Compatibility of arithmetic and algebraic local constants II. The tame abelian potentially Barsotti–Tate case.

Jan Nekovář

Dedicated to the memory of Ian Cassels

Abstract: We prove the compatibility of arithmetic local constants of Mazur and Rubin with the usual local constants for pairs of congruent self-dual Galois representations that become Barsotti–Tate over a tamely ramified abelian extension. This allows us to complete the proof of the p-parity conjecture ($p > 2$) for Selmer groups of Hilbert modular forms of parallel weight two and abelian varieties with real multiplication (in particular, elliptic curves) over totally real number fields.

Introduction

Let L be a finite extension of $\mathbf{Q}_\ell$, let $\mathcal{K}$ be a finite extension of $\mathbf{Q}_p$ (where $p > 2$) with ring of integers $\mathcal{O}$, and let V be a finite-dimensional vector space over $\mathcal{K}$ equipped with a continuous $\mathcal{K}$-linear action of $\Gamma_L = \mathrm{Gal}(\overline{L}/L)$. Assume that V is self-dual in the sense that there exists a Γ_L-equivariant nondegenerate skew-symmetric pairing $\langle\ ,\ \rangle : V \times V \longrightarrow \mathcal{K}(1) = \mathcal{K} \otimes_{\mathbf{Z}_p} \mathbf{Z}_p(1)$ and that V contains a Γ_L-stable $\mathcal{O}$-lattice $T \subset V$ for which $\langle\ ,\ \rangle$ induces an isomorphism $T \xrightarrow{\sim} T^*(1) := \mathrm{Hom}_{\mathcal{O}}(T, \mathcal{O}(1))$. The residual representation $\overline{T} := T/\pi T$ (where $\pi \in \mathcal{O}$ is a uniformiser) has coefficients in the finite field $\mathbf{F} := \mathcal{O}/\pi\mathcal{O}$ and the skew-symmetric pairing $\overline{\langle\ ,\ \rangle} : \overline{T} \times \overline{T} \longrightarrow \mathbf{F}(1)$ induced by $\langle\ ,\ \rangle$ is again nondegenerate.

The Bloch–Kato subspace $H^1_f(L, V) \subset H^1(L, V) = H^1(\Gamma_L, V)$ (equal to $H^1_{\mathrm{ur}}(L, V)$ if $\ell \neq p$) defines, by propagation, subspaces

$$H^1_f(L, T) := \mathrm{Ker}\left(H^1(L, T) \longrightarrow H^1(L, V)/H^1_f(L, V)\right) \subset H^1(L, T)$$

and

$$\mathscr{F} := \mathrm{Im}\left(H^1_f(L, T) \longrightarrow H^1(L, \overline{T})\right) \subset H^1(L, \overline{T}).$$

According to Tate local duality, the cup product attached to $\overline{\langle\ ,\ \rangle}$ induces a nondegenerate symmetric pairing

$$\cup : H^1(L, \overline{T}) \times H^1(L, \overline{T}) \longrightarrow H^2(L, \mathbf{F}(1)) \simeq \mathbf{F}$$

under which $\mathscr{F}$ is a Lagrangian (i.e., maximal isotropic) subspace of $H^1(L, \overline{T})$ if $\ell \neq p$. This is still the case if $\ell = p$, provided V is a de Rham representation of Γ_L, which we assume henceforth.

Assume that $V', T', \langle\ ,\ \rangle'$ is another triple as above which has the property that the pair $(\overline{T}' = T'/\pi T', \overline{\langle\ ,\ \rangle}')$ is isomorphic to $(\overline{T}, \overline{\langle\ ,\ \rangle})$. Fix such an isomorphism and use it to identify the quadratic spaces $(H^1(L, \overline{T}), \cup)$ and $(H^1(L, \overline{T}'), \cup)$.

The arithmetic local constant of Mazur and Rubin [MR, Def. 4.5], [N5, (2.2.1)] attached to the above data is defined as

$$\delta_L(T, T') = \delta_L(T', T) := \dim_{\mathbf{F}}(\mathscr{F}/\mathscr{F} \cap \mathscr{F}')\ \pmod 2 \in \mathbf{Z}/2\mathbf{Z}.$$

Denote by $WD(V)$ the representation of the Weil-Deligne group of L attached to V (resp. to $D_{\mathrm{pst}}(V)$, [Fo2], [FoPR, I.1.3.2]) if $\ell \neq p$ (resp. if $\ell = p$). Let ψ be a nontrivial additive character of L and dx_ψ the Haar measure on L that is self-dual with respect to ψ. The local constant $\varepsilon(V) := \varepsilon(WD(V), \psi, dx_\psi)$ does not depend on ψ and is equal to ± 1 [N2, Prop. 2.2.1].

Mazur and Rubin expect their arithmetic local constant $\delta_L(T, T')$ to be related to $\varepsilon(V)/\varepsilon(V')$. This was checked by explicit calculations in certain cases arising from abelian varieties [Ch]. It was subsequently proved [N6, Thm. 2.17] that

Keywords: local constants, Selmer groups, parity conjecture, Hilbert modular forms, elliptic curves.
MSC: 11G05, 11G40, 11S40

$$\delta_L(T,T') = \varepsilon(V)/\varepsilon(V')$$

holds in full generality if $\ell \neq p$. One expects this relation to be true even if $\ell = p$, provided the Hodge–Tate weights of V and V' are the same (including the multiplicities). This was verified in two very special cases in [N6, §3].

The main local result of the present article is the following.

Theorem A (= Theorem 5.5). *If $\ell = p \neq 2$ and if there exist abelian tamely ramified finite extensions K/L and K'/L and p-divisible groups (equipped with an $\mathcal{O}$-action) G over O_K (resp. G' over $O_{K'}$) such that $T|_{\Gamma_K} = T_\pi G$ and $T'|_{\Gamma_{K'}} = T_\pi G'$, then $\delta_L(T,T') = \varepsilon(V)/\varepsilon(V')$.*

If $K = K' = L$, then the representations V and V' are crystalline and $\varepsilon(V) = \varepsilon(V') = 1$. In this case $\dim_{\mathbf{F}}(\mathscr{F}/\mathscr{F} \cap \mathscr{F}') \equiv 0 \pmod{(p-1)[k : k \cap \mathbf{F}]}$, without assuming that T and T' are self-dual, by Theorem 2.16.

In general, one can assume that $K' = K$ and that the abelian extension K/L is totally tamely ramified (by Proposition 5.3). Theorem A is then a consequence of the fact that the subspace

$$\mathscr{F} = H^1_{fl}(O_K, G[\pi])^{\mathrm{Gal}(K/L)} \subset H^1(K, \overline{T})^{\mathrm{Gal}(K/L)} = H^1(L, \overline{T})$$

can be expressed explicitly in terms of the Breuil–Kisin module with descent data with respect to K/L attached to the finite flat $\mathbf{F}$-vector space scheme $G[\pi]$ over O_K, combined with some very simple linear algebra (and a slightly more involved symplectic algebra if $K \neq L$).

It is very likely that the method of proof will extend to the case when K/L is an arbitrary Galois extension of order prime to p, but our assumption that K/L is totally tamely ramified greatly simplifies the description of the descent data and is suficient for the global applications discussed below.

In the global case we need to slightly change the notation and assume that L is a number field, $p \neq 2$ and T, T' are representations (self-dual as before) of the group $\Gamma_{L,S} = \mathrm{Gal}(L_S/L)$, where L_S is the maximal extension of L unramified outside a fixed finite set S of primes of L which contains all primes dividing $p\infty$. We assume that V and V' are de Rham representations of Γ_{L_v}, for all primes $v \mid p$.

As above, we obtain, for all finite primes v of L, local epsilon constants $\varepsilon_v(V), \varepsilon_v(V') \in \{\pm 1\}$, Lagrangian subspaces $\mathscr{F}_v, \mathscr{F}'_v \subset H^1(L_v, \overline{T}) = H^1(\Gamma_{L_v}, \overline{T})$ and arithmetic local constants $\delta_v(T,T') = \delta_{L_v}(T,T') \in \mathbf{Z}/2\mathbf{Z}$.

The Selmer group attached to the Selmer structure $\mathscr{F} := (\mathscr{F}_v)$ is defined as

$$H^1_{\mathscr{F}}(L, \overline{T}) := \mathrm{Ker}(H^1(\Gamma_{L,S}, \overline{T}) \longrightarrow \bigoplus_{v \in S_f} H^1(L_v, \overline{T})/\mathscr{F}_v),$$

where S_f is the set of finite primes of L contained in S (and similarly for $\mathscr{F}' = (\mathscr{F}'_v)$). As explained in [N5, (2.2.1)], the formula of Mazur and Rubin [MR, Thm. 1.4]

$$\dim_{\mathbf{F}} H^1_{\mathscr{F}}(L, \overline{T}) - \dim_{\mathbf{F}} H^1_{\mathscr{F}'}(L, \overline{T}) \equiv \sum_{v \in S_f} \delta_v(T,T') \pmod 2$$

together with the existence of a cohomological version of the Cassels–Tate pairing constructed by Flach [Fl, Thm. 1] imply that

$$\chi_f(L,V) - \chi_f(L,V') \equiv \sum_{v \in S_f} \delta_v(T,T') \pmod 2,$$

where

$$\chi_f(L,V) := \dim_{\mathcal{K}} H^1_f(L,V) - \dim_{\mathcal{K}} H^0(L,V) = h^1_f(L,V) - h^0(L,V)$$

($h^0(L,V) = 0$ if the Galois representation V is pure – necessarily of weight -1 – at some finite prime of L).

The compatibilities $(-1)^{\delta_v(T,T')} = \varepsilon_v(V)/\varepsilon_v(V')$ proved for $v \nmid p$ in [N6, Thm. 2.17] and for $v \mid p$ in Theorem A imply the following result (the assumption of tame ramification is no longer necessary, since the statement is invariant under base change to an arbitrary abelian extension of odd degree).

Theorem B (= Theorem 6.7). *Assume that, in the global situation considered above, for every prime $v \mid p$ of L there exist finite abelian extensions $K(v)/L_v, K(v)'/L_v$ and p-divisible groups G (resp. G') (equipped with an $\mathcal{O}$-action) over $O_{K(v)}$ (resp. $O_{K(v)'}$) such that $T|_{\Gamma_{K(v)}} = T_\pi G$ and $T'|_{\Gamma_{K(v)'}} = T_\pi G'$. Then*

$$(-1)^{\chi_f(L,V)}/\varepsilon(V) = (-1)^{\chi_f(L,V')}/\varepsilon(V'),$$

where $\varepsilon(V) := \prod_v \varepsilon_v(V)$ and $\varepsilon(V') := \prod_v \varepsilon_v(V')$ (the product is taken over all primes of L and $\varepsilon_v(V) = \varepsilon_v(V') := (-1)^{\dim_{\mathcal{K}}(V)/2}$ for all $v \mid \infty$).

Let F be a totally real number field and f a cuspidal Hilbert modular newform over F of level $\mathfrak{n}$, parallel weight 2 and trivial character. The field K_f generated over $\mathbf{Q}$ by the Hecke eigenvalues $\lambda_f(v) = \lambda_f(T(v))$ of f is a totally real finite extension of $\mathbf{Q}$. For every prime number p and every prime $\mathfrak{p} \mid p$ in K_f one can attach to f an irreducible two-dimensional representation $V_\mathfrak{p}(f)$ of the Galois group $\Gamma_F = \mathrm{Gal}(\overline{F}/F)$ with coefficients in any fixed finite extension $\mathcal{K}$ of $(K_f)_\mathfrak{p}$, characterised by the fact that

$$\forall v \nmid p\mathfrak{n} \qquad \det(1 - X\,\mathrm{Fr}_{\mathrm{geom}}(v) \mid V_\mathfrak{p}(f)) = 1 - \lambda_f(v)X + (Nv)X^2.$$

The Tate twist $V := V_\mathfrak{p}(f)(1)$ admits a nondegenerate Γ_F-equivariant skew-symmetric pairing $V \times V \longrightarrow \mathcal{K}(1)$ and any Γ_F-stable $\mathcal{O}$-lattice $T \subset V$ ($\mathcal{O} = O_\mathcal{K}$) becomes self-dual $T \xrightarrow{\sim} T^*(1)$ if we multiply the pairing by a suitable scalar in $\mathcal{K}^*$.

Let $\pi(f)$ be the automorphic representation of $PGL_2(\mathbf{A}_F)$ attached to f. The conjectures of Bloch and Kato ([BK], [FoPR]) predict that $h^1_f(F, V_\mathfrak{p}(f)(1)) := \dim_\mathcal{K} H^1_f(F, V_\mathfrak{p}(f)(1))$ should be equal to

$$h^1_f(F, V_\mathfrak{p}(f)(1)) \stackrel{?}{=} \mathrm{ord}_{s=1} L(f,s) = \mathrm{ord}_{s=1/2}\, L(\pi(f), s).$$

The following result was proved in [N5, Thm. 1.4] if $2 \nmid [F : \mathbf{Q}]$ or if $\pi(f)_v$ is not a principal series representation for some finite prime v of F (and then generalised to almost all non CM cases and many CM cases in [N5, Thm. 3.5]). Thanks to Theorem B (and a separate argument in the case when the residual representation $\overline{T}$ is reducible) we obtain the following definitive result.

Theorem C (= Theorem 8.7). *If $p \neq 2$, then*

$$\dim_\mathcal{K} H^1_f(F, V_\mathfrak{p}(f)(1)) \equiv \mathrm{ord}_{s=1} L(f,s) \pmod 2$$

holds, for every cuspidal Hilbert modular newform f over F of parallel weight 2 and trivial character.

As explained in [N1, 12.11.6] and [N5, 4.2], potential modularity results of [BLGGT] and [W] imply, respectively, the following consequences of Theorem C (which were proved in [N5, Thm. 4.3, Thm. A] and [N6, Thm. 5.10] under additional hypotheses).

Theorem D (= Theorem 8.9). *Let A be an abelian variety with real multiplication by O_M (where M is a totally real number field of degree $[M : \mathbf{Q}] = \dim(A)$) defined over a totally real number field F. If $\mathfrak{p} \mid p$ in M and $p \neq 2$, then*

$$\dim_{M_\mathfrak{p}} H^1_f(F, V_\mathfrak{p}(A)) = \mathrm{rk}_{O_M} A(F) + \mathrm{cork}_{O_{M_\mathfrak{p}}} Ш(A/F)[\mathfrak{p}^\infty] \equiv \mathrm{ord}_{s=1} L(\iota A/F, s) \pmod 2$$

holds, for every $\iota : M \hookrightarrow \mathbf{R}$.

Theorem E (= Theorem 8.10). *Let E be an elliptic curve defined over a totally real number field F. If $p \neq 2$, then*

$$\dim_{\mathbf{Q}_p} H^1_f(F, V_p(E)) = \mathrm{rk}_\mathbf{Z} E(F) + \mathrm{cork}_{\mathbf{Z}_p} Ш(E/F)[p^\infty] \equiv \mathrm{ord}_{s=1} L(E/F, s) \pmod 2$$

(this is also known to be true for $p = 2$ in all non CM cases and in many CM cases, by [N5, Thm. A] and an earlier result of [DD2, Thm. 2.4]).

The proof of Theorem C goes as follows. Firstly, one can assume that $2 \mid [F : \mathbf{Q}]$ and that $\pi(f)_v$ is a principal series representation for all finite primes v of F. Secondly, after replacing F by a suitable abelian extension of p-power degree (which does not change the statement, since p is odd) one can assume that $\pi(f)_v$

becomes an unramified principal series representation after a base change to an abelian extension of F_v of degree prime to p, for all finite primes v of F. In particular, $\pi(f)_v$ is a tame principal series representation of $PGL_2(F_v)$, for all $v \mid p$. A refinement of Taylor's level raising [T1, Thm. 1] involving types [BDJ, Lemma 2.9 and its proof] produces another eigenform f' of parallel weight 2 and trivial character with the following properties:

- $\pi(f')_{v_0}$ is an unramified twist of the Steinberg representation for some $v_0 \nmid \mathfrak{n}p$;
- the level of f' divides $\mathfrak{n}v_0$;
- for all $v \mid p$, $\pi(f')_v$ is a tame principal series representation of $PGL_2(F_v)$;
- the residual representations $\overline{T}$ and $\overline{T}'$ of V and V', respectively, have isomorphic semisimplifications.

In particular, if $\overline{T}$ is (absolutely) irreducible, then $\overline{T} \simeq \overline{T}'$. Theorem B then applies and yields

$$\dim_{\mathcal{K}} H^1_f(F, V_{\mathfrak{p}}(f)(1)) - \mathrm{ord}_{s=1} L(f,s) \equiv \dim_{\mathcal{K}} H^1_f(F, V_{\mathfrak{p}}(f')(1)) - \mathrm{ord}_{s=1} L(f',s) \pmod 2,$$

but the right hand side is conguent to 0 (mod 2), by [N5, Thm. 1.4].

If $\overline{T}$ is reducible, one applies a different argument based on a combination of an Euler characteristic formula for Breuil–Kisin modules (equipped with tame descent data) with a generalisation of a formula of Cassels [C1, Thm. 1.1]. This yields the following abstract result (see [DD1, Thm. 2], [DD2, Thm. 5.7], [Č, Thm. 1.4] and [CFKS, Thm. 2.1] for analogous results for Selmer groups of elliptic curves and abelian varieties, respectively).

Theorem F (= Theorem 7.10). *If, in the global situation discussed before Theorem B (with $p \neq 2$), the following conditions are satisfied:*
(i) *$\overline{T}$ contains a Γ_L-stable Lagrangian subspace;*
(ii) *for each finite prime $v \nmid p$ of L there exist a finite abelian extension $L(v)/L_v$ and a finite Galois extension $K(v)/L(v)$ such that $p \nmid [K(v) : L(v)]$ and $T|_{\Gamma_{K(v)}}$ is unramified;*
(iii) *for each finite prime $v \mid p$ of L there exists a finite abelian extension $K(v)/L_v$ such that $T|_{\Gamma_{K(v)}} = T_\pi G$ for some p-divisible group G (equipped with an $\mathcal{O}$-action) over $O_{K(v)}$; then*

$$(-1)^{\chi_f(L,V)} = \varepsilon(V).$$

If $\dim_{\mathcal{K}}(V) = 2$, then the statement still holds if there exist finite primes v of L not satisfying (ii) or (iii), but for which $WD(V|_{\Gamma_{L_v}})$ has nontrivial monodromy.

This article is dedicated to the memory of Ian Cassels, who passed away in July 2015. His celebrated survey [C2] and the series of articles "Arithmetic of curves of genus 1, I–VIII" formed a very important part of the author's mathematical education. It is no coincidence that the Cassels–Tate pairing in its various incarnations features prominently in all proofs of parity results such as Theorems B, C, D, E and F above.

Acknowledgements. The author is grateful to James Newton for patiently answering questions about Breuil–Kisin modules with tame descent data and to the referee for a very careful reading of the article and a number of helpful comments.

Notation and conventions. The cardinality of a finite set X is denoted by $|X|$. We abbreviate $\otimes_{\mathbf{Z}}$ as $\otimes$.

1. Flat cohomology of finite flat group schemes

(1.1) Let $p \neq 2$ be a prime number, let K (the base field) be a finite extension of $\mathbf{Q}_p$, with ring of integers O_K and residue field k. Denote by $\Gamma_K := \mathrm{Gal}(\overline{K}/K)$ and $I_K := \mathrm{Gal}(\overline{K}/K^{ur})$, respectively, its absolute Galois group and inertia group, and by $\| \cdot \|_K : K^\times \longrightarrow |k|^{\mathbf{Z}}$ the normalised valuation ($\|\varpi\|_K = |k|^{-1}$, for any uniformiser $\varpi \in O_K$). Let $\mathcal{K}$ (the coefficient field) be another finite extension of $\mathbf{Q}_p$, with ring of integers $\mathcal{O} \subset \mathcal{K}$ and residue field $\mathbf{F} := \mathcal{O}/\pi\mathcal{O}$, where $\pi \in \mathcal{O}$ is a fixed uniformiser.

For an arbitrary finite extension L of $\mathbf{Q}_p$ we denote by $\mathrm{rec}_L : L^\times \longrightarrow \mathrm{Gal}(L^{ab}/L) = \Gamma_L^{ab}$ the reciprocity map, normalised by letting uniformisers correspond to geometric Frobenius elements. If ℓ is any prime number, let

$$\chi_{cycl,L,\ell} : \Gamma_L^{ab} \longrightarrow \mathrm{Aut}_{\mathbf{Z}_\ell}(\mu_{\ell^\infty}(\overline{L})) = \mathbf{Z}_\ell^\times$$

be the ℓ-adic cyclotomic character and $\overline{\chi}_{cycl,L,\ell} : \Gamma_L^{ab} \longrightarrow \mathrm{Aut}_{\mathbf{F}_\ell}(\mu_\ell(\overline{L})) = \mathbf{F}_\ell^\times$ its reduction modulo ℓ. Recall that $\chi_{cycl,L,\ell} = \chi_{cycl,\mathbf{Q}_p,\ell} \circ N_{L/\mathbf{Q}_p}$ and

$$\forall u \in \mathbf{Z}_p^\times \quad \forall n \in \mathbf{Z} \qquad \chi_{cycl,\mathbf{Q}_p,\ell}(\mathrm{rec}_{\mathbf{Q}_p}(p^n u)) = \begin{cases} u, & \ell = p, \\ p^{-n}, & \ell \neq p \end{cases} \tag{1.1.1}$$

([Se2, Thm. 2], with a sign change arising from our normalisation of the reciprocity map).

(1.2) Denote by $(p-\mathrm{Gr}/O_K)$ the exact category of finite flat abelian group schemes of p-power rank over $\mathrm{Spec}(O_K)$ and by $(\mathbf{F}-\mathrm{vs}/O_K)$ the $\mathbf{F}$-linear subcategory of finite flat $\mathbf{F}$-vector space schemes over $\mathrm{Spec}(O_K)$ (in particular, $(\mathbf{F}_p-\mathrm{vs}/O_K)$ consists of all objects of $(p-\mathrm{Gr}/O_K)$ killed by p). Similarly, let $(p-\mathrm{div}/O_K)$ be the $\mathbf{Z}_p$-linear exact category of p-divisible groups (Barsotti–Tate groups) over $\mathrm{Spec}(O_K)$ and $(\mathcal{O}-\mathrm{div}/O_K)$ the $\mathcal{O}$-linear subcategory of π-divisible $\mathcal{O}$-modules (i.e., p-divisible groups equipped with an $\mathcal{O}$-action). If G is an object of any of the above categories, we denote by G^D its Cartier dual.

(1.3) The generic fibre G_K of any $G \in (p-\mathrm{Gr}/O_K)$ can be identified with the finite Γ_K-module $G_K(\overline{K})$. The flat cohomology groups $H^i_{fl}(O_K, G)$ (for the fppf or the fpqf topologies) have the following properties ([M], [Mi, III.1]).

(1.3.1) The canonical map

$$H^i_{fl}(O_K, G) \longrightarrow H^i_{fl}(K, G_K) = H^i_{et}(K, G_K) = H^i(\Gamma_K, G_K(\overline{K})) = H^i(K, G_K(\overline{K})) = H^i(K, G_K)$$

is bijective (resp. injective) for $i = 0$ (resp. for $i = 1$).

(1.3.2) $H^i_{fl}(O_K, G) = 0$ for $i > 1$.

(1.3.3) An exact sequence $0 \longrightarrow G_1 \longrightarrow G_2 \longrightarrow G_3 \longrightarrow 0$ in $(p-\mathrm{Gr}/O_K)$ gives rise to an exact sequence of finite p-primary abelian groups

$$0 \longrightarrow H^0_{fl}(O_K, G_1) \longrightarrow H^0_{fl}(O_K, G_2) \longrightarrow H^0_{fl}(O_K, G_3) \longrightarrow H^1_{fl}(O_K, G_1) \longrightarrow$$
$$\longrightarrow H^1_{fl}(O_K, G_2) \longrightarrow H^1_{fl}(O_K, G_3) \longrightarrow 0.$$

(1.3.4) The orthogonal complement of $H^1_{fl}(O_K, G) \subset H^1(K, G_K)$ under the pairing

$$\cup : H^1(K, G_K) \times H^1(K, G_K^D) \longrightarrow H^2(\Gamma_K, \mathbf{G}_m(\overline{K})) \xrightarrow{\sim} \mathbf{Q}/\mathbf{Z}$$

is equal to $H^1_{fl}(O_K, G^D)$. In particular, if $G \xrightarrow{\sim} G^D$ is self-dual, then $H^1_{fl}(O_K, G)$ is a Lagrangian subspace of $H^1(K, G_K)$.

(1.3.5) The Euler characteristic formula [MRo, Prop. 8.1]:

$$|H^0_{fl}(O_K, G)|/|H^1_{fl}(O_K, G)| = \|\mathrm{disc}_{G/O_K}\|_K^{1/\mathrm{rk}(G)},$$

where $\mathrm{disc}_{G/O_K} \in (O_K - \{0\})/O_K^{\times 2}$ is the discriminant of the finite free (generically étale) O_K-algebra $\Gamma(G, O_G)$.

(1.4) If $G = (G[\pi^n])_{n\geq 1} \in (\mathcal{O}-\mathrm{div}/O_K)$, then $T := T_\pi G = \varprojlim_n G[\pi^n](\overline{K}) = \varprojlim_n T/\pi^n T$ is a Γ_K-stable $\mathcal{O}$-lattice in $V := V_\pi G = T \otimes_{\mathcal{O}} \mathcal{K}$, which is a crystalline representation of Γ_K with coefficients in $\mathcal{K}$ and whose Hodge–Tate weights are contained in $\{0, 1\}$. Conversely, any such V is of the form $V = V_\pi G$ for some $G \in (\mathcal{O}-\mathrm{div}/O_K)$, by [B3, Thm. 5.3.2]. Note that $\overline{T} := T/\pi T = G[\pi](\overline{K})$.

The maps $H^1_{fl}(O_K, G[\pi^{n+1}]) \longrightarrow H^1_{fl}(O_K, G[\pi^n])$ induced by multiplication by π are surjective (by (1.3.3)); their projective limit

$$\varprojlim_n H^1_{fl}(O_K, G[\pi^n]) \subset \varprojlim_n H^1(K, G[\pi^n](\overline{K})) = \varprojlim_n H^1(K, T/\pi^n T) = H^1(K, T)$$

is equal to the Bloch–Kato subspace

$$\varprojlim_n H^1_{fl}(O_K, G[\pi^n]) = H^1_f(K,T) \tag{1.4.1}$$

and $H^1_f(K,T)/\pi^n H^1_f(K,T) = H^1_{fl}(O_K, G[\pi^n])$ for all $n \geq 1$ (see [N4, Prop. A.2.6]). In particular,

$$\mathscr{F} := \mathrm{Im}(H^1_f(K,T) \longrightarrow H^1(K,\overline{T})) = H^1_f(K,T)/\pi H^1_f(K,T) = H^1_{fl}(O_K, G[\pi]) \subset H^1(K,\overline{T}). \tag{1.4.2}$$

(1.5) Let $G' = (G'[\pi^n])_{n\geq 1} \in (\mathcal{O} - \mathrm{div}/O_K)$. Assume that there exists an isomorphism of the generic fibres $G[\pi]_K \xrightarrow{\sim} G'[\pi]_K$ (equivalently, an isomorphism of $\mathbf{F}[\Gamma_K]$-modules $\overline{T} = T/\pi T \xrightarrow{\sim} T'/\pi T' =: \overline{T}'$, where $T' := T_\pi G'$), which we fix. As in Introduction, we are interested in the relative position of $\mathscr{F}$ and

$$\mathscr{F}' := \mathrm{Im}(H^1_f(K,T') \longrightarrow H^1(K,\overline{T}')) = H^1_{fl}(O_K, G'[\pi]) \subset H^1(K,\overline{T}') \xrightarrow{\sim} H^1(K,\overline{T}).$$

According to [R, Prop. 2.2.2], the two flat models $G[\pi]$ and $G'[\pi]$ of $\overline{T}$ admit an infimum, i.e., a universal object $H \in (p - \mathrm{Gr}/O_K)$ for which $H_K(\overline{K}) = \overline{T}$ and for which there exist morphisms

$$G[\pi] \longrightarrow H \longleftarrow G'[\pi].$$

This is again an object of $(\mathbf{F} - \mathrm{vs}/O_K)$. We show in Proposition 2.13(1) below that the sum of the two canonical maps

$$\mathscr{F} = H^1_{fl}(O_K, G[\pi]) \longrightarrow H^1_{fl}(O_K, H) \longleftarrow H^1_{fl}(O_K, G'[\pi]) = \mathscr{F}' \tag{1.5.1}$$

(which are injective, since all three cohomology groups inject into the same space $H^1(K,\overline{T})$, thanks to (1.3.1) for $i = 1$) is surjective. As a result,

$$\mathscr{F}/(\mathscr{F}\cap\mathscr{F}') \xrightarrow{\sim} (\mathscr{F}+\mathscr{F}')/\mathscr{F}' = H^1_{fl}(O_K,H)/H^1_{fl}(O_K, G'[\pi]). \tag{1.5.2}$$

In Theorem 2.16 below we show that

$$\dim_{\mathbf{F}} \mathscr{F}/(\mathscr{F}\cap\mathscr{F}') \equiv 0 \pmod{(p-1)[k : k\cap\mathbf{F}]},$$

which implies Theorem A in the case $K = L$.

2. Breuil–Kisin modules and flat cohomology

(2.1) Let K and $\mathcal{K}$ be as in 1.1 (in particular, $p \neq 2$). We need some additional notation: $W := W(k)$, $K_0 := W[1/p]$, $e := e(K/\mathbf{Q}_p) = [K : K_0]$. Fix a uniformiser ϖ of O_K and denote by $E(X) \in W[X]$ the minimal polynomial of ϖ over K_0. This is an Eisenstein polynomial: $E(X) \equiv X^e \pmod{pW[X]}$, $E(0)/p \in W^\times$.

Let $\varphi : W \longrightarrow W$ be the lift of the absolute Frobenius $\varphi : a \mapsto a^p$ on k and define $\varphi : W[[u]] \longrightarrow W[[u]]$ by $\varphi(A(u)) = ({}^\varphi A)(u^p)$, where ${}^\varphi(\sum a_i u^i) = \sum \varphi(a_i) u^i$. The same formula defines φ on the p-adic completion $O_\mathcal{E}$ of $W((u)) = W[[u]][1/u]$.

