1}$) and $L^-_\emptyset = \langle B_{\mathrm{nr}}, B_{\mathrm{tr}} \rangle$ (with $\vec{b} = \vec{2}$).

The most interesting is the $-$ case when $S = \{0\}$ or $\{1\}$. For example, if $S = \{0\}$, $\vec{a} = (p, 0)$ and $\vec{b} = (0, 1)$, the proof of Lemma 7.11 breaks down, but we see that, if the associated sequence of Wach modules is not exact, then $\vec{a}' = (0, 1)$ and $\vec{b}' = (p, 0)$, so the extension of (φ, Γ)-modules associated to $\overline{T}$ is in $V^+_{\{1\}}$. Since $V^-_{\{0\}} \subset V^+_{\{1\}}$, it follows that $L^-_{\{0\}} \subset V^+_{\{1\}}$, and dimension counting implies equality. We therefore have that $V^-_{\{0\}}$ is contained in $L^-_{\{0\}} = V^+_{\{1\}} = L^+_{\{1\}}$ with codimension one. Similarly $V^-_{\{1\}}$ is contained in $L^-_{\{1\}} = V^+_{\{0\}} = L^+_{\{0\}}$ with codimension one.

Putting everything together we get the following theorem.

Theorem 7.15. *Suppose that $f = 2$, $\vec{c} = \vec{0}$.*

(i) *If $C \neq 1$, then:*

- *if $p > 2$ then $L_S = V_S = \mathrm{Ext}^1(M_{\vec{0}}, M_{C\vec{0}})$;*

https://doi.org/10.1112/S0010437X1000504X Published online by Cambridge University Press

– *if* $p=2$ *then* $L^{\pm}_S = V^{\pm}_S = \mathrm{Ext}^1(M_{\vec{0}}, M_{C\vec{0}})$;
– $V^{-}_{\{0\}} = V^{-}_{\{1\}} = \{0\}$ *and* $L^{-}_{\{0\}} = L^{+}_{\{1\}} = V^{+}_{\{1\}} \neq V^{+}_{\{0\}} = L^{+}_{\{0\}} = L^{-}_{\{1\}}$;
– *if* $p>2$ *then* $L_\emptyset = V_\emptyset = \{0\}$; *and*
– *if* $p=2$ *then* $L^{\pm}_\emptyset = V^{\pm}_\emptyset = \{0\}$.

(ii) *If* $C=1$, *then:*

– *if* $p>2$ *then* $L_S = V_S = \mathrm{Ext}^1(M_{\vec{0}}, M_{\vec{0}})$;
– *if* $p=2$ *then* $L^{+}_S = V^{\pm}_S = \mathrm{Ext}^1(M_{\vec{0}}, M_{\vec{0}})$ *and* $L^{-}_S = \langle B_{\mathrm{nr}}, B_0, B_1\rangle$;
– $V^{-}_{\{0\}} = V^{-}_{\{1\}} = \langle B_{\mathrm{nr}}\rangle$, $L^{-}_{\{0\}} = L^{+}_{\{1\}} = V^{+}_{\{1\}} = \langle B_{\mathrm{nr}}, B_1\rangle$ *and* $L^{-}_{\{1\}} = L^{+}_{\{0\}} = V^{+}_{\{0\}} = \langle B_{\mathrm{nr}}, B_0\rangle$;
– *if* $p>2$ *then* $V_\emptyset = \{0\}$ *and* $L_\emptyset = \langle B_{\mathrm{nr}}, B_{\mathrm{cyc}}\rangle$; *and*
– *if* $p=2$ *then* $V^{\pm}_\emptyset = \{0\}$, $L^{+}_\emptyset = \langle B_{\mathrm{nr}}, B_{\mathrm{cyc}}\rangle$ *and* $L^{-}_\emptyset = \langle B_{\mathrm{nr}}, B_{\mathrm{tr}}\rangle$.

Note that the strict inclusion $V^{-}_{\{0\}} \subset L^{-}_{\{0\}}$ implies the existence of *non-split* crystalline extensions $0 \to F(\psi_1) \to V \to F(\psi_2) \to 0$ with Galois stable $\mathcal{O}_F$-lattices T such that the corresponding sequence of Wach modules over $\mathbf{A}^{+}_{K,F}$ is not exact (with ψ_1 and ψ_2 of labeled Hodge–Tate weights $(p,0)$ and $(0,1)$ respectively).

As in Remark 7.13, we see that the definitions of L_J are independent of the choice of unramified twist, unless $C=1$, $J=\emptyset$ and F is ramified, in which case twisting by an unramified character that is trivial $\mathrm{mod}\,\varpi_F$ but not $\mathrm{mod}\,p$ would give $L'_J = L_J = \langle B_{\mathrm{nr}}\rangle$.

