Iwasawa Theory I

Ben Forrás

Oberseminar Arithmetische Geometrie, Regensburg

8 February 2024

These notes were written in preparation for my Oberseminar talk, providing an overview of §§7.1–7.3 of Rubin's book [Rub00], with a few remarks towards the rest of Chapter 7. I claim responsibility for all errors, mistakes and typos. All references point to Rubin. The numbering of theorems (but not of displayed equations) follows that of the book, and these numbers are provided for reference whenever appropriate.

1 Goals, strategy, and assumptions

Standing assumptions. $K/\mathbb{Q}$ number field, $\Phi/\mathbb{Q}_p$ finite extension with ring of integers $\mathcal{O}$ and residue field $\Bbbk = \mathcal{O}/\mathfrak{p}$. We have $\Gamma := \mathrm{Gal}(K_\infty/K) \simeq \mathbb{Z}_p^d$ and $\Lambda := \mathcal{O}[\![\Gamma]\!]$. The field F will always satisfy $K \subseteq_{\mathrm{f}} F \subset K_\infty$. We fix a p-adic representation T of G_{K_∞}, $V := T \otimes_{\mathcal{O}} \Phi$, $W := V/T = T \otimes_{\mathcal{O}} \mathbf{D}$, and $W_M := M^{-1}T/T \subseteq W$ for $0 \neq M \in \mathcal{O}$. Finally, let $\mathbf{c}$ be an Euler system for (T, K_∞).

Goals. We wish to prove the following three theorems on Euler systems, as stated in Talk 3:

Theorem 2.3.2. *Let* $\mathbf{c}$ *be an Euler system such that* $\mathrm{Hyp}(K_\infty, V)$ *holds. If* $\mathbf{c}_{K,\infty} = (\mathbf{c}_F)_F \in H^1_\infty(K,T)$ *is not torsion, then* X_∞ *is a torsion* Λ*-module (i.e. weak Leopoldt holds for* T*).*

Theorem 2.3.3. *Let* $\mathbf{c}$ *be an Euler system such that* $\mathrm{Hyp}(K_\infty, T)$ *and* $\mathrm{Hyp}(K_\infty/K)$ *hold. Then* $\mathrm{char}(X_\infty) \mid \mathrm{ind}_\Lambda(\mathbf{c})$*.*

Theorem 2.3.4. *Let* $\mathbf{c}$ *be an Euler system such that* $\mathrm{Hyp}(K_\infty, V)$ *and* $\mathrm{Hyp}(K_\infty/K)$ *hold. Then* $\mathrm{char}(X_\infty) \mid p^t \,\mathrm{ind}_\Lambda(\mathbf{c})$ *for some* $t \geq 0$*.*

The index of divisibility occurring in the last two statement measures divisibility of $\mathbf{c}_{K,\infty}$ by looking at its homomorphic images in Λ. Formally speaking, this means [Rub00, Definition 2.2.1]:

$$\mathrm{ind}_\Lambda(\mathbf{c}) := \left\{\varphi(\mathbf{c}_{K,\infty}) : \varphi(\mathbf{c}_{K,\infty}) \in \mathrm{Hom}_\Lambda(H^1_\infty(K,T), \Lambda)\right\} \subseteq \Lambda$$

We recall what the hypotheses mean, see [Rub00, p. 41]. The hypothesis $\mathrm{Hyp}(K_\infty, V)$ asserts the existence of an automorphism $\tau \in G_{K_\infty}$ acting trivially on μ_{p^∞}, $(\mathcal{O}_K^\times)^{1/p^\infty}$ and $K(\mathbf{1})$ such that $\dim_\Phi(V/(\tau-1)V) = 1$ and V is irreducible as a $\Phi[G_{K_\infty}]$-module. The hypothesis $\mathrm{Hyp}(K_\infty, T)$ is stronger: it's defined analogously, but we mandate $T/(\tau-1)T$ to be $\mathcal{O}$-free and $T \otimes \Bbbk$ to be irreducible over $\Bbbk[G_{K_\infty}]$.

The hypothesis $\mathrm{Hyp}(K_\infty/K)$ is only meaningful when $d = 1$ and when $G_{K_\infty} \curvearrowright V$ either trivially or by the cyclotomic character: in this case, it requires that

- either K is totally real and Leopoldt's conjecture holds for K,
- or K is imaginary quadratic.

For the rest of this talk, we assume $\mathrm{Hyp}(K_\infty, V)$, as this is required for all three theorems above. Furthermore, we assume that $\mathbf{c}_{K,\infty}$ is not a torsion element: this is explicitly assumed in Theorem 2.3.2, and follows from $\mathrm{Hyp}(K_\infty/K)$ for the other two. We also fix an automorphism τ as in $\mathrm{Hyp}(K_\infty, V)$.

Strategy. A very rough outline: we will first assume Theorem 2.3.2 along with two black-boxed statements, and use these to prove the two theorems on characteristic ideals. Then we will sketch a proof of Theorem 2.3.2. The two black boxes will remain unproven: their proof takes up the second half of Chapter 7.

There will be similarities between the proofs in this talk and that of the bound on the Selmer group seen in Talk 9 (Theorem 2.2.2). We will also enlist the help of derivative classes, again focusing on the class for $\mathfrak{r} = \mathbf{1}$, and at the end we will let M be a sufficiently large power of p. However, there is a key algebraic difference between the two setups: in that proof, we always worked over the field K, whereas here we need to work over extensions $K \subseteq_{\mathrm{f}} F \subset K_\infty$, which will also mean that instead of $\mathcal{O}$-modules, we have to deal with $\mathcal{O}[\mathrm{Gal}(F/K)]$-modules – this makes things more difficult.

2 Selmer sequences and Kolyvagin sequences

In this section, we make preparations for proving Theorems 2.3.3 and 2.3.4. We begin with some basic observations.

Definition 7.1.2. Let $(-)_{\mathrm{div}}$ denote the maximal divisible submodule of a module, and let Z resp. Z^* be the maximal G_{K_∞}-stable submodule of $(\tau-1)W$ resp. $(\tau-1)W^*$. Define $a_\tau := \left[W^{\tau=1} : \left(W^{\tau=1}\right)_{\mathrm{div}}\right] \cdot \max\{\#Z, \#Z^*\}$.

Lemma 7.1.3. *The quantity a_τ is finite. If $\mathrm{Hyp}(K_\infty, T)$ holds, then we even have $a_\tau = 1$.*

Remark. The proofs of Theorems 2.3.3 and 2.3.4 will be very similar. The difference between them is precisely the second assertion of Lemma 7.1.3: it will allow us to remove the p-factors.