(2.2) Fix a compatible system of p-power roots ϖ^{1/p^n} of ϖ and let $K_\infty = \bigcup_{n\geq 1} K(\varpi^{1/p^n})$. Fontaine's construction [Fo1, Thm. 3.4.3] based on the field of norms $k((u))$ of K_∞/K rather than that of $K(\mu_{p^\infty})/K$ ([B1], [K2, 1.1.12]) attaches to every continuous representation of $\Gamma_{K_\infty} = \mathrm{Gal}(\overline{K}/K_\infty)$ on a $\mathbf{Z}_p$-module of finite type T_0 (not necessarily free) an $O_\mathcal{E}$-module of finite type $D(T_0)$ (free if T_0 is free over $\mathbf{Z}_p$) equipped with a φ-semilinear map $\varphi : D(T_0) \longrightarrow D(T_0)$ for which

$$\varphi \otimes \mathrm{id} : \varphi^* D(T_0) = D(T_0) \otimes_{O_\mathcal{E},\varphi} O_\mathcal{E} \longrightarrow D(T_0)$$

is an isomorphism ($D(T_0)$ is an étale φ-module over $O_\mathcal{E}$). The functor

$$T_0 \mapsto D(T_0) := \left(T_0 \otimes_{\mathbf{Z}_p} O_{\widehat{\mathcal{E}}^{ur}}\right)^{\Gamma_{K_\infty}}$$

defines an equivalence of abelian categories (compatible with tensor products and duals)

$$\begin{array}{c}\{\text{continuous representations of } \Gamma_{K_\infty} \text{ on finite type } \mathbf{Z}_p\text{−modules}\}\\ \Big\downarrow\approx\\ \{\text{étale } \varphi\text{−modules of finite type over } O_{\mathcal{E}}\}\end{array}$$

with quasi-inverse given by

$$M \mapsto T_0(M) := \left(M \otimes_{O_{\mathcal{E}}} O_{\widehat{\mathcal{E}^{ur}}}\right)^{\varphi=\mathrm{id}}$$

Above, $O_{\widehat{\mathcal{E}^{ur}}}$ denotes a certain Cohen ring with uniformiser p and residue field $k((u))^{sep}$.

(2.3) Kisin ([K1, Thm. 2.2.7], [K2, Cor. 2.2.22]), building upon an earlier work of Breuil [B3, Thm. 4.2.2.9], established an exact antiequivalence of exact categories between $(p-\mathrm{div}/O_K)$ and the category BT_φ of pairs (M,φ), where:

(2.3.1) M is a free $W[[u]]$-module of finite type;
(2.3.2) $\varphi = \varphi_M : M \longrightarrow M$ is a φ-semilinear map;
(2.3.3) $M^\circ = \mathrm{Im}(\varphi \otimes \mathrm{id} : \varphi^*(M) \longrightarrow M)$ (i.e., the $W[[u]]$-submodule of M generated by $\varphi(M)$) contains $E(u)M$;
(2.3.4) morphisms are $W[[u]]$-linear maps commuting with φ.

(2.4) It will be more convenient for us to use covariant functors. The composition of Kisin's functor with Cartier duality yields an exact equivalence of exact $\mathbf{Z}_p$-linear categories

$$M : (p-\mathrm{div}/O_K) \xrightarrow{\approx} \mathrm{BT}_\varphi$$

with the following properties [K3, Thm. 1.2.1, Thm. 1.4.2]. If $G = (G[p^n])_{n\geq 1} \in (p-\mathrm{div}/O_K)$, $T_pG := \varprojlim G[p^n](\overline{K})$ and $V_pG := T_pG \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$, then:

(2.4.1) there is a functorial isomorphism

$$M(G) \otimes_{W[[u]]} O_{\mathcal{E}} \xrightarrow{\sim} D((T_pG)(-1)|_{\Gamma_{K_\infty}});$$

(2.4.2) the filtered φ-module of the crystalline representation $(V_pG)(-1)$ of Γ_K (whose Hodge–Tate weights are contained in $\{-1,0\}$) is given by functorial isomorphisms

$$D_{cris}((V_pG)(-1)) \xrightarrow{\sim} (M(G)/uM(G))[1/p],$$
$$D_{dR}((V_pG)(-1)) = Fil^0 \xrightarrow{\sim} \varphi^*(M(G))\otimes_{W[[u]]}K \supset Fil^1 \xrightarrow{\sim} (\varphi\otimes\mathrm{id})^{-1}(E(u)M(G))\otimes_W K_0 \supset Fil^2 = 0,$$

where the morphism $W[[u]] \longrightarrow K$ is given by sending u to ϖ;
(2.4.3) if $G = (\mu_{p^n})_{n\geq 1}$, then $M(G) = W[[u]]$ and $\varphi(1) = 1$;
(2.4.4) if $G = \underline{\mathbf{Z}}_p = (\mathbf{Z}/p^n\mathbf{Z})_{n\geq 1}$, then $M(G) = W[[u]](-1)$, whose underlying $W[[u]]$-module is equal to $W[[u]]$ and where $\varphi(1) = pE(u)/E(0)$.

(2.5) Proposition. *Let $G \in (p-\mathrm{div}/O_K)$, $M = M(G) \in \mathrm{BT}_\varphi$. The cohomology groups $H^i(C^\bullet(M))$ of the complex*

$$C^\bullet(M) := [\varphi_M - pE(u)/E(0) : M \longrightarrow M^\circ]$$

concentrated in degrees 0 and 1 are functorially isomorphic to

$$H^i(C^\bullet(M)) \xrightarrow{\sim} \mathrm{Ext}^i_{\mathrm{BT}_\varphi}(M(\underline{\mathbf{Z}}_p), M) = \mathrm{Ext}^i_{(p-\mathrm{div}/O_K)}(\underline{\mathbf{Z}}_p, G) \qquad (i = 0, 1).$$

Proof. For $i = 0$ the isomorphism $\mathrm{Hom}_{\mathrm{BT}_\varphi}(M(\underline{\mathbf{Z}}_p), M) \xrightarrow{\sim} \mathrm{Ker}(\varphi_M - pE(u)/E(0) : M \longrightarrow M^\circ)$ is obtained by sending $\alpha : W[[u]](-1) \longrightarrow M$ to $\alpha(1)$. For $i = 1$ we need to study exact sequences

$$0 \longrightarrow M \longrightarrow N \longrightarrow W[[u]](-1) \longrightarrow 0,$$

where N is a free $W[[u]]$-module equipped with a φ-semilinear map $\varphi_N : N \longrightarrow N$ and where the two morphisms commute with φ.

A choice of a $W[[u]]$-linear splitting $s : W[[u]](-1) \longrightarrow N$ identifies (N, φ_N) with

$$M \oplus W[[u]](-1), \qquad \varphi_N(m, f) = (\varphi_M(m) + \varphi(f)m_s, \varphi(f)pE(u)/E(0)),$$

where

$$m_s = \varphi_N(s(1)) - pE(u)/E(0) \cdot s(1) \in M.$$

If we choose another splitting s', then $m_{s'} - m_s \in (\varphi_M - pE(u)/E(0))M$. We claim that

$$N^\circ \supset E(u)N \iff (M \oplus W[[u]](-1))^\circ \supset E(u)(M \oplus W[[u]](-1)) \iff m_s \in M^\circ.$$

Indeed, if $N^\circ \supset E(u)N$, then there exist $f_i, g_i \in W[[u]]$ and $m_i \in M$ such that

$$(0, pE(u)/E(0)) = \sum_{i=1}^{n} g_i\, \varphi_N(m_i, f_i) = \left(\sum_i g_i\, \varphi_M(m_i) + (\sum_i g_i\, \varphi(f_i))\, m_s, (\sum_i g_i\, \varphi(f_i))\, pE(u)/E(0) \right),$$

hence $\sum_i g_i\, \varphi(f_i) = 1$ and $m_s = -\sum_i g_i\, \varphi_M(m_i) \in M^\circ$. Conversely, if $m_s \in M^\circ$, then $m_s = \sum_i h_i\, \varphi_M(m_i)$ for some $h_i \in W[[u]]$ and $m_i \in M$, which implies that

$$(m_s, 0) = \sum_i h_i\, \varphi_N(m_i, 0), \qquad (0, pE(u)/E(0)) = \varphi_N(0, 1) - \sum_i h_i\, \varphi_N(m_i, 0) \in N^\circ.$$

As $(E(u)M, 0) \subset M^\circ \subset N^\circ$, it follows that $E(u)N \subset N^\circ$, as claimed.

As a result, the map $\mathrm{Ext}^1_{\mathrm{BT}_\varphi}(M(\underline{\mathbf{Z}}_p), M) \longrightarrow H^1(C^\bullet(M))$ sending the class of N to the class of m_s is well defined and surjective. It is clearly additive and injective.

(2.6) Corollary. *For $G \in (p - \mathrm{div}/O_K)$ and $M = M(G)$ there is a functorial isomorphism*

$$H^1_f(K, T_pG) \xrightarrow{\sim} H^1(C^\bullet(M)) = M^\circ/(\varphi_M - pE(u)/E(0))M.$$

Proof. The subspace $H^1_f(K, T_pG) \subset H^1(K, T_pG)$ classifies those extensions of continuous $\mathbf{Z}_p$-representations of Γ_K

$$0 \longrightarrow T_pG \longrightarrow T \longrightarrow \mathbf{Z}_p \longrightarrow 0$$

for which $T = T_pG'$, for some $G' \in (p - \mathrm{div}/O_K)$ (by [BK, 3.7] and [B3, Thm. 5.3.2]). As the functor $G \mapsto T_pG$ is fully faithful [Ta, Thm. 4], the group of such extensions is isomorphic to the group of extensions

$$0 \longrightarrow G \longrightarrow G' \longrightarrow \underline{\mathbf{Z}}_p \longrightarrow 0$$

in $(p - \mathrm{div}/O_K)$, which is, in turn, isomorphic to $H^1(C^\bullet(M))$, by Proposition 2.5.

As the referee pointed out, the above argument (which gives another proof of (1.4.1), when combined with Proposition 2.9 below) can be replaced by a direct appeal to the equality (1.4.1) (and Proposition 2.9).

(2.7) The above discussion has a version with coefficients, namely, an exact equivalence of categories

$$M : (\mathcal{O} - \mathrm{div}/O_K) \xrightarrow{\approx} \mathrm{BT}_{\mathcal{O},\varphi},$$

where $\mathrm{BT}_{\mathcal{O},\varphi}$ is the $\mathcal{O}$-linear category of $(\mathcal{O} \otimes_{\mathbf{Z}_p} W)[[u]]$-modules of finite type, free as $W[[u]]$-modules, equipped with an $\mathcal{O}$-linear and $(\mathrm{id} \otimes \varphi)$-semilinear map $\varphi_M : M \longrightarrow M$ for which $M^\circ \supset E(u)M$.

It turns out that such a module is automatically free as an $(\mathcal{O} \otimes_{\mathbf{Z}_p} W)[[u]]$-module; this follows from the following two facts. Firstly, the $\mathcal{O}$-algebra $\mathcal{O} \otimes_{\mathbf{Z}_p} W$ is isomorphic to a product of r copies of the ring of integers $\mathcal{O}'$ of a finite unramified extension $\mathcal{K}'$ of $\mathcal{K}$ of degree $[\mathcal{K}' : \mathcal{K}] = [k : \mathbf{F}_p]/r$. Secondly, the semigroup

of all nonnegative powers $(\mathrm{id}\otimes\varphi)^n$ $(n\geq 0)$ of the Frobenius map $\mathrm{id}\otimes\varphi : \mathcal{O}\otimes_{\mathbf{Z}_p} W \longrightarrow \mathcal{O}\otimes_{\mathbf{Z}_p} W$ acts transitively on the set of $\mathcal{O}$-algebra morphisms $\mathcal{O}\otimes_{\mathbf{Z}_p} W \longrightarrow \mathcal{O}'$, since φ generates $\mathrm{Gal}(k/\mathbf{F}_p)$.

For $G\in(\mathcal{O}-\mathrm{div}/O_K)$ and $M=M(G)$, the complex $C^\bullet(M)$ from Proposition 2.5 satisfies

$$H^i(C^\bullet(M)) \xrightarrow{\sim} \mathrm{Ext}^i_{\mathrm{BT}_{\mathcal{O},\varphi}}(M(\underline{\mathcal{O}}),M) = \mathrm{Ext}^i_{(\mathcal{O}-\mathrm{div}/O_K)}(\underline{\mathcal{O}},G) \qquad (i=0,1),$$

which yields, as in Corollary 2.6, a functorial $\mathcal{O}$-linear isomorphism

$$H^1_f(K,T_\pi G) \xrightarrow{\sim} M^\circ/(\varphi_M - pE(u)/E(0))M.$$

(2.8) There is a similar description of $(\mathbf{F}-\mathrm{vs}/O_K)$ ([B3, Thm. 3.3.7], [K2, Prop. 1.1.11]), given by a commutative diagram of exact functors

$$\begin{array}{ccc} M:(\mathcal{O}-\mathrm{div}/O_K) & \longrightarrow & \mathrm{BT}_{\mathcal{O},\varphi} \\ \downarrow & & \downarrow \\ M:(\mathbf{F}-\mathrm{vs}/O_K) & \longrightarrow & \mathrm{BT}_{\mathbf{F},\varphi}, \end{array} \tag{2.8.1}$$

where

(2.8.2) $\mathrm{BT}_{\mathbf{F},\varphi}$ is the $\mathbf{F}$-linear category of pairs (M,φ_M), where M is a free $(\mathbf{F}\otimes k)[[u]]$-module of finite type equipped with an $\mathbf{F}$-linear and $(\mathrm{id}\otimes\varphi)$-semilinear map $\varphi_M : M\longrightarrow M$ such that $u^eM\subset M^\circ$ (where M° is the $(\mathbf{F}\otimes k)[[u]]$-submodule of M generated by $\varphi_M(M)$);

(2.8.3) the vertical functors are given, respectively, by $G\mapsto G[\pi]$ and $M\mapsto M/\pi M$;

(2.8.4) the horizontal functors are equivalences of categories;

(2.8.5) for every $G\in(\mathbf{F}-\mathrm{vs}/O_K)$ there is a functorial isomorphism

$$M(G)[1/u] := M(G)\otimes_{k[[u]]} k((u)) \xrightarrow{\sim} D(G_K(\overline{K})(-1)|_{\Gamma_{K_\infty}}),$$

which is a vector space over $k((u))$ of dimension $\mathrm{rk}_{\mathbf{F}}(G)=\dim_{\mathbf{F}} G_K(\overline{K})$.

(2.9) Proposition. *Let $G\in(\mathbf{F}-\mathrm{vs}/O_K)$, $M=M(G)\in\mathrm{BT}_{\mathbf{F},\varphi}$. The cohomology groups $H^i(C^\bullet(M))$ of the complex*

$$C^\bullet(M) := [\varphi_M - cu^e : M\longrightarrow M^\circ] \qquad (c:=p/E(0) \pmod{pW}\in k^\times)$$

concentrated in degrees 0 and 1 are functorially isomorphic to

$$H^i(C^\bullet(M)) \xrightarrow{\sim} \mathrm{Ext}^i_{\mathrm{BT}_{\mathbf{F},\varphi}}(M(\underline{\mathbf{F}}),M) = \mathrm{Ext}^i_{(\mathbf{F}-\mathrm{vs}/O_K)}(\underline{\mathbf{F}},G) = H^i_{fl}(O_K,G) \qquad (i=0,1).$$

Proof. The proof of Proposition 2.5 applies, with straightforward modifications.

(2.10) Proposition (The Euler characteristic formula). *Let $G\in(\mathbf{F}-\mathrm{vs}/O_K)$, $M=M(G)\in\mathrm{BT}_{\mathbf{F},\varphi}$.*
(1) For every integer $n>e/(p-1)$ the subcomplex $C^\bullet_n(M) := [\varphi_M - cu^e : u^nM\longrightarrow u^{n+e}M]\subset C^\bullet(M)$ is acyclic and $C^\bullet(M)$ is quasi-isomorphic to

$$C^\bullet(M)/C^\bullet_n(M) = \left[\varphi_M - cu^e : M/u^nM \longrightarrow M^\circ/u^{n+e}M\right].$$

(2) The Euler characteristic $\chi_{\mathbf{F}}(O_K,G) := \dim_{\mathbf{F}} H^0_{fl}(O_K,G) - \dim_{\mathbf{F}} H^1_{fl}(O_K,G)$ is equal to

$$\chi_{\mathbf{F}}(O_K,G) = \dim_{\mathbf{F}}(M/M^\circ) - [K:\mathbf{Q}_p]\,\mathrm{rk}_{\mathbf{F}}(G).$$

Proof. (1) If $pn>n+e$, then $(u^{-e}\varphi_M)(u^{n+e}M)\subset u^{-e}u^{p(n+e)}M\subset u^{n+pe+1}M$, the series

$$\sum_{i\geq 0} -(c^{-1}u^{-e}\varphi_M)^i((cu^e)^{-1}m)$$

converges for $m \in u^{n+e}M$ and defines an inverse map to $\varphi_M - cu^e : u^nM \longrightarrow u^{n+e}M$.
(2) It follows from (1) that $\chi_{\mathbf{F}}(O_K, G)$ is equal to

$$\dim_{\mathbf{F}}(M/u^nM) - \dim_{\mathbf{F}}(M^\circ/u^{n+e}M) = \dim_{\mathbf{F}}(M/M^\circ) - \dim_{\mathbf{F}}(M/u^eM) = \dim_{\mathbf{F}}(M/M^\circ) - e[k:\mathbf{F}_p]\,\mathrm{rk}_{\mathbf{F}}(G).$$

(2.11) Corollary. *If $G, G' \in (\mathbf{F}-\mathrm{vs}/O_K)$ have isomorphic generic fibres $G_K \xrightarrow{\sim} G'_K$, then*

$$\dim_{\mathbf{F}} H^1_{fl}(O_K, G) - \dim_{\mathbf{F}} H^1_{fl}(O_K, G') = \dim_{\mathbf{F}} M(G')/M(G')^\circ - \dim_{\mathbf{F}} M(G)/M(G)^\circ.$$

(2.12) If $G, G' \in (\mathbf{F}-\mathrm{vs}/O_K)$ have isomorphic generic fibres, then any choice of an isomorphism $f : G_K \xrightarrow{\sim} G'_K$ induces an isomorphism

$$M(f) : M(G)[1/u] \xrightarrow{\sim} M(G')[1/u] \tag{2.12.1}$$

of étale φ-modules over $(\mathbf{F}\otimes k)((u))$, by (2.8.5) (conversely, any isomorphism (2.12.1) arises from an isomorphism $G_K \xrightarrow{\sim} G'_K$, by [B4, Thm. 3.4.3], but we are not going to use this fact).

If we fix f and use $M(f)$ to identify $M(G)[1/u]$ with $M(G')[1/u]$, then the sum $M(G) + M(G') \subset M(G)[1/u] \xrightarrow{\sim} M(G')[1/u]$ is an object of $\mathrm{BT}_{\mathbf{F},\varphi}$, corresponding to $H \in (\mathbf{F}-\mathrm{vs}/O_K)$ which is, in the language of [R, Prop. 2.2.2], the infimum of G and G'. The inclusions $M(G) \hookrightarrow M(H) = M(G) + M(G') \hookleftarrow M(G')$ correspond to morphisms $G \longrightarrow H \longleftarrow G'$ inducing isomorphisms of generic fibres $G_K \xrightarrow{\sim} H_K \xleftarrow{\sim} G'_K$ compatible with f.

(2.13) Proposition. *Assume that we are in the situation of 2.12.*
(1) *The sum of the canonical (injective – see 1.5) maps $H^1_{fl}(O_K, G) \longrightarrow H^1_{fl}(O_K, H) \longleftarrow H^1_{fl}(O_K, G')$ defines a surjection $H^1_{fl}(O_K, G) \oplus H^1_{fl}(O_K, G') \longrightarrow H^1_{fl}(O_K, H)$.*
(2) *$H^1_{fl}(O_K, G)/(H^1_{fl}(O_K, G) \cap H^1_{fl}(O_K, G')) \xrightarrow{\sim} H^1_{fl}(O_K, H)/H^1_{fl}(O_K, G')$, where the intersection takes place inside $H^1_{fl}(O_K, H)$.*
(3) $\dim_{\mathbf{F}} H^1_{fl}(O_K, G)/(H^1_{fl}(O_K, G) \cap H^1_{fl}(O_K, G')) = \dim_{\mathbf{F}} M(G')/M(G')^\circ - \dim_{\mathbf{F}} M(H)/M(H)^\circ$.

Proof. We have $M(H)^\circ = M(G)^\circ + M(G')^\circ$, since $M(H) = M(G) + M(G')$. It follows that the canonical map $H^1(C^\bullet(M(G)) \oplus H^1(C^\bullet(M(G')) \longrightarrow H^1(C^\bullet(M(H))$ is surjective, which proves (1). The statement (2) is a consequence of (1), and (3) follows from (2) and Corollary 2.11 applied to H and G'.

(2.14) Decompositions of $\mathbf{F}\otimes k$ and $M(G)$. Fix embeddings of $\mathbf{F}$ and k into a sufficiently large finite extension of $\mathbf{F}_p$. Let $f = [k:\mathbf{F}_p]$, $f' = [\mathbf{F}\cap k : \mathbf{F}_p]$. The map

$$\mathbf{F}\otimes k \xrightarrow{\sim} \prod_{i=0}^{f'-1} \mathbf{F}k, \qquad a\otimes b \mapsto (i \mapsto a\varphi^i(b)) \tag{2.14.1}$$

is an isomorphism of $\mathbf{F}$-algebras under which the action of $\mathrm{id}\otimes\varphi$ on the left hand side corresponds to the map $(x_0, \dots, x_{f'-1}) \mapsto (x_1, \dots, x_{f'-1}, \varphi^v(x_0))$ on the right hand side, where $v \in \mathbf{Z}$ satisfies $v \equiv 0 \pmod{[\mathbf{F}:\mathbf{F}_p]}$ and $v \equiv f' \pmod{f}$.

For every $M \in \mathrm{BT}_{\mathbf{F},\varphi}$ we obtain from (2.14.1) a decomposition

$$M \xrightarrow{\sim} \bigoplus_{i=0}^{f'-1} M_i, \qquad M_i := M \otimes_{\mathbf{F}\otimes k, \mathrm{id}\otimes\varphi^i} \mathbf{F}k, \tag{2.14.2}$$

where each M_i is a free $\mathbf{F}k[[u]]$-module (of rank independent of i) and $\varphi_M|_{M_i} : M_i \longrightarrow M_{i-1}$ satisfies

$$\forall m \in M_i \quad \forall A(u) \in \mathbf{F}k[[u]] \qquad \varphi_M(A(u)m) = ({}^{\varphi^{v_i}}A)(u^p)\,\varphi_M(m), \tag{2.14.3}$$

where $v_0 = v$ and $v_i = 0$ for $i \neq 0$ (we consider the index i in (2.14.3) and in the proof of Proposition 2.15, but not in (2.14.1) and (2.14.2), as an element of $\mathbf{Z}/f'\mathbf{Z}$).

In particular, if there exists an embedding $k \hookrightarrow \mathbf{F}$, then $f' = f$, $\mathbf{F}k = \mathbf{F}$, $v = 0$ and

$$M \xrightarrow{\sim} \bigoplus_{\overline{\sigma}:k\hookrightarrow\mathbf{F}} M_{\overline{\sigma}}, \qquad M_{\overline{\sigma}} := M \otimes_{\mathbf{F}\otimes k,\mathrm{id}\otimes\overline{\sigma}} \mathbf{F}, \qquad \varphi_M|_{M_{\overline{\sigma}}} : M_{\overline{\sigma}} \longrightarrow M_{\overline{\sigma}\circ\varphi^{-1}}. \tag{2.14.4}$$

(2.15) Proposition. *Let $M, M' \in \mathrm{BT}_{\mathbf{F},\varphi}$. If the corresponding étale φ-modules $M[1/u], M'[1/u]$ over $(\mathbf{F}\otimes k)((u))$ are isomorphic, then*

$$\dim_{\mathbf{F}}(M'/M'^{\circ}) \equiv \dim_{\mathbf{F}}(M/M^{\circ}) \pmod{(p-1)[k : k\cap\mathbf{F}]}.$$

Proof. A choice of bases

$$M = \bigoplus_{\beta} \mathbf{F}k[[u]]\, m_\beta \qquad (m_\beta \in M_{i(\beta)}), \qquad M' = \bigoplus_{\beta'} \mathbf{F}k[[u]]\, m'_{\beta'} \qquad (m'_{\beta'} \in M'_{i(\beta')})$$

yields matrices $\Phi, \Phi' \in M_r(\mathbf{F}k[[u]]) \cap GL_r(\mathbf{F}k((u)))$ and $C \in GL_r(\mathbf{F}k((u)))$ such that

$$\varphi(m_\beta) = \sum_\alpha \Phi_{\alpha\beta}(u)\, m_\alpha, \qquad \varphi(m'_{\beta'}) = \sum_{\alpha'} \Phi'_{\alpha'\beta'}(u)\, m'_{\alpha'}, \qquad m'_{\gamma'} = \sum_\gamma C_{\gamma\gamma'}(u)\, m_\gamma. \tag{2.15.1}$$

As $i(\alpha) = i(\beta) - 1$, $i(\alpha') = i(\beta') - 1$ and $i(\gamma) = i(\gamma')$ if the coefficients in (2.15.1) are nonzero, these matrices have a block form

$$C = \begin{pmatrix} C_0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & C_{f'-1} \end{pmatrix}, \qquad \Phi = \begin{pmatrix} 0 & \Phi_1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \Phi_{f'-1} \\ \Phi_0 & 0 & \cdots & 0 \end{pmatrix} \tag{2.15.2}$$

(and similarly for Φ'), where the block C_i represents the identification between $M'_i[1/u]$ and $M_i[1/u]$, the block Φ_i the map $\varphi_M : M_i \longrightarrow M_{i-1}$ and the block Φ'_i the map $\varphi_{M'} : M'_i \longrightarrow M'_{i-1}$.

If we compute $\varphi(m'_{\beta'})$ in two different ways, we obtain

$$\varphi(m'_{\beta'}) = \sum_{\alpha'} \Phi'_{\alpha'\beta'}(u)\, m'_{\alpha'} = \sum_{\alpha',\alpha} C_{\alpha\alpha'}(u)\Phi'_{\alpha'\beta'}(u)\, m_\alpha,$$
$$\varphi(m'_{\beta'}) = \sum_\beta \varphi(C_{\beta\beta'}(u)\, m_\beta) = \sum_\beta \left({}^{\varphi^{v_{i(\beta)}}}C_{\beta\beta'}\right)(u^p)\, \varphi(m_\beta) = \sum_{\alpha,\beta} \Phi_{\alpha\beta}(u) \left({}^{\varphi^{v_{i(\beta)}}}C_{\beta\beta'}\right)(u^p)\, m_\alpha,$$

hence

$$C(u)\,\Phi'(u) = \Phi(u)\,({}^{\varphi^v}C)(u^p), \qquad {}^{\varphi^v}C = \begin{pmatrix} {}^{\varphi^v}C_0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & C_{f'-1} \end{pmatrix}, \tag{2.15.3}$$

which can be rewritten as

$$C_{i-1}(u)\,\Phi'_i(u) = \Phi_i(u)\,({}^{\varphi^{v_i}}C_i)(u^p).$$

Theory of elementary divisors yields

$$\dim_{\mathbf{F}k}(M_i/M_i^{\circ}) = \mathrm{ord}_u(\det(\Phi_{i+1}(u))), \qquad \dim_{\mathbf{F}k}(M'_i/M'^{\circ}_i) = \mathrm{ord}_u(\det(\Phi'_{i+1}(u)))$$

(where $M_i^{\circ} = M^{\circ} \cap M_i$ and $M'^{\circ}_i = M'^{\circ} \cap M'_i$), hence

$$\dim_{\mathbf{F}k}(M'/M'^{\circ}) - \dim_{\mathbf{F}k}(M/M^{\circ}) = \mathrm{ord}_u\left(\frac{\det(\Phi'(u))}{\det(\Phi(u))}\right) = (p-1)\,\mathrm{ord}_u(\det C(u)) \equiv 0 \pmod{(p-1)},$$

which proves the claim.

(2.16) Theorem. *Assume that $G, G' \in (\mathbf{F}-\mathrm{vs}/O_K)$ have isomorphic generic fibres; fix an isomorphism $G_K \xrightarrow{\sim} G'_K$. The subspaces $\mathscr{F} = H^1_{fl}(O_K, G) \subset H^1(K, G_K(\overline{K}))$ and $\mathscr{F}' = H^1_{fl}(O_K, G') \subset H^1(K, G'_K(\overline{K})) \xrightarrow{\sim} H^1(K, G_K(\overline{K}))$ then satisfy*

$$\dim_{\mathbf{F}} \mathscr{F}' \equiv \dim_{\mathbf{F}} \mathscr{F} \equiv \dim_{\mathbf{F}}(\mathscr{F} \cap \mathscr{F}') \pmod{(p-1)[k : k \cap \mathbf{F}]}.$$

Proof. The first congruence follows from Corollary 2.11 and Proposition 2.15 for $M = M(G)$ and $M' = M(G')$. The second congruence follows from Proposition 2.13(3) and Proposition 2.15 for $M = M(G) + M(G') = M(H)$ and $M' = M(G')$.

