ASIAN J. MATH.
Vol. 4, No. 2, pp. 437–498, June 2000

011

ON THE PARITY OF RANKS OF SELMER GROUPS*

JAN NEKOVÁŘ† AND ANDREW PLATER‡

0. Introduction. Let $f = \sum_{n\geq 1} a_n(f)q^n \in S_{k_0}(\Gamma_0(N))$ be a normalized newform of even weight $k_0 \geq 2$. Let F be the number field generated by the coefficients of f and $\mathfrak{p}$ a prime of F lying above a rational prime p. There is a two-dimensional representation $V(f)$ of $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ over $F_{\mathfrak{p}}$ associated to f, characterized by the conditions

$$\mathrm{Tr}\,(\mathrm{Fr}(\ell)_{\mathrm{geom}}|V(f)) = a_\ell(f)$$
$$\det\,(\mathrm{Fr}(\ell)_{\mathrm{geom}}|V(f)) = \ell^{k_0-1}$$

for all primes $\ell \nmid pN$. The Tate twist $V_{k_0} = V(f)(k_0/2)$ is self dual: there is a skew-symmetric bilinear form

$$V_{k_0} \times V_{k_0} \longrightarrow F_{\mathfrak{p}}(1)$$

inducing an isomorphism $V_{k_0} \xrightarrow{\sim} V_{k_0}^*(1) = \mathrm{Hom}_{F_{\mathfrak{p}}}(V_{k_0}, F_{\mathfrak{p}}(1))$.

The complex L-function $L_\infty(f,s) = \sum_{n\geq 1} a_n(f)n^{-s}$ satisfies the functional equation

$$\Lambda_\infty(f,s) := \left(\frac{\sqrt{N}}{2\pi}\right)^s \Gamma(s)L_\infty(f,s) = w_\infty(f)\Lambda_\infty(f,k_0-s),$$

where $w_\infty(f) = \pm 1 = (-1)^{e_\infty}$ for $e_\infty = 0$ or 1. Bloch and Kato [Bl-Ka] defined a generalized "Selmer group" $H^1_f(\mathbb{Q}, V_{k_0}) \subseteq H^1(\mathbb{Q}, V_{k_0})$ and conjectured that

$$\mathrm{ord}_{s=k_0/2}L_\infty(f,s) \stackrel{?}{=} \dim_{F_{\mathfrak{p}}} H^1_f(\mathbb{Q}, V_{k_0}).$$

We are interested in a (mod 2) version of this conjecture:

The Parity Conjecture for ranks of Selmer groups

$$\mathrm{ord}_{s=k_0/2}L_\infty(f,s) \stackrel{?}{\equiv} \dim_{F_{\mathfrak{p}}} H^1_f(\mathbb{Q}, V_{k_0}) \pmod 2.$$

Assume that $p > 3$ and that f is ordinary at p, i.e. that $a_p(f) \in F_{\mathfrak{p}}$ is a $\mathfrak{p}$-adic unit. According to Hida's theory, there is a p-adic family of ordinary modular forms of varying weights containing f (we ignore the phenomenon of "p-stabilization" in this Introduction). In concrete terms, this means that there is an integer $c \geq 0$ such that for every integer $k \geq 2$ satisfying $k \equiv k_0 \pmod{(p-1)p^c}$, there is an ordinary newform f_k of weight k on $\Gamma_0(N)$ such that $f_{k_0} = f$ and

$$k \equiv k' \pmod{(p-1)p^{n+c}} \quad \text{implies} \quad f_k \equiv f_{k'} \pmod{p^n}.$$

Let

$$\varepsilon_k = \begin{cases} 1 & \text{if } p \,\|\, N,\ k = 2,\ a_p(f) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

* Received December 11, 1998; accepted for publication April 19, 1999.

† Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WB, UK (nekovar@dpmms.cam.ac.uk).

‡ Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WB, UK (ajp@dpmms.cam.ac.uk).
The author was supported by an EPSRC grant.

The value of ε_k indicates the presence of a trivial zero of a suitable p-adic L-function [Ma-Ta-Te]. More precisely, for every weight $k \geq 2$, $k \equiv k_0 \pmod{(p-1)p^c}$, there is a p-adic L-function $L_p(f_k, s)$ depending on $s \in \mathbb{Z}_p$ such that

$$L_p(f_k, k/2) \doteq (\mathrm{Eul}_k)\frac{L_\infty(f_k, k/2)}{\Omega_k}, \qquad L_p(f_k, k-s) \doteq w_p(f_k)L_p(f_k, s).$$

Here, $\doteq$ means equal up to a non-zero elementary factor, $\Omega_k \in \mathbb{R}^\times$ is a real period of f_k, (Eul_k) is an Euler factor satisfying

$$(\mathrm{Eul}_k) = 0 \Leftrightarrow \varepsilon_k = 1$$

and

$$w_p(f_k) = \pm 1 = w_\infty(f_k)(-1)^{\varepsilon_k}.$$

Moreover, there exists a two-variable p-adic L-function $L_p(k, s)$ defined for $s \in \mathbb{Z}_p$ and $k \in k_0 + p^c\mathbb{Z}_p$, such that $L_p(k, k-s) = w_p L_p(k, s)$, and, if $k \equiv k_0 \pmod{2(p-1)p^c}$, $k \geq 2$ is an integer, then

$$L_p(k, s) = C_k L_p(f_k, s) \qquad \text{for some } C_k \neq 0.$$

In particular, the value of

$$w_p(f_k) = w_\infty(f_k)(-1)^{\varepsilon_k} = w_p = (-1)^{e_p}$$

does not depend on k (of course, $e_p \equiv e_\infty + \varepsilon_{k_0} \pmod 2$). We shall consider Selmer groups $H^1_f(\mathbb{Q}, V_k)$ associated to Galois representations $V_k = V(f_k)(k/2)$ and also "extended Selmer groups" sitting in exact sequences

$$0 \longrightarrow (F_\mathfrak{p})^{\varepsilon_k} \longrightarrow \widetilde{H}^1_f(\mathbb{Q}, V_k) \longrightarrow H^1_f(\mathbb{Q}, V_k) \longrightarrow 0$$

(for technical reasons, it may be necessary to replace $F_\mathfrak{p}$ by a suitable finite extension and V_{k_0} by the corresponding base change). Our main result is

THEOREM A. *Let $p > 3$ and let f be ordinary at p. If $k_0 \equiv 2 \pmod{(p-1)}$, assume in addition that $V(f)$ has an irreducible residual representation. Then there is an integer $n \geq c$ such that*

$$\dim_{F_\mathfrak{p}} \widetilde{H}^1_f(\mathbb{Q}, V_k) \equiv \dim_{F_\mathfrak{p}} \widetilde{H}^1_f(\mathbb{Q}, V_{k_0}) \pmod 2$$

whenever $k \geq 2$ and $k \equiv k_0 \pmod{2(p-1)p^n}$.

It is known that

$$\mathrm{ord}_{s=k/2} L_p(f_k, s) = 0 \Rightarrow H^1_f(\mathbb{Q}, V_k) = 0 \qquad ([\mathrm{Ka}])$$

$(\star)$

$$\mathrm{ord}_{s=k/2} L_p(f_k, s) = 1 \Rightarrow \dim_{F_\mathfrak{p}} H^1_f(\mathbb{Q}, V_k) = 1 \qquad \text{for } p \nmid N, k > 2 \qquad ([\mathrm{Ne}\ 2])$$

Recall a fundamental non-vanishing conjecture for the two-variable p-adic L-function.

GREENBERG'S CONJECTURE. *The generic order of vanishing of $L_p(k, s)$ on the line $s = k/2$ is equal to zero or one (and hence to e_p).*

In other words, the function of k

$$\left.\frac{L_p(k, s)}{(s - k/2)^{e_p}}\right|_{s=k/2}$$

should not be identically zero. Theorem A and $(\star)$ immediately imply

THEOREM B. *Under the assumptions of Theorem A, Greenberg's Conjecture implies the parity conjecture*

$$\dim_{F_\mathfrak{p}} H^1_f(\mathbb{Q}, V_{k_0}) \equiv e_p - \varepsilon_{k_0} \equiv e_\infty \pmod 2.$$

Consider the special case of $k_0 = 2$ and $F = \mathbb{Q}$. The form f then corresponds to (the isogeny class of) a modular elliptic curve E over $\mathbb{Q}$. The Selmer group associated to $V_{k_0} = T_pE \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ coincides with the usual Selmer group with $\mathbb{Q}_p$-coefficients; it sits in an exact sequence

$$0 \longrightarrow E(\mathbb{Q}) \otimes \mathbb{Q}_p \longrightarrow H^1_f(\mathbb{Q}, V_{k_0}) \longrightarrow T_p Ш(E/\mathbb{Q}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \longrightarrow 0.$$

In this case, Theorem B reduces to

THEOREM C. *Let E be a modular elliptic curve over $\mathbb{Q}$ with ordinary reduction at a prime $p > 3$. Assume that the p-torsion $E_p(\overline{\mathbb{Q}})$ is an irreducible $\mathbb{F}_p[G_\mathbb{Q}]$-module and that Greenberg's conjecture holds for the two-variable p-adic L-function of E. Then*

$$\dim_{\mathbb{Q}} (E(\mathbb{Q}) \otimes \mathbb{Q}) + \operatorname{cork}_{\mathbb{Z}_p} Ш(E/\mathbb{Q}) \equiv \operatorname{ord}_{s=1} L_\infty(E, s) \pmod 2.$$

See [Gr 3], [Ko 2] (resp. [Bi-St], [Gu], [Ko 1], [Mo]) for other conditional (resp. unconditional) results in this direction. At present, Greenberg's conjecture is known only if E has complex multiplication and $e_p = 0$ ([Gr 1], [Ro]).

There are several possible approaches to Theorem A, all of which use the existence of a "big Galois representation" T that interpolates suitable Galois invariant lattices $T_k \subset V_k$. In the most elementary approach, one studies a version of $\widetilde{H}^1_f$ for the discrete modules $A_k = V_k/T_k$. It is relatively easy to show that the p^n-torsion subgroup $\widetilde{H}^1_f(\mathbb{Q}, A_k)_{p^n} \subseteq \widetilde{H}^1_f(\mathbb{Q}, A_k)$ is locally constant as a function of k. The existence of generalized Cassels-Tate pairings on $\widetilde{H}^1_f(\mathbb{Q}, A_k)/\mathrm{div}$ then gives the desired parity result.

In fact, there is a stronger version of Theorem A. Classical modular forms in (the primitive part of) Hida's family containing f are parametrized by certain prime ideals $\mathcal{P}$ in a suitable factor of the ordinary Hecke algebra. Denote by $f_\mathcal{P}$ the form corresponding to $\mathcal{P}$; it has weight $k(\mathcal{P}) \geq 2$ and character $\chi_\mathcal{P}$. For $k(\mathcal{P})$ even there is a well-defined choice of a square root $\chi_\mathcal{P}^{1/2}$ of $\chi_\mathcal{P}$. The twisted modular form $\widetilde{f}_\mathcal{P} = f_\mathcal{P} \otimes \chi_\mathcal{P}^{-1/2}$ has trivial character (i.e. lies in $S_{k(\mathcal{P})}(\Gamma_0(Np^{r(\mathcal{P})})$ for some $r(\mathcal{P})$). The Galois representation

$$V_{[\mathcal{P}]} = V(f_\mathcal{P})(k(\mathcal{P})/2) \otimes [\chi_\mathcal{P}^{-1/2}] = V(\widetilde{f}_\mathcal{P})(k(\mathcal{P})/2)$$

is two-dimensional over $F_\mathfrak{p}(\chi_\mathcal{P})$ and self dual in the same way as V_{k_0}.

THEOREM A′. *Under the assumptions of Theorem A, the parity of $\dim_{F_\mathfrak{p}(\chi_\mathcal{P})} \widetilde{H}^1_f(\mathbb{Q}, V_{[\mathcal{P}]})$ does not depend of $\mathcal{P}$.*

Together with ($\star$), this implies

THEOREM B′. *Let $p > 3$ be a prime not dividing N and $f = \sum_{n\geq 1} a_n q^n$ an ordinary newform of even weight $k \geq 2$ and character χ^{-2} on $\Gamma_1(Np^r)$, where $\mathrm{cond}(\chi) = p^s$ (necessarily with $s = r$, if $\chi \neq 1$). Then $\widetilde{f} = \sum_{n\geq 1} a_n \chi(n) q^n$ is a newform of weight k on $\Gamma_0(Np^{2r})$ (resp. $\Gamma_0(Np^r)$) if $\chi \neq 1$ (resp. $\chi = 1$). If the tame part of χ^2 is equal to ω^{k-2}, where ω is the Teichmüller character, assume that $V(f)$ has an irreducible residual representation. If Greenberg's Conjecture holds for the two-variable*

p-adic L-function of f, then

$$\dim_{\widetilde{F}_{\mathfrak{p}}} H^1_f(\mathbb{Q}, V(\widetilde{f})(k/2)) \equiv \mathrm{ord}_{s=k/2} L_\infty(\widetilde{f}, s) \pmod 2.$$

The proof of Theorem A′ uses "big Selmer groups" associated to T and a suitable big discrete module A. The ultimate explanation of this parity phenomenon relies on the general duality formalism developed in [Ne 3]. What happens is that each Selmer group $\widetilde{H}^1_f(\mathbb{Q}, A_k)$ contains a "generic subgroup" $\widetilde{H}^1_f(\mathbb{Q}, A_k)^{\mathrm{gen}}$ that is constant in the whole Hida family. The duality results of [Ne 3] give a symplectic form on the Pontryagin dual of $\widetilde{H}^1_f(\mathbb{Q}, A_k)/\widetilde{H}^1_f(\mathbb{Q}, A_k)^{\mathrm{gen}}$, tensored with $\mathbb{Q}$ (i.e. on the *infinite* part of the Selmer group!). This can be viewed as a non-classical generalization of the Cassels-Tate pairing to big Selmer groups. Assuming Greenberg's conjecture, $\widetilde{H}^1_f(\mathbb{Q}, A_k)^{\mathrm{gen}}$ has co-rank equal to e_p. In the special case when the local component of the Hecke algebra corresponding to the Hida family in question is equal to the Iwasawa algebra, there is a more elementary argument that uses big Selmer groups introduced in [Pl].

This work was inspired by a lecture of R. Greenberg [Gr 3]. We are grateful to K. Buzzard, F. Diamond, R. Taylor, J. Tilouine and A. Wiles for dispelling some – but certainly not all – of our misconceptions concerning Hecke algebras.

1. Modular forms and Galois representations.

(1.1) Modular curves and modular forms. In this section we recall basic notation and normalizations concerning modular curves and modular forms, following the conventions of [KaN] and [Gro].

(1.1.1) For an integer $N > 4$, $X_1(N) \longrightarrow \mathrm{Spec}(\mathbb{Z}[1/N])$ is the complete modular curve classifying pairs $(E, \alpha : \mu_N \hookrightarrow E_N)$, where E is a generalized elliptic curve ([De-Ra]) and the image of α meets every irreducible component in each geometric fibre of E. We assume that $N > 4$ from now on.

(1.1.2) For a generalized elliptic curve $\pi : E \longrightarrow S$, let $\underline{\omega}_E$ be the invertible sheaf $\underline{\mathrm{Lie}}(E^{reg})^\vee$ on S ($\underline{\omega}_E = \pi_*\Omega^1_{E/S}$ if π is smooth). For any $\mathbb{Z}[1/N]$-algebra R, the space of holomorphic modular forms of weight $k \geq 1$ on $\Gamma_1(N)$ defined over R is, by definition, equal to $H^0\left(X_1(N)_{/R}, \underline{\omega}^{\otimes k}\right)$. One can interpret a modular form $f \in H^0\left(X_1(N)_{/R}, \underline{\omega}^{\otimes k}\right)$ as a rule assigning an element $f(E, \alpha) \in \underline{\omega}_E^{\otimes k}$ to each pair $(E, \alpha : \mu_N \hookrightarrow E_N)$ defined over an R-algebra R', compatible with base change.

(1.1.3) The Tate curve $E = \mathbb{G}_m/q^{\mathbb{Z}}$ is an elliptic curve over $\mathbb{Z}[[q]][q^{-1}]$ which extends to a generalized elliptic curve over $\mathbb{Z}[[q]]$. The exact sequence

$$0 \longrightarrow \mu_N \xrightarrow{\mathrm{Id}_N} E_N \longrightarrow \mathbb{Z}/N\mathbb{Z} \longrightarrow 0$$

gives the tautological embedding $\mathrm{Id}_N : \mu_N \hookrightarrow E_N$. Evaluation of a modular form $f \in H^0\left(X_1(N)_{/R}, \underline{\omega}^{\otimes k}\right)$ on the Tate curve gives the Fourier expansion $F(f) \in R[[q]]$ of f :

$$f\left(\mathbb{G}_m/q^{\mathbb{Z}}, \mathrm{Id}_N\right) = F(f)(q)\left(\frac{dt}{t}\right)^{\otimes k}$$

where t is the coordinate on $\mathbb{G}_m$. The map $F : H^0\left(X_1(N)_{/R}, \underline{\omega}^{\otimes k}\right) \longrightarrow R[[q]]$ is injective ([KaN, 1.6.1]).

(1.1.4) If $S \longrightarrow T$ is smooth and $\pi : E \longrightarrow S$ is an elliptic curve, then the Gauss-Manin connection

$$\nabla : \mathbb{R}^1\pi_*\Omega^\bullet_{E/S} \longrightarrow \left(\mathbb{R}^1\pi_*\Omega^\bullet_{E/S}\right) \otimes \Omega^1_{S/T}$$

and relative Poincaré duality

$$\langle\ ,\ \rangle_{dR} : \left(\mathbb{R}^1\pi_*\Omega^\bullet_{E/S}\right) \times \left(\mathbb{R}^1\pi_*\Omega^\bullet_{E/S}\right) \longrightarrow \mathbb{R}^2\pi_*\Omega^\bullet_{E/S} \xrightarrow[\sim]{\mathrm{Tr}} \mathcal{O}_S$$

define the Kodaira-Spencer map

$$\begin{aligned} i\ :\ \underline{\omega}_E^{\otimes 2} &\longrightarrow \Omega^1_{S/T} \\ \omega \otimes \nu &\mapsto \langle \omega, \nabla\nu \rangle_{dR} \end{aligned}$$

For the Tate curve, $i\left((dt/t)^{\otimes 2}\right) = dq/q$. In fact, i extends to an isomorphism of invertible sheaves on $X_1(N)$,

$$\underline{\omega}^{\otimes 2} \xrightarrow{\sim} \Omega^1_{X_1(N)}(\text{cusps}).$$

(1.2) Hecke operators

(1.2.1) For $a \in (\mathbb{Z}/N\mathbb{Z})^\times$, the diamond operator $< a >$ acts on $X_1(N)$ by $< a > (E, \alpha) = (E, a \cdot \alpha)$ and on modular forms by

$$(< a >_{\mathrm{Alb}} f)(E, \alpha) = f(E, a \cdot \alpha),$$

(the covariant, or "Albanese," action), and also by

$$(< a >_{\mathrm{Pic}} f)(E, \alpha) = f(E, a^{-1} \cdot \alpha) = \left(< a^{-1} >_{\mathrm{Alb}} f\right)(E, \alpha)$$

(the contravariant, or "Picard," action). If $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow R^\times$ satisfies $\chi(-1) = (-1)^k$, a modular form $f \in H^0\left(X_1(N)_{/R}, \underline{\omega}^{\otimes k}\right)$ has character χ if $< a >_{\mathrm{Alb}} f = \chi(a) f$ for all $a \in (\mathbb{Z}/N\mathbb{Z})^\times$.

(1.2.2) For integers $n \geq 1$ with $(n, N) = 1$, the Hecke operators $T(n)$ act on modular forms by

$$(T(n)_{\mathrm{Alb}} f)(E, \alpha) = \frac{1}{n} \sum_{\substack{\lambda : E \longrightarrow E' \\ \deg(\lambda) = n}} \lambda^*(f(E', \lambda \circ \alpha))$$

$$(T(n)_{\mathrm{Pic}} f)(E, \alpha) = \frac{1}{n} \sum_{\substack{\mu : E' \longrightarrow E \\ \deg(\mu) = n}} \mu_*(f(E', \mu^{-1} \circ \alpha))$$

If $n = \ell \nmid N$ is a prime and

$$F(f)(q) = \sum_{n \geq 0} a_n q^n, \qquad F\left(< \ell >_{\mathrm{Alb}} f\right)(q) = \sum_{n \geq 0} b_n q^n,$$

then a short calculation gives

$$\begin{aligned}
&(T(\ell)_{\mathrm{Alb}} f)\,(\mathbb{G}_m/q^{\mathbb{Z}}, \mathrm{Id}_N) \\
&\quad = \frac{1}{\ell} f\,(\mathbb{G}_m/q^{\ell\mathbb{Z}}, \ell\cdot \mathrm{Id}_N)\left(\ell\frac{dt}{t}\right)^{\otimes k} + \frac{1}{\ell}\sum_{q'^{\ell}=q} f\left(\mathbb{G}_m/q'^{\mathbb{Z}}, \mathrm{Id}_N\right)\left(\frac{dt}{t}\right)^{\otimes k} \\
&\quad = \left(\ell^{k-1}\sum_{n\geq 0} b_n q^{n\ell} + \sum_{n\geq 0} a_{n\ell} q^n\right)\left(\frac{dt}{t}\right)^{\otimes k} \\
&\quad = (T(\ell)_{\mathrm{Pic}} f)\,(\mathbb{G}_m/q^{\mathbb{Z}}, \ell\cdot \mathrm{Id}_N)\,.
\end{aligned}$$

This means that the usual Hecke operator $T(\ell)$ on Fourier expansions of modular forms corresponds to $T(\ell)_{\mathrm{Alb}} = <\ell>_{\mathrm{Alb}} T(\ell)_{\mathrm{Pic}}$. Of course, if f has character χ, then $b_n = \chi(n)a_n$ for all $n \geq 1$ prime to N.

(1.2.3) For a prime $\ell \mid N$, one defines

$$(T(\ell)_{\mathrm{Alb}} f)\,(E,\alpha) = \frac{1}{\ell}\sum_{\substack{\lambda: E\to E',\deg(\lambda)=\ell,\\ \mathrm{Ker}(\lambda)\cap\mathrm{Im}(\alpha)=0}} \lambda^*(f(E', \lambda\circ\alpha))$$

and $T(\ell^m)_{\mathrm{Alb}} = T(\ell)^m_{\mathrm{Alb}}$. The same calculation as in 1.2.2 shows that

$$(T(\ell)_{\mathrm{Alb}} f)\,(\mathbb{G}_m/q^{\mathbb{Z}}, \mathrm{Id}_N) = \left(\sum_{n\geq 0} a_{n\ell} q^n\right)\left(\frac{dt}{t}\right)^{\otimes k}.$$

One defines $T(n)_{\mathrm{Alb}} f$ for any $n \geq 1$ by requiring $T(mn)_{\mathrm{Alb}} = T(m)_{\mathrm{Alb}} T(n)_{\mathrm{Alb}}$ whenever $(m,n) = 1$.

(1.2.4) A more geometric definition of $T(\ell)$ comes from Hecke correspondences. For a prime ℓ, let $X_1(N;\ell)$ be the curve over $\mathrm{Spec}(\mathbb{Z}[1/N])$ classifying triples $(E, \alpha : \mu_N \hookrightarrow E_N, C)$, where (E,α) is as in 1.1.1 and $C \subset E_\ell$ is a locally free subgroup scheme of rank ℓ such that $\mathrm{Im}(\alpha)\cap C = 0$ and $\mathrm{Im}(\alpha)\times C$ meets every irreducible component of each geometric fibre of E. There are finite maps $s, t : X_1(N;\ell) \longrightarrow X_1(N)$ given over the affine curve $Y_1(N) = X_1(N) - \{\text{cusps}\}$ by

$$(E,\alpha) \xleftarrow{\ s\ } (E,\alpha,C) \xmapsto{\ t\ } (E' = E/C, \alpha' = \lambda\circ\alpha),$$

where $\lambda : E \longrightarrow E/C$ is the degree ℓ isogeny associated to C. The maps s, t define a correspondence

$$\begin{array}{ccc} & X_1(N;\ell) & \\ {\scriptstyle s}\swarrow & & \searrow{\scriptstyle t} \\ X_1(N) & \xrightarrow{\quad T(\ell)\quad} & X_1(N) \end{array}$$

which acts on various cohomology groups, both covariantly: $T(\ell)_{\mathrm{Alb}} = t_*\circ s^*$ (the "Albanese action") and contravariantly: $T(\ell)_{\mathrm{Pic}} = s_*\circ t^*$ (the "Picard action").

(1.2.5) Similarly, the diamond operators $< a >: X_1(N) \longrightarrow X_1(N)$, $a \in (\mathbb{Z}/N\mathbb{Z})^\times$, act on cohomology by

$$< a >_{\mathrm{Alb}} = < a >_*, \qquad < a >_{\mathrm{Pic}} = < a >^* = < a^{-1} >_* = < a^{-1} >_{\mathrm{Alb}}.$$

(1.2.6) For modular forms of weight two, the Kodaira-Spencer isomorphism

$$i : H^0\left(X_1(N), \underline{\omega}^{\otimes 2}\right) \xrightarrow{\sim} H^0\left(X_1(N), \Omega^1_{X_1(N)}(\text{cusps})\right)$$

is compatible with the actions of $T(l)_{\text{Alb}}$ and $< a >_{\text{Alb}}$ on both sides (1.2.2 and 1.2.3 on the left hand side, 1.2.4 and 1.2.5 on the right hand side). The factor $1/n$ in the formulas of 1.2.2 comes from the equality

$$\langle \lambda^*(\nu), \lambda^*(\nabla\nu')\rangle^E_{dR} = \deg(\lambda)\langle \nu, \nabla\nu'\rangle^{E'}_{dR}$$

valid for any isogeny $\lambda : E \longrightarrow E'$.

(1.2.7) There are two definitions of the Weil pairing

$$e_N = e_{N,E} : E_N \times E_N \longrightarrow \mu_N$$

which differ by a sign. We use the one normalized by $e_{N,E}(\zeta, q^{1/N}) = \zeta$ for all $\zeta \in \mu_N$ and all $q^{1/N}$ for the Tate curve $E = \mathbb{G}_m/q^{\mathbb{Z}}$.

(1.2.8) For a primitive N-th root of unity $\zeta \in \mu_N$, the Fricke involution $W_\zeta : X_1(N) \longrightarrow X_1(N)$ (defined over $\mathbb{Z}[1/N, \mu_N]$) is given on $Y_1(N)$ by $W_\zeta(E, \alpha : \mu_N \hookrightarrow E_N) = (E', \beta_\zeta)$, where $E' = E/\text{Im}(\alpha)$ and $\beta_\zeta : \mu_N \hookrightarrow E'$ is characterized by

$$e_{N,E}(\alpha(\zeta), \text{any lift of } \beta_\zeta(\zeta) \text{ to } E_N) = \zeta.$$

For $a \in (\mathbb{Z}/N\mathbb{Z})^\times$, one has $\beta_\zeta(\zeta) = \beta_{\zeta^a}(\zeta^a) = a\beta_{\zeta^a}(\zeta)$. Hence,

(1.2.8.1) $W_\zeta =< a > \circ W_{\zeta^a}, \qquad W_{\zeta^a} < a >=< a >^{-1} \circ W_\zeta = W_{\zeta^a}, \qquad \text{as } W_\zeta^2 = \text{id}.$

If $g \in \text{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})$ acts on μ_N by $\zeta \mapsto \zeta^a$, then

(1.2.8.2) $$g \circ W_\zeta = W_{\zeta^a} \circ g = W_\zeta \circ < a > \circ g.$$

For every prime ℓ, there is an equality of correspondences on $X_1(N)$, $W_\zeta \circ T(\ell) = T(\ell)^t \circ W_\zeta$. this implies that the induced action on cohomology satisfies

(1.2.8.3) $$T(\ell)_{\text{Pic}} = W_\zeta \circ T(\ell)_{\text{Alb}} \circ W_\zeta$$

for all primes ℓ.

(1.2.9) For integers $d \geq 1, M, N > 4$ such that $dM \mid N$, there are finite degeneration maps $\pi_d : X_1(N) \longrightarrow X_1(M)$ given on $Y_1(M)$ by

$$\pi_d(E, \alpha : \mu_N \hookrightarrow E_N) = (E' = E/\alpha(\mu_d), \alpha' : \mu_M \hookrightarrow E'_M)$$

with

$$\alpha' : \mu_M \hookrightarrow \mu_{N/d} \xleftarrow[\sim]{d} \mu_N/\mu_d \overset{\alpha \bmod \mu_d}{\hookrightarrow} E/\alpha(\mu_d) = E'.$$

In particular,

$$\pi_1(E, \alpha : \mu_N \hookrightarrow E_N) = (E, \alpha\,|_{\mu_M})$$

and

$$\pi_d\left(\mathbb{G}_m/q^{\mathbb{Z}}, \text{Id}_N\right) = \left(\mathbb{G}_m/(q^d)^{\mathbb{Z}}, \text{Id}_M\right).$$

If $\zeta_N \in \mu_N$ is a primitive N-th root of unity and $\zeta_M = \zeta_N^{N/M}$, then $\pi_d \circ W_{\zeta_N} = W_{\zeta_M} \circ \pi_{N/dM}$.

(1.2.10) We now consider the induced action on cohomology. π_1^* commutes with $< a >_{\text{Alb}}$ (and therefore with $< a >_{\text{Pic}}$ too) for $a \in (\mathbb{Z}/N\mathbb{Z})^\times$, and commutes with

$T(n)_{\mathrm{Alb}}$ (and $T(n)_{\mathrm{Pic}}$ too) for $(n,N)=1$, and with $T(\ell)_{\mathrm{Alb}}$ for primes $\ell \mid M$. The trace operator π_{1*} commutes with $<a>_{\mathrm{Alb}}$ (and hence with $<a>_{\mathrm{Pic}}$) for $a \in (\mathbb{Z}/N\mathbb{Z})^\times$, and with $T(n)_{\mathrm{Alb}}$ (and hence with $T(n)_{\mathrm{Pic}}$) for $(n,N)=1$. Moreover, if $\ell \mid M$ is a prime, then both squares in the commutative diagram

$$\begin{array}{ccccc} X_1(N) & \xleftarrow{s} & X_1(N;\ell) & \xrightarrow{t} & X_1(N) \\ \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi_1} \\ X_1(M) & \xleftarrow{s} & X_1(M;\ell) & \xrightarrow{t} & X_1(M) \end{array}$$

are cartesian, which implies that $s^* \circ \pi_{1*} = \pi_{1*} \circ s^*$, $t^* \circ \pi_{1*} = \pi_{1*} \circ t^*$, and

$$T(\ell)_{\mathrm{Pic}} \circ \pi_{1*} = s_* \circ t^* \circ \pi_{1*} = s_* \circ \pi_{1*} \circ t^* = \pi_{1*} \circ s_* \circ t^* = \pi_{1*} \circ T(\ell)_{\mathrm{Pic}}$$
$$T(\ell)_{\mathrm{Alb}} \circ \pi_{1*} = t_* \circ s^* \circ \pi_{1*} = t_* \circ \pi_{1*} \circ s^* = \pi_{1*} \circ t_* \circ s^* = \pi_{1*} \circ T(\ell)_{\mathrm{Alb}}.$$

In particular, if $N = \ell M$ for a prime $\ell \mid M$, then π_{1*} commutes with both $T(\ell)_{\mathrm{Alb}}$ and $T(\ell)_{\mathrm{Pic}}$, and $\pi_{\ell *} = W_{\zeta_M} \circ \pi_{1*} \circ W_{\zeta_N}$ commutes with both $T(\ell)_{\mathrm{Pic}} = W_\zeta \circ T(\ell)_{\mathrm{Alb}} \circ W_\zeta$ and $T(\ell)_{\mathrm{Alb}} = W_\zeta \circ T(\ell)_{\mathrm{Pic}} \circ W_\zeta$.

(1.2.11) The Eichler-Shimura relation on $X_1(N)$ defined as in 1.1.1 has the following form: for every prime $\ell \nmid N$,

$$T(\ell) \equiv \mathrm{Fr}(\ell)^t + <\ell> \mathrm{Fr}(\ell) \pmod{\ell}$$

as a correspondence on $X_1(N)_{/\mathbb{F}_\ell}$. This implies that the induced contravariant action on étale cohomology $H^1(\overline{X_1(N)}_{et}, \mathbb{Z}_p)$ (where $p \neq \ell$ and $\overline{X_1(N)} = X_1(N) \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$) satisfies

$$T(\ell)_{\mathrm{Pic}} = \ell \cdot \mathrm{Fr}(\ell)^{-1}_{\mathrm{geom}} + <\ell>_{\mathrm{Pic}} \mathrm{Fr}(\ell)_{\mathrm{geom}}.$$

Consequently, $\mathrm{Fr}(\ell)_{\mathrm{geom}}$ is a root of $X^2 - T(\ell)_{\mathrm{Alb}} X + \ell <\ell>_{\mathrm{Alb}} = 0$.

(1.3) Galois representations

Fix algebraic closures $\overline{\mathbb{Q}}$ (resp. $\overline{\mathbb{Q}}_p$) of $\mathbb{Q}$ (resp. $\mathbb{Q}_p$), and embeddings $i_\infty : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$, $i_p : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ (for a given prime p).

(1.3.1) Let $f = \sum_{n \geq 1} a_n q^n \in S_k(\Gamma_1(N), \chi)$ be a cusp form on $\Gamma_1(N)$ of weight $k \geq 2$ and character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$, defined over $\mathbb{C}$. It is a normalized eigenform if $a_1 = 1$ and $T(\ell)_{\mathrm{Alb}} f = \lambda_\ell f$ for all primes ℓ (necessarily with $\lambda_\ell = a_\ell$). A normalized newform is a normalized eigenform such that the set of eigenvalues $\{\lambda_\ell : \ell \nmid N\}$ does not occur for any eigenform of weight k on $\Gamma_1(M)$, for any proper divisor $M \mid N$.

(1.3.2) Assume that f from 1.3.1 is a normalized newform. Let F be a finite extension of $\mathbb{Q}$ in $\overline{\mathbb{Q}}$ containing all $i_\infty^{-1}(a_n)$ and all values of $i_\infty^{-1} \circ \chi$. The embedding i_p induces on F a prime $\mathfrak{p}$ above p. Let $S = \{\text{primes } \ell : \ell \nmid pN\} \cup \{\infty\}$. The p-adic Galois representation associated to f

$$\rho = \rho_{f,\mathfrak{p}} : G_{\mathbb{Q},S} \longrightarrow GL_2(F_{\mathfrak{p}})$$

(where $G_{\mathbb{Q},S}$ denotes the Galois group with restricted ramification; cf. 2.1.1 below) is characterized by the conditions

$$\mathrm{Tr}\,(\rho(\mathrm{Fr}(\ell)_{\mathrm{geom}})) = i_p(a_\ell)$$
$$\det\,(\rho(\mathrm{Fr}(\ell)_{\mathrm{geom}})) = i_p(\chi(\ell)\ell^{k-1})$$

for all $\ell \notin S$. It was constructed in [Ei],[Sh] for $k = 2$ and [De] for $k > 2$. Ribet [Ri 1, Thm. 2.3] showed that ρ is irreducible (hence absolutely irreducible, by the same argument as in 1.5.3(3) below).