Finally we remark that the proof of Corollary 7.14 goes through when $\vec{c} = \vec{0}$ except in the following two cases where $C=1$.

– If $p=2$ and $\vec{a} = \vec{1}$, then only classes in L^{-}_S lift (see Remark 6.14).
– If $\vec{a} = (1,0)$ and $\vec{b} = (0,p)$ (or $\vec{a} = (0,1)$ and $\vec{b} = (p,0)$), then we have not determined whether B_{nr} lifts.

Acknowledgements

This paper grew out of the first author's Brandeis Ph.D. thesis [Cha06] written under the supervision of the second author. The thesis already contains most of the key technical results in §§ 4 and 5. The authors are grateful to Laurent Berger for helpful conversations and correspondence, and to the referee for useful comments suggesting corrections and improvements to the exposition. The first author expresses his sincere gratitude to the second author for suggesting the project and for the guidance and encouragement during doctoral study. He would like to thank POSTECH, in particular Professor YoungJu Choie, for the hospitality in the final stages of writing the paper. He was supported by RP-Grant 2009 of Ewha Womans University. The second author is grateful to the Isaac Newton Institute for its hospitality in the final stages of writing this paper. The research was supported by NSF grant 0300434.

References

Ber02 L. Berger, *Représentations p-adiques et équations différentielles*, Invent. Math. **148** (2002), 219–284.

Ber04a L. Berger, *An introduction to the theory of p-adic representations*, in *Geometric aspects of Dwork theory* (Walter de Gruyter, Berlin, 2004), 255–292.

Ber04b L. Berger, *Limites de représentations cristallines*, Compositio Math. **140** (2004), 1473–1498.

Bre09 C. Breuil, *Sur un problème de compatibilité local–global modulo p pour* GL_2. Preprint (2009), http://www.math.u-psud.fr/breuil/PUBLICATIONS/compamodp.pdf.

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.

Cha06 S. Chang, *Extensions of rank one (φ, Γ)-modules*, PhD thesis, Brandeis University (2006).

CC98 F. Cherbonnier and P. Colmez, *Représentations p-adiques surconvergentes*, Invent. Math. **133** (1998), 581–611.

Col99 P. Colmez, *Représentations cristallines et représentations de hauteur finie*, J. Reine Angew. Math. **514** (1999), 119–143.

CF00 P. Colmez and J.-M. Fontaine, *Constructions des représentations p-adiques semi-stables*, Invent. Math. **140** (2000), 1–43.

Dou08 G. Dousmanis, *On reductions of families of crystalline Galois representations*. Preprint (2008), arXiv:0805.1634.

Fon90 J.-M. Fontaine, *Représentations p-adiques des corps locaux I*, in *The Grothendieck Festschrift, vol. II* (Birkhäuser, Boston, 1990), 249–309.

Fon94a J.-M. Fontaine, *Le corps des périodes p-adiques*, in *Périodes p-adiques (Bures-sur-Yvette, 1988)*, Astérisque **223** (1994), 59–102.

Fon94b J.-M. Fontaine, *Représentations p-adiques semi-stables*, in *Périodes p-adiques (Bures-sur-Yvette, 1988)*, Astérisque **223** (1994), 113–184.

Her98 L. Herr, *Sur la cohomologie galoisienne des corps p-adiques*, Bull. Soc. Math. France **126** (1998), 563–600.

Her01 L. Herr, *Une approche nouvelle de la dualité locale de Tate*, Math. Ann. **320** (2001), 307–337.

KW09a C. Khare and J.-P. Wintenberger, *On Serre's conjecture for 2-dimensional mod p representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Ann. of Math. (2) **169** (2009), 229–253.

KW09b C. Khare and J.-P. Wintenberger, *Serre's modularity conjecture (II)*, Invent. Math. **178** (2009), 505–586.

Liu08 R. Liu, *Cohomology and duality for (φ, Γ)-modules over the Robba ring*, Int. Math. Res. Not. IMRN **3** (2008), 32pp, Art. ID rnm150.

Wac96 N. Wach, *Représentations p-adiques potentiellement cristallines*, Bull. Soc. Math. France **124** (1996), 375–400.

Wac97 N. Wach, *Représentations cristallines de torsion*, Compositio Math. **108** (1997), 185–240.

Seunghwan Chang schang@ewha.ac.kr
Institute of Mathematical Sciences, Ewha Womans University, Seoul 120-750, Republic of Korea

Fred Diamond Fred.Diamond@kcl.ac.uk
Department of Mathematics, King's College London, Strand, London WC2R 2LS, UK

https://doi.org/10.1112/S0010437X1000504X Published online by Cambridge University Press