(2.17) Example. If $\mu_p \subset K$, then $(p-1) \mid e \mid [K : \mathbf{Q}_p]$ and the group schemes $G = \mu_p$, $G' = \underline{\mathbf{Z}/p\mathbf{Z}}$ have isomorphic generic fibres. The corresponding cohomology groups are

$$\begin{gathered}\mathscr{F} = O_K^\times \otimes \mathbf{Z}/p\mathbf{Z} \subset K^\times \otimes \mathbf{Z}/p\mathbf{Z} = H^1(K, \mu_p),\\ \mathscr{F}' = \mathrm{Hom}(\Gamma_K/I_K, \mathbf{Z}/p\mathbf{Z}) \subset \mathrm{Hom}(\Gamma_K, \mathbf{Z}/p\mathbf{Z}) = H^1(K, \mathbf{Z}/p\mathbf{Z}),\\ \mathscr{F} \cap \mathscr{F}' = \mathbf{Z}/p\mathbf{Z}(u \otimes 1), \quad u \in O_K^\times, \quad K(\sqrt[p]{u})/K \text{ unramified},\end{gathered}$$

hence

$$\dim_{\mathbf{F}_p} \mathscr{F} = 1 + [K : \mathbf{Q}_p], \qquad \dim_{\mathbf{F}_p} \mathscr{F}' = \dim_{\mathbf{F}_p}(\mathscr{F} \cap \mathscr{F}') = 1.$$

(2.18) Corollary. *Theorem A holds in the case $L = K$.*

Proof. As V and V' are crystalline, the Weil-Deligne representations $WD(V)$ and $WD(V')$ are unramified (and $\|\cdot\|_K$-symplectic, in the language of [N2, 1.5.3]), which implies that $\varepsilon(V) = \varepsilon(V') = 1$. As p is odd, $\dim_{\mathbf{F}} \mathscr{F}/(\mathscr{F} \cap \mathscr{F}') \equiv 0 \pmod 2$, by Theorem 2.16.

3. Interlude: invariants of symplectic lattices

(3.1) The goal of this section is to prove a result comparing two invariants of pairs of symplectic lattices (Proposition 3.10 below) that will be used in the proof of Theorem A. A key technical point (Lemma 3.14) was inspired by the arguments in [KMR, Lemma 2.3, Proposition 2.4].

(3.2) If Δ is a group acting on a commutative ring R by ring automorphisms, we denote by $R_\tau[\Delta] = \{\sum_{\delta\in\Delta} r_\delta \delta \mid r_\delta \in R, \text{the sum is finite}\}$ the twisted group ring with multiplication $(\sum r_\delta \delta)(\sum r'_{\delta'}\delta') = \sum r_\delta \delta(r'_{\delta'})\delta\delta'$.

(3.3) From now on until the end of §3, Δ will be a finite cyclic group of even order d and $\eta : \Delta \longrightarrow F^\times$ an injective group morphism into the multiplicative group of a field F (in particular, the characteristic of F is prime to d, hence different from 2).

We let Δ act on $F[[u]] \subset F((u))$ by $\delta(\sum a_i u^i) = \sum a_i(\eta(\delta)u)^i$ (so that $F[[u]]^\Delta = F[[u^d]]$ and $F((u))^\Delta = F((u^d))$). The twisted group rings $F[[u]]_\tau[\Delta] \subset F((u))_\tau[\Delta]$ satisfy $F[[u]]_\tau[\Delta]/(u) = F[\Delta]$.

The Grothendieck group $G_0(F[\Delta]) = K_0(F[\Delta])$ is a free abelian group on $[\eta^i]$ (the class of the character $\eta^i : \Delta \longrightarrow F^\times$), for $i \in \mathbf{Z}/d\mathbf{Z}$.

(3.4) Proposition-Definition. (1) *The morphisms of abelian groups*

$$\begin{aligned} I : K_0(F[\Delta]) &\longrightarrow \mathbf{Z}/d\mathbf{Z}, \qquad [\eta^i] \mapsto i\\ I' : G_0(F[[u]]_\tau[\Delta]) &\longrightarrow \mathbf{Z}/d\mathbf{Z}, \qquad X \mapsto I([X/uX]) - I([X[u] \otimes \eta])\end{aligned}$$

are well defined and the following relations hold: $I(X^\vee) = -I(X)$ (where $X^\vee$ denotes the dual representation) and $I'(X) + I'(Y) = I'(X \cap Y) + I'(X + Y)$.

(2) *If X is a $F[[u]]_\tau[\Delta]$-module which has finite length $\ell_{F[[u]]}(X)$ over $F[[u]]$, then*

$$I'(X) = -\ell_{F[[u]]}(X) \pmod d.$$

Proof. (1) If $0 \longrightarrow X \longrightarrow Y \longrightarrow Z \longrightarrow 0$ is an exact sequence of $F[[u]]_\tau[\Delta]$-modules of finite type, the snake lemma implies that

$$0 \longrightarrow X[u] \otimes \eta \longrightarrow Y[u] \otimes \eta \longrightarrow Z[u] \otimes \eta \xrightarrow{\partial} X/uX \longrightarrow Y/uY \longrightarrow Z/uZ \longrightarrow 0$$

is an exact sequence of $F[\Delta]$-modules of finite type (the map ∂ is induced by multiplication by u, whence the twist by η). Therefore I' is well defined, as claimed. The formula for $I(X^\vee)$ is immediate; the remaining formula follows from the exact sequence

$$0 \longrightarrow X \cap Y \longrightarrow X \oplus Y \longrightarrow X + Y \longrightarrow 0.$$

(2) As both I' and $\ell_{F[[u]]}$ factor through the Grothendieck group of modules of finite length, it is enough to check the statement in the case when X is a simple $F[[u]]_\tau[\Delta]$-module. This means that $X = X[u] = X/uX = F$ with Δ acting by η^i, hence $I'(X) = i - (i+1) \pmod d = -1 \pmod d$, as claimed.

(3.5) Definition. *Let W be a $F((u))_\tau[\Delta]$-module of finite type (which is equivalent to W being a finite-dimensional vector space over $F((u))$ equipped with a semilinear action of Δ). We say that $X \subset W$ is a* **τ-lattice in** *W if it is a $F[[u]]_\tau[\Delta]$-module of finite type such that $F((u))X = W$ (in other words, if it is a Δ-stable $F[[u]]$-lattice in W). In this case $X[u] = 0$ and $I'(X) = I(X/uX)$.*

(3.6) From now on until the end of §3 we assume that we are given a nonzero W as in Definition 3.5, equipped with a nondegenerate skew-symmetric $F((u))$-bilinear pairing

$$(\ ,\ ) : W \times W \longrightarrow F((u)) \tag{3.6.1}$$

satisfying

$$\forall \delta \in \Delta \quad \forall x, y \in W \qquad (\delta(x), \delta(y)) = \delta((x, y))$$

(briefly, (3.6.1) is a Δ-equivariant symplectic form on W).

(3.7) If $X \subset W$ is a τ-lattice, so is

$$X^* = \{y \in W \mid \forall x \in X \quad (x, y) \in F[[u]]\}.$$

If $Y \subset W$ is another τ-lattice, then

$$(X^*)^* = X, \qquad (X + Y)^* = X^* \cap Y^*, \qquad (X \cap Y)^* = X^* + Y^*. \tag{3.7.1}$$

If $X \subset Y$ are τ-lattices, then (3.6.1) induces a nondegenerate $F[[u]]$-bilinear Δ-equivariant pairing

$$Y/X \times X^*/Y^* \longrightarrow F((u))/F[[u]]. \tag{3.7.2}$$

We say that a τ-lattice X is **self-dual** if $X = X^*$. If this is the case, then (3.6.1) restricted to $X \times X$ induces a symplectic (i.e., nondegenerate, F-bilinear and alternating) pairing

$$\overline{(\ ,\ )} : X/uX \times X/uX \longrightarrow F,$$

which is Δ-equivariant (with Δ acting trivially on F). In other words, X/uX is a (finite-dimensional) symplectic $F[\Delta]$-module.

(3.8) The Grothendieck group $G_0(F[\Delta]_{Sp}) = K_0(F[\Delta]_{Sp})$ of such symplectic modules is isomorphic to the image

$$\mathrm{Im}(K_0(F[\Delta]) \longrightarrow K_0(F[\Delta])), \qquad A \mapsto A + A^\vee, \tag{3.8.1}$$

which is a free abelian group on $[\eta^i] + [\eta^{-i}]$ $(0 < i < d/2)$, $2[1]$ and $2[\eta^{d/2}]$.

(3.9) Proposition-Definition. *The morphism of abelian groups*

$$J : K_0(F[\Delta]_{Sp}) \longrightarrow \mathbf{Z}/2\mathbf{Z}, \qquad A + A^\vee \mapsto I(A) \pmod 2$$

is well defined.

Proof. This follows from the fact that the kernel of (3.8.1) is generated by elements of the form $A - A^\vee$, for which $I(A - A^\vee) = 2I(A) \in 2\mathbf{Z}$.

(3.10) Proposition. *If $X, Y \subset W$ are self-dual τ-lattices, then*

$$I'(X + Y) \pmod 2 = I((X + Y)/u(X + Y)) \pmod 2 = J(X/uX) + J(Y/uY) \in \mathbf{Z}/2\mathbf{Z}.$$

(3.11) Lemma. *Proposition 3.10 holds if $uX \subset Y \subset u^{-1}X$.*

Proof. The inclusions $uX \subset Y \subset u^{-1}X$ imply that $u(X + Y) \subset X \cap Y \subset X + Y$. Applying (3.7.2) to the inclusions $u(X + Y) \subset X$, $X \cap Y \subset X$ and using (3.7.1), we obtain nondegenerate Δ-equivariant F-bilinear pairings

$$\frac{X \cap Y}{u(X + Y)} \times \frac{u^{-1}(X \cap Y)}{X + Y} \longrightarrow u^{-1}F[[u]]/F[[u]] = [\eta^{-1}] \longleftarrow \frac{X}{X \cap Y} \times \frac{Y}{X \cap Y}.$$

If we multiply the first pairing by u, we obtain on $(X \cap Y)/u(X + Y)$ a structure of a symplectic $F[\Delta]$-module, which means that the corresponding classes in $K_0(F[\Delta])$ satisfy

$$M = \left[\frac{X \cap Y}{u(X + Y)}\right] = M^\vee, \qquad N = \left[\frac{X}{X \cap Y}\right] = [\eta^{-1}]P^\vee, \qquad P = \left[\frac{Y}{X \cap Y}\right] = [\eta^{-1}]N^\vee.$$

The graded quotients of the filtrations by $F[\Delta]$-submodules

$$\frac{X \cap Y}{u(X + Y)} \subset \frac{X}{u(X + Y)} \subset \frac{X + Y}{u(X + Y)}, \qquad \frac{u(X + Y)}{uX} \subset \frac{X \cap Y}{uX} \subset \frac{X}{uX}, \qquad \frac{u(X + Y)}{uY} \subset \frac{X \cap Y}{uY} \subset \frac{Y}{uY}$$

can be expressed in terms of M, N and P, which yields the following relations in $K_0(F[\Delta])$:

$$\left[\frac{X + Y}{u(X + Y)}\right] = M + N + P, \qquad [X/uX] = M + N + [\eta]P, \qquad [Y/uY] = M + P + [\eta]N.$$

Therefore

$$[X/uX] + [Y/uY] = \left[\frac{X + Y}{u(X + Y)}\right] + \left[\frac{X + Y}{u(X + Y)}\right]^\vee,$$

which implies that $J(X/uX) + J(Y/uY) = I((X + Y)/u(X + Y)) \pmod 2$, as claimed.

(3.12) Lemma. *If $X, Y \subset W$ are self-dual τ-lattices, then there exists a chain of self-dual τ-lattices $X = X_0, X_1, \ldots, X_n = Y$ such that $uX_i \subset X_{i+1} \subset u^{-1}X_i$ holds, for all $i = 0, \ldots, n - 1$.*

Proof. There exists $n \geq 0$ such that $u^n X \subset Y \subset u^{-n}X$. There is nothing to prove if $n = 0, 1$. If $n > 1$, then $Z = uX + (Y \cap u^{-1}X)$ is a τ-lattice satisfying

$$Z^* = (uX)^* \cap (Y \cap u^{-1}X)^* = u^{-1}X \cap (Y + uX) = (u^{-1}X \cap Y) + uX = Z,$$

thanks to (3.7.1). Moreover, $uX \subset Z \subset u^{-1}X$, $Z \subset uX + Y \subset u^{1-n}Y$ and $u^{n-1}Y = (u^{1-n}Y)^* \subset Z^* = Z$. We define $X_1 = Z$ and repeat the argument with X_1, Y and $n - 1$.

(3.13) Lemma. *Assume that $X, Y, Z \subset W$ are self-dual τ-lattices.*
(1) *$I'(X) = I'(Y) = 0$ and $I'(X+Y) = -I'(X \cap Y)$.*
(2) *The τ-lattice $U := (X+Y) \cap Z + (X \cap Y)$ is self-dual.*
(3) *The formula $[x+y, x'+y'] := (x, y') \pmod{F[[u]]}$ defines a symmetric $F[[u]]$-bilinear Δ-equivariant pairing $[\ ,\ ] : ((X+Y)\cap Z) \times ((X+Y)\cap Z) \longrightarrow F((u))/F[[u]]$ with kernel $(X \cap Z) + (Y \cap Z)$.*

Proof. (1) $I'(X) = I([X/uX])$, but X/uX is symplectic, hence $[X/uX] = A + A^\vee$ for some $A \in K_0(F[\Delta])$, which implies that $I([X/uX]) = I(A) + I(A^\vee) = 0$. The same argument applies to Y. The remaining formula follows from Proposition 3.4(1).
(2) The rules (3.7.1) imply that

$$U^* = ((X+Y)\cap Z)^* \cap (X \cap Y)^* = ((X+Y)^* + Z) \cap (X+Y) = ((X\cap Y) + Z) \cap (X+Y) = (X \cap Y) + Z \cap (X+Y).$$

(3) We apply the argument from [KMR, Lemma 2.3]. The pairing is well defined, since $x \in X$ and $y' \in Y$ are unique modulo $X \cap Y = (X+Y)^*$. It is symmetric, since $(x,y') - (x',y) = (x+y, x'+y') - (x,x') - (y,y') = (z,z') - (x,x') - (y,y') \in F[[u]]$ (note that both $z = x+y$ and $z' = x'+y'$ lie in Z). The submodule $(X \cap Z) + (Y \cap Z)$ is contained in the kernel of $[\ ,\ ]$, by definition. Conversely, if $z = x + y$ lies in the kernel of $[\ ,\ ]$, then

$$\forall z' = x' + y' \in (X+Y) \cap Z \ \ \forall x'' \in X \cap Y \quad 0 = [z, z'] = (x, y') \pmod{F[[u]]} = (x, z' + x'') \pmod{F[[u]]},$$

which means that $x \in U^* = U$. As a result, after modifying $x \in X$ and $y \in Y$ by an element of $X \cap Y$, we can assume that $x, y \in Z$, hence $z = x + y \in (X \cap Z) + (Y \cap Z)$.

(3.14) Lemma. *If $X, Y, Z \subset W$ are self-dual τ-lattices, then:*
(1) *$I'((X+Y)\cap Z)) \equiv I'((X\cap Z) + (Y \cap Z)) \pmod 2$.*
(2) *$I'(X+Y) - I'(X+Z) + I'(Y+Z) \pmod 2 = 0 \in \mathbf{Z}/2\mathbf{Z}$.*

Proof. (1) The quotient $A := ((X+Y)\cap Z)/((X\cap Z) + (Y \cap Z))$ has finite length over $F[[u]]$, which implies, by Proposition 3.4(2), that

$$I'((X+Y)\cap Z)) - I'((X\cap Z) + (Y \cap Z)) = -\ell_{F[[u]]}(A) \pmod d.$$

We are going to deduce from the existence of a nondegenerate symmetric Δ-equivariant $F[[u]]$-bilinear pairing $[\ ,\ ] : A \times A \longrightarrow F((u))/F[[u]]$ established in Lemma 3.13(3) that the length of A is even.

There exists an isomorphism of $F[[u]]$-modules $A \xrightarrow{\sim} \bigoplus_{i=1}^n (u^{-i}F[[u]]/F[[u]])^{b_i}$. The F-vector space $A[u]$ has a filtration

$$A[u] =: F^1 \supset uA[u^2] =: F^2 \supset \cdots \supset u^{n-1}A =: F^n \supset 0 =: F^{n+1}$$

with graded quotients $gr_F^i = F^i/F^{i+1}$ satisfying $\dim_F(gr_F^i) = b_i$. For each $i = 1, \dots, n$, the pairing

$$[\ ,\ ]_i : gr_F^i \times gr_F^i \longrightarrow u^{i-2}F[[u]]/u^{i-1}F[[u]] = [\eta^{i-2}]$$

defined by the formula

$$[u^{i-1}x, u^{i-1}y]_i := u^{2i-2}\left([x,y] \pmod{u^{1-i}F[[u]]}\right) \qquad (x, y \in A[u^i])$$

is F-bilinear, nondegenerate and Δ-equivariant. If $i = 2m+1$ is odd, this implies that

$$[gr_F^{2m+1}] = \sum_{j=1}^{d/2} c_j \left([\eta^{m-j}] + [\eta^{m-1+j}]\right) \in K_0(F[\Delta])$$

for some $c_j \in \mathbf{Z}$, hence $b_{2m+1} \equiv 0 \pmod 2$. It follows that

$$\ell_{F[[u]]}(A) = \sum_{i=1}^{n} ib_i \equiv 0 \pmod 2,$$

as required.
(2) As in the proof of [KMR, Prop. 2.4], we use repeatedly the last formula from Proposition 3.4(1). The congruence (1) implies that

$$I'(X\cap Z)+I'(Y\cap Z) = I'((X\cap Z)+(Y\cap Z))+I'(X\cap Y\cap Z) \equiv I'((X+Y)\cap Z)+I'(X\cap Y\cap Z) \pmod 2,$$

hence

$$I'(X\cap Y)+I'(X\cap Z)+I'(Y\cap Z) \equiv I'(X\cap Y)+I'((X+Y)\cap Z)+I'(X\cap Y\cap Z) = \\ = I'(U)+2I'(X\cap Y\cap Z) \equiv I'(U) \equiv 0 \pmod 2.$$

The last congruence follows from Lemma 3.13(1), since the τ-lattice $U = (X+Y)\cap Z + (X\cap Y)$ is self-dual, by Lemma 3.13(2). This finishes the proof of Lemma 3.14.

Proof of Proposition 3.10. We must show that the invariant $f(X,Y) = I'(X+Y) \pmod 2 + J(X/uX) + J(Y/uY) \in \mathbf{Z}/2\mathbf{Z}$ of a pair of self-dual τ-lattices X, Y is identically zero. Lemma 3.14(2) tells us that $f(X,Y)+f(Y,Z) = f(X,Z)$. In particular, if $X = X_0, \dots, X_n = Y$ are as in Lemma 3.12, then $f(X,Y) = \sum_{i=1}^{n} f(X_{i-1}, X_i)$, but $f(X_{i-1}, X_i) = 0$ for all i, by Lemma 3.11, which implies that $f(X,Y) = 0$.

4. Breuil–Kisin modules with totally tamely ramified descent data

(4.1) We return to the situation of 2.1 and 2.2 (in particular, $p \neq 2$). Assume that L is an intermediate field $\mathbf{Q}_p \subset L \subset K$ such that K/L is a Galois extension with Galois group Δ.

(4.2) Definition [BCDT, 4.1], [Sav1, Def. 3.1]. *A* **descent datum relative to** K/L *on* $G \in (p - \mathrm{Gr}/O_K)$ *is a collection of morphisms* $[\delta] : G \longrightarrow {}^{\delta}G$ *(*$\delta \in \Delta$*), where* $[\mathrm{id}] = \mathrm{id}$, $[\delta\delta'] = ({}^{\delta}[\delta']) \circ [\delta]$ *and* ${}^{\delta}G$ *is defined by a cartesian diagram*

$$\begin{array}{ccc} {}^{\delta}G & \xrightarrow{\ \mathrm{can}\ } & G \\ \downarrow & & \downarrow \\ \mathrm{Spec}(O_K) & \xrightarrow{\mathrm{Spec}(\delta)} & \mathrm{Spec}(O_K). \end{array}$$

Note that these conditions ensure that each $[\delta]$ *is an isomorphism.*

(4.3) Such a descent datum gives rise to a descent datum on the Cartier dual G^D and to an action of Γ_L on $G_K(\overline{K})$ that extends the canonical action of Γ_K ([BCDT, 4.1], [Sav1, 3.1]): if $\gamma \in \Gamma_L$ and $\delta = \gamma|_K \in \Delta$, then the action of γ on a point $Q \in G_K(\overline{K}) = G(O_{\overline{K}}) = \mathrm{Hom}_{(Sch/\mathrm{Spec}(O_K))}(\mathrm{Spec}(O_{\overline{K}}), G)$ is given by

$$\gamma(Q) = \mathrm{can}\circ[\delta^{-1}]\circ Q\circ\mathrm{Spec}(\gamma) : \mathrm{Spec}(O_{\overline{K}}) \xrightarrow{\mathrm{Spec}(\gamma)} \mathrm{Spec}(O_{\overline{K}}) \xrightarrow{Q} G(O_{\overline{K}}) \xrightarrow{[\delta^{-1}]} ({}^{\delta^{-1}}G)(O_{\overline{K}}) \xrightarrow{\mathrm{can}} G(O_{\overline{K}}). \quad (4.3.1)$$

Equivalently, the generic fibre G_K descends to a finite flat group scheme G_L over $\mathrm{Spec}(L)$ and the action (4.3.1) is the Galois action of Γ_L on $G_L(\overline{K})$.

(4.4) Similarly, a descent datum relative to K/L on $G = (G[\pi^n])_{n\geq 1} \in (\mathcal{O} - \mathrm{div}/O_K)$ consists of a compatible system of descent data on all $G[\pi^n]$. We obtain, therefore, a diagram of exact $\mathcal{O}$-linear categories and functors

$$\begin{array}{ccc} (\mathcal{O} - \mathrm{div}/O_K)_{dd,K/L} & \longrightarrow & (\mathcal{O} - \mathrm{div}/O_K) \\ \downarrow & & \downarrow \\ (\mathcal{O}[\Gamma_L] - \mathrm{Mod}) & \longrightarrow & (\mathcal{O}[\Gamma_K] - \mathrm{Mod}) \end{array} \quad (4.4.1)$$

in which the vertical functors are given by $G \mapsto T_\pi G$ and the horizontal ones forget the descent data. Tate's full faithfulness theorem [Ta, Thm. 4] for the right vertical arrow implies that the diagram (4.4.1) is 2-cartesian, i.e., if $G \in (\mathcal{O} - \mathrm{div}/O_K)$, then an extension of the Γ_K-action on $T_\pi G$ to a Γ_L-action defines a descent datum relative to K/L on G.

There is a similar diagram of exact $\mathbf{F}$-linear categories and functors

$$\begin{array}{ccc} (\mathbf{F} - \mathrm{vs}/O_K)_{dd,K/L} & \longrightarrow & (\mathbf{F} - \mathrm{vs}/O_K) \\ \downarrow & & \downarrow \\ (\mathbf{F}[\Gamma_L] - \mathrm{Mod}) & \longrightarrow & (\mathbf{F}[\Gamma_K] - \mathrm{Mod}), \end{array}$$

which is not 2-cartesian in general.

(4.5) Proposition. *For each $G \in (\mathcal{O} - \mathrm{div}/O_K)_{dd,K/L}$ the diagram*

$$\begin{array}{ccc} \mathrm{Ext}^1_{(\mathcal{O}-\mathrm{div}/O_K)_{dd,K/L}}(\underline{\mathcal{O}}, G) & \longrightarrow & \mathrm{Ext}^1_{(\mathcal{O}-\mathrm{div}/O_K)}(\underline{\mathcal{O}}, G) \\ \downarrow & & \downarrow \\ \mathrm{Ext}^1_{(\mathcal{O}[\Gamma_L]-\mathrm{Mod})}(\mathcal{O}, T_\pi G) & \longrightarrow & \mathrm{Ext}^1_{(\mathcal{O}[\Gamma_K]-\mathrm{Mod})}(\mathcal{O}, T_\pi G) \end{array}$$

is cartesian, both vertical arrows are injective and their respective images are equal to $H^1_f(L, T_\pi G) \subset H^1(\Gamma_L, T_\pi G)$ and $H^1_f(K, T_\pi G) \subset H^1(\Gamma_K, T_\pi G)$, respectively.

Proof. The statement about the right vertical arrow was discussed in 2.6. The diagram is cartesian, since (4.4.1) is 2-cartesian. This implies that the left vertical arrow is injective and its image is equal to

$$\mathrm{Ker}(H^1(L, T_\pi G) \longrightarrow H^1(K, T_\pi G) \longrightarrow H^1(K, V_\pi G)/H^1_f(K, V_\pi G)) =$$
$$\mathrm{Ker}(H^1(L, T_\pi G) \longrightarrow (H^1(K, V_\pi G)/H^1_f(K, V_\pi G))^\Delta = H^1(L, V_\pi G)/H^1_f(L, V_\pi G)) = H^1_f(L, T_\pi G).$$

(4.6) It would be natural to try to generalise the results of §2 to the subspaces

$$\mathscr{F} = \mathrm{Im}(H^1_f(L, T) \longrightarrow H^1(L, \overline{T})), \qquad \mathscr{F}' = \mathrm{Im}(H^1_f(L, T') \longrightarrow H^1(L, \overline{T}') \xrightarrow{\sim} H^1(L, \overline{T})) \tag{4.6.1}$$

(where $T = T_\pi G$ and $T' = T_\pi G'$), whenever $G, G' \in (\mathcal{O} - \mathrm{div}/O_K)_{dd,K/L}$ have isomorphic $\overline{T} = G[\pi](\overline{K}) \xrightarrow{\sim} \overline{T}' = G'[\pi](\overline{K})$ (as $\mathbf{F}[\Gamma_L]$-modules).

The equivalences of categories discussed in 2.3 and 2.8 were extended – in their original version due to Breuil [B3] – to the case incorporating descent data in [BCDT, 5.6]. The description of general descent data on Breuil modules is fairly complicated, especially if the extension K/L is wildly ramified. If K/L is tamely ramified and if there exists a uniformiser $\varpi \in O_K$ such that $\varpi^{e(K/L)} \in O_L$, then $\Delta \simeq \mathrm{Gal}(K_\infty/L_\infty) \simeq \mathrm{Gal}(k((u))/k_L((u^{e(K/L)})))$ and the theory becomes much simpler [Sav2, Prop. 3.2]. The corresponding theory for Kisin modules was discussed in this particular case in [NY, §5]. For our purposes it will be sufficient to consider the simplest possible case, namely, when the extension K/L is totally tamely ramified.

(4.7) From now on until the end of §4 we assume that K/L is a totally tamely ramified Galois extension. Its Galois group Δ is then cyclic of order d dividing $q-1$, where $q = p^f = |k|$ is the cardinality of the common residue field of K and L. After changing the uniformiser if necessary we can – and will – assume that $\varpi^d \in O_L$. The isomorphism

$$\eta : \Delta \xrightarrow{\sim} \mu_d(O_L) = \mu_d(W) \xrightarrow{\sim} \mu_d(k), \qquad \eta(\delta) = \delta(\varpi)/\varpi \tag{4.7.1}$$

is canonical (it does not depend on the choice of ϖ). The restriction of the character $\eta \circ \mathrm{rec}_L : L^\times \longrightarrow \mu_d(k)$ to $O_L^\times$ factors through $(O_L/\varpi^d O_L)^\times = k^\times$ and

$$(\eta \circ \mathrm{rec}_L)(-1) = (-1)^{(q-1)/d}. \tag{4.7.2}$$

If $L_\infty = \bigcup_{n\geq 1} L((\varpi^{1/p^n})^d)$, then there are canonical isomorphisms

$$\Delta \simeq \mathrm{Gal}(K_\infty/L_\infty) \simeq \mathrm{Gal}(k((u))/k((u^d))),$$

where $k((u))$ (resp. $k((u^d))$) is the field of norms of K_∞/K (resp. of L_∞/L) and $\delta(u) = \eta(\delta)u$ for all $\delta \in \Delta$. We let, therefore, Δ act on $(\mathcal{O}\otimes_{\mathbf{Z}_p} W)[[u]]$, $\mathcal{O}\otimes_{\mathbf{Z}_p} O_{\mathcal{E}}$ and $(\mathbf{F}\otimes k)[[u]]$ by the following formula (cf. 3.3):

$$\delta\big(\sum_{i\geq 0} a_i u^i\big) = \sum_{i\geq 0} a_i (1\otimes \eta(\delta))^i u^i.$$

Note that $(\mathcal{O}\otimes_{\mathbf{Z}_p} O_{\mathcal{E}})^\Delta$ is the p-adic completion of $(\mathcal{O}\otimes_{\mathbf{Z}_p} W)[[u^d]][1/u^d]$.

(4.8) In this particular situation the descent data on Kisin modules have the following explicit form ([Sav2, Prop. 3.2], [NY, Def. 5.3]). An object of $(\mathrm{BT}_{\mathcal{O},\varphi})_{dd,K/L}$ (resp. of $(\mathrm{BT}_{\mathbf{F},\varphi})_{dd,K/L}$) is an object M of $\mathrm{BT}_{\mathcal{O},\varphi}$ (resp. of $\mathrm{BT}_{\mathbf{F},\varphi}$) equipped with maps $[\delta] : M \longrightarrow M$ ($\delta \in \Delta$) satisfying

(4.8.1) $[\delta](m+m') = [\delta](m) + [\delta](m')$;

(4.8.2) $[\mathrm{id}] = \mathrm{id}$ and $[\delta\delta'] = [\delta]\circ[\delta']$;

(4.8.3) $[\delta]\circ\varphi_M = \varphi_M \circ [\delta]$;

(4.8.4) $[\delta]\Big((\sum_{i\geq 0} a_i u^i)m\Big) = (\sum_{i\geq 0} a_i(1\otimes\eta(\delta)^i)u^i)[\delta](m)$, for all $m \in M$ and $a_i \in \mathcal{O}\otimes_{\mathbf{Z}_p} W$ (resp. $a_i \in \mathbf{F}\otimes k$). As pointed out by the referee, this semilinearity condition was initially stated incorrectly in [NY], where the authors considered only the special case when $\sum_{i\geq 0} a_i u^i = a_j u^j$ is a monomial.

