The Euler system method for CM points on Shimura curves

Jan Nekovář

Let E be an elliptic curve over $\mathbf{Q}$ of conductor N; let $\pi : X_0(N) \longrightarrow E$ be a modular parametrization sending the cusp ∞ to the origin. If $K = \mathbf{Q}(\sqrt{D})$ is an imaginary quadratic field of discriminant $D < 0$ satisfying the "Heegner condition" of Birch [Bi] ("each prime dividing N splits in $K/\mathbf{Q}$"), a choice of an ideal $\mathcal{N} \subset \mathcal{O}_K$ satisfying $\mathcal{N}\overline{\mathcal{N}} = N\mathcal{O}_K$ and $(\mathcal{N}, \overline{\mathcal{N}}) = (1)$ determines a Heegner point

$$x_1 = [\mathbf{C}/\mathcal{O}_K \longrightarrow \mathbf{C}/\mathcal{N}^{-1}] \in X_0(N)(K[1]),$$

defined over the Hilbert class field $K[1]$ of K. Set $y_1 = \pi(x_1) \in E(K[1])$ and $y = \mathrm{Tr}_{K[1]/K}(y) \in E(K)$. A fundamental result of Kolyvagin [Ko, Thm. A] (explained in a simplified setting in [Gr 1]) states that

(K) if $y \notin E(K)_{\mathrm{tors}}$, then the abelian groups $E(K)/\mathbf{Z}y$, $Ш(E/K)$ are finite.

More precisely, Kolyvagin showed that $|Ш(E/K)|$ divides a certain multiple of $[E(K) : \mathbf{Z}y]^2$. Kolyvagin's result (K) has been generalized in several directions: Kolyvagin and Logačev [Ko-Lo 1] considered higher-dimensional simple quotients of $J_0(N)$ instead of elliptic curves, as well as [Ko-Lo 2] quotients of Jacobians of some Shimura curves over totally real number fields. Bertolini and Darmon [Be-Da] proved, under some additional assumptions, a "mod p" version of (K) over ring class fields $K[c]$ ($(c, N) = 1$). Tian and Zhang ([Ti], [Ti-Zh]) considered a common generalization of [Ko-Lo 2] and [Be-Da]. The more refined "quantitative" results of Kolyvagin were generalized by Bertolini [Be] and Howard [Ho 1,2].

The main result of the present article is the following generalization of (K), which is one of the ingredients in the proof of the parity conjecture for Selmer groups of Hilbert modular forms ([Ne, Ch. 12]).

Theorem. *Let F be a totally real number field, X a Shimura curve over F, and A an F-simple quotient of the Jacobian of X, which corresponds to (the Galois conjugacy class of) a Hilbert modular form f with trivial character (A is an abelian variety of GL_2-type and $\mathrm{End}_F(A)$ is an order in a totally real number field of degree equal to $\dim(A)$). Let x be a CM point on X by a totally imaginary quadratic extension K of F and α a character of the Galois group $\mathrm{Gal}(K(x)/K)$. Assume that A does not acquire CM over any totally imaginary quadratic extension K' of F contained in $K(x)^{\mathrm{Ker}(\alpha)}$ (i.e., f is not a θ-series associated to a Hecke character of K'). If the α-component of the image y of x in A is not torsion, then the α-components of $A(K(x))/\mathrm{End}_F(A) \cdot y$ and $Ш(A/K(x))$ are finite.*

See Theorem 3.2 for a precise formulation. The proof follows the main lines of the argument of [Be-Da]; the novelty lies in the fact that under our minimalist assumptions there is no "geometric" formula for the action of the complex conjugation on x. Unlike all previous works in this direction, our version of the Euler system argument (in particular, 7.6.4 below) does not require such a formula.

Theorem 3.2 is expected to be related to arithmetic properties of the Rankin-Selberg L-function $L(f_K \otimes \alpha^{-1}, s)$ at the central point $s = 1$ ([Zh 1,2], [Co-Va 1]). The assumption that f has trivial character ensures that $f_K \otimes \alpha^{-1}$ is self-dual in the sense that there is a "symmetric" functional equation relating $L(f_K \otimes \alpha^{-1}, s)$ (which turns out to be equal to $L(f_K \otimes \alpha, s)$ in our case) and $L(f_K \otimes \alpha^{-1}, 2 - s)$. As explained in [Gr 2] (see also [Co-Va 1]), it is possible for $L(f_K \otimes \alpha^{-1}, s)$ to be self-dual even if f has non-trivial character ω, provided that ω is equal to the restriction of α (considered as a character of $\mathbf{A}_K^*/K^*$) to $\mathbf{A}_F^*/F^*$. It is an interesting question whether Theorem 3.2 can be generalized to such a more general self-dual setting.

A substantial part of the present article was written during the author's visit at the COE programme at Nagoya University in spring 2005. The author is grateful to K. Fujiwara for inviting him to Nagoya. He would also like to thank H. Carayol, C. Cornut and M. Dimitrov for useful discussions, and the referee for helpful comments.

1. Quaternionic Shimura curves and their Jacobians

In this section we recall basic properties of Shimura curves associated to quaternion algebras over totally real fields. The standard reference is [Ca 1] (see also [Zh 1,2]), but we follow the notations and sign conventions of [Co-Va 1,2] (with the parameter $\epsilon = 1$). In particular, the reciprocity map of class field theory is normalized by making uniformizers correspond to *geometric* Frobenius elements.

(1.1) Let F be a totally real number field of degree $d = [F : \mathbf{Q}]$. Fix an archimedean prime τ_1 of F and a finite set S_B of non-archimedean primes of F satisfying

$$|S_B| \equiv [F : \mathbf{Q}] - 1 \pmod 2.$$

Let B be the (unique) quaternion algebra over F ramified at the set

$$Ram(B) = \{v|\infty,\, v \neq \tau_1\} \cup S_B.$$

For each real embedding $\tau_j : F \hookrightarrow \mathbf{R}$ $(j = 1, \ldots, d)$ put $B_{\tau_j} = B \otimes_{F,\tau_j} \mathbf{R}$. We fix an isomorphism of $\mathbf{R}$-algebras

$$B_{\tau_1} = B \otimes_{F,\tau_1} \mathbf{R} \xrightarrow{\sim} M_2(\mathbf{R}) \tag{1.1.1}$$

(for $j > 1$, B_{τ_j} is isomorphic to the algebra of Hamilton quaternions, but there is no need to fix a specific isomorphism).