Proof. Finiteness of a_τ is routine. We check that both factors are finite. For the first factor, recall that by definition, we have $W^* = \mathrm{Hom}_{\mathcal{O}}(T, \mathbf{D}(1))$, and thus $\mathrm{corank}_{\mathbb{Z}_p}(W) = \mathrm{rank}_{\mathbb{Z}_p}(W^*) = \mathrm{rank}_{\mathbb{Z}_p} \mathrm{Hom}_{\mathcal{O}}(T, \mathbf{D}(1))$ is finite, because T has finite $\mathcal{O}$-rank; since the $\mathbb{Z}_p$-coranks are finite, the index must also be finite. As for the second factor, consider $Z_{\mathrm{div}} \subseteq Z \subseteq (\tau-1)W$: since this is a divisible G_{K_∞}-submodule, it corresponds to a G_{K_∞}-stable subspace $V_0 \subseteq (\tau-1)V$. By $\mathrm{Hyp}(K_\infty, V)$ we have $(\tau-1)V \subsetneq V$, but $\mathrm{Hyp}(K_\infty, V)$ also asserts irreducibility of V, hence $V_0 = 0$, and consequently $Z_{\mathrm{div}} = 0$ and Z is finite. The same argument works for Z^*. Hence $a_\tau < \infty$.

We show $a_\tau = 1$, checking that both factors are 1. As for the first one, it is true in general that $W^{\tau=1}/(W^{\tau=1})_{\mathrm{div}}$ and $(T/(\tau-1)T)_{\mathrm{tors}}$ have the same length over $\mathcal{O}$ (see A.2.5, the proof is via Herbrand quotients; we have already used this in Talk 9); here $\mathrm{Hyp}(K_\infty, T)$ shows that the latter is 1. Turning to the second factor, and writing $\mathfrak{p} \subset \mathcal{O}$ for the maximal ideal, the assumption $\mathrm{Hyp}(K_\infty, T)$ implies that have that $W_{\mathfrak{p}}$ is an irreducible G_{K_∞}-module. Since $W_M/(\tau-1)W_M$ is a free $\mathcal{O}/M\mathcal{O}$-module of rank 1 by $\mathrm{Hyp}(K_\infty, V)$, the module $W_{\mathfrak{p}}$ cannot be contained in $(\tau-1)W$. It follows from the definition that $Z = 0$, and similarly $Z^* = 0$. □

Definition 7.1.1. Recall that $V^* := \mathrm{Hom}_{\mathcal{O}}(V, \Phi(1))$. Since $\tau \curvearrowright \mu_{p^\infty}$ trivially, we have

$$\dim_\Phi(V^*/(\tau-1)V^*) = \dim_\Phi(V/(\tau-1)V) = 1$$

by using $\mathrm{Hyp}(K_\infty, V)$. Recalling that $W^* = V^*/T^*$, we may thus fix an isomorphism

$$\vartheta^* : W^*/(\tau-1)W^* \xrightarrow{\sim} \mathbf{D} := \Phi/\mathcal{O}.$$

Recall that $\Omega := K(\mathbf{1})K(\mu_{p^\infty}, (\mathcal{O}_K^\times)^{1/p^\infty})K(W)$ where $K(\mathbf{1})$ is the maximal p-extension of K inside its Hilbert class field, and $K(W)$ is the smallest extension of K such that $G_{K(W)} \curvearrowright W$ is trivial. Set $\Omega_\infty := \Omega K_\infty$. We define an evaluation map

$$\begin{aligned} \mathrm{Ev}^* : G_{\Omega_\infty^{\langle\tau\rangle}} &\to \mathrm{Hom}\left(\mathcal{S}_{\Sigma_p}(K_\infty, W^*), \mathbf{D}\right) =: X_\infty \\ \sigma &\mapsto \Big(c \mapsto \vartheta^*(c(\sigma))\Big) \end{aligned}$$

Using $\mathrm{Hyp}(K_\infty, V)$, it is easily seen that Ev^* is well-defined, and the cocycle condition for c shows it to be a homomorphism.

For the rest of this section, we assume the validity of Theorem 2.3.2, so that X_∞ is a torsion Λ-module. Then X_∞ has characteristic ideal $\mathrm{char}\, X_\infty = \prod_{i=1}^r f_i\Lambda$ where the factors f_i are uniquely determined up to $\Lambda^\times$ by the condition $f_{i+1} \mid f_i$ via the elementary divisor theorem.

Proposition 7.1.7. *There exist elements $z_1, \ldots, z_r \in X_\infty$ and ideals $\mathfrak{g}_1, \ldots, \mathfrak{g}_r \subseteq \Lambda$ such that for all $1 \le k \le r$:*

(1) $z_k \in \mathrm{Ev}^*(\tau G_{\Omega_\infty})$;

(2) $a_\tau \mathfrak{g}_k \subseteq f_k\Lambda$, *and* $\mathfrak{g}_1 \subseteq \mathfrak{g}_2 \subseteq \ldots \subseteq \mathfrak{g}_r$;

(3) *there is a split exact sequence*

$$0 \to \sum_{i=1}^{k-1} \Lambda z_i \to \sum_{i=1}^{k} \Lambda z_i \to \Lambda/\mathfrak{g}_k \to 0;$$

(4) $a_\tau \cdot X_\infty \big/ \sum_{i=1}^r \Lambda z_i$ *is a pseudo-null Λ-module.*

Remark. Without the first condition, this is easy: let $\mathfrak{g}_k := f_k\Lambda$. The difficulty is to have z_k in the image of the evaluation map.

From now on, fix a sequence $(z_k)_k$ as above; this is necessary because it need not be unique. Let

$$Z_\infty := \sum_{i=1}^{r} \Lambda z_i \subseteq X_\infty$$

Write $\mathcal{M} \subseteq \Lambda$ for the unique maximal ideal.

Definition 7.1.8. A *Selmer sequence* of length $0 \le k \le r$ is a tuple $\boldsymbol{\sigma} = (\sigma_i)_i \in (\tau G_{\Omega_\infty})^k$ such that $\mathrm{Ev}^*(\sigma_i) - z_i \in \mathcal{M}Z_\infty$ for all $1 \le i \le k$.

Remark. Selmer sequences exist by Proposition 7.1.7: for instance, let σ_k be any preimage of z_k under Ev^*, and then $\mathrm{Ev}^*(\sigma_k) - z_k = 0 \in \mathcal{M}Z_\infty$. Of course, this is not that impressive.