(1.3.3) Scholl [Sc] constructed a (Grothendieck) motive $M = M(f)$ associated to f, pure of weight $k-1$ and of rank two over F. Geometrically, $M \subset h^{k-1}(Z) \otimes F$, where Z is a suitable smooth compactification of the $(k-1)$-dimensional Kuga-Sato variety over $Y(N)$ (at least for $N \geq 3$). The p-adic étale realization $M_p \subset H^{k-1}(\overline{Z}_{et}, F \otimes \mathbb{Q}_p)$ of M is free of rank two over $F \otimes \mathbb{Q}_p = \prod_{v|p} F_v$; its $\mathfrak{p}$-component $M_\mathfrak{p}$ gives the representation $\rho_{f,\mathfrak{p}}$. By [La], [Ca] the L-series of the motive M agrees with

$$L_\infty(f,s) = \sum_{n \geq 1} a_n n^{-s} = \prod_{\ell | N} (1 - a_\ell \ell^{-s})^{-1} \prod_{\ell \nmid N} (1 - a_\ell \ell^{-s} + \chi(\ell)\ell^{k-1-2s})^{-1}$$

even at Euler factors at bad primes $\ell \mid N$.

(1.3.4) A suitably twisted Poincaré duality on Z gives a non-degenerate skew-symmetric pairing

$$M_\mathfrak{p} \times M_\mathfrak{p} \longrightarrow M_\mathfrak{p} \otimes_{F_\mathfrak{p}} M_\mathfrak{p} \longrightarrow F_\mathfrak{p}(1-k) \otimes_{F_\mathfrak{p}} [\chi],$$

where $[\chi]$ is the one-dimensional representation of $G_{\mathbb{Q},S}$ over $F_\mathfrak{p}$ given by $[\chi](\mathrm{Fr}(\ell)_{\mathrm{geom}}) = \chi(\ell)$, $(\ell \nmid pN)$. In the special case when k is even and $\chi = 1$, then $V = M_\mathfrak{p}(k/2)$ is pure of weight -1 and the above pairing defines a non-degenerate skew-symmetric pairing

$$V \times V \longrightarrow V \otimes_{F_\mathfrak{p}} V \longrightarrow F_\mathfrak{p}(1),$$

which induces an isomorphism $V \xrightarrow{\sim} V^*(1) = \mathrm{Hom}_{F_\mathfrak{p}}(V, F_\mathfrak{p}(1))$.

(1.3.5) A normalized eigenform f from 1.3.1 is **ordinary** (with respect to i_∞, i_p) if $i_p(a_p) \in F_\mathfrak{p}$ is a $\mathfrak{p}$-adic unit. In particular, $a_p \neq 0$, which implies ([Mi, Thm. 4.6.17]) that either

(i) $\mathrm{ord}_p(N) = \mathrm{ord}_p(\mathrm{cond}(\chi))$

or

(ii) $p \parallel N$, $k = 2$, $p \nmid \mathrm{cond}(\chi)$, $a_p^2 = \chi(p)$.

Furthermore, the Galois representation $M_\mathfrak{p}$ restricted to $G_{\mathbb{Q}_p} = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ is reducible [Wi 1, Thm. 2.2.2] and there is an exact sequence of $F_\mathfrak{p}[G_{\mathbb{Q}_p}]$-modules

$$0 \longrightarrow F^+M_\mathfrak{p} \longrightarrow M_\mathfrak{p} \longrightarrow F^-M_\mathfrak{p} \longrightarrow 0 \tag{1.3.5.1}$$

with $\dim(F^\pm M_\mathfrak{p}) = 1$ and $F^+M_\mathfrak{p}$ unramified. The quadratic equation $X^2 - a_pX + \chi(p)p^{k-1} = 0$ has two distinct roots in $F_\mathfrak{p}$: one of them, α_p, is a $\mathfrak{p}$-adic unit and the other is

$$\beta_p = \begin{cases} \frac{\chi(p)p^{k-1}}{\alpha_p} & if\ p \nmid N \\ 0 & if\ p \mid N. \end{cases}$$

The geometric Frobenius $\mathrm{Fr}(p)_{\mathrm{geom}} \in G_{\mathbb{Q}_p}/I_p$ acts on $F^+M_\mathfrak{p}$ by the scalar α_p. The duality 1.3.4 gives

$$F^-M_\mathfrak{p} \xrightarrow{\sim} (F^+M_\mathfrak{p})^*(1-k) \otimes [\chi] \tag{1.3.5.1}$$

(as $F_\mathfrak{p}[G_{\mathbb{Q}_p}]$-modules).

(1.3.6) If $p \nmid N$, then $f^0 = \sum_{n\geq 1} a_n q^n - \beta_p \sum_{n\geq 1} a_n q^{pn}$ is a normalized eigenform on $\Gamma_1(Np)$ satisfying

$$T(\ell)_{\mathrm{Alb}} f^0 = a_\ell f^0 \qquad \text{if} \quad \ell \nmid p, \qquad T(p)_{\mathrm{Alb}} f^0 = \alpha_p f^0.$$

One says that f^0 is the **p-stabilization** of f. By abuse of language, we shall call $\rho_{f,\mathfrak{p}}$ the Galois representation associated to f^0.

(1.3.7) Assume that $p \nmid N$. A normalized eigenform f of weight $k \geq 2$ on $\Gamma_1(Np^n)$ is said to be an **ordinary p-stabilized newform of tame level** N if f is ordinary, $n \geq 1$, and f is new at N, i.e. the set of eigenvalues $\{a_\ell : \ell \nmid Np\}$ does not occur for any newform of weight k on $\Gamma_1(Mp^m)$ for any proper divisor M of N and $m \leq n$. Equivalently, f is ordinary and either a newform on $\Gamma_1(Np^r)$ for some $r \geq 1$, or is equal to the p-stabilization of a newform on $\Gamma_1(N)$.

(1.4) Hida's theory

Assume that $p > 3$. Fix a finite extension $F_\mathfrak{p}$ of $\mathbb{Q}_p$ (in $\overline{\mathbb{Q}}_p$); let $\mathcal{O} = \mathcal{O}_\mathfrak{p}$ be its ring of integers. Fix an integer $N \geq 1$ not divisible by p.

(1.4.1) Hecke algebras

For $k \geq 2$, and $r \geq 1$, let $\mathfrak{h}_k(\Gamma_1(Np^r))$ be the subring of $\mathrm{End}\,(S_k(\Gamma_1(Np^r)))$ generated (over $\mathbb{Z}$) by the Hecke operators $T(n) = T(n)_{\mathrm{Alb}}$, $n \geq 1$, and the diamond operators $< a > = < a >_k$, $(a \in (\mathbb{Z}/N\mathbb{Z})^\times)$. Put $\mathfrak{h}_{k,r} := \mathfrak{h}_k(\Gamma_1(Np^r)) \otimes_{\mathbb{Z}} \mathcal{O}$. This is free of finite rank over $\mathcal{O}$; diamond operators give an $\mathcal{O}$-algebra homomorphism

$$< >_k : \mathcal{O}[(\mathbb{Z}/N\mathbb{Z})^\times] \longrightarrow \mathfrak{h}_{k,r}.$$

For fixed $k \geq 2$ and $s \geq r \geq 1$, there are canonical homomorphisms $\mathfrak{h}_{k,s} \to \mathfrak{h}_{k,r}$, given by $T(n) \mapsto T(n)$, $< a >_k \mapsto < a >_k$ (these are dual to the maps π_1^* from 1.2.10 acting on cusp forms of weight k). The projective limit

$$\mathfrak{h}_{k,\infty} := \varprojlim_r \mathfrak{h}_{k,r}$$

is equipped with morphisms

$$< >_k : \mathcal{O}[[\mathbb{Z}_p^\times]] \hookrightarrow \mathcal{O}[[Z_N]] \longrightarrow \mathfrak{h}_{k,\infty},$$

where $Z_N = \varprojlim_r (\mathbb{Z}/Np^r\mathbb{Z})^\times = \mathbb{Z}_p^\times \times (\mathbb{Z}/N\mathbb{Z})^\times$ and $\mathcal{O}[[Z_N]] = \varprojlim_r \mathcal{O}[(\mathbb{Z}/Np^r\mathbb{Z})^\times]$. Put $\Gamma = \{x \in \mathbb{Z}_p^\times : x \equiv 1 \pmod{p}\}$ and denote the canonical inclusion $\Gamma \hookrightarrow \mathcal{O}[[\Gamma]] \hookrightarrow \mathcal{O}[[Z_N]]$ by $\imath$.

(1.4.2) Ordinary projector e

For each $1 \leq r \leq \infty$, there is a decomposition $\mathfrak{h}_{k,r} = \mathfrak{h}_{k,r}^{ord} \times \mathfrak{h}_{k,r}^{ss}$ such that $\mathfrak{h}_{k,r}^{ord}$ (resp. $\mathfrak{h}_{k,r}^{ss}$) is the largest quotient of $\mathfrak{h}_{k,r}$ on which $T(p)_{\mathrm{Alb}}$ is invertible (resp. $T(p)_{\mathrm{Alb}}$ is topologically nilpotent). More precisely,

$$\mathfrak{h}_{k,r}^{ord} = e\mathfrak{h}_{k,r}, \qquad \mathfrak{h}_{k,r}^{ss} = (1-e)\mathfrak{h}_{k,r},$$

for Hida's ordinary projector

$$e = \lim_{n\to\infty} T(p)_{\mathrm{Alb}}^{n!} \in \mathfrak{h}_{k,r}.$$

One defines the ordinary part of any $\mathfrak{h}_{k,r}$-module M to be $M^{ord} = eM = \mathfrak{h}_{k,r}^{ord} \otimes_{\mathfrak{h}_{k,r}} M$. There is a bijection between the set of ordinary normalized eigenforms of weight $k \geq 2$

on $\Gamma_1(Np^r)$ $(r \geq 1)$ and $\mathcal{O}$-algebra homomorphisms $\mathfrak{h}_{k,r}^{ord} \longrightarrow \overline{\mathbb{Q}}_p$ (given by Hecke eigenvalues).

(1.4.3) PROPOSITION. *(i) [Hi 1, Thm. 1.1] For $l \geq k \geq 2$ there are canonical isomorphisms $\mathfrak{h}_{l,\infty}^{ord} \xrightarrow{\sim} \mathfrak{h}_{k,\infty}^{ord}$. We use them to identify all $\mathfrak{h}_{k,\infty}^{ord}$ $(k \geq 2)$ with $\mathfrak{h}_{\infty}^{ord} = \mathfrak{h}_{2,\infty}^{ord}$.*
(ii) [Hi 2, Thm. 3.1] Consider $\mathfrak{h}_{\infty}^{ord}$ as an $\mathcal{O}[[Z_N]]$-algebra via diamond operators $< >_2$ acting on weight two cusp forms. Then $\mathfrak{h}_{\infty}^{ord}$ is finite and free over $\Lambda = \mathcal{O}[[\Gamma]]$.
(iii) [Hi 1, Thm. 1.2] The canonical maps $\mathfrak{h}_{\infty}^{ord} \xleftarrow{\sim} \mathfrak{h}_{k,\infty}^{ord} \to \mathfrak{h}_{k,r}^{ord}$ induce isomorphisms

$$\mathfrak{h}_{\infty}^{ord}/\omega_{k,r}\mathfrak{h}_{\infty}^{ord} \xrightarrow{\sim} \mathfrak{h}_{k,r}^{ord}, \qquad (k \geq 2, r \geq 1)$$

where $\omega_{k,r} = \imath(\gamma)^{p^{r-1}} - \gamma^{(k-2)p^{r-1}}$ for any fixed topological generator γ of Γ.

(1.4.4) Decomposition of $\mathfrak{h}_{\infty}^{ord}$

It follows from Prop. 1.4.3 (ii) that $\mathfrak{h}_{\infty}^{ord} = \prod R$ is a product of local rings, finite and free over Λ. The local factors R are localizations of $\mathfrak{h}_{\infty}^{ord}$ at its maximal prime ideals. They are not necessarily integral domains; to get a further decomposition one must introduce denominators. We shall be interested only in the primitive part; let $\mathcal{L}$ be the fraction field of Λ. Hida [Hi 2, p. 250, 252] constructed an idempotent $e_{prim} \in \mathfrak{h}_{\infty}^{ord} \otimes_{\Lambda} \mathcal{L}$ such that $e_{prim}\left(\mathfrak{h}_{\infty}^{ord} \otimes_{\Lambda} \mathcal{L}\right) = \prod \mathcal{K}$ is a product of fields (finite extensions of $\mathcal{L}$). Making a finite extension of $F_{\mathfrak{p}}$ if necessary, one may assume the $F_{\mathfrak{p}}$ is equal to the algebraic closure of $\mathbb{Q}_p$ in $\mathcal{K}$ (i.e. "$\mathcal{K}$ is defined over $F_{\mathfrak{p}}$" in the terminology of [Hi 2, p.252]) for each $\mathcal{K}$. As in [Hi 1, p.554], fix one of the factors $\mathcal{K}$, and put

$$\begin{aligned} \mathfrak{h}(\mathcal{K}) &= \text{the image of } \mathfrak{h}_{\infty}^{ord} \text{ in } \mathcal{K}. \\ \cap & \\ \widetilde{\mathfrak{h}}(\mathcal{K}) &= \text{the free } \Lambda\text{-closure of } \mathfrak{h}(\mathcal{K}) \text{ in } \mathcal{K}. \\ \cap & \\ \mathcal{J}(\mathcal{K}) &= \text{the normalization of } \Lambda \text{ in } \mathcal{K}. \end{aligned}$$

Equivalently, $\widetilde{\mathfrak{h}}(\mathcal{K})$ is the intersection $\bigcap_P \mathfrak{h}(\mathcal{K})_P \subset \mathfrak{h}(\mathcal{K}) \otimes_{\Lambda} \mathcal{L}$, where P runs through height one prime ideals of Λ. Denote

$$\mathfrak{h}^{prim} := \prod_{\mathcal{K}} \mathfrak{h}(\mathcal{K}) \subset \mathcal{J} = \prod_{\mathcal{K}} \mathcal{J}(\mathcal{K}).$$

(1.4.5) Fix a topological generator γ of Γ. For an integer $k \geq 2$ and a character $\varepsilon : \Gamma \to \mathcal{O}^{\times}$ of finite order, we put

$$P_{k,\varepsilon} = \imath(\gamma) - \varepsilon(\gamma)\gamma^{k-2} \in \Lambda.$$

We define an arithmatic point of any finite Λ-algebra A to be a prime ideal $\mathfrak{p} \in \mathrm{Spec}(A)$ lying above some prime ideal $P = (P_{k,\varepsilon}) \in \mathrm{Spec}(\Lambda)$. The set of arithmetic points of A will be denoted by $\mathfrak{X}^{arith}(A)$.

(1.4.6) PROPOSITION. *(i) [Hi 1] The "restriction map" $\mathrm{Spec}(\mathcal{J}) \longrightarrow \mathrm{Spec}(\mathfrak{h}^{prim})$ gives a bijection $\mathfrak{X}^{arith}(\mathcal{J}) \xrightarrow{\sim} \mathfrak{X}^{arith}(\mathfrak{h}^{prim})$.*
(ii) [Hi 1, Cor. 1.4] For every $\mathcal{P} \in \mathfrak{X}^{arith}(\mathfrak{h}^{prim})$ and the corresponding $\mathcal{P}' \in \mathfrak{X}^{arith}(\mathcal{J})$ above $P = (P_{k,\varepsilon}) \in \mathrm{Spec}(\Lambda)$, the localization $(\mathfrak{h}^{prim})_{\mathcal{P}} = \mathcal{J}_{\mathcal{P}'}$ is a discrete valuation ring unramified over Λ_P.

(iii) [Hi 1, Cor. 1.3] For every arithmetic point $\mathcal{P} \in \mathfrak{X}^{arith}(\mathfrak{h}^{prim})$, the map $\mathcal{O} \hookrightarrow \mathfrak{h}^{prim} \longrightarrow \mathfrak{h}^{prim}/\mathcal{P}$ is an isomorphism and the homomorphism

$$\mathfrak{h}_\infty^{ord} \longrightarrow \mathfrak{h}^{prim} \longrightarrow \mathfrak{h}^{prim}/\mathcal{P} \xleftarrow{\sim} \mathcal{O}$$

corresponds to an ordinary p-stabilized newform f of tame level N. Conversely, every f arises in this way, for a unique $\mathcal{P} \in \mathfrak{X}^{arith}(\mathfrak{h}^{prim})$.

Remark. (i) follows from the fact that

$$\mathfrak{h}(\mathcal{K}) \otimes_\Lambda \Lambda_P = \widetilde{\mathfrak{h}}(\mathcal{K}) \otimes_\Lambda \Lambda_P = \mathcal{J}(\mathcal{K}) \otimes_\Lambda \Lambda_P$$

for every $P = (P_{k,\varepsilon})$. The first equality holds because $\widetilde{\mathfrak{h}}(\mathcal{K})/\mathfrak{h}(\mathcal{K})$ is a pseudo-null Λ-module. The second follows from the proof of [Hi 1, Cor.1.4].

(1.4.7) In the notation of 1.3, let f be an ordinary p-stabilized newform on $\Gamma_1(Np^r)$ of weight $k_0 \geq 2$ and character $\chi : (\mathbb{Z}/Np^r\mathbb{Z})^\times \to \mathcal{O}^\times$. The homomorphism $\mathfrak{h}_\infty^{ord} \to \mathcal{O}$ corresponding to f factors through a unique local factor R of $\mathfrak{h}_\infty^{ord}$ and through a unique simple factor $\mathcal{K}$ of $e_{prim}(R \otimes_\Lambda \mathcal{L})$. Replacing $F_\mathfrak{p}$ by a finite extension if necessary, we may assume that $\mathcal{K}$ is defined over $F_\mathfrak{p}$, in the language of 1.4.4. Write $e_{prim}(R \otimes_\Lambda \mathcal{L}) = \mathcal{K} \times \mathcal{A}$, and define $\mathfrak{h}(\mathcal{A})$ to be the image of R in $\mathcal{A}$, and $\widetilde{\mathfrak{h}}(\mathcal{A})$ the free Λ-closure of $\mathfrak{h}(\mathcal{A})$ in $\mathcal{A}$. Hida [Hi 2, p.253] defines the congruence module $C = C(\mathcal{K})$ by the exact sequence

$$0 \longrightarrow R \longrightarrow \widetilde{\mathfrak{h}}(\mathcal{K}) \oplus \widetilde{\mathfrak{h}}(\mathcal{A}) \longrightarrow C \longrightarrow 0.$$

It is shown in [Hi 2, Thm. 3.6, Cor. 3.8] that C is a torsion Λ-module and $C/P_{k,\varepsilon}C$ is finite (for all integers $k \geq 2$ and characters of finite order $\varepsilon : \Gamma \to \mathcal{O}^\times$).

Denote by $\omega : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{Z}_p^\times$ the Teichmüller character and decompose $\chi\omega^{k_0-2} = \psi\varepsilon$ into its tame, $\psi : (\mathbb{Z}/Np\mathbb{Z})^\times \to \mathcal{O}^\times$, and wild, $\varepsilon : \Gamma \to \Gamma/\Gamma^{p^{r-1}} \to \mathcal{O}^\times$, parts. Denote by $\overline{\mathcal{P}} \in \mathfrak{X}^{arith}(\mathfrak{h}(\mathcal{K}))$ the arithmetic point corresponding to f (lying above $P = (P_{k_0,\varepsilon}) \in \mathrm{Spec}(\Lambda)$) and by $\mathcal{P} \in \mathfrak{X}^{arith}(R)$ its preimage in R. Localizing the exact sequence

$$0 \longrightarrow R \longrightarrow \mathfrak{h}(\mathcal{K}) \oplus \mathfrak{h}(\mathcal{A}) \longrightarrow C' \longrightarrow 0$$

(where $C' \subset C$ is a subgroup of finite index) at $\mathcal{P}$, we get

$$R_\mathcal{P} \xrightarrow{\sim} \mathfrak{h}(\mathcal{K})_{\overline{\mathcal{P}}} \oplus \mathfrak{h}(\mathcal{A})_\mathcal{P}.$$

As $\mathfrak{h}(\mathcal{K})_{\overline{\mathcal{P}}} \neq 0$, this implies that $\mathfrak{h}(\mathcal{A})_\mathcal{P} = 0$ (which also follows from the multiplicity one statement of Prop. 1.4.6(iii)), hence $R_\mathcal{P} \xrightarrow{\sim} \mathfrak{h}(\mathcal{K})_{\overline{\mathcal{P}}}$ is a discrete valuation ring, unramified over Λ_P. One obtains in this way an embedding

$$\mathfrak{h}(\mathcal{K}) \hookrightarrow \mathcal{F}_c = \left\{ \sum_{i \geq 0} u_i(x-k_0)^i : u_i \in F_\mathfrak{p}, \lim_{i\to\infty} \mathrm{ord}_p(u_i) + ci = +\infty \right\} \subseteq F_\mathfrak{p}[[x-k_0]]$$

for a suitable integer $c \geq 0$ (cf. [Gr-St, 2.7]). The composite map

$$Z_N \hookrightarrow \mathcal{O}[[Z_N]] \longrightarrow \mathfrak{h}(\mathcal{K}) \hookrightarrow F_\mathfrak{p}[[x-k_0]]$$

is equal to

$$t \longmapsto \psi(t)\varepsilon(t)\kappa(t)^{x-2} = \chi(t)\omega(t)^{k_0-2}\kappa(t)^{x-2},$$

where κ is the projection to the group of principal units $1 + p\mathbb{Z}_p$.

For $k \in k_0 + p^c\mathbb{Z}_p$, the evaluation map "$x = k$" $\mathrm{ev}_k : \mathcal{F}_c \longrightarrow F_\mathfrak{p}$ is well defined. If $k \equiv k' \pmod{p^{n+c}}$ for $n \geq 0$, then $\mathrm{ev}_k \equiv \mathrm{ev}_{k'} \pmod{p^n}$.

For every integer $k \geq 2$ satisfying $k \equiv k_0 \pmod{p^c}$,

$$\mathcal{P}_k := \mathrm{Ker}\left(\mathfrak{h}(\mathcal{K}) \hookrightarrow \mathcal{F}_c \xrightarrow{\mathrm{ev}_k} F_\mathfrak{p}\right)$$

is an arithmetic point of $\mathfrak{h}(\mathcal{K})$ above $(P_{k,\varepsilon})$. It corresponds to a p-stabilized newform f_k on $\Gamma_1(Np^r)$ of weight k and character $\chi\omega^{k_0-k}$. If $k' \geq 2$ is an integer satisfying $k \equiv k' \pmod{p^{n+c}}$ (for some $n \geq 0$), then the two morphisms

$$\mathfrak{h}(\mathcal{K}) \longrightarrow \mathfrak{h}(\mathcal{K})/\mathcal{P}_k = \mathcal{O}, \qquad \mathfrak{h}(\mathcal{K}) \longrightarrow \mathfrak{h}(\mathcal{K})/\mathcal{P}_{k'} = \mathcal{O}$$

are congruent $\pmod{p^n}$, i.e. $f_k \equiv f_{k'} \pmod{p^n}$.

(1.5) Big Galois representations

The assumptions are as in 1.4 (but we do not assume that $F_\mathfrak{p}$ is "big enough" as in 1.4.4–7).

(1.5.1) Denote by $J_1(M) = \mathrm{Pic}^0(X_1(M))$ the Jacobian of the modular curve $X_1(M)_{/\mathbb{Q}}$ (for $M > 4$). The degeneracy maps $\pi_1 : X_1(Np^{r+1}) \to X_1(Np^r)$ induce maps on p-primary torsion

$$\pi_1^* : J_1(Np^r)(\overline{\mathbb{Q}})_{p^\infty} \longrightarrow J_1(Np^{r+1})(\overline{\mathbb{Q}})_{p^\infty}.$$

The inductive limit

$$J_\infty = \varinjlim_{\pi_1^*} \left(J_1(Np^r)(\overline{\mathbb{Q}})_{p^\infty}\right) \otimes_{\mathbb{Z}_p} \mathcal{O}$$

is an $\mathfrak{h}_{2,\infty}$-module; denote by $J_\infty^{ord} = eJ_\infty$ its ordinary part, which is a module over $\mathfrak{h}_\infty^{ord}$. Fix one of the local factors R of $\mathfrak{h}_\infty^{ord}$ and denote by $e_R \in \mathfrak{h}_\infty^{ord}$ the corresponding idempotent. The "big Galois representation" we are most interested in is

$$T(R) = \mathrm{Hom}_\mathcal{O}\left(e_R J_\infty^{ord}, \mu_{p^\infty} \otimes_{\mathbb{Z}_p} \mathcal{O}\right).$$

It is an R-module of finite type with a continuous R-linear action of $G_{\mathbb{Q},S}$ (with $S = \{\ell : \ell \mid Np\} \cup \{\infty\}$).

(1.5.2) PROPOSITION. *(i) (Eichler-Shimura relation) For every prime $\ell \nmid Np$, the relation*

$$T(\ell)_{\mathrm{Alb}} = \mathrm{Fr}(\ell)^{-1}_{\mathrm{geom}} + \ell < \ell >_{\mathrm{Alb}} \mathrm{Fr}(\ell)_{\mathrm{geom}}$$

holds in $\mathrm{End}_R(T(R))$.

(ii) [Ma-Ti, Thm. 7] If $T(R)$ has an irreducible residual representation, then R is a Gorenstein ring and $T(R)$ is free of rank two over R.

(iii) [Ti 1, Sect.4] Let $a \in \mathbb{Z}/(p-1)\mathbb{Z}$ be the exponent such that $(\mathbb{Z}/p\mathbb{Z})^\times \subset Z_N$ acts on R by ω^a. If $a \neq 0, -1 \pmod{(p-1)}$, then there is a canonical exact sequence of $R[G_{\mathbb{Q}_p}]$-modules

$$0 \longrightarrow T(R)^+ \longrightarrow T(R) \longrightarrow T(R)^- \longrightarrow 0$$

such that $T(R)^+ \xrightarrow{\sim} R$ and $T(R)^- \xrightarrow{\sim} \omega_R := \mathrm{Hom}_\Lambda(R, \Lambda)$ as R-modules, and the inertia subgroup $I_p \subset G_{\mathbb{Q}_p}$ acts trivially on $T(R)^-$ and by $\chi_{\mathrm{cycl}} < \chi_{\mathrm{cycl}} >_{\mathrm{Alb}}$ on $T(R)^+$, where

$$\chi_{\mathrm{cycl}} : G_{\mathbb{Q}_p} \to Gal(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p) \xrightarrow{\sim} \mathbb{Z}_p^\times$$

is the cyclotomic character.

(1.5.3) A few remarks are in order.

(1) As $H^1(\overline{X_1(Np^r)}_{et}, \mu_{p^\infty}) = J_1(Np^r)(\overline{\mathbb{Q}})_{p^\infty}$, the statement (i) follows from the Eichler-Shimura relation 1.2.11.

(2) A residual representation of $T(R)$ is a representation $\rho : G_{\mathbb{Q},S} \to GL_2(R/\mathfrak{m})$, (where $\mathfrak{m}$ is the maximal ideal of R) such that the characteristic polynomial of $\overline{\rho}(\mathrm{Fr}(\ell)^{-1}_{\mathrm{geom}})$ is equal to $X^2 - T(\ell)_{\mathrm{Alb}}X + \ell < \ell >_{\mathrm{Alb}} \pmod{\mathfrak{m}}$ for all primes $\ell \nmid Np$.

(3) $\overline{\rho}$ is irreducible if and only if $\overline{\rho}$ is absolutely irreducible, because $\overline{\rho}$(complex conjugation) has two distinct eigenvalues $\pm 1 \in R/\mathfrak{m}$ (recall that $\mathrm{char}(R/\mathfrak{m}) = p \neq 2$).

(4) As R is finite and flat over the regular ring Λ, it is Cohen-Macaulay and $\omega_R = \mathrm{Hom}_\Lambda(R, \Lambda)$ is a dualizing module of R [Br-He, Thm. 3.3.7(b)]. In particular, R is Gorenstein if and only if ω_R is free of rank one over R.

(5) The statement (iii) of Proposition 1.5.2 probably holds also for $a \equiv 0 \pmod{(p-1)}$.

(1.5.4) PROPOSITION. *In the notation of Proposition 1.5.2 (iii), assume that* $a \equiv 0 \pmod{(p-1)}$ *and that* $T(R)$ *admits an irreducible residual representation. Then the conclusions of Proposition 1.5.2 (iii) hold, with both* $T(R)^{\pm}$ *free of rank one over* R.

Proof. By Prop. 1.5.2 (ii), $T(R)$ is free of rank two over R. By a version of 1.3.5.1 over $R/\mathfrak{m}$ ([Ti 2, Thm. 3.2]), the inertia subgroup $I_p \subset G_{\mathbb{Q}_p}$ acts on $\overline{\rho}$ by

$$\begin{pmatrix} \omega^{1+a} & * \\ 0 & 1 \end{pmatrix}$$

As $a \neq -1 \pmod{(p-1)}$, we have $\omega^{1+a} \neq 1$, which means that $\overline{\rho}$ is "distinguished" in the sense of [Ti 2, Def. 3.3], [Wi 2, p. 481]. Fix $r \geq 1$ and consider the quotient $T(R)/\omega_{2,r}T(R)$ as a module over $R_r = R/\omega_{2,r}R$. It follows from [Ti 2, Theorem 3.4] and its proof and [Wi 2, Thm. 2.1, Cor. 1] that there is an exact sequence of $R_r[G_{\mathbb{Q}_p}]$-modules

$$0 \longrightarrow F_r^+ \longrightarrow T(R)/\omega_{2,r}T(R) \longrightarrow F_r^- \longrightarrow 0$$

with $F_r^{\pm}$ free of rank one over R_r and I_p acting on $F_r^{\pm}$ as in Proposition 1.5.2 (iii) (freeness of $F_r^{\pm}$ follows from Nakayama's lemma, because it holds $\pmod{\mathfrak{m}}$. As $\omega^{1+a} \neq 1$, $F_{r+1}^{\pm}$ map to $F_r^{\pm}$ under the canonical maps $T(R)/\omega_{2,r+1}T(R) \to T(R)/\omega_{2,r}T(R)$, and hence we get in the limit the desired sequence

$$0 \longrightarrow \varprojlim_r F_r^+ \longrightarrow T(R) \longrightarrow \varprojlim_r F_r^- \longrightarrow 0.$$

(1.5.5) Assume that $a \neq -1 \pmod{(p-1)}$ and that $T(R)$ has an irreducible residual representation. Let $\mathcal{P} \in \mathfrak{X}^{arith}(R)$ be an arithmetic point corresponding to an ordinary eigenform g of weight k on $\Gamma_1(Np^r)$. It is not necessarily a newform, but there is a unique newform f of weight k and character χ on $\Gamma_1(M)$ for some $M \mid Np^r$ with the same set of Hecke eigenvalues $\{a_\ell : \ell \nmid Np\}$. The quotient $T(R)/\mathcal{P}T(R)$ is free of rank two over $\mathcal{O}' = R/\mathcal{P}$. Tensoring with the fraction field $F'_{\mathfrak{p}}$ of $\mathcal{O}'$ we get a two-dimensional representation of $G_{\mathbb{Q},S}$ over $F'_{\mathfrak{p}}$ such that $\mathrm{Fr}(\ell)^{-1}_{\mathrm{geom}}$ satisfies the equation

$$X^2 - a_\ell X + \ell^{k-1}\chi(\ell) = 0$$

for all primes $\ell \nmid Np$. By the Čebotarev density theorem and irreducibility of $\rho_{f,\mathfrak{p}}$, it follows that the Galois representation $(T(R)/\mathcal{P}T(R)) \otimes_{\mathcal{O}'} F'_{\mathfrak{p}}$ is isomorphic to the

base change $-\otimes_{F_\mathfrak{p}} F'_\mathfrak{p}$ of the dual of $\rho_{f,\mathfrak{p}}$, namely

$$\rho^*_{f,\mathfrak{p}} \simeq \rho_{f,\mathfrak{p}}(k-1)\otimes[\chi^{-1}].$$

In the notation of 1.3.5, $(T(R)^\pm/\mathcal{P}T(R)^\pm)\otimes_{\mathcal{O}'} F'_\mathfrak{p}$ corresponds to $F^\pm M_\mathfrak{p}(k-1)\otimes[\chi^{-1}]$.

(1.5.6) If $a \neq 0,-1 \pmod{(p-1)}$, but without any assumptions on a residual representation, let $\mathcal{P}\in\mathfrak{X}^{arith}(R)$ correspond to a p-stabilized newform f. As in 1.4.6–7, there is a unique simple component $\mathcal{K}$ of $R\otimes_\Lambda \mathcal{L}$ through which $R\to R/\mathcal{P}$ factors. Denote by $\overline{\mathcal{P}}\in\mathfrak{X}^{arith}(\mathfrak{h}(\mathcal{K}))$ the arithmetic point of $\mathfrak{h}(\mathcal{K})$ corresponding to f. Then $\mathcal{P}=\mathrm{pr}^{-1}(\overline{\mathcal{P}})$, where $\mathrm{pr}: R\to\mathfrak{h}(\mathcal{K})$ is the canonical projection. For every pair of R-modules M,N one has

$$\mathrm{Tor}_i^R(M,N)_\mathcal{P}\simeq \mathrm{Tor}_i^{R_\mathcal{P}}(M_\mathcal{P},N_\mathcal{P}).$$

In particular,

$$\mathrm{Supp}(\mathrm{Tor}_i^R(R/\mathcal{P},\omega_R))\subseteq \mathrm{Supp}(R/\mathcal{P})=\{\mathcal{P},\mathfrak{m}\}.$$

On the other hand, $R_\mathcal{P}$ is a discrete valuation ring (by 1.4.7), and hence $(\omega_R)_\mathcal{P}\xrightarrow{\sim}\omega_{R_\mathcal{P}}=R_\mathcal{P}$ and

$$\mathrm{Tor}_i^R(R/\mathcal{P},\omega_R)_\mathcal{P}=\begin{cases} k(\mathcal{P}) & if\ i=0\\ 0 & if\ i>0.\end{cases}$$

It follows that $\mathrm{Tor}_i^R(R/\mathcal{P},\omega_R)$ is finite for $i>0$ and $\omega_R/\mathcal{P}\omega_R\xrightarrow{\sim}R/\mathcal{P}\oplus(\text{finite})$. In the exact sequence

$$\mathrm{Tor}_1^R(R/\mathcal{P},T(R)^-)\xrightarrow{\partial}T(R)^+/\mathcal{P}T(R)^+\longrightarrow T(R)/\mathcal{P}T(R)\longrightarrow T(R)^-/\mathcal{P}T(R)^-\longrightarrow 0$$

the second term is free over $R/\mathcal{P}$, hence flat over $\mathcal{O}$. The first term being $\mathcal{O}$-torsion by the previous discussion, we see that the map ∂ must be zero. As a result, we get an exact sequence

$$0\longrightarrow T(R)^+/\mathcal{P}T(R)^+\longrightarrow T(R)/\mathcal{P}T(R)\longrightarrow T(R)^-/\mathcal{P}T(R)^-\longrightarrow 0,$$

in which $T(R)^+/\mathcal{P}T(R)^+$ is free of rank one over $R/\mathcal{P}=\mathcal{O}'$ and $T(R)^-/\mathcal{P}T(R)^-$ is the sum of a free rank one $R/\mathcal{P}$-module and a finite group. As in 1.5.5, the Galois representation $(T(R)/\mathcal{P}T(R))\otimes_{\mathcal{O}'}F'_\mathfrak{p}$ is isomorphic to the base change of $\rho^*_{f,\mathfrak{p}}$, where f is the p-stabilized newform corresponding to $\mathcal{P}$. Similarly, $T(R)^\pm/\mathcal{P}T(R)^\pm\otimes_{\mathcal{O}'}F'_\mathfrak{p}$ corresponds to $F^\pm M_\mathfrak{p}(k-1)\otimes[\chi^{-1}]$.