Fix an embedding $\overline{F} \hookrightarrow \mathbf{C}$ extending $\tau_1 : F \hookrightarrow \mathbf{R}$.

(1.2) Let G be the algebraic group over $\mathbf{Q}$ satisfying $G(A) = (B \otimes_{\mathbf{Q}} A)^*$, for every commutative $\mathbf{Q}$-algebra A. Denote by Z the centre of G and by $nr : G(A) \longrightarrow (F \otimes_{\mathbf{Q}} A)^*$ the reduced norm. For $j = 1, \ldots, d$, denote by G_j the algebraic group over $\mathbf{R}$ given by $G_j = G \otimes_{F,\tau_j} \mathbf{R}$; we have $G_{\mathbf{R}} \xrightarrow{\sim} G_1 \times \cdots \times G_d$. We denote, for any abelian group A, $\widehat{A} = A \otimes \widehat{\mathbf{Z}}$.

Quaternionic Shimura curves are associated to the Shimura datum (G, X), where G is as above and X is the $G(\mathbf{R})$-conjugacy class of the morphism

$$\begin{aligned} h_0 : \mathbf{S} = \mathrm{Res}_{\mathbf{C}/\mathbf{R}}(\mathbf{G}_{m,\mathbf{C}}) &\longrightarrow G(\mathbf{R}) = G_1(\mathbf{R}) \times \cdots \times G_d(\mathbf{R}) \\ x + iy &\mapsto \left(\begin{pmatrix} x & y \\ -y & x \end{pmatrix}, 1, \ldots, 1 \right). \end{aligned}$$

In concrete terms, X has a natural complex structure ([Mi 2, p. 320]) and the map

$$\mathrm{Ad}(g)h_0 = gh_0g^{-1} \mapsto g(i) \qquad\qquad (g \in G(\mathbf{R}))$$

(where g acts on $\mathbf{C} - \mathbf{R}$ as in 1.3 below) defines a holomorphic isomorphism $X \xrightarrow{\sim} \mathbf{C} - \mathbf{R}$.

(1.3) The Shimura curves in question form a projective system $\{M_H\}$ indexed by open compact subgroups $H \subset G(\mathbf{A}_f) = \widehat{B}^*$. Each curve M_H is smooth over $\mathrm{Spec}(F)$ and each transition map $\mathrm{pr} : M_H \longrightarrow M_{H'}$ (for $H \subset H'$) is finite and flat. The Riemann surface associated to M_H

$$M_H^{\mathrm{an}} = (M_H \otimes_{F,\tau_1} \mathbf{C})\,(\mathbf{C})$$

is identified with $B^* \backslash (X \times \widehat{B}^*/H)$, where $B^* \subset B_{\tau_1}^*$ acts on $X \xrightarrow{\sim} \mathbf{C} - \mathbf{R}$ via the isomorphism $B_{\tau_1}^* \xrightarrow{\sim} GL_2(\mathbf{R})$ induced by (1.1.1), and the standard action $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}$ of $GL_2(\mathbf{R})$ on $\mathbf{C} - \mathbf{R}$. We denote by $[z, b] = [z, b]_H$ the point of M_H^{an} represented by a pair $(z, b) \in X \times \widehat{B}^*$. For $H \subset H'$, the transition map $\mathrm{pr} : M_H \longrightarrow M_{H'}$ corresponds to the natural projection

$$\mathrm{pr} : M_H^{\mathrm{an}} \longrightarrow M_{H'}^{\mathrm{an}}, \qquad [z, b]_H \mapsto [z, b]_{H'}.$$

In the "classical case" $F = \mathbf{Q}$, $S_B = \emptyset$ ($\Longleftrightarrow$ $B = M_2(\mathbf{Q})$), the curves M_H are the usual modular curves; we denote by

$$M_H^* = M_H \cup \{\text{cusps}\}_H$$

their standard smooth compactifications; they form again a projective system with finite flat transition maps. If $B \neq M_2(\mathbf{Q})$, then the curves M_H are proper over $\mathrm{Spec}(F)$; we put $M_H^* = M_H$.

(1.4) The group $G(\mathbf{A}_f) = \widehat{B}^*$ acts on the right on the projective systems $\{M_H\}$ and $\{M_H^*\}$. More precisely, the right multiplication by $g \in \widehat{B}^*$ induces an F-isomorphism $[\cdot g] : M_H \xrightarrow{\sim} M_{g^{-1}Hg}$; the corresponding holomorphic isomorphism

$$[\cdot g] : M_H^{\mathrm{an}} = B^* \backslash (X \times \widehat{B}^*/H) \xrightarrow{\sim} M_{g^{-1}Hg}^{\mathrm{an}} = B^* \backslash (X \times \widehat{B}^*/g^{-1}Hg)$$

is given by the formula $[x, b] \mapsto [x, bg]$.

In particular, the centre $\widehat{F}^* = Z(\mathbf{A}_f) \subset \widehat{B}^*$ acts on M_H (and M_H^*) via its finite quotient $\widehat{F}^*/(\widehat{F}^* \cap H) = \widehat{F}^*/(\widehat{\mathcal{O}}_F^* \cap H)$; we denote by $N_H \subset N_H^*$ the corresponding quotient curves, which are again smooth over $\mathrm{Spec}(F)$ [Ka-Ma, p. 508] (the curve M_H (resp., N_H) was denoted by Y (resp., X) in [Zh 1]). The Riemann surface associated to N_H

$$N_H^{\mathrm{an}} = (N_H \otimes_{F,\tau_1} \mathbf{C})(\mathbf{C})$$

is identified with $B^* \backslash (X \times \widehat{B}^*/H\widehat{F}^*)$. In particular, N_H (and N_H^*) depend only on the subgroup $H\widehat{F}^* \subset \widehat{B}^*$. In abstract terms, the projective system $\{N_H\}$ is associated to the Shimura datum $(G/Z, X)$.