We now introduce Kolyvagin sequences, which are associated with *interesting* Selmer sequences.

From now on, $M \in p^{\mathbb{N}_0}$ will always denote a power of p. Let

$$\Omega_M := K(\mathbf{1})K(W_M)K(\mu_M, (\mathcal{O}_K^\times)^{1/M}).$$

The field F will always satisfy $K \subseteq_{\mathrm{f}} F \subset K_\infty$, and we write $L_{F,M}$ for the fixed field of

$$\bigcap_{c \in \mathcal{S}_{\Sigma_p(F,W_M^*)}} \ker((c)_{F\Omega_M}) \subseteq G_{F\Omega_M}.$$

One checks that $L_{F,M}/F\Omega_M$ is finite abelian, and that $L_{F,M}/K$ is finite Galois.

Definition. A *Kolyvagin sequence* for F and M is a k-tuple $\boldsymbol{\pi} = (\mathfrak{q}_i)_i$ of primes of K with $0 \leq k \leq r$ such that there is a Selmer sequence $\boldsymbol{\sigma}$ of length k such that for all $1 \leq i \leq k$, we have $\mathfrak{q}_i \nmid \mathcal{N}$ and $\mathrm{Fr}_{\mathfrak{q}_i} \in G_K$ is conjugate to $\sigma_i \in \tau G_{\Omega_\infty}$ in $L_{F,M}$. If $k = 0$, the sole Kolyvagin sequence is the empty sequence.

We introduce some notation associated with Kolyvagin sequences. Let

$$\mathfrak{r}(\boldsymbol{\pi}) := \prod_{i=1}^{k} \mathfrak{q}_i$$

be the product of the ideals in the sequence; we have seen in Talk 7 that $\mathfrak{r}(\boldsymbol{\pi}) \in \mathcal{R}_{F,M}$, cf. Lemma 4.1.3. Write

$$\Pi(k, F, M) := \{\text{Kolyvagin sequences of length } k \text{ for } F \text{ and } M\}.$$

Let $\Psi(k, F, M) \subseteq \Lambda_{F,M}$ be the ideal generated by all homomorphic images of modules generated by derivative classes associated with $\mathfrak{r}(\boldsymbol{\pi})$ for all $\boldsymbol{\pi}$:

$$\Psi(k, F, M) := \sum_{\boldsymbol{\pi} \in \Pi(k,F,M)} \sum_{\psi \in \mathrm{Hom}(\langle \kappa_{[F,\mathfrak{r}(\boldsymbol{\pi}),M]} \rangle, \Lambda_{F,M})} \psi\left(\kappa_{[F,\mathfrak{r}(\boldsymbol{\pi}),M]}\right) \subseteq \Lambda_{F,M}$$

Proposition 7.1.9. *There is an $h \in \Lambda$ satisfying the following two conditions:*

(1) *h is coprime to $\mathrm{char}(X_\infty) = \prod_{i=1}^{r} f_i\Lambda$;*

(2) *for every intermediate extension $K \subseteq_{\mathrm{f}} F \subset K_\infty$, there $N_F \in p^{\mathbb{N}_0}$ such that for all $M \in p^{\mathbb{N}_0}$ and all $0 \leq k \leq r$:*

$$a_\tau^5 h\Psi(k, F, MN_F)\Lambda_{F,M} \subseteq f_{k+1}\Psi(k+1, F, M).$$

Remark. The second condition may look technical. As we will witness momentarily, it should be seen as a tool enabling one to do finite induction on the factors f_i of the characteristic ideal.

The proofs of Propositions 7.1.7 and 7.1.9 are difficult and will be omitted. We still wish to say a few words on a zeroth step towards proving them, as this is also relevant to the proofs of Theorems 2.3.3 and 2.3.4 (but not for Theorem 2.3.2). The point is that one can make the following finiteness assumptions:

(7.1.4) $\Lambda_F/\mathrm{char}(X_\infty)\Lambda_F$ and $X_\infty \otimes \Lambda_F$ are finite for all F,

(7.1.5) for all primes $\lambda \subset \mathcal{O}_F$ dividing the ideal of definition $\mathcal{N}$, there exists γ_λ in the decomposition group $G_\lambda \subset G_K$ such that $T^{\gamma_\lambda^{p^n}=1} = (T^*)^{\gamma_\lambda^{p^n}=1} = 0$ for all $n \geq 0$.

These assumptions will be used for making sure that the modules

$$\Lambda_F/f_1\Lambda_F, \quad \mathcal{S}_{\Sigma_p}(K_\infty, W^*)^{G_F}, \quad W^{G_F}, \quad (W^*)^{G_F}, \quad W^{G_{F_\lambda}}, \quad (W^*)^{G_{F_\lambda}}$$

are all finite. But why can we make these assumptions? This is where the results on twisting discussed in Talk 10 come into play: if we twist T by a character ρ, then X_∞ resp. $\mathbf{c}$ are replaced by $X_\infty \otimes \rho$ resp. $\mathbf{c}^\rho$. We have seen in Theorem 6.4.1 that the validity of our theorems for $(T, \mathbf{c})$ and $(T \otimes \rho, \mathbf{c}^\rho)$ are equivalent. So it suffices to find a character ρ such that the finiteness assumptions above hold – this is indeed doable by Lemma 6.1.3, which we haven't actually seen, but the proof is relatively elementary and has nothing to do with Euler systems.

Remark. Proposition 7.1.7 admits an easy proof in a certain interesting special case, see the beginning of §7.6. This uses Lemma 7.2.4.iii below.

3 Proof of Theorems 2.3.3 and 2.3.4

We still assume the validity of Theorem 2.3.2, so that X_∞ is a torsion Λ-module. Recall that K_Σ denotes the maximal Σ-ramified extension of K. For $K \subseteq_{\mathrm{f}} F \subset K_\infty$, let $\Lambda_F := \mathcal{O}[\mathrm{Gal}(F/K)]$ and $\Lambda_{F,M} := \Lambda_F/M\Lambda_F \simeq (\mathcal{O}/M\mathcal{O})[\mathrm{Gal}(F/K)]$.