(1.6) Self duality of $T(R)$

The results of this section are well known, but we were unable to find a good reference that would cover all of them. The notation is as in 1.4.

(1.6.1) For every integer $r\geq 1$, put $\Delta_r=(\mathbb{Z}/Np^r\mathbb{Z})^\times$, and

$$X_r:=H^1(\overline{X_1(Np^r)}_{et},\mathcal{O})=H^1(\overline{X_1(Np^r)}_{et},\mathbb{Z}_p)\otimes_{\mathbb{Z}_p}\mathcal{O}=T_p(J_1(Np^r))(-1)\otimes_{\mathbb{Z}_p}\mathcal{O}.$$

Poincaré duality gives an $\mathcal{O}$-bilinear skew-symmetric perfect pairing

$$\langle\ ,\ \rangle_{P,r}: X_r\times X_r\longrightarrow H^2_{et}(\overline{X_1(Np^r)}_{et},\mathcal{O})\xrightarrow[\sim]{\mathrm{Tr}}\mathcal{O}(-1),$$

which induces an isomorphism

$$\begin{aligned} X_r &\xrightarrow{\sim}\mathrm{Hom}_\mathcal{O}(X_r,\mathcal{O})(-1)\\ x &\longmapsto (y\mapsto\langle x,y\rangle_{P,r})\end{aligned}$$

of $\mathcal{O}[G_{\mathbb{Q}}]$-modules. In other words, the Galois action satisfies

$$\langle g(x), g(y)\rangle_{P,r} = g(\langle x, y\rangle_{P,r}) = \chi_{\mathrm{cycl}}^{-1}(g)\langle x, y\rangle_{P,r},$$

where $g \in G_{\mathbb{Q}}$, $x, y \in X_r$, and $\chi_{\mathrm{cycl}} : G_{\mathbb{Q}} \to \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \xrightarrow{\sim} \mathbb{Z}_p^\times$ is the cyclotomic character given by the action on μ_{p^∞}. In this section, we denote by

$$\chi_{\mathrm{cycl},N} : G_{\mathbb{Q}} \longrightarrow \mathrm{Gal}(\mathbb{Q}(\mu_{Np^\infty})/\mathbb{Q}) \xrightarrow{\sim} \Delta_\infty = \varprojlim_r \Delta_r$$

the character taking into account also the action on μ_N.

(1.6.2) The pairing $\langle\ ,\ \rangle_{P,r}$ is functorial as follows:

Hecke operators:

$$\begin{aligned} \langle T(n)_{\mathrm{Alb}}(x), y\rangle_{P,r} &= \langle x, T(n)_{\mathrm{Pic}}(y)\rangle_{P,r} \qquad (n \geq 1), \\ \langle < a >_{\mathrm{Alb}} (x), y\rangle_{P,r} &= \langle x, < a >_{\mathrm{Pic}} (y)\rangle_{P,r} \qquad (a \in \Delta_r). \end{aligned} \tag{1.6.2.1}$$

Degeneration maps:

$\pi_1, \pi_p : X_1(Np^{r+1}) \to X_1(Np^r)$ satisfy $\langle \pi_{i*}(x), y\rangle_{P,r} = \langle x, \pi_i^*(y)\rangle_{P,r+1}$.

Fricke involutions:

Fix a compatible system of primitive Np^r-th roots of unity $\zeta_{Np^r} \in \mu_{Np^r}$, $\zeta_{Np^{r+1}}^p = \zeta_{Np^r}$, and put $W_r := W_{\zeta_{Np^r}}$. Then $\langle W_r(x), W_r(y)\rangle_{P,r} = \langle x, y\rangle_{P,r}$.

(1.6.3) We define a twisted pairing (depending on the choice of ζ_{Np^r})

$$\begin{aligned} (\ ,\ )_r : X_r \times X_r &\longrightarrow \mathcal{O}(-1), \\ (x, y)_r &= \langle x, W_r(y)\rangle_{P,r} \end{aligned}$$

This is again skew-symmetric and $\mathcal{O}$-bilinear. The formulas (1.6.2.1) and (1.2.8.1,3) imply

$$\begin{aligned} (T(n)_{\mathrm{Alb}}(x), y)_r &= \langle x, T(n)_{\mathrm{Pic}} W_r(y)\rangle_{P,r} = \langle x, W_r T(n)_{\mathrm{Alb}}(y)\rangle_{P,r} \\ &= (x, T(n)_{\mathrm{Alb}}(y))_r \qquad (n \geq 1) \end{aligned} \tag{1.6.3.1}$$

and $(< a >_{\mathrm{Alb}} (x), y)_r = (x, < a >_{\mathrm{Alb}} (y))_r$, for $a \in \Delta_r$. For $g \in G_{\mathbb{Q}}$, we have (by 1.6.1 and (1.2.8.2))

$$\begin{aligned} &\chi_{\mathrm{cycl}}^{-1}(g)(x, y)_r = \chi_{\mathrm{cycl}}^{-1}(g)\langle x, W_r(y)\rangle_{P,r} = \langle g(x), gW_r(y)\rangle_{P,r} \\ &= \langle g(x), W_r < \chi_{\mathrm{cycl},N}(g) >_{\mathrm{Alb}} g(y)\rangle_{P,r} = (g(x), < \chi_{\mathrm{cycl},N}(g) >_{\mathrm{Alb}} g(y))_r. \end{aligned}$$

Hence,

$$(g(x), g(y))_r = \chi_{\mathrm{cycl}}^{-1}(g)(x, < \chi_{\mathrm{cycl},N}(g) >_{\mathrm{Alb}}^{-1} y)_r. \tag{1.6.3.2}$$

The Hecke algebra $\mathfrak{h}_{2,r} = \mathfrak{h}(\Gamma_1(Np^r), \mathcal{O})$ acts on X_r by $T(n)_{\mathrm{Alb}}$ and $< a >_{\mathrm{Alb}}$. The formulas (1.6.3.1–2) can be reformulated by saying that the map

$$\begin{aligned} \alpha_r : X_r &\xrightarrow{\sim} \mathrm{Hom}_{\mathcal{O}}(X_r, \mathcal{O})(-1) \\ x &\longmapsto\ (y \mapsto (x, y)_r)) \end{aligned}$$

induces an isomorphism

$$\alpha_r : X_r \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{O}}(X_r, \mathcal{O})(-1) < -1 > \tag{1.6.3.3}$$

of $\mathfrak{h}_{2,r}[G_{\mathbb{Q}}]$-modules. Here, the notation $Y < n >$, for an $\mathfrak{h}_{2,r}[G_{\mathbb{Q}}]$-module Y and $n \in \mathbb{Z}$, means that the original Galois action by $g \in G_{\mathbb{Q}}$ on Y is multiplied by the action of $< \chi_{\mathrm{cycl},N}(g) >^n_{\mathrm{Alb}} \in \mathfrak{h}_{2,r}$.

Taking the limit $r \to \infty$

We know from 1.2.10 that the maps $X_{r+1} \xrightarrow{\pi_{i*}} X_r$ and $X_{r+1} \xleftarrow{\pi_i^*} X_r$ $(i = 1, p)$ are compatible (for $r \geq 1$) with the canonical maps $\mathfrak{h}_{2,r+1} \to \mathfrak{h}_{2,r}$. Note that, by 1.2.9,

$$\begin{aligned}(\pi_{i*}(x), y)_r &= \langle \pi_{i*}(x), W_r(y)\rangle_{P,r} = \langle x, \pi_i^* W_r(y)\rangle_{P,r+1} \\ &= \langle x, W_{r+1}\pi_{p/i}^*(y)\rangle_{P,r+1} = (x, \pi_{p/i}^*(y))_{r+1}.\end{aligned} \tag{1.6.3.4}$$

This means that the isomorphisms α_r induce in the limit an isomorphism of $\mathfrak{h}_{2,\infty}[G_{\mathbb{Q}}]$-modules

$$\begin{aligned}\alpha_\infty : \varprojlim_{\pi_{p*}} X_r &\xrightarrow{\sim} \mathrm{Hom}_{\mathcal{O}}(\varinjlim_{\pi_1^*}(X_r \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p), \mathcal{O} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)(-1) < -1 > \\ &= \mathrm{Hom}_{\mathcal{O}}(J_\infty, \mathcal{O} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p) < -1 >\end{aligned} \tag{1.6.3.5}$$

(this is because the right hand side of (1.6.3.3) is canonically isomorphic to $\mathrm{Hom}_{\mathcal{O}}(X_r \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p, \mathcal{O} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)(-1) < -1 >$).

(1.6.4) LEMMA. *Let $\mathcal{O}$ be a commutative ring, Δ a finite group and X a left $\mathcal{O}[\Delta]$-module. Let $f \in \mathrm{Hom}_{\mathcal{O}}(X, \mathcal{O})$, $F \in \mathrm{Hom}_{\mathcal{O}[\Delta]-\mathrm{left}}(X, \mathcal{O}[\Delta])$. Then*
(i) The formulas $(f * a)(x) = f(ax)$, $(F * a)(x) = F(x)[a]$ $(a \in \Delta,\ x \in X)$ define right actions of Δ on $\mathrm{Hom}_{\mathcal{O}}(X, \mathcal{O})$ and $\mathrm{Hom}_{\mathcal{O}[\Delta]-\mathrm{left}}(X, \mathcal{O}[\Delta])$.
(ii) the formulas

$$(\Phi(f))(x) = \sum_{a \in \Delta} f(a(x))[a^{-1}], \qquad (\Psi(F))(x) = \mathrm{pr}_e(F(x)),$$

define mutually inverse isomorphisms of right $\mathcal{O}[\Delta]$-modules

$$\mathrm{Hom}_{\mathcal{O}}(X, \mathcal{O}) \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \mathrm{Hom}_{\mathcal{O}[\Delta]-\mathrm{left}}(X, \mathcal{O}[\Delta])$$

(here, $\mathrm{pr}_b(\sum_{a \in \Delta} n_a[a]) = n_b$ for $b \in \Delta$, and $e \in \Delta$ is the identity element).

Proof. Straightforward calculation.

If Δ is commutative, the formulas in (i) can be used to define a left action of Δ : $a * f := f * a$, $a * F := F * a$, and (ii) will be an isomorphism of left $\mathcal{O}[\Delta]$-modules.

(1.6.5) Applying Lemma 1.6.4 to $X = X_r$ and $\Delta = \Delta_r$, the formula defining Φ gives yet another skew-symmetric pairing, this time with values in the group ring $\mathcal{O}[\Delta_r]$:

$$\begin{aligned}\langle\ ,\ \rangle_{\Delta_r} &: X_r \times X_r \longrightarrow \mathcal{O}[\Delta_r] \\ \langle x, y\rangle_{\Delta_r} &= \sum_{a \in \Delta_r} (x, < a >_{\mathrm{Alb}} y)_r [a]^{-1}.\end{aligned}$$

It satisfies

$$\begin{aligned}\langle T(n)_{\mathrm{Alb}}(x), y\rangle_{\Delta_r} &= \langle x, T(n)_{\mathrm{Alb}}(y)\rangle_{\Delta_r} \qquad (n \geq 1) \\ \langle < a >_{\mathrm{Alb}} (x), y\rangle_{\Delta_r} &= \langle x, < a >_{\mathrm{Alb}} (y)\rangle_{\Delta_r} = [a]\langle x, y\rangle_{\Delta_r} \qquad (a \in \Delta_r) \\ \langle g(x), g(y)\rangle_{\Delta_r} &= \chi_{\mathrm{cycl}}(g)^{-1}[\chi_{\mathrm{cycl},N}(g)^{-1}]\langle x, y\rangle_{\Delta_r} \qquad (g \in G_{\mathbb{Q}}).\end{aligned}$$

the induced map

$$\beta_r : X_r \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{O}[\Delta_r]}(X_r, \mathcal{O}[\Delta_r])(-1) < -1 >$$

(1.6.5.1)

$$x \longmapsto (y \mapsto \langle x, y \rangle_{\Delta_r})$$

is again an isomorphism of $\mathfrak{h}_{2,r}[G_{\mathbb{Q}}]$-modules, equal to $\Phi \circ \alpha_r$. The same is true of the projection of β_r to the ordinary component:

$$\beta_r^{ord} : eX_r \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{O}[\Delta_r]}(eX_r, \mathcal{O}[\Delta_r])(-1) < -1 >$$

(1.6.5.2)

$$x \longmapsto (y \mapsto \langle x, y \rangle_{\Delta_r})$$

This is an isomorphism of $\mathfrak{h}_{2,r}^{ord}[G_{\mathbb{Q}}]$-modules.

(1.6.6) LEMMA. *Fix $r \geq 1$. Then*

(i) $\pi_{1*}(eX_{r+1}) \subseteq p(eX_r)$. Denote by $\frac{1}{p}\pi_{1*} : eX_{r+1} \to eX_r$ the unique map satisfying $p \cdot (\frac{1}{p}\pi_{1*}) = \pi_{1*}$.

(ii) $(\frac{1}{p}\pi_{1*}) \circ \pi_1^* = p$ on eX_r.

(iii) $\pi_1^* \circ (\frac{1}{p}\pi_{1*}) = \sum_{a \in \Gamma_r/\Gamma_{r+1}} < a >_{\mathrm{Alb}}$ on eX_{r+1}, where $\Gamma_r = \Gamma^{p^{r-1}}$.

(iv) $T(p)_{\mathrm{Alb}} \circ (\frac{1}{p}\pi_{1*}) = \pi_{p*}$ on eX_{r+1}.

Proof. See 1.6.11 below.

(1.6.7) COROLLARY. *For $x, y \in eX_{r+1}$, $(r \geq 1)$, the canonical projection $\mathcal{O}[\Delta_{r+1}] \to \mathcal{O}[\Delta_r]$ maps $\langle x, y \rangle_{\Delta_{r+1}}$ to $\langle \pi_{p*}(x), \frac{1}{p}\pi_{1*}(y) \rangle_{\Delta_r}$.*

Proof. $\langle x, y \rangle_{\Delta_{r+1}}$ maps to

$$\sum_{a \in \Delta_r} \Big(\sum_{\substack{b \in \Delta_{r+1} \\ b \mapsto a}} (x, < b >_{\mathrm{Alb}} (y))_{r+1} \Big)[a^{-1}]$$

$$= \sum_{a \in \Delta_r} (x, \pi_1^* \circ (\frac{1}{p}\pi_{1*}) < a >_{\mathrm{Alb}} (y))_{r+1}[a^{-1}] \qquad \text{(by (1.6.6.iii))}$$

$$= \sum_{a \in \Delta_r} (\pi_{p*}(x), (\frac{1}{p}\pi_{1*}) < a >_{\mathrm{Alb}} (y))_r[a^{-1}] \qquad \text{(by (1.6.3.4))}$$

$$= \langle \pi_{p*}(x), \frac{1}{p}\pi_{1*}(y) \rangle_{\Delta_r}$$

as claimed.

(1.6.8) COROLLARY. *The map*

$$\gamma = (\gamma_r) : X = \varprojlim_{\pi_{p*}} eX_r \longrightarrow \varprojlim_{\frac{1}{p}\pi_{1*}} eX_r$$

$$(x_r)_{r \geq 1} \longmapsto (T(p)_{\mathrm{Alb}}^{r-1}(x_r))_{r \geq 1}$$

is an isomorphism of $\mathfrak{h}_{\infty}^{ord}[G_{\mathbb{Q}}]$-modules.

Proof. Follows immediately from Lemma 1.6.6 (iv).

(1.6.9) Combining the two corollaries, we obtain a skew-symmetric pairing on X:

$$\langle\ ,\ \rangle_X : \varprojlim_{\pi_{p*}} eX_r \times \varprojlim_{\pi_{p*}} eX_r \longrightarrow \Lambda(-1) < -1 >$$

given by $\langle (x_r), (y_r) \rangle_X = (\langle x_r, T(p)_{\mathrm{Alb}}^{r-1}(y)_r \rangle_{H_r})$.

THEOREM. $\langle\ ,\ \rangle_X$ *induces an isomorphism of* $\mathfrak{h}_\infty^{ord}[G_\mathbb{Q}]$*-modules* $\beta_\infty : X \xrightarrow{\sim} \mathrm{Hom}_\Lambda(X,\Lambda)(-1) < -1 >$, $(\beta_\infty(x))(y) = \langle x,y\rangle_X$. *In particular,* X *is free of finite rank over* Λ.

Proof. Firstly, the ordinary part of α_∞ gives an isomorphism

$$\alpha_\infty^{ord} : X \xrightarrow{\sim} \mathrm{Hom}_\mathcal{O}(eJ_\infty, \mathcal{O}\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p) < -1 >,$$

and we know that the right hand side is of finite type over $\mathfrak{h}_\infty^{ord}$. A fundamental result of Hida [Hi 1, Thm. 3.1] states that π_1^* induces isomorphisms

$$eJ_1(Np^r)(\overline{\mathbb{Q}})_{p^\infty} \xrightarrow{\sim} (eJ_\infty)^{\Gamma_r} \qquad (r \geq 1).$$

Dualizing – using (1.6.3.4) – we see that π_{p*} induces isomorphisms $X_{\Gamma_r} \xrightarrow{\sim} eX_r$. Together with (1.6.5.2), this implies that β_∞ is an isomorphism.

(1.6.10) As in 1.5.1, fix a local component R of $\mathfrak{h}_\infty^{ord}$. Let $X(R) = e_R X$ be the R-part of X. Then α_∞^{ord} induces an isomorphism

$$X(R) \xrightarrow{\sim} T(R)(-1) < -1 >$$

and $\langle\ ,\ \rangle_X$ defines a skew-symmetric pairing

$$\langle\ ,\ \rangle_{T(R)} : T(R)\times T(R) \longrightarrow \Lambda(1) < 1 >$$

inducing an isomorphism of $R[G_\mathbb{Q}]$-modules $T(R) \xrightarrow{\sim} \mathrm{Hom}_\Lambda(T(R),\Lambda)(1) < 1 >$. Whenever 1.5.2 (iii) or Proposition 1.5.4 apply, the pairing $\langle\ ,\ \rangle_{T(R)}$ induces isomorphisms of $R[G_\mathbb{Q}]$-modules $T(R)^\pm \xrightarrow{\sim} \mathrm{Hom}_\Lambda(T(R)^\mp,\Lambda)(1) < 1 >$. The canonical map of R-modules

$$\mathrm{Hom}_R(T(R), \mathrm{Hom}_\Lambda(R,\Lambda)) \longrightarrow \mathrm{Hom}_\Lambda(T(R),\Lambda)$$

is an isomorphism, and hence the pairing $\langle\ ,\ \rangle_{T(R)}$ induces an isomorphism of $R[G_\mathbb{Q}]$-modules

$$T(R) \xrightarrow{\sim} \mathrm{Hom}_R(T(R),\omega_R)(1) < 1 >$$

i.e. can be viewed as an R-bilinear pairing

$$T(R)\times T(R) \longrightarrow \omega_R(1) < 1 > .$$

(1.6.11) For the proof of Lemma 1.6.6, it will be convenient to use a group theoretic description of the Hecke operators. Let $\Gamma \subseteq SL_2(\mathbb{R})$ be a discrete subgroup of the form $\gamma\Gamma'\gamma^{-1}$, where $\gamma \in GL_2(\mathbb{Q})$ and $\Gamma' \subseteq SL_2(\mathbb{Z})$ is a congruence subgroup. Denote by $X(\Gamma) = \Gamma\backslash\mathcal{H}^*$ (where $\mathcal{H}^* = \mathcal{H}\cup\mathbb{P}^1(\mathbb{Q})$) the corresponding complex modular curve over $\mathbb{C}$. Let H be a reasonable cohomology theory, say $H^0(X,\Omega^1)$ or $H^1(\overline{X}_{et},\mathbb{Z}_p)$; put $H(\Gamma) = H(X(\Gamma))$.

Functoriality: $\gamma \in GL_2(\mathbb{Q})$ gives an isomorphism $[\gamma] : X(\Gamma) \to X(\gamma\Gamma\gamma^{-1})$, which induces an isomorphism

$$[\gamma]^* = [\gamma^{-1}]_* : H(\gamma\Gamma\gamma^{-1}) \xrightarrow{\sim} H(\Gamma).$$

Inclusion $i : \Gamma \hookrightarrow \Gamma'$ gives a finite map $X(\Gamma) \to X(\Gamma')$, which induces $i_* : H(\Gamma) \longrightarrow H(\Gamma')$, and $i^* : H(\Gamma') \longrightarrow H(\Gamma)$.

Double cosets: For $\gamma \in GL_2(\mathbb{Q})$ and $\Gamma_1,\Gamma_2 \subseteq GL_2(\mathbb{R})$ of the above form, the maps

$$\Gamma_1 \xleftarrow{i_1} \Gamma_1\cap\gamma\Gamma_2\gamma^{-1} \xrightarrow{[\gamma^{-1}]} \gamma^{-1}\Gamma_1\gamma\cap\Gamma_2 \xhookrightarrow{i_2} \Gamma_2$$

induce the action of the double coset

$$[\Gamma_1\gamma\Gamma_2] : H(\Gamma_1)\xrightarrow{i_1^*}H(\Gamma_1\cap\gamma\Gamma_2\gamma^{-1})\xrightarrow{[\gamma^{-1}]_*}H(\gamma^{-1}\Gamma_1\gamma\cap\Gamma_2)\xrightarrow{i_{2*}}H(\Gamma_2).$$

In the coordinates on the upper half plane $\mathcal{H}$, $[\Gamma_1\gamma\Gamma_2]$ corresponds to $\sum_i(\gamma\alpha_i)^*$, where $\alpha_i \in GL_2(\mathbb{Q})$ are representatives of $(\gamma^{-1}\Gamma_1\gamma\cap\Gamma_2)\backslash\Gamma_2$ (equivalently, $\Gamma_1\gamma\Gamma_2 = \bigcup\Gamma_1\gamma\alpha_i$).

Example: $\Gamma_1 = \Gamma_2 = \Gamma = \Gamma_1(M)$, $\gamma = \begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}$, with p prime. Then

$$\Gamma_1(M)\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\Gamma_1(M) = \coprod_{i\in\mathbb{Z}/p\mathbb{Z}}\Gamma_1(M)\begin{pmatrix}1 & i\\ 0 & p\end{pmatrix} \quad \left(\cup\,\Gamma_1(M)\begin{pmatrix}p & 0\\ 0 & 1\end{pmatrix}\sigma_p \text{ if } p\nmid M\right),$$

where $\sigma_p \in SL_2(\mathbb{Z})$, $\sigma_p \equiv \begin{pmatrix}p^{-1} & 0\\ 0 & p\end{pmatrix} \pmod M$. The action of $[\Gamma\gamma\Gamma]$ on $H(\Gamma) = H^0(X(\Gamma),\Omega^1)$ gives the usual Hecke operator $T(p) = T(p)_{\mathrm{Alb}}$ on cusp forms of weight two on $\Gamma_1(M)$.

Proof of Lemma 1.6.6. Let

$$\gamma = \begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}, \quad \Gamma = \Gamma_1(Np^r) \supset \Gamma\cap\gamma\Gamma\gamma^{-1} = \Gamma_1(Np^r)\cap\Gamma_0(Np^{r+1}) \supset \Gamma' = \Gamma_1(Np^{r+1}),$$

where $r \geq 1$. Consider the maps

$$\begin{array}{ccccccc} & & \Gamma & & & & \\ & & \uparrow{\scriptstyle i_2} & & & & \\ \Gamma' & \xhookrightarrow{i_1} & \Gamma\cap\gamma\Gamma\gamma^{-1} & \xrightarrow{[\gamma^{-1}]} & \gamma^{-1}\Gamma\gamma\cap\Gamma & \xhookrightarrow{i_3} & \Gamma \end{array}$$

and their action on cohomology $H(X) = H^1(X,\mathbb{Z})\otimes_{\mathbb{Z}}\mathbb{Z}_p$. Each modular curve X corresponding to Γ, Γ', or $\Gamma\cap\gamma\Gamma\gamma^{-1}$ has a model $X_{/\mathbb{Q}}$, and hence $H(X) = H^1((X_{/\mathbb{Q}}\otimes_{\mathbb{Q}}\overline{\mathbb{Q}})_{et},\mathbb{Z}_p)$. By definition, we have

$$\begin{aligned} \pi_{1*} &= i_{2*}i_{1*} : H(\Gamma') \longrightarrow H(\Gamma)\\ \pi_{p*} &= i_{3*}[\gamma^{-1}]_*i_{1*} : H(\Gamma') \longrightarrow H(\Gamma)\\ T(p)_{\mathrm{Alb}} &= [\Gamma\gamma\Gamma] = i_{3*}[\gamma^{-1}]_*i_2^* : H(\Gamma) \longrightarrow H(\Gamma)\end{aligned}$$

Denote $[(\Gamma\cap\gamma\Gamma\gamma^{-1})\gamma(\Gamma\cap\gamma\Gamma\gamma^{-1})] : H(\Gamma\cap\gamma\Gamma\gamma^{-1}) \longrightarrow H(\Gamma\cap\gamma\Gamma\gamma^{-1})$ also by $T(p)_{\mathrm{Alb}}$. It follows from the definitions that the operator $\xi = [(\Gamma\cap\gamma\Gamma\gamma^{-1})\gamma\Gamma] = i_{3*}[\gamma^{-1}]_* : H(\Gamma\cap\gamma\Gamma\gamma^{-1}) \longrightarrow H(\Gamma)$ satisfies

$$\begin{aligned} \xi i_2^* &= T(p)_{\mathrm{Alb}} \qquad \text{on } H(\Gamma)\\ i_2^*\xi &= T(p)_{\mathrm{Alb}} \qquad \text{on } H(\Gamma\cap\gamma\Gamma\gamma^{-1})\end{aligned}$$

This fact – due to Shimura – is at the basis of all Hida's theory [Hi 1, Thm. 4.4]. Applying the ordinary projector $e = \lim_{n\to\infty}T(p)_{\mathrm{Alb}}^{n!}$, we see that i_2^* induces an isomorphism between the ordinary parts ([Hi 1, Cor. 4.5])

$$i_2^* : eH(\Gamma) \xrightarrow{\sim} eH(\Gamma\cap\gamma\Gamma\gamma^{-1}),$$

with inverse

$$(i_2^*)^{-1} = T(p)_{\mathrm{Alb}}^{-1}\xi = \xi T(p)_{\mathrm{Alb}}^{-1}.$$

As $i_{2*}i_2^* = p$, it follows that the map

$$(i_2^*)^{-1}i_{1*} : eH(\Gamma') \longrightarrow eH(\Gamma)$$

satisfies $p(i_2^*)^{-1}i_{1*} = i_{2*}i_{1*} = \pi_{1*}$, which proves Lemma 1.6.6 (i) and in fact shows that $\frac{1}{p}\pi_{1*} = (i_2^*)^{-1}i_{1*}$. The rest is easy:

$$\left(\frac{1}{p}\pi_{1*}\right)\pi_1^* = (i_2^*)^{-1}i_{1*}i_1^*i_2^* = p(i_2^*)^{-1}i_2^* = p \qquad \text{on } eH(\Gamma)$$

$$\pi_1^*(\frac{1}{p}\pi_{1*}) = i_1^*i_2^*(i_2^*)^{-1}i_{1*} = i_1^*i_{1*} = \sum_{a\in\Gamma_r/\Gamma_{r+1}} < a >_{\mathrm{Alb}} \qquad \text{on } eH(\Gamma').$$

The last equality here is because Γ' is a normal subgroup of $\Gamma\cap\gamma\Gamma\gamma^{-1}$, with quotient equal to Γ_r/Γ_{r+1}. Finally,

$$T(p)_{\mathrm{Alb}}(\frac{1}{p}\pi_{1*}) = \xi i_{2*}(i_2^*)^{-1}i_{1*} = \xi i_{1*} = i_{3*}[\gamma^{-1}]_*i_{1*} = \pi_{p*} \qquad \text{on } eH(\Gamma').$$

This finishes the proof of Lemma 1.6.6.

(1.6.12) The arguments in the previous section show that all the statements of Lemma 1.6.6 hold if eX_r is replaced by the maximal direct summand of $(X_r\otimes\mathbb{Q})$ on which $T(p)_{\mathrm{Alb}}$ is invertible (i.e. the sum of generalized eigenspaces of $T(p)_{\mathrm{Alb}}$ for non-zero eigenvalues).

(1.6.13) Using the formula $\pi_p\circ W_{r+1} = W_r\circ\pi_1$ (which follows from 1.2.9) and (1.2.8.3), (1.2.10), we see that the map

$$W = (W_r) : (x_r)_{r\geq 1} \longmapsto (W_r(x_r))_{r\geq 1}$$

induces an isomorphism of $\mathcal{O}$-modules

$$\varprojlim_{\pi_{1*}} e^*X_r \xrightarrow{\sim} \varprojlim_{\pi_{p*}} eX_r = X,$$

where $e^* = \lim_{n\to\infty} T(p)_{\mathrm{Pic}}^{n!}$ is Hida's dual projector.

2. Selmer groups in families.

(2.1) Generalities on Selmer groups

(2.1.1) Notation. Let p be a rational prime, $F_{\mathfrak{p}}$ a finite extension of $\mathbb{Q}_p$ with ring of integers $\mathcal{O} = \mathcal{O}_{\mathfrak{p}}$, and $\pi\in\mathcal{O}$ a prime element. Let K be a number field, S a finite set of primes of K containing all archimedean primes and all primes dividing p, and K_S the maximal extension of K unramified outside S. Let $S_f\subset S$ be the subset of non-archimedean primes. For $v\in S_f$, fix embeddings $\overline{K}\hookrightarrow\overline{K}_v$. They induce maps $G_v = \mathrm{Gal}(\overline{K}_v/K_v)\to G_K = \mathrm{Gal}(\overline{K}/K)\to G_{K,S} = \mathrm{Gal}(K_S/K)$.

(2.1.2) Let T be an $\mathcal{O}$-adic representation of $G_{K,S}$ (i.e. a free $\mathcal{O}$-module of finite rank equipped with a continuous $\mathcal{O}$-linear action of $G_{K,S}$). There is a tautological exact sequence

$$0\to T\xrightarrow{i}V\xrightarrow{\mathrm{pr}}A\longrightarrow 0$$

with $V = T\otimes_{\mathcal{O}}F_{\mathfrak{p}}$, $A = V/T$. All Galois cohomology groups with values in T or V will be continuous cohomology ([Ta], [Ja]). Recall that $H^i(G,V) = H^i(G,T)\otimes_{\mathcal{O}}F_{\mathfrak{p}}$

and that $H^i(G,T)$ coincides with the naive cohomology group

$$\varprojlim_n H^i(G, T/\pi^n T)$$

for $i \leq 1$ (resp. for all i if $G = G_v$ or $G_{K,S}$). For $G = G_v$ or $G_{K,S}$, the $\mathcal{O}$-modules $H^i(G,T)$ (resp. $H^i(G,A)$) are of finite (resp. co-finite) type.

(2.1.3) Recall Flach's abstract treatment of Selmer groups [Fl]. Given $F_\mathfrak{p}$-subspaces $W_v \subseteq H^1(G_v, V)$ for all $v \in S$, the Selmer groups associated to $W = (W_v)$ are defined by

$$S(K,A;W) = \mathrm{Ker}\left[H^1(G_{K,S},A) \to \bigoplus_{v\in S} H^1(G_v,A)/\mathrm{pr}_*(W_v)\right]$$

$$S(K,V;W) = \mathrm{Ker}\left[H^1(G_{K,S},V) \to \bigoplus_{v\in S} H^1(G_v,V)/W_v\right]$$

They do not change if S is replaced by $S' \supset S$ with $W_v = H^1_{ur}(G_v,V) = H^1(G_v/I_v,V)$ for $v \in S' - S$ (as $\mathrm{pr}_*(H^1_{ur}(G_v,V)) = H^1_{ur}(G_v,A)$ for such v). The $\mathcal{O}$-module $S(K,A;W)$ is of co-finite type and $\mathrm{pr}_*(S(K,V;W))$ coincides with its maximal $\mathfrak{p}$-divisible subgroup $S(K,A;W)_{\mathrm{div}}$, i.e. $S(K,A;W)_{\mathrm{div}} \xrightarrow{\sim} (F_\mathfrak{p}/\mathcal{O})^r$, where $r = \dim_{F_\mathfrak{p}} S(K,V;W)$, and the quotient $Ш(K,A;W) := S(K,A;W)/S(K,A;W)_{\mathrm{div}}$ is finite.

(2.1.4) Duality. Put $\mathbb{Z}_p(1) = \varprojlim_n \mu_{p^n}$, $\mathcal{O}(1) = \mathcal{O} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(1)$, $T^*(1) = \mathrm{Hom}_\mathcal{O}(T, \mathcal{O}(1))$, $V^*(1) = T^*(1) \otimes_\mathcal{O} F_\mathfrak{p}$, $A^*(1) = V^*(1)/T^*(1)$. For $v \in S_f$, let $W_v^\perp \subseteq H^1(G_v, V^*(1))$ be the annihilator of W_v under Tate's local duality

$$H^1(G_v,V) \times H^1(G_v,V^*(1)) \xrightarrow{\cup} H^2(G_v,F_\mathfrak{p}(1)) \xrightarrow{\sim} F_\mathfrak{p}.$$

For $v \nmid p$, $H^1_{ur}(G_v,V)^\perp = H^1_{ur}(G_v,V^*(1))$. Flach [Fl] constructed a pairing[(1)]

$$S(K,A;W) \times S(K,A^*(1);W^\perp) \longrightarrow F_\mathfrak{p}/\mathcal{O}$$

and showed that its left (resp. right) kernel is equal to $S(K,A;W)_{\mathrm{div}}$ (resp. $S(K,A;W^\perp)_{\mathrm{div}}$). In other words, the induced pairing

$$Ш(K,A;W) \times Ш(K,A^*(1);W^\perp) \longrightarrow F_\mathfrak{p}/\mathcal{O}$$

is non-degenerate.

(2.1.5) Let

$$\langle\ ,\ \rangle_V : V \times V \longrightarrow F_\mathfrak{p}(1)$$

be a Galois-invariant non-degenerate skew-symmetric bilinear form such that $T \times T$ is mapped to $\mathcal{O}(1)$. The formula $\alpha(x)(y) = \langle x,y\rangle_V$ defines an isomorphism of $F_\mathfrak{p}[G_{K,S}]$-modules $\alpha : V \xrightarrow{\sim} V^*(1)$ which is skew-symmetric (i.e. $\alpha^*(1) = -\alpha$) and such that $\alpha(T) \subseteq T^*(1)$. If the local conditions W are self dual in the sense that $\alpha_*(W_v) = W_v^\perp$ for all $v \in S$, then α induces a map

$$\alpha_* : S(K,A;W) \longrightarrow S(K,A^*(1);W^\perp)$$

---

(1) Flach considered only $F_\mathfrak{p} = \mathbb{Q}_p$, but the generalization to $F_\mathfrak{p}$-representations is straightforward.

with finite kernel and cokernel. The induced pairing

$$S(K,A;W)\times S(K,A;W)\xrightarrow{(id,\alpha_*)} S(K,A;W)\times S(K,A^*(1);W^\perp)\longrightarrow F_\mathfrak{p}/\mathcal{O}$$

is skew-symmetric [Fl].