Note that, for each open compact subgroup $H \subset \widehat{B}^*$, there exists an $\mathcal{O}_F$-order $R \subset B$ such that $\widehat{R}^* \subset H\widehat{\mathcal{O}}_F^*$. In particular, $\widehat{R}^*\widehat{F}^* \subset H\widehat{F}^*$, hence the curves $N_{\widehat{R}^*}$ (where R runs through all $\mathcal{O}_F$-orders of B) form a co-final subsystem of $\{N_H\}$.

(1.5) Each curve M_H^* (hence also N_H^*) is irreducible ([Ca 1, 1.3], [Co-Va 1, 3.2]), but not necessarily geometrically irreducible. Denote by $F(\mathcal{M}_H)$ (resp., $F(\mathcal{N}_H)$) the algebraic closure of F in the function field of M_H^* (resp., of N_H^*). The reciprocity law [De, 3.9], [Mi 2, II.5.1] (with the sign corrected, [Mi 3, 1.10]) implies that the fields $F(\mathcal{N}_H) \subseteq F(\mathcal{M}_H)$ are abelian over F and that the reciprocity map

$$\mathrm{rec}_F : \widehat{F}^* \longrightarrow \mathrm{Gal}(F^{ab}/F)$$

induces isomorphisms (depending on a choice of embedding $F(\mathcal{M}_H) \hookrightarrow F^{ab}$)

$$F_+^* \backslash \widehat{F}^*/nr(H) \xrightarrow{\sim} \mathrm{Gal}(F(\mathcal{M}_H)/F), \qquad F_+^* \backslash \widehat{F}^*/\widehat{F}^{*2} nr(H) \xrightarrow{\sim} \mathrm{Gal}(F(\mathcal{N}_H)/F),$$

where $F_+^* = \mathrm{Ker}(F^* \longrightarrow \pi_0((F \otimes_{\mathbf{Q}} \mathbf{R})^*))$ denotes the subgroup of totally positive elements of F^*.

(1.6) Differentials and automorphic forms of "weight 2" ([Co-Va 1, 3.6]) Denote by Ω^{an} the sheaf of holomorphic 1-forms on any given Riemann surface. As in the classical case $B = M_2(\mathbf{Q})$, the space of global holomorphic 1-forms

$$\varinjlim_H \Gamma((M_H^*)^{\mathrm{an}}, \Omega^{\mathrm{an}}),$$

equipped with a canonical left action of $\widehat{B}^*$ given by

$$[\cdot g]^* : \Gamma((M_{g^{-1}Hg}^*)^{\mathrm{an}}, \Omega^{\mathrm{an}}) \longrightarrow \Gamma((M_H^*)^{\mathrm{an}}, \Omega^{\mathrm{an}}), \tag{1.6.1}$$

can be naturally identified with a certain space of automorphic forms on $G(\mathbf{A}) = G(\mathbf{R}) \times \widehat{B}^* = B_{\mathbf{A}}^*$.

More precisely, for each compact open subgroup $H \subset \widehat{B}^*$ we have [(1)]

$$G(\mathbf{A}) = \coprod_{\alpha \in C} G(\mathbf{Q}) \cdot (G(\mathbf{R})^+ \times \alpha H),$$

[(1)] As the case $B = M_2(\mathbf{Q})$ is well-known, we discuss only the case $B \neq M_2(\mathbf{Q})$, when $M_H^* = M_H$.

where

$$G(\mathbf{R})^+ = GL_2^+(\mathbf{R}) \times G_2(\mathbf{R}) \times \cdots \times G_d(\mathbf{R}), \qquad G(\mathbf{Q})^+ = G(\mathbf{Q}) \cap G(\mathbf{R})^+ = \mathrm{Ker}\left(B^* \xrightarrow{nr} F^* \longrightarrow F^*/F_+^*\right)$$

and $C \subset \widehat{B}^*$ is a fixed (finite) set of representatives of the double cosets $G(\mathbf{Q})^+\backslash G(\mathbf{A}_f)/H$. Put, for each $\alpha \in C$,

$$\Gamma_\alpha = \alpha H \alpha^{-1} \cap G(\mathbf{Q})^+ \subset G(\mathbf{R})^+, \qquad \overline{\Gamma}_\alpha = \mathrm{Im}\left(\Gamma_\alpha \longrightarrow PGL_2^+(\mathbf{R})\right).$$

Writing $\mathcal{H} = \{z \in \mathbf{C} \mid \mathrm{Im}(z) > 0\}$ for the complex upper half plane, the map

$$\begin{array}{rcl} \coprod_{\alpha \in C} \overline{\Gamma}_\alpha\backslash\mathcal{H} & \xrightarrow{\sim} & M_H^{\mathrm{an}} = (M_H^*)^{\mathrm{an}} \\ \overline{\Gamma}_\alpha \cdot g(i) & \mapsto & [gh_0g^{-1}, \alpha]_H \end{array} \qquad (g \in GL_2^+(\mathbf{R}))$$

is a holomorphic isomorphism. Using the standard notation

$$j(g,z) = \det(g)^{-1/2}(cz+d), \qquad g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2^+(\mathbf{R}), \qquad z \in \mathcal{H},$$

the formula

$$f_\omega(\gamma(g^+, \alpha h)) = j(g_1^+)^{-2} f_\alpha(g_1^+(i)), \qquad (\gamma \in G(\mathbf{Q}),\ g^+ = (g_1^+, g_2, \ldots, g_d) \in G(\mathbf{R})^+,\ h \in H)$$

defines a bijection

$$\begin{array}{ccccc} \Gamma((M_H^*)^{\mathrm{an}}, \Omega^{\mathrm{an}}) & \xrightarrow{\sim} & \bigoplus_{\alpha \in C} \Gamma(\overline{\Gamma}_\alpha\backslash\mathcal{H}, \Omega^{\mathrm{an}}) & \xrightarrow{\sim} & \mathcal{S}_2^H \\ \omega & \mapsto & (f_\alpha(z)\,dz)_{\alpha \in C} & \mapsto & (f_\omega : G(\mathbf{A}) \longrightarrow \mathbf{C}), \end{array} \tag{1.6.2}$$

where $\mathcal{S}_2^H$ denotes the space of functions $f : G(\mathbf{A}) \longrightarrow \mathbf{C}$ satisfying

$$f\left(\gamma\, g\, z_\infty \left(\begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}, g_2, \ldots, g_d\right) h\right) = e^{-2i\theta} f(g) \qquad \begin{array}{r} (\gamma \in G(\mathbf{Q}),\ g \in G(\mathbf{A}),\ z_\infty \in Z(\mathbf{R}), \\ \theta \in \mathbf{R},\ g_j \in G_j(\mathbf{R})\,(j>1),\ h \in H) \end{array}$$

and such that, for each $g \in G(\mathbf{A})$, the function

$$x + iy \mapsto \frac{1}{y} f\left(g\left(\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}, 1, \ldots, 1\right)\right)$$

is holomorphic on $\mathcal{H}$ (in the case $B = M_2(\mathbf{Q})$ one has to impose an additional cuspidality condition on the function f; this is automatic if $B \neq M_2(\mathbf{Q})$).