Corollary 7.1.10. *Let $K \subseteq_{\mathrm{f}} F \subset K_\infty$ and let h be as in Proposition 7.1.9. Let Σ be a finite set of places of K containing all p-adic and infinite places as well as places where T ramifies. Then for all $\psi \in \mathrm{Hom}_\Lambda\left(H^1(K_\Sigma/F, T), \Lambda_F\right)$:*

$$a_r^5 h^r \psi(\mathbf{c}_F) \in \mathrm{char}(X_\infty)\Lambda_F$$

Remark. The statement makes sense. While a priori, $\mathbf{c}_F$ is an element in $H^1(F, T)$, we may in fact view it as a class in $H^1(K_\Sigma/F, T)$. This is because for sets Σ as in the statement, there is an equality

$$\varprojlim_F H^1(F, T) = \varprojlim_F H^1(K_\Sigma/F, T),$$

see Corollary B.3.6 (general properties of inverse limits and continuous cohomology).

Proof of Corollary 7.1.10. The image of $\mathbf{c}_F$ under the following natural map is the derivative class associated with $[F, \mathbf{1}, M]$:

$$\begin{aligned} H^1(F, T) &\to H^1(F, W_M) \\ \mathbf{c}_F &\mapsto \kappa_{[F,\mathbf{1},M]} \end{aligned} \tag{1}$$

This is Lemma 4.4.13(i); we haven't quite seen this statement in Talk 7, but it's not deep: it follows directly by unravelling the definition of $\kappa_{[F,\mathbf{1},M]}$ and using the corestriction property of Euler systems.

This allows us to describe the image of $\mathbf{c}_F$ under the following induced composition:

$$\begin{aligned} H^1(K_\Sigma/F, T)/MN_F^r \hookrightarrow H^1(K_\Sigma/F, W_{MN_F^r}) &\hookrightarrow H^1(F, W_{MN_F^r}) \\ \mathbf{c}_F &\longmapsto \kappa_{[F,\mathbf{1},MN_F^r]} \end{aligned} \tag{2}$$

Since both maps here are injective, they are invertible on the submodule of $H^1(F, W_{MN_F^r})$ generated by $\kappa_{[F,\mathbf{1},M]}$, and there is a map

$$\overline{\psi} : \Lambda_{F,M}\kappa_{[F,\mathbf{1},M]} \hookrightarrow H^1(K_\Sigma/F,T)/MN_F^r \xrightarrow{\psi} \Lambda_{F,MN_F^r} \xrightarrow{\bmod M} \Lambda_{F,M}$$

By definition of Ψ, this yields

$$\overline{\psi}\left(\kappa_{[F,\mathbf{1},MN_F^r]}\right) \in \Psi(0,F,MN_F^r). \tag{3}$$

We apply Proposition 7.1.9 inductively on $0 \leq k < r$:

$$a_\tau^{5r}h^r\Psi(0,F,MN_F^r)\Lambda_{F,M} \subseteq a_\tau^{5(r-1)}h^{r-1}f_1\Psi(1,F,MN_F^{r-1})\Lambda_{F,M} \subseteq \ldots \subseteq$$
$$\subseteq \left(\prod_{i=1}^r f_i\right)\Psi(r,F,M)\Lambda_{F,M} \subseteq \left(\prod_{i=1}^r f_i\right)\Lambda_{F,M} = \mathrm{char}(X_\infty)\Lambda_{F,M}$$

This together with (3) shows

$$a_\tau^{5r}h^r\overline{\psi}\left(\kappa_{[F,\mathbf{1},MN_F^r]}\right) \in \mathrm{char}(X_\infty)\Lambda_{F,M}$$

Since $\overline{\psi}\left(\kappa_{[F,\mathbf{1},MN_F^r]}\right)$ is the mod M reduction of $\psi(\mathbf{c}_F)$ by (2), the assertion follows by taking $M \to \infty$. □

Theorem 7.1.12. $\mathrm{char}(X_\infty) \mid a_\tau^{5r}\,\mathrm{ind}_\Lambda(\mathbf{c})$.

Corollary 7.1.10 provides divisibilities between the characteristic ideal and multiples of homomorphic images of the Euler system at all levels. It should not be surprising that we lose the h-factor, because Proposition 7.1.9 tells us that this is coprime to $\mathrm{char}(X_\infty)$. To move from the homomorphic images $a_\tau^5h^r\psi(\mathbf{c}_F)$ to $a_\tau^5h^r\mathbf{c}_F$, we will require the following algebraic result, the proof of which we omit (nothing surprising happens in it). Theorem 7.1.12 will then follow by going up the tower.

Lemma 7.1.11. *Let G be a finite abelian group, R a PID, B a finitely generated $R[G]$-module without R-torsion, and $f \in R[G]$ an element that is not a zero divisor. Now if $b \in B$ satisfies*

$$\{\psi(b) : \psi \in \mathrm{Hom}_{R[G]}(B, R[G])\} \subseteq fR[G],$$

then $b \in fB$. In words: if all homomorphic images of b in $R[G]$ are multiples of f, then b itself is a multiple of f.

Proof of Theorem 7.1.12. Let $K \subseteq_\mathrm{f} F \subset K_\infty$ be fixed. We apply Lemma 7.1.11 with $R := \mathbb{Z}_p$, $G := \mathrm{Gal}(F/K)$, $f := \prod_{i=1}^r f_i$ the characteristic polynomial, $B := H^1(K_\Sigma/F,T)/H^1(K_\Sigma/F,T)_\mathrm{tors}$, and $b := a_\tau^{5r}h^r\mathbf{c}_F$. Note that Lemma is applicable: G is a quotient of $\mathbb{Z}_p^d$ and thus abelian, B is finitely generated over $\mathbb{Z}_p$ because $H^1(K_\Sigma/F,T)$ is, which in turn follows from class field theory, and finally the condition on homomorphic images of b is precisely Corollary 7.1.10. We obtain

$$a_\tau^{5r}h^r\mathbf{c}_F \in \mathrm{char}(X_\infty)\cdot H^1(K_\Sigma/F,T)/H^1(K_\Sigma/F,T)_\mathrm{tors} \tag{4}$$

We claim that there is a containment

$$\varprojlim_F H^1(F,T)_\mathrm{tors} \subseteq H^1_\infty(K,T)_\mathrm{tors} = \left(\varprojlim_F H^1(F,T)\right)_\mathrm{tors} \tag{5}$$

To justify this, recall from Lemma 1.2.2(ii) that there is an exact sequence $V^{G_F} \to W^{G_F} \to H^1(F,T)_{\mathrm{tors}} \to 0$; this is a general property of p-adic representations of G_F. If $x \in \Lambda$ kills $W^{G_{K_\infty}}$, then it surely kills W^{G_F} too, and the exact sequence shows that it also kills $H^1(F,T)_{\mathrm{tors}}$, and (5) follows.