(2.1.6) For $v \mid p$, Bloch-Kato [Bl-Ka, Sect.3] introduced subgroups $H^1_f(G_v,V)\subseteq H^1_g(G_v,V)\subseteq H^1(G_v,V)$ of a crystalline nature;

$$H^1_f(G_v,V)=\mathrm{Ker}\left[H^1(G_v,V)\longrightarrow H^1(G_v,V\otimes_{\mathbb{Q}_p}B_{cris})\right]$$
$$H^1_g(G_v,V)=\mathrm{Ker}\left[H^1(G_v,V)\longrightarrow H^1(G_v,V\otimes_{\mathbb{Q}_p}B_{dR})\right]$$

(see [Bures, Exp. II] for more details on Fontaine's rings $B_{cris}\subset B_{dR}$). Write $D_*(V)=H^0(G_v,V\otimes_{\mathbb{Q}_p}B_*)$, for $*\in\{cris,\ dR\}$. If we define

$$W_v=\begin{cases} H^1_{ur}(G_v,V) & v\in S_f, v\nmid p\\ H^1_f(G_v,V) & v\mid p\end{cases}$$

then the Selmer group $S(K,V;W)$ is usually denoted by $H^1_f(K,V)$. The basic properties of $H^1_f\subseteq H^1_g$ are as follows:

(i) If V is a de Rham representation of G_v, then $H^1_g(G_v,V)/H^1_f(G_v,V)$ is dual to $D_{cris}(V^*(1))/(f-1)$ ([Bl-Ka, Prop. 3.8, Cor. 3.8.4]).

(ii) If V satisfies Pančiškin's condition at v ([Ne 1, 6.7]), i.e. if there is an exact sequence of $F_\mathfrak{p}[G_v]$-modules

$$0\longrightarrow V_v^+\longrightarrow V\longrightarrow V_v^-\longrightarrow 0$$

such that $F^0D_{dR}(V_v^+)=D_{dR}(V_v^-)/F^0=0$ (where $F^iD_{dR}(W)=H^0(G_v,W\otimes_{\mathbb{Q}_p}\mathrm{Fil}^iD_{dR})$), then

$$H^1(G_v,V_v^+)\longrightarrow H^1_g(G_v,V)\longrightarrow H^1_g(G_v,V_v^-)$$

is exact. If V_v^- is a semi-stable representation of G_v, then

$$H^1_g(G_v,V_v^-)=H^1_f(G_v,V_v^-)=D_{cris}(V_v^-)/(f-1)$$

(by weak admissibility and [Bl-Ka, Cor. 3.8.4]), which has dimension equal to that of

$$D_{cris}(V_v^-)^{f=1}=D_{cris}(V_v^-)^{f=1}\cap F^0D_{dR}(V_v^-)=H^0(G_v,V_v^-).$$

In particular, if $H^0(G_v,V_v^-)=0$, then

$$H^1_g(G_v,V)=\mathrm{Im}\left[H^1(G_v,V_v^+)\longrightarrow H^1(G_v,V)\right].$$

(2.2) Selmer complexes

As observed in [Ne 3], a more satisfactory theory of Selmer groups is obtained if one imposes local conditions on the level of complexes, rather than on cohomology (as in 2.1.3). In this section we recall the basic setup of [Ne 3] for the coefficient ring $\mathcal{O}$. In what follows, if $p=2$ and K is not totally imaginary, then most statements are valid only modulo 2-torsion.

(2.2.1) Let G be a profinite group and M a topological G-module (i.e. such that the action $G\times M\to M$ is continuous). The complex of (non-homogeneous) continuous cochains on G with values in M will be denoted $C^\bullet_{cont}(G,M)$; in degree q, $C^q_{cont}(G,M)$

consists of continuous maps $G^q \to M$. The cohomology of $\mathcal{C}^\bullet_{cont}(G,M)$ will be denoted by $H^i(G,M)$. If M has discrete topology, then

$$\mathcal{C}^\bullet_{cont}(G,M) = \varinjlim_{U} \mathcal{C}^\bullet_{cont}(G/U, M^U),$$

with U running through all open normal subgroups of G.

(2.2.2) In the notation of 2.1.2, we consider $M = T$ (with the $\mathfrak{p}$-adic topology) and $M = V = \bigcup_{n\geq 0} \pi^{-n}T$ (with the inductive limit topology) as topological modules over $G = G_K$, $G_{K,S}$, or G_v. In this case, $\mathcal{C}^\bullet_{cont}(G,T) = \varprojlim_n \mathcal{C}^\bullet_{cont}(G, T/\pi^n T)$ and $\mathcal{C}^\bullet_{cont}(G,V) = \mathcal{C}^\bullet_{cont}(G,T) \otimes_{\mathcal{O}} F_\mathfrak{p}$ ([Ja, Thm. 5.15]) and

$$0 \longrightarrow \mathcal{C}^\bullet_{cont}(G,T) \xrightarrow{i_*} \mathcal{C}^\bullet_{cont}(G,V) \xrightarrow{\mathrm{pr}_*} \mathcal{C}^\bullet_{cont}(G,A) \longrightarrow 0$$

is an exact sequence of complexes (as i is strict and pr admits a continuous section).

(2.2.3) In order to define Selmer complexes we need the following data: for each $v \in S_f$, complexes $U_v^\pm(T)$ of $\mathcal{O}$-modules together with maps of complexes

$$\Delta_v : U_v^+(T) \longrightarrow \mathcal{C}^\bullet_{cont}(G,T) \longrightarrow U_v^-(T)$$

such that Δ_v defines a distinguished triangle in $D^b_{ft}(\mathcal{O}\text{-mod})$ (the derived category of cohomologically bounded complexes of $\mathcal{O}$-modules, with cohomology of finite type over $\mathcal{O}$). Putting $U_v^\pm(V) = U_v^\pm(T) \otimes_{\mathcal{O}} F_\mathfrak{p}$ and $U_v^\pm(A) = \mathrm{Cone}\,(U_v^\pm(T) \longrightarrow U_v^\pm(V))$ (isomorphic to $U_v^\pm(T) \otimes^{\mathbb{L}}_{\mathcal{O}} (F_\mathfrak{p}/\mathcal{O})$ in $D^b(\mathcal{O}\text{-mod})$), we get distinguished triangles in $D^b(\mathcal{O}\text{-mod})$

$$U_v^+(X) \longrightarrow \mathcal{C}^\bullet_{cont}(G,X) \longrightarrow U_v^-(X)$$

for $X = T, V, A$. The Selmer complex with values in $X \in \{T,V,A\}$ associated to local conditions $\Delta = (\Delta_v)$ is defined as

$$\mathcal{C}^\bullet_f(G_{K,S}, X; \Delta) = \mathrm{Cone}\Big(\mathcal{C}^\bullet_{cont}(G_{K,S},X) \longrightarrow \bigoplus_{v\in S_f} U_v^-(X)\Big)[-1].$$

The corresponding object of $D^b(\mathcal{O}\text{-mod})$ will be denoted by $\mathbb{R}\widetilde{\Gamma}_f(G_{K,S}, X; \Delta)$ and its cohomology by $\widetilde{H}^i_f(G_{K,S}, X; \Delta)$.

(2.2.4) Properties of Selmer complexes

(i) $\mathbb{R}\widetilde{\Gamma}_f(G_{K,S}, X; \Delta)$ for $X = T$ (resp. $X = A$) is an object of $D^b_{ft}(\mathcal{O}\text{-mod})$ (resp. $D^b_{coft}(\mathcal{O}\text{-mod})$) i.e. the cohomology groups $\widetilde{H}^i_f(G_{K,S}, X; \Delta)$ are of finite type (resp. cofinite type) over $\mathcal{O}$.

(ii) There is a distinguished triangle

$$\mathbb{R}\widetilde{\Gamma}_f(G_{K,S}, T; \Delta) \xrightarrow{i_*} \mathbb{R}\widetilde{\Gamma}_f(G_{K,S}, V; \Delta) \xrightarrow{\mathrm{pr}_*} \mathbb{R}\widetilde{\Gamma}_f(G_{K,S}, A; \Delta)$$

with

$$\mathbb{R}\widetilde{\Gamma}_f(G_{K,S}, V; \Delta) \xrightarrow{\sim} \mathbb{R}\widetilde{\Gamma}_f(G_{K,S}, T; \Delta) \otimes_{\mathcal{O}} F_\mathfrak{p}$$

$$\mathbb{R}\widetilde{\Gamma}_f(G_{K,S}, A; \Delta) \xrightarrow{\sim} \mathbb{R}\widetilde{\Gamma}_f(G_{K,S}, T; \Delta) \overset{\mathbb{L}}{\otimes}_{\mathcal{O}} (F_\mathfrak{p}/\mathcal{O})$$

(iii) The cohomology sequence of the triangle in (ii) induces isomorphisms

$$\widetilde{H}^q_f(G_{K,S},T;\Delta)_{\mathrm{tors}} \xrightarrow{\sim} \mathrm{Im}\left[\widetilde{H}^{q-1}_f(G_{K,S},A;\Delta) \longrightarrow \widetilde{H}^q_f(G_{K,S},T;\Delta)\right]$$

$$\widetilde{H}^q_f(G_{K,S},A;\Delta)_{\mathrm{div}} \xrightarrow{\sim} \mathrm{Im}\left[\mathrm{pr}_* : \widetilde{H}^q_f(G_{K,S},V;\Delta) \longrightarrow \widetilde{H}^q_f(G_{K,S},A;\Delta)\right].$$

(iv) There is an exact sequence

$$\cdots \longrightarrow \bigoplus_{v\in S_f} H^{q-1}(G_v,U_v^-(X)) \longrightarrow \widetilde{H}^q_f(G_{K,S},X;\Delta) \longrightarrow H^q(G_{K,S},X)$$
$$\longrightarrow \bigoplus_{v\in S_f} H^q(G_v,U_v^-(X)) \longrightarrow \cdots$$

(2.2.5) Duality

Local Tate duality can be reformulated as an isomorphism

$$\mathbb{R}\Gamma(G_v,T^*(1)) \xrightarrow{\sim} \mathbb{R}\mathrm{Hom}_{\mathcal{O}}\left(\mathbb{R}\Gamma(G_v,T),\mathcal{O}\right)[-2] \qquad (v\nmid\infty)$$

in $D^b_{ft}(\mathcal{O}\text{-mod})$, where $\mathbb{R}\Gamma(G_v,T)$ denotes the image of $\mathcal{C}^\bullet_{cont}(G_v,T)$ in the derived category. Assume that, for each $v\in S_f$, we are given local conditions

$$\Delta_v^*(1) : U_v^+(T^*(1)) \longrightarrow \mathcal{C}^\bullet_{cont}(G_v,T^*(1)) \longrightarrow U_v^-(T^*(1))$$

and isomorphisms in $D^b_{ft}(\mathcal{O}\text{-mod})$,

$$U_v^\pm(T^*(1)) \xrightarrow{\sim} \mathbb{R}\mathrm{Hom}_{\mathcal{O}}\left(U_v^\mp(T)\right)[-2],$$

compatible with local Tate duality. One defines Selmer conditions for $T^*(1)$, $V^*(1)$, $A^*(1)$ using local conditions $\Delta^*(1)=(\Delta_v^*(1))$.

Examples: (i) If $U_v^+(T)=0$, then $U_v^+(T^*(1))=\mathcal{C}^\bullet_{cont}(G_v,T^*(1))$.

(ii) If $0\to T_v^+\to T\to T_v^-\to 0$ is an exact sequence of $\mathcal{O}[G_v]$-modules with T_v^- free over $\mathcal{O}$ and $U_v^\pm(T)=\mathcal{C}^\bullet_{cont}(G_v,T_v^\pm)$, then $U_v^\pm(T)=\mathcal{C}^\bullet_{cont}(G_v,T^*(1)_v^\pm)$, where $T^*(1)_v^\pm=(T_v^\mp)^*(1)$.

It is proven in [Ne 3] that there is a pairing

$$\widetilde{H}^1_f(G_{K,S},A;\Delta)\times\widetilde{H}^1_f(G_{K,S},A^*(1);\Delta^*(1)) \longrightarrow F_{\mathfrak{p}}/\mathcal{O}$$

with left kernel equal to $\widetilde{H}^1_f(G_{K,S},A;\Delta)_{\mathrm{div}}$ (resp. right kernel equal to $\widetilde{H}^1_f(G_{K,S},A^*(1);\Delta^*(1))_{\mathrm{div}}$).

(2.3) Big Galois representations

(2.3.1) Let R be a complete local noetherian ring containing $\mathcal{O}$, with maximal ideal $\mathfrak{m}$ and finite residue field $R/\mathfrak{m}$. Let T be an R-module of finite type equipped with a continuous (with respect to the $\mathfrak{m}$-adic topology) R-linear action of $G_{K,S}$. Assume that, for each $v\mid p$, there is an exact sequence of $R[G_v]$-modules

$$0\longrightarrow T_v^+\longrightarrow T\longrightarrow T_v^-\longrightarrow 0$$

with T_v^+ free over R.

(2.3.2) Specializations of T

Let $X\subseteq \mathrm{Spec}(R)$ be the set of prime ideals $I\subset R$ such that

(i) R/I is free of finite rank over $\mathcal{O}$.

(ii) For all $v \mid p$, $T_v^- \otimes_R R_I$ is free over R_I.

The same argument as in 1.5.6 shows that, for every $I \in X$, $\mathrm{Tor}_1^R(T_v^-, R/I)$ is finite and

$$0 \longrightarrow T_v^+/IT_v^+ \longrightarrow T/IT \longrightarrow T_v^-/IT_v^- \longrightarrow 0$$

is an exact sequence of $(R/I)[G_v]$-modules, with T_v^+/IT_v^+ free over $\mathcal{O}$ (for all $v \mid p$). Fix, once and for all, $I \in X$. Let $c_0 \geq 0$ be the smallest integer such that π^{c_0} kills the $\mathcal{O}$-torsion of T_v^-/IT_v^-, for all $v \mid p$. Put

$$X(I) = \left\{J \in X : \mathrm{rk}_{\mathcal{O}}(T_v^-/JT_v^-) = \mathrm{rk}_{\mathcal{O}}(T_v^-/IT_v^-)\ \forall\, v \mid p, \text{ and } (J, \pi^{c_0+1}) = (I, \pi^{c_0+1})\right\}$$
$$X(I)_n = \left\{J \in X(I) \ :\ (J, \pi^{c_0+n}) = (I, \pi^{c_0+n})\right\} \qquad (n \geq 1)$$

(here, $\mathrm{rk}_{\mathcal{O}}(M) = \dim_{F_{\mathfrak{p}}}(M \otimes_{\mathcal{O}} F_{\mathfrak{p}})$).

(2.3.3) LEMMA. *For every $J \in X(I)$, (i) $\mathrm{rk}_{\mathcal{O}}(R/J) = \mathrm{rk}_{\mathcal{O}}(R/I)$.*
(ii) $\mathrm{rk}_{\mathcal{O}}(T/JT) = \mathrm{rk}_{\mathcal{O}}(T/IT)$.
(iii) There are canonical isomorphisms of $\mathcal{O}/\pi^{c_0}$-modules

$$(T_v^-/JT_v^-)_{\mathrm{tors}} \xrightarrow{\sim} (T_v^-/IT_v^-)_{\mathrm{tors}} \qquad \textit{(for all } v \mid p\textit{)}$$
$$(T/JT)_{\mathrm{tors}} \xrightarrow{\sim} (T/IT)_{\mathrm{tors}}$$

Proof. (i) This follows from the isomorphism $R/(J,\pi) \xrightarrow{\sim} R/(I,\pi)$.

(ii) By (i) and freeness of T_v^+, $\mathrm{rk}_{\mathcal{O}}(T_v^+/JT_v^+) = \mathrm{rk}_{\mathcal{O}}(T_v^+/IT_v^+)$ for all $v \mid p$. For T_v^-, the analogous equality hold by definition, proving (ii).

(iii) The exact sequence (for every $v \mid p$)

$$T_v^+/(I,\pi^{c_0+1})T_v^+ \longrightarrow T/(I,\pi^{c_0+1})T \longrightarrow T_v^-/(I,\pi^{c_0+1})T_v^- \longrightarrow 0$$

is isomorphic to the corresponding sequence for J. The free parts of T_v^-/IT_v^- and T_v^-/JT_v^- are isomorphic by definition and the torsion part of T_v^-/IT_v^- is killed by π^{c_0}. This implies that the torsion parts of T_v^-/IT_v^- and T_v^-/JT_v^- are again isomorphic. As $(T/IT)_{\mathrm{tors}}$ injects into $(T_v^-/IT_v^-)_{\mathrm{tors}}$ (and similarly for J), it is killed by π^{c_0}. The isomorphism $T/(I,\pi^{c_0+1})T \xrightarrow{\sim} T/(J,\pi^{c_0+1})T$ together with (ii) imply that $(T/JT)_{\mathrm{tors}} \xrightarrow{\sim} (T/IT)_{\mathrm{tors}}$.

(2.3.4) For $J \in X(I)$ and $v \mid p$, put

$$V_J = (T/JT) \otimes_{\mathcal{O}} F_{\mathfrak{p}},\ T_J = \mathrm{Im}\,(T/JT \to V_J),\ A_J = V_J/T_J,\ (V_J)_v^{\pm} = \left(T_v^{\pm}/JT_v^{\pm}\right) \otimes_{\mathcal{O}} F_{\mathfrak{p}},$$

$$(T_J)_v^+ = T_J \cap (V_J)_v^+, \qquad (T_J)_v^- = \mathrm{Im}\left(T_J \to (V_J)_v^-\right), \qquad (A_J)_v^{\pm} = (V_J)_v^{\pm}\,/\,(T_J)_v^{\pm}.$$

There are exact sequences of $\mathcal{O}[G_v]$-modules

$$0 \longrightarrow (X_J)_v^+ \longrightarrow X_J \longrightarrow (X_J)_v^- \longrightarrow 0$$

for all $v \mid p$ and $X \in \{T, V, A\}$.

(2.3.5) LEMMA. *If $J \in X(J)_n$ for $n \geq 1$, then there are canonical isomorphisms (for all $v \mid p$)*

$$(A_J)_{\pi^n} \xrightarrow{\sim} (A_I)_{\pi^n}, \qquad \left((A_J)_v^{\pm}\right)_{\pi^n} \xrightarrow{\sim} \left((A_I)_v^{\pm}\right)_{\pi^n}.$$

Proof. This follows from the definitions and Lemma 2.3.3.

(2.3.6) Consider the following conditions on V_J, T_J, and A_J :

(C1) $H^0(G_K, V_J) = 0$ and (for all $v \in S_f$, $v \nmid p$) $H^0(G_v, V_J) = 0$.

(C1′) There exists $c_1 \geq 0$ such that $\pi^{c_1} H^0(G_K, A_J) = 0$ and (for all $v \in S_f$, $v \nmid p$) $\pi^{c_1} H^0(G_v, A_J) = 0$.

(C2) V_J is an absolutely irreducible $F_{\mathfrak{p}}[G_K]$-module.

(C2′) There exists $c_2 \geq 0$ such that $\pi^{c_2} \mathrm{End}_{\mathcal{O}}(T_J) \subseteq \mathrm{Im}\,(\mathcal{O}[G_K] \to \mathrm{End}_{\mathcal{O}}(T_J))$.

(C3) There exists $\alpha_J : V_J \xrightarrow{\sim} V_J^*(1)$, a skew-symmetric ($\alpha_J^*(1) = -\alpha_J$) isomorphism of $F_{\mathfrak{p}}[G_K]$-modules.

(C4) α_J from (C3) induces isomorphisms $(V_J)_v^{\pm} \xrightarrow{\sim} \left((V_J)_v^{\mp}\right)^*(1)$ for all $v \mid p$.

We have (C1) $\iff$ (C1′) and (C2) $\iff$ (C2′). Of course, the condition $H^0(G_K, V_J) = 0$ in (C1) is superfluous if the set $\{v \in S_f : v \nmid p\}$ is non-empty. Note that (C1) implies that $H^1_{ur}(G_v, V_J) = 0$ for all $v \in S_f$, $v \nmid p$. We shall consider Selmer groups associated to local conditions

$$W_v = \begin{cases} 0 & v \in S_f,\ v \nmid p \\ \mathrm{Ker}\left(H^1(G_v, V_J) \to H^1(G_v, (V_J)_v^-)\right) & v \mid p \end{cases}$$

and Selmer complexes corresponding to

$$U_v^+(T_J) = \begin{cases} 0 & v \in S_f,\ v \nmid p \\ C^\bullet_{cont}(G_v, (T_J)_v^+) & v \mid p \end{cases}$$

$$U_v^-(T_J) = \begin{cases} C^\bullet_{cont}(G_v, T_J) & v \in S_f,\ v \nmid p \\ C^\bullet_{cont}(G_v, (T_J)_v^-) & v \mid p \end{cases}$$

The exact sequence 2.2.4 (iv) then becomes

$$0 \longrightarrow \bigoplus_{v \mid p} H^0(G_v, (V_J)_v^-) \longrightarrow \widetilde{H}^1_f(G_{K,S}, V_J; \Delta) \longrightarrow S(K, V_J; W) \longrightarrow 0. \tag{2.3.6.1}$$

(2.3.7) Theorem ("Continuity Principle"). *Assume that V_I satisfies (C1) and let $c_1 \geq 0$ be as in (C1′). If $J \in X(I)_{n+c_1}$ with $n \geq 1$, then*
(1) A_J satisfies (C1′) with the same value of c_1 (hence V_J satisfies (C1)).
(2) There is a canonical isomorphism

$$\widetilde{H}^1_f(G_{K,S}, A_J; \Delta)_{\pi^n} \xrightarrow{\sim} \widetilde{H}^1_f(G_{K,S}, A_I; \Delta)_{\pi^n}.$$

Proof. (1) This follows from Lemma 2.3.5.

(2) For every $m \geq 1$, we define Selmer complexes for the finite $G_{K,S}$-modules $(A_J)_{\pi^m}$ by local conditions

$$U_v^+ = 0, \qquad U_v^- = C^\bullet_{cont}(G_v, (A_J)_{\pi^m}), \qquad v \in S_f, v \nmid p,$$
$$U_v^{\pm} = C^\bullet_{cont}(G_v, ((A_J)_v^{\pm})_{\pi^m}), \qquad v \mid p.$$

The local conditions are compatible with the isomorphisms of Lemma 2.3.5, which means that the induced maps

$$\widetilde{H}^1_f(G_{K,S}, (A_J)_{\pi^{n+c_1}}; \Delta) \xrightarrow{\sim} \widetilde{H}^1_f(G_{K,S}, (A_I)_{\pi^{n+c_1}}; \Delta)$$

are again isomorphisms. Applying $\widetilde{\mathbb{R}\Gamma}_f(G_{K,S}, -; \Delta)$ to all entries of the commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & (A_J)_{\pi^n} & \longrightarrow & A_J & \xrightarrow{\pi^n} & A_J & \longrightarrow & 0 \\
 & & \| & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & (A_J)_{\pi^n} & \longrightarrow & (A_J)_{\pi^{n+c_1}} & \xrightarrow{\text{“}\pi^n\text{”}} & (A_J)_{\pi^{c_1}} & \longrightarrow & 0 \\
 & & \downarrow\wr & & \downarrow\wr & & \downarrow\wr & & \\
0 & \longrightarrow & (A_I)_{\pi^n} & \longrightarrow & (A_I)_{\pi^{n+c_1}} & \xrightarrow{\text{“}\pi^n\text{”}} & (A_I)_{\pi^{c_1}} & \longrightarrow & 0 \\
 & & \| & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & (A_I)_{\pi^n} & \longrightarrow & A_I & \xrightarrow{\pi^n} & A_I & \longrightarrow & 0
\end{array}$$

we get a commutative diagram with exact rows (dropping $G_{K,S}$ and Δ from the notation):

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \widetilde{H}^0_f(A_J)/\pi^n & \longrightarrow & \widetilde{H}^1_f((A_J)_{\pi^n}) & \longrightarrow & \widetilde{H}^1_f(A_J)_{\pi^n} & \longrightarrow & 0 \\
 & & \uparrow{\scriptstyle \beta_J} & & \| & & & & \\
0 & \longrightarrow & \widetilde{H}^0_f((A_J)_{\pi^{c_1}})/\mathrm{Im}(\text{“}\pi^n_*\text{”}) & \longrightarrow & \widetilde{H}^1_f((A_J)_{\pi^n}) & \longrightarrow & \widetilde{H}^1_f((A_J)_{\pi^{n+c_1}}) & \longrightarrow & 0 \\
 & & \downarrow\wr & & \downarrow\wr & & \downarrow\wr & & \\
0 & \longrightarrow & \widetilde{H}^0_f((A_I)_{\pi^{c_1}})/\mathrm{Im}(\text{“}\pi^n_*\text{”}) & \longrightarrow & \widetilde{H}^1_f((A_I)_{\pi^n}) & \longrightarrow & \widetilde{H}^1_f((A_I)_{\pi^{n+c_1}}) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \beta_I} & & \| & & & & \\
0 & \longrightarrow & \widetilde{H}^0_f(A_I)/\pi^n & \longrightarrow & \widetilde{H}^1_f((A_I)_{\pi^n}) & \longrightarrow & \widetilde{H}^1_f(A_I)_{\pi^n} & \longrightarrow & 0
\end{array}$$

It follows from the exact sequence 2.2.4(iv) that both arrows β_I and β_J in the diagram above are isomorphisms, proving that

$$\widetilde{H}^1_f(A_J)_{\pi^n} \xrightarrow{\sim} \widetilde{H}^1_f(A_I)_{\pi^n}$$

as claimed.

(2.3.8) LEMMA. *Assume that V_I satisfies (C2) and let $c_2 \geq 0$ be as in (C2′). If $J \in X(I)_{n+c_2}$ with $n \geq 1$, then*
(1) T_J satisfies (C2′) with the same value of c_2 (hence V_J satisfies (C2)).
(2) If $n \geq 1 + \mathrm{ord}_\pi(2)$ and if V_I satisfies (C3), then V_J also satisfies (C3). If the groups $\mathrm{Hom}_{F_\mathfrak{p}[G_v]}\left((V_J)_v^{\pm}, \left((V_J)_v^{\pm}\right)^*(1)\right) = 0$ vanish for all $v \mid p$, then V_J satisfies

(C4).

Proof. (1) Put $C_J := \mathrm{Im}\,(\mathcal{O}[G_K] \to \mathrm{End}_{\mathcal{O}}(T_J))$. Under the isomorphism

$$\mathrm{End}_{\mathcal{O}}(T_J)/\pi^{c_2+1} = \mathrm{End}_{\mathcal{O}}(T_J/\pi^{c_2+1}) \xrightarrow{\sim} \mathrm{End}_{\mathcal{O}}(T_I/\pi^{c_2+1}) = \mathrm{End}_{\mathcal{O}}(T_I)/\pi^{c_2+1}$$

$C_J \pmod{\pi^{c_2+1}}$ corresponds to $C_I \pmod{\pi^{c_2+1}}$. As $\pi^{c_2}\mathrm{End}_{\mathcal{O}}(T_I) \subseteq C_J$ by assumption, we have

$$\pi^{c_2}\mathrm{End}_{\mathcal{O}}(T_J) \subseteq C_J + \pi^{c_2+1}\mathrm{End}_{\mathcal{O}}(T_J).$$

Nakayama's Lemma then implies $\pi^{c_2}\mathrm{End}_{\mathcal{O}}(T_J) \subseteq C_J$.

(2) As V_I satisfies (C2) and (C3), $\mathrm{Hom}_{\mathcal{O}[G_v]}(T_I, T_I^*(1))$ is a free $\mathcal{O}$-module of rank one. In the exact sequence

$$0 \to \mathrm{Hom}_{\mathcal{O}[G_v]}(T_I, T_I^*(1))/\pi^{n+c_2} \to \mathrm{Hom}_{\mathcal{O}[G_v]}(T_I/\pi^{n+c_2}, T_I^*(1)/\pi^{n+c_2})$$
$$\to \mathrm{Ext}^1_{\mathcal{O}[G_v]}(T_I, T_I^*(1))^{\pi^{n+c_2}} \to \cdots$$

the Ext^1 term is killed by π^{c_2} ([Cu-Re, Thm. 29.4]), and the same is true if T_I is replaced by T_J (by (1)). Using the isomorphism

$$\gamma : \mathrm{Hom}_{\mathcal{O}[G_v]}(T_I/\pi^{n+c_2}, T_I^*(1)/\pi^{n+c_2}) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{O}[G_v]}(T_J/\pi^{n+c_2}, T_J^*(1)/\pi^{n+c_2})$$

we see that there is a non-zero element $\alpha \in \mathrm{Hom}_{\mathcal{O}[G_v]}(T_J, T_J^*(1))$ such that $\pi^{c_2}(\alpha_I \pmod{\pi^{n+c_2}})$ corresponds to $\pi^{c_2}(\alpha \pmod{(\pi^{n+c_2})}$ under the isomorphism γ. As V_J satisfies (C2), α induces an isomorphism $\alpha_J : V_J \xrightarrow{\sim} V_J^*(1)$ such that $\alpha_J^*(1) = \varepsilon\alpha_J$ for $\varepsilon = \pm 1$. Since $\alpha_I^*(1) = -\alpha_I$, the definition of α implies that $\varepsilon \equiv -1 \pmod{\pi^n} \equiv -1 \pmod{2\pi}$, hence $\varepsilon = -1$. If $\mathrm{Hom}_{F_v[G_v]}((V_J)_v^{\pm}, ((V_J)_v^{\pm})^*(1)) = 0$ for all $v \mid p$ (for example, this is always true if $(V_J)_v^{\pm}$ are of the form described in 2.1.6(ii) ("Pančiškin's condition")), then α_J induces injective maps

$$\alpha_{J,v}^{\pm} : (V_J)_v^{\pm} \hookrightarrow ((V_J)_v^{\mp})^*(1).$$

Counting dimensions, we see that all maps $\alpha_{J,v}^{\pm}$ are isomorphisms, which means that V_J satisfies (C4).

(2.3.9) LEMMA. *Assume that V_J satisfies (C1'), (C2') and (C3). Then*

$$\pi^{c_1 d} H^1_{ur}(G_v, A_J) = 0, \qquad \pi^{c_1+c_2}\left(H^1(G_v, A_J)/H^1_{ur}(G_v, A_J)\right) = 0$$

for all $v \in S_f$, $v \nmid p$ (where $d = \dim_{F_p}(V_J)$).

Proof. $H^1(G_v, A_J)/H^1_{ur}(G_v, A_J)$ is dual to

$$H^1_{ur}(G_v, T_J^*(1)) = \left(T_J^*(1)^{I_v}\right)/(\mathrm{Fr}(v) - 1) \xrightarrow{\sim} \left(A_J^*(1)^{I_v}\right)^{\mathrm{Fr}(v)=1} = H^0(G_v, A_J^*(1))$$

(as $\mathrm{Fr}(v) - 1$ acting on $V_J^{I_v} \xrightarrow{\sim} V_J^*(1)^{I_v}$ is an isomorphism). Multiplying $\alpha_J(T_J)$ by a constant, we may assume that $\alpha_J(T_J) \subseteq T_J^*(1)$ and $\alpha_J(T_J) \not\subseteq \pi T_J^*(1)$, which implies that $\pi^{c_2} T_J^*(1) \subseteq \alpha_J(T_J)$. It follows that the module M defined by

$$0 \longrightarrow M \longrightarrow A_J \xrightarrow{\alpha_J} A_J^*(1) \longrightarrow 0$$

is killed by π^{c_2}. As $\pi^{c_1} H^0(G_v, A_J) = 0$, $\pi^{c_1+c_2}$ kills $H^0(G_V, A_J^*(1))$. Writing

$$0 \longrightarrow V_J^{I_v}/T_J^{I_v} \longrightarrow A_J^{I_v} \longrightarrow N_v \longrightarrow 0$$

(with N_v finite) and (again) using the fact that $\mathrm{Fr}(v)-1$ acting on $V_J^{I_v} \xrightarrow{\sim} V_J^*(1)^{I_v}$ is an isomorphism, we get

$$H^1_{ur}(G_v, A_J) = A_J^{I_v}/(\mathrm{Fr}(v)-1) = N_v/(\mathrm{Fr}(v)-1).$$

This is an $\mathcal{O}$-module of length equal to

$$\ell_{\mathcal{O}}\left(N_v/(\mathrm{Fr}(v)-1)\right) = \ell_{\mathcal{O}}\left(N_v^{\mathrm{Fr}(v)=1}\right) = \ell_{\mathcal{O}}\left(H^0(G_v, A_J)\right) \leq c_1 d,$$

hence killed by $\pi^{c_1 d}$ as claimed.

(2.3.10) THEOREM. *Assume that V_I satisfies (C1)-(C4) with constants c_1, c_2 in (C1'),(C2'). Put $d = \dim_{F_\mathfrak{p}}(V_I)$ and let $c_3 \geq 0$ be an integer such that π^{c_3} kills*

$$Ш(G_{K,S}, A_I; \Delta) := \widetilde{H}^1_f(G_{K,S}, A_I; \Delta)/\mathrm{pr}_* \widetilde{H}^1_f(G_{K,S}, V_I; \Delta).$$

Let $J \in X(I)_n$ with $n \geq (d+3)c_1 + 4c_2 + 2\mathrm{ord}_\pi(2) + 1 + c_3$ and assume that V_J satisfies (C4). Then

$$\dim_{F_\mathfrak{p}} \widetilde{H}^1_f(G_{K,S}, V_I; \Delta) - \widetilde{H}^1_f(G_{K,S}, V_J; \Delta) \geq 0$$

is an even integer.