Passing to the inductive limit with respect to all open compact subgroups of $\widehat{B}^*$, we obtain a $\widehat{B}^*$-equivariant bijection

$$\varinjlim_H \Gamma((M_H^*)^{\mathrm{an}}, \Omega^{\mathrm{an}}) \xrightarrow{\sim} \mathcal{S}_2 := \bigcup_H \mathcal{S}_2^H, \tag{1.6.3}$$

with $\widehat{B}^*$ acting (on the left) on $\mathcal{S}_2$ by right translations: $(b \cdot f)(g) = f(gb)$ (which means that $\mathcal{S}_2^H$ coincides, as the notation suggests, with the space of H-invariant elements of $\mathcal{S}_2$).

Note that the centre $Z(\mathbf{A}_f) = \widehat{F}^*$ acts on $\mathcal{S}_2^H$ via its finite quotient $\widehat{F}^*/(\widehat{F}^* \cap H) = \widehat{F}^*/(\widehat{\mathcal{O}}_F^* \cap H)$, hence (1.6.2) induces bijections

$$\Gamma((N_H^*)^{\mathrm{an}}, \Omega^{\mathrm{an}}) \xrightarrow{\sim} \mathcal{S}_2^{H\widehat{F}^*} = \{f \in \mathcal{S}_2^H \mid (\forall g \in G(\mathbf{A}))\,(\forall z \in Z(\mathbf{A}))\ \ f(gz) = f(g)\}. \tag{1.6.4}$$

(1.7) Automorphic representations. The multiplicity one theorem for automorphic forms on $B_{\mathbf{A}}^*$ ([Ge], VI.2) implies that the space $\mathcal{S}_2$ (as an admissible smooth representation of $\widehat{B}^*$) decomposes as a countable direct sum

$$\mathcal{S}_2 \xrightarrow{\sim} \bigoplus_{\pi = \sigma_2 \otimes \pi_f} \pi_f, \tag{1.7.1}$$

where π runs through all irreducible cuspidal (this is automatic if $B \neq M_2(\mathbf{Q})$) unitary automorphic representations of $B_{\mathbf{A}}^*$ whose archimedean component π_∞ is isomorphic to

$$\sigma_2 = \begin{pmatrix} \text{the weight 2 holomorphic discrete} \\ \text{series representation of } G_1(\mathbf{R}) \end{pmatrix} \otimes \begin{pmatrix} \text{the trivial representation of} \\ G_2(\mathbf{R}) \times \cdots \times G_d(\mathbf{R}) \end{pmatrix}.$$

In particular, (1.6.4) induces an isomorphism of admissible smooth representations of $\widehat{B}^*/\widehat{F}^*$

$$\varinjlim_H \Gamma((N_H^*)^{\mathrm{an}}, \Omega^{\mathrm{an}}) \xrightarrow{\sim} \mathcal{S}_2^{\widehat{F}^*} \xrightarrow{\sim} \bigoplus_{\substack{\pi = \sigma_2 \otimes \pi_f \\ \omega_\pi = 1}} \pi_f, \tag{1.7.2}$$

where $\omega_\pi : Z(\mathbf{A}) \longrightarrow \mathbf{C}^*$ denotes the central character of π.

(1.8) The Hecke algebra. For each non-archimedean prime v of F, let dg_v be the (bi-invariant) Haar measure on B_v^* normalized so that $\int_{H_v} dg_v = 1$ for one (hence for every) maximal compact subgroup $H_v \subset B_v^*$. The product $dg = \prod dg_v$ then defines a bi-invariant Haar measure on $\widehat{B}^*$. We denote by $\mathrm{vol}(X) = \int_X dg$ the corresponding volume.

The Hecke algebra

$$\mathcal{H}(\widehat{B}^*) = \mathcal{C}_c^\infty(\widehat{B}^*, \mathbf{C}) = \{\alpha : \widehat{B}^* \longrightarrow \mathbf{C} \mid \alpha \text{ is locally constant, with compact support}\}$$

with the convolution product

$$(\alpha * \beta)(g) = \int_{\widehat{B}^*} \alpha(gh^{-1})\beta(h)\, dh$$

is isomorphic to the direct limit (over all open compact subgroups $H \subset \widehat{B}^*$) of the double coset algebras

$$\begin{aligned} \varinjlim_H \mathbf{C}[H\backslash\widehat{B}^*/H] &\xrightarrow{\sim} \mathcal{H}(\widehat{B}^*) \\ HbH &\mapsto \mathrm{vol}(H)^{-1}\, 1_{HbH} \end{aligned}$$

The product structure on $\mathbf{C}[H\backslash\widehat{B}^*/H]$ is as in [Sh 2, 3.1], [Miy, (2.7.3)] (hence is the *opposite* to that in [Co-Va 1, 3.4, 3.11]).

Any smooth representation (π, V) of $\widehat{B}^*$ gives rise to a left action of $\mathcal{H}(\widehat{B}^*)$ on V, given by the formula

$$\alpha \cdot v = \int_{\widehat{B}^*} \alpha(h)\pi(h)v\, dh \qquad\qquad (\alpha \in \mathcal{H}(\widehat{B}^*),\, v \in V).$$

In particular, $\alpha \in \mathcal{H}(\widehat{B}^*)$ acts on $\mathcal{S}_2$ by

$$(\alpha \cdot f)(g) = \int_{\widehat{B}^*} \alpha(h) f(gh)\, dh.$$

Note that, for any open compact subgroups $H, H' \subset \widehat{B}^*$ and $b \in \widehat{B}^*$, the action of $1_{HbH'}$ maps $\mathcal{S}_2^{H'}$ to $\mathcal{S}_2^H$.