Using (5), we can take the inverse limit of (4) along $K \subseteq_{\mathrm{f}} F \subset K_\infty$:

$$a_\tau^{5r} h^r \mathbf{c}_{K,\infty} \in \mathrm{char}(X_\infty) \cdot H^1_\infty(K,T)/H^1_\infty(K,T)_{\mathrm{tors}}$$

Thus for all homomorphisms $\varphi \in \mathrm{Hom}_\Lambda(H^1_\infty(K,T),\Lambda)$, we have

$$a_\tau^{5r} h^r \varphi(\mathbf{c}_{K,\infty}) \in \mathrm{char}(X_\infty)\Lambda.$$

Since h is coprime to $\mathrm{char}(X_\infty)$ by Proposition 7.1.9, we even have the following:

$$a_\tau^{5r} \varphi(\mathbf{c}_{K,\infty}) \in \mathrm{char}(X_\infty)\Lambda.$$

The desired divisibility follows by the definition of $\mathrm{ind}_\Lambda(\mathbf{c})$. □

Theorems 2.3.3 and 2.3.4 quickly follow from Theorem 7.1.12.

Proof of Theorem 2.3.4. We want to show that $\mathrm{char}(X_\infty) \mid p^t \mathrm{ind}_\Lambda(\mathbf{c})$ holds for some $t \geq 0$. Theorem 7.1.12 tells us that $\mathrm{char}(X_\infty) \mid a_\tau^{5r} \mathrm{ind}_\Lambda(\mathbf{c})$. Writing $a_\tau^{5r} = p^t m$ with $p \nmid m \in \mathbb{Z}_{\geq 0}$, we have $m \in \Lambda^\times$, and the theorem follows. □

Proof of Theorem 2.3.3. The proof is the same, but now taking into account the second half of Lemma 7.1.3, we have that $\mathrm{Hyp}(K_\infty,T)$ implies $t = 0$. □

4 A plethora of evaluation maps

As we move on to working towards the proof of Theorem 2.3.2, our treatment also becomes more sketchy, as there is no way this will fit into 90 minutes.

Definition 7.2.1. Let $q_\tau(x) := \det(1 - \tau^{-1}x \mid T^*)/(x-1) \in \mathcal{O}[x]$. (We have already encountered this polynomial in Talk 8.)

Claim. *This induces an isomorphism of* 1*-dimensional* Φ*-vector spaces*

$$q_\tau(\tau^{-1}) : V/(\tau-1)V \xrightarrow{\sim} V^{\tau=1}.$$

Proof. This is A.2.4. The first space has dimension 1 by $\mathrm{Hyp}(K_\infty,V)$. View V as a $\Phi[x]$-module with x-action by τ^{-1}: then there is a decomposition

$$V \simeq \bigoplus_j \Phi[x]/g_j(x)^{e_j}\Phi[x]$$

with $g_j(x) \in \Phi[x]$ irreducible, $g_j(0) = 1$ for all j, and $\prod_j g_j(x)^{e_j} = (1-x)q_\tau(x)$. By irreducibility, there is exactly one j such that $g_j(x) = 1 - x$. □

Recall the fixed isomorphism $\vartheta^* : W^*/(\tau-1)W^* \xrightarrow{\sim} \mathbf{D}$.

Definition. The inverse of the $\mathbf{D}(1)$-dual $\mathcal{O}(1) \xrightarrow{\sim} T^{\tau=1}$ of ϑ^* defines an isomorphism

$$\vartheta : (W^{\tau=1})_{\mathrm{div}} \xrightarrow{\sim} \mathbf{D},$$

using that we have fixed a generator $\xi \in \varprojlim_n \mu_{p^n}$ (see Talk 7, §4.4). We fix an extension

$$\vartheta : W^{\tau=1} \to \mathbf{D};$$

this is not canonical, but the difference between any two choices is killed by any homomorphism in the group $\mathrm{Hom}(W^{\tau=1}/(W^{\tau=1})_{\mathrm{div}}, \mathbf{D})$ and thus by the index $\left[W^{\tau=1} : \left(W^{\tau=1}\right)_{\mathrm{div}}\right]$, and therefore also by a_τ. Finally, define a composition

$$\overline{\vartheta} : W/(\tau - 1)W \xrightarrow{q_\tau(\tau^{-1})} (W^{\tau=1})_{\mathrm{div}} \xrightarrow{\vartheta} \mathbf{D};$$

this is a composite of two surjective maps, and thus itself surjective. Note that $\overline{\vartheta}$ is canonical.

Recall that we have defined an evaluation map $\mathrm{Ev}^* : G_{\Omega_\infty^{\langle\tau\rangle}} \to \mathrm{Hom}(\mathcal{S}_{\Sigma_p}(K_\infty, W^*), \mathbf{D}) = X_\infty$ by setting $\mathrm{Ev}^*(\sigma)(c) = \vartheta^*(c(\sigma))$.

Definition 7.2.2. We define the dual evaluation map:

$$\begin{aligned} \mathrm{Ev} : G_{\Omega_\infty^{\langle\tau\rangle}} &\to \mathrm{Hom}(H^1(K_\infty, W), \mathbf{D}) \\ \sigma &\mapsto (c \mapsto \overline{\vartheta}(c(\sigma))), \end{aligned}$$

The two evaluation maps admit finite level modulo M versions defined by the same formulæ:

$$\begin{aligned} \mathrm{Ev}^*_{F,M} &: G_{F\Omega_M^{\langle\tau\rangle}} \to \mathrm{Hom}(\mathcal{S}_{\Sigma_p}(F, W^*_M), \mathcal{O}/M\mathcal{O}) \\ \mathrm{Ev}_{F,M} &: G_{F\Omega_M^{\langle\tau\rangle}} \to \mathrm{Hom}(H^1(F, W_M), \mathcal{O}/M\mathcal{O}) \end{aligned}$$

Definition 7.2.3. Let $-^\bullet : \Lambda \to \Lambda$ denote the homomorphism induced by the involution $\Gamma \to \Gamma$, $\gamma \mapsto \gamma^{-1}$.