Proof. By Theorem 2.3.7 and Lemma 2.3.8, V_J satisfies (C1)–(C3), with the same constants c_1, c_2 in (C1'),(C2'). Adjusting α_J as in the proof of Lemma 2.3.9, it follows from the condition (C4) for V_J that

$$\pi^{c_2}\left((T_J)_v^{\mp}\right)^*(1) \subseteq \alpha_J\left((T_J)_v^{\pm}\right) \tag{2.3.10.1}$$

for all $v \mid p$. The local conditions for $M = \mathrm{Ker}\,(\alpha_J : A_J \to A_J^*(1))$

$$U_v^+(M) = \begin{cases} 0 & v \in S_f,\ v \nmid p \\ \mathcal{C}^\bullet_{cont}(G_v, M \cap (A_J)_v^+) & v \mid p. \end{cases}$$

define a Selmer complex $\mathbb{R}\widetilde{\Gamma}_f(G_{K,S}, M; \Delta)$ sitting in a distinguished triangle

$$\mathbb{R}\widetilde{\Gamma}_f(G_{K,S}, M; \Delta) \longrightarrow \mathbb{R}\widetilde{\Gamma}_f(G_{K,S}, A_J; \Delta) \xrightarrow{\alpha_J} \mathbb{R}\widetilde{\Gamma}_f(G_{K,S}, A_J^*(1); \Delta)$$

The dual local conditions $\Delta^*(1)$ for $T_J^*(1)$ are given by

$$U_v^+(T_J^*(1)) = \begin{cases} \mathcal{C}^\bullet_{cont}(G_v, T_J) & v \in S_f,\ v \nmid p \\ \mathcal{C}^\bullet_{cont}(G_v, ((T_J^-)_v)^*(1)) & v \mid p. \end{cases}$$

It follows from 2.3.10.1 that there is a distinguished triangle

$$\mathbb{R}\widetilde{\Gamma}_f(G_{K,S}, A_J^*(1); \Delta) \longrightarrow \mathbb{R}\widetilde{\Gamma}_f(G_{K,S}, A_J^*(1); \Delta^*(1)) \longrightarrow \bigoplus_{\substack{v \in S_f \\ v \nmid p}} \mathcal{C}^\bullet_{cont}(G_v, A_J) \oplus \mathcal{C}^\bullet$$

with $\pi^{c_2} H^q(\mathcal{C}^\bullet) = 0$ for all q. Combining the two triangles and using Lemma 2.3.9, we deduce that the kernel (resp. cokernel) of the map

$$(\alpha_J)_* : \widetilde{H}^1_f(G_{K,S}, A_J; \Delta) \to \widetilde{H}^1_f(G_{K,S}, A_J^*(1); \Delta^*(1))$$

is killed by $\pi^{c_1+c_2}$ (resp. by $\pi^{(d+1)c_1+c_2}$). The pairing 2.2.5 (non-degenerate up to 2-torsion)

$$Ш(G_{K,S}, A_J; \Delta) \times Ш(G_{K,S}, A_J^*(1); \Delta^*(1)) \to F_\mathfrak{p}/\mathcal{O}$$

then induces via $\mathrm{id} \times (\alpha_J)_*$ a skew-symmetric pairing on $Ш(G_{K,S}, A_J; \Delta)$, with kernel killed by $2\pi^{(d+2)c_1+4c_2}$. It follows from the theory of symplectic spaces that there is an exact sequence of finite $\mathcal{O}$-modules

$$0 \longrightarrow Y(J) \longrightarrow Z(J) \oplus Z(J) \longrightarrow Ш(G_{K,S}, A_J; \Delta) \longrightarrow 0$$

with $4\pi^{(d+2)c_1+4c_2} Y(J) = 0$. Put $r(J) := \dim_{F_\mathfrak{p}} \widetilde{H}^1_f(G_{K,S}, V_J; \Delta)$. Then

$$\widetilde{H}^1_f(G_{K,S}, A_J; \Delta) \cong (F_\mathfrak{p}/\mathcal{O})^{r(J)} \oplus (Z(J) \oplus Z(J))/Y(J)$$
$$\widetilde{H}^1_f(G_{K,S}, A_I; \Delta) \cong (F_\mathfrak{p}/\mathcal{O})^{r(I)} \oplus (Z(I) \oplus Z(I))/Y(I)$$

In the isomorphism of Theorem 2.3.7,

$$\widetilde{H}^1_f(G_{K,S}, A_J; \Delta)_{\pi^{n-c_1}} \xrightarrow{\sim} \widetilde{H}^1_f(G_{K,S}, A_I; \Delta)_{\pi^{n-c_1}},$$

the right hand side is isomorphic to

$$\left(\mathcal{O}/\pi^{n-c_1}\mathcal{O}\right)^{r(I)} \oplus K, \qquad \pi^{c_3} K = 0$$

and the left hand side is isomorphic to

$$\left(\mathcal{O}/\pi^{n-c_1}\mathcal{O}\right)^{r(J)} \oplus ((Z(J) \oplus Z(J))/Y(J))_{\pi^{n-c_1}}.$$

This implies that

$$r(I) - r(J) = 2 \times \left(\text{number of generators of the } \mathcal{O}\text{-module } 4\pi^{(d+2)c_1+4c_2+c_3} Z(J)\right)$$

is even as claimed.

3. Selmer groups in Hida families.

(3.1) The notation is as in 1.3; in particular, i_p and i_∞ are fixed.

(3.1.1) Let f be a normalized newform on $\Gamma_1(N)$ of weight $k \geq 2$ and character χ. We assume that

- f is ordinary at p.
- $k \geq 2$ is even.
- $p \nmid \mathrm{cond}(\chi)$.

Under these assumptions, the two cases (i), (ii) of 1.3.5 boil down to

Case (I): $p \nmid N$.

Case (II): $p \parallel N$, $k = 2$, $a_p^2 = \chi(p)$.

We say that we are in the exceptional case (a subcase of (II)) if $p \parallel N$, $k = 2$, $a_p = \chi(p) = 1$.

(3.1.2) Let V be the two-dimensional $F_\mathfrak{p}$-representation $V = M_\mathfrak{p}(k/2) = V(f)(k/2)$ of $G_{\mathbb{Q},S}$ (where S consists of primes dividing pN and ∞). As in 1.3.4, we have

$$\Lambda^2 V \xrightarrow{\sim} F_\mathfrak{p}(1) \otimes [\chi], \qquad V \otimes [\chi^{-1}] \xrightarrow{\sim} V^*(1).$$

(3.1.3) LEMMA. *For every finite extension $K/\mathbb{Q}$ and every non-archimedian prime $v \nmid p$ of K,*

$$H^1_{ur}(G_v, V) = 0, \qquad H^i(G_v, V) = H^i(G_v, V^*(1)) = 0 \qquad \text{for } i = 0, 1, 2.$$

Proof. V is pure of weight -1. This means that, for every $v \nmid N$, all eigenvalues of $\mathrm{Fr}(v)_{\mathrm{geom}}$ on V have absolute values $(Nv)^{-1/2}$, hence $H^0(G_v, V) = H^0(G_v, V^*(1)) =$

0. If $v \mid N$, then results of [La], [Ca] imply that both spaces V^{I_v}, $V^*(1)^{I_v}$ are either zero or $\mathrm{Fr}(v)_{\mathrm{geom}}$ acts on them with weights less than zero, showing that $H^0(G_v, V) = H^0(G_v, V^*(1)) = 0$. The rest follows from Tate's local duality $H^i(G_v, V^*(1)) \xrightarrow{\sim} H^{2-i}(G_v, V)^*$ and Euler characteristic formula $\sum_{i=0}^{2}(-1)^i \dim H^i(G_v, V) = 0$ (and $\dim H^1_{ur}(G_v, V) = \dim H^0(G_v, V)$).

(3.1.4) V is reducible as a representation of $G_{\mathbb{Q}_p}$; we have a short exact sequence

$$0 \longrightarrow V_p^+ \longrightarrow V \longrightarrow V_p^- \longrightarrow 0 \tag{3.1.4.1}$$

with $V_p^{\pm} = F^{\pm} M_{\mathfrak{p}}(k/2)$ in the notation of 1.3.5. Both $V_p^{\pm}$ are crystalline representations of $G_{\mathbb{Q}_p}$. The filtered module $D_{cris}(V_p^{\pm}) = H^0(G_{\mathbb{Q}_p}, V_p^{\pm} \otimes_{\mathbb{Q}_p} B_{cris})$ is one-dimensional over $F_{\mathfrak{p}}$, with crystalline Frobenius f acting by the scalar $\alpha_p p^{-k/2}$ on V^+ and $\beta_p p^{-k/2} = \chi(p)\alpha_p^{-1} p^{k/2-1}$ on V^-. We have $\mathrm{gr}_F^i D_{dR}(V_p^{\pm}) \neq 0$ if and only if $i = -k/2$ for V_p^+ and $i = k/2 - 1$ for V_p^-, so the exact sequence 3.1.4.1 satisfies Pančiškin's condition (2.1.6 (ii)).

(3.1.5) The subspace $H^1_f(G_{\mathbb{Q}_p}, V) \subset H^1(G_{\mathbb{Q}_p}, V)$ can be described fairly explicitly. Let us first analyse

Case (I): $p \nmid N$.

This implies that V is a crystalline representation of $G_{\mathbb{Q}_p}$. In fact, for $k > 2$, every extension of A by $B(k-1)$ with A, B unramified (such as $M_{\mathfrak{p}} = V(-k/2)$) is automatically crystalline ([Bures, Exp. IV, Prop. 3.1]). If $k = 2$, then $V \subset V_p(J_1(N))$ and $J_1(N)$ has good reduction at p. Both $\alpha_p p^{-k/2}, \beta_p p^{-k/2}$ have absolute values $p^{-1/2}$, hence

$$D_{cris}(W)^{f=1} = D_{cris}(W^*(1))^{f=1} = 0, \qquad W = V, V_p^{\pm}. \tag{3.1.5.1}$$

This is still true if $G_{\mathbb{Q}_p}$ is replaced by G_{K_v}, for a finite extension $K_v/\mathbb{Q}_p$. As a result, we get from 2.1.6

$$H^1_f(G_{K_v}, V) = H^1_g(G_{K_v}, V) = \mathrm{Im}\big[H^1(G_{K_v}, V_p^+) \to H^1(G_{K_v}, V)\big]$$

$$H^0(G_{K_v}, W) = H^0(G_{K_v}, W^*(1)) = 0, \qquad W = V, V_p^{\pm}.$$

(3.1.6) Case (II): $p \parallel N$, $k = 2$, $a_p^2 = \chi(p)$.

In this case, $V \subset V_p(J_1(N/p;p)^{p-new})$, where $J_1(N/p;p)$ is the Jacobian of $X_1(N/p;p)$ and $J_1(N/p;p)^{p-new}$ is its quotient by the image of

$$(s^*, t^*) : J_1(N/p) \times J_1(N/p) \to J_1(N/p;p).$$

It is known that $J_1(N/p;p)^{p-new}$ has completely toric reduction at p ([De-Ra]), which implies that V is *not* crystalline. The quotient V_p^- is unramified, with $\mathrm{Fr}(v)_{\mathrm{geom}}$ acting by the scalar a_p, and $V_p^+ \xrightarrow{\sim} V_p^-(1)$: in the exceptional case, $G_{\mathbb{Q}_p}$ acts trivially on V_p^- and V is a Kummer extension

$$0 \longrightarrow F_{\mathfrak{p}}(1) \longrightarrow V \longrightarrow F_{\mathfrak{p}} \longrightarrow 0$$

with extension class $q \in H^1(G_{\mathbb{Q}_p}, F_{\mathfrak{p}}(1)) = \mathbb{Q}_p^{\times} \widehat{\otimes} F_{\mathfrak{p}}$ such that $q \notin \mathbb{Z}_p^{\times} \widehat{\otimes} F_{\mathfrak{p}}$. For example, if $\chi = 1$ and f has coefficients in $\mathbb{Q}$, it corresponds to (the isogeny class of) an elliptic curve $E/\mathbb{Q}$ with ordinary reduction at p. The exceptional case occurs iff E has split multiplicative reduction at p, in which case $q = q_E \otimes 1$, where $q_E \in \mathbb{Q}_p^{\times}$

is Tate's multiplicative period of $E/\mathbb{Q}_p$: $E(\overline{\mathbb{Q}}_p) = \overline{\mathbb{Q}}_p^{\times}/q_E^{\mathbb{Z}}$. In the exceptional case ($V_p^- = V_p^+(-1) = F_\mathfrak{p}$), there is an exact sequence

$$0 \longrightarrow H^0(G_{\mathbb{Q}_p}, F_\mathfrak{p}) \xrightarrow{\partial} \mathbb{Q}_p^{\times} \widehat{\otimes} F_\mathfrak{p} \xrightarrow{\alpha} H_g^1(G_{\mathbb{Q}_p}, V) \xrightarrow{\beta} H_g^1(G_{\mathbb{Q}_p}, F_\mathfrak{p}) \xrightarrow{\partial'} H_g^2(G_{\mathbb{Q}_p}, F_\mathfrak{p}(1)) \longrightarrow H_g^2(G_{\mathbb{Q}_p}, V)$$

with $\partial(1) = q$. The groups H_g^i are defined in [Fo-PR, I.3.3.3]; for a semistable representation W this H_g^1 coincides with that of [Bl-Ka] and $H_g^2(G_{\mathbb{Q}_p}, W)$ is dual to $D_{cris}(W^*(1))^{f=1}$. The dual extension

$$0 \longrightarrow F_\mathfrak{p}(1) \longrightarrow V^*(1) \longrightarrow F_\mathfrak{p} \longrightarrow 0$$

has extension class equal to q^{-1}. It follows that the map $D_{cris}(F_\mathfrak{p}(1)) \longrightarrow D_{cris}(V^*(1))$ is an isomorphism, hence $H_g^1(G_{\mathbb{Q}_p}, V) = H_f^1(G_{\mathbb{Q}_p}, V)$ by 2.1.6 (i). The group $H_g^2(G_{\mathbb{Q}_p}, V)$ vanishes, as $D_{cris}(V^*(1))^{f=1} = D_{cris}(F_\mathfrak{p}(1))^{f=1} = 0$. Both groups $H_g^1(G_{\mathbb{Q}_p}, F_\mathfrak{p})$, $H_g^2(G_{\mathbb{Q}_p}, F_\mathfrak{p}(1)) = H^2(G_{\mathbb{Q}_p}, F_\mathfrak{p}(1))$ are isomorphic to $F_\mathfrak{p}$ ([Bl-Ka, Ex. 3.9]), which implies that ∂' is an isomorphism and $\beta = 0$. Putting everything together, we obtain an exact sequence

$$0 \longrightarrow F_\mathfrak{p} \longrightarrow H^1(G_{\mathbb{Q}_p}, V_p^+) \longrightarrow H_f^1(G_{\mathbb{Q}_p}, V) \longrightarrow 0.$$

If not in the exceptional case, then 3.1.5.1 holds again, which implies that

$$H_f^1(G_{\mathbb{Q}_p}, V) = H_g^1(G_{\mathbb{Q}_p}, V) = \mathrm{Im}\big[H^1(G_{\mathbb{Q}_p}, V_p^+) \to H^1(G_{\mathbb{Q}_p}, V)\big]$$

$$H^0(G_{\mathbb{Q}_p}, W) = H^0(G_{\mathbb{Q}_p}, W^*(1)) = 0, \qquad W = V, V_p^{\pm}.$$

(3.1.7) The local calculations from 3.1.3–6 can be summed up as follows; for $K/\mathbb{Q}$ finite, consider local conditions

$$W_v = \begin{cases} H_{ur}^1(G_v, V) & v \in S_f, v \nmid p \\ H_f^1(G_v, V) & v \mid p \end{cases}$$

corresponding to $H_f^1(K, V) := S(K, V; W)$, resp.

$$U_v^+(V) = \begin{cases} 0 & v \in S_f, v \nmid p \\ C_{cont}^\bullet(G_v, V_p^+) & v \mid p \end{cases}$$

$$U_v^-(V) = \begin{cases} C_{cont}^\bullet(G_v, V) & v \in S_f, v \nmid p \\ C_{cont}^\bullet(G_v, V_p^-) & v \mid p \end{cases}$$

(S contains primes dividing pN and ∞). Then $W_v = 0$ for $v \nmid p$. It follows from (2.3.6.1) that,

In Case (I), $\widetilde{H}_f^1(G_{K,S}, V; \Delta) = H_f^1(K, V)$.

In Case (II), in the exceptional case, there is an exact sequence

$$0 \longrightarrow F_\mathfrak{p} \longrightarrow \widetilde{H}_f^1(G_{\mathbb{Q},S}, V; \Delta) \longrightarrow H_f^1(\mathbb{Q}, V) \longrightarrow 0,$$

otherwise, $\widetilde{H}_f^1(G_{\mathbb{Q},S}, V; \Delta) = H_f^1(\mathbb{Q}, V)$.

(3.2) For the rest of Section 3, the notation is as in 1.4. In particular, $p > 3$ (with the exception of 3.4.1–3).

(3.2.1) Let g be a p-stabilized ordinary newform of tame level N, with trivial character $\chi = 1$ and even weight $k_0 \geq 2$. Then either

Case (I): $g = f^0$ is the p-stabilization of a newform f on $\Gamma_1(N)$.

Case (II): $g = f$ is a newform on $\Gamma_1(Np)$, $k_0 = 2, a_p = \pm 1$.

(3.2.2) As in 1.4.7, $g = g_{k_0}$ is an element of a p-adic family of p-stabilized newforms g_k of weight k on $\Gamma_1(Np)$ for all $k \geq 2$, $k \equiv k_0 \pmod{p^c}$. Assuming that $F_\mathfrak{p}$ is big enough in the sense of 1.4.4, each g_k corresponds to an arithmetic point $\mathcal{P}_k \in \mathfrak{X}^{arith}(R)$ of a fixed local factor R of $\mathfrak{h}^{ord}_\infty$. The character of g_k is equal to $\chi_k = \chi\omega^{k_0}\omega^{-k} = \omega^{k_0-k}$. In particular, for $k \equiv k_0 \pmod{(p-1)p^c}$, $k \geq 2$, we have again either $g_k = (f_k)^0$ or $g_k = f_k$ for a newform f_k (the latter possible only if $k = 2$). The tame part ψ (resp. the wild part ε) of $\chi\omega^{k_0-2}$ is equal to $\psi = \omega^{k_0-2}$ (resp. $\varepsilon = 1$). this implies that each $\mathcal{P}_k$ lies above $(P_k) = (\imath(\gamma) - \gamma^{k-2}) \in \mathrm{Spec}(\Lambda)$ and that the invariant $a \in \mathbb{Z}/(p-1)\mathbb{Z}$ from 1.5.2 (iii) is equal to $a \equiv k_0 - 2 \pmod{(p-1)}$.

(3.2.3) Let $T(R)$ be the big Galois representation of $G_{\mathbb{Q},S}$ from 1.5.1. In order to apply 1.5.2,4 we need the following

Assumption. If $k_0 \equiv 2 \pmod{(p-1)}$, then $\rho_{f,\mathfrak{p}}$ has an irreducible residual representation.

The action of $a \in \mathbb{Z}_p^\times$ on $T(R)$ satisfies $< a >_{\mathrm{Alb}} = \omega(a)^{k_0-2} < \kappa(a) >_{\mathrm{Alb}}$, where κ denotes the projection of $\mathbb{Z}_p^\times$ to $1 + p\mathbb{Z}_p$. Define a twisted Galois representation

$$T = \text{“}T(R) < -1/2 >\text{”}$$

as follows: as an R-module, $T = T(R)$. The action of $g \in G_\mathbb{Q}$ such that $\chi_{\mathrm{cycl}}(g) = a \in \mathbb{Z}_p^\times$ is given by the action of g on $T(R)$ followed by $\omega(a)^{1-k_0/2} < \kappa(a)^{-1/2} >_{\mathrm{Alb}}$ (morally, this is “$< a >_{\mathrm{Alb}}^{-1/2}$”). The skew-symmetric bilinear form

$$\langle\ ,\ \rangle_{T(R)} : T(R) \times T(R) \longrightarrow \Lambda < 1 > (1)$$

defines a skew-symmetric pairing

$$\langle\ ,\ \rangle_T : T \times T \longrightarrow \Lambda(1)$$

which induces an isomorphism

$$T \xrightarrow{\sim} T^*(1) := \mathrm{Hom}_\Lambda\,(T, \Lambda)\,(1) \xrightarrow{\sim} \mathrm{Hom}_R\,(T, \omega_R)\,(1).$$

It follows from 1.5.2,4 that there is an exact sequence of $R[G_{\mathbb{Q}_p}]$-modules

$$0 \longrightarrow T^+ \longrightarrow T \longrightarrow T^- \longrightarrow 0$$

with $T^\pm = \text{“}T(R)^\pm < -1/2 >\text{”}$.

(3.2.4) For $k \equiv k_0 \pmod{(p-1)p^c}$, $k \geq 2$, let $V(f_k)$ be the Galois representation associated to f_k. We know from 1.5.5 that the specialization of $T(R)$ at $\mathcal{P}_k$ is isomorphic to

$$(T(R)/\mathcal{P}_k T(R)) \otimes_\mathcal{O} F_\mathfrak{p} \xrightarrow{\sim} V(f_k)^* \xrightarrow{\sim} V(f_k)(k-1).$$

Recall that we transform Dirichlet characters into characters of $G_\mathbb{Q}$ by using *geometric* Frobenius elements (1.3.4). This forces us to adopt the same convention for p-adic characters, namely $[\kappa](\mathrm{Fr}(\ell)_{\mathrm{geom}}) = \kappa(\ell)$. This implies that $\chi_{\mathrm{cycl}} = [\kappa]^{-1}[\omega]^{-1}$, since $\chi_{\mathrm{cycl}}(\mathrm{Fr}(\ell)_{\mathrm{geom}}) = \ell^{-1} = \kappa(\ell)^{-1}\omega(\ell)^{-1}$.

As $< \kappa(a) >_{\mathrm{Alb}} \equiv \kappa(a)^{k-2} \pmod{\mathcal{P}_k}$ for all $a \in \mathbb{Z}_p^\times$, it follows that the specialization of T at $\mathcal{P}_k$ is isomorphic to

$$(T/\mathcal{P}_k T) \otimes_{\mathcal{O}} F_{\mathfrak{p}} \xrightarrow{\sim} V(f_k)(k-1) \otimes [\omega^{k_0/2-1}] \otimes [\kappa^{k/2-1}] = V(f_k) \otimes [\omega^{k_0/2-k}] \otimes [\kappa^{-k/2}]$$
$$= V(f_k)(k/2) \otimes [\omega^{(k_0-k)/2}] = V(f_k)(k/2) \otimes \left[\left(\frac{\cdot}{p}\right)^{(k_0-k)/2(p-1)}\right].$$

In particular, for $k \equiv k_0 \pmod{2(p-1)p^c}$,

$$(T/\mathcal{P}_k T) \otimes_{\mathcal{O}} F_{\mathfrak{p}} \xrightarrow{\sim} V(f_k)(k/2).$$

Similarly, the specializations $(T^\pm/\mathcal{P}_k T^\pm) \otimes_{\mathcal{O}} F_{\mathfrak{p}}$ are then isomorphic to the $F_{\mathfrak{p}}[G_{\mathbb{Q}_p}]$-modules $V_p^\pm$ from 3.1.4 (for f_k instead of f).

(3.3) Theorem A

(3.3.1) THEOREM A. *Let f_k be the family of newforms as in 3.2.2. If $k_0 \equiv 2 \pmod{(p-1)}$, assume in addition that $V(f_{k_0})$ has an irreducible residual representation. Then there is an integer $n \geq c$ such that for every $k \equiv k_0 \pmod{2(p-1)p^n}$,*

$$\dim_{F_{\mathfrak{p}}} \widetilde{H}^1_f(G_{\mathbb{Q},S}, V(f_{k_0})(k_0/2); \Delta) - \dim_{F_{\mathfrak{p}}} \widetilde{H}^1_f(G_{\mathbb{Q},S}, V(f_k)(k/2); \Delta) \geq 0$$

is even (where the local conditions are as in 3.1.7).

Proof. We apply Theorem 2.3.10 to the big representation T of $G_{\mathbb{Q},S}$ and to its specializations at $I = \mathcal{P}_{k_0}$, $J = \mathcal{P}_k$. We must check the assumptions: First of all, T^+ is free over R by Prop. 1.5.2(iii) and 1.5.4. The representation $V_J = V(f_k)(k/2)$ satisfies (C1) by Lemma 3.1.3, (C2) by [Ri 1, Thm. 2.3], (C3) by 1.3.4. The condition (C4) follows from Lemma 2.3.8 (2) (or from (1.3.5.2)).

(3.3.2) COROLLARY. *Put $\varepsilon_k = 1$ if f_k is in the exceptional case, $\varepsilon_k = 0$ otherwise. Then*

$$\varepsilon_{k_0} + \dim_{F_{\mathfrak{p}}} H^1_f(\mathbb{Q}, V(f_{k_0})(k_0/2)) \equiv \dim_{F_{\mathfrak{p}}} H^1_f(\mathbb{Q}, V(f_k)(k/2)) + \varepsilon_k \pmod 2$$

whenever $k \equiv k_0 \pmod{(2(p-1)p^n)}$.

Proof. Use 3.1.7.

(3.4) Theorem B and Theorem C

(3.4.1) p-adic L-functions

Recall the basic properties of p-adic L-functions of modular forms, after Mazur-Tate-Teitelbaum [Ma-Ta-Te]: let $f = \sum_{n \geq 1} a_n q^n$ be a newform of weight $k \geq 2$ and character ε on $\Gamma_1(N)$. Fix a root α of $X^2 - a_p X + \varepsilon(p)p^{k-1} = 0$ satisfying $\mathrm{ord}_p(\alpha) < k-1$ (with the convention that $\varepsilon(p) = 0$ if $p \mid N$). The p-adic L-function

$$\chi \mapsto L^{MTT}_{p,\alpha}(f, \chi)$$

constructed in [Ma-Ta-Te] is a function of continuous characters $\chi : \mathbb{Z}_p^\times \longrightarrow \mathbb{C}_p^\times$ satisfying the following interpolation property:

$$L^{MTT}_{p,\alpha}(f, x^j \psi)$$
$$= \left(\frac{p^{j+1}}{\alpha}\right)^\nu \frac{j!}{(-2\pi i)^j G(\overline{\psi})} \left(1 - \frac{\overline{\psi}(p)\varepsilon(p)p^{k-2-j}}{\alpha}\right) \left(1 - \frac{\psi(p)p^j}{\alpha}\right) L_\infty(f, \overline{\psi}, j+1),$$

where $j = 0, 1, \ldots, k-2$, ψ is a Dirichlet character of conductor p^ν, $G(\overline{\psi})$ is the Gauss sum associated to $\overline{\psi}$, $L_\infty(f, \overline{\psi}, s) = \sum_{n \geq 1} a_n \overline{\psi}(n) n^{-s}$ and $x : \mathbb{Z}_p^\times \hookrightarrow \mathbb{C}_p^\times$ is the inclusion map.

Rather confusingly, this p-adic L-function has values in a certain module of periods, rather than in $\mathbb{C}_p$, as the value of the complex L-function is not divided by a complex period. For $s \in \mathbb{Z}_p$ one often writes $L_{p,\alpha}^{MTT}(f, \chi, s)$ for $L_{p,\alpha}^{MTT}(f, \chi\kappa^s)$. The case $p = 2$ is allowed in [Ma-Ta-Te]; κ then denotes the projection from $\mathbb{Z}_2^*$ to $1 + 4\mathbb{Z}_2$. If the form f is ordinary, there is only one choice of α, namely $\alpha = \alpha_p$ in the notation of 1.3.5; it is often omitted from the notation.

(3.4.2) Assume that k is even and $\varepsilon = 1$. In this case the p-adic L-function satisfies a particularly simple functional equation [Ma-Ta-Te, Sect. 17]:

$$L_{p,\alpha}^{MTT}(f, x^{k/2-1}\psi, s) = w_p(f)\psi^{-1}(-Q)\kappa(Q)^{-s} L_{p,\alpha}^{MTT}(f, x^{k/2-1}\psi^{-1}, -s), \tag{3.4.2.1}$$

where ψ is as above, $w_p(f) = \pm 1$ and Q denotes the largest positive divisor of N prime to p. Putting

$$\Lambda_{p,\alpha}(f, s) = \kappa(Q)^{s/2} L_{p,\alpha}^{MTT}(f, x^{k/2-1}, s - k/2),$$

the functional equation implies that

$$\Lambda_{p,\alpha}(f, s) = w_p(f)\Lambda_{p,\alpha}(f, k - s).$$

The value at the centre of symmetry of the functional equation is equal to

$$L_{p,\alpha}^{MTT}(f, x^{k/2-1}) = \frac{(k/2-1)!}{(-2\pi i)^{k/2-1}} \left(1 - \frac{\varepsilon(p)p^{k/2-1}}{\alpha}\right)\left(1 - \frac{p^{k/2-1}}{\alpha}\right) L_\infty(f, k/2).$$

(3.4.3) We now restrict our attention to ordinary forms. Changing notation, assume that $p \nmid N$ and let g be an ordinary p-stabilized newform of weight $k \geq 2$ and character ε on $\Gamma_1(Np^r)$, $r \geq 1$. Then either $g = f$ is a newform on $\Gamma_1(Np^r)$, $r \geq 1$, or $g = f^0$ is equal to the p-stabilization of a newform f on $\Gamma_1(N)$. In either case, $a_p(g) = \alpha_p(f)$. Greenberg-Stevens [Gr-St] use a slightly different normalization of p-adic L-functions, namely

$$L_p^{GS}(g, \psi\kappa^s) = \frac{L_p^{MTT}(f, \psi\kappa^{s-1})}{\Omega_f^{\mathrm{sgn}(\psi)}},$$

with ψ as in 3.4.1 and suitable periods $\Omega_f^{\pm} \in \mathbb{C}^\times$ of f. As before, the function on the L.H.S. will be denoted by $L_p^{GS}(g, \psi, s)$. If k is even and $\varepsilon = 1$, put

$$L_p(f, s) = L_p^{GS}(g, \omega^{k/2-1}, s).$$

(3.4.4) Two-variable p-adic L-functions

Assume now that $p > 3$ and that we are in the situation of 3.2.2. There is a two-variable p-adic L-function interpolating the p-adic L-functions of the forms f_k ([Gr-St], [Ki]). In the notation of [Gr-St] (omitting the variables Φ, κ), this function $L_p^{GS}(k, \psi, s)$ depends on $k \in k_0 + p^c\mathbb{Z}_p$ and ψ, s as in 3.4.3. Its main properties are the following ([Gr-St, Thm. 5.15, Cor. 5.17]):

(i) $L_p^{GS}(k, \psi, s)$ is analytic in $(k, s) \in (k_0 + p^c\mathbb{Z}_p) \times \mathbb{Z}_p$.

(ii) If $k \in k_0 + p^c\mathbb{Z}_p$ is an integer, $k \geq 2$, then $L_p^{GS}(k,\psi,s) = C_k L_p^{GS}(g_k,\psi,s)$ for some $C_k \in \mathbb{C}_p^\times$.

(iii) $L_p^{GS}(k,\psi,s) = -u\psi^{-1}(-N)\kappa(-N)^{k/2-s}L_p^{GS}(k,\omega^{k_0-2}\psi^{-1},k-s)$, where $u^2 = \omega^{k_0-2}(-N)$.

Put

$$L_p(k,s) = L_p^{GS}(k,\omega^{k_0/2-1},s)$$
$$\Lambda_p(k,s) = \kappa(N)^{s/2}L_p(k,s)$$

Then (iii) implies that

$$\Lambda_p(k,s) = w_p\Lambda_p(k,k-s)$$

with $w_p = \pm 1$. Comparing with (3.4.2.1) - with N playing the rôle of Q - we see that, for every integer $k \geq 2$, $k \equiv k_0 \pmod{(2(p-1)p^c)}$, we have

$$w_p(f_k) = w_p, \qquad L_p(k,s) = C_k L_p(f_k,s)$$

and

$$L_p(k,k/2) = C_k\frac{(k/2-1)!}{(-2\pi i)^{k/2-1}}(\mathrm{Eul}_k)\frac{L_\infty(f_k,k/2)}{\Omega_{f_k}^{\pm}}, \qquad (\pm = (-1)^{k/2-1})$$

where the Euler factor is equal to

$$(\mathrm{Eul}_k) = \left(1 - \frac{p^{k/2-1}}{\alpha_p(f_k)}\right)^{b_k}, \qquad b_k = \begin{cases} 1 & if \quad g_k = f_k \\ 2 & if \quad g_k = (f_k)^0 \end{cases}$$

It follows from [Ma-Ta-Te, Prop. 15] and 1.3.5 that the Euler factor Eul_k vanishes iff we are in the exceptional case (in the language of 3.1.1). The vanishing of Eul_k is sometimes referred to as a "trivial zero "of $L_p(f_k,s)$.

The value of w_p is related to the sign in the archimedean functional equation

$$\Lambda_\infty(f_k,s) = w_\infty(f_k)\Lambda_\infty(f_k,k-s)$$

by

$$w_p(f_k) = w_\infty(f_k) \times \begin{cases} -1 & \textit{in the exceptional case} \\ 1 & \textit{otherwise} \end{cases}$$

i.e. $w_p(f_k) = w_\infty(f_k)(-1)^{\varepsilon_k}$ ([Ma-Ta-Te, Sect. 18).

(3.4.5) Write $w_p = (-1)^{e_p}$ with $e_p = 0$ or 1. It follows that the function

$$F(k) := \left.\frac{L_p(k,s)}{(s-k/2)^{e_p}}\right|_{s=k/2}$$

is analytic for $k \in k_0 + p^c\mathbb{Z}_p$. A variant of conjectures formulated in [Gr 2] says the following:

GREENBERG'S CONJECTURE. *The function $F(k)$ is not identically zero.*

Equivalently, for all but finitely many $k \in \mathbb{Z}, k \geq 2$, $k \equiv k_0 \pmod{(p-1)p^c}$, we have $\mathrm{ord}_{s=k/2}L_p(f_k,s) = e_p$. This conjecture is known when f_{k_0} is a modular form of weight 2 corresponding to an elliptic curve E over $\mathbb{Q}$ with complex multiplication for which $e_p = 0$ ([Gr 1], [Ro]).

(3.4.6) As before, let $k \equiv k_0 \pmod{2(p-1)p^c}$, $k \geq 2$. We recall some of the known results relating behaviour of $L_p(f_k, s)$ at the central point $s = k/2$ and Selmer groups of Galois representations $V_k := V(f_k)(k/2)$.

(1) [Ne 2, Thm. C,D] Assume $k > 2$ (hence f_k is a newform on $\Gamma_0(N), p \nmid N$).

(i) If $\mathrm{ord}_{s=k/2} L_p(f_k, s) = 1$ then $\dim_{F_\mathfrak{p}} H^1_f(\mathbb{Q}, V_k) = 1$.

(ii) If $L_p(f_k, k/2) \neq 0$ and if there is an imaginary quadratic field $K = \mathbb{Q}(\sqrt{D})$ with odd discriminant $D < 0$ such that all primes dividing pN split in K and

$$\mathrm{ord}_{s=k/2} L_p(f_k \otimes \left(\frac{D}{\cdot}\right), s) = 1$$

then $H^1_f(\mathbb{Q}, V_k) = 0$.

(2) [Ka] If $L_p(f_k, k/2) \neq 0$, then $H^1_f(\mathbb{Q}, V_k) = 0$. In fact, Kato has announced a proof of the inequality

$$\dim_{F_\mathfrak{p}} H^1_f(\mathbb{Q}, V_k) \leq \mathrm{ord}_{s=k/2} L_p(f_k, s)$$

even without the ordinarity assumption.

(3.4.7) THEOREM B. *Under the assumptions of Theorem A, Greenberg's Conjecture for $L_p(k, s)$ implies that*

$$\dim_{F_\mathfrak{p}} H^1_f(\mathbb{Q}, V_{k_0}) \equiv e_\infty \pmod 2,$$

where $e_\infty \equiv e_p + \varepsilon_{k_0} \pmod 2$ is such that $w_\infty(f_{k_0}) = (-1)^{e_\infty}$.

Proof. Choose $k \equiv k_0 \pmod{2(p-1)p^n}$, $k > 2, k \in \mathbb{Z}$ for big enough n. Greenberg's Conjecture together with 3.4.3 imply that

$$\dim_{F_\mathfrak{p}} H^1_f(\mathbb{Q}, V_k) = \mathrm{ord}_{s=k/2} L_p(f_k, s) = e_p.$$

By Theorem A,

$$\dim_{F_\mathfrak{p}} H^1_f(\mathbb{Q}, V_{k_0}) \equiv \dim_{F_\mathfrak{p}} H^1_f(\mathbb{Q}, V_k) + \varepsilon_{k_0} \equiv e_p + \varepsilon_{k_0} \pmod 2$$

(we have $\varepsilon_k = 0$, since $k > 2$).