(1.9) Hecke correspondences. Let H, H' be open compact subgroups of $\widehat{B}^*$ and $g \in \widehat{B}^*$. The diagram

$$\begin{array}{ccc} M^*_{H\cap gH'g^{-1}} & \xrightarrow{[\cdot g]} & M^*_{g^{-1}Hg\cap H'} \\ \Big\downarrow{\scriptstyle \mathrm{pr}} & & \Big\downarrow{\scriptstyle \mathrm{pr}'} \\ M^*_H & \overset{[HgH']}{- - - - \twoheadrightarrow} & M^*_{H'} \end{array} \tag{1.9.1}$$

defines a multivalued map (a "Hecke correspondence")

$$[HgH'] : M^*_H - - - \twoheadrightarrow M^*_{H'}.$$

On non-cuspidal complex points,

$$[HgH'] : M^{\mathrm{an}}_H = B^*\backslash(X \times \widehat{B}^*/H) - - - - \twoheadrightarrow M^{\mathrm{an}}_{H'} = B^*\backslash(X \times \widehat{B}^*/H')$$

is given by the formula

$$[x, b]_H \mapsto \sum_i [x, bg_i]_{H'}, \qquad HgH'F^* = \coprod_i g_i H' F^*. \tag{1.9.2}$$

The degree of $[HgH']$ is the degree of pr, namely $(HF^* : (H\cap gH'g^{-1})F^*)$ (which is equal to $(H : H\cap gH'g^{-1})$, if $\mathcal{O}_F^* \subset H \cap H'$). If $z \in Z(\mathbf{A}_f) = \widehat{F}^*$, then we have

$$[HzH] = [\cdot z] : M^*_H \longrightarrow M^*_H, \qquad [H'zH'] = [\cdot z] : M^*_{H'} \longrightarrow M^*_{H'}, \qquad [\cdot z] \circ [HgH'] = [HgH'] \circ [\cdot z].$$

For any "reasonable" cohomology theory $H^*_?$, the correspondences $[HgH']$ induce maps

$$[HgH']^* : H^q_?(M^*_{H'}) \longrightarrow H^q_?(M^*_H), \qquad [HgH']_* : H^q_?(M^*_H) \longrightarrow H^q_?(M^*_{H'}).$$

As the transpose of the diagram (1.9.1) is given by

$$\begin{array}{ccc} M^*_{g^{-1}Hg\cap H'} & \xrightarrow{[\cdot g^{-1}]} & M^*_{H\cap gH'g^{-1}} \\ \Big\downarrow{\scriptstyle \mathrm{pr}'} & & \Big\downarrow{\scriptstyle \mathrm{pr}} \\ M^*_{H'} & \overset{[H'g^{-1}H]}{- - - - \twoheadrightarrow} & M^*_H, \end{array}$$

we have

$$[HgH']_* = [H'g^{-1}H]^*, \qquad [HgH']^* = [H'g^{-1}H]_* \tag{1.9.3}$$

If we replace H, H' by $H\widehat{F}^*, H'\widehat{F}^*$, then we obtain Hecke correspondences

$$N^*_H - - - \twoheadrightarrow N^*_{H'}$$

with similar properties.

(1.10) Action on holomorphic differentials. In the situation of (1.9.1), we deduce from (1.9.2) and the $\widehat{B}^*$-equivariance of (1.6.3) that the map

$$[HgH']^* : \Gamma((M^*_{H'})^{\mathrm{an}}, \Omega^{\mathrm{an}}) \longrightarrow \Gamma((M^*_H)^{\mathrm{an}}, \Omega^{\mathrm{an}})$$

corresponds to the action of $1_{HgH'}$, suitably normalized:

$$\begin{array}{ccc} \mathcal{S}_2^{H'} & \longrightarrow & \mathcal{S}_2^H \\ f' & \mapsto & \mathrm{vol}(H')^{-1}\, 1_{HgH'} \cdot f'. \end{array}$$

If $z \in Z(\mathbf{A}_f) = \widehat{F}^*$ and $H = H'$, then

$$[HzH']^* = [\cdot z]^* : \Gamma((M_H^*)^{\mathrm{an}}, \Omega^{\mathrm{an}}) \longrightarrow \Gamma((M_H^*)^{\mathrm{an}}, \Omega^{\mathrm{an}})$$

corresponds to the action of z on $\mathcal{S}_2^H$, which we denote by $[z]$.

(1.11) Adjoints. Up to a scalar multiple, the hermitian scalar product

$$\langle \omega_1, \omega_2 \rangle = \frac{i}{2} \int\limits_{(M_H^*)^{\mathrm{an}}} \omega_1 \wedge \overline{\omega_2} \qquad (\omega_1, \omega_2 \in \Gamma((M_H^*)^{\mathrm{an}}, \Omega^{\mathrm{an}})) \tag{1.11.1}$$

corresponds, via the isomorphism (1.6.2), to the hermitian scalar product

$$\langle f_1, f_2 \rangle = \int\limits_{G(\mathbf{Q})\backslash G(\mathbf{A})/Z_\infty K_\infty^+} f_1(g)\overline{f_2(g)}\, dg \qquad (f_1, f_2 \in \mathcal{S}_2^H),$$

where

$$Z_\infty K_\infty^+ = \left\{ \left(\begin{pmatrix} z & 0 \\ 0 & z \end{pmatrix} \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}, g_2, \ldots, g_d \right) \;\middle|\; z \in \mathbf{R}^*,\, \theta \in \mathbf{R},\, g_j \in G_j(\mathbf{R}) \right\} \subset G(\mathbf{R})^+.$$

For $\alpha \in \mathcal{H}(\widehat{B}^*)$ and $f_1, f_2 \in \mathcal{S}_2$, we have

$$\langle \alpha \cdot f_1, f_2 \rangle = \langle f_1, {}^t\alpha \cdot f_2 \rangle, \qquad {}^t\alpha(g) = \overline{\alpha(g^{-1})} \tag{1.11.2}$$