The following property of $-^\bullet$ is easily checked:

Claim. *If B is a Λ-module and $\mathcal{A} \subseteq \Lambda$ an ideal such that $\mathcal{A} \subseteq \mathrm{Ann}_\Lambda B$, then $\mathcal{A}^\bullet \subseteq \mathrm{Ann}_\Lambda(\mathrm{Hom}(B, \mathbf{D}))$.*

Lemma 7.2.4. *We have the following annihilator relations involving Galois cohomology over Ω_∞/K_∞ and evaluation maps:*

(i) *Let $c \in H^1(K_\infty, W)$ such that for all $\gamma \in G_{\Omega_\infty}$, $\mathrm{Ev}(\gamma)(c) = 0$. Then*

$$a_\tau \,\mathrm{Ann}_\Lambda(H^1(\Omega_\infty)/K_\infty, W)c = 0.$$

(ii) $a_\tau \,\mathrm{Ann}_\Lambda(H^1(\Omega_\infty)/K_\infty, W)^\bullet \,\mathrm{Hom}(H^1(K_\infty, W), \mathbf{D}) \subseteq \mathcal{O}\,\mathrm{Ev}(G_{\Omega_\infty})$.

(iii) $a_\tau \,\mathrm{Ann}_\Lambda(H^1(\Omega_\infty)/K_\infty, W)^\bullet X_\infty \subseteq \mathcal{O}\,\mathrm{Ev}^*(G_{\Omega_\infty})$.

Remark. We will only need (i) and (iii) in the sequel. Note that a_τ is present in all three statements: it becomes clear how it arises when one looks at the proof.

Proof. The evaluation map Ev induces a dual map $H^1(K_\infty, W) \to \mathrm{Hom}(G_{\Omega_\infty^{\langle\tau\rangle}}, \mathbf{D})$. The main part of the proof is investigating this map. Staring at the definition of Ev long enough, we find that it is given by the composition

$$H^1(K_\infty, W) \xrightarrow{\mathrm{res}^{K_\infty}_{\Omega_\infty}} H^1(\Omega_\infty, W)^{G_{K_\infty}} \to \mathrm{Hom}(\Omega_\infty, W/(\tau-1)W) \xrightarrow{\overline{\vartheta}} \mathrm{Hom}(\Omega_\infty, \mathbf{D}) \qquad (6)$$

We describe the kernels of these maps. Observe that the first map has kernel $H^1(\Omega_\infty/K_\infty/W)$ by inflation–restriction. The second map has kernel $\mathrm{Hom}(\Omega_\infty, W)^{G_{K_\infty}} \cap \mathrm{Hom}(\Omega_\infty, (\tau-1)W)$. The third map is induced by $\overline{\vartheta}$, and thus has kernel $W^{q_\tau(\tau^{-1})=0}/(\tau-1)W$, which can be shown to have the same order as $W^{\tau=1}/(W^{\tau=1})_{\mathrm{div}}$ (this is again the Herbrand quotient computation from A.2.5). Since the image of G_{K_∞} under a homomorphism in the kernel of the second map is a G_{K_∞}-stable submodule of $(\tau-1)W$, it follows from the definition of a_τ that a_τ kills the kernel of the composition of the last two maps.

To see (i), note that the condition $\mathrm{Ev}(\gamma)(c) = 0$ means that c maps to 0 under (6). The claim follows from the description of the kernels.

For (ii), dualise the evaluation map $\mathrm{Ev} : G_{\Omega_\infty} \otimes \mathcal{O} \to \mathrm{Hom}(H^1(K_\infty, W), \mathbf{D})$ by applying $\mathrm{Hom}_{\mathcal{O}}(-, \mathbf{D})$. The statement follows from the description of the kernels plus the Claim above.

Finally, (iii) can be proven analogously, but now we put asterisks everywhere and replace the last map $\overline{\vartheta}$ in (6) by the injective map ϑ^*. □

Recall the following two sets of ideals of K. The set $\mathcal{R}$ consists of square-free products of primes, coprime to $\mathcal{N}$ (the ideal of definition of $\mathbf{c}$), and $\mathcal{R}_{F,M} \subset \mathcal{R}$ is the indexing set for the derivative classes $\kappa_{[F,\mathfrak{r},M]}$.

Definition 7.2.5. Let $K \subseteq_{\mathrm{f}} F \subset K_\infty$ and $M \in p^{\mathbb{N}_0}$. Define

$$\mathcal{R}_{F,M,\tau} := \{\mathfrak{r} \in \mathcal{R} : \forall \mathfrak{q} \mid \mathfrak{r}, \mathrm{Fr}_q \text{ is conjugate to } \tau \text{ in } \mathrm{Gal}(F\Omega_M/K)\}.$$

In Talk 7 (Lemma 4.1.3), we have seen that $\mathcal{R}_{F,M,\tau} \subset \mathcal{R}_{F,M}$.

We define three more evaluation maps – and there are even more to come later!

Definition. We define *finite evaluation maps*. Let $\mathfrak{q} \in \mathcal{R}_{F,M,\tau}$ be a prime and fix $\mathfrak{Q} \mid \mathfrak{q}$ a prime above it in the algebraic closure such that $\mathrm{Fr}_\mathfrak{q} = \tau$ on $F\Omega_M$, which is doable by Definition 7.2.5. (Note: $\mathrm{Fr}_\mathfrak{q} \in G_{F\Omega_M^{\langle\tau\rangle}}$.) Then the maps are:

$$\mathrm{Ev}^*_{\mathfrak{q},f} := \mathrm{Ev}^*_{F,M}(\mathrm{Fr}_\mathfrak{q}) : \mathcal{S}_{\Sigma_p}(F, W_M^*) \to \mathcal{O}/M\mathcal{O},$$
$$\mathrm{Ev}_{\mathfrak{q},f} := \mathrm{Ev}_{F,M}(\mathrm{Fr}_\mathfrak{q}) : H^1(F, W_M) \to \mathcal{O}/M\mathcal{O}.$$

Definition. We define *singular evaluation maps*. Recall that we have fixed a generator $\sigma_\mathfrak{q}$ of $\mathrm{Gal}(K(\mathfrak{q})/K(\mathbf{1}))$ in Talk 7 (Definition 4.4.1). Fix a lift of $\sigma_\mathfrak{q}$ to the inertia group $\mathcal{I}_\mathfrak{Q}$, by abuse of notation also denoted by $\sigma_\mathfrak{q}$. (Note: $\sigma_\mathfrak{q} \in G_{F\Omega_M^{\langle\tau\rangle}}$.) Define the map as the composition

$$\mathrm{Ev}_{\mathfrak{q},s} : H^1(F, W_M) \to H^1(F_\mathfrak{Q}, W_M) \twoheadrightarrow H^1_s(F_\mathfrak{Q}, W_M) \xrightarrow[1.4.7.\mathrm{i}]{\sim} W_M^{\mathrm{Fr}_\mathfrak{q}=1} = W_M^{\tau=1} \xrightarrow{\vartheta} \mathcal{O}/M\mathcal{O}.$$

Another way of saying this is that $\mathrm{Ev}_{\mathfrak{q},s}(c) = \vartheta(c(\sigma_\mathfrak{q}))$ for $c \in H^1(F, W_M)$.