(3.4.8) THEOREM C. *Let E be a modular elliptic curve over $\mathbb{Q}$ with ordinary reduction at a prime $p > 3$. Assume that the p-torsion $E_p(\overline{\mathbb{Q}})$ is an irreducible $\mathbb{F}_p[G_\mathbb{Q}]$-module and that Greenberg's conjecture holds for the two-variable p-adic L-function of E. Then*

$$\dim_\mathbb{Q} (E(\mathbb{Q}) \otimes \mathbb{Q}) + \mathrm{cork}_{\mathbb{Z}_p} Ш(E/\mathbb{Q}) \equiv \mathrm{ord}_{s=1} L_\infty(E, s) \pmod 2.$$

Proof. By modularity, E corresponds to a cusp form f of weight $k_0 = 2$ on $\Gamma_0(N)$ with rational coefficients. The form f is ordinary iff E has ordinary reduction (possibly bad) at p. The p-torsion $E_p(\overline{\mathbb{Q}})$ is a residual representation of $V_{k_0} = V_p(E)$. Apply Theorem B.

(3.4.9) The parity statement of Theorem C has been proved in the following cases:

Unconditional results:

(1) $E : y^2 = x^3 - Dx$ (resp. $E : x^3 + y^3 = A$), $p = 2$ (resp. $p = 3$) (Birch-Stephens [Bi-St]).

(2) E is modular and $\mathrm{ord}_{s=1} L_\infty(E, s) \leq 1$; in this case $\dim_\mathbb{Q} (E(\mathbb{Q}) \otimes \mathbb{Q}) = \mathrm{ord}_{s=1} L_\infty(E, s)$ and $Ш(E/\mathbb{Q})$ is finite (Kolyvagin [Ko 1]).

(3) E has complex multiplication and ordinary reduction at $p > 3$ (Guo [Gu], who also proves Theorem A for some modular forms of higher weight with complex multiplication).

(4) E is modular and either $p = 2$, or $E_p(\overline{\mathbb{Q}})$ is a reducible $\mathbb{F}_p[G_{\mathbb{Q}}]$-module (Monsky [Mo]).

Conditional results:

(5) E is modular, $p > 2$, the Galois representation $G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}_{\mathcal{O}\otimes\mathbb{Z}_p}(T_p(E))$ is surjective (where $\mathcal{O} = \mathrm{End}(E)$) and the higher Heegner points satisfy a suitable non-degeneracy conjecture (Kolyvagin [Ko 2]).

(6) E is modular with split multiplicative reduction at $p > 3$, $w_\infty = -1$ and a variant of Greenberg's conjecture holds (Greenberg [Gr 3]).

(3.4.10) The results of Greenberg [Gr 1] and [Ro] on Greenberg's Conjecture for elliptic curves with complex multiplication and $e_p = 0$ give one instance when Theorem C gives an unconditional result. However, this case is already covered by (3) above.

(3.5) Theorem A′ and Theorem B′

(3.5.1) In the situation of 3.2, we can also consider specializations of T at more general arithmetic points. Using the notation of 1.4.7, fix an arithmetic point $\overline{\mathcal{P}} \in \mathfrak{X}^{arith}(\mathfrak{h}(\mathcal{K}))$ and denote by $\mathcal{P} = \mathrm{pr}^{-1}(\overline{\mathcal{P}}) \in \mathfrak{X}^{arith}(R)$ its preimage in R. Alternatively, we can forget $\overline{\mathcal{P}}$ and simply fix $\mathcal{P} \in \mathfrak{X}^{arith}(R)$ containing the minimal prime ideal $\mathfrak{q} = \mathrm{Ker}\,[R \longrightarrow \mathfrak{h}(\mathcal{K})]$ of R.

(3.5.2) Let us compute the Galois representation $T/\mathcal{P}T$. First of all, $\mathcal{P}$ lies above $(P_{k,\varepsilon}) \in \mathrm{Spec}(\Lambda)$ for some integer $k \geq 2$ and a character of finite order $\varepsilon : \Gamma \longrightarrow \mathcal{O}^\times$. By 1.4.7, $\mathcal{P}$ corresponds to a p-stabilized ordinary newform $f_{\mathcal{P}}$ of weight k and character $\chi_{\mathcal{P}} = \varepsilon\omega^{k_0-k}$. As $< \kappa(a) >_{\mathrm{Alb}} \equiv \varepsilon(a)\kappa(a)^{k-2} \pmod{\mathcal{P}}$, the same calculation as in 3.2.4 shows that

$$\begin{aligned} V_{[\mathcal{P}]} := (T/\mathcal{P}T) \otimes_{\mathcal{O}} F_{\mathfrak{p}} &\xrightarrow{\sim} V(f_{\mathcal{P}})^* \otimes [\kappa^{k_0/2-1}] \otimes [\varepsilon^{1/2}\kappa^{k/2-1}] \\ &\xrightarrow{\sim} V(f_{\mathcal{P}})(k-1) \otimes [\chi_{\mathcal{P}}^{-1}\omega^{k_0/2-1}\varepsilon^{1/2}\kappa^{k/2-1}] \\ &= V(f_{\mathcal{P}}) \otimes [\omega^{-k_0/2}\kappa^{-k/2}\varepsilon^{-1/2}] \end{aligned}$$

(as $p \neq 2$, $\varepsilon^{1/2} : \Gamma \longrightarrow \mathcal{O}^\times$ is well defined). If k is even, we have

$$V_{[\mathcal{P}]} \xrightarrow{\sim} V(f_{\mathcal{P}})(k/2) \otimes [\omega^{(k-k_0)/2}\varepsilon^{-1/2}].$$

As $(\omega^{(k-k_0)/2}\varepsilon^{-1/2})^2 = \chi_{\mathcal{P}}^{-1}$, it makes sense to denote $\omega^{(k-k_0)/2}\varepsilon^{-1/2}$ by "$\chi_{\mathcal{P}}^{-1/2}$", hence

$$V_{[\mathcal{P}]} \xrightarrow{\sim} V(f_{\mathcal{P}})(k/2) \otimes [\text{“}\chi_{\mathcal{P}}^{-1/2}\text{”}]. \tag{3.5.2.1}$$

If the Fourier expansion of $f_{\mathcal{P}}$ is $\sum_{n\geq 1} a_n(f_{\mathcal{P}})q^n$, then $\sum_{n\geq 1}$ "$\chi_{\mathcal{P}}^{-1/2}$"$(n)a_n(f_{\mathcal{P}})q^n$ is the Fourier expansion of a Hecke eigenform $\widetilde{f}_{\mathcal{P}}$ on some $\Gamma_0(Np^r)$ (i.e. $\widetilde{f}_{\mathcal{P}}$ has trivial character). The formula (3.5.2.1) then becomes

$$V_{[\mathcal{P}]} \xrightarrow{\sim} V(\widetilde{f}_{\mathcal{P}})(k/2).$$

This representation is self-dual in the usual way: $V_{[\mathcal{P}]} \xrightarrow{\sim} V_{[\mathcal{P}]}^*(1)$.

(3.5.3) From now on, $\mathcal{P}$ is fixed and we assume that the weight k of $f_{\mathcal{P}}$ is even. We have the following Galois representations associated to T:

$$T^* = \mathrm{Hom}_\Lambda(T,\Lambda), \qquad (T^*)^\pm = \mathrm{Hom}_\Lambda(T^\mp,\Lambda), \qquad A^* = \mathrm{Hom}_{\mathcal{O},\mathrm{cont}}(T, F_\mathfrak{p}/\mathcal{O}),$$
$$A = \mathrm{Hom}_{\mathcal{O},\mathrm{cont}}(T^*, F_\mathfrak{p}/\mathcal{O}), \qquad A^\pm = \mathrm{Hom}_{\mathcal{O},\mathrm{cont}}((T^*)^\mp, F_\mathfrak{p}/\mathcal{O})$$

and also various specializations

$$T_{[\mathcal{P}]} = \mathrm{Im}\left(T/\mathcal{P}T \longrightarrow V_{[\mathcal{P}]}\right), \quad T^+_{[\mathcal{P}]} = T^+/\mathcal{P}T^+ \subset T_{[\mathcal{P}]}, \quad V^+_{[\mathcal{P}]} = T^+_{[\mathcal{P}]} \otimes_{\mathcal{O}} F_\mathfrak{p} \subset V_{[\mathcal{P}]},$$
$$A_{[\mathcal{P}]} = V_{[\mathcal{P}]}/T_{[\mathcal{P}]}, \qquad A^+_{[\mathcal{P}]} = V^+_{[\mathcal{P}]}/T^+_{[\mathcal{P}]}.$$

The isomorphism $T \xrightarrow{\sim} T^*(1)$ defined by the pairing $\langle\ ,\ \rangle_T : T \times T \longrightarrow \Lambda(1)$ induces isomorphisms

$$T^\pm \xrightarrow{\sim} (T^*)^\pm(1), \qquad A \xrightarrow{\sim} A^*(1). \tag{3.5.3.1}$$

As in 2.2, we consider Selmer complexes, this time for "big Galois representations" $X = T, A$ of $G_{\mathbb{Q},S}$, where $S = \{\ell \mid pN\} \cup \{\infty\}$. All cochains will be continuous with respect to the $\mathfrak{m}$-adic topology on $T, T^*, T^\pm$ and the discrete topology on $A, A^*, A^\pm$. The local conditions will be given by

$$\Delta_v: \qquad U_v^+(X) = \begin{cases} 0 & v \neq p,\ v \in S_f \\ \mathcal{C}^\bullet_{cont}(G_{\mathbb{Q}_p}, X^+) & v = p \end{cases}$$

Identifying $X^*(1)$ with X as in (3.5.3.1), the dual local conditions become

$$\Delta_v^*(1): \qquad U_v^+(X) = \begin{cases} \mathcal{C}^\bullet_{cont}(G_{\mathbb{Q}_v}, X) & v \neq p,\ v \in S_f \\ \mathcal{C}^\bullet_{cont}(G_{\mathbb{Q}_p}, X^+) & v = p \end{cases}$$

(one can make the local conditions at $v \neq p$ also self dual, but it is irrelevant for our purposes). For the specializations $X_{[\mathcal{P}]} = T_{[\mathcal{P}]}, A_{[\mathcal{P}]}, V_{[\mathcal{P}]}$ we use the same local conditions

$$\Delta_v: \qquad U_v^+(X_{[\mathcal{P}]}) = \begin{cases} 0 & v \neq p,\ v \in S_f \\ \mathcal{C}^\bullet_{cont}(G_{\mathbb{Q}_p}, X^+_{[\mathcal{P}]}) & v = p \end{cases}$$

In this case, the above formula for $\Delta_v^*(1)$ will be true up to a finite error term.

(3.5.4) Recall that an R-module M of finite type is *pseudo-null* if $\mathrm{Supp}(M)$ has codimension ≥ 2 in $\mathrm{Spec}(R)$. As $\dim(R) = 2$ and $R/\mathfrak{m}$ is finite, this is equivalent to M being finite. We shall ignore pseudo-null modules and work in the category $(R\text{-mod})/(\text{ps-null})$ which is obtained from $(R\text{-mod})$ by inverting all morphisms with pseudo-null kernel and cokernel. Recall that, for every R-module of finite type with $\mathcal{P} \in \mathrm{Supp}(M)$, there is a non-zero homomorphism $M/\mathcal{P}M \longrightarrow R/\mathcal{P}$.

(3.5.5) LEMMA. *The canonical maps*

(*i*) $\quad T^+ \overset{\mathbb{L}}{\otimes}_R R/\mathcal{P} \longrightarrow T^+/\mathcal{P}T^+ \longrightarrow T^+_{[\mathcal{P}]}$

(*ii*) $\quad T \overset{\mathbb{L}}{\otimes}_R R/\mathcal{P} \longrightarrow T/\mathcal{P}T \longrightarrow T_{[\mathcal{P}]}$

(*iii*) $\quad \mathbb{R}\widetilde{\Gamma}_f(G_{\mathbb{Q},S}, T; -) \overset{\mathbb{L}}{\otimes}_R R/\mathcal{P} \longrightarrow \mathbb{R}\widetilde{\Gamma}_f(G_{\mathbb{Q},S}, T_{[\mathcal{P}]}; -) \qquad (- = \Delta, \Delta^*(1))$

are isomorphisms in (i) $D^b(R\text{-mod})$; (ii), (iii) $D^b(R\text{-mod})/(\text{ps-null})$.

Proof. (i) T^+ is free over R.

(ii) This was proved in 1.5.6.

(iii) Taking $C^\bullet_{cont}(G,-)$ commutes with tensor products with flat R-modules, for a suitable definition of "*cont*" ([Ne3]). The statement then follows from (i), (ii) and the fact that $H^i(G,M)$ is finite (and zero for $i \geq 2$) for $G = G_{\mathbb{Q},S}, G_{\mathbb{Q}_v}$ and every finite G-module M.

(3.5.6) Duality ([Ne 3])

Local duality: $H^i(G_{\mathbb{Q}_v},T) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{O},\mathrm{cont}}(H^{2-i}(G_{\mathbb{Q}_v},A^*(1)),F_\mathfrak{p}/\mathcal{O})$

Global duality:
(a) $\mathrm{Hom}_{\mathcal{O},\mathrm{cont}}(\widetilde{H}^i_f(G_{\mathbb{Q},S},T;\Delta),F_\mathfrak{p}/\mathcal{O}) \xrightarrow{\sim} \widetilde{H}^{3-i}_f(G_{\mathbb{Q},S},A^*(1);\Delta^*(1))$

(b) $\mathbb{R}\widetilde{\Gamma}_f(G_{\mathbb{Q},S},\ T;\ \Delta) \xrightarrow{\sim} \mathbb{R}\mathrm{Hom}_R(\mathbb{R}\widetilde{\Gamma}_f(G_{\mathbb{Q},S},\ T^*(1);\ \Delta^*(1)),\ \omega_R)[-3]$ in $D^b_{ft}(R\text{-mod})$ (this isomorphism being suitably skew-symmetric).

(3.5.7) PROPOSITION. *The canonical map*

$$\widetilde{H}^2_f(G_{\mathbb{Q},S},T;-)/\mathcal{P} \longrightarrow \widetilde{H}^2_f(G_{\mathbb{Q},S},T_{[\mathcal{P}]};-) \qquad (-=\Delta,\Delta^*(1))$$

is an isomorphism in (R-mod)/(ps-null).

Proof. Lemma 3.5.5 (iii) boils down to a spectral sequence

$$E^2_{i,j} = \mathrm{Tor}^R_i(R/\mathcal{P},\widetilde{H}^{-j}_f(G_{\mathbb{Q},S},T;-)) \Rightarrow \widetilde{H}^{-i-j}_f(G_{\mathbb{Q},S},T_{[\mathcal{P}]};-)$$

in (R-mod)/(ps-null) which gives an exact sequence

$$0 \longrightarrow E^2_{0,-2} \longrightarrow \widetilde{H}^2_f(G_{\mathbb{Q},S},T_{[\mathcal{P}]};-) \longrightarrow E^2_{1,-3} \longrightarrow 0. \tag{3.5.7.1}$$

However, global duality 3.5.6 implies that

$$\mathrm{Hom}_{\mathcal{O},\mathrm{cont}}(\widetilde{H}^3_f(G_{\mathbb{Q},S},T;-),F_\mathfrak{p}/\mathcal{O}) \xrightarrow{\sim} \widetilde{H}^0_f(G_{\mathbb{Q},S},A^*(1);(-)^*(1))$$

is a subgroup of $H^0(G_\mathbb{Q},A^*(1)) = H^0(G_\mathbb{Q},A)$, which is dual to $H_0(G_\mathbb{Q},T)$. The representation $V_{[\mathcal{P}]}$ has weight -1, hence $H_0(G_\mathbb{Q},T)/\mathcal{P}$ is finite and $(E^2_{1,-3})_\mathcal{P} = 0$. As $\mathrm{Supp}(E^2_{1,-3}) \subseteq \{\mathcal{P},\mathfrak{m}\}$, $E^2_{1,-3}$ is pseudo-null. We conclude by (3.5.7.1).

(3.5.8) PROPOSITION. *For every prime $v \in S_f$, $v \neq p$,*

$$H^0(G_{\mathbb{Q}_v},T) = 0, \qquad H^1(G_{\mathbb{Q}_v},T)_\mathcal{P} = H^2(G_{\mathbb{Q}_v},T)_\mathcal{P} = 0.$$

Proof. Lemma 3.1.3 applies to $V_{[\mathcal{P}]}$ (as k is even), hence $H^0(G_{\mathbb{Q}_v},T_{[\mathcal{P}]}) = 0$, and $H^0(G_{\mathbb{Q}_v},T) = 0$. By the same argument, the $\mathcal{P}$-torsion in $H^0(G_{\mathbb{Q}_v},A^*(1)) = H^0(G_{\mathbb{Q}_v},A)$ is finite, hence $H^2(G_{\mathbb{Q}_v},T)/\mathcal{P}$ is finite by local duality. This implies that $H^2(G_{\mathbb{Q}_v},T)_\mathcal{P} = 0$ (cf. the remark at the end of 3.5.4). For H^1, consider the spectral sequence in (R-mod)/(ps-null)

$$E^2_{i,j} = \mathrm{Tor}^R_i(R/\mathcal{P},H^{-j}(G_{\mathbb{Q}_v},T)) \Rightarrow H^{-i-j}(G_{\mathbb{Q}_v},T_{[\mathcal{P}]})).$$

In the exact sequence

$$0 \longrightarrow E^2_{0,-1} \longrightarrow H^1(G_{\mathbb{Q}_v},T_{[\mathcal{P}]}) \longrightarrow E^2_{1,-2} \longrightarrow 0$$

the middle term is finite (again by Lemma 3.1.3), and so $E^2_{0,-1} = H^1(G_{\mathbb{Q}_v},T)/\mathcal{P}$ must be finite, too.

(3.5.9) COROLLARY. *The canonical map*

$$\mathbb{R}\widetilde{\Gamma}_f(G_{\mathbb{Q},S},T;\Delta) \longrightarrow \mathbb{R}\widetilde{\Gamma}_f(G_{\mathbb{Q},S},T;\Delta^*(1))$$

induces isomorphisms on localizations $\widetilde{H}^i_f(G_{\mathbb{Q},S},T;\Delta)_{\mathcal{P}} \xrightarrow{\sim} \widetilde{H}^i_f(G_{\mathbb{Q},S},T;\Delta^*(1))_{\mathcal{P}}$.

Proof. This follows from Prop. 3.5.8 and a distinguished triangle

$$\mathbb{R}\widetilde{\Gamma}_f(G_{\mathbb{Q},S},T;\Delta) \longrightarrow \mathbb{R}\widetilde{\Gamma}_f(G_{\mathbb{Q},S},T;\Delta^*(1)) \longrightarrow \bigoplus_{\substack{v\in S_f\\ v\neq p}} \mathbb{R}\Gamma(G_{\mathbb{Q}_v},T).$$

(3.5.10) The global duality 3.5.6 gives a spectral sequence in (R-mod) (with all $E_2^{i,j}$ of finite type over R)

$$E_2^{i,j} = \mathrm{Ext}^i_R(\widetilde{H}^{3-j}_f(G_{\mathbb{Q},S},T;\Delta^*(1)),\omega_R) \Rightarrow \widetilde{H}^{i+j}_f(G_{\mathbb{Q},S},T;\Delta).$$

We shall localize this sequence at $\mathcal{P}$. As $R_{\mathcal{P}}$ is a discrete valuation ring, there is an isomorphism $(\omega_R)_{\mathcal{P}} = \omega_{R_{\mathcal{P}}} \xrightarrow{\sim} R_{\mathcal{P}}$, well-defined up to a unit in $R_{\mathcal{P}}$ (the exact normalization is irrelevant). The localization gives an exact sequence (using Corollary 3.5.9)

$$0 \longrightarrow \mathrm{Ext}^1_{R_{\mathcal{P}}}(N_{\mathcal{P}},R_{\mathcal{P}}) \xrightarrow{\alpha} N_{\mathcal{P}} \longrightarrow \mathrm{Hom}_{R_{\mathcal{P}}}(\widetilde{H}^1_f(G_{\mathbb{Q},S},T;\Delta)_{\mathcal{P}},R_{\mathcal{P}}) \longrightarrow 0,$$

where $N = \widetilde{H}^2_f(G_{\mathbb{Q},S},T;\Delta)$. This is an R-module of finite type; denote its torsion submodule by $M = \mathrm{Tors}_R(N)$ ($x \in N$ is torsion iff $rx = 0$ for some $r \in R$ which is not a zero-divisor) and put $Q = N/M$. As $M_{\mathcal{P}} = \mathrm{Tors}_{R_{\mathcal{P}}}(N_{\mathcal{P}})$, the exact sequence of Ext's associated to

$$0 \longrightarrow M_{\mathcal{P}} \longrightarrow N_{\mathcal{P}} \longrightarrow Q_{\mathcal{P}} \longrightarrow 0$$

implies that the canonical map

$$\mathrm{Ext}^1_{R_{\mathcal{P}}}(N_{\mathcal{P}},R_{\mathcal{P}}) \xrightarrow{\sim} \mathrm{Ext}^1_{R_{\mathcal{P}}}(M_{\mathcal{P}},R_{\mathcal{P}})$$

is an isomorphism ($Q_{\mathcal{P}}$ is torsion free, hence free over $R_{\mathcal{P}}$). This implies that α induces an isomorphism

$$\alpha' : \mathrm{Ext}^1_{R_{\mathcal{P}}}(M_{\mathcal{P}},R_{\mathcal{P}}) \xrightarrow{\sim} \mathrm{Tors}_{R_{\mathcal{P}}}(N_{\mathcal{P}}) = M_{\mathcal{P}}.$$

The $R_{\mathcal{P}}$-module $M_{\mathcal{P}}$ is killed by some $r \in R_{\mathcal{P}}$, $r \neq 0$. The sequence

$$0 \longrightarrow R_{\mathcal{P}} \xrightarrow{r} R_{\mathcal{P}} \longrightarrow R_{\mathcal{P}}/rR_{\mathcal{P}} \longrightarrow 0$$

gives an isomorphism

$$\mathrm{Hom}_{R_{\mathcal{P}}}(M_{\mathcal{P}},R_{\mathcal{P}}/rR_{\mathcal{P}}) \xrightarrow{\sim} \mathrm{Ext}^1_{R_{\mathcal{P}}}(M_{\mathcal{P}},R_{\mathcal{P}})$$

which, combined with α', yields an isomorphism

$$\mathrm{Hom}_{R_{\mathcal{P}}}(M_{\mathcal{P}},R_{\mathcal{P}}/rR_{\mathcal{P}}) \xrightarrow{\sim} M_{\mathcal{P}}$$

which is skew-symmetric, i.e. comes from a skew-symmetric bilinear form

$$M_{\mathcal{P}} \times M_{\mathcal{P}} \longrightarrow R_{\mathcal{P}}/rR_{\mathcal{P}}$$

(by skew-symmetry of the global duality isomorphism). The residue field of $R_{\mathcal{P}}$ has characteristic zero, which implies that the form is alternating. Standard structure theory of symplectic modules of finite length over discrete valuation rings implies that

$$M_{\mathcal{P}} \xrightarrow{\sim} X \oplus X$$

for an $R_{\mathcal{P}}$-module X of finite length.

(3.5.11) LEMMA. *Let A be an integral domain and $I \subset A$ a prime ideal such that the localization A_I is a discrete valuation ring. If Y is a torsion-free A-module of finite type, then*

$$\mathrm{rk}_{A/I}(Y/IY) = \mathrm{rk}_A(Y)$$

(recall that $\mathrm{rk}_A(Y) = \dim_K(Y \otimes_A K)$, where K is the fraction field of A).

Proof. The localization Y_I is a torsion-free A_I-module of finite type, hence free of rank n. Then

$$\mathrm{rk}_{A/I}(Y/IY) = \dim_{A_I/IA_I}(Y_I/IY_I) = n$$
$$\dim_K(Y \otimes_A K) = \dim_K(Y_I \otimes_{A_I} K) = n.$$

(3.5.12) PROPOSITION.

$$\mathrm{rk}_{R/\mathcal{P}}(N/\mathcal{P}N) \equiv \mathrm{rk}_{R/\mathfrak{q}}(Q/\mathfrak{q}Q) \pmod 2.$$

Proof. Recall that $\mathfrak{q} = \mathrm{Ker}\,[R \longrightarrow \mathfrak{h}(\mathcal{K})]$, $R/\mathfrak{q} = \mathfrak{h}(\mathcal{K})$. We have

$$\mathrm{rk}_{R/\mathcal{P}}(N/\mathcal{P}N) = \mathrm{rk}_{R/\mathcal{P}}(M/\mathcal{P}M) + \mathrm{rk}_{R/\mathcal{P}}(Q/\mathcal{P}Q),$$

as $Q_{\mathcal{P}}$ is free over $R_{\mathcal{P}}$ (of course, $R/\mathcal{P} = \mathcal{O}$). However,

$$\mathrm{rk}_{R/\mathcal{P}}(M/\mathcal{P}M) = \dim_{R_{\mathcal{P}}/\mathcal{P}R_{\mathcal{P}}}(M_{\mathcal{P}}/\mathcal{P}M_{\mathcal{P}}) = 2\dim_{R_{\mathcal{P}}/\mathcal{P}R_{\mathcal{P}}}(X/\mathcal{P}X)$$

is even and

$$\mathrm{rk}_{R/\mathcal{P}}(Q/\mathcal{P}Q) = \mathrm{rk}_{R/\mathfrak{q}}(Q/\mathfrak{q}Q)$$

by Lemma 3.5.11 applied to $A = R/\mathfrak{q}, I = \mathcal{P}/\mathfrak{q} = \overline{\mathcal{P}}$ and $Y = Q/\mathfrak{q}Q$.

(3.5.13) THEOREM A′. *In the notation of (3.5.1–2) – in particular, if $k_0 \equiv 2 \pmod{(p-1)}$, assume that $V(f_{k_0})$ has an irreducible residual representation – for every $\mathcal{P} \in \mathfrak{X}^{arith}(R)$ containing $\mathfrak{q}$ and such that $f_{\mathcal{P}}$ has even weight,*

$$\dim_{F_{\mathfrak{p}}} \widetilde{H}^1_f(G_{\mathbb{Q},S}, V_{[\mathcal{P}]}; \Delta) \equiv \mathrm{rk}_{R/\mathfrak{q}}(Q/\mathfrak{q}Q) \pmod 2,$$

hence the parity of the L.H.S. does not depend on $\mathcal{P}$.

Proof. The dimension on the L.H.S. is equal to

$$\begin{aligned}\mathrm{cork}_{\mathcal{O}}\widetilde{H}^1_f(G_{\mathbb{Q},S}, A_{[\mathcal{P}]}; \Delta) &= \mathrm{cork}_{\mathcal{O}}\widetilde{H}^1_f(G_{\mathbb{Q},S}, A^*(1)_{[\mathcal{P}]}; \Delta^*(1)) \\ &\quad \text{(by almost self duality of the local conditions; cf. proof of 2.3.10)} \\ &= \mathrm{rk}_{\mathcal{O}}\widetilde{H}^2_f(G_{\mathbb{Q},S}, T_{[\mathcal{P}]}; \Delta) \qquad \text{(global duality 3.5.6)} \\ &= \mathrm{rk}_{\mathcal{O}}(N/\mathcal{P}N) \qquad \text{(Prop. 3.5.7)}\end{aligned}$$

Now apply Proposition 3.5.12.

(3.5.14) Let us compare the group $\widetilde{H}^1_f(G_{\mathbb{Q},S}, V_{[\mathcal{P}]}; \Delta)$ and the Bloch-Kato Selmer group $H^1_f(\mathbb{Q}, V_{[\mathcal{P}]})$. First of all, Lemma 3.1.3 still holds for $V = V_{[\mathcal{P}]}$, thus the local conditions for both groups vanish at all primes $v \in S_f, v \neq p$. As a representation of $G_{\mathbb{Q}_p}$, there is an exact sequence

$$0 \longrightarrow V_p^+ \longrightarrow V \longrightarrow V_p^- \longrightarrow 0,$$

with $\left(V_p^{\pm}\right)^*(1) \xrightarrow{\sim} V_p^{\mp}$ by self duality of V. Each $V_p^{\pm}$ is a twist of a crystalline representation by "$\chi_{\mathcal{P}}^{-1/2}$". Note that "$\chi_{\mathcal{P}}^{-1/2}$" $= \omega^{(k-k_0)/2}\varepsilon^{-1/2}$ is unramified iff

"$\chi_{\mathcal{P}}^{-1/2}$" $= 1$ (which is equivalent to $k \equiv k_0 \pmod{2(p-1)}$ and $\varepsilon = 1$). In this case, results of 3.1.6–7 apply. Assume that "$\chi_{\mathcal{P}}^{-1/2}$" $\neq 1$. Then neither of $V_p^{\pm}$ is a crystalline representation of $G_{\mathbb{Q}_p}$, hence

$$D_{cris}(V_p^{\pm}) = D_{cris}(V) = H^0(G_{\mathbb{Q}_p}, V_p^{\pm}) = H^0(G_{\mathbb{Q}_p}, V) = 0.$$

The representation V is potentially semistable (in fact is semistable over $\mathbb{Q}_p(\mu_{p^r})$ for suitable r), therefore de Rham. It follows from 2.1.6 and self-duality $V \xrightarrow{\sim} V^*(1)$ that

$$H_f^1(G_{\mathbb{Q}_p}, V) = H_g^1(G_{\mathbb{Q}_p}, V) = \mathrm{Im}[H^1(G_{\mathbb{Q}_p}, V^+) \longrightarrow H^1(G_{\mathbb{Q}_p}, V)].$$

Combining with the results of 3.1.7, we obtain an exact sequence

$$0 \longrightarrow F_{\mathfrak{p}}^{\varepsilon(\mathcal{P})} \longrightarrow \widetilde{H}_f^1(G_{\mathbb{Q},S}, V_{[\mathcal{P}]}; \Delta) \longrightarrow H_f^1(\mathbb{Q}, V) \longrightarrow 0, \tag{3.5.14.1}$$

in which $\varepsilon(\mathcal{P}) = 1$ in the exceptional case, and $\varepsilon(\mathcal{P}) = 0$ otherwise. The exceptional case occurs iff $k = 2$, $\varepsilon = 1$, $k \equiv k_0 \pmod{2(p-1)}$, and $a_p(f_{\mathcal{P}}) = 1$.

(3.5.15) THEOREM B′. *Let $p > 3$ be a prime not dividing N and $f = \sum_{n \geq 1} a_n q^n$ an ordinary newform of even weight $k \geq 2$ and character χ^{-2} on $\Gamma_1(Np^r)$, where $\mathrm{cond}(\chi) = p^s$ (necessarily with $s = r$, if $\chi \neq 1$). Then $\widetilde{f} = \sum_{n \geq 1} a_n \chi(n) q^n$ is a newform of weight k on $\Gamma_0(Np^{2r})$ (resp. $\Gamma_0(Np^r)$) if $\chi \neq 1$ (resp. $\chi = 1$). If the tame part of χ^2 is equal to ω^{k-2}, where ω is the Teichmüller character, assume that $V(f)$ has an irreducible residual representation. If Greenberg's Conjecture holds for the two-variable p-adic L-function of f, then*

$$\dim_{\widetilde{F}_{\mathfrak{p}}} H_f^1(\mathbb{Q}, V(\widetilde{f})(k/2)) \equiv \mathrm{ord}_{s=k/2} L_\infty(\widetilde{f}, s) \pmod 2.$$

Proof. Replacing $\widetilde{F}_{\mathfrak{p}}$ by a finite extension (and $V(\widetilde{f})$ by its base change) we can assume that $\widetilde{F}_{\mathfrak{p}}$ contains all values of χ. The form f – or its p-stabilization, if $r = 0$ – is then equal to $f_{\mathcal{P}}$ and $\widetilde{f}$ to $\widetilde{f}_{\mathcal{P}}$, for a suitable Hida family of the type considered in 3.5.1–2 and $\mathcal{P} \in \mathfrak{X}^{arith}(R)$, $\mathcal{P} \supset \mathfrak{q}$, "$\chi_{\mathcal{P}}^{-1/2}$" $= \chi$. If $\chi = 1$, then $\widetilde{f}$ is ordinary and Theorem B applies. Assume that $\chi \neq 1$ (hence χ is ramified at p). In this case

$$H_f^1(\mathbb{Q}, V(\widetilde{f})(k/2)) = \widetilde{H}_f^1(G_{\mathbb{Q},S}, V(\widetilde{f})(k/2); \Delta)$$

by (3.5.14.1). Choose a p-stabilized newform $f_{k'}$ corresponding to some $\mathcal{P}' \in \mathfrak{X}^{arith}(R)$ containing $\mathfrak{q}$, of even weight $k' \geq 2$, with trivial character and such that $e_p = \mathrm{ord}_{s=k'/2} L_p(f_{k'}, s) \leq 1$. It follows from Theorem A′ and 3.4.6 that

$$\dim_{\widetilde{F}_{\mathfrak{p}}} H_f^1(\mathbb{Q}, V(\widetilde{f})(k/2)) \equiv e_p \pmod 2.$$

It remains to show that $w_p(f_{k'}) = (-1)^{e_p}$ (the sign in the functional equation of $L_p(f_{k'}, s)$) coincides with $w_\infty(\widetilde{f})$, the sign in the functional equation of $L_\infty(\widetilde{f}, s)$. First of all, $w_p(f_{k'}) = w_p = w_p(f)$, by 3.4.4. The formula [Ma-Ta-Te, Sect. 17, Cor.2] implies that

$$L_{p,\alpha}^{MTT}(f, x^{k/2-1}, \chi^{-1}, s) = (-1)^{k/2} c_N \chi^{-1}(N) \kappa(N)^{-s} L_{p,\alpha}^{MTT}(f, x^{k/2-1}, \chi^{-1}, -s)$$

where c_N is the eigenvalue of the Atkin-Lehner involution acting on f: $f|W_N = c_N \chi^{-1}(-N) f$. Hence

$$w_p(f) = (-1)^{k/2} c_N \chi^{-1}(-N).$$

The archimedean sign $w_\infty(\widetilde{f})$ is also equal to

$$w_\infty(\widetilde{f}) = (-1)^{k/2} c_N \chi^{-1}(-N)$$

by [Ma-Ta-Te, Sect.18, Rmk] (in their notation, $q = N$, $q' = p^r$, $\psi = \chi$, $\varepsilon = \chi^{-2}$, $\phi = \chi$, $f_\psi = \widetilde{f}$, $g = c_N f$). Theorem follows.

4. Λ-adic Selmer groups. In this section, we give an elementary approach to an important special case of theorem A′, when the local component R of the Hecke algebra is equal to the Iwasawa algebra $\Lambda = \mathcal{O}[[X]]$, using the Λ-adic Selmer groups and Tate-Šafarevič groups introduced in [Pl]. To a self dual Λ-adic Galois representation T, we shall associate a Λ-adic Tate-Šafarevič group whose Pontryagin dual $\widehat{Ш}$ is a finitely generated torsion Λ-module, and prove the following result.

(4.0.1) PROPOSITION. *Let $p > 2$. If T satisfies the assumptions of 4.1.1 below, then there is a finitely generated torsion Λ-module X such that $\widehat{Ш}$ is pseudo-isomorphic to $X \oplus X$.*

The corresponding result for specializations of T is a consequence of a generalized Cassels-Tate pairing. We deduce the Λ-adic result by specializing at enough primes.