(i.e., ${}^t\alpha$ is the adjoint of α). For example,

$${}^t 1_{HgH'} = 1_{H'g^{-1}H}. \tag{1.11.3}$$

In particular, if $H = H' = H_v H^v$, where $v \notin S_B$, $H_v \subset B_v^*$ is a maximal compact subgroup and $b_v \in B_v^* \subset \widehat{B}^*$, then

$$H_v b_v^{-1} H_v = nr(b_v)^{-1}\, H_v b_v H_v,$$

as H_v is isomorphic to $GL_2(\mathcal{O}_{F,v})$ and

$$GL_2(\mathcal{O}_{F,v}) \begin{pmatrix} t_1^{-1} & 0 \\ 0 & t_2^{-1} \end{pmatrix} GL_2(\mathcal{O}_{F,v}) = (t_1 t_2)^{-1} GL_2(\mathcal{O}_{F,v}) \begin{pmatrix} t_2 & 0 \\ 0 & t_1 \end{pmatrix} GL_2(\mathcal{O}_{F,v}) =$$
$$= (t_1 t_2)^{-1} GL_2(\mathcal{O}_{F,v}) \begin{pmatrix} t_1 & 0 \\ 0 & t_2 \end{pmatrix} GL_2(\mathcal{O}_{F,v}),$$

hence

$${}^t 1_{Hb_vH} = [nr(b_v)^{-1}] \circ 1_{Hb_vH} = 1_{Hb_vH} \circ [nr(b_v)^{-1}] \tag{1.11.4}$$

in this case.

(1.12) Hecke operators and cup products. Fix an open compact subgroup $H \subset \widehat{B}^*$. There exists a finite set $S \supset S_B$ of non-archimedean primes of F such that $H = H_S H^S$, where

$$H_S \subset \prod_{v \in S} B_v^*, \qquad H^S = \prod_{v \notin S} H_v = \text{ a maximal compact subgroup of } G(\mathbf{A}_f)^S = \prod\nolimits'_{v \notin S} B_v^*. \tag{1.12.1}$$

More precisely, for each non-archimedean prime $v \notin S$ there exists a (unique) maximal $\mathcal{O}_{F,v}$-order $R(v) \subset B_v$ such that $H_v = R(v)^*$ (in other words, there exists an isomorphism of groups $B_v^* \xrightarrow{\sim} GL_2(F_v)$ inducing an isomorphism $H_v \xrightarrow{\sim} GL_2(\mathcal{O}_{F,v})$).

For such $v \notin S$, we define the **Hecke correspondence** $T(v)$ as

$$T(v) = [Hb_vH] : \ M_H^* \ - - - \twoheadrightarrow M_H^* \ , \tag{1.12.2}$$

for any element $b_v \in R(v) \cap B_v^* \subset B_v^* \subset \widehat{B}^*$ satisfying $\mathrm{ord}_v(nr(b_v)) = 1$. For example, we can fix a uniformizer ϖ_v of $\mathcal{O}_{F,v}$ and take the element b_v which corresponds, under some isomorphism $H_v \xrightarrow{\sim} GL_2(\mathcal{O}_{F,v})$, to the matrix

$$\begin{pmatrix} \varpi_v & 0 \\ 0 & 1 \end{pmatrix}.$$

The **Hecke operator** $T(v)$ is defined as the induced map

$$T(v) := [Hb_vH]^* : \Gamma((M_H^*)^{\mathrm{an}}, \Omega^{\mathrm{an}}) \longrightarrow \Gamma((M_H^*)^{\mathrm{an}}, \Omega^{\mathrm{an}}).$$

According to 1.10, the action of $T(v)$ on $\Gamma((M_H^*)^{\mathrm{an}}, \Omega^{\mathrm{an}}) \xrightarrow{\sim} \mathcal{S}_2^H$ is given by

$$T(v) = [Hb_vH]^* \quad \text{corresponds to} \quad \mathrm{vol}(H)^{-1}\, 1_{Hb_vH}.$$

Combining 1.10 with (1.11.4), we see that the adjoint ${}^tT(v)$ of $T(v)$ with respect to the hermitian scalar product (1.11.1) corresponds to

$$\mathrm{vol}(H)^{-1}\, ({}^t 1_{Hb_vH}) = \mathrm{vol}(H)^{-1}\, 1_{Hb_v^{-1}H} = \mathrm{vol}(H)^{-1}\, [\varpi_v^{-1}] \circ 1_{Hb_vH},$$

hence

$${}^tT(v) = [Hb_v^{-1}H]^* = [\varpi_v^{-1}] \circ T(v) = T(v) \circ [\varpi_v^{-1}] \tag{1.12.3}$$

Fix a prime number ℓ and define

$$W := H^1((M_H^*)^{\mathrm{an}}, \mathbf{Q}), \quad W_{\mathbf{C}} := \Gamma((M_H^*)^{\mathrm{an}}, \Omega^{\mathrm{an}}), \quad W_\ell := H^1_{et}(M_H^* \otimes_F \overline{F}, \mathbf{Q}_\ell), \quad W_{\mathrm{dR}} := H^1_{\mathrm{dR}}(M_H^*/F).$$

The comparison isomorphisms

$$W \otimes_{\mathbf{Q}} \mathbf{C} \xrightarrow{\sim} W_{\mathbf{C}} \oplus \overline{W_{\mathbf{C}}}, \qquad W \otimes_{\mathbf{Q}} \mathbf{Q}_\ell \xrightarrow{\sim} W_\ell \tag{1.12.4}$$

are $\widehat{B}^*$-equivariant, hence $\mathbf{Q}[H\backslash\widehat{B}^*/H]$-equivariant (the second isomorphism is defined by using the embedding $\overline{F} \hookrightarrow \mathbf{C}$ that was fixed in 1.1).