(4.9) The equivalences of categories discussed in 2.4, 2.7 and 2.8 extend as follows. The diagram (2.8.1) has an analogue (compatible with (2.8.1) via the functors "forget the descent data")

$$\begin{array}{ccc} M : (\mathcal{O}-\mathrm{div}/O_K)_{dd,K/L} & \longrightarrow & (\mathrm{BT}_{\mathcal{O},\varphi})_{dd,K/L} \\ \downarrow & & \downarrow \\ M : (\mathbf{F}-\mathrm{vs}/O_K)_{dd,K/L} & \longrightarrow & (\mathrm{BT}_{\mathbf{F},\varphi})_{dd,K/L}, \end{array}$$

in which the horizontal functors are equivalences of categories and the vertical functors are as in (2.8.3). The properties from 2.4 have the following analogues. If $G \in (\mathcal{O}-\mathrm{div}/O_K)_{dd,K/L}$, then the following statements hold.

(4.9.1) $M(G)\otimes_{(\mathcal{O}\otimes_{\mathbf{Z}_p}W)[[u]]} O_{\mathcal{E}}$ is an étale φ-module over $\mathcal{O}\otimes_{\mathbf{Z}_p} O_{\mathcal{E}}$ equipped with a semilinear action of Δ, which implies that it comes, by extension of scalars, from an étale φ-module $(M(G)\otimes_{(\mathcal{O}\otimes_{\mathbf{Z}_p}W)[[u]]} O_{\mathcal{E}})^\Delta$ over $(\mathcal{O}\otimes_{\mathbf{Z}_p} O_{\mathcal{E}})^\Delta$ attached to L_∞/L. Moreover, there is a functorial isomorphism

$$(M(G)\otimes_{(\mathcal{O}\otimes_{\mathbf{Z}_p}W)[[u]]} O_{\mathcal{E}})^\Delta \xrightarrow{\sim} D_L((T_\pi G)(-1)|_{L_\infty}),$$

where D_L denotes Fontaine's functor attached to L_∞/L.

(4.9.2) The $\mathcal{K}$-linear continuous representation $V_\pi G = (T_\pi G)(-1)\otimes_{\mathcal{O}}\mathcal{K}$ of Γ_L becomes crystalline (with Hodge–Tate weights contained in $\{-1,0\}$) after restriction to Γ_K. Its filtered $(\varphi, \mathrm{Gal}(K/L)) = (\varphi,\Delta)$-module $D := D_{cris}((V_\pi G)(-1)|_{\Gamma_K})$ is functorially isomorphic to $(M(G)/uM(G))[1/p]$, with filtration on D_{dR} as in (2.4.2).

(4.9.3) In particular, D is a free $\mathcal{K}\otimes_{\mathbf{Q}_p} K_0$-module equipped with an $\mathrm{id}\otimes\varphi$-semilinear bijection $\varphi_D : D \longrightarrow D$ and a $\mathcal{K}\otimes_{\mathbf{Q}_p} K_0$-linear action of Δ commuting with φ_D. The Weil-Deligne representation $WD((V_\pi G)(-1))$ of the Weil group W_L of L attached to $(V_\pi G)(-1)$ is defined as follows ([Fo2], [FoPR, I.1.3.2]). Fix a sufficiently large finite extension $\mathcal{K}'$ of $\mathcal{K}$ and an embedding $\sigma : K_0 \hookrightarrow \mathcal{K}'$. The $\mathcal{K}'$-vector space $D_\sigma := D_{\mathcal{K}\otimes_{\mathbf{Q}_p}K_0,\mathrm{id}\otimes\sigma}\mathcal{K}'$ is then equipped with a $\mathcal{K}'$-linear action of the Weil group W_L, given by the formula

$$w(d\otimes\lambda) := (\varphi_D^{[K_0:\mathbf{Q}_p]n(w)}\circ w|_K)(d)\otimes\lambda,$$

where $n : W_L \longrightarrow W_L/I_L \xrightarrow{\sim} \mathbf{Z}$ sends the geometric Frobenius element $\mathrm{Fr}_{\mathrm{geom}} \in W_L/I_L$ of L to $1 \in \mathbf{Z}$ (note that the action of the inertia group I_L on D_σ factors through $I_L/I_K = \Delta$). By definition, $WD((V_\pi G)(-1))$ is the isomorphism class of the $\mathcal{K}'[W_L]$-module D_σ. It does not depend on the choice of σ, since $\varphi_D \otimes \mathrm{id} : D_\sigma \longrightarrow D_{\sigma\varphi^{-1}}$ is an isomorphism of $\mathcal{K}'[W_L]$-modules.

(4.9.4) If $L = \mathbf{Q}_p$ and $K = \mathbf{Q}_p(\mu_p)$, then $e = d = p-1$, $k = \mathbf{F}_p$, $f = 1$ and $\eta = \mathrm{id} : \Delta = (\mathbf{Z}/p\mathbf{Z})^\times \xrightarrow{\sim} \mathrm{Aut}(\mathbf{F}_p)$. If $\mathcal{O} = \mathbf{Z}_p$, $\mathbf{F} = \mathbf{F}_p$, $\mathcal{K} = \mathbf{Q}_p$ and $0 \le a < p-1$, then $M = \mathbf{Z}_p[[u]]m$, $\varphi(m) = m$, $\delta(m) = \eta(\delta)^{-a}m$ is an object $M \in (\mathrm{BT}_{\mathcal{O},\varphi})_{dd,K/L}$ corresponding to $G = (\mu_{p^n})_{n\ge1}$ with an appropriate descent datum. In this case $M^\Delta = u^a\mathbf{Z}_p[[u^{p-1}]]$, $(M(G) \otimes_{(\mathcal{O}\otimes_{\mathbf{Z}_p}W)[[u]]} O_\mathcal{E})^\Delta = u^a O_\mathcal{E}^\Delta$ and the Γ_L-module $T = T_pG$ is isomorphic to $\mathbf{Z}_p(1) \otimes \eta^{-a}$.

(4.10) The discussion in 2.5–2.13 has straightforward analogues in our situation, since $p \nmid |\Delta|$. If $G \in (\mathcal{O} - \mathrm{div}/O_K)_{dd,K/L}$ and $M = M(G)$, then $T := T_\pi G$ and $\overline{T} := T/\pi T = G[\pi](\overline{K})$ are Γ_L-modules and the restriction maps $H^i(\Gamma_L, X) \longrightarrow H^i(\Gamma_K, X)^\Delta$ $(X = T, \overline{T})$ are isomorphisms. This implies that $H^1_f(L,T) \simeq H^1_f(K,T)^\Delta$ and

$$\mathscr{F} := \mathrm{Im}\left(H^1_f(L,T) \longrightarrow H^1(L,\overline{T})\right) \simeq \mathrm{Im}\left(H^1_f(K,T) \longrightarrow H^1(K,\overline{T})\right)^\Delta = H^1_{fl}(O_K, G[\pi])^\Delta. \tag{4.10.1}$$

Let $\overline{M} := M/\pi M = M(G[\pi]) \in (\mathbf{F} - \mathrm{vs}/O_K)_{dd,K/L}$ and $c := p/E(0) \pmod p W \in k^\times$. The complexes

$$C^\bullet(M) = [\varphi_M - pE(u)/E(0) : M \longrightarrow M^\circ], \qquad C^\bullet(\overline{M}) = \left[\varphi_{\overline{M}} - cu^e : \overline{M} \longrightarrow \overline{M}^\circ\right]$$

are complexes of $(\mathcal{O} \otimes_{\mathbf{Z}_p} W)[\Delta]$-modules and $(\mathbf{F} \otimes k)[\Delta]$-modules, respectively, since Δ acts trivially on $E(u) = E_L(u^d)$, where E_L is the minimal polynomial of ϖ^d over K_0.

(4.11) Proposition. *The functorial morphisms*

$$H^i(C^\bullet(M)) \xrightarrow{\sim} \mathrm{Ext}^i_{\mathrm{BT}_{\mathcal{O},\varphi}}(M(\underline{\mathcal{O}}), M) \longrightarrow H^i(K,T), \quad H^i(C^\bullet(\overline{M})) \xrightarrow{\sim} \mathrm{Ext}^i_{\mathrm{BT}_{\mathbf{F},\varphi}}(M(\underline{\mathbf{F}}), \overline{M}) \longrightarrow H^i(K,\overline{T})$$

$(i = 0, 1)$ from (2.7) and Proposition 2.9 are Δ-equivariant. They induce functorial isomorphisms

$$H^0(C^\bullet(M)^\Delta) = H^0(C^\bullet(M))^\Delta \xrightarrow{\sim} H^0(K,T)^\Delta, \qquad H^0(C^\bullet(\overline{M})^\Delta) = H^0(C^\bullet(\overline{M}))^\Delta \xrightarrow{\sim} H^0(K,\overline{T})^\Delta,$$
$$H^1(C^\bullet(M)^\Delta) = H^1(C^\bullet(M))^\Delta \xrightarrow{\sim} H^1_f(K,T)^\Delta, \qquad H^1(C^\bullet(\overline{M})^\Delta) = H^1(C^\bullet(\overline{M}))^\Delta \xrightarrow{\sim} \mathscr{F}.$$

Proof. The Δ-equivariance follows from the functoriality aspects of Propositions 2.5 and 2.9. The statement of this proposition can be reinterpreted as follows.

(4.12) Proposition. *There are functorial isomorphisms*

$$H^i(C^\bullet(M)^\Delta) \xrightarrow{\sim} \mathrm{Ext}^i_{(\mathrm{BT}_{\mathcal{O},\varphi})_{dd,K/L}}(M(\underline{\mathcal{O}}), M), \qquad H^i(C^\bullet(\overline{M})^\Delta) \xrightarrow{\sim} \mathrm{Ext}^i_{(\mathrm{BT}_{\mathbf{F},\varphi})_{dd,K/L}}(M(\underline{\mathbf{F}}), \overline{M})$$

$(i = 0, 1)$ compatible with those from (2.7) and Proposition 2.9 via the functor "forget the descent data".

Proof. As $p \nmid |\Delta|$, the splitting s in the proof of Proposition 2.5 can be chosen to be Δ-equivariant, which implies that $s(1) \in N^\Delta$ and $m_s = (\varphi_N - pE(u)/E(0))s(1) \in M^\Delta$, since $E(u) = E_L(u^d)$ is Δ-invariant.

(4.13) Proposition (The Euler characteristic formula). *Let $G \in (\mathbf{F} - \mathrm{vs}/O_K)_{dd,K/L}$, $M := M(G) \in (\mathrm{BT}_{\mathbf{F},\varphi})_{dd,K/L}$ and $C^\bullet(M)^\Delta := \left[\varphi_M - cu^e : M^\Delta \longrightarrow (M^\circ)^\Delta\right]$.*

(1) *There are functorial isomorphisms $H^i(C^\bullet(M)^\Delta) \xrightarrow{\sim} H^i_{fl}(O_K, G)^\Delta$.*

(2) *For every integer $n > e/(p-1)$ divisible by d the subcomplex $C^\bullet_n(M)^\Delta := \left[\varphi_M - cu^e : u^nM^\Delta \longrightarrow u^{n+e}M^\Delta\right] \subset C^\bullet(M)^\Delta$ is acyclic and $C^\bullet(M)^\Delta$ is quasi-isomorphic to*

$$C^\bullet(M)^\Delta / C^\bullet_n(M)^\Delta = \left[\varphi_M - cu^e : (M/u^nM)^\Delta \longrightarrow (M^\circ/u^{n+e}M)^\Delta\right].$$

(3) *The Euler characteristic $\chi_\mathbf{F}(O_L, G) := \dim_\mathbf{F} H^0_{fl}(O_K, G)^\Delta - \dim_\mathbf{F} H^1_{fl}(O_K, G)^\Delta$ is equal to*

$$\chi_\mathbf{F}(O_L, G) = \dim_\mathbf{F}(M/M^\circ)^\Delta - [L : \mathbf{Q}_p]\,\mathrm{rk}_\mathbf{F}(G).$$

Proof. (1) Combine (4.10.1) with Proposition 4.11. Part (2) is a direct consequence of Proposition 2.10(1). Part (3) follows from (2) as in the proof of Proposition 2.10(2):

$$-\chi_{\mathbf{F}}(O_L,G)+\dim_{\mathbf{F}}(M/M^\circ)^\Delta=\dim_{\mathbf{F}}(M/u^eM)^\Delta=ed^{-1}\dim_{\mathbf{F}}(M/u^dM)^\Delta.$$

For every integer $j\geq 0$ and every $i=0,\dots,d-1$, multiplication by u^i induces an isomorphism of $\mathbf{F}\otimes k$-modules

$$u^i:\left(u^jM/u^{j+1}M\right)^{(\eta^{-i})}:=\{x\in u^jM/u^{j+1}M\mid\forall\delta\in\Delta\quad[\delta](x)=(\mathrm{id}\otimes\eta(\delta)^{-i})(x)\}\simeq\left(u^{j+i}M/u^{j+i+1}M\right)^\Delta,$$

which implies that

$$\dim_{\mathbf{F}}(u^jM/u^{j+d}M)^\Delta=\sum_{i=0}^{d-1}\dim_{\mathbf{F}}\left(u^jM/u^{j+1}M\right)^{(\eta^{-i})}=\dim_{\mathbf{F}}(u^jM/u^{j+1}M)=[k:\mathbf{F}_p]\,\mathrm{rk}_{\mathbf{F}}(G)$$

and $ed^{-1}\dim_{\mathbf{F}}(M/u^dM)^\Delta=ed^{-1}[k:\mathbf{F}_p]\,\mathrm{rk}_{\mathbf{F}}(G)=[L:\mathbf{Q}_p]\,\mathrm{rk}_{\mathbf{F}}(G)$.

The referee pointed out that this argument shows that every Δ-eigenspace $M^{(\eta^{-i})}$ ($i\in\mathbf{Z}/d\mathbf{Z}$) is free of rank $\mathrm{rk}_{(\mathbf{F}\otimes k)[[u]]}(M)=\mathrm{rk}_{\mathbf{F}}(G)$ over $(\mathbf{F}\otimes k)[[u]]^\Delta=(\mathbf{F}\otimes k)[[u^d]]$.

(4.14) Corollary. *If $G,G'\in(\mathbf{F}-\mathrm{vs}/O_K)_{dd,K/L}$ have isomorphic generic fibres $G_K\xrightarrow{\sim}G'_K$ (as $\mathbf{F}$-vector space schemes over $\mathrm{Spec}(K)$ equipped with descent data relative to K/L, i.e., as $\mathbf{F}$-vector space schemes over $\mathrm{Spec}(L)$), then*

$$\dim_{\mathbf{F}}H^1_{fl}(O_K,G)^\Delta-\dim_{\mathbf{F}}H^1_{fl}(O_K,G')^\Delta=\dim_{\mathbf{F}}(M(G')/M(G')^\circ)^\Delta-\dim_{\mathbf{F}}(M(G)/M(G)^\circ)^\Delta.$$

(4.15) Under the asumptions of Corollary 4.14, a choice of an isomorphism $f:G_K\xrightarrow{\sim}G'_K$ induces a Δ-equivariant isomorphism $M(G)[1/u]\xrightarrow{\sim}M(G')[1/u]$ of étale φ-modules over $(\mathbf{F}\otimes k)((u))$. As in 2.12, the sum $M(G)+M(G')\subset M(G)[1/u]$ is an object of $(\mathrm{BT}_{\mathbf{F},\varphi})_{dd,K/L}$ corresponding to $H\in(\mathbf{F}-\mathrm{vs}/O_K)_{dd,K/L}$ equipped with morphisms $G\longrightarrow H\longleftarrow G'$ inducing isomorphisms $G_K\xrightarrow{\sim}H_K\xleftarrow{\sim}G'_K$ compatible with f.

(4.16) Proposition. *Assume that we are in the situation of 4.15.*
(1) *The sum of the canonical injective maps $\mathscr{F}=H^1_{fl}(O_K,G)^\Delta\longrightarrow H^1_{fl}(O_K,H)^\Delta\longleftarrow H^1_{fl}(O_K,G')^\Delta=\mathscr{F}'$ defines a surjection $\mathscr{F}\oplus\mathscr{F}'\longrightarrow H^1_{fl}(O_K,H)^\Delta$.*
(2) *$\mathscr{F}/(\mathscr{F}\cap\mathscr{F}')\xrightarrow{\sim}H^1_{fl}(O_K,H)^\Delta/\mathscr{F}'$, where the intersection takes place inside $H^1_{fl}(O_K,H)^\Delta$.*
(3) $\dim_{\mathbf{F}}\mathscr{F}/(\mathscr{F}\cap\mathscr{F}')=\dim_{\mathbf{F}}(M(G')/M(G')^\circ)^\Delta-\dim_{\mathbf{F}}(M(H)/M(H)^\circ)^\Delta$.

Proof. Taking Δ-invariants is exact, since $p\nmid|\Delta|$, so the claims (1) and (2) follow from Proposition 2.13. The statement (3) follows from (2) and Corollary 4.14.

(4.17) Decomposition of M (the case $k\hookrightarrow\mathbf{F}$). From now on until the end of §4 we assume that there exists an embedding $\sigma_0:k\hookrightarrow\mathbf{F}$. This condition is not very restrictive, since one can always replace $\mathbf{F}$ by a finite extension $\mathbf{F}'$, $\mathcal{O}$ by $\mathcal{O}'=\mathcal{O}\otimes_{W(\mathbf{F})}W(\mathbf{F}')$ and $G\in(\mathcal{O}-\mathrm{div}/O_K)_{dd,K/L}$ (resp. $G\in(\mathbf{F}-\mathrm{vs}/O_K)_{dd,K/L}$) by $\mathcal{O}'\otimes_{\mathcal{O}}G$ (resp. by $\mathbf{F}'\otimes_{\mathbf{F}}G$). As in (2.14.4), any $M\in(\mathrm{BT}_{\mathbf{F},\varphi})_{dd,K/L}$ decomposes as

$$M\xrightarrow{\sim}\bigoplus_{i\in\mathbf{Z}/f\mathbf{Z}}M_i,\quad M_i:=M\otimes_{\mathbf{F}\otimes k,\mathrm{id}\otimes\sigma_i}\mathbf{F},\quad\sigma_i:=\sigma_0\circ\varphi^i:k\hookrightarrow\mathbf{F},\quad\varphi_M|_{M_i}:M_i\longrightarrow M_{i-1},\qquad(4.17.1)$$

where M_i is a free $\mathbf{F}[[u]]$-module of rank $\mathrm{rk}_{\mathbf{F}}(M)$, for each $i\in\mathbf{Z}/f\mathbf{Z}$ ($f=[k:\mathbf{F}_p]$). The relation (4.8.4) implies that

$$\forall\delta\in\Delta\quad\forall A(u)\in\mathbf{F}[[u]]\quad\forall m\in M_i\qquad[\delta](A(u)m)=A(\eta_i(\delta)u)[\delta](m),\qquad(4.17.2)$$

where

$$\eta_i:=\sigma_i\circ\eta=\eta_{i-1}^p:\Delta\xrightarrow{\sim}\mu_d(\mathbf{F}).\qquad(4.17.3)$$

In particular, M_i is Δ-stable and M_i/uM_i is an $\mathbf{F}[\Delta]$-module, of dimension $\mathrm{rk}_{\mathbf{F}}(M)$ as an $\mathbf{F}$-vector space.

(4.18) Proposition-Definition. (1) *Every* $M \in (\mathrm{BT}_{\mathbf{F},\varphi})_{dd,K/L}$ *is of the form* $M = \bigoplus_\beta \mathbf{F}[[u]]m_\beta$, *where* $m_\beta \in M_{i(\beta)}$ *and, for all* $\delta \in \Delta$, $[\delta]m_\beta = \eta_{i(\beta)}(\delta)^{-a(\beta)}m_\beta$, $a(\beta) \in \{0,1,\dots,d-1\}$. *Such a basis* $\{m_\beta\}$ *will be called* **Δ-adapted**. *Define* $b(\beta) \in \{0,1,\dots,d-1\}$ *by* $b(\beta) \equiv p\,a(\beta) \pmod d$.
(2) *For each* $i \in \mathbf{Z}/f\mathbf{Z}$ *the class* $[M_i/uM_i] \in K_0(\mathbf{F}[\Delta])$ *is equal to* $\sum_{i(\beta)=i}[\eta_i^{-a(\beta)}]$.
(3) *For each* $i \in \mathbf{Z}/f\mathbf{Z}$ *the multisets* $\mathscr{A}_i(M) := \{a(\beta) \mid i(\beta) = i\}$ *and* $\mathscr{B}_i(M) := \{b(\beta) \mid i(\beta) = i\}$ *are independent of the chosen* Δ*-adapted basis. We define* $a_i(M) := \sum_{a\in\mathscr{A}_i(M)} a$ *and* $b_i(M) := \sum_{b\in\mathscr{B}_i(M)} b$.

Proof. We only need to prove (1). Fix $i \in \mathbf{Z}/f\mathbf{Z}$. There exists a basis $\{\overline{m}_\beta\}$ of M_i/uM_i over $\mathbf{F}$ on which Δ acts diagonally, by a morphism $D : \Delta \longrightarrow \prod_{\beta=1}^t \mathbf{F}^\times \subset GL_t(\mathbf{F})$, where $t = \dim_{\mathbf{F}} M_i/uM_i$. Choose representatives n_β in M_i of all $\overline{m}_\beta$; they form a basis of M_i over $\mathbf{F}[[u]]$. The action of Δ on $\{n_\beta\}$ is given by a 1-cocycle $A \in Z^1(\Delta, GL_t(\mathbf{F}[[u]]))$ such that $A \pmod u = D$. For $n \geq 1$ let $U_n = \mathrm{Ker}(GL_t(\mathbf{F}[[u]]) \longrightarrow GL_t(\mathbf{F}[[u]]/u^n))$. We have $A_1 = AD^{-1} \in Z^1(\Delta, U_1)$ for a new action of Δ on U_1, given by $\delta * B = D(\delta)\,[\delta](B)\,D(\delta)^{-1}$. As $U_1 = \varprojlim_n U_1/U_n$ and $H^1(\Delta, U_n/U_{n+1}) = H^1(\Delta, M_t(\mathbf{F})) = 0$ (since $p \nmid |\Delta|$), the cohomology set $H^1(\Delta, U_1)$ is trivial, which means that there exists $B \in U_1$ such that $A_1(\delta) = B^{-1}\,(\delta * B)$. After changing $\{n_\beta\}$ by the matrix B^{-1} we obtain a basis $\{m_\beta\}$ of M_i over $\mathbf{F}[[u]]$ on which Δ acts by D.

(4.19) The Frobenius matrix. Let $M \in (\mathrm{BT}_{\mathbf{F},\varphi})_{dd,K/L}$. The action of $\varphi = \varphi_M : M \longrightarrow M$ in any Δ-adapted basis $\{m_\beta\}$ of M can be written as

$$\varphi(m_\beta) = \sum_\alpha \Phi_{\alpha\beta}(u)\, m_\alpha, \tag{4.19.1}$$

where $i(\alpha) = i(\beta) - 1$ and $\Phi_{\alpha\beta}(u) \in \mathbf{F}[[u]]$. The formulas (4.8.3) and (4.17.2) then yield, for each $\delta \in \Delta$,

$$(\varphi \circ [\delta])m_\beta = \varphi(\eta_i(\delta)^{-a(\beta)}m_\beta) = \eta_i(\delta)^{-a(\beta)} \sum_\alpha \Phi_{\alpha\beta}(u)\, m_\alpha = ([\delta] \circ \varphi)m_\beta =$$
$$= \sum_\alpha [\delta](\Phi_{\alpha\beta}(u)\, m_\alpha) = \sum_\alpha \Phi_{\alpha\beta}(\eta_{i-1}(\delta)u)\,[\delta]m_\alpha = \sum_\alpha \Phi_{\alpha\beta}(\eta_{i-1}(\delta)u)\,\eta_{i-1}(\delta)^{-a(\alpha)}m_\alpha,$$

where $i = i(\beta) = i(\alpha) + 1$. This implies, thanks to (4.17.3), that

$$\forall \zeta \in \mu_d(\mathbf{F}) \qquad \Phi_{\alpha\beta}(\zeta u) = \zeta^{a(\alpha)-pa(\beta)}\Phi_{\alpha\beta}(u). \tag{4.19.2}$$

Recall that $b(\beta)$ was defined by the conditions

$$b(\beta) \equiv pa(\beta) \pmod d, \qquad 0 \leq b(\beta) < d; \tag{4.19.3}$$

we can rewrite (4.19.2) as

$$\widetilde{\Phi}_{\alpha\beta}(u) := u^{-a(\alpha)}\,\Phi_{\alpha\beta}(u)\,u^{b(\beta)} \in \mathbf{F}((u^d)). \tag{4.19.4}$$

By the definition of a Δ-adapted basis, M^Δ is a free $\mathbf{F}[[u^d]]$-module with basis $\{\widetilde{m}_\beta = u^{a(\beta)}m_\beta\}$. The formula (4.19.4) implies that

$$\mathbf{F}[[u]]\varphi(m_\beta) \cap M^\Delta = \mathbf{F}[[u^d]]u^{b(\beta)}\varphi(m_\beta),$$

hence $(M^\circ)^\Delta$ is the $\mathbf{F}[[u^d]]$-submodule of M^Δ (freely) generated by the elements

$$u^{b(\beta)}\varphi(m_\beta) = \sum_\alpha \widetilde{\Phi}_{\alpha\beta}(u)\,\widetilde{m}_\beta.$$

It follows that the matrix $\widetilde{\Phi}(u) := (\widetilde{\Phi}_{\alpha\beta}(u)) \in GL_r(\mathbf{F}((u^d)))$ lies in $M_r(\mathbf{F}[[u^d]])$ and that

$$\dim_{\mathbf{F}}(M/M^\circ)^\Delta = \mathrm{ord}_{u^d}(\det\widetilde{\Phi}(u)). \tag{4.19.5}$$

We can reformulate (4.19.4) in a matrix form as

$$\widetilde{\Phi} = A^{-1}\Phi B \in GL_r(\mathbf{F}((u^d))), \tag{4.19.6}$$

where A (resp. B) is the diagonal matrix with entries $A_{\beta\beta} = u^{a(\beta)}$ (resp. $B_{\beta\beta} = u^{b(\beta)}$). As in (2.15.2), these matrices have the following block form:

$$A = \begin{pmatrix} A_0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & A_{f-1} \end{pmatrix}, \qquad \Phi = \begin{pmatrix} 0 & \Phi_1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \Phi_{f-1} \\ \Phi_0 & 0 & \cdots & 0 \end{pmatrix} \tag{4.19.7}$$

(and similarly for B and $\widetilde{\Phi}$), where Φ_i is the matrix of $\varphi|_{M_i} : M_i \longrightarrow M_{i-1}$. The formulas (4.19.5-6) can then be refined as

$$\widetilde{\Phi}_i = A_{i-1}^{-1}\Phi_i B_i \tag{4.19.8}$$

and

$$\dim_{\mathbf{F}}(M_{i-1}/M_{i-1}^{\circ})^{\Delta} = \mathrm{ord}_{u^d}(\det \widetilde{\Phi}_i(u)) = \frac{r_i(M) + b_i(M) - a_{i-1}(M)}{d}, \tag{4.19.9}$$

where

$$r_i(M) := \mathrm{ord}_u(\det \Phi_i(u)) \equiv a_{i-1}(M) - b_i(M) \equiv a_{i-1}(M) - p\,a_i(M) \pmod{d}. \tag{4.19.10}$$

In (4.19.8)-(4.19.10) above we consider the index i as an element of $\mathbf{Z}/f\mathbf{Z}$.

The following result is a variant of Proposition 2.15. However, only the calculations from its proof (but not the statement itself) will be used in the proof of the general case of Theorem A.

(4.20) Proposition. *If $M, M' \in (\mathrm{BT}_{\mathbf{F},\varphi})_{dd,K/L}$ and if the corresponding étale φ-modules $M[1/u], M'[1/u]$ over $(\mathbf{F}\otimes k)((u)) \simeq \prod_{i\in\mathbf{Z}/f\mathbf{Z}} \mathbf{F}((u))$ are Δ-equivariantly isomorphic, then*

$$\dim_{\mathbf{F}}(M'/M'^{\circ})^{\Delta} - \dim_{\mathbf{F}}(M/M^{\circ})^{\Delta} \equiv \sum_{i\in\mathbf{Z}/f\mathbf{Z}} \left(\frac{b_i(M') - p\,a_i(M')}{d} - \frac{b_i(M) - p\,a_i(M)}{d} \right) \pmod{(p-1)}.$$

Proof. As in 4.19, choose Δ-adapted bases $\{m_\beta\}$ and $\{m'_{\beta'}\}$ of M and M', respectively. We obtain matrices $\Phi, A, B, \widetilde{\Phi}$ satisfying (4.19.1-8) and analogous matrices $\Phi', A', B', \widetilde{\Phi}'$ for M'. We have

$$\varphi(m'_{\beta'}) = \sum_{\alpha'} \Phi'_{\alpha'\beta'}(u)\, m'_{\alpha'}, \qquad m'_{\beta'} = \sum_{\beta} C_{\beta\beta'}(u)\, m_\beta,$$

where $C_{\beta\beta'}(u) \in \mathbf{F}((u))$ are the matrix elements of a matrix $C = C(u) = (C_{\beta\beta'}(u))$ representing an isomorphism of étale φ-modules $M[1/u] \xrightarrow{\sim} M'[1/u]$. Note that $i(\beta') = i(\beta)$ whenever $C_{\beta\beta'}(u) \neq 0$. Applying $[\delta]$ ($\delta \in \Delta$) to the identities above and using (4.8.3) and (4.17.2), we obtain

$$\sum_{\beta} C_{\beta\beta'}(\eta_i(\delta)u)\,\eta_i(\delta)^{-a(\beta)} m_\beta = [\delta]m'_{\beta'} = \eta_i(\delta)^{-a(\beta')} m'_{\beta'} = \sum_{\beta} \eta_i(\delta)^{-a(\beta')} C_{\beta\beta'}(u)\, m_\beta,$$

where $i = i(\beta') = i(\beta)$, hence

$$u^{-a(\beta)}\, C_{\beta\beta'}(u)\, u^{a(\beta')} \in \mathbf{F}((u^d)),$$

which can be restated in a matrix form as

$$\widetilde{C}(u) := A^{-1}C(u)A' \in GL_r(\mathbf{F}((u^d))). \tag{4.20.1}$$

As in (2.15.3) we have $\Phi' = C^{-1}\,\Phi\,\varphi(C) = C(u)^{-1}\,\Phi\,C(u^p)$, which can be rewritten, using the matrices $U(u^d) := A(u^p)^{-1}B(u)$, $U'(u^d) := A'(u^p)^{-1}B'(u) \in GL_r(\mathbf{F}((u^d)))$ and (4.19.6), as

$$\widetilde{\Phi}' = \widetilde{C}(u)^{-1}\,\widetilde{\Phi}\,U(u^d)^{-1}\,\widetilde{C}(u^p)\,U'(u^d).$$

Combined with (4.19.5) this yields

$$\dim_{\mathbf{F}}(M'/M'^{\circ})^{\Delta} - \dim_{\mathbf{F}}(M/M^{\circ})^{\Delta} = (p-1)\,\mathrm{ord}_{u^d}(\det\widetilde{C}(u)) + \mathrm{ord}_{u^d}\left(\frac{\det(U'(u^d))}{\det(U(u^d))}\right),$$

which proves the claim, since the first term on the right hand side is divisible by $p-1$ and

$$\mathrm{ord}_u(\det(U(u^d))) = \sum_{i\in\mathbf{Z}/f\mathbf{Z}} (b_i(M) - p\,a_i(M)).$$

(4.21) Proposition (The Euler characteristic formula). *If $M \in (\mathrm{BT}_{\mathbf{F},\varphi})_{dd,K/L}$, then $\chi_{\mathbf{F}}(M) = \dim_{\mathbf{F}} H^0(C^{\bullet}(M)^{\Delta}) - \dim_{\mathbf{F}} H^1(C^{\bullet}(M)^{\Delta})$ is equal to*

$$\chi_{\mathbf{F}}(M) = \left(\sum_{i\in\mathbf{Z}/f\mathbf{Z}} \frac{r_i(M) + b_i(M) - a_{i-1}(M)}{d}\right) - \frac{ef}{d}\,\mathrm{rk}_{\mathbf{F}}(M),$$

in the notation of 4.18 and 4.19.