(4.1) Λ-adic Galois representations

(4.1.1) Let p be a rational prime, $F_\mathfrak{p}$ a finite extension of $\mathbb{Q}_p$ with ring of integers $\mathcal{O}$ and prime element $\pi \in \mathcal{O}$. Let $\Lambda = \mathcal{O}[[X]]$ with maximal ideal $\mathfrak{m} = (X, \pi)$. Let T be a free rank two Λ-module with a continuous Λ-linear $G_{\mathbb{Q},S}$-action, where S is some finite set of primes including p and infinity. We assume that T is ordinary at p, by which we mean that T sits in an exact sequence of $\Lambda[G_{\mathbb{Q}_p}]$-modules

$$0 \longrightarrow T^+ \longrightarrow T \longrightarrow T^- \longrightarrow 0 \tag{4.1.1.1}$$

with T^+ and T^- free rank one Λ-modules, and assume there is a skew-symmetric Galois-invariant bilinear form

$$\langle\ ,\ \rangle_T\ :\ T \times T \longrightarrow \Lambda(1) \tag{4.1.1.2}$$

inducing an isomorphism

$$T \xrightarrow{\sim} T^*(1) := \mathrm{Hom}_\Lambda(T, \Lambda)(1), \qquad t \mapsto \langle t,\ .\ \rangle_T$$

and isomorphisms $T^\pm \xrightarrow{\sim} (T^*)^\pm(1)$, where $(T^*)^\pm := \mathrm{Hom}_\Lambda(T^\mp, \Lambda)$.

We also assume that the following cohomology groups are trivial:

$$H^0(\mathbb{Q}_v, T) = 0 \qquad \text{for all } v \neq p, \tag{4.1.1.3}$$

$$H^0(\mathbb{Q}_p, T^+) = H^0(\mathbb{Q}_p, T^-) = 0. \tag{4.1.1.4}$$

(4.1.2) Specializations

The height one primes of Λ are the prime (π) and primes (λ), where $\lambda \in \Lambda$ is an irreducible distinguished polynomial, i.e. λ is irreducible and of the form $\lambda = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ with $\pi \mid a_i$ for $0 \leq i \leq n-1$. Let $X = \mathrm{Spec}(\Lambda) - \{(\pi)\}$. This agrees with the definition of X in 2.3.2 in this special case. For $(\lambda) \in X$, we write $\mathcal{O}_\lambda = \Lambda/(\lambda)$ and $T_\lambda = T/\lambda T = T \otimes_\Lambda \mathcal{O}_\lambda$, $T_\lambda^\pm = T^\pm/\lambda T^\pm$. So $\mathcal{O}_\lambda$ is free of finite rank over $\mathcal{O}$ and T_λ (resp. $T_\lambda^\pm$) is a free $\mathcal{O}_\lambda$-module of rank two (resp. one). We call T_λ the specialization of T at λ.

(4.1.3) Let $G = G_{\mathbb{Q},S}$ or $G_{\mathbb{Q}_v}$. The continuous cohomology groups $H^n(G,T)$ are finitely generated Λ-modules and the $H^n(G,T_\lambda)$ are finitely generated $\mathcal{O}_\lambda$-modules. Let $M = T, T^+$ or T^-. Taking cohomology of the short exact sequence

$$0 \longrightarrow M \xrightarrow{\lambda} M \longrightarrow M_\lambda \longrightarrow 0 \tag{4.1.3.1}$$

as G-modules gives a short exact sequence of $\mathcal{O}_\lambda$-modules

$$0 \longrightarrow \frac{H^n(G,M)}{\lambda H^n(G,M)} \longrightarrow H^n(G,M_\lambda) \longrightarrow H^{n+1}(G,M)[\lambda] \longrightarrow 0. \tag{4.1.3.2}$$

(4.1.4) In the special case when $R = \Lambda = \mathcal{O}[[\Gamma]]$, and assuming the Assumption of 3.2.3, the twisted Galois representation T of 3.2.3 satisfies the conditions of 4.1.1. If we identify $\mathcal{O}[[\Gamma]]$ with $\mathcal{O}[[X]]$ via $\gamma = 1+p \mapsto 1+X$ (choosing $\gamma = 1+p$ as a topological generator for $\Gamma \xrightarrow{\sim} 1 + p\mathbb{Z}_p$) then the arithmetic point $(P_{k,\varepsilon}) \in \mathrm{Spec}(\Lambda)$ corresponds to the height one prime ideal generated by $\lambda_{k,\varepsilon} = 1+X-\varepsilon(1+p)(1+p)^{k-2} \in \mathcal{O}[[X]]$. We just need to check conditions (4.1.1.3) and (4.1.1.4); To check (4.1.1.3), it is enough to specialize at any arithmetic point λ, where $H^0(\mathbb{Q}_v,T_\lambda) = 0$ by Lemma 3.1.3. Then 4.1.3.2 gives

$$0 \longrightarrow \frac{H^0(\mathbb{Q}_v,T)}{\lambda H^n(\mathbb{Q}_v,T)} \longrightarrow H^0(\mathbb{Q}_v,T_\lambda) = 0$$

and so $H^0(\mathbb{Q}_v,T) = 0$ by Nakayama's lemma. For (4.1.1.4) we do the same thing, using 3.1.4, for any non-exceptional arithmetic point.

(4.1.5) The exact sequence (4.1.3.2) allows us to compare specializations of Λ-adic cohomology groups (the left hand term) with cohomology groups of the specializations (the middle term). The right hand term is an error term which we handle using the following simple lemma:

LEMMA. *Let M be a finitely generated Λ-module. For λ not in the support of M, the groups $M[\lambda]$ are finite of order bounded independently of λ.*

Proof. Without loss of generality we may take M to be Λ-torsion. By the structure theory of finitely generated Λ-modules, M sits in an exact sequence of the form

$$0 \longrightarrow A \longrightarrow M \longrightarrow \bigoplus_{i=1}^{r} \frac{\Lambda}{\mathcal{P}_i^{n_i}} \longrightarrow B \longrightarrow 0,$$

where A and B are finite and the $\mathcal{P}_i$ are the height one primes in the support of M. So there is an exact sequence

$$0 \longrightarrow A[\lambda] \longrightarrow M[\lambda] \longrightarrow \bigoplus_{i=1}^{r} \frac{\Lambda}{\mathcal{P}_i^{n_i}}[\lambda].$$

For λ not in the support of M, the last term of this sequence is zero, and so $M[\lambda]$ is finite, of order bounded by the order of A.

(4.1.6) For $v \in S_f$ and $M = T, T^+$ or T^-, the Λ-rank of $H^n(\mathbb{Q}_v,M)$ is equal to the $\mathcal{O}_\lambda$-rank of $H^n(\mathbb{Q}_v,M_\lambda)$, for any λ not in the support of $\mathrm{Tors}_\Lambda H^n(\mathbb{Q}_v,M)$ or $\mathrm{Tors}_\Lambda H^{n+1}(\mathbb{Q}_v,M)$ (this is immediate from (4.1.3.2)). So the $\mathcal{O}_\lambda$-ranks of the $H^n(\mathbb{Q}_v,M_\lambda)$ are constant and equal to this "generic"rank outside of this explicit bad set (which depends on v). Staying away from this bad set, we obtain Λ-adic Euler

characteristic formulas:

$$\sum_{n=0}^{2}(-1)^n \mathrm{rk}_\Lambda H^n(\mathbb{Q}_v, M) = \begin{cases} 0 & v \neq p \\ -\mathrm{rk}_\Lambda(M) & v = p. \end{cases}$$

Using (4.1.1.2–4) we deduce the following:

$$\begin{aligned} v \in S_f, v \neq p: \quad & H^0(\mathbb{Q}_v, T) = 0 \quad \mathrm{rk}_\Lambda H^1(\mathbb{Q}_v, T) = 0 \quad \mathrm{rk}_\Lambda H^2(\mathbb{Q}_v, T) = 0 \\ v = p: \quad & H^0(\mathbb{Q}_p, T) = 0 \quad \mathrm{rk}_\Lambda H^1(\mathbb{Q}_p, T) = 2 \quad \mathrm{rk}_\Lambda H^2(\mathbb{Q}_p, T) = 0 \\ & H^0(\mathbb{Q}_p, T^+) = 0 \quad \mathrm{rk}_\Lambda H^1(\mathbb{Q}_p, T^+) = 1 \quad \mathrm{rk}_\Lambda H^2(\mathbb{Q}_p, T^+) = 0 \\ & H^0(\mathbb{Q}_p, T^-) = 0 \quad \mathrm{rk}_\Lambda H^1(\mathbb{Q}_p, T^-) = 1 \quad \mathrm{rk}_\Lambda H^2(\mathbb{Q}_p, T^-) = 0 \end{aligned}$$

(4.1.7) Write X_{bad} for the finite set of $(\lambda) \in X$ in the support of $\mathrm{Tors}_\Lambda H^1(\mathbb{Q}_p, T^+)$, $\mathrm{Tors}_\Lambda H^1(\mathbb{Q}_p, T^-)$, or $H^1(\mathbb{Q}_v, T)$ for some $v \in S_f, v \neq p$, and let $X_{\mathrm{good}} = X - X_{\mathrm{bad}}$. For any $(\lambda) \in X_{\mathrm{good}}$ we have $H^0(\mathbb{Q}_v, T_\lambda) = 0$ for $v \in S_f, v \neq p$, and $H^0(\mathbb{Q}_p, T_\lambda^\pm) = 0$. Euler characteristic calculations then show that the $\mathcal{O}_\lambda$-ranks of the $H^i(\mathbb{Q}_v, M_\lambda)$, $i = 0, 1, 2$, $M = T, T^\pm$, are equal to the "generic" Λ-adic ranks of the $H^i(\mathbb{Q}_v, M)$ in 4.1.6. Combining this with (4.1.3.2), it follows that X_{bad} already contains those λ in the support of $\mathrm{Tors}_\Lambda H^n(\mathbb{Q}_v, M)$, for all $v \in S_f$, $n = 0, 1, 2$, and $M = T, T^+, T^-$.

(4.1.8) Local conditions

For a local ring R and a finitely generated R-module M and an R-submodule $N \subseteq M$, we define the R-saturation of N in M to be the set of $m \in M$ such that $rm \in N$ for some non zero-divisor $r \in R$ (when $R = \mathcal{O}_\lambda$, the $\mathcal{O}_\lambda$-saturation is equal to the $\mathbb{Z}_p$-saturation, because $\mathcal{O}_\lambda$ is finite over $\mathbb{Z}_p$).

For each prime $v \in S_f$, we define a Λ-submodule $H^1_f(\mathbb{Q}_v, T) \subseteq H^1(\mathbb{Q}_v, T)$ as follows.

For $v \in S_f$, $v \neq p$: define $H^1_f(\mathbb{Q}_v, T) = H^1(\mathbb{Q}_v, T)$.

For $v = p$: define

$$H^1_f(\mathbb{Q}_p, T)^0 = \mathrm{Ker}\left[H^1(\mathbb{Q}_p, T) \to H^1(I_p, T^-)\right],$$

and define $H^1_f(\mathbb{Q}_p, T)$ to be the Λ-saturation of $H^1_f(\mathbb{Q}_p, T)^0$ in $H^1(\mathbb{Q}_p, T)$. Condition (4.1.1.4) for T^- implies that

$$\mathrm{Ker}\left[H^1(\mathbb{Q}_p, T^-) \to H^1(I_p, T^-)\right]$$

is Λ-torsion, hence $H^1_f(\mathbb{Q}_p, T)$ is also the Λ-saturation of

$$\mathrm{Ker}\left[H^1(\mathbb{Q}_p, T) \to H^1(\mathbb{Q}_p, T^-)\right]$$

in $H^1(\mathbb{Q}_p, T)$. The Λ-rank of $H^1_f(\mathbb{Q}_p, T)$ is one.

We use the same local conditions to define $\mathcal{O}_\lambda$-submodules $H^1_f(\mathbb{Q}_v, T_\lambda) \subseteq H^1(\mathbb{Q}_v, T_\lambda)$ for the specializations at any $(\lambda) \in X_{\mathrm{good}}$. For $v \in S_f$, $v \neq p$: define $H^1_f(\mathbb{Q}_v, T_\lambda) = H^1(\mathbb{Q}_v, T_\lambda)$.

For $v = p$: define

$$H^1_f(\mathbb{Q}_p, T_\lambda)^0 = \mathrm{Ker}\left[H^1(\mathbb{Q}_p, T_\lambda) \to H^1(I_p, T_\lambda^-)\right],$$

and define $H^1_f(\mathbb{Q}_p, T_\lambda)$ to be the $\mathcal{O}_\lambda$-saturation of $H^1_f(\mathbb{Q}_p, T_\lambda)^0$ in $H^1(\mathbb{Q}_p, T_\lambda)$. As in the Λ-adic case, $H^1_f(\mathbb{Q}_p, T_\lambda)$ is also equal to the $\mathcal{O}_\lambda$-saturation of

$$\mathrm{Ker}\left[H^1(\mathbb{Q}_p, T_\lambda) \to H^1(\mathbb{Q}_p, T_\lambda^-)\right]$$

in $H^1(\mathbb{Q}_p, T_\lambda)$ and $H^1_f(\mathbb{Q}_p, T)$ has $\mathcal{O}_\lambda$-rank one.

(4.1.9) LEMMA. *For $(\lambda) \in X_{\mathrm{good}}$, $v \in S_f$, specialization gives a homomorphism*

$$\frac{H^1(\mathbb{Q}_v, T)}{\lambda H^1(\mathbb{Q}_v, T)} \longrightarrow H^1(\mathbb{Q}_v, T_\lambda)$$

which is injective, with cokernel that is finite and bounded independently of λ.

Proof. This follows from (4.1.3.2) and Lemma 4.1.5, if we take λ not in the support of $H^2(\mathbb{Q}_v, T)$. However, for $(\lambda) \in X_{\mathrm{good}}$, both sides have $\mathcal{O}_\lambda$-rank two (resp. zero) for $v = p$ (resp. $v \neq p$), and so $H^2(\mathbb{Q}_v, T)[\lambda]$ is finite. So the support of $H^2(\mathbb{Q}_v, T)$ is already included in X_{bad}.

(4.1.10) We now need the analogues of Lemma 4.1.9, both for the subgroups $H^1_f(\mathbb{Q}_p, T)$ and for the quotient groups $H^1(\mathbb{Q}_p, T)/H^1_f(\mathbb{Q}_p, T)$.

LEMMA. *For $(\lambda) \in X_{\mathrm{good}}$, the image of $H^1_f(\mathbb{Q}_p, T)$ in $H^1(\mathbb{Q}_p, T_\lambda)$ lies in $H^1_f(\mathbb{Q}_p, T_\lambda)$.*

Proof. It is clear from the definition that the image of $H^1_f(\mathbb{Q}_p, T)^0$ lies in $H^1_f(\mathbb{Q}_p, T_\lambda)^0$. If $(\lambda) \in X_{\mathrm{good}}$, then the image of $H^1_f(\mathbb{Q}_p, T)$ contains a subgroup of finite index in $H^1_f(\mathbb{Q}_p, T_\lambda)^0$ and has the same $\mathcal{O}_\lambda$-rank. So it is contained in the $\mathcal{O}_\lambda$-saturation of $H^1_f(\mathbb{Q}_p, T_\lambda)^0$ in $H^1(\mathbb{Q}_p, T_\lambda)$, which is $H^1_f(\mathbb{Q}_p, T_\lambda)$.

(4.1.11) The kernel of the map $H^1_f(\mathbb{Q}_p, T) \to H^1_f(\mathbb{Q}_p, T_\lambda)$ is $H^1_f(\mathbb{Q}_p, T) \cap \lambda H^1(\mathbb{Q}_p, T) = \lambda H^1_f(\mathbb{Q}_p, T)$, so specialization gives an injection

$$\frac{H^1_f(\mathbb{Q}_p, T)}{\lambda H^1_f(\mathbb{Q}_p, T)} \hookrightarrow H^1_f(\mathbb{Q}_p, T_\lambda).$$

Write Y for $H^1(\mathbb{Q}_p, T)/H^1_f(\mathbb{Q}_p, T)$. So Y has Λ-rank one, for $(\lambda) \in X_{\mathrm{good}}$. Because $H^1_f(\mathbb{Q}_p, T)$ is Λ-saturated in $H^1(\mathbb{Q}_p, T)$, Y is Λ-torsion free, and so we have a short exact sequence

$$0 \longrightarrow \frac{H^1_f(\mathbb{Q}_p, T)}{\lambda H^1_f(\mathbb{Q}_p, T)} \longrightarrow \frac{H^1(\mathbb{Q}_p, T)}{\lambda H^1(\mathbb{Q}_p, T)} \longrightarrow \frac{Y}{\lambda Y} \longrightarrow 0.$$

The index of $H^1_f(\mathbb{Q}_p, T)/\lambda H^1_f(\mathbb{Q}_p, T)$ in its $\mathcal{O}_\lambda$-saturation in $H^1(\mathbb{Q}_p, T)/\lambda H^1(\mathbb{Q}_p, T)$ is equal to the order of the maximal finite $\mathcal{O}_\lambda$-submodule of $Y/\lambda Y$. By the structure theory, Y sits in an exact sequence

$$0 \longrightarrow Y \longrightarrow \Lambda \longrightarrow B \longrightarrow 0$$

where B is finite, so the order of this finite submodule is the order of $B[\lambda]$, which is bounded independently of λ. Let Z be the inverse image of $H^1_f(\mathbb{Q}_p, T_\lambda)$ in $H^1(\mathbb{Q}_p, T)/\lambda H^1(\mathbb{Q}_p, T)$ under the inclusion

$$\frac{H^1(\mathbb{Q}_p, T)}{\lambda H^1(\mathbb{Q}_p, T)} \hookrightarrow H^1(\mathbb{Q}_p, T_\lambda).$$

So Z is equal to the $\mathcal{O}_\lambda$-saturation of $H^1_f(\mathbb{Q}_p,T)/\lambda H^1_f(\mathbb{Q}_p,T)$ in $H^1(\mathbb{Q}_p,T)/\lambda H^1(\mathbb{Q}_p,T)$. By the above, the index of $H^1_f(\mathbb{Q}_p,T)/\lambda H^1_f(\mathbb{Q}_p,T)$ in Z is finite and bounded for $\lambda \in X_{\text{good}}$. This implies the following lemma.

(4.1.12) LEMMA. *For $(\lambda) \in X_{\text{good}}$, the specialization map*

$$\frac{H^1(\mathbb{Q}_p,T)/H^1_f(\mathbb{Q}_p,T)}{\lambda\left(H^1(\mathbb{Q}_p,T)/H^1_f(\mathbb{Q}_p,T)\right)} \longrightarrow \frac{H^1(\mathbb{Q}_p,T_\lambda)}{H^1_f(\mathbb{Q}_p,T_\lambda)}$$

is injective, with cokernel that is finite and bounded independently of λ.

(4.1.13) LEMMA. *For $(\lambda) \in X_{\text{good}}$, the specialization map*

$$\frac{H^1_f(\mathbb{Q}_p,T)}{\lambda H^1_f(\mathbb{Q}_p,T)} \longrightarrow H^1_f(\mathbb{Q}_p,T_\lambda)$$

is injective, with cokernel that is finite and bounded independently of λ.

Proof. We already know that it is injective. We have a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \frac{H^1_f(T)}{\lambda H^1_f(T)} & \longrightarrow & \frac{H^1(T)}{\lambda H^1(T)} & \longrightarrow & \frac{H^1(T)/H^1_f(T)}{\lambda H^1(T)/H^1_f(T)} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & H^1_f(T_\lambda) & \longrightarrow & H^1(T_\lambda) & \longrightarrow & H^1(T_\lambda)/H^1_f(T_\lambda) & \longrightarrow & 0 \end{array}$$

(dropping $\mathbb{Q}_p$ from the notation). By Lemmas 4.1.9 and 4.1.12, the kernels and cokernels of the vertical arrows are all finite and bounded for $(\lambda) \in X_{\text{good}}$, except possibly the cokernel of the first vertical arrow. This now follows from the snake lemma.

(4.1.14) Discrete modules

Write $\widehat{M} := \text{Hom}_{\text{cont}}(M, \mathbb{Q}_p/\mathbb{Z}_p)$ for the Pontryagin dual of a Λ-module M. We define a discrete dual A of T by $A = \text{Hom}_{\text{cont}}(T, \mathbb{Q}_p/\mathbb{Z}_p(1))$. Since T is a free Λ-module, we have a canonical isomorphism $A \xrightarrow{\sim} T^*(1) \otimes_\Lambda \widehat{\Lambda}$. Since $T \xrightarrow{\sim} T^*(1)$, this is also isomorphic to $T \otimes_\Lambda \widehat{\Lambda}$ (so there is no discrepancy with the notation of 3.5.3). A is a (discrete) Λ-module with Λ-action $(\lambda\phi)(t) := \phi(\lambda t)$ for $\phi \in A, t \in T$. We have a perfect pairing

$$A \times T \to \mathbb{Q}_p/\mathbb{Z}_p(1)$$

which induces perfect pairings (Tate local duality) for any $v \in S_f$

$$H^i(\mathbb{Q}_v, A) \times H^{2-i}(\mathbb{Q}_v, T) \to \mathbb{Q}_p/\mathbb{Z}_p$$

for $i = 0, 1, 2$.

For the specializations at $(\lambda) \in X_{\text{good}}$, we define $A_\lambda = \text{Hom}(T_\lambda, \mathbb{Q}_p/\mathbb{Z}_p(1))$. As in the Λ-adic case, because T_λ is a free $\mathcal{O}_\lambda$-module, A_λ is canonically isomorphic to $T^*_\lambda(1) \otimes_{\mathcal{O}_\lambda} \widehat{\mathcal{O}}_\lambda$, where $T^*_\lambda := \text{Hom}_{\mathcal{O}_\lambda}(T_\lambda, \mathcal{O}_\lambda)$ (and also to $T_\lambda \otimes_{\mathcal{O}_\lambda} \widehat{\mathcal{O}}_\lambda$ via $T^*_\lambda(1) \xrightarrow{\sim} T_\lambda$). Note that $\mathcal{O}_\lambda$, being a complete intersection, is a Gorenstein ring. Fixing a generator for $\text{Hom}_{\mathbb{Z}_p}(\mathcal{O}_\lambda, \mathbb{Z}_p)$ as a free rank one $\mathcal{O}_\lambda$-module gives an isomorphism

$$\widehat{\mathcal{O}}_\lambda = \text{Hom}_{\mathbb{Z}_p}(\mathcal{O}_\lambda, \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{\sim} \mathcal{O}_\lambda \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{\sim} F_{\mathfrak{p},\lambda}/\mathcal{O}_\lambda,$$

where $F_{\mathfrak{p},\lambda} = \mathcal{O}_\lambda \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is the fraction field of $\mathcal{O}_\lambda$. So we also have

$$A_\lambda \xrightarrow{\sim} T^*_\lambda(1) \otimes_{\mathcal{O}_\lambda} F_{\mathfrak{p},\lambda}/\mathcal{O}_\lambda$$

(in the case where $\mathcal{O}_\lambda$ is the ring of integers of $F_{\mathfrak{p},\lambda}$, this would have been called $A^*(1)_{[\mathcal{P}]}$ in 3.5.3). We can also canonically identify A_λ with $A[\lambda]$. With this identification, we have an exact sequence

$$0 \longrightarrow A_\lambda \longrightarrow A \xrightarrow{\lambda} A \longrightarrow 0. \tag{4.1.14.1}$$

Local duality gives a perfect pairing

$$H^i(\mathbb{Q}_v, A_\lambda) \times H^{2-i}(\mathbb{Q}_v, T_\lambda) \to \mathbb{Q}_p/\mathbb{Z}_p \tag{4.1.14.2}$$

for $i = 0, 1, 2$.

(4.1.15) Local conditions for discrete modules

For any $v \in S_f$, we define $H^1_f(\mathbb{Q}_v, A)$ to be the orthogonal complement to $H^1_f(\mathbb{Q}_v, T)$ under the pairing (4.1.14.2), for $i = 1$. In particular, for $v \neq p$, we get $H^1_f(\mathbb{Q}_v, A) = 0$.

Similarly for the specializations at $(\lambda) \in X_{\text{good}}$, we define $H^1_f(\mathbb{Q}_v, A_\lambda)$ to be the orthogonal complement to $H^1_f(\mathbb{Q}_v, T_\lambda)$. For $v \neq p$, $H^1_f(\mathbb{Q}_v, A_\lambda) = 0$.

(4.1.16) LEMMA. *Let $G = G_{\mathbb{Q},S}$ or $G_{\mathbb{Q}_v}$ for $v \in S_f$. For $(\lambda) \in X_{\text{good}}$, the natural map*

$$H^1(G, A_\lambda) \to H^1(G, A)[\lambda] \tag{4.1.16.1}$$

is surjective with kernel that is finite and bounded independently of λ.

Proof. Taking cohomology of (4.1.14.1) as G-modules gives an exact sequence

$$H^0(G, A) \xrightarrow{\lambda} H^0(G, A) \longrightarrow H^1(G, A_\lambda) \longrightarrow H^1(\mathbb{Q}_v, A)[\lambda] \longrightarrow 0. \tag{4.1.16.1}$$

The lemma follows, for λ not in the support of $H^0(G, A)\widehat{\ }$. For $G = G_{\mathbb{Q}_v}$, this module is equal to $H^2(\mathbb{Q}_v, T)$ whose support is already included in X_{bad} by Lemma 4.1.9 (alternatively for $\mathbb{Q}_v$, the lemma follows immediately from Lemma 4.1.9 and local duality). For $G = G_{\mathbb{Q},S}$, λ is in the support of $H^0(G, A)\widehat{\ }$ iff $H^0(G, A)[\lambda]$ is infinite which is true iff $H^0(G, A_\lambda)$ is infinite, which again implies that λ is already included in X_{bad}.

(4.1.17) LEMMA. *For $v \in S_f, (\lambda) \in X_{\text{good}}$, the image of $H^1_f(\mathbb{Q}_v, A_\lambda)$ in $H^1(\mathbb{Q}_v, A)[\lambda]$ lies in $H^1_f(\mathbb{Q}_v, A)[\lambda]$. The map*

$$H^1_f(\mathbb{Q}_v, A_\lambda) \to H^1_f(\mathbb{Q}_v, A)[\lambda]$$

has kernel and cokernel that are finite and bounded independently of λ.

Proof. For $v \neq p$, both $H^1_f(\mathbb{Q}_v, A_\lambda)$ and $H^1_f(\mathbb{Q}_v, A)$ are zero, so the result is trivial. For $v = p$, this is the dual of Lemma 4.1.12 (using Lemma 4.1.13).

(4.1.18) Selmer groups

We define the Selmer group $\mathbb{S} \subseteq H^1(G_{\mathbb{Q},S}, A)$ by

$$\mathbb{S} = \operatorname{Ker}\left[H^1(G_{\mathbb{Q},S}, A) \to \bigoplus_{v \in S} \frac{H^1(\mathbb{Q}_v, A)}{H^1_f(\mathbb{Q}_v, A)}\right].$$

Similarly for the specializations, define

$$\mathbb{S}_\lambda = \operatorname{Ker}\left[H^1(G_{\mathbb{Q},S}, A_\lambda) \to \bigoplus_{v \in S} \frac{H^1(\mathbb{Q}_v, A_\lambda)}{H^1_f(\mathbb{Q}_v, A_\lambda)}\right].$$

(4.1.19) LEMMA. *For $(\lambda) \in X_{\text{good}}$, the image of $\mathbb{S}_\lambda$ in $H^1(G_{\mathbb{Q},S}, A)[\lambda]$ under the map* (4.1.16.1) *lies in $\mathbb{S}$, and the map*

$$\mathbb{S}_\lambda \longrightarrow \mathbb{S}[\lambda] \tag{4.1.19.1}$$

has kernel and cokernel that are finite and bounded independently of λ.

Proof. Apply the snake lemma to the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathbb{S}_\lambda & \longrightarrow & H^1(G_{\mathbb{Q},S}, A_\lambda) & \longrightarrow & \bigoplus_{v\in S} H^1(\mathbb{Q}_v, A_\lambda)/H^1_f(\mathbb{Q}_v, A_\lambda) \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \mathbb{S}[\lambda] & \longrightarrow & H^1(G_{\mathbb{Q},S}, A)[\lambda] & \longrightarrow & \bigoplus_{v\in S} H^1(\mathbb{Q}_v, A)/H^1_f(\mathbb{Q}_v, A)[\lambda]. \end{array}$$

We just need to know that the kernel of the maps

$$\frac{H^1(\mathbb{Q}_v, A_\lambda)}{H^1_f(\mathbb{Q}_v, A_\lambda)} \longrightarrow \frac{H^1(\mathbb{Q}_v, A)}{H^1_f(\mathbb{Q}_v, A)}[\lambda]$$

are finite and bounded, and this follows from dualizing Lemma 4.1.13.

(4.1.20) Tate-Šafarevič groups

An $\mathcal{O}_\lambda$-module M is called π-divisible if $\pi M = M$. A Λ-module M is said to be $\mathfrak{m}$-divisible if $\mathfrak{m}M = M$. A co-finitely generated Λ-module M is $\mathfrak{m}$-divisible if and only if $\mathrm{Hom}(M, \mathbb{Q}_p/\mathbb{Z}_p)$ is Λ-torsion free.

For any specialization $\mathbb{S}_\lambda$, we define a Tate-Šafarevič group by $Ш_\lambda = \mathbb{S}_\lambda/\mathrm{div}(\mathbb{S}_\lambda)$, where $\mathrm{div}(\mathbb{S}_\lambda)$ is the maximal π-divisible submodule of $\mathbb{S}_\lambda$. So $Ш_\lambda$ is finite and $\widehat{Ш}_\lambda$ is the torsion subgroup of $\widehat{\mathbb{S}}_\lambda$. By analogy, for $\mathbb{S}$ itself, we define $Ш = \mathbb{S}/\mathfrak{m}\text{-div}(\mathbb{S})$, where $\mathfrak{m}$-div$(\mathbb{S})$ is the maximal $\mathfrak{m}$-divisible submodule of $\mathbb{S}$. Equivalently, $\widehat{Ш} = \mathrm{Tors}_\Lambda \widehat{\mathbb{S}}$ is the maximal Λ-torsion submodule of $\widehat{\mathbb{S}}$.

Dualizing (4.1.19) gives a map $\widehat{\mathbb{S}}/\lambda\widehat{\mathbb{S}} \longrightarrow \widehat{\mathbb{S}}_\lambda$ which restricts to a map

$$\widehat{Ш}/\lambda\widehat{Ш} \longrightarrow \widehat{Ш}_\lambda. \tag{4.1.20.1}$$

(4.1.21) LEMMA. *The map (4.1.20.1) has kernel and cokernel which are finite and bounded independently of λ, for $(\lambda) \in X'_{\text{good}}$, where we define $X'_{\text{bad}} = X_{\text{bad}} \cup \{\lambda \in \mathrm{Supp}(\mathrm{Tors}_\Lambda \widehat{\mathbb{S}})\}$ and $X'_{\text{good}} = X - X'_{\text{bad}}$.*

Proof. If M is any finitely generated Λ module, then, for λ not in the support of $\mathrm{Tors}_\Lambda M$, the map $\mathrm{Tors}_\Lambda M/\lambda \mathrm{Tors}_\Lambda M \to \mathrm{Tors}_{\mathbb{Z}_p}(M/\lambda M)$ has kernel and cokernel that are finite and bounded independently of λ. Combining this fact with Corollary 4.1.19 proves the lemma.

(4.1.22) We shall now study the structure of $\widehat{\mathbb{S}}$ via its specializations. We fix an irreducible distinguished polynomial λ and write $\lambda_k = \lambda + \pi^k$. For k sufficiently large, λ_k is also an irreducible distinguished polynomial. Also, for k sufficiently large, λ_k is not in any finite bad set that we might need to avoid and, in particular, is not in X'_{bad}. We shall write T_k for T_{λ_k}, A_k for A_{λ_k}, $\mathbb{S}_k$ for $\mathbb{S}_{\lambda_k}$, and $Ш_k$ for $Ш_{\lambda_k}$.

By the structure theory of finitely generated Λ-modules, $\widehat{Ш} = \mathrm{Tors}_\Lambda \widehat{\mathbb{S}}$ sits in an exact sequence

$$0 \longrightarrow A \longrightarrow \bigoplus_{i=1}^{r} \frac{\Lambda}{\mathcal{P}_i^{n_i}} \longrightarrow \widehat{Ш} \longrightarrow B \longrightarrow 0, \tag{4.1.22.1}$$

where A and B are finite. Decompose the second term in this sequence as

$$\bigoplus_{i=1}^{r} \frac{\Lambda}{\mathcal{P}_i^{n_i}} = M \oplus \overline{M}$$

where M consists of those direct summands with $\mathcal{P}_i = (\lambda)$ for our fixed λ, and consider the composite map

$$\frac{M}{\lambda_k M} \longrightarrow \frac{\widehat{Ш}}{\lambda \widehat{Ш}} \longrightarrow \frac{\widehat{\mathbb{S}}}{\lambda_k \widehat{\mathbb{S}}} \longrightarrow \widehat{\mathbb{S}}_k.$$

For k sufficiently large, λ_k is not in the support of $\mathrm{Tors}_\Lambda \widehat{\mathbb{S}}$ and so the image of this composite map is finite and therefore lies in $\widehat{Ш}_k$. Lemma 4.1.21 now implies the following lemma.

(4.1.23) LEMMA. *For k sufficiently large, the map*

$$\frac{M}{\lambda_k M} \longrightarrow \widehat{Ш}_k$$

has kernel and cokernel that are finite of order bounded independently of k.

Remark. We do not need to assume that λ itself is not in X'_{bad}, so there is no restriction on λ, since we study T_λ via the specializations at $\lambda + \pi^k$, which are not in X'_{bad} for k sufficiently large.

(4.2) Alternating pairings

Recall the following classical result.

PROPOSITION. *Suppose A is a finite abelian group equipped with a non-degenerate alternating pairing*

$$\langle\ ,\ \rangle : A \times A \longrightarrow \mathbb{Q}/\mathbb{Z}.$$

Then there is a group B such that $A \xrightarrow{\sim} B \oplus B$.

Applying this proposition when $\langle\ ,\ \rangle$ is the Cassels pairing allows one to deduce that the order of the Tate-Šafarevič group of an elliptic curve divided by its maximal divisible subgroup is a square. In what follows, we shall consider certain Tate-Šafarevič groups as Λ-modules rather than just $\mathbb{Z}$-modules, and so we shall now prove a version of this result in the context of $\Lambda/(g)$-modules, where $g \in \Lambda$ is an irreducible distinguished polynomial.

(4.2.1) Fix an irreducible distinguished polynomial $f \in \Lambda$, and a Λ-module

$$M = \left(\frac{\Lambda}{(f^{n_1})}\right)^{\alpha_1} \oplus \cdots \oplus \left(\frac{\Lambda}{(f^{n_r})}\right)^{\alpha_r} \qquad \text{with} \qquad n_1 > \cdots > n_r.$$

For k sufficiently large, $f + \pi^k$ is also an irreducible distinguished polynomial. Let $M_k = M/(f + \pi^k)$. So M_k is a finite $\mathcal{O}_k$-module, where $\mathcal{O}_k = \Lambda/(f + \pi^k)$.

(4.2.2) THEOREM. *Suppose we have a non-degenerate alternating pairing*

$$\langle\ ,\ \rangle : M_k \times M_k \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p$$

satisfying $\langle rx, y\rangle = \langle x, ry\rangle$ for all r in $\mathcal{O}_k$ and all x and y in M_k. Then the α_i are all even.