Up to a scalar multiple, the hermitian pairing (1.11.1)

$$W_{\mathbf{C}} \otimes_{\mathbf{C}} \overline{W_{\mathbf{C}}} \longrightarrow \mathbf{C}$$

is equal to the $\mathbf{C}$-linear extension of the cup product

$$(\ ,\ ) : W \otimes_{\mathbf{Q}} W \xrightarrow{\cup} H^2((M_H^*)^{\mathrm{an}}, \mathbf{Q}) \xrightarrow{Tr} \mathbf{Q}(-1)$$

(note that $W_{\mathbf{C}}$ and $\overline{W_{\mathbf{C}}}$ are isotropic subspaces of $W \otimes_{\mathbf{Q}} \mathbf{C}$ with respect to $(\ ,\ ) \otimes_{\mathbf{Q}} \mathbf{C}$). Similarly, $(\ ,\ ) \otimes_{\mathbf{Q}} \mathbf{Q}_\ell$ is identified with the étale cup product

$$(\ ,\ )_\ell : W_\ell \otimes_{\mathbf{Q}_\ell} W_\ell \xrightarrow{\cup} H^2_{et}(M_H^* \otimes_F \overline{F}, \mathbf{Q}_\ell) \xrightarrow{Tr} \mathbf{Q}_\ell(-1).$$

Taking into account (1.12.3), this implies that the adjoint of $T(v) := [Hb_vH]^*$ acting on W (resp., on W_ℓ) with respect to the pairing $(\ ,\ )$ (resp., to $(\ ,\ )_\ell$) is equal to $[\varpi_v^{-1}] \circ T(v) = T(v) \circ [\varpi_v^{-1}]$.

(1.13) Integral models. Integral models of the curves M_H were studied, in an increasing level of generality, by Deligne-Rapoport [De-Ra], Katz-Mazur [Ka-Ma] and Carayol [Ca 1].

Fix a non-archimedean prime $v \notin S_B$ of F; denote by $\mathcal{O}(v)$ the localization of $\mathcal{O}_F$ at v. Assume that $H \subset \widehat{B}^*$ factorizes as $H = H_v H^v$, where H_v (resp., H^v) is an open compact subgroup of B_v^* (resp., of $G(\mathbf{A}_f)^v = \{g \in \widehat{B}^* \mid g_v = 1\}$).

In the classical case $B = M_2(\mathbf{Q})$, the curve M_H is a coarse moduli space of elliptic curves with an H-level structure, for schemes over $\mathrm{Spec}(\mathbf{Q})$. Katz-Mazur [Ka-Ma] extended this moduli problem to schemes over $\mathrm{Spec}(\mathcal{O}(v))$, using the theory of Drinfeld bases. They obtained a regular model $\mathbf{M}_H \longrightarrow \mathrm{Spec}(\mathcal{O}(v))$ of M_H, which they compactified - somewhat artificially - to a regular model $\mathbf{M}_H^*$ of M_H^*, proper over $\mathrm{Spec}(\mathcal{O}(v))$.

Similar techniques apply in the case $F = \mathbf{Q}$, $B \neq M_2(\mathbf{Q})$, when M_H is a coarse moduli space of abelian surfaces with quaternionic multiplication with a suitable level structure [Bu]; one obtains proper regular models $\mathbf{M}_H = \mathbf{M}_H^* \longrightarrow \mathrm{Spec}(\mathcal{O}(v))$ of $M_H = M_H^*$.

If $F \neq \mathbf{Q}$, then M_H has no longer a moduli interpretation, but it can be related to a unitary Shimura curve parametrizing a certain class of abelian varieties of dimension $4[F : \mathbf{Q}]$. Carayol [Ca 1] extended this moduli problem to schemes over $\mathrm{Spec}(\mathcal{O}(v))$ and described, in the case when H^v is *sufficiently small* (this condition depends on H_v), a regular model $\mathbf{M}_H = \mathbf{M}_H^*$ of $M_H = M_H^*$, proper over $\mathrm{Spec}(\mathcal{O}(v))$. If H_v is a maximal open compact subgroup of B_v^*, then $\mathbf{M}_H^*$ is smooth over $\mathrm{Spec}(\mathcal{O}(v))$.

As explained in [Co-Va 2, 3.1.3], Carayol's results [(1)] can be used to construct regular models $\mathbf{M}_H^*$ of M_H^*, proper over $\mathrm{Spec}(\mathcal{O}(v))$, even if H^v is not sufficiently small: fix a sufficiently small open compact normal subgroup H'^v of H^v and put $H' = H_v H'^v \subset \widehat{B}^*$. The right action of the finite group H/H' on $M_{H'}^*$ extends naturally to an $\mathcal{O}(v)$-linear action on $\mathbf{M}_{H'}^*$; one defines $\mathbf{M}_H^*$ as the quotient of $\mathbf{M}_{H'}^*$ by this action of H/H'. The model $\mathbf{M}_H^*$ is regular, proper over $\mathrm{Spec}(\mathcal{O}(v))$, and independent on the choice of H'^v. Taking an additional quotient of $\mathbf{M}_H^*$ by the action of the finite abelian group $\widehat{F}^*/(\widehat{F}^* \cap H)$, we obtain a regular model $\mathbf{N}_H^*$ of N_H^*, proper over $\mathrm{Spec}(\mathcal{O}(v))$. If H_v is a maximal open compact subgroup of B_v^*, then $\mathbf{M}_H^*$ and $\mathbf{N}_H^*$ are again smooth over $\mathrm{Spec}(\mathcal{O}(v))$ (by [Ka-Ma, p. 508]).

(1.14) The Eichler-Shimura congruence relation [Sh 1, Thm. 2.2.3], [Oh, Thm. 3.4.3], [Ca 1, 10.3]. In the situation of (1.12.1), fix $v \notin S$ and a prime number ℓ different from the residue characteristic of v. As H_v is a maximal compact subgroup of B_v^*, the model $\mathbf{M}_H^*$ is proper and smooth over $\mathrm{Spec}(\mathcal{O}(v))$, hence the proper and smooth base change theorems yield a canonical isomorphism

$$W_\ell \xrightarrow{\sim} H^1_{et}(\mathbf{M}_H^{*\circ} \otimes_{\kappa(v)} \overline{\kappa(v)}, \mathbf{Q}_\ell) =: W_\ell^\circ,$$

where $\kappa(v)$ is the residue field of v and $\mathbf{M}_H^{*\circ} = \mathbf{M}_H^* \otimes_{\mathcal{O}(v)} \kappa(v)$ the special fibre of $\mathbf{M}_H^*$. In particular, the natural action of $G_F = \mathrm{Gal}(\overline{F}/F)$ on W_ℓ is unramified at v.