Proof. Combine Proposition 4.13(3) with (4.19.9).

(4.22) Definition. *We say that $M \in (\mathrm{BT}_{\mathbf{F},\varphi})_{dd,K/L}$ is* **Δ-balanced** *if the $\mathbf{F}[\Delta]$-modules M_i/uM_i ($i \in \mathbf{Z}/f\mathbf{Z}$) are all isomorphic (which is equivalent to the class $[M_i/uM_i] \in K_0(\mathbf{F}[\Delta])$ being independent of i).*

(4.23) Proposition. (1) *$M \in (\mathrm{BT}_{\mathbf{F},\varphi})_{dd,K/L}$ is Δ-balanced if and only if $\mathscr{A}_{i-1}(M) = \mathscr{B}_i(M)$ for all $i \in \mathbf{Z}/f\mathbf{Z}$.*
(2) *If $M \in (\mathrm{BT}_{\mathbf{F},\varphi})_{dd,K/L}$ is Δ-balanced, then*

$$\sum_{i\in\mathbf{Z}/f\mathbf{Z}} \frac{p\,a_i(M) - b_i(M)}{d} = \frac{p-1}{d}\sum_{i\in\mathbf{Z}/f\mathbf{Z}} a_i(M) \equiv \frac{p^f-1}{d}\,a_{i_0}(M) \pmod{(p-1)},$$

for any $i_0 \in \mathbf{Z}/f\mathbf{Z}$.
(3) *If $N \in (\mathrm{BT}_{\mathcal{O},\varphi})_{dd,K/L}$, then $M = N/\pi N \in (\mathrm{BT}_{\mathbf{F},\varphi})_{dd,K/L}$ is Δ-balanced. More precisely, $N = M(G)$ for some $G \in (\mathcal{O}-\mathrm{div}/O_K)_{dd,K/L}$ and $[M_i/uM_i]$ corresponds to $[(N_i/uN_i)[1/p]] = [WD((V_\pi G)(-1))|_\Delta] = [WD((V_\pi G))|_\Delta] \in K_0(\mathcal{K}[\Delta])$ under the canonical isomorphism $K_0(\mathbf{F}[\Delta]) \simeq K_0(\mathcal{K}[\Delta])$.*

Proof. (1) According to Proposition 4.18(2) and (4.17.3), $[M_i/uM_i] = \sum_{a\in\mathscr{A}_i(M)}[\eta_i^{-a}] = \sum_{a\in\mathscr{A}_i(M)}[\eta_{i-1}^{-pa}] = \sum_{b\in\mathscr{B}_i(M)}[\eta_{i-1}^{-b}]$, which implies that $[M_i/uM_i] = [M_{i-1}/uM_{i-1}]$ is equivalent to $\mathscr{A}_{i-1}(M) = \mathscr{B}_i(M)$.
(2) It follows from (1) that $\sum_i b_i(M) = \sum_i a_i(M)$ and $a_i(M) \equiv pa_{i+1}(M) \pmod d$, hence $\sum_i a_i(M) \equiv (1+p+\cdots+p^{f-1})a_{i_0}(M) \pmod d$.
(3) We have $[M_i/uM_i] = [(N_i/uN_i)[1/p]]$, by the definition of the isomorphism $K_0(\mathbf{F}[\Delta]) \simeq K_0(\mathcal{K}[\Delta])$ [Se1, §15.5]. The equality $[(N_i/uN_i)[1/p]] = [WD((V_\pi G)(-1))|_\Delta]$ follows from (4.9.3).

(4.24) Proposition-Definition (Cartier duality). (1) *For $M \in (\mathrm{BT}_{\mathcal{O},\varphi})_{dd,K/L}$ we define its dual $M^D \in (\mathrm{BT}_{\mathcal{O},\varphi})_{dd,K/L}$ as follows. As an $(\mathcal{O}\otimes_{\mathbf{Z}_p} W)[[u]]$-module, $M^D := \mathrm{Hom}_{(\mathcal{O}\otimes_{\mathbf{Z}_p}W)[[u]]}(M, (\mathcal{O}\otimes_{\mathbf{Z}_p}W)[[u]])$, and we require the tautological pairing $\langle\ ,\ \rangle : M^D \times M \longrightarrow (\mathcal{O}\otimes_{\mathbf{Z}_p}W)[[u]]$ to be Δ-equivariant and satisfy*

$$\langle\varphi(m^D), \varphi(m)\rangle = (pE(u)/E(0))\,\varphi(\langle m^D, m\rangle),$$

where φ on $(\mathcal{O}\otimes_{\mathbf{Z}_p}W)[[u]]$ is given by $\varphi(1) = 1$.
(2) *There exist functorial isomorphisms $M(G)^D \xrightarrow{\sim} M(G^D)$, for all $G \in (\mathcal{O}-\mathrm{div}/O_K)_{dd,K/L}$.*
(3) *If $G \in (\mathcal{O}-\mathrm{div}/O_K)_{dd,K/L}$ and if $T := T_\pi G$ is equipped with an isomorphism of $\mathcal{O}[\Gamma_L]$-modules $j : T \xrightarrow{\sim} T^*(1) = \mathrm{Hom}_{\mathcal{O}}(T, \mathcal{O})(1)$, then j is induced by a unique isomorphism $j_G : G \xrightarrow{\sim} G^D$ in $(\mathcal{O}-\mathrm{div}/O_K)_{dd,K/L}$,*

which in turn gives rise to a perfect Δ*-equivariant* $(\mathcal{O}\otimes_{\mathbf{Z}_p} W)[[u]]$*-bilinear pairing* $(\ ,\ ): M(G)\times M(G)\longrightarrow (\mathcal{O}\otimes_{\mathbf{Z}_p} W)[[u]]$ *defined by* $(x,y)=\langle j_G(x), y\rangle$*. This pairing satisfies*

$$(\varphi(m),\varphi(m')) = (pE(u)/E(0))\,\varphi((m,m')).$$

If, in addition, j *is skew-symmetric (i.e.,* $j^*=-j$*), then* $j_G^D=-j_G$ *and* $(\ ,\ )$ *is skew-symmetric, too.*
(4) *For* $M\in(\mathrm{BT}_{\mathbf{F},\varphi})_{dd,K/L}$ *we define its dual* $M^D\in(\mathrm{BT}_{\mathbf{F},\varphi})_{dd,K/L}$ *as follows: as an* $(\mathbf{F}\otimes k)[[u]]$*-module,* $M^D:=\mathrm{Hom}_{(\mathbf{F}\otimes k)[[u]]}(M,(\mathbf{F}\otimes k)[[u]])$*, with the tautological pairing* $\langle\ ,\ \rangle: M^D\times M\longrightarrow(\mathbf{F}\otimes k)[[u]]$ *being* Δ*-equivariant and satisfying*

$$\langle\varphi(m^D),\varphi(m)\rangle = cu^e\,\varphi(\langle m^D,m\rangle),$$

where $c\in k^\times$ *is as in Proposition 2.9.*
(5) *There exist functorial isomorphisms* $M(H)^D\xrightarrow{\sim} M(H^D)$*, for all* $H\in(\mathbf{F}-\mathrm{vs}/O_K)_{dd,K/L}$.

Proof. (1) Firstly, we must check that the formula for $\langle\varphi(m^D),\varphi(m)\rangle$ does, indeed, define a map $\varphi: M^D\longrightarrow M^D$ (which is then unique). If $m\in M$, then we can write $(pE(u)/E(0))m=\sum_{i=1}^n f_i\,\varphi(m_i)$, $f_i\in(\mathcal{O}\otimes_{\mathbf{Z}_p}W)[[u]]$ and $m_i\in M$, which implies that

$$\langle\varphi(m^D),m\rangle=\sum_{i=1}^n f_i\,\varphi(\langle m^D,m_i\rangle),$$

which proves the claim. Secondly, we must check that, for each $m^D\in M^D$, there exist finitely many elements $g_l\in(\mathcal{O}\otimes_{\mathbf{Z}_p}W)[[u]]$ and $m_l^D\in M^D$ such that $(pE(u)/E(0))m^D=\sum_l g_l\,\varphi(m_l^D)$. This equality is equivalent to

$$\forall m\in M\qquad \langle(pE(u)/E(0))m^D,\varphi(m)\rangle=\sum_l g_l\,\langle\varphi(m_l^D),\varphi(m)\rangle,$$

hence to

$$\forall m\in M\qquad \langle m^D,\varphi(m)\rangle=\sum_l g_l\,\varphi(\langle m_l^D,m\rangle).$$

Fix a basis $\{e_i\}$ of M over $(\mathcal{O}\otimes_{\mathbf{Z}_p}W)[[u]]$; let $\{e_i^D\}$ be the dual basis of M^D. It is enough to treat the case $m^D=e_i^D$. If we write $\varphi(e_j)=\sum_l f_{jl}\,e_l$ ($f_{jl}\in(\mathcal{O}\otimes_{\mathbf{Z}_p}W)[[u]]$), then

$$\forall m\in M\qquad \langle e_i^D,\varphi(m)\rangle=\sum_l f_{li}\,\varphi(\langle e_l^D,m\rangle),$$

as required. This finishes the proof that M^D is a well-defined object of $(\mathrm{BT}_{\mathcal{O},\varphi})_{dd,K/L}$.
(2) Write $M=M(G)$ and $M^D=M(G')$, for $G,G'\in(\mathcal{O}-\mathrm{div}/O_K)_{dd,K/L}$. We need to exhibit a functorial isomorphism between G' and G^D.

Note that the perfect pairing in (1) can be written in a more canonical φ-equivariant form as

$$\langle\ ,\ \rangle: M^D\times M\longrightarrow M(\underline{\mathbf{Z}}_p),$$

since $M(\underline{\mathbf{Z}}_p)=W[[u]](-1)$, $\varphi(1)=pE(u)/E(0)$ and $M(\mu_{p^\infty})=W[[u]]$, $\varphi(1)=1$.

It follows from (4.9.2) and the fact that D_{cris} and D_{dR} are tensor functors that $\langle\ ,\ \rangle$ induces a perfect pairing

$$D_{cris}((V_\pi G')(-1)|_{\Gamma_K})\otimes_{\mathcal{O}\otimes_{\mathbf{Z}_p}W} D_{cris}((V_\pi G)(-1)|_{\Gamma_K})\longrightarrow D_{cris}(\mathcal{K}(-1)|_{\Gamma_K})$$

of filtered (φ,Δ)-modules with coefficients in $\mathcal{K}\otimes_{\mathbf{Q}_p}K_0$, hence a perfect pairing of $\mathcal{K}[\Gamma_L]$-modules

$$(V_\pi G')(-1)\otimes_{\mathcal{K}}(V_\pi G)(-1)\longrightarrow\mathcal{K}(-1).$$

Similarly, (4.9.1) implies that $\langle\ ,\ \rangle$ induces a perfect pairing

$$(T_\pi G')(-1)|_{\Gamma_{L_\infty}} \otimes_{\mathcal{O}} (T_\pi G)(-1)|_{\Gamma_{L_\infty}} \longrightarrow \mathcal{O}(-1)$$

of $\mathcal{O}[\Gamma_{L_\infty}]$-modules, compatible with the previous pairing. As a result, it induces an isomorphism of $\mathcal{O}[\Gamma_L]$-modules

$$T_\pi G' \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{O}[\Gamma_L]}(T_\pi(G), \mathcal{O}(1)) = T_\pi(G^D).$$

Tate's full faithfulness theorem implies that this isomorphism is induced by a (unique) isomorphism $G' \xrightarrow{\sim} G^D$ in $(\mathcal{O} - \mathrm{div}/O_K)_{dd,K/L}$, which yields an isomorphism $M(G)^D \xrightarrow{\sim} M(G^D)$, functorial by construction.
(3) The existence and uniqueness of j_G follow from Tate's full faithfulness theorem. The remaining statements are direct consequences of (1) and (2).
(4) The same arguments as in (1) show that M^D is a well-defined object of $(\mathrm{BT}_{\mathbf{F},\varphi})_{dd,K/L}$.
(5) There exist $G \in (\mathrm{BT}_{\mathcal{O},\varphi})_{dd,K/L}$ and an exact sequence $0 \longrightarrow H \longrightarrow G[\pi]$. Denote by $G' \in (\mathrm{BT}_{\mathcal{O},\varphi})_{dd,K/L}$ the quotient of G by H: there exists a morphism $\beta : G \longrightarrow G'$ which induces an exact sequence of group schemes

$$0 \longrightarrow H \longrightarrow G[\pi^n] \longrightarrow G'[\pi^n]$$

and an exact sequence of $\mathcal{O}[\Gamma_L]$-modules

$$0 \longrightarrow T_\pi(G) \longrightarrow T_\pi(G') \longrightarrow H(\overline{L}) \longrightarrow 0.$$

In order to ease the notation we are going to write $R := (\mathcal{O} \otimes_{\mathbf{Z}_p} W)[[u]]$.

It follows from [K1, §2.3] that the exact sequence

$$0 \longrightarrow M(H) \longrightarrow M(G[\pi]) \xrightarrow{M(\beta_1)} M(G'[\pi])$$

can also be obtained by applying the snake lemma to the multiplication by π on the exact sequence of R-modules (equipped with actions of φ and Δ)

$$0 \longrightarrow M(G) \xrightarrow{M(\beta)} M(G') \longrightarrow M(H) \longrightarrow 0.$$

After applying $\mathbf{R}\mathrm{Hom}_R(-, R)$ to the latter sequence, we get exact sequences

$$0 \longrightarrow M(G')^D \longrightarrow M(G)^D \longrightarrow N \longrightarrow 0$$

and (via the snake lemma, as before)

$$0 \longrightarrow N \longrightarrow M(G')^D/\pi M(G')^D \longrightarrow M(G)^D/\pi M(G)^D,$$

the second of which is isomorphic, thanks to (2), to

$$0 \longrightarrow N \longrightarrow M(G'[\pi]^D) \xrightarrow{M(\beta_1^D)} M(G[\pi]^D).$$

However,

$$N = \mathrm{Ext}^1_R(M(H), R) \xrightarrow{\sim} \mathrm{Hom}_R(M(H), R/\pi) = M(H)^D$$

and all of the maps above are compatible with the actions of φ and Δ, which implies that

$$M(H)^D \xrightarrow{\sim} M(\mathrm{Ker}(G'[\pi]^D \xrightarrow{\beta_1^D} G[\pi]^D)) = M(H^D),$$

as claimed (this isomorphism is functorial, by construction).

(4.25) Proposition. *If $M \in (\mathrm{BT}_{\mathbf{F},\varphi})_{dd,K/L}$ and if $M \oplus M^D$ is Δ-balanced, then:*
(1) $\sum_{i=0}^{f-1}(a_i(M) - b_{i+1}(M))\,p^i \equiv 0 \pmod{2d}$.
(2) $\chi_{\mathbf{F}}(M) \equiv \frac{1}{d}\sum_{i=0}^{f-1}(r_{i+1}(M) - e\,\mathrm{rk}_{\mathbf{F}}(M))\,p^i \pmod 2$.

Proof. (1) For each $i \in \mathbf{Z}/f\mathbf{Z}$ consider the following multisets: $\mathscr{A}_i^*(M) = \{a \in \mathscr{A}_i(M) \mid a \neq 0\}$, $\mathscr{B}_i^*(M) = \{b \in \mathscr{B}_i(M) \mid b \neq 0\}$, $\mathscr{A}_i(M^D) = \mathscr{A}_i(M)_- = \{a_- \mid a \in \mathscr{A}_i(M)\}$, $\mathscr{B}_i(M^D) = \mathscr{B}_i(M)_- = \{b_- \mid b \in \mathscr{B}_i(M)\}$, where $a_- = d - a$ if $a \neq 0$ (resp. $a_- = 0$ if $a = 0$).

According to Proposition 4.23, the assumption that $M \oplus M^D$ is Δ-balanced is equivalent to an equality of multisets

$$\forall i \in \mathbf{Z}/f\mathbf{Z} \qquad \mathscr{A}_i(M \oplus M^D) = \mathscr{A}_i(M) \,\dot\cup\, \mathscr{A}_i(M)_- = \mathscr{B}_{i+1}(M \oplus M^D) = \mathscr{B}_{i+1}(M) \,\dot\cup\, \mathscr{B}_{i+1}(M)_-,$$

which is, in turn, equivalent to

$$\forall i \in \mathbf{Z}/f\mathbf{Z} \qquad \mathscr{A}_i^*(M) \,\dot\cup\, \mathscr{A}_i^*(M)_- = \mathscr{B}_{i+1}^*(M) \,\dot\cup\, \mathscr{B}_{i+1}^*(M)_-.$$

It follows that there exist bijections

$$\mathscr{A}_0^*(M) \xrightarrow{\sim} \mathscr{A}_i^*(M), \qquad a \mapsto a[i]$$

and signs $\lambda(a,i) \in \{\pm 1\}$ ($a \in \mathscr{A}_0^*(M)$, $i \in \mathbf{Z}/f\mathbf{Z}$) such that

$$p^i\,a[i] \equiv \lambda(a,i)\,a \pmod d.$$

If we let $\mu(a,i) = \lambda(a,i+1)\lambda(a,i)^{-1} \in \{\pm 1\}$ and

$$b_a[i+1] = \begin{cases} a[i] & a \in \mathscr{A}_0^*(M),\ \mu(a,i) = 1, \\ d - a[i] & a \in \mathscr{A}_0^*(M),\ \mu(a,i) = -1, \end{cases}$$

then

$$\mathscr{B}_{i+1}^*(M) = \{b_a[i+1] \mid a \in \mathscr{A}_0^*(M)\}.$$

Fix $a \in \mathscr{A}_0^*(M)$. The equality $\prod_{i \in \mathbf{Z}/f\mathbf{Z}} \mu(a,i) = 1$ implies that

$$\sum_{\substack{i \in \mathbf{Z}/f\mathbf{Z} \\ \mu(a,i) = -1}} a[i]\,p^i \equiv a \sum_{\substack{i \in \mathbf{Z}/f\mathbf{Z} \\ \mu(a,i) = -1}} \lambda(a,i) \equiv 0 \pmod d,$$

hence

$$\sum_{i \in \mathbf{Z}/f\mathbf{Z}} (a[i] - b_a[i+1])\,p^i \equiv \sum_{\substack{i \in \mathbf{Z}/f\mathbf{Z} \\ \mu(a,i) = -1}} (2a[i] - d)\,p^i \equiv d \sum_{\substack{i \in \mathbf{Z}/f\mathbf{Z} \\ \mu(a,i) = -1}} 1 \equiv 0 \pmod{2d}.$$

Taking the sum over all $a \in \mathscr{A}_0^*(M)$ yields (1).
(2) Write $r_{i+1}(M) = a_i(M) - b_{i+1}(M) + dt_i$ ($t_i \in \mathbf{Z}$), for all $i \in \mathbf{Z}/f\mathbf{Z}$. We have just proved that

$$0 \equiv \sum_{i=0}^{f-1}(r_{i+1}(M) - dt_i)\,p^i \equiv \sum_{i=0}^{f-1} r_{i+1}(M)\,p^i + d\sum_{i=0}^{f-1} t_i \pmod{2d},$$

which implies, thanks to Proposition 4.21, that

$$\chi_{\mathbf{F}}(M) = \sum_{i=0}^{f-1}(t_i - e\,\mathrm{rk}_{\mathbf{F}}(M)/d) \equiv \frac{1}{d}\sum_{i=0}^{f-1}(r_{i+1}(M) - e\,\mathrm{rk}_{\mathbf{F}}(M))\,p^i \pmod 2.$$

(4.26) Proposition (The inertia character, [NY, Cor. 5.7]). *If $M = M(G) \in (\mathrm{BT}_{\mathbf{F},\varphi})_{dd,K/L}$ for $G \in (\mathbf{F} - \mathrm{vs}/O_K)_{dd,K/L}$, then the action of I_L on $T = \wedge^{\mathrm{rk}_{\mathbf{F}}(G)} G_L(\overline{K})$ is given by the character*

$$\det_{G_L} : I_L \longrightarrow \mathbf{F}^\times, \qquad \forall \lambda \in \mu_{p^f-1}(O_L) = \mu_{p^f-1}(k) \qquad \det_{G_L}(\mathrm{rec}_L(\lambda)) = \sigma_0(\lambda)^{-\frac{p^f-1}{d}\, a_0(M) - y_0},$$

where $y_0 = \frac{1}{d}\sum_{i=0}^{f-1}(r_{i+1}(M) - e\,\mathrm{rk}_{\mathbf{F}}(G))\,p^i$. In particular,

$$\det_{G_L}(\mathrm{rec}_L(-1)) = (-1)^{\frac{p^f-1}{d}\, a_0(M)}(-1)^{y_0}.$$

Proof. If $\mathrm{rk}_{\mathbf{F}}(G) = 1$, this is a special case of [NY, Cor. 5.7], which generalises a result of Savitt [Sav2, Cor. 2.6], which is, in turn, a generalisation – in the case of finite extensions of $\mathbf{Q}_p$ – of an earlier result of Raynaud [R, Thm. 3.4.1]. However, the notation and conventions of [NY] differ from ours, which is why we repeat the details of the calculation in our context.

The character $\psi = \det_{G_L}$ is tame; its composition with $\mathrm{rec}_L : O_L^\times \longrightarrow \mathrm{Im}(I_L \longrightarrow \Gamma_L^{ab})$ factors through $O_L^\times \longrightarrow k^\times = \mu_{p^f-1}(k)$. It is sufficient to describe the action of I_{L_∞} on the Tate twist

$$T(-\mathrm{rk}_{\mathbf{F}}(G))|_{\Gamma_{L_\infty}} = \left(N^\Delta \otimes_{(\mathbf{F}\otimes k)[[u^d]]} (\mathbf{F} \otimes k_{\widehat{\mathcal{E}}^{ur}})\right)^{\varphi=\mathrm{id}}, \tag{4.26.1}$$

where $k_{\widehat{\mathcal{E}}^{ur}} \simeq k((u^d))^{sep}$ and $N := \wedge^{\mathrm{rk}_{\mathbf{F}}(G)} M(G)[1/u]$. The calculations in 4.19 imply that $N = \bigoplus_{i\in\mathbf{Z}/f\mathbf{Z}} N_i$, where $N_i = \mathbf{F}((u))\,n_i'$ and n_i' is the wedge product of all m_β such that $i(\beta) = i$. The action of $\delta \in \Delta$ is given by $[\delta]n_i' = \eta_i(\delta)^{-a_i(M)} n_i'$ and the Frobenius acts as $\varphi(n_i') = u^{r_i(M)} A_i(u^d)\, n_{i-1}'$ for some $A_i(u^d) \in \mathbf{F}[[u^d]]$ such that $A_i(0) \neq 0$.

There exist power series $B_i(u^d) \in 1 + u^d\mathbf{F}[[u^d]]$ such that the new basis elements $n_i = B_i(u^d)n_i'$ of the N_i satisfy (cf. [Sav2, Thm. 3.5], [NY, Thm. 5.5])

$$\varphi(n_i) = c_{i-1} u^{r_i(M)} n_{i-1}$$

for some $c_{i-1} = A_i(u^d)B_i(u^{pd})B_{i-1}(u^d)^{-1} \in \mathbf{F}^\times$ (this follows from the fact that the map

$$1 + u^d\mathbf{F}[[u^d]] \longrightarrow 1 + u^d\mathbf{F}[[u^d]], \qquad B(u^d) \mapsto B(u^{p^f d})/B(u^d)$$

is surjective). As a result, $N^\Delta = \bigoplus_{i\in\mathbf{Z}/f\mathbf{Z}} \mathbf{F}((u^d))\widetilde{n}_i$, where $\widetilde{n}_i = u^{a_i(M)} n_i$ and

$$\varphi(\widetilde{n}_i) = c_{i-1} u^{s_i} \widetilde{n}_{i-1}, \qquad s_i = pa_i(M) + r_i(M) - a_{i-1}(M) \in d\mathbf{Z}.$$

As explained in [NY, Lemma 5.6], there exist $\alpha_i \in \overline{k}^\times$ such that $\alpha_i^p c_{i-1} = \alpha_{i-1}$ for all $i \in \mathbf{Z}/f\mathbf{Z}$.

We are looking for integers $x_i \in \mathbf{Z}$ ($i \in \mathbf{Z}/f\mathbf{Z}$) for which the elements $\beta_i = ((u^d)^{1/(p^f-1)})^{x_i} \in \mathbf{F}((u^d))^{sep}$ satisfy

$$\forall i \in \mathbf{Z}/f\mathbf{Z} \qquad \varphi(\alpha_i\beta_i\widetilde{n}_i) = \alpha_{i-1}\beta_{i-1}\widetilde{n}_{i-1},$$

which is equivalent to

$$\forall i \in \mathbf{Z}/f\mathbf{Z} \qquad \frac{p^f-1}{d}\, s_i = x_{i-1} - px_i. \tag{4.26.2}$$

If these relations are satisfied, then (4.26.1) implies that $T|_{\Gamma_{L_\infty}} = \mathbf{F}\cdot\alpha\beta\widetilde{n}$, where $\alpha\beta\widetilde{n} = (\alpha_i\beta_i\widetilde{n}_i)_i$. The solution of the system (4.26.2) is given by

$$-x_0 = \sum_{i=0}^{f-1} \frac{s_{i+1}}{d}\, p^i = \sum_{i=0}^{f-1} \frac{r_{i+1}(M)}{d}\, p^i + \frac{p^f-1}{d}\, a_0(M), \qquad x_{i-1} = \frac{p^f-1}{d}\, s_i + px_i.$$

For $g \in \Gamma_{L_\infty}$ and $p \nmid m$, the actions of g on $\varpi_L^{1/m} = (\varpi^d)^{1/m}$ and $(u^d)^{1/m}$ are compatible as follows ([NY, §5.1]): $g(\varpi_L^{1/m})/\varpi_L^{1/m} = g((u^d)^{1/m})/(u^d)^{1/m}$.

On the other hand, $\mathrm{rec}_L(\lambda)(\varpi_L^{1/(p^f-1)})/\varpi_L^{1/(p^f-1)} = \lambda$ for all $\lambda \in \mu_{p^f-1}(O_L)$, by [Se3, §1.5, Prop. 3] (with a sign change, due to our normalisation of the reciprocity map). Putting everything together, we deduce that I_L acts on (4.26.1) by the character

$$\mathrm{rec}_L(\lambda)(\alpha\beta\widetilde{n})/\alpha\beta\widetilde{n} = (\mathrm{rec}_L(\lambda)(\beta_i)/\beta_i)_i = (\sigma_i(\lambda)^{x_i})_i \in \mathbf{F}^\times \subset (\mathbf{F}\otimes\overline{k})^\times$$

(note that $\sigma_i(\lambda)^{x_i} = \sigma_0(\lambda)^{x_0}$). As it acts on $\mathbf{F}(1)$ by the character $\mathrm{rec}_L(\lambda) \mapsto \lambda^z$, where $z = e(1+p+\cdots+p^{f-1})/d$, the statement of the proposition follows from the fact that $x_0 + z\,\mathrm{rk}_{\mathbf{F}}(G) = -y_0 - (p^f-1)a_0(M)/d$.

(4.27) The reader may be puzzled by the fact that the right hand side of the formula for $\det_{G_L}(\mathrm{rec}_L(\lambda))$ in Proposition 4.26 seemingly depends on the choice of $\sigma_0 : k \hookrightarrow \mathbf{F}$. However, this is not the case. Indeed, if we replace σ_0 by $\sigma_0^{new} = \sigma_1 = \sigma_0\circ\varphi$, then $\sigma_0^{new}(\lambda) = \sigma_0(\lambda)^p$ and $\eta_i^{new} = \eta_{i+1} = \eta_i^p$, which implies that $a_i^{new}(M) = a_{i+1}(M)$ and $r_i^{new}(M) = r_{i+1}(M)$. Therefore

$$p\,y_0^{new} = \frac{1}{d}\sum_{i=0}^{f-1}(r_{i+2}(M) - e\,\mathrm{rk}_{\mathbf{F}}(G))\,p^{i+1} = \frac{1}{d}\sum_{j=1}^{f}(r_{j+1}(M) - e\,\mathrm{rk}_{\mathbf{F}}(G))\,p^j = y_0 + \frac{p^f-1}{d}(r_1(M) - e\,\mathrm{rk}_{\mathbf{F}}(G)).$$

After multiplying the congruence

$$pa_1(M) + (r_1(M) - e\,\mathrm{rk}_{\mathbf{F}}(G)) \equiv a_0(M) \pmod{d}$$

by $(p^f-1)/d$, we obtain

$$p\left(\frac{p^f-1}{d}a_0^{new}(M) + y_0^{new}\right) \equiv \frac{p^f-1}{d}a_0(M) + y_0 \pmod{(p^f-1)},$$

which implies that

$$\forall\lambda \in \mu_{p^f-1}(O_L) \qquad \sigma_0^{new}(\lambda)^{\frac{p^f-1}{d}\,a_0^{new}(M)+y_0^{new}} = \sigma_0(\lambda)^{\frac{p^f-1}{d}\,a_0(M)+y_0}.$$

(4.28) Proposition. *Let $H \in (\mathbf{F}-\mathrm{vs}/O_K)_{dd,K/L}$, $M = M(H) \in (\mathrm{BT}_{\mathbf{F},\varphi})_{dd,K/L}$. If $M\oplus M^D$ is Δ-balanced, then*

$$\det_{H_L}(\mathrm{rec}_L(-1)) = (-1)^{\frac{p^f-1}{d}\,a_0(M)}(-1)^{\chi_{\mathbf{F}}(O_L,H)} = ((\eta\circ\mathrm{rec}_L)(-1))^{a_0(M)}\,(-1)^{\chi_{\mathbf{F}}(O_L,H)}.$$

Proof. Combine Proposition 4.26 with Proposition 4.25(2), Proposition 4.13(1) and (4.7.2).