The following general algebraic statement will allow us to create even more evaluation maps from our already extensive arsenal:

Lemma 7.2.7. *Let $K \subseteq_{\mathrm{f}} F \subset K_\infty$, $M \in p^{\mathbb{N}_0}$, and let B be a $\Lambda_F = \mathcal{O}[\mathrm{Gal}(F/K)]$-module. Then*

(i) *There is an $\mathcal{O}$-module isomorphism*

$$\widetilde{-} : \mathrm{Hom}_{\mathcal{O}}(B, \mathcal{O}/M\mathcal{O}) \to \mathrm{Hom}_{\Lambda}(B, \Lambda_{F,M})$$
$$\psi \mapsto \left(\widetilde{\psi} : b \mapsto \sum_{\rho \in \mathrm{Gal}(F/K)} \psi(\rho b)\rho^{-1} \right)$$

(ii) *We have $\widetilde{\rho\psi} = \rho^{-1}\widetilde{\psi}$ for all $\psi \in \mathrm{Hom}_{\mathcal{O}}(B, \mathcal{O}/M\mathcal{O})$ and $\rho \in \mathrm{Gal}(F/K)$. In particular, $\widetilde{-}$ is not an isomorphism of $\Lambda_{F,M}$-modules.*

Proof. The inverse map is $\sum_{\rho \in \mathrm{Gal}(F/K)} \alpha_\rho \rho \mapsto \alpha_1$. □

The following is essentially a restatement of Theorem 4.5.4 about finite–singular comparison map, which states $(\kappa_{[F,\mathfrak{r}\mathfrak{q},M]})^s_{\mathfrak{q}} = \varphi^{fs}_{\mathfrak{q}}(\kappa_{[F,\mathfrak{r},M]})$ for $\mathfrak{r}\mathfrak{q} \in \mathcal{R}_{F,M}$.

Theorem 7.2.10. *If $\mathfrak{r} \in \mathcal{R}_{F,M}$ and $\mathfrak{q} \in \mathcal{R}_{F,M,\tau}$ is a prime with $\mathfrak{q} \nmid \mathfrak{r}$, then*

$$\widetilde{\mathrm{Ev}}_{\mathfrak{q},f}(\kappa_{[F,\mathfrak{r},M]}) = \widetilde{\mathrm{Ev}}_{\mathfrak{q},s}(\kappa_{[F,\mathfrak{r}\mathfrak{q},M]}).$$

We can also state the following global (Poitou–Tate) duality theorem in terms of evaluation maps: the images of $\mathrm{loc}^s_{\Sigma,\Sigma_0}(\mathcal{S}^\Sigma(K, W_M))$ and $\mathrm{loc}^f_{\Sigma,\Sigma_0}(\mathcal{S}_{\Sigma_0}(K, W_M^*))$ are orthogonal complements (Theorem 1.7.3.ii). The maps here are localisations to the sum of singular resp.finite local cohomology groups over $\Sigma - \Sigma_0$.

Theorem 7.2.11. *For $\mathfrak{r}\mathfrak{q} \in \mathcal{R}_{F,M}$ with $\mathfrak{q} \in \mathcal{R}_{F,M,\tau}$ a prime, let $\Sigma_{p\mathfrak{r}}$ resp. $\Sigma_{p\mathfrak{r}\mathfrak{q}}$ denote the primes of K dividing $p\mathfrak{r}$ resp. $p\mathfrak{r}\mathfrak{q}$. Then*

$$\underbrace{a_\tau}_{\in\mathbb{N}} \underbrace{\widetilde{\mathrm{Ev}}_{\mathfrak{q},s}\left(\mathcal{S}^{\Sigma_{p\mathfrak{r}\mathfrak{q}}}(F, W_M)\right)}_{\in \Lambda_{F,M}} \underbrace{\mathrm{Ev}^*_{\mathfrak{q},f}|_{\mathcal{S}_{\Sigma_{p\mathfrak{r}}}(F,W_M^*)}}_{\in \mathrm{Hom}\left(\mathcal{S}_{\Sigma_{p\mathfrak{r}}}(F,W_M^*), \mathcal{O}/M\right)} = 0$$

Corollary 7.2.12. *Let $K \subseteq_{\mathrm{f}} F \subset K_\infty$, let $M \in p^{\mathbb{N}_0}$, $\mathfrak{r} \in \mathcal{R}_{F,M}$, and $\gamma \in \tau G_{\Omega_\infty}$. Then*

$$a_\tau \widetilde{\mathrm{Ev}}_{F,M}(\gamma)(\kappa_{[F,\mathfrak{r},M]})\, \mathrm{Ev}^*_{F,M}(\gamma)|_{\mathcal{S}_{\Sigma_{p\mathfrak{r}}}(F,W_M^*)} = 0.$$

Proof. This follows from Theorem 7.2.10 (finite–singular comparison) and Theorem 7.2.11 (aka Poitou–Tate duality). □

Remark. We will only use this statement with $\mathfrak{r} = \mathbf{1}$ in the proof of Theorem 2.3.2. The statement for general $\mathfrak{r}$ is needed for proving Proposition 7.1.9, which we shan't do.

5 Proof of Theorem 2.3.2

Having everything from the previous section at our disposal, the idea of the proof is simple: we will use Corollary 7.2.12 to construct a nonzero annihilator of X_∞.

Lemma 7.3.2. *X_∞ is a finitely generated Λ-module.*

Sketch of proof. The proof is a Nakayama style argument: it's sufficient to show that X_∞ modulo the augmentation ideal $\ker(\mathcal{O}[\![\Gamma]\!] \twoheadrightarrow \mathcal{O})$ is finitely generated over $\mathcal{O}$. Then the proof boils down to studying finiteness properties of (Pontryagin duals of) Selmer groups and using restrictions maps. □

Lemma 7.3.3. *Suppose that X_∞ is not torsion over Λ. Let*

$$J := \{\gamma \in \tau G_{\Omega_\infty} : \mathrm{Ev}^*(\gamma) \notin (X_\infty)_{\mathrm{tors}}\};$$

Then the subgroup $\langle J\rangle \leq G_K$ generated by J contains an open subgroup of G_{Ω_∞}.