Note that we only need the existence of $\langle\ ,\ \rangle$ for any one fixed k to deduce the result for M, and non-degenerate just means that the left and right kernels are both

zero. Also, the condition $\langle rx, y\rangle = \langle x, ry\rangle$ means that the isomorphism of abelian groups

$$M_k \xrightarrow{\sim} \mathrm{Hom}(M_k, \mathbb{Q}_p/\mathbb{Z}_p)$$
$$x \longmapsto \langle x, \ . \ \rangle$$

is an isomorphism of $\mathcal{O}_k$-modules, where here the $\mathcal{O}_k$-module structure on $\mathrm{Hom}(M_k, \mathbb{Q}_p/\mathbb{Z}_p)$ is given by defining $(r\phi)(x) = \phi(rx)$.

(4.2.3) The proof of Theorem 4.2.2 consists of a series of reduction steps. Write $L_n = \Lambda/(f^n, f + \pi^k)$ (recall that k is fixed throughout). So we have

$$M_k \xrightarrow{\sim} (L_{n_1})^{\alpha_1} \oplus (L_{n_2})^{\alpha_2} \oplus \cdots \oplus (L_{n_r})^{\alpha_r} = A \oplus B$$

where $A = (L_{n_1})^{\alpha_1}$ and $B = (L_{n_2})^{\alpha_2} \oplus \cdots \oplus (L_{n_r})^{\alpha_r}$. We have $f = -\pi^k$ in $\mathcal{O}_k$, so $L_n \cong \mathcal{O}_k/(f^n) \cong \mathcal{O}_k/(\pi^{nk})$.

(4.2.4) LEMMA. *$\langle \ , \ \rangle|_A$ is non-degenerate.*

Proof. Suppose $a \in A$ is such that $\pi^k a = 0$. Then $\langle a, b\rangle = 0$ for all $b \in B$. To see this, notice that we can find $a' \in A$ such that $a = \pi^{(n_1-1)k}a'$ (this is easy to check). So

$$\langle a, b\rangle = \langle \pi^{(n_1-1)k}a', b\rangle = \langle a', \pi^{(n_1-1)k}b\rangle = \langle a', 0\rangle = 0.$$

Now suppose that $a \in A$ is non-zero and such that $\langle a, x\rangle = 0$ for all $x \in A$. Multiplying a by some power of π we may assume that $\pi a = 0$ but $a \neq 0$. So

$$\langle a, x\rangle = 0 \qquad \text{for all } x \in A$$
$$\text{and} \qquad \langle a, b\rangle = 0 \qquad \text{for all } b \in B \ \ (\text{since } \pi^k a = 0).$$

So $\langle a, m\rangle = 0$ for all $m \in M_k$, giving a contradiction.

(4.2.5) Lemma 4.2.4 tells us that

$$\langle \ , \ \rangle : A \times A \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p$$

is non-degenerate, and so gives an isomorphism

$$A \xrightarrow{\sim} \mathrm{Hom}(A, \mathbb{Q}_p/\mathbb{Z}_p)$$
$$a \longmapsto \langle a, \ . \ \rangle$$

of $\mathcal{O}_k$-modules. In particular, any map $A \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p$ can be written as $\langle a, \ . \ \rangle$ for some $a \in A$.

(4.2.6) LEMMA. *$\langle \ , \ \rangle|_B$ is non-degenerate.*

Proof. Suppose $b \in B$ is non-zero and such that $\langle b, y\rangle = 0$, for all $y \in B$. Multiplying by a power of π if necessary, we may assume that $b \neq 0$ but $\pi b = 0$. Now consider the map

$$A \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p$$
$$a \longmapsto \langle b, a\rangle$$

By Lemma 4.2.4, there is some $\alpha \in A$ such that this map is given by $\langle \alpha, \ . \ \rangle$, i.e. such that $\langle b, a\rangle = \langle \alpha, a\rangle$ for all $a \in A$. Also, $\pi b = 0$. So

$$\langle \pi\alpha, a\rangle = \langle \alpha, \pi a\rangle = \langle b, \pi a\rangle = \langle \pi b, a\rangle = 0$$

for all $a \in A$. Therefore $\pi\alpha = 0$, which implies that $\langle \alpha, y\rangle = 0$ for all $y \in B$. So we have $\alpha \in A$ and $b \in B$ such that $\langle \alpha, y\rangle = 0$ for all $y \in B$, $\langle b, y\rangle = 0$ for all $y \in B$, and

$\langle \alpha, a\rangle = \langle b, a\rangle$ for all $a \in A$, So $\langle \alpha - b, m\rangle = 0$ for all $m \in M_k$. So $\alpha - b = 0$ which implies that $\alpha = b = 0$. This proves Lemma 4.2.6.

(4.2.7) Lemmas 4.2.4 and 4.2.6 allow us to reduce Theorem 4.2.2 to the case where $M_k \xrightarrow{\sim} (L_n)^\alpha$. The next step is to reduce to the case $n = 1$. For this, note that we have isomorphisms of $\mathcal{O}_k$-modules

$$L_1 \xrightarrow{\sim} \pi^{(n-1)k} L_n \qquad \text{and} \qquad L_n/\pi^k L_n \xrightarrow{\sim} L_1.$$

Also, the orthogonal complement to $\pi^{(n-1)k} M_k$ is $\pi^k M_k$, since

$$\begin{aligned} \langle \pi^{(n-1)k} x, y\rangle = 0 \text{ for all } x &\iff \langle x, \pi^{(n-1)k} y\rangle = 0 \text{ for all } x \\ &\iff \pi^{(n-1)k} y = 0 \\ &\iff \text{there exists } y' \text{ such that } y = \pi^k y' \\ &\iff y \in \pi^k M_k. \end{aligned}$$

So we get a non-degenerate pairing

$$\pi^{(n-1)k} M_k \times \frac{M_k}{\pi^k M_k} \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p.$$

So we have reduced Theorem 4.2.2 to proving the following result.

(4.2.8) LEMMA. *Let $\overline{\mathcal{O}}_k = \Lambda/(f + \pi^k, \pi^k)$. Let M be a free $\overline{\mathcal{O}}_k$-module of rank α and*

$$\langle\ ,\ \rangle : M \times M \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p$$

a non-degenerate alternating pairing satisfying $\langle rx, y\rangle = \langle x, ry\rangle$ for all r in $\overline{\mathcal{O}}_k$ and all x and y in M. Then α is even.

Proof. One can easily reduce to the case of fields where the result is well known, but we give a direct proof by induction on α. Let X be any free rank one direct summand of M and let N be any complementary direct summand. So $M = X \oplus N$. Let $N^\perp = \{x \in M : \langle n, x\rangle = 0 \text{ for all } n \in N\}$. It is easy to see that $\langle\ ,\ \rangle : X \times N^\perp \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p$ is non-degenerate. Now $N^\perp$ is a rank one direct summand of M, (in fact $M = N^\perp \oplus X^\perp$) and so $\langle\ ,\ \rangle : N^\perp \times N^\perp \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p$ is zero (since $\langle\ ,\ \rangle$ is alternating). So $N^\perp \subseteq \left(N^\perp\right)^\perp = N$. Let $L = N \cap X^\perp$. We claim that $N = N^\perp \oplus L$. To prove this, let $n \in N$ and consider the map $\langle\ .\ , n\rangle : X \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p$. There is some $y \in N^\perp$ such that this map is given by $\langle\ .\ , y\rangle$, ie such that $\langle x, n\rangle = \langle x, y\rangle$ for all $x \in X$. So $\langle x, n-y\rangle = 0$. So $n-y \in X^\perp$. So $n = (n-y)+y$ with $y \in N^\perp$ and $n-y \in X^\perp \cap N = L$. Also, if $y \in N^\perp \cap L$ then $y \in N^\perp$ and $y \in X^\perp$, so $y \in M^\perp = 0$. This proves the claim. So we have $M = X \oplus N^\perp \oplus L$. Finally, we claim that $\langle\ ,\ \rangle : L \times L \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p$ is non-degenerate. This will be enough to finish the inductive proof of the lemma since the rank of L is $\alpha - 2$. For this, suppose that $l \in L$ is such that $\langle l, z\rangle = 0$ for all $z \in L$. Consider the map $\langle l,\ .\ \rangle : N^\perp \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p$. There is some $x \in X$ such that this map is given by $\langle x,\ .\ \rangle$, i.e. such that $\langle l, w\rangle = \langle x, w\rangle$ for all $w \in N^\perp$. So $\langle l - x, w\rangle = 0$ for all $w \in N^\perp$. So $l - x \in \left(N^\perp\right)^\perp = N$. So we have $l \in L = X^\perp \cap N$, $x \in X$, and $l - x \in N$. So $x \in N \cap X = 0$. So $x = 0$. So $\langle l, w\rangle = 0$ for all $w \in N^\perp$. Also we have $l \in X^\perp$ so we have $\langle l, x\rangle = 0$ for all $x \in X$, $\langle l, z\rangle = 0$ for all $z \in L$, and $\langle l, w\rangle = 0$ for all $w \in N^\perp$. So $\langle l, m\rangle = 0$ for all $m \in M$. So $l = 0$, which proves the lemma.

(4.2.9) Theorem 4.4.2 allows us to study the structure of certain Λ-modules at height one primes which are of the form (f) for some irreducible distinguished

polynomial f. For completeness, we also need a version to treat the height one prime (π). For this case, let

$$M = \left(\frac{\Lambda}{(\pi^{n_1})}\right)^{\alpha_1} \oplus \cdots \oplus \left(\frac{\Lambda}{(\pi^{n_r})}\right)^{\alpha_r} \qquad \text{with} \qquad n_1 > \cdots > n_r.$$

Then for any k, $X^k + \pi$ is an irreducible distinguished polynomial and we let $M_k = M/(X^k + \pi)$. So M_k is an $\mathcal{O}_k$-module, where $\mathcal{O}_k = \Lambda/(X^k + \pi)$. We get the following theorem.

(4.2.10) THEOREM. *Suppose we have a non-degenerate alternating pairing*

$$\langle\ ,\ \rangle\ :\ M_k\ \times M_k \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p$$

satisfying $\langle rx, y\rangle = \langle x, ry\rangle$ *for all* r *in* $\mathcal{O}_k$ *and all* x *and* y *in* M_k. *Then the* α_i *are all even.*

The proof of this is exactly the same as the proof of Theorem 4.2.2.

(4.2.11) The modules that arise in the application to Tate-Šafarevič groups need not be of the standard form considered in 4.2.1, so we need the following generalization of Theorem 4.2.2. Rather than proving Theorem 4.2.2 for modules which are only pseudo-isomorphic to M (and non-degenerate pairings), we prove a version for M of standard form, but where the pairing is only non-degenerate up to finite groups.

(4.2.12) THEOREM. *Let* M *and* M_k *be as in 4.2.1. Suppose for each* k *sufficiently large we have an alternating pairing*

$$\langle\ ,\ \rangle_k\ :\ M_k\ \times M_k \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p$$

satisfying $\langle rx, y\rangle_k = \langle x, ry\rangle_k$ *for all* r *in* $\mathcal{O}_k$ *and all* x *and* y *in* M_k, *and such that the left and right kernels are finite and bounded independently of* k. *Then the* α_i *are all even.*

Proof. The proof is essentially the same as that of Theorem 4.2.2, but taking account of the finite bounded kernels. Let π^c kill the left and right kernels of $\langle\ ,\ \rangle_k$ for all k. We begin with the analogue of Lemma 4.2.4.

(4.2.13) LEMMA. *For all* k *sufficiently large,* π^c *kills the left and right kernels of* $\langle\ ,\ \rangle_k|_A$.

Proof. Suppose the lemma is false. Then for infinitely many k, there is $a \in A$ such that $\langle a, x\rangle_k = 0$ for all $x \in A$ but $\pi^c a \neq 0$. Multiplying by a power of π if necessary, we may assume that $\pi^c a \neq 0$ but $\pi^{c+1}a = 0$. Choosing $k \geq c+1$, we have $\pi^k a = 0$. So $\langle a, b\rangle_k = 0$ for all $b \in B$ as in Lemma 4.2.4. So $\langle a, m\rangle_k = 0$ for all $m \in M_k$. So $\pi^c a = 0$, which is a contradiction.

(4.2.14) LEMMA. *For all* k *sufficiently large,* π^{2c} *kills the left and right kernels of* $\langle\ ,\ \rangle_k|_B$.

Proof. Suppose the lemma is false. Then for infinitely many k, there is $b \in B$ with $\pi^{2c}b \neq 0, \pi^{2c+1}b = 0$ and $\langle b, y\rangle_k = 0$ for all $y \in B$. By Lemma 4.2.13, the right kernel of $\langle\ ,\ \rangle_k|_A$ lies in the kernel of the map

$$\begin{aligned} A &\longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \\ a &\longmapsto \langle b, \pi^c a\rangle \end{aligned}$$

so there is $\alpha \in A$ such that this map can be written as $\langle \alpha,\ .\ \rangle_k$, i.e. such that $\langle \alpha, a\rangle_k = \langle b, \pi^c a\rangle_k = \langle \pi^c b, a\rangle_k$ for all $a \in A$. Also, for all $a \in A$,

$$\langle \pi^{c+1}\alpha, a\rangle_k = \langle \alpha, \pi^{c+1}a\rangle_k = \langle \pi^c b, \pi^{c+1}a\rangle_k = \langle \pi^{2c+1}b, a\rangle_k = \langle 0, a\rangle = 0.$$

So $\pi^{2c+1}\alpha = 0$ by Lemma 4.2.13. Now take $k \geq 2c+1$, so $\pi^k\alpha = 0$. So $\langle \alpha, y\rangle_k = 0$ for all $y \in B$ as in Lemma 4.2.4. So $\langle \pi^c b - \alpha, m\rangle_k = 0$ for all $m \in M_k$. So $\pi^c(\pi^c b - \alpha) = 0$. So $\pi^{2c}b = \pi^c\alpha = 0$ which is a contradiction.

(4.2.15) We have now reduced Theorem 4.2.12 to the case $M_k \xrightarrow{\sim} (L_n)^\alpha$. The arguments of 4.2.7 show that, if H is the orthogonal complement of $\pi^{(n-1)k}M_k$, then $\pi^k M_k \subseteq H \subseteq \pi^{k-c}M_k$, and so we deduce a pairing

$$\pi^{(n-1)k}M_k \times \frac{M_k}{\pi^k M_k} \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p.$$

and reduce to the case $n = 1$ as before. Finally, we need the analogue of Lemma 4.2.8.

(4.2.16) LEMMA. *With notation as in Lemma 4.2.8, suppose for all k sufficiently large, we have an alternating pairing*

$$\langle\ ,\ \rangle\ :\ M\ \times M \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p$$

satisfying $\langle rx, y\rangle = \langle x, ry\rangle$ for all r in $\overline{\mathcal{O}}_k$ and all x and y in M, where $\overline{\mathcal{O}}_k$ and M are as in Lemma 4.2.8 (with α fixed) and such that the left and right kernels of $\langle\ ,\ \rangle$ are killed by p^c for some c independent of k. Then α is even.

Proof. We rewrite the proof of Lemma 4.2.8, keeping track track of the small kernels involved. Briefly; since $\langle\ ,\ \rangle$ is alternating, the left and right kernels are equal, call them K. Also, write K_1 for the left kernel of

$$\langle\ ,\ \rangle\ :\ X\ \times N^\perp \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p.$$

Then $\#K_1 \leq \#K$. Write $M = X \oplus N$ as in Lemma 4.2.8. Then $M = X^\perp + N^\perp$ and $X^\perp \cap N^\perp = K$. Define $L = (N+K_1)\cap X^\perp$. Then one can show that $L + N^\perp \subseteq N + K_1$ with index independent of k (explicitly, the index is $\leq \#K \cdot p^{c\alpha}$). So we can choose a $(N^\perp)' \supset N^\perp$ with index $\leq \#K \cdot p^{c\alpha}$ such that $L + (N^\perp)' \supset N + K_1$ and so $M = X + L + (N^\perp)'$. Now one can choose direct summands $A \subseteq L$ and $B \subseteq (N^\perp)'$ of rank $\alpha - 2$ and 1 respectively, such that $M = X \oplus A \oplus B$, and such that the index of A in L and B in $(N^\perp)'$ are independent of k. Finally one checks that

$$\langle\ ,\ \rangle\ :\ A\ \times A \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p.$$

has left and right kernels which are killed by $p^{c'}$ for some new c' (defined in terms of c and α, but independent of k). This completes the proof.

(4.2.17) One can use variants of Lemmas 4.2.13–16 to treat the case of the height one prime (π) of Λ, so that Theorem 4.2.12 holds in this case too (with $M_k = M/(X^k + \pi)$ as in 4.2.9). In this case, suppose the left and right kernels of $\langle\ ,\ \rangle_k$ are finite and bounded independently of k; then there is some constant c such that X^c kills these kernels, independently of k. Now proceed using this X^c in place of the p^c in Lemmas 4.2.13–16. The proofs are essentially the same.

(4.3) Cassels-Tate pairings

(4.3.1) From now on, let $p > 2$. Returning to the situation of Section 4.1.1, if λ is any irreducible distinguished polynomial, then the specialization T_λ is a free rank two $\mathcal{O}_\lambda$-module and there is an $\mathcal{O}_\lambda$-bilinear skew-symmetric pairing

$$T_\lambda \times T_\lambda \longrightarrow \mathcal{O}_\lambda(1) \tag{4.3.1.1}$$

coming from specializing (4.1.1.2), giving an isomorphism $T_\lambda \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{O}_\lambda}(T_\lambda, \mathcal{O}_\lambda)(1)$.

(4.3.2) We will work with pairings taking values in $\mathbb{Z}_p$ rather than $\mathcal{O}_\lambda$, and so we recall how to switch between the two. Recall that any $\mathcal{O}_\lambda$ is Gorenstein and that $\mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{O}_\lambda, \mathbb{Z}_p)$ is free of rank one as an $\mathcal{O}_\lambda$-module. Now we have a canonical isomorphism

$$\begin{aligned} \mathrm{Hom}_{\mathcal{O}_\lambda}(T_\lambda, \mathcal{O}_\lambda) \otimes_{\mathcal{O}_\lambda} \mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{O}_\lambda, \mathbb{Z}_p) &\xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}_p}(T_\lambda, \mathbb{Z}_p)\,. \\ \theta \otimes \phi \qquad\qquad &\mapsto \quad \phi \circ \theta \end{aligned}$$

If we fix a generator for $\mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{O}_\lambda, \mathbb{Z}_p)$, this gives an isomorphism

$$\mathrm{Hom}_{\mathcal{O}_\lambda}(T_\lambda, \mathcal{O}_\lambda) \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}_p}(T_\lambda, \mathbb{Z}_p)$$

and so the isomorphism $T_\lambda \tilde{\to} \mathrm{Hom}_{\mathcal{O}_\lambda}(T_\lambda, \mathcal{O}_\lambda)(1)$ translates to an isomorphism $T_\lambda \tilde{\to} \mathrm{Hom}_{\mathbb{Z}_p}(T_\lambda, \mathbb{Z}_p)(1)$, i.e. gives a pairing

$$(4.3.2.1) \qquad (\ ,\ )_\lambda : T_\lambda \times T_\lambda \longrightarrow \mathbb{Z}_p(1)$$

satisfying $(rx, y)_\lambda = (x, ry)_\lambda$ for all $x, y \in T_\lambda$ and all $r \in \mathcal{O}_\lambda$. The construction of (4.3.2.1) from (4.3.1.1) is non-canonical, depending on a choice of generator for $\mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{O}_\lambda, \mathbb{Z}_p)$. Once we fix such a generator, this also fixes isomorphisms $A_\lambda \xrightarrow{\sim} T_\lambda \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p$ and so we also have pairings

$$(4.3.2.2) \qquad (\ ,\ )_\lambda : A_\lambda \times A_\lambda \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p(1)$$

satisfying $(rx, y)_\lambda = (x, ry)_\lambda$ for all $x, y \in A_\lambda, r \in \mathcal{O}_\lambda$.

(4.3.3) The generalization by Flach [Fl] of the Cassels-Tate pairing gives the following result.

THEOREM. *For $(\lambda) \in X_{\mathrm{good}}$, there is a non-degenerate alternating pairing*

$$[\ ,\ ]_\lambda : Ш_\lambda \times Ш_\lambda \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p$$

satisfying $[rx, y]_\lambda = [x, ry]_\lambda$ for all $x, y \in Ш_\lambda$ and all $r \in \mathcal{O}_\lambda$.

Proof. For $(\lambda) \in X_{\mathrm{good}}$, $H^1(\mathbb{Q}_p, T_\lambda)$ has $\mathcal{O}_\lambda$-rank two and the subspace $H^1_f(\mathbb{Q}_p, T_\lambda)$ has $\mathcal{O}_\lambda$-rank one and is its own orthogonal complement under the local duality pairing

$$H^1(\mathbb{Q}_p, T_\lambda) \times H^1(\mathbb{Q}_p, T_\lambda) \longrightarrow \mathbb{Z}_p$$

coming from (4.3.2.1) (we know that this is true after tensoring with the field of fractions, but because we defined $H^1_f(\mathbb{Q}_p, T_\lambda)$ to be $\mathcal{O}_\lambda$-saturated, it is true at the integral level too). So Flach's construction gives a non-degenerate alternating pairing

$$[\ ,\ ]_\lambda : Ш_\lambda \times Ш_\lambda \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p.$$

One can easily check through the construction of the pairing using cocycles that the relation $(rx, y)_\lambda = (x, ry)_\lambda$ on (4.3.2.2) implies the relation $[rx, y]_\lambda = [x, ry]_\lambda$.

(4.3.4) Dualizing this result, we deduce the existence of a non-degenerate alternating pairing

$$\langle\ ,\ \rangle_\lambda : \widehat{Ш}_\lambda \times \widehat{Ш}_\lambda \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p,$$

depending upon our fixed choice of generator for the free module $\mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{O}_\lambda, \mathbb{Z}_p)$.

(4.3.5) We can now use the results of 4.2 to prove Proposition 4.0.1. We choose a pseudo-isomorphism between $\widehat{Ш}$ and a module of standard form as in (4.1.22.1).

Fix any irreducible distinguished polynomial f (or $f = \pi$) in the support of $\widehat{Ш}$ and write this module of standard form as $M \oplus \overline{M}$ as in 4.1.22. So M can be written as

$$M = \left(\frac{\Lambda}{(f^{n_1})}\right)^{\alpha_1} \oplus \cdots \oplus \left(\frac{\Lambda}{(f^{n_r})}\right)^{\alpha_r} \qquad \text{with} \qquad n_1 > \cdots > n_r.$$

We need to show that all the α_i in this expression are even. Write $M_k = M/\lambda_k M$ where $\lambda_k = f + \pi^k$ (or $\lambda_k = X^k + \pi$ if $f = \pi$). Then we know from Lemma 4.1.23 that we have maps

$$M_k \longrightarrow \widehat{Ш}_k$$

with kernel and cokernel that are finite and bounded independently of k. If these kernels and cokernels are trivial we can apply the results of 4.2; if we take M as above, then the pairing of 4.3.4 on $M_k \xrightarrow{\sim} \widehat{Ш}_k$ satisfies the conditions of Theorem 4.2.2 (or Theorem 4.2.10 in the case $f = \pi$) and we deduce that the α_i are even. If the kernels and cokernels are non-trivial, we define a pairing on M_k as follows. Let $\phi_k : M_k \longrightarrow \widehat{Ш}_k$ be the maps of Lemma 4.1.23. Define a pairing

$$\langle\ ,\ \rangle'_k\ :\ M_k\ \times\ M_k\ \longrightarrow\ \mathbb{Q}_p/\mathbb{Z}_p$$

by $\langle x, y\rangle'_k = \langle \phi_k(x), \phi_k(y)\rangle_k$, where $\langle\ ,\ \rangle_k = \langle\ ,\ \rangle_{\lambda_k}$ is the pairing on $\widehat{Ш}_k$ of 4.3.4. The left and right kernels of the pairings $\langle\ ,\ \rangle'_k$ are finite and bounded independently of k, as $k \to \infty$, and we can apply Theorem 4.2.12 (and 4.2.17). This proves Proposition 4.0.1.

(4.3.6) COROLLARY. *For any $(\lambda) \in X_{\text{good}}$, we have*

$$\mathrm{rk}_{\mathcal{O}_\lambda}\widehat{\mathbb{S}}_\lambda \equiv \mathrm{rk}_\Lambda\widehat{\mathbb{S}} \pmod 2.$$

Proof. From Lemma 4.1.19, we get

$$\begin{aligned}\mathrm{rk}_{\mathcal{O}_\lambda}\widehat{\mathbb{S}}_\lambda &= rk_\Lambda\widehat{\mathbb{S}} + \mathrm{rk}_{\mathcal{O}_\lambda}\frac{\mathrm{Tors}_\Lambda(\widehat{\mathbb{S}})}{\lambda\mathrm{Tors}_\Lambda(\widehat{\mathbb{S}})}\\ &= \mathrm{rk}_\Lambda\widehat{\mathbb{S}} + 2\,\mathrm{rk}_{\mathcal{O}_\lambda}\frac{X}{\lambda X}\\ &\equiv \mathrm{rk}_\Lambda\widehat{\mathbb{S}} \pmod 2.\end{aligned}$$

(4.3.7) In the situation of 4.1.4, let $\mathcal{P} = (P_{k,\varepsilon}) \in \mathrm{Spec}(\Lambda)$ be any arithmetic point. So $\mathcal{P}$ is the height one prime $(\lambda) = (\lambda_{k,\varepsilon})$ of $\mathcal{O}[[X]]$ under the identification $\Lambda \xrightarrow{\sim} \mathcal{O}[[X]]$ of 4.1.4. If k is even and we are not in the exceptional case then the $\mathcal{O}_\lambda$-ranks of the $H^i(\mathbb{Q}_v, M)$ for $M = T, T^+, T^-$, are equal to the "generic"ranks of 4.1.6 by 3.1.3–5, and so $(\lambda) \in X_{\text{good}}$. In this case, the local conditions are the same as those defined by the Bloch-Kato subgroups $H^1_f(\mathbb{Q}_v, T_\lambda \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)$, again by the arguments of 3.1.3–5, and so $\mathbb{S}_\lambda$ is equal to the Bloch-Kato Selmer group $H^1_f(\mathbb{Q}, A_\lambda)$.

(4.3.8) COROLLARY. *With notation as in 4.3.7, if k is even and we are not in the exceptional case, then*

$$\mathrm{cork}_{\mathcal{O}_\lambda} H^1_f(\mathbb{Q}, A_\lambda) \equiv \mathrm{rk}_\Lambda\widehat{\mathbb{S}} \pmod 2.$$

(4.3.9) This Corollary proves Theorem A′ in the special case when $R = \Lambda$ (for non-exceptional $\mathcal{P}$). How often is $R = \Lambda$? In the notation of 3.2.2, this equality holds if g_{k_0} is not congruent to any other normalized eigenform of weight k_0 on $\Gamma_1(Np)$ (with respect to the embedding i_p).

For example, let E be a modular elliptic curve over $\mathbb{Q}$ of conductor N and let $f = \sum a_n q^n$ be the corresponding modular form of weight 2 on $\Gamma_0(N)$. Let p be a prime satisfying the following assumptions:

(1) p does not divide $6N$.

(2) E has ordinary reduction at p, i.e. $p \nmid a_p$.

(3) $E_p(\overline{\mathbb{Q}})$ is an irreducible $\mathbb{F}_p[G_{\mathbb{Q}}]$-module.

(4) p does not divide $\varphi(N)$.

(5) p does not divide the degree of some modular parametrization $X_0(N) \longrightarrow E$ of E.

(6) $p \nmid (a_p \pm 1)$.

The first three conditions mean that the discussion in Sect. 3–4 applies to f. It follows from (4) that all modular forms corresponding to arithmetic points of R have trivial character modulo N. According to [Ri 2, Thm. 1.4] (cf. [Za, Thm. 3]), the conditions (1) and (5) imply that f is not congruent (modulo a prime above p) to any other normalized eigenform on $\Gamma_0(N)$, and hence not even on $\Gamma_1(N)$, by (4). It follows from [Mi, Thm. 4.6.17] and (6) that there is no congruence between f and a normalized eigenform on $\Gamma_1(Np)$ (cf. 1.3.5). This implies that $R/(\gamma - 1)R = \mathbb{Z}_p$, hence $R = \Lambda = \mathbb{Z}_p[[X]]$, for all primes satisfying (1)–(6). Note that, if E has no complex multiplication, the set of such p has density one.

REFERENCES

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

[Bl-Ka] S. Bloch and 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.

[Br-He] W. Bruns and J. Herzog, *Cohen-Macaulay Rings*, Cambridge Univ. Press, Cambridge, 1993.

[Ca] H. Carayol, *Sur les représentations ℓ-adiques attachées aux formes modulaires de Hilbert*, Ann. Sci. Ec. Norm. Supér., 19 (1986), pp. 409–469.

[Cu-Re] C. W. Curtis and I. Reiner, *Methods of Representation Theory, vol. I*, Wiley, New York, 1990.

[De] P. Deligne, *Formes modulaires et représentations ℓ-adiques*, in Séminaire Bourbaki 1968/69, Exp. 355, Lect. Notes in Math. 179, Springer, Berlin, Heidelberg, New York, 1971, pp. 139–172.

[De-Ra] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, in Modular Functions in One Variable II, Lect. Notes in Math. 349, Springer, Berlin, Heidelberg, New York, 1973, pp. 143–316.

[Ei] M. Eichler, *Quaternare quadratische Formen und die Riemannische Vermutung für die Kongruenzzetafunktion*, Arch. Math., 5 (1954), pp. 355–366.

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

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

[Gr 1] R. Greenberg, *On the Birch and Swinnerton-Dyer conjecture*, Invent. Math., 72 (1983), pp. 241–265.

[Gr 2] R. Greenberg, *Elliptic curves and p-adic deformations*, in Elliptic curves and related topics, CRM Proc. Lecture Notes 4, Amer. Math. Soc., Providence, RI, 1994,

pp. 101–110.

[Gr 3] R. GREENBERG, *Lecture in Cambridge (UK)*, July 1996.

[Gr-St] R. GREENBERG AND G. STEVENS, *p-adic L-functions and p-adic periods of modular forms*, Invent. Math., 111 (1993), pp. 407–447.

[Gross] B. H. GROSS, *A tameness criterion for Galois representations associated to modular forms* mod p, Duke Math. J., 61 (1990), pp. 445–517.

[Gu] L. GUO, *General Selmer groups and critical values of Hecke L-functions*, Math. Ann., 297 (1993), pp. 221–233.

[Hi 1] H. HIDA, *Galois representations into* $GL_2(\mathbb{Z}_p[[X]])$ *attached to ordinary cusp forms*, Invent. Math., 85 (1986), pp. 545–613.

[Hi 2] H. HIDA, *Iwasawa modules attached to congruences of cusp forms*, Ann. Sci. Ec. Norm. Supér., 4-e série, 19 (1986), pp. 231–273.

[Hi 3] H. HIDA, *Modules of congruences of Hecke algebras and L-functions associated with cusp forms*, Amer. J. Math., 110 (1988), pp. 323–382.

[Ja] U. JANNSEN, *Continuous étale cohomology*, Math. Annalen, 280 (1988), pp. 207–245.

[Ka] K. KATO, *p-adic Hodge theory and values of zeta-functions of modular forms*, in preparation.

[KaN] N. KATZ, *p-adic properties of modular schemes and modular forms*, in Modular Functions in One Variable III, Lect. Notes in Math. 350, Springer, Berlin, Heidelberg, New York, 1973, pp. 70–189.

[Ki] K. KITAGAWA, *On standard p-adic L-functions of families of elliptic cusp forms*, in p-adic Monodromy and the Birch and Swinnerton-Dyer Conjecture (Boston, MA, 1991), Contemp. Math. 165, Amer. Math. Soc., Providence, RI, 1994, pp. 81–110.

[Ko 1] V. A. KOLYVAGIN, *Euler systems*, in The Grothendieck Festschrift II, Progress in Mathematics 87, Birkhäuser, Boston, Basel, Berlin, 1990, pp. 435–483.

[Ko 2] V. A. KOLYVAGIN, *On the structure of Selmer groups*, Math. Annalen, 291 (1991), pp. 253–259.

[La] R. LANGLANDS, *Modular forms and ℓ-adic representations*, in Modular Functions in One Variable II, Lect. Notes in Math. 349, Springer, Berlin, Heidelberg, New York, 1973, pp. 361–500.

[Ma-Ta-Te] B. MAZUR, J. TATE, AND J. TEITELBAUM, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math., 84 (1986), pp. 1–48.

[Ma-Ti] B. MAZUR AND J. TILOUINE, *Représentations galoisiennes, diffŕentielles de Kähler et "conjectures principales"*, Publ. Math. de l'I.H.E.S., 71 (1990), pp. 65–103.

[Miy] T. MIYAKE, *Modular Forms*, Springer, Berlin-New York, 1989.

[Mo] P. MONSKY, *Generalizing the Birch-Stephens theorem. I. Modular curves*, Math. Z., 221 (1996), pp. 415–420.

[Ne 1] J. NEKOVÁŘ, *On p-adic height pairings*, in Séminaire de Théorie des Nombres de Paris 1990/91, S. David, ed., Progress in Math. 108, Birkhäuser, Boston, 1993, pp. 127–202.

[Ne 2] J. NEKOVÁŘ, *On the p-adic height of Heegner cycles*, Math. Annalen, 302 (1995), pp. 609–686.

[Ne 3] J. NEKOVÁŘ, *Selmer complexes*, in preparation.

[Pl] A. PLATER, *Height pairings in families of deformations*, J. reine angew. Math., 486 (1997), pp. 97–127.

[Ri 1] K. RIBET, *Galois representations attached to eigenforms with Nebentypus*, in Modular Functions in One Variable V, Lect. Notes in Math. 601, Springer, Berlin, Heidelberg, New York, 1977, pp. 17–52.

[Ri 2] K. RIBET, *Mod p Hecke operators and congruences between modular forms*, Invent. Math., 71 (1983), pp. 193–205.

[Ro] D. ROHRLICH, *On L-functions of elliptic curves and anticyclotomic towers*, Invent. Math., 75 (1984), pp. 383–408.

[Sc] A. J. SCHOLL, *Motives for modular forms*, Invent. Math., 100 (1990), pp. 419–430.

[Sh] G. SHIMURA, *Correspondances modulaires et les fonctions ζ des courbes algébriques*, J. Math. Soc. Jap., 10 (1958), pp. 1–28.

[Ta] J. TATE, *Relations between K_2 and Galois cohomology*, Invent. Math., 36 (1976), pp. 257–274.

[Ti 1] J. TILOUINE, *Un sous-groupe p-divisible de la jacobienne de $X_1(Np^r)$ comme module sur l'algèbre de Hecke*, Bull. Soc. Math. France, 115 (1987), pp. 329–360.

[Ti 2] J. TILOUINE, *Hecke algebras and the Gorenstein property*, in Modular Forms and Fermat's Last Theorem, G. Cornell, J. Silverman, and G. Stevens, ed., Springer, New York, 1997, pp. 327–342.

[Wi 1] A. WILES, *On ordinary λ-adic representations associated to modular forms*, Invent. Math., 94 (1988), pp. 529–573.

[Wi 2] A. WILES, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math., 141 (1995), pp. 443–551.

[Za] D. ZAGIER, *Modular parametrization of elliptic curves*, Canad. Math. Bull., 28 (1985), pp. 372–384.

[Bures] *Périodes p-adiques*, Astérisque 223, Soc. Math. de France, Paris, 1994.