(4.29) Proposition. *Let $G \in (\mathcal{O}-\mathrm{div}/O_K)_{dd,K/L}$. If there exists a skew-symmetric isomorphism $G \simeq G^D$ and an exact sequence $0 \longrightarrow H \longrightarrow G[\pi] \longrightarrow H^D \longrightarrow 0$ in $(\mathbf{F}-\mathrm{vs}/O_K)_{dd,K/L}$, then*

$$(-1)^{\chi_{\mathbf{F}}(O_L,H)} = \det_{H_L}(\mathrm{rec}_L(-1))\;\varepsilon(V_\pi G).$$

Proof. If $[M(H)_0/uM(H)_0] = \sum_{j=0}^d c_j[\eta_0^{-j}] \in K_0(\mathbf{F}[\Delta])$ ($c_j \in \mathbf{N}$), then $a_0(M(H)) = \sum_j jc_j$ and the class $[WD(V_\pi G)|_{I_L}] \in K_0(\mathcal{K}[\Delta]_{Sp}) \simeq K_0(\mathbf{F}[\Delta]_{Sp})$ is equal to $[M(G[\pi])_0/uM(G[\pi])_0] = \sum_{j=0}^d c_j([\eta_0^{-j}] + [\eta_0^j])$, by Proposition 4.23(3). The formula (5.5.1) from the proof of Theorem 5.5 below states that $\varepsilon(V_\pi G) = \varepsilon(WD(V_\pi G)) = (-1)^{\frac{p^f-1}{d}\,a_0(M(H))}$; we conclude by applying Proposition 4.28.

5. Proof of Theorem A

(5.1) Let $\mathbf{Q}_p \subset \mathcal{K} \supset \mathcal{O} \longrightarrow \mathcal{O}/\pi\mathcal{O} = \mathbf{F}$ ($p \neq 2$) be as in 1.1. Let L be a finite extension of $\mathbf{Q}_p$ with ring of integers O_L, residue field k_L and absolute Galois group $\Gamma_L = \mathrm{Gal}(\overline{L}/L)$. Assume that T and T' are free $\mathcal{O}$-modules of finite rank equipped with a continuous $\mathcal{O}$-linear action of Γ_L; set $V = T\otimes_{\mathcal{O}}\mathcal{K}$ and $V' = T'\otimes_{\mathcal{O}}\mathcal{K}$.

(5.2) Definition. *If $K \subset \overline{L}$ is a finite extension of L, we say that $V|_{\Gamma_K}$ is a Barsotti–Tate representation if the following equivalent conditions are satisfied (the equivalence between (2) and (3) was proved in [B3, Thm. 5.3.2]).*
(1) *There exists $G \in (\mathcal{O} - \mathrm{div}/O_K)$ such that $T|_{\Gamma_K} = T_\pi G$;*
(2) *there exists $G \in (\mathcal{O} - \mathrm{div}/O_K)$ such that $V|_{\Gamma_K} = V_\pi G$;*
(3) *$V|_{\Gamma_K}$ is a crystalline representation of Γ_K, with Hodge–Tate weights contained in $\{0, 1\}$.*

(5.3) Proposition. *Let $K, K' \subset \overline{L}$ be finite extensions of L.*
(1) *If $V|_{\Gamma_K}$ is Barsotti–Tate and $K^{ur} \subset K'^{ur}$, then $V|_{\Gamma_{K'}}$ is Barsotti–Tate.*
(2) *If K/L and K'/L are tamely ramified, then $K^{ur} \subset K'^{ur}$ if and only if $e(K/L) \mid e(K'/L)$.*
(3) *If K/L is an abelian tamely ramified extension, then, for every uniformiser $\varpi_L \in O_L$, $K' = L(\varpi_L^{1/|k_L^\times|})$ is a totally tamely ramified (cyclic) extension of L and $e(K/L) \mid e(K'/L) = |k_L^\times|$.*

Proof. (1) The condition 5.2(3) depends only on $V|_{I_K}$. The statements (2) and (3) are straightforward.

(5.4) Assume that $\langle\ ,\ \rangle : T \times T \longrightarrow \mathcal{O}(1)$ and $\langle\ ,\ \rangle' : T' \times T' \longrightarrow \mathcal{O}(1)$ are Γ_L-equivariant skew-symmetric $\mathcal{O}$-bilinear pairings inducing isomorphisms $T \xrightarrow{\sim} T^*(1) = \mathrm{Hom}_{\mathcal{O}}(T, \mathcal{O}(1))$, $T' \xrightarrow{\sim} T'^*(1)$, and that there exists an isomorphism of $\mathbf{F}[\Gamma_L]$-modules $\overline{T} = T/\pi T \xrightarrow{\sim} \overline{T}' = T'/\pi T'$ compatible with the pairings $\overline{\langle\ ,\ \rangle} : \overline{T} \times \overline{T} \longrightarrow \mathbf{F}(1)$ and $\overline{\langle\ ,\ \rangle}' : \overline{T}' \times \overline{T}' \longrightarrow \mathbf{F}(1)$ induced by $\langle\ ,\ \rangle$ and $\langle\ ,\ \rangle'$.

Fix such an isomorphism and use it to identify $H^1(L, \overline{T}) = H^1(\Gamma_L, \overline{T}) \xrightarrow{\sim} H^1(\Gamma_L, \overline{T}')$. The arithmetic local constant of Mazur and Rubin ([MR, Def. 4.5], [N5, (2.2.1)]) attached to the above data is defined as

$$\delta_L(T, T') = \delta_L(T', T) = \dim_{\mathbf{F}}(\mathscr{F}/\mathscr{F} \cap \mathscr{F}') \pmod 2 \in \mathbf{Z}/2\mathbf{Z},$$

where

$$\mathscr{F} = \mathrm{Im}\left(H^1_f(L, T) \longrightarrow H^1(L, \overline{T})\right) \subset H^1(L, \overline{T}), \qquad \mathscr{F}' = \mathrm{Im}\left(H^1_f(L, T') \longrightarrow H^1(L, \overline{T}')\right) \subset H^1(L, \overline{T}').$$

(5.5) Theorem (= Theorem A). *If, in the situation of 5.4, there exist abelian tamely ramified finite extensions K/L and K'/L such that $V|_{\Gamma_K}$ and $V'|_{\Gamma_{K'}}$ are Barsotti–Tate representations, then*

$$(-1)^{\delta_L(T,T')} = \varepsilon(WD(V))/\varepsilon(WD(V')) = \varepsilon(V)/\varepsilon(V').$$

Proof. According to Proposition 5.3 there exists a totally tamely ramified (cyclic) extension K/L such that $V|_{\Gamma_K}$ and $V'|_{\Gamma_K}$ are Barsotti–Tate. The extension $L \subset K = L(\varpi)$ ($\varpi^d = \varpi_L$) is of the form considered in 4.7–4.29, with $k_L = k = \mathcal{O}_K/\varpi O_K$ and $d = e(K/L) \mid (p^f - 1)$, where $f = [k : \mathbf{F}_p]$. We can – and will – assume that d is even. As in (4.7.1), there is a canonical isomorphism $\eta : \Delta = \mathrm{Gal}(K/L) \xrightarrow{\sim} \mu_d(O_L) = \mu_d(k)$.

After replacing $\mathbf{F}$ by a suitable finite extension $\mathbf{F}'$, $\mathcal{O}$ by $\mathcal{O}' = \mathcal{O} \otimes_{W(\mathbf{F})} W(\mathbf{F}')$, T by $T \otimes_{\mathcal{O}} \mathcal{O}'$ and T' by $T' \otimes_{\mathcal{O}} \mathcal{O}'$, we can – and will – assume that there exists an embedding $\sigma_0 : k \hookrightarrow \mathbf{F}$.

By assumption, there exist $G, G' \in (\mathcal{O} - \mathrm{div}/O_K)_{dd,K/L}$ such that $T_\pi G = T$ and $T_\pi G' = T'$. As in (4.17.1), the Breuil–Kisin modules with descent data $M = M(G[\pi]), M' = M(G'[\pi]) \in (\mathrm{BT}_{\mathbf{F},\varphi})_{dd,K/L}$ decompose into $M = \bigoplus_i M_i$, $M' = \bigoplus_i M'_i$ ($i \in \mathbf{Z}/f\mathbf{Z}$). As in 4.15, the fixed isomorphism $\overline{T} = G[\pi]_L(\overline{K}) \xrightarrow{\sim} \overline{T}' = G'[\pi]_L(\overline{K})$ of $\mathbf{F}[\Gamma_L]$-modules gives rise to a Δ-equivariant isomorphism $M[1/u] \xrightarrow{\sim} M'[1/u]$ of étale φ-modules over $(\mathbf{F} \otimes k)((u)) \xrightarrow{\sim} \prod_i \mathbf{F}((u))$. According to Proposition 4.16,

$$\mathscr{F}/(\mathscr{F} \cap \mathscr{F}') \xrightarrow{\sim} H^1_{fl}(O_K, H)^\Delta / H^1_{fl}(O_K, G'[\pi])^\Delta,$$

where $H \in (\mathbf{F} - \mathrm{vs}/O_K)_{dd,K/L}$ and $M(H) = M + M'$, hence, in the notation of Proposition 4.21,

$$\delta_L(T, T') = \chi_{\mathbf{F}}(M') - \chi_{\mathbf{F}}(M + M') \pmod 2.$$

According to Proposition 4.24(3), the pairings $\langle\ ,\ \rangle$ and $\langle\ ,\ \rangle'$ are induced by skew-symmetric isomorphisms $G \xrightarrow{\sim} G^D$ and $G' \xrightarrow{\sim} G'^D$. The corresponding isomorphisms $G[\pi] \xrightarrow{\sim} G[\pi]^D$ and $G'[\pi] \xrightarrow{\sim} G[\pi]'^D$ give rise to Δ-equivariant skew-symmetric $(\mathbf{F} \otimes k)[[u]]$-bilinear perfect pairings

$$M \times M \longrightarrow (\mathbf{F} \otimes k)[[u]] \longleftarrow M' \times M'$$

compatible with the isomorphism $M[1/u] \xrightarrow{\sim} M'[1/u]$. In other words, for each $i \in \mathbf{Z}/f\mathbf{Z}$, M_i and M'_i are self-dual τ-lattices in $M_i[1/u] \xrightarrow{\sim} M'_i[1/u]$, in the language of 3.7 (for $F = \mathbf{F}$ and $\eta_i = \sigma_i \circ \tau : \Delta \xrightarrow{\sim} \mu_d(\mathbf{F})$).

As $M = M(G)/\pi M(G)$ and $M' = M(G')/\pi M(G')$, Proposition 4.23(3) tells us that M and M' are Δ-balanced. The exact sequence

$$0 \longrightarrow M \cap M' \longrightarrow M \oplus M' \longrightarrow M + M' \longrightarrow 0$$

can be identified with

$$0 \longrightarrow M(H^D) \longrightarrow M \oplus M' \longrightarrow M(H) \longrightarrow 0,$$

since

$$\forall i \in \mathbf{Z}/f\mathbf{Z} \qquad M(H^D)_i = M(H)_i^* = (M_i + M'_i)^* = M_i^* \cap M_i'^* = M_i \cap M'_i.$$

It follows that $M(H) \oplus M(H^D)$ is Δ-balanced as well. Applying Proposition 4.28 to $G'[\pi]$ and H (and using the fact that $G'[\pi]_L = H_L$), we obtain

$$(-1)^{\delta_L(T,T')} = (-1)^{\chi_{\mathbf{F}}(M+M')}/(-1)^{\chi_{\mathbf{F}}(M')} = \left(\eta_0^{a_0(M+M')-a_0(M')}\right)(\mathrm{rec}_L(-1)).$$

The Weil-Deligne representation $WD(V) = WD(V_\pi G)$ has trivial monodromy $N = 0$ and the action of I_L factors through the cyclic group $I_L/I_K = \Delta$. It follows that that the Frobenius semisimplification $WD(V)^{f-ss}$ is a direct sum of one-dimensional representations of W_L. As it is $\|\cdot\|_L$-symplectic in the sense of [N2, 1.5.3], it is of the form

$$WD(V)^{f-ss} = \bigoplus_\alpha (\chi_\alpha \oplus \chi_\alpha^{-1}\|\cdot\|_L), \qquad \chi_\alpha : W_L \longrightarrow \overline{\mathcal{K}}^\times,$$

which implies that

$$\varepsilon(V) = \varepsilon(WD(V)) = \prod_\alpha \chi_\alpha(\mathrm{rec}_L(-1)) = \prod_\alpha (\chi_\alpha|_{I_L})(\mathrm{rec}_L(-1)).$$

The restriction $WD(V)|_{I_L} = WD(V(-1))|_{I_L}$ is a symplectic $\mathcal{K}[\Delta]$-module and its class in the group $K_0(\mathcal{K}[\Delta]_{Sp}) \xrightarrow{\sim} K_0(\mathbf{F}[\Delta]_{Sp})$ (see 3.8) is equal to the class of M_0/uM_0, by Proposition 4.23(3). The same arguments apply to V' and M'; in particular, $a_0(M') = -I'(M'_0/uM'_0) = 0 \in \mathbf{Z}/d\mathbf{Z}$, by Lemma 3.13(1).

If we write

$$[M_0/uM_0] = \sum_{j=0}^{d/2} c_j([\eta_0^j] + [\eta_0^{-j}]), \qquad [M'_0/uM'_0] = \sum_{j=0}^{d/2} c'_j([\eta_0^j] + [\eta_0^{-j}]) \in K_0(\mathbf{F}[\Delta]_{Sp})$$

(with $c_j, c'_j \in \mathbf{Z}$), then

$$\varepsilon(V) = \eta_0(\mathrm{rec}_L(-1))^{\sum_j jc_j} = (-1)^{\frac{p^f-1}{d}\sum_j jc_j}, \qquad \varepsilon(V') = (-1)^{\frac{p^f-1}{d}\sum_j jc'_j}. \tag{5.5.1}$$

Proposition 3.10, which is the main result of §3, tells us that

$$-a_0(M+M') = I'(M_0+M'_0) \equiv J(M_0/uM_0) + J(M'_0/uM'_0) = \sum_j jc_j + \sum_j jc'_j \pmod 2,$$

which implies the desired formula

$$(-1)^{\delta_L(T,T')} = (-1)^{\frac{p^f-1}{d}a_0(M+M')} = \varepsilon(V)/\varepsilon(V').$$

6. Proof of Theorem B

(6.1) Let $\mathbf{Q}_p \subset \mathcal{K} \supset \mathcal{O} \longrightarrow \mathcal{O}/\pi\mathcal{O} = \mathbf{F}$ be as in 1.1 ($p \neq 2$).

(6.2) From now on until the end of §6 we consider the following global situation. Let L be a number field, S a finite set of primes of L containing $S_\infty \cup S_p = \{v \mid \infty\} \cup \{v \mid p\}$, L_S/L the maximal subextension of $\overline{L}/L$ unramified outside S, $\Gamma_{L,S} = \mathrm{Gal}(L_S/L)$, $S_f = S \smallsetminus S_\infty$.

(6.3) Let T be a free $\mathcal{O}$-module of finite rank equipped with a continuous $\mathcal{O}$-linear action of $\Gamma_{L,S}$; set $V := T \otimes_{\mathcal{O}} \mathcal{K}$. Assume that, for each $v \in S_p$, $V_v := V|_{\Gamma_{L_v}}$ is a de Rham representation of $\Gamma_{L_v} = \mathrm{Gal}(\overline{L}_v/L_v)$. For each $v \in S_f$, the Bloch–Kato subspace $H^1_f(L_v, V) \subset H^1(L_v, V) = H^1(\Gamma_{L_v}, V)$ [BK, (3.7.1),(3.7.2)] (equal to $H^1_{ur}(L_v, V) = H^1(\Gamma_{L_v}/I_v, V^{I_v})$ if $v \notin S_p$) defines subspaces $H^1_f(L_v, T) := \mathrm{Ker}(H^1(L_v, T) \longrightarrow H^1(L_v, V)/H^1_f(L_v, V)) \subset H^1(L_v, T)$ and $H^1_f(L_v, V/T) := \mathrm{Im}(H^1_f(L_v, V) \longrightarrow H^1(L_v, V/T)) \subset H^1(L_v, V/T)$. The corresponding Bloch–Kato Selmer groups and generalised Tate–Šafarevič groups ([BK, Def. 5.1, (5.13)], [Fl, p. 114–115], [FoPR, II.1.3.1, II.5.3.4]) are defined as

$$H^1_f(L, X) := \mathrm{Ker}(H^1(\Gamma_{L,S}, X) \longrightarrow \bigoplus_{v \in S_f} H^1(L_v, X)/H^1_f(L_v, X)) \qquad (X = T, V, V/T),$$
$$Ш(T) := H^1_f(L, V/T)/\mathrm{Im}(H^1_f(L, V)) = H^1_f(L, V/T)/H^1_f(L, V/T)_{\mathrm{div}}$$

(these groups are independent of S, since $H^1_f(L_v, X) = H^1_{ur}(L_v, X)$ if $v \notin S_p$ and $V = V^{I_v}$).

Fontaine and Perrin-Riou [FoPR, II.1.3.1, II.5.3.6] also defined

$$H^0_f(L, X) := H^0(\Gamma_{L,S}, X) \qquad (X = T, V),$$
$$H^i_f(L, T) := \mathrm{Hom}_{\mathcal{O}}(H^{3-i}_f(L, V^*(1)/T^*(1)), \mathcal{K}/\mathcal{O}) \qquad (i = 2, 3),$$
$$H^i_f(L, V) := \mathrm{Hom}_{\mathcal{K}}(H^{3-i}_f(L, V^*(1)), \mathcal{K}) \qquad (i = 2, 3),$$

where $T^*(1) := \mathrm{Hom}_{\mathcal{O}}(T, \mathcal{O})(1)$ and $V^*(1) := T^*(1) \otimes_{\mathcal{O}} \mathcal{K} = \mathrm{Hom}_{\mathcal{K}}(V, \mathcal{K})(1)$; then $H^i_f(L, V) = H^i_f(L, T) \otimes_{\mathcal{O}} \mathcal{K}$ for all $i = 0, 1, 2, 3$ and $H^1_f(L, T)_{\mathrm{tors}} = H^0(\Gamma_{L,S}, V/T)/\mathrm{Im}(H^0(\Gamma_{L,S}, V)) = H^0(L, V/T)/H^0(L, V/T)_{\mathrm{div}}$. Strictly speaking, the groups $H^i_f(L, X)$ were denoted by $\widetilde{H}^i_f(L, X)$ in [FoPR], but we prefer to reserve the notation $\widetilde{H}^i_f$ for the extended Selmer groups defined in [N1, 6.1.2].

Flach [Fl, Thm. 1] (see also [FoPR, II.5.4.2]) constructed a nondegenerate pairing of $\mathcal{O}$-modules of finite length

$$Ш(T) \times Ш(T^*(1)) \longrightarrow \mathcal{K}/\mathcal{O}, \tag{6.3.1}$$

which coincides (perhaps up to a sign) with the classical Cassels–Tate pairing between the groups $Ш(T) = Ш(A/L)[p^\infty]/Ш(A/L)[p^\infty]_{\mathrm{div}}$ and $Ш(T^*(1)) = Ш(\widehat{A}/L)[p^\infty]/Ш(\widehat{A}/L)[p^\infty]_{\mathrm{div}}$ if $\mathcal{O} = \mathbf{Z}_p$, $T = T_p(A)$ and $T^*(1) = T_p(\widehat{A})$, for an abelian variety A over L.

(6.4) One can also define the Selmer group (again independent of S)

$$H^1_{\mathscr{F}}(L, \overline{T}) := \mathrm{Ker}(H^1(\Gamma_{L,S}, \overline{T}) \longrightarrow \bigoplus_{v \in S_f} H^1(L_v, \overline{T})/\mathscr{F}_v)$$

for the $\mathbf{F}[\Gamma_{L,S}]$-module $\overline{T} = T/\pi T$ and the Selmer structure [MR, Def. 1.2] $\mathscr{F} = (\mathscr{F}_v)_{v \in S_f}$, where

$$\mathscr{F}_v := \mathrm{Im}(H^1_f(L_v, T) \longrightarrow H^1(L_v, \overline{T})). \tag{6.4.1}$$

According to [N5, (1.1.1)],

$$\dim_{\mathbf{F}} H^1_{\mathscr{F}}(L, \overline{T}) - \dim_{\mathbf{F}} H^0(L, \overline{T}) = \dim_{\mathbf{F}} H^1_f(L, V/T)[\pi] - \dim_{\mathcal{K}} H^0(L, V) = \chi_f(L, V) + \dim_{\mathbf{F}} Ш(T)[\pi], \tag{6.4.2}$$

where

$$\chi_f(L,V) := \dim_{\mathcal{K}} H^1_f(L,V) - \dim_{\mathcal{K}} H^0(L,V) = h^1_f(L,V) - h^0(L,V).$$

(6.5) If $\langle\ ,\ \rangle : V \times V \longrightarrow \mathcal{K}(1)$ is a skew-symmetric pairing inducing an isomorphism of $\mathcal{O}[\Gamma_{L,S}]$-modules $T \xrightarrow{\sim} T^*(1)$, then the composition of (6.3.1) with $Ш(T) \xrightarrow{\sim} Ш(T^*(1))$ is a skew-symmetric ([Fl, Thm. 2], [FoPR, II.5.4.3]) nondegenerate pairing

$$Ш(T) \times Ш(T) \longrightarrow \mathcal{K}/\mathcal{O} \tag{6.5.1}$$

of $\mathcal{O}$-modules of finite length, which implies that $Ш(T) = Y \oplus Y$ for some Lagrangian (maximal isotropic with respect to (6.5.1)) submodule $Y \subset Ш(T)$ (recall that $p \neq 2$). The formula (6.4.2) then yields [N5, (1.1.3)]

$$\dim_{\mathbf{F}} H^1_{\mathscr{F}}(L,\overline{T}) - \dim_{\mathbf{F}} H^0(L,\overline{T}) \equiv \chi_f(L,V) \pmod 2. \tag{6.5.2}$$

Moreover, each $\mathscr{F}_v$ is a Lagrangian subspace (see [BK, Prop. 3.8] for $v \in S_p$) of the quadratic space $(H^1(L_v,\overline{T}),\cup)$. Recall that the cup product attached to $\overline{\langle\ ,\ \rangle} : \overline{T} \times \overline{T} \longrightarrow \mathbf{F}(1)$

$$\cup : H^1(L_v,\overline{T}) \times H^1(L_v,\overline{T}) \longrightarrow H^2(L_v,\mathbf{F}(1)) \simeq \mathbf{F}$$

is nondegenerate, by Tate local duality. In other words, $\mathscr{F}$ is a self-dual Selmer structure on $\overline{T}$.

For each $v \in S_f \smallsetminus S_p$ (resp. $v \in S_p$) the representation $WD(V_v)$ of the Weil-Deligne group of L_v atached to $V_v = V|_{\Gamma_{L_v}}$ (resp. to $D_{\mathrm{pst}}(V_v)$) is $\|\cdot\|_{L_v}$-symplectic, in the language of [N2, 1.5.3]. The local epsilon constant

$$\varepsilon_v(V) := \varepsilon(WD(V_v),\psi,dx_\psi) \in \{\pm 1\}$$

(where dx_ψ is a Haar measure on L_v self-dual with respect to an additive character $\psi \neq 1$ of L_v) does not depend on ψ [N2, Prop. 2.2.1].

(6.6) Assume that T' is another free $\mathcal{O}$-module of finite rank equipped with a continuous $\mathcal{O}$-linear action of $\Gamma_{L,S}$, $\langle\ ,\ \rangle' : V' \times V' \longrightarrow \mathcal{K}(1)$ ($V' := T' \otimes_{\mathcal{O}} \mathcal{K}$) is a pairing inducing an isomorphism of $\Gamma_{L,S}$-modules $T' \xrightarrow{\sim} T'^*(1)$ and $\overline{T} \xrightarrow{\sim} \overline{T}' = T'/\pi T'$ is an isomorphism of $\mathbf{F}[\Gamma_{L,S}]$-modules compatible with the pairings $\overline{\langle\ ,\ \rangle}$ and $\overline{\langle\ ,\ \rangle}' : \overline{T}' \times \overline{T}' \longrightarrow \mathbf{F}(1)$.

Fix such an isomorphism and use it to identify the quadratic spaces $(H^1(L_v,\overline{T}),\cup) \xrightarrow{\sim} (H^1(L_v,\overline{T}'),\cup)$, for all $v \in S_f$. We obtain the arithmetic local constants of Mazur and Rubin ([MR, Def. 4.5], [N5, (2.2.1)])

$$\delta_v(T,T') = \delta_v(T',T) := \dim_{\mathbf{F}} \mathscr{F}_v/(\mathscr{F}_v \cap \mathscr{F}'_v) \pmod 2 \in \mathbf{Z}/2\mathbf{Z},$$

where $\mathscr{F}'_v \subset H^1(L_v,\overline{T}')$ is defined as in (6.4.1). The ranks of the Selmer groups $H^1_{\mathscr{F}}(L,\overline{T}) \subset H^1(\Gamma_{L,S},\overline{T})$ and $H^1_{\mathscr{F}'}(L,\overline{T}') \subset H^1(\Gamma_{L,S},\overline{T}')$ are related by a formula of Mazur and Rubin [MR, Thm. 1.4]

$$\dim_{\mathbf{F}} H^1_{\mathscr{F}}(L,\overline{T}) - \dim_{\mathbf{F}} H^1_{\mathscr{F}'}(L,\overline{T}') \equiv \sum_{v\in S_f} \delta_v(T,T') \pmod 2, \tag{6.6.1}$$

which implies, thanks to (6.5.2), that

$$\chi_f(L,V) - \chi_f(L,V') \equiv \sum_{v\in S_f} \delta_v(T,T') \pmod 2. \tag{6.6.2}$$

(6.7) Theorem (= Theorem B). *If, in the situation of 6.6, there exist finite abelian extensions $K(v)/L_v$ and $K(v)'/L_v$ (for all $v \in S_p$) such that the representations $V_{\Gamma_{K(v)}}$ and $V'_{\Gamma_{K(v)'}}$ are Barsotti–Tate, then*

$$(-1)^{\chi_f(L,V)}/\varepsilon(V) = (-1)^{\chi_f(L,V')}/\varepsilon(V'),$$

where $\varepsilon(V) := \prod_{v\in S}\varepsilon_v(V)$, $\varepsilon(V') := \prod_{v\in S}\varepsilon_v(V')$ *and* $\varepsilon_v(V) = \varepsilon_v(V') := (-1)^{\dim_{\mathcal{K}}(V)/2}$ *for all* $v \in S_\infty$.

Proof. Firstly, we observe that $\chi_f(L,V) \pmod 2 \in \mathbf{Z}/2\mathbf{Z}$ and $\varepsilon_L(V) = \varepsilon(V)$ (and the analogous expressions for V') do not change if we replace L by an abelian extension L'/L of odd degree. Indeed, the set of nontrivial characters of $\mathrm{Gal}(L'/L)$ can be written as a disjoint union of pairs $\{\alpha, \alpha^{-1}\}$ and

$$\varepsilon_{L'}(V)/\varepsilon_L(V) = \prod_{\alpha}\varepsilon_L(V\otimes\alpha)\varepsilon_L(V\otimes\alpha^{-1}),$$

but $\varepsilon_L(V\otimes\alpha)\varepsilon_L(V\otimes\alpha^{-1}) = 1$. Similarly,

$$\chi_f(L',V) - \chi_f(L,V) = \sum_{\alpha}(\chi_f(L,V\otimes\alpha) + \chi_f(L,V\otimes\alpha^{-1})),$$

but $\chi_f(L,V\otimes\alpha) = \chi_f(L,V\otimes\alpha^{-1})$, by [N1, Prop. 12.5.9.5(iv)].

Secondly, we can replace $K(v)$ by $K(v)K(v)'$ and assume that $K(v) = K(v)'$, for all $v \in S_p$. Let $M(v)$ be an intermediate field $L_v \subset M(v) \subset K(v)$ such that $[M(v) : L_v] = p^{m_v}$ and $p \nmid [K(v) : M(v)]$. There exist integers $r, n \geq 1$ and characters $\beta_i^{(v)} : \mathrm{Gal}(M(v)/L_v) \longrightarrow \mu_{p^n}$ such that $(\beta_1^{(v)}, \ldots, \beta_r^{(v)}) : \mathrm{Gal}(M(v)/L_v) \hookrightarrow \mu_{p^n}^{\oplus r}$ is injective, for all $v \in S_p$. According to [AT, ch. 10, Thm. 5] (see also [NSW, Cor. 9.2.3]) there exist global characters $\beta_1, \ldots, \beta_r : \mathrm{Gal}(L^{ab}/L) \longrightarrow \mu_{p^n}$ such that $\beta_i|_{\Gamma_{L_v}} = \beta_i^{(v)}$, for all $i = 1, \ldots, r$ and $v \in S_p$. The fixed field $L' = (L^{ab})^G$ of $G = \bigcap_{i=1}^r \mathrm{Ker}(\beta_i)$ is a finite abelian extension of L such that $[L' : L] = p^m$ and $L'_{v'} \supset M(v)$, for all $v' \mid v \in S_p$.