Proof. We first show that J is non-empty (for the empty set, the generated subgroup would be the trivial group, which isn't open because G_K isn't discrete). By a general statement, we have that $H^1(\Omega_\infty/K_\infty, W^*)$ is torsion over Λ. This supposedly follows from Corollary C.2.2, although it's not clear to me how. Recall from Lemma 7.2.4.iii that

$$a_\tau \operatorname{Ann}_\Lambda \left(H^1(\Omega_\infty/K_\infty, W^*)\right)^\bullet X_\infty \subseteq \mathcal{O}\,\mathrm{Ev}^*(G_{\Omega_\infty}).$$

This shows that there is a $\gamma_0 \in G_{\Omega_\infty}$ such that $\mathrm{Ev}^*(\gamma_0) \notin (X_\infty)_{\mathrm{tors}}$: indeed, $\not\downarrow$ otherwise we would have

$$a_\tau \operatorname{Ann}_\Lambda \left(H^1(\Omega_\infty/K_\infty, W^*)\right)^\bullet X_\infty \subseteq (X_\infty)_{\mathrm{tors}},$$

which contradicts the assumption of X_∞ not being torsion. $\lightning$ Since $\mathrm{Ev}^*(\tau\gamma_0) = \mathrm{Ev}^*(\tau)\,\mathrm{Ev}^*(\gamma_0)$, it follows that at least one of $\tau\gamma_0$ and τ is contained in J; in particular, $J \neq \emptyset$.

By definition, $J = (\mathrm{Ev}^*)^{-1}(X_\infty - (X_\infty)_{\mathrm{tors}}) \cap \tau G_{\Omega_\infty}$. As X_∞ is finitely generated over Λ by Lemma 7.3.2, we have that $(X_\infty)_{\mathrm{tors}} \subseteq X_\infty$ is closed, so $X_\infty - (X_\infty)_{\mathrm{tors}}$ is open, thus its preimage under Ev^* is also open in G_{Ω_∞}. So J is the intersection of two open sets, thus itself an open set. □

Sketch of the proof of Theorem 2.3.2. As it's probably clear from Lemma 7.3.3, we will argue by contradiction: $\not\downarrow$ assuming that X_∞ is not Λ-torsion, we will show that $\mathbf{c}_{K,\infty} \in H^1_\infty(K,T)_{\mathrm{tors}}$. Using Lemma 7.3.3, let $\gamma \in J$.

Let $K \subseteq_{\mathrm{f}} F \subset K_\infty$ and let M be a power of p. Then Corollary 7.2.12 shows

$$a_\tau \widetilde{\mathrm{Ev}}_{F,M}(\gamma)(\kappa_{[F,\mathbf{1},M]})\,\mathrm{Ev}^*_{F,M}(\gamma) = 0 \tag{7}$$

We want to go up the tower along F. We show that the elements $\widetilde{\mathrm{Ev}}_{F,M}(\gamma)(\kappa_{[F,\mathbf{1},M]})$ form a projective system. To this end, first note that for $F \subseteq_{\mathrm{f}} F' \subset K_\infty$, we have

$$(\kappa_{[F,\mathbf{1},M]})_{F'} = \left(\mathrm{cor}^F_{F'}\,\kappa_{[F',\mathbf{1},M]}\right)_{F'} = \sum_{\rho\in\mathrm{Gal}(F'/F)} \rho\kappa_{[F',\mathbf{1},M]}$$

Since $\widetilde{\mathrm{Ev}}_{F,M}(\gamma)$ factors through its restriction to K_∞, this together with the definition of $\widetilde{\mathrm{Ev}}_{F,M}$ shows that

$$\Lambda_{F',M} \xrightarrow{\mathrm{res}^{F'}_F} \Lambda_{F,M}$$

$$\widetilde{\mathrm{Ev}}_{F',M}(\gamma)(\kappa_{[F',\mathbf{1},M]}) \longmapsto \widetilde{\mathrm{Ev}}_{F',M}(\gamma)(\kappa_{[F,\mathbf{1},M]})$$

Therefore the projective limit $\varprojlim_{F,M} \widetilde{\mathrm{Ev}}_{F,M}(\gamma)(\kappa_{[F,\mathbf{1},M]}) \in \Lambda$ exists, and (7) becomes

$$a_\tau \left(\varprojlim_{F,M} \widetilde{\mathrm{Ev}}_{F,M}(\gamma)(\kappa_{[F,\mathbf{1},M]})\right) \mathrm{Ev}^*(\gamma) = 0.$$

Our choice of γ makes sure that $\mathrm{Ev}^*(\gamma) \notin (X_\infty)_{\mathrm{tors}}$, which forces

$$\varprojlim_{F,M} \widetilde{\mathrm{Ev}}_{F,M}(\gamma)(\kappa_{[F,\mathbf{1},M]}) = 0. \tag{8}$$

We go back to finite level, extending the result to G_{Ω_∞} as follows. The conclusion (8) holds for all $\gamma \in J$ and thus for all $\gamma \in \langle J \rangle$. Once again looking at the definition of $\widetilde{\mathrm{Ev}}_{F,M}$, and taking into account the facts that $\langle J \rangle$ has finite index in G_{Ω_∞} (because it's an open subgroup) and that Λ is torsion-free, we deduce that

$$\mathrm{Ev}_{F,M}(\gamma)(\kappa_{[F,\mathbf{1},M]}) = 0$$

for all $\gamma \in G_{\Omega_\infty}$, or equivalently

$$\mathrm{Ev}(\gamma)((\kappa_{[F,\mathbf{1},M]})_{K_\infty}) = 0 \tag{9}$$

where $(\kappa_{[F,\mathbf{1},M]})_{K_\infty} \in H^1(K_\infty, W)$.

Using Lemma 7.2.4.i, this (9) implies

$$a_\tau \,\mathrm{Ann}_\Lambda(H^1(\Omega_\infty/K_\infty, W))(\kappa_{[F,\mathbf{1},M]})_{K_\infty} = 0.$$

To get a contradiction, we want to turn this into a nonzero annihilator of $\mathbf{c}_{K,\infty}$. To this end, we use the map (1) to go from the derivative class $\kappa_{[F,\mathbf{1},M]}$ to $\mathbf{c}_F$, and change the annihilator in a way so that it can be seen to be nonzero and independent of F: the latter will mean that it also annihilates $\mathbf{c}_{K,\infty}$, delivering our desired contradiction. For the details, we refer to Rubin. □

References

[Rub00] Karl Rubin. *Euler systems*. Vol. 147. Annals of Mathematics Studies. Hermann Weyl Lectures. The Institute for Advanced Study. Princeton University Press, Princeton, NJ, 2000, pp. xii+227. ISBN: 0-691-05076-7. DOI: 10.1515/9781400865208.