Thirdly, we can replace L by L' (thanks to the first step) and assume that $K(v)$ and $K(v)'$ are tamely ramified abelian extensions of L_v, for all $v \in S_p$, by the second step. We have

$$\forall v \in S_f \qquad (-1)^{\delta_v(T,T')} = \varepsilon_v(V)/\varepsilon_v(V'),$$

by Theorem 5.5 (= Theorem A) if $v \in S_p$ (resp. by [N6, Thm. 2.17] if $v \notin S_p$). Applying (6.6.2), we obtain

$$(-1)^{\chi_f(L,V)-\chi_f(L,V')} = \prod_{v\in S_f}\varepsilon_v(V)/\varepsilon_v(V') = \prod_{v\in S}\varepsilon_v(V)/\varepsilon_v(V') = \varepsilon(V)/\varepsilon(V')$$

(the middle equality follows from the fact that $\varepsilon_v(V) = \varepsilon_v(V')$ for all $v \mid \infty$, by definition). Theorem is proved.

7. Tamagawa numbers and isogenies

(7.1) Let $\mathcal{K}, \mathcal{O}, \pi, \mathbf{F}, L, S, T$ and V be as in 6.1–6.3.

(7.2) The formalism of Fontaine and Perrin-Riou ([FoPR, II.4.2, II.5.3]). Consider the following determinant objects, which are invertible modules over $\mathcal{K}$ or $\mathcal{O}$ (we ignore the issue of signs, which plays no role in what follows).

$$\det_{\mathcal{K}}\mathbf{R}\Gamma_f(L,V) := \bigotimes_{i=0}^{3}(\det_{\mathcal{K}}H^i_f(L,V))^{(-1)^i} \supset \det_{\mathcal{O}}\mathbf{R}\Gamma_f(L,T) := \bigotimes_{i=0}^{3}(\det_{\mathcal{O}}H^i_f(L,T))^{(-1)^i}$$

$$\widetilde{\Delta}'_f(T) := \det_{\mathcal{O}}\mathbf{R}\Gamma_f(L,T)\otimes_{\mathcal{O}}\det_{\mathcal{O}}H^0(L\otimes\mathbf{R},T)^{-1},$$

$$\Delta'_f(T) := \bigotimes_{i=0}^{1}(\det_{\mathcal{O}}H^i_f(L,T)\otimes\det_{\mathcal{O}}H^i_f(L,T^*(1)))^{(-1)^i}\otimes_{\mathcal{O}}\det_{\mathcal{O}}H^0(L\otimes\mathbf{R},T)^{-1},$$

$$\Delta'_f(V) := \det_{\mathcal{K}}\mathbf{R}\Gamma_f(L,V)\otimes_{\mathcal{K}}\det_{\mathcal{K}}H^0(L\otimes\mathbf{R},V)^{-1} \supset \widetilde{\Delta}'_f(T),\ \Delta'_f(T).$$

According to [FoPR, II.5.3.8(ii)],

$$\widetilde{\Delta}'_f(T) = \Delta'_f(T) \otimes_{\mathcal{O}} \det_{\mathcal{O}} Ш(T^*(1))$$

(recall that $\det_{\mathcal{O}}(M) = \pi^{-\ell_{\mathcal{O}}(M)}\mathcal{O} \subset \mathcal{K}$, for every $\mathcal{O}$-module M of finite length).

(7.3) The Tamagawa factors [FoPR, I.4]. The tangent space at $v \in S_p$ is defined [BK, Def. 3.10] as

$$t_{V,v} := D_{dR}(V_v)/Fil^0 = H^0(\Gamma_{L_v}, V_v \otimes_{\mathbf{Q}_p} B_{dR}/B_{dR}^+).$$

Let ω_v be a basis of $\det_{\mathcal{K}}(t_{V,v})$; then $\omega = \otimes_{v\in S_p}\omega_v$ is a basis of $\det_{\mathcal{K}}(t_V) = \otimes_{v\in S_p}\det_{\mathcal{K}}(t_{V,v})$. For $v \in S_f \smallsetminus S_p$ we let $\det_{\mathcal{K}}(t_{V,v}) = \mathcal{K}$ and $\omega_v = 1$.

For every $v \in S_f$ the determinants

$$\det_{\mathcal{K}} \mathbf{R}\Gamma_f(L_v, V) := \bigotimes_{i=0}^{1} (\det_{\mathcal{K}} H^i_f(L_v, V))^{(-1)^i} \supset \det_{\mathcal{O}} \mathbf{R}\Gamma_f(L_v, T) := \bigotimes_{i=0}^{1} (\det_{\mathcal{O}} H^i_f(L_v, T))^{(-1)^i}$$

are canonically (up to a sign) isomorphic to

$$\det_{\mathcal{K}}(t_{V,v})^{-1} = \mathcal{K}\cdot\omega_v^{-1} \supset \mathcal{O}\cdot \mathrm{Tam}^0_{\omega_v}(T)\,\omega_v^{-1},$$

where

$$\mathrm{Tam}^0_{\omega_v}(T) \in \mathcal{K}^\times/\mathcal{O}^\times$$

is the local Tamagawa factor [FoPR, I.4.1.2]. If $v \in S_f \smallsetminus S_p$, then

$$\mathrm{Tam}^0_{\omega_v}(T)\,\mathcal{O} = \det_{\mathcal{O}}\left(H^1(I_v, T)^{\mathrm{Fr}(v)=\mathrm{id}}_{\mathrm{tors}}\right)^{-1}, \tag{7.3.1}$$

by [FoPR, I.4.2.2(ii)]. We denote by

$$\mathrm{Tam}^0_{\omega}(T) := \prod_{v\in S_f} \mathrm{Tam}^0_{\omega_v}(T)$$

the (finite part of the) global Tamagawa factor.

(7.4) The fundamental line $\Delta_f(V)$. Let $\widetilde{\omega}'_T$ be any generator of the invertible $\mathcal{O}$-module $\widetilde{\Delta}'_f(T)$. According to [FoPR, II.5.3.6, II.5.3.8], the invertible $\mathcal{O}$-module

$$\Delta'_f(T) \otimes_{\mathcal{O}} \det_{\mathcal{O}} Ш(T^*(1)) \otimes_{\mathcal{O}} \mathrm{Tam}^0_{\omega}(T)^{-1}\omega = \widetilde{\Delta}'_f(T) \otimes_{\mathcal{O}} \mathrm{Tam}^0_{\omega}(T)^{-1}\omega \subset \Delta_f(V) := \Delta'_f(V) \otimes_{\mathcal{K}} \det_{\mathcal{K}}(t_V) \tag{7.4.1}$$

is equal to $\widetilde{\Delta}'_f(T) \otimes \omega\,|\widetilde{\omega}'_T \otimes \omega|_{EP,V} = \mathcal{O}\cdot(\widetilde{\omega}'_T \otimes \omega)\,|\widetilde{\omega}'_T \otimes \omega|_{EP,V}$, where $|\cdot|_{EP,V}$ is an $\mathcal{O}$-linear version of the Euler–Poincaré norm on $\Delta_f(V)$ defined in [FoPR, II.4.1.9] (in the context considered here the norm has values in $\mathcal{K}^\times/\mathcal{O}^\times$). This norm depends only on V, which implies that the invertible $\mathcal{O}$-module (7.4.1) does not depend on T, nor on ω. Equivalently, for fixed ω,

$$\bigotimes_{i=0}^{1}(\det_{\mathcal{O}} H^i_f(L,T) \otimes \det_{\mathcal{O}} H^i_f(L, T^*(1)))^{(-1)^i} \otimes_{\mathcal{O}} \det_{\mathcal{O}} H^0(L\otimes\mathbf{R}, T)^{-1}\pi^{-\ell_{\mathcal{O}}(Ш(T^*(1)))}\mathrm{Tam}^0_{\omega}(T)^{-1} \tag{7.4.2}$$

does not depend on T. Note that

$$\bigotimes_{i=0}^{1}(\det_{\mathcal{O}} H^i_f(L,T))^{(-1)^i} = \pi^{\ell_{\mathcal{O}}(H^1_f(L,T)_{\mathrm{tors}})}\det_{\mathcal{O}} H^0(L,T) \otimes_{\mathcal{O}} \det_{\mathcal{O}}(H^1_f(L,T)/\mathrm{tors})^{-1} \tag{7.4.3}$$

(and similarly for $T^*(1)$).

(7.5) The self-dual case. If $T \xrightarrow{\sim} T^*(1)$ is self-dual with respect to a skew-symmetric pairing $\langle\ ,\ \rangle : V \times V \longrightarrow \mathcal{K}(1)$ as in 6.5, then $H^1_f(L,T)_{\mathrm{tors}} = H^1_f(L,T^*(1))_{\mathrm{tors}}$ and $\ell_{\mathcal{O}}(Ш(T^*(1))) \equiv 0 \pmod 2$, which implies that

$$\bigotimes_{i=0}^{1}(\det_{\mathcal{O}}(H^i_f(L,T)/\mathrm{tors}) \otimes \det_{\mathcal{O}}(H^i_f(L,T^*(1))/\mathrm{tors}))^{(-1)^i} \otimes_{\mathcal{O}} \det_{\mathcal{O}} H^0(L\otimes\mathbf{R},T)^{-1}\mathrm{Tam}^0_\omega(T)^{-1} \pmod{\mathcal{K}^{\times 2}} \tag{7.5.1}$$

does not depend on T.

(7.6) A formula of Cassels. If $T' \supset T$ is a $\Gamma_{L,S}$-stable $\mathcal{O}$-lattice in V such that $T'^*(1) = \{x \in V \mid \langle x, T'\rangle \in \mathcal{O}(1)\} = aT'$ for some $a \in \mathcal{O} \smallsetminus \{0\}$, then we can apply (7.5.1) to T' (and the pairing $a^{-1}\langle\ ,\ \rangle$). Comparing the expressions for T and T', we deduce that

$$a^{\chi_f(L,V)}\mathrm{Tam}^0_\omega(T)/\mathrm{Tam}^0_\omega(T') \pmod{\mathcal{K}^{\times 2}} = \pi^{\ell_{\mathcal{O}}(H^0(L\otimes\mathbf{R},T')/H^0(L\otimes\mathbf{R},T))} \pmod{\mathcal{K}^{\times 2}} \in \mathcal{K}^\times/\mathcal{O}^\times\mathcal{K}^{\times 2}. \tag{7.6.1}$$

The statement (7.4.2) is an abstract version of a formula of Cassels [C1, Thm. 1.1] comparing the global Tamagawa factors of two isogeneous eliptic curves. Its consequence (7.6.1) (cf. [C1, Thm. 1.5]) gives a formula for $\chi_f(L,V) \pmod 2 \in \mathbf{Z}/2\mathbf{Z}$, provided that $\mathrm{ord}_\pi(a) \equiv 1 \pmod 2$.

(7.7) From now on until the end of §7 assume that we are in the situation of 7.6 with $a = \pi$. In concrete terms, $\pi T' \subset T$ and $H_L := \pi T'/\pi T \subset T/\pi T = \overline{T}$ is a $\Gamma_{L,S}$-stable Lagrangian subspace with respect to the pairing $\overline{\langle\ ,\ \rangle} : \overline{T} \times \overline{T} \longrightarrow \mathbf{F}(1)$. Moreover, there are exact sequences of $\mathcal{O}[\Gamma_{L,S}]$-modules

$$0 \longrightarrow T \longrightarrow T' \longrightarrow H_L \longrightarrow 0, \qquad 0 \longrightarrow H_L \longrightarrow \overline{T} \longrightarrow H'_L \longrightarrow 0 \tag{7.7.1}$$

and an isomorphism $H'_L \xrightarrow{\sim} H^*_L(1) = \mathrm{Hom}_{\mathbf{F}}(H_L,\mathbf{F})(1)$. Conversely, if $H_L \subset \overline{T}$ is a $\Gamma_{L,S}$-stable Lagrangian subspace, then its inverse image under $T \longrightarrow \overline{T}$ is of the form $\pi T'$, with $T' \supset T$ as above.

For $v \in S_f$ define $h_v \in \mathbf{Z}$ (independent of ω_v) by

$$\pi^{h_v}\mathcal{O}^\times := \mathrm{Tam}^0_{\omega_v}(T')/\mathrm{Tam}^0_{\omega_v}(T).$$

The exact sequence

$$0 \longrightarrow H^0(L_v,T) \longrightarrow H^0(L_v,T') \longrightarrow H^0(L_v,H_L) \longrightarrow H^1_f(L_v,T) \xrightarrow{\alpha} H^1_f(L_v,T') \tag{7.7.2}$$

induced by (7.7.1) implies that

$$h_v = \ell_{\mathcal{O}}(\mathrm{Coker}(\alpha)) - \ell_{\mathcal{O}}(H^0(L_v,H_L)).$$

For $v \in S_\infty$ define

$$h_v := \ell_{\mathcal{O}}(H^0(L_v,T')/H^0(L_v,T)), \qquad \varepsilon_v(V) = (-1)^{\dim_{\mathcal{K}}(V)/2}. \tag{7.7.3}$$

(7.8) Denote by

$$\det_{H_L} : \Gamma^{ab}_{L,S} \longrightarrow \mathbf{F}^\times$$

the Galois action on $\wedge^r H_L$, where $r = \dim_{\mathbf{F}}(H_L) = \dim_{\mathcal{K}}(V)/2$. Conjecturally (cf. [BS], [CFKS, Thm. 2.7]),

$$(-1)^{h_v}\det_{H_L}(\mathrm{rec}_{L_v}(-1)) \stackrel{?}{=} \varepsilon_v(V) \tag{7.8.1}$$

holds, for all $v \in S$. If this is the case, then (7.6.1) yields

$$(-1)^{\chi_f(L,V)} = \prod_{v\in S}\varepsilon_v(V)\det_{H_L}(\mathrm{rec}_{L_v}(-1)) = \prod_{v\in S}\varepsilon_v(V) = \varepsilon(V). \tag{7.8.2}$$

(7.9) Proposition. *Assume that we are in the situation of 7.7.*
(1) *If $L_v \simeq \mathbf{C}$, then $h_v = r = \dim_{\mathcal{K}}(V)/2$, $\det_{H_L}(\mathrm{rec}_{L_v}(-1)) = 1$ and (7.8.1) holds.*
(2) *If $L_v \simeq \mathbf{R}$, let $r_v^{\pm} := \dim_{\mathbf{F}} \mathrm{Ker}(c_v \mp \mathrm{id} : H_L(\overline{L}_v) \longrightarrow H_L(\overline{L}_v))$ be the multiplicity of the eigenvalue ± 1 for the action of the complex conjugation $c_v \in \mathrm{Gal}(\overline{L}_v/L_v)$ on $H_L(\overline{L}_v)$. In this case $h_v = r_v^+ = r - r_v^-$, $\det_{H_L}(\mathrm{rec}_{L_v}(-1)) = (-1)^{r_v^-}$ and (7.8.1) holds.*
(3) *If $v \in S_f$, $\dim_{\mathcal{K}}(V) = 2$ and the monodromy operator N on $WD(V_v)$ is nonzero, then (7.8.1) holds.*
(4) *If $v \in S_f \smallsetminus S_p$ and if the inertia group $I_v = I_{L_v}$ acts on V through a finite quotient of order prime to p, then $\mathrm{Tam}^0_{\omega_v}(T') = \mathrm{Tam}^0_{\omega_v}(T) = 1$, $h_v = 0$, $\varepsilon_v(V) = \det_{H_L}(\mathrm{rec}_{L_v}(-1))$ and (7.8.1) holds.*
(5) *If $v \in S_p$ and if there exists an abelian tamely ramified extension $K(v)/L_v$ such that $V|_{\Gamma_{K(v)}}$ is a Barsotti–Tate representation, then (7.8.1) holds.*

Proof. The statements (1) and (2) follow from (7.7.3), by definition.
(3) Nontriviality of N together with $\wedge^2 \simeq \mathcal{O}(1)$ imply that $T_v = T|_{\Gamma_{L_v}}$ is reducible and that there is an exact sequence of $\mathcal{O}[\Gamma_{L_v}]$-modules

$$0 \longrightarrow T_v^+ \longrightarrow T_v \longrightarrow T_v^- \longrightarrow 0, \qquad T_v^+ \simeq \mathcal{O}(1) \otimes \mu, \qquad T_v^- \simeq \mathcal{O} \otimes \mu, \qquad \mu : \Gamma_{L_v} \longrightarrow \{\pm 1\},$$

and the extension class

$$[T_v] \in \mathrm{Ext}^1_{\mathcal{O}[\Gamma_{L_v}]}(\mathcal{O}, \mathcal{O}(1)) = \left(\varprojlim_n L_v^\times \otimes \mathbf{Z}/p^n\mathbf{Z}\right) \otimes_{\mathbf{Z}_p} \mathcal{O} =: L_v^\times \widehat{\otimes} \mathcal{O}$$

does not lie in $O_{L_v}^\times \widehat{\otimes} \mathcal{O}$. In other words,

$$a(T_v) := (\mathrm{ord}_v \otimes \mathrm{id})([T_v]) \in \mathcal{O} \setminus \{0\}$$

(and similarly for T_v' and $a(T_v')$).

This implies that $H^0(L_v, V) = 0$, hence $H^2(L_v, V) \simeq H^0(L_v, V^*(1))^* \simeq H^0(L_v, V)^* = 0$ and

$$\dim_{\mathcal{K}} H^1_f(L_v, V) = \frac{1}{2} \dim_{\mathcal{K}} H^1(L_v, V) = \delta_v \cdot [L_v : \mathbf{Q}_p], \qquad \delta_v := \begin{cases} 1, & v \mid p, \\ 0, & v \nmid p, \end{cases}$$

by the local Euler characteristic formula. Let $V_v^\pm := T_v^\pm \otimes_{\mathcal{O}} \mathcal{K} = T_v'^\pm \otimes_{\mathcal{O}} \mathcal{K}$.

The local epsilon factor is given by the standard formula ([N1, Lemma 12.3.13(vi)])

$$\varepsilon_v(V) = \mu(\mathrm{rec}_{L_v}(-1)) \cdot \begin{cases} -1, & \mu = 1, \\ 1, & \mu \neq 1. \end{cases}$$

We are now going to compute h_v. The vanishing of $H^0(L_v, V)$ implies that

$$h_v = \ell_{\mathcal{O}}(\mathrm{Coker}(\alpha)) - \ell_{\mathcal{O}}(\mathrm{Ker}(\alpha)),$$

where the map $\alpha : H^1_f(L_v, T) \longrightarrow H^1_f(L_v, T')$ from (7.7.2) is induced by the inclusion $u : T \hookrightarrow T'$. Multiplication by π on T factors as $T \xrightarrow{u} T' \xrightarrow{u'} T$. Denote by $\alpha' : H^1_f(L_v, T') \longrightarrow H^1_f(L_v, T)$ the map induced by u' and let

$$h_v' := \ell_{\mathcal{O}}(\mathrm{Coker}(\alpha')) - \ell_{\mathcal{O}}(\mathrm{Ker}(\alpha')).$$

Again, $\alpha'\alpha$ is given by multiplication by π on $H^1_f(L_v, T)$, which implies that

$$h_v + h_v' = \ell_{\mathcal{O}}(\mathrm{Coker}(\alpha'\alpha)) - \ell_{\mathcal{O}}(\mathrm{Ker}(\alpha'\alpha)) = \dim_{\mathcal{K}} H^1_f(L_v, V) = \delta_v \cdot [L_v : \mathbf{Q}_p].$$

As $\mathrm{Hom}_{\mathcal{O}[\Gamma_{L_v}]}(\mathcal{O}(1) \otimes \mu, \mathcal{O} \otimes \mu) = 0$, the inclusion $u : T \hookrightarrow T'$ induces morphisms of $\mathcal{O}[\Gamma_{L_v}]$-modules $u^\pm : T_v^\pm \longrightarrow T_v'^\pm$ satisfying

$$\mathrm{Ker}(u^\pm) = 0, \qquad \ell_{\mathcal{O}}(\mathrm{Coker}(u^+)) + \ell_{\mathcal{O}}(\mathrm{Coker}(u^-)) = \ell_{\mathcal{O}}(\mathrm{Coker}(u)) = \mathrm{rk}_{\mathbf{F}}(H_L) = 1.$$

We say that the inclusion $u : T \hookrightarrow T'$ is *generic* if $H_L \neq T_v^+/\pi T_v^+$ (which is equivalent to u^+ being an isomorphism). If $H_L = T_v^+/\pi T_v^+$ (which is equivalent to u^- being an isomorphism) we say that u is *special*. Note that u is generic if and only if $u' : T' \hookrightarrow T$ is special.

Returning to the computation of h_v, assume first that $v \nmid p$. The wild inertia subgroup $I_v^w \subset I_v$ acts trivially on V, since $p \neq 2$; it follows that $H^1(I_v, T) \simeq T_{I_v}(-1)$ (and similarly for T').

If μ is ramified, then $T_{I_v} = T'_{I_v} = 0$, hence $\mathrm{Tam}^0_{\omega_v}(T') = \mathrm{Tam}^0_{\omega_v}(T) = 1$ and $h_v = 0$.

If μ is unramified, then there is an exact sequence of Γ_{L_v}/I_v-modules

$$0 \longrightarrow T_v^+/a(T)T_v^+ \longrightarrow T_{I_v} \longrightarrow T_v^- \longrightarrow 0,$$

which implies that

$$H^1(I_v, T)^{\mathrm{Fr}(v)=\mathrm{id}}_{\mathrm{tors}} = ((\mathcal{O}/a(T)\mathcal{O}) \otimes \mu)^{\mathrm{Fr}(v)=\mathrm{id}} = \begin{cases} \mathcal{O}/a(T)\mathcal{O}, & \mu(\mathrm{Fr}(v)) = 1, \\ 0, & \mu(\mathrm{Fr}(v)) = -1 \end{cases}$$

(and similarly for T').

To sum up the case $v \nmid p$,

$$h_v = \begin{cases} \mathrm{ord}_\pi(a(T'_v)/a(T_v)), & \mu = 1, \\ 0, & \mu \neq 1. \end{cases}$$

If $\mu = 1$, then $T_v^+ = \mathcal{O}(1)$, $T_v^- = \mathcal{O}$ and $[T_v]$ is the image of $1 \in H^0(L_v, T_v^-)$ under the boundary map $H^0(L_v, T_v^-) \longrightarrow H^1(L_v, T_v^+)$. If, in addition, u is special, then u^- is an isomorphism and $\mathrm{ord}_\pi(a(T'_v)) = \mathrm{ord}_\pi(a(T_v)) + 1$ (for example, if $\mathcal{O} = \mathbf{Z}_p$ and if T_v is the Tate module of an elliptic curve over L_v with Tate parameter $q \in L_v^\times$, then u arises from the isogeny $L_v^\times/q^{\mathbf{Z}} \longrightarrow L_v^\times/q^{p\mathbf{Z}}$ given by $z \mapsto z^p$). Combined with the previous discussion, this yields, for $v \nmid p$ and $\mu = 1$,

$$h_v = \begin{cases} -1, & H_L \neq T_v^+/\pi T_v^+, \\ 1, & H_L = T_v^+/\pi T_v^+. \end{cases}$$

Assume now that $v \mid p$.

The vanishing of

$$\mathrm{Ker}(H^1(L_v, T_v^-) \longrightarrow H^1(L_v, V_v^-)) = H^1(L_v, T_v^-)_{\mathrm{tors}} \simeq H^0(L_v, T_v^- \otimes \mathcal{K}/\mathcal{O})/\mathrm{div}$$

combined with the fact that

$$H^1_f(L_v, V) = \mathrm{Ker}(H^1(L_v, V) \longrightarrow H^1(L_v, V^-))$$

([N2, Prop. 3.3.2(2)]) imply – together with analogous statements for T'_v – that there is a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^0(L_v, T_v^-) & \longrightarrow & H^1(L_v, T_v^+) & \longrightarrow & H^1_f(L_v, T) & \longrightarrow & 0 \\ & & \downarrow u_*^- & & \downarrow u_*^+ & & \downarrow \alpha & & \\ 0 & \longrightarrow & H^0(L_v, T_v'^-) & \longrightarrow & H^1(L_v, T_v'^+) & \longrightarrow & H^1_f(L_v, T') & \longrightarrow & 0 \end{array}$$

If u is generic, then the map u_*^+ is an isomorphism, hence

$$h_v = -\ell_{\mathcal{O}}(\mathrm{Coker}(u_*^-)) = \begin{cases} -1, & \mu = 1, \\ 0, & \mu \neq 1. \end{cases}$$

If u is special, then u' is generic and the previous formula holds for h'_v, which implies that

$$h_v = \delta_v \cdot [L_v : \mathbf{Q}_p] + \begin{cases} 1, & \mu = 1, \\ 0, & \mu \neq 1. \end{cases}$$

We are now ready to conclude the proof of (7.8.1) in the case (3) of Proposition 7.9 (no longer distinguishing the cases $v \nmid p$ and $v \mid p$).

If u is generic, then the $\mathbf{F}[\Gamma_{L_v}]$-module $H_L(\overline{L}_v)$ is isomorphic to $T_v^-/\pi T_v^- = \mathbf{F}\otimes\mu$, which implies that the left hand side of (7.8.1) is equal to

$$(-1)^{h_v}\mu(\mathrm{rec}_{L_v}(-1)),$$

which is, in turn, equal to $\varepsilon_v(V)$.

If u is special, then the $\mathbf{F}[\Gamma_{L_v}]$-module $H_L(\overline{L}_v)$ is isomorphic to $T_v^+/\pi T_v^+ = \mathbf{F}(1)\otimes\mu$, hence $\det_{H_L} = \mu\overline{\chi}_{cycl,L_v,p}$. The formula (1.1.1) then implies that the left hand side of (7.8.1) is given by

$$(-1)^{h_v}\mu(\mathrm{rec}_{L_v}(-1))(-1)^{\delta_v\cdot[L_v:\mathbf{Q}_p]} = (-1)^{h'_v}\mu(\mathrm{rec}_{L_v}(-1)),$$

which is again equal to $\varepsilon_v(V)$.

(4) The arguments from [CFKS, 2.17] apply. The assumptions imply that $H^1(I_v,T)_{\mathrm{tors}} = H^1(I_v,T')_{\mathrm{tors}} = 0$, hence $\mathrm{Tam}^0_{\omega_v}(T') = \mathrm{Tam}^0_{\omega_v}(T) = 1$ and $h_v = 0$. According to [CFKS, Lemma 2.14(4)] (and its proof) there exists a free $\mathcal{O}$-module U of rank $\dim_{\mathcal{K}}(V)/2$ equipped with a continuous action of W_{L_v} such that the semisimplification of $U/\pi U$ is isomorphic to the semisimplification of $H_L|_{W_{L_v}}$. According to [D, Thm. 6.5], modified ε-constants ε_0 respect congruences modulo π, hence

$$\varepsilon_v(V)\det(-\mathrm{Fr}(v)\mid V^{I_v}) \equiv \varepsilon(U\oplus U^*(1))\det(-\mathrm{Fr}(v)\mid (U\oplus U^*(1))^{I_v}) \pmod{\pi}.$$

The congruences

$$\varepsilon(U\oplus U^*(1)) \pmod{\pi} = \det_U(\mathrm{rec}_{L_v}(-1)) \pmod{\pi} = \det_{H_L}(\mathrm{rec}_{L_v}(-1)) \in \{\pm 1\}\subset \mathbf{F}^\times,$$
$$\det(-\mathrm{Fr}(v)\mid V^{I_v}) \pmod{\pi} = \det(-\mathrm{Fr}(v)\mid \overline{T}^{I_v}) = \det(-\mathrm{Fr}(v)\mid (U\oplus U^*(1))^{I_v}) \pmod{\pi} \in \mathbf{F}^\times$$

imply that $\varepsilon_v(V) \equiv \det_{H_L}(\mathrm{rec}_{L_v}(-1)) \pmod{\pi}$, hence $\varepsilon_v(V) = \det_{H_L}(\mathrm{rec}_{L_v}(-1))$, since $1 \neq -1 \in \mathbf{F}^\times$.

(5) Thanks to Proposition 5.3 we can assume that the extension $K(v)/L_v$ is totally tamely ramified. By assumption, there exist $G, G' \in (\mathcal{O}-\mathrm{div}/O_{K(v)})_{dd,K(v)/L_v}$ such that $T = T_\pi G$ and $T' = T_\pi G'$; then $\overline{T} = G[\pi]$ and there exists an exact sequence

$$0 \longrightarrow H \longrightarrow G[\pi] \longrightarrow H^D \longrightarrow 0$$

in $H \in (\mathbf{F}-\mathrm{vs}/O_{K(v)})_{dd,K(v)/L_v}$ whose generic fibre is given by the right exact sequence in (7.7.1). Moreover, there are exact sequences of finite flat group schemes over $O_{K(v)}$ (with descent data relative to $L_v/K(v)$)

$$0 \longrightarrow H \longrightarrow G[\pi^n] \longrightarrow G'[\pi^n]$$

whose generic fibres give rise, in the limit, to the left exact sequence in (7.7.1). The discussion in 1.4 and 4.10 implies that the exact sequence (7.7.2) extends to an exact sequence

$$0 \longrightarrow H^0(L_v,T) \longrightarrow H^0(L_v,T') \longrightarrow H^0_{fl}(O_{K(v)},H)^\Delta \longrightarrow H^1_f(L_v,T) \longrightarrow$$
$$H^1_f(L_v,T') \longrightarrow H^1_{fl}(O_{K(v)},H)^\Delta \longrightarrow 0,$$

where $\Delta = \mathrm{Gal}(K(v)/L_v)$. As a result,

$$h_v = \dim_{\mathbf{F}} H^1_{fl}(O_{K(v)},H)^\Delta - \dim_{\mathbf{F}} H^0_{fl}(O_{K(v)},H)^\Delta = -\chi_{\mathbf{F}}(O_{L_v},H),$$

in the notation of Proposition 4.13. The formula (7.8.1) was proved in this case in Proposition 4.29.

(7.10) Theorem (= Theorem F). *If, in the situation of 7.7, the following conditions are satisfied:*
(i) *for each $v \in S_f \smallsetminus S_p$ either there exist a finite abelian extension $L(v)/L_v$ and a finite Galois extension $K(v)/L(v)$ such that $p \nmid [K(v):L(v)]$ and $T|_{\Gamma_{K(v)}}$ is unramified, or $\dim_{\mathcal{K}}(V) = 2$ and $WD(V_v)$ has nontrivial monodromy;*

(ii) *for each $v \in S_p$ either there exists a finite abelian extension $K(v)/L_v$ such that $T|_{\Gamma_{K(v)}}$ is a Barsotti–Tate representation, or* $\dim_{\mathcal{K}}(V) = 2$ *and $WD(V_v)$ has nontrivial monodromy; then*

$$(-1)^{\chi_f(L,V)} = \varepsilon(V).$$

Proof. After replacing L by a suitable abelian extension of p-power degree (using the arguments from the proof of Theorem 6.7) we can assume that $p \nmid [L(v) : L_v]$ in (i) and $K(v)/L_v$ is tamely ramified in (ii). The formula (7.8.1) holds for all $v \in S_\infty$ (by Proposition 7.9(1),(2)), all $v \in S_f \smallsetminus S_p$ (by Proposition 7.9(3),(4)) and all $v \in S_p$, by Proposition 7.9(3),(5). We conclude by (7.8.2).

8. The parity conjecture for Selmer groups of Hilbert modular forms of weight two

(8.1) Let F be a totally real number field and f a cuspidal Hilbert modular newform over F of level $\mathfrak{n}$, parallel weight 2 and trivial character. The field K_f generated over $\mathbf{Q}$ by the Hecke eigenvalues $\lambda_f(v) = \lambda_f(T(v))$ $(v \nmid \mathfrak{n})$ of f is a totally real finite extension of $\mathbf{Q}$. For every prime number p and every prime $\mathfrak{p} \mid p$ in K_f one can attach to f an absolutely irreducible continuous two-dimensional representation $V_{\mathfrak{p}}(f)$ of $\Gamma_F = \mathrm{Gal}(\overline{F}/F)$ with coefficients in any fixed finite extension $\mathcal{K}$ of $(K_f)_{\mathfrak{p}}$, characterised by the fact that

$$\forall v \nmid p\mathfrak{n} \qquad \det(1 - X\,\mathrm{Fr}_{\mathrm{geom}}(v) \mid V_{\mathfrak{p}}(f)) = 1 - \lambda_f(v)X + (Nv)X^2. \tag{8.1.1}$$

The Tate twist $V := V_{\mathfrak{p}}(f)(1)$ admits a nondegenerate Γ_F-equivariant skew-symmetric pairing $\langle\ ,\ \rangle : V \times V \longrightarrow \mathcal{K}(1)$ and any Γ_F-stable $\mathcal{O}$-lattice $T \subset V$ $(\mathcal{O} = O_{\mathcal{K}})$ becomes self-dual $T \xrightarrow{\sim} T^*(1)$ if we multiply the pairing by a suitable scalar in $\mathcal{K}^*$. Note that we use a cohomological, rather than a homological, normalisation of $V_{\mathfrak{p}}(f)$: in the case when $F = \mathbf{Q}$ and $f = \sum_{n\geq 1} a_n q^n$ $(a_n \in \mathbf{Q},\ a_1 = 1)$ corresponds to the isogeny class of an elliptic curve E defined over $\mathbf{Q}$, then $K_f = \mathbf{Q}$, $\mathfrak{p} = p$, $\lambda_f(\ell) = a_\ell$ for all prime numbers $\ell \nmid N_E$, $V_{\mathfrak{p}}(f) := H^1_{\acute{e}t}(E_{\overline{\mathbf{Q}}}, \mathbf{Q}_p) = V_p(E)^* \simeq V_p(E)(-1)$ (for $\mathcal{K} = \mathbf{Q}_p$) and $V = V_p(E) = T_p(E) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$.

Denote by $\pi(f)$ the automorphic representation of $PGL_2(\mathbf{A}_F)$ attached to f ([N1, §12.3]); the corresponding Euler factors are related by

$$\forall v \nmid \infty p\mathfrak{n} \qquad L_v(\pi(f), s + 1/2) = L_v(f, s + 1) = L_v(V_{\mathfrak{p}}(f), s + 1) = L_v(V, s) \tag{8.1.2}$$

(which boils down to (8.1.1) if $v \nmid p\mathfrak{n}$). The archimedean factors are given by

$$\forall v \mid \infty \qquad L_v(\pi(f), s - 1/2) = L_v(f, s) = 2(2\pi)^{-s}\Gamma(s), \qquad \varepsilon_v(\pi(f), 1/2) = -1.$$

(8.2) More precisely, the following local compatibilities are satisfied, for all primes $v \nmid \infty$ of F ([Ca, Thm. A], [T2, Thm. 1.6], [Sa, Thm. 1], [B2, Thm. 1], [Sk, Thm. 1]). Let $V_{\mathfrak{p}}(f)_v := V_{\mathfrak{p}}(f)|_{\Gamma_{F_v}}$ and $V_v := V_{\mathfrak{p}}(f)_v(1)$.

(8.2.1) If $v \mid p$, then V_v is a de Rham representation of Γ_{F_v}, with Hodge–Tate weights contained in $\{0, 1\}$.

(8.2.2) The Frobenius-semisimplification $WD(V_{\mathfrak{p}}(f)_v)^{f-ss}$ of the Weil-Deligne representation attached to $V_{\mathfrak{p}}(f)_v$ if $v \nmid p$ (resp. to $D_{\mathrm{pst}}(V_{\mathfrak{p}}(f)_v)$ if $v \mid p$) corresponds to $\pi(f)_v$ under the local Langlands correspondence ([BH, Thm. 35.1]).

(8.2.3) If $v \mid p$ and $v \nmid \mathfrak{n}$, then $\pi(f)_v$ is an unramified principal series representation; the Galois representation V_v is crystalline with Hodge–Tate weights contained in $\{0, 1\}$, hence Barsotti–Tate [B3, Thm. 5.3.2].

(8.2.4) If $\pi(f)_v = i_B^G(\chi_1, \chi_2)$ $(\chi_i : F_v^\times \longrightarrow \overline{\mathbf{Q}}^\times)$ is a principal series representation (normalised induction from the upper-triangular Borel subgroup B to $G = GL_2(F_v)$), then $WD(V_v)^{f-ss} = \psi_1 \oplus \psi_2$ $(\psi_i : W_{F_v}^{ab} \longrightarrow \overline{\mathbf{Q}}^\times)$, where $\chi_i|\cdot|^{1/2} = \psi_i \circ \mathrm{rec}_{F_v}$. This implies – thanks to (8.2.3) and cyclic base change for Hilbert modular forms if $v \mid p$ ([Sk, §2.2]) – that there exists an abelian extension $K(v)/F_v$ such that the representation $V_v|_{\Gamma_{K(v)}}$ is unramified if $v \nmid p$ (resp. Barsotti–Tate if $v \mid p$). If the finite order characters $\psi_i|_{I_v}$ have orders prime to p, then one can choose $K(v)$ such that $p \nmid [K(v) : F_v]$.

(8.2.5) $\varepsilon_v(V) = \varepsilon(V_{\mathfrak{p}}(f)_v(1)) = \varepsilon(\pi(f)_v, 1/2) = \varepsilon_v(\pi(f), 1/2)$.

(8.2.6) $WD(V_{\mathfrak{p}}(f)_v)$ is pure of weight 1 [Bl], hence $H^0(F', V_{\mathfrak{p}}(f)(1)) = 0$, for all finite extensions F'/F.

(8.3) Digression on representations of GL_2. Let ℓ be a prime number and E a finite extension of $\mathbf{Q}_\ell$, with ring of integers O_E and residue field k_E.

Let $G = GL_2(E)$, $K = GL_2(O_E) \supset K_1 = \mathrm{Ker}(K \longrightarrow \overline{G} = GL_2(k_E))$. Denote by $B \subset G$ and $\overline{B} \subset \overline{G}$ the standard upper-triangular Borel subgroups.

Let Π be a nonzero smooth admissible complex representation of G. For every open compact subgroup $U \subset G$ the restriction $\Pi|_U$ is a direct sum of irreducible finite-dimensional smooth representations of U (each of which factors through U/U', for some open subgroup $U' \subset U$). We say that a nonzero irreducible finite-dimensional smooth representation of U is a **type of** Π if it occurs in $\Pi|_U$.

(8.4) Proposition. *The irreducible smooth representations Π of G of dimension $\dim(\Pi) > 1$ satisfying $\Pi^K = 0 \neq \Pi^{K_1}$ are the following ones.*
(1) *A principal series representation $\Pi = i_B^G(\chi_1, \chi_2)$ (normalised induction), where the restriction to $O_E^\times$ of each χ_i factors as $\chi_i|_{O_E^\times} : O_E^\times \longrightarrow k_E^\times \xrightarrow{\overline{\chi}_i} \mathbf{C}^\times$, and $\overline{\chi}_1 \neq 1$ or $\overline{\chi}_2 \neq 1$ (in other words, Π is a tame principal series representation).*
(2) *A twisted Steinberg representation $\Pi = St \otimes \chi$, where $\chi|_{O_E^\times} : O_E^\times \longrightarrow k_E^\times \xrightarrow{\overline{\chi}} \mathbf{C}^\times$.*
(3) *A level 0 cuspidal representation [BH, Prop. 12.6].*
The group $K/K_1 = \overline{G}$ acts on Π^{K_1} as follows.
(1) $\Pi^{K_1} = I_{\overline{B}}^{\overline{G}}(\overline{\chi}_1, \overline{\chi}_2)$.
(1a) *If $\overline{\chi}_1 = \overline{\chi}_2$ (which is equivalent to $\Pi \otimes \chi_1^{-1}$ being an unramified principal series representation), then $\Pi^{K_1} = (\overline{\chi}_1 \circ \det) \oplus (\overline{St} \otimes \overline{\chi}_1)$, where $\overline{St} = \mathbf{C}[\mathbf{P}^1(k_E)]/\mathbf{C}$ is an irreducible representation of $\overline{G}$ of dimension $|k_E|$;*
(1b) *if $\overline{\chi}_1 \neq \overline{\chi}_2$ (in other words, if no twist $\Pi \otimes \chi$ is an unramified principal series representation), then Π^{K_1} is an irreducible principal series representation of $\overline{G}$.*
(2) $\Pi^{K_1} = \overline{St} \otimes \overline{\chi}$.
(3) Π^{K_1} *is an irreducible cuspidal representation of $\overline{G}$.*

Proof. Combine [BH, 6.3 Cor. 1] with [BH, Thm. 11.5, Prop. 12.6, Prop. 14.3, Thm. 14.5].

(8.5) Corollary. *Let Π' be an irreducible smooth representation of G of dimension $\dim(\Pi') > 1$. If $\Pi = i_B^G(\chi_1, \chi_2)$ is a tame principal series representation as in Proposition 8.4(1) such that the type $I_{\overline{B}}^{\overline{G}}(\overline{\chi}_1, \overline{\chi}_2)$ in the case 8.4(1a) (resp. the type $(\overline{\chi}_1 \circ \det)$ in the case 8.4(1b)) occurs in $\Pi'|_K$, then $\Pi' = i_B^G(\chi_1', \chi_2')$ with $\chi_i'|_{O_E^\times} = \chi_i|_{O_E^\times}$ $(i = 1, 2)$. In other words, Π' is also a tame principal series representation.*

Proof. This follows directly from Proposition 8.4.

(8.6) The conjectures of Bloch and Kato ([BK, Conj. 5.3], [FoPR, III.4.2.2]) predict that the dimension $\chi_f(F, V_\mathfrak{p}(f)(1)) = h_f^1(F, V_\mathfrak{p}(f)(1)) := \dim_\mathcal{K} H_f^1(F, V_\mathfrak{p}(f)(1))$ should be equal to

$$h_f^1(F, V_\mathfrak{p}(f)(1)) \stackrel{?}{=} \mathrm{ord}_{s=1} L(f, s) = \mathrm{ord}_{s=1/2} L(\pi(f), s)$$

(the second equality follows from the fact that $\mathrm{ord}_{s=1/2} L_v(\pi(f), s) = 0$ for all $v \mid \infty$). The (mod 2) version of this conjecture

$$h_f^1(F, V_\mathfrak{p}(f)(1)) \stackrel{?}{\equiv} \mathrm{ord}_{s=1} L(f, s) = \mathrm{ord}_{s=1/2} L(\pi(f), s) \pmod 2$$

is equivalent to

$$(-1)^{h_f^1(F, V_\mathfrak{p}(f)(1))} \stackrel{?}{=} (-1)^{\mathrm{ord}_{s=1/2} L(\pi(f), s)} = \varepsilon(\pi(f), 1/2) = \prod_v \varepsilon_v(V_\mathfrak{p}(f)(1)) \tag{8.6.1}$$

(by the functional equation for $L(\pi(f), s)$), if we define $\varepsilon_v(V_\mathfrak{p}(f)(1)) := \varepsilon(\pi(f)_v, 1/2) = -1$ for all $v \mid \infty$.

(8.7) Theorem (= Theorem C). *If $p \neq 2$, then*

$$\dim_\mathcal{K} H_f^1(F, V_\mathfrak{p}(f)(1)) \equiv \mathrm{ord}_{s=1} L(f, s) \pmod 2$$

holds, for every cuspidal Hilbert modular newform f over F of parallel weight 2 and trivial character.

Proof. This was proved in [N5, Thm. 1.4] if $2 \nmid [F : \mathbf{Q}]$ or if $\pi(f)_v$ is not a principal series representation for some finite prime v of F. We reduce the general case to this particular instance using Theorem B (=

Theorem 6.7) and the level raising techniques that were employed in [N5, Thm. 3.5] to deduce the congruence in Theorem 8.7 from [N5, Thm. 1.4] in most non CM cases and many CM cases. However, the argument below will be more direct in the sense that it will not appeal to [N4, Thm. B(c)], the proof of which is fairly involved.

Firstly, throughout the proof we are free to replace $\mathcal{K}$ by a finite extension. Secondly, we can assume that $2 \mid [F : \mathbf{Q}]$ and that $\pi(f)_v$ is a principal series representation, for each $v \nmid \infty$. The arguments used in the proof of Theorem 6.7 imply, thanks to (8.2.4), that there exists an abelian extension F'/F of p-power degree (necessarily totally real) such that $V_{\mathfrak{p}}(f)(1)$ will become unramified (resp. Barsotti–Tate) over a finite abelian extension $K(w)/F'_w$ of degree prime to p, for each prime $w \nmid \infty p$ (resp. $w \mid p$) of F'. We can replace F by F' and f by its (necessarily cuspidal) base change to F'.

After this reduction step the representation $V = V_{\mathfrak{p}}(f)(1)$ of $\Gamma_{F,S}$ (where $S = \{v \mid \infty p\mathfrak{n}\}$) will satisfy conditions (i) and (ii) of Theorem 7.10 (with $L = F$ and all finite abelian extensions $K(v)/L_v$ in Theorem 7.10(ii) being tamely ramified). On the automorphic side, the "tamely ramified" condition corresponds to the fact that, for each $v \mid p$, the representation $\pi(f)_v$ of $GL_2(F_v)$ is a tame principal series representation, i.e., is of the form described in Proposition 8.4(1).

If the residual representation $\overline{T} := T/\pi T$ is reducible, then (8.6.1) holds, by Theorem 7.10.

It remains to treat the case when $\overline{T}$ is irreducible (hence absolutely irreducible, since the complex conjugation at any infinite prime of F acts on $\overline{T}$ with two distinct eigenvalues $\pm 1 \in \mathbf{F}$).

According to [BDJ, Lemma 2.9 and its proof], there exist

(8.7.1) a prime $v_0 \nmid \infty p\mathfrak{n}$ of F;
(8.7.2) a cuspidal Hilbert newform f' of weight 2 of level dividing $\mathfrak{n}v_0$ and divisible by v_0;
(8.7.3) a prime $\mathfrak{p}' \mid \mathfrak{p}$ in $K_{f'}$;
(8.7.4) a finite extension $\mathcal{K}$ of $\mathbf{Q}_p$ equipped with fixed embeddings $(K_f)_{\mathfrak{p}} \hookrightarrow \mathcal{K} \hookleftarrow (K_{f'})_{\mathfrak{p}'}$

with the following properties:

(8.7.5) The form f' has trivial character (by taking $\psi = 1$ in the proof of [BDJ, Lemma 2.9]).
(8.7.6) The automorphic representation $\pi(f')$ of $PGL_2(\mathbf{A}_F)$ attached to f' has the following property. For each $v \mid p$, the representation $\pi(f')_v$ of $GL_2(F_v)$ contains the following type of $K_{v,1} = \mathrm{Ker}(GL_2(O_{F_v}) \longrightarrow GL_2(k(v)))$ (where $k(v)$ is the residue field of v): the type $I_{\overline{B}}^{\overline{G}}(\overline{\chi}_1, \overline{\chi}_2)$ if $\pi(f)_v$ is as in the case (1a) of Proposition 8.4 (resp. the type $(\overline{\chi}_1 \circ \det)$ if $\pi(f)_v$ is as in the case (1b) of Proposition 8.4).
(8.7.7) The two-dimensional Galois representations $V = V_{\mathfrak{p}}(f)(1)$ and $V' = V_{\mathfrak{p}'}(f')(1)$ of Γ_F with coefficients in $\mathcal{K}$ admit Γ_F-stable $\mathcal{O}_{\mathcal{K}}$-lattices $T \subset V$ and $T' \subset V'$ such that the residual representations $\overline{T} = T/\pi T$ and $\overline{T}' = T'/\pi T'$ of Γ_F have isomorphic semisimplifications.

According to Corollary 8.5, condition (8.7.6) implies that

(8.7.8) for each $v \mid p$, $\pi(f')_v$ is as in Proposition 8.4(1).

As a result, the representation V' becomes Barsotti–Tate over a tamely ramified abelian extension of F_v, for all $v \mid p$.

After rescaling the pairings $V \times V \longrightarrow \mathcal{K}(1)$ and $V' \times V' \longrightarrow \mathcal{K}(1)$ we can assume that they induce isomorphisms $T \xrightarrow{\sim} T^*(1)$ and $T' \xrightarrow{\sim} T'^*(1)$. Condition (8.7.7) combined with the absolute irreducibility of $\overline{T}$ imply that, after rescaling the pairing $\langle\ ,\ \rangle : T \times T \longrightarrow \mathcal{O}'(1)$ by an element of $\mathcal{O}^\times$, there exists an isomorphism $\overline{T} \xrightarrow{\sim} \overline{T}'$ compatible with the pairings on T and T'.

Therefore the representations T and T' of $\Gamma_{F,S\cup\{v_0\}}$ satisfy the assumptions of Theorem 6.7, hence

$$(-1)^{\chi_f(F,V)}/\varepsilon(V) = (-1)^{\chi_f(F,V')}/\varepsilon(V').$$

The right hand side is equal to 1, by [N5, Thm. 1.4] (since $\pi(f')_{v_0}$ is an unramified twist of the Steinberg representation), which means that (8.6.1) holds, as claimed. Theorem 8.7 is proved.

(8.8) As pointed out by the referee of the present article, the level raising argument in the proof of [N5, Thm. 3.5] (which combined [T1, Thm. 1] with [DS, Lemme 6.11]) needs to be made more precise to ensure that the form g in the proof of [loc. cit.] has trivial character. As above, this follows from the proof of [BDJ, Lemma 2.9]. Equivalently, one can replace the space of functions on $D^\times \backslash \widehat{D}^\times / U$ in the proof of [T1, Thm. 1] (for the trivial local system $L_k = \mathbf{C}$) by the space of functions on $D^\times \backslash \widehat{D}^\times / \widehat{F}^\times U$ (cf. [N4, §1.1, 1.2]).

(8.9) Theorem (= Theorem D). *Let A be an abelian variety with real multiplication by O_M (where M is a totally real number field of degree $[M : \mathbf{Q}] = \dim(A)$) defined over a totally real number field F. If $\mathfrak{p} \mid p$ in M and $p \neq 2$, then*

$$\dim_{M_\mathfrak{p}} H^1_f(F, V_\mathfrak{p}(A)) = \mathrm{rk}_{O_M} A(F) + \mathrm{cork}_{O_{M_\mathfrak{p}}} Ш(A/F)[\mathfrak{p}^\infty] \equiv \mathrm{ord}_{s=1} L(\iota A/F, s) \pmod 2$$

holds, for every $\iota : M \hookrightarrow \mathbf{R}$.

Proof. As explained in [N1, 12.11.6], [N5, 4.2] and [N6, 4.13], this is a consequence of Theorem 8.7, potential modularity of A [BLGGT, Cor. 5.4.2, Cor. 5.4.3] and Solomon's induction theorem [CR, Thm. 15.10].

(8.10) Theorem (= Theorem E). *Let E be an elliptic curve defined over a totally real number field F. If $p \neq 2$, then*

$$\dim_{\mathbf{Q}_p} H^1_f(F, V_p(E)) = \mathrm{rk}_{\mathbf{Z}} E(F) + \mathrm{cork}_{\mathbf{Z}_p} Ш(E/F)[p^\infty] \equiv \mathrm{ord}_{s=1} L(E/F, s) \pmod 2.$$

Proof. This is a special case of Theorem 8.9 when $M = \mathbf{Q}$. Potential modularity of E is proved in [W, Thm. A.1].

References

[AT] E. Artin, J. Tate, *Class field theory*, Second ed., Addison-Wesley, Redwood City, 1990.

[BLGGT] T. Barnet-Lamb, T. Gee, D. Geraghty, R. Taylor, *Potential automorphy and change of weight*, Annals of Math. (2) **179** (2014), 501–609.

[Bl] D. Blasius, *Hilbert modular forms and the Ramanujan conjecture*, in: Noncommutative geometry and number theory, Aspects Math. E37, Vieweg, Wiesbaden, 2006, 35–56.

[BCDT] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$, J. Amer. Math. Soc. **14** (2001), 843–939.

[BS] B. Birch, N. Stephens, *The parity of the rank of the Mordell-Weil group*, Topology **5** (1966), 295–299.

[BK] S. Bloch, K. Kato, *L-functions and Tamagawa numbers of motives*, in: The Grothendieck Festschrift I, Progress in Mathematics **86**, Birkhäuser, Boston, Basel, Berlin, 1990, pp. 333–400.

[B1] C. Breuil, *Une application du corps des normes*, Compositio Math. **117** (1999), 189–203.

[B2] C. Breuil, *Une remarque sur les représentations locales p-adiques et les congruences entre formes modulaires de Hilbert*, Bull. Soc. Math. de France **127** (1999), 459–472.

[B3] C. Breuil, *Groupes p-divisibles, groupes finis et modules filtrés*, Annals of Math. (2) **152** (2000), 489–549.

[B4] C. Breuil, *Integral p-adic Hodge theory*, in: Algebraic Geometry 2000, Azumino, Advanced Studies in Pure Math. **36**, Math. Soc. Japan, 2002, pp. 51–80.

[BH] C. Bushnell, G. Henniart, *The local Langlands conjecture for GL(2)*, Grundlehren der mathematischen Wissenschaften **335**, Springer, Berlin, 2006.

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

[Ca] H. Carayol, *Sur les représentations ℓ-adiques associées aux formes modulaires de Hilbert*, Ann. Sci. E.N.S. (4) **19** (1986), 409–468.

[C1] J.W.S. Cassels, *Arithmetic of curves of genus 1 (VIII). On the conjectures of Birch and Swinnerton-Dyer*, J. reine angew. Math. **217** (1965), 180–189.

[C2] J.W.S. Cassels, *Diophantine equations with special reference to elliptic curves*, J. London Math. Soc. **41** (1966), 193–291.

[Č] K. Česnavičius, *The p-parity conjecture for elliptic curves with a p-isogeny*, J. reine angew. Math. **719** (2016), 45–73.

[Ch] S. Chetty, *Comparing local constants of elliptic curves in dihedral extensions*, Funct. Approx. Comment. Math. **54** (2016), 241–250.

[CFKS] J. Coates, T. Fukaya, K. Kato, R. Sujatha, *Root numbers, Selmer groups and non-commutative Iwasawa theory*, J. Alg. Geom. **19** (2010), 19–97.

[CR] C.W. Curtis, I. Reiner, *Methods of Representation Theory, Vol. I*, Wiley, New York, 1981.

[D] P. Deligne, *Les constantes des équations fonctionnelles des fonctions L*, in: Modular functions of one variable II (Antwerp, 1972), Lect. Notes in Math. **349**, Springer, Berlin, 1973, pp. 501–597.

[DS] P. Deligne, J.-P. Serre, *Formes modulaires de poids* 1, Ann. Sci. E.N.S. (4) **7** (1974), 507–530.

[DD1] T. Dokchitser, V. Dokchitser, *Ranks of elliptic curves with a cyclic isogeny*, J. Number Theory **128** (2008), 662–679.

[DD2] T. Dokchitser, V. Dokchitser, *Root numbers and parity of ranks of elliptic curves*, J. reine angew. Math. **658** (2011), 39–64.

[Fl] M. Flach, *A generalization of the Cassels-Tate pairing*, J. reine angew. Math. **412** (1990), 113–127.

[Fo1] J.-M. Fontaine, *Représentations p-adiques des corps locaux*, in: The Grothendieck Festschrift II, Progress in Mathematics **87**, Birkhäuser, Boston, Basel, Berlin, 1990, pp. 249–309.

[Fo2] J.-M. Fontaine, *Représentations ℓ-adiques potentiellement semi-stables*, in: Périodes p-adiques (Bures-sur-Yvette, 1988), Astérisque **223** (1994), Soc. Math. de France, Paris, pp. 321–347.

[FoPR] J.-M. Fontaine, B. Perrin-Riou, *Autour des conjectures de Bloch et Kato: cohomologie galoisienne et valeurs de fonctions L*, in: Motives (Seattle, 1991), Proc. Symposia in Pure Math. **55/I**, American Math. Society, Providence, Rhode Island, 1994, pp. 599–706.

[K1] M. Kisin, *Crystalline Representations and F-crystals*, in: Algebraic Geometry and Number Theory, Progress in Mathematics **253**, Birkhäuser, Boston, 2006, pp. 459–496.

[K2] M. Kisin, *Moduli of finite flat group schemes, and modularity*, Ann. of Math. (2) **170** (2009), 1085–1180.

[K3] M. Kisin, *Integral models for Shimura varieties of abelian type*, J. Amer. Math. Soc. **23** (2010), 967–1012.

[KMR] Z. Klagsbrun, B. Mazur, K. Rubin, *Disparity in Selmer ranks of quadratic twists of elliptic curves*, Ann. of Math. (2) **178** (2013), 287–320.

[M] B. Mazur, *Local flat duality*, Amer. J. Math. **92**, (1970), 343–361.

[MRo] B. Mazur, L. Roberts, *Local Euler characteristics*, Invent. Math. **9** (1970), 201–234.

[MR] B. Mazur, K. Rubin, *Finding large Selmer rank via an arithmetic theory of local constants*, Ann. of Math. (2) **166** (2007), 581–614.

[Mi] J. Milne, *Arithmetic duality theorems*, Perspect. Math. **1**, Academic Press, Boston, 1986.

[N1] J. Nekovář, *Selmer complexes*, Astérisque **310** (2006), Soc. Math. de France, Paris.

[N2] J. Nekovář, *On the parity of ranks of Selmer groups III*, Doc. Math. **12** (2007), 243–274. Erratum: Doc. Math. **14** (2009), 191–194.

[N3] J. Nekovář, *On the parity of ranks of Selmer groups IV*, Compositio Math. **145** (2009), 1351–1359.

[N4] J. Nekovář, *Level raising and anticyclotomic Selmer groups for Hilbert modular forms of weight two*, Canadian J. Math **64** (2012), 588–668.

[N5] J. Nekovář, *Some consequences of a formula of Mazur and Rubin for arithmetic local constants*, Algebra and Number Theory **7** (2013), 1101–1120.

[N6] J. Nekovář, *Compatibility of arithmetic and algebraic local constants (the case $\ell \neq p$)*, Compositio Math. **151** (2015), 1626–1646.

[NSW] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of Number Fields*, Grund. Math. Wiss. **323**, Springer, Berlin, 2000.

[NY] J. Newton, T. Yoshida, *Shimura curves, the Drinfeld curve and Serre weights*, `https://nms.kcl.ac.uk/james.newton/ccny.pdf`

[R] M. Raynaud, *Schémas en groupes de type* $(p, \ldots, p)$, Bull. S.M.F. **102** (1974), 241–280.

[Sa] T. Saito, *Hilbert modular forms and p-adic Hodge theory*, Compositio Math. **145** (2009), 1081–1113.

[Sav1] D. Savitt, *On a conjecture of Conrad, Diamond, and Taylor*, Duke Math. J. **128** (2005), 141–197.

[Sav2] D. Savitt, *Breuil modules for Raynaud schemes*, J. Number Theory **128** (2008), 2939–2950.

[Se1] J.-P. Serre, *Représentations linéaires des groupes finis*, Hermann, Paris, 1967.

[Se2] J.-P. Serre, *Local class field theory*, in: Algebraic Number Theory (J.W.S. Cassels, A. Fröhlich, eds.), Academic Press, London, 1967, pp. 128–161.

[Se3] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.

[Sk] C. Skinner, *A note on p-adic Galois representations attached to Hilbert modular forms*, Doc. Math. **14** (2009), 241–258.

[Ta] J. Tate, *p-divisible groups*, Proc. Conf. Local Fields (Driebergen, 1966), Springer, 1967, pp. 158–183.

[T1] R. Taylor, *On Galois representations associated to Hilbert modular forms*, Invent. Math. **98** (1989), 265–280.

[T2] R. Taylor, *On Galois representations associated to Hilbert modular forms II*, in: Elliptic Curves, Modular Forms and Fermat's Last Theorem (J. Coates and S. T. Yau, eds.), International Press, 1997, pp. 333–340.

[W] J.-P. Wintenberger, *Potential modularity of elliptic curves over totally real fields*, appendix to [N3].

Université Pierre et Marie Curie (Paris 6)
Institut de Mathématiques de Jussieu
Théorie des Nombres, Case 247
4, place Jussieu
F-75252 Paris cedex 05
FRANCE