As the diagram (1.9.1) for $g = b_v$ from (1.12.2) naturally extends to the integral models, the graph of the Hecke correspondence $T(v)$ (which is a divisor on $M_H^* \times_F M_H^*$) naturally extends to a divisor on $\mathbf{M}_H^* \times_{\mathcal{O}(v)} \mathbf{M}_H^*$; denote by $T(v)^\circ \subset \mathbf{M}_H^{*\circ} \times_{\kappa(v)} \mathbf{M}_H^{*\circ}$ its special fibre. The generalized **Eichler-Shimura congruence relation** states that

$$T(v)^\circ = \Gamma_\varphi + \Gamma_{[\varpi_v \cdot]} \circ {}^t\Gamma_\varphi, \tag{1.14.1}$$

where Γ_φ denotes the graph of the Frobenius morphism $\varphi = \varphi_v : \mathbf{M}_H^{*\circ} \longrightarrow \mathbf{M}_H^{*\circ}$ and ${}^t\Gamma_\varphi$ its transpose. As the contravariant action of Γ_φ (resp., of ${}^t\Gamma_\varphi$) on W_ℓ° coincides with the Galois action of $F = \mathrm{Fr}(v)_{\mathrm{geom}}$ (resp., with the action of ${}^tF = (Nv)F^{-1}$), it follows that

$$(1 - XF)(1 - X[\varpi_v](Nv)F^{-1}) = 1 - XT(v) + X^2(Nv)[\varpi_v] \in \mathrm{End}_{\mathbf{Q}_\ell}(W_\ell^\circ)[X].$$

As $[\varpi_v](Nv)F^{-1}$ is the adjoint of F with respect to the pairing $(\ ,\ )_\ell$, it follows from (1.12.4) and the compatibility of the various pairings discussed in 1.12 that

$$\det(1 - XF \mid W_\ell^\circ) = \det(1 - XT(v) + X^2(Nv)[\varpi_v] \mid W_{\mathbf{C}}). \tag{1.14.2}$$

[(1)] Note that Carayol [Ca 1,2] uses different sign conventions. This is discussed in detail in [Co-Va 2, 3.3.1].

For the curve N_H^* and its model $\mathbf{N}_H^*$, the congruence relation (1.14.1) simplifies ([Zh 1, Prop. 1.4.10]) to

$$T(v)^\circ = \Gamma_\varphi + {}^t\Gamma_\varphi. \tag{1.14.3}$$

(1.15) The L-function of M_H^*. Combining the discussion from 1.14 (the notations and assumptions of which are still in force) with the decomposition (1.7.1), we obtain

$$W_{\mathbf{C}} \xrightarrow{\sim} \mathcal{S}_2^H \xrightarrow{\sim} \bigoplus_{\pi=\sigma_2\otimes\pi_f} \pi_f^H.$$

If $\pi = \sigma_2 \otimes \pi_f = \otimes_v' \pi_v$ is an irreducible unitary cuspidal automorphic representation of $B_{\mathbf{A}}^*$ with $\pi_f^H \neq 0$, then $T(v)$ acts on the one-dimensional space $\pi_v^{H_v}$ of spherical vectors (recall that $v \notin S$, by assumption) by a scalar $\lambda_\pi(v) \in \mathbf{C}$. The relation (1.14.2) then gives a formula for the local Euler factor

$$L_v(h^1(M_H^*), s) := \det(1 - (Nv)^{-s}\,\mathrm{Fr}(v)_{\mathrm{geom}} \mid W_\ell^{I_v})^{-1},$$

namely

$$L_v(h^1(M_H^*), s) = \prod_{\pi=\sigma_2\otimes\pi_f} (1 - \lambda_\pi(v)(Nv)^{-s} + \omega_\pi(v)(Nv)^{1-2s})^{-\dim(\pi_f^H)} = \prod_{\pi=\sigma_2\otimes\pi_f} L_v(\pi, s-1/2)^{\dim(\pi_f^H)}, \tag{1.15.1}$$

where $\omega_\pi : \mathbf{A}_F^*/F^* \longrightarrow \mathbf{C}^*$ denotes the central character (of finite order) of π. Taking a product of (1.15.1) over all $v \notin S$, we obtain an equality of partial L-functions

$$L^S(h^1(M_H^*), s) = \prod_{\pi=\sigma_2\otimes\pi_f} L^S(\pi, s-1/2)^{\dim(\pi_f^H)}, \tag{1.15.2}$$

where

$$L^S(h^1(M_H^*), s) = \prod_{v\notin S} L_v(h^1(M_H^*), s), \qquad L^S(\pi, s) = \prod_{v\notin S} L_v(\pi, s).$$

Above, the automorphic L-functions are normalized as in [Ja-La] (the centre of symmetry of the functional equation lies at $s = 1/2$).

It is a much deeper fact that the extreme left and right terms in (1.15.1) are equal even for $v \in S$. For $v \in S - S_B$ this is proved in [Ca 2]; for $v \in S_B$ one can reduce to the previous case by switching to a quaternion algebra unramified at v (possibly after a cyclic base change to a suitable totally real number field in which v splits completely).

The Jacquet-Langlands correspondence [Ja-La, §14] associates to each (irreducible, cuspidal) $\pi = \sigma_2 \otimes \pi_f$ with $\pi_f^H \neq 0$ an irreducible cuspidal representation $JL(\pi)$ of $GL_2(\mathbf{A}_F)$, which corresponds to a Hilbert modular newform of weight $(2, \ldots, 2)$ and central character ω_π. This representation is characterized by the property

$$(\forall w \notin Ram(B))\ \ JL(\pi)_w \xrightarrow{\sim} \pi_w \ \text{ as representations of } \ GL_2(F_w) \xrightarrow{\sim} B_w^* \quad (\Longrightarrow\ L_w(JL(\pi), s) = L_w(\pi, s))$$

(where w is a prime of F). In particular,

$$L^S(JL(\pi), s) = L^S(\pi, s).$$

In fact, the equality $L_w(JL(\pi), s) = L_w(\pi, s)$ holds also for $w \in Ram(B)$ ([Ja-La], Rmk. before Thm. 14.4).

(1.16) The Jacobian of M_H^* and N_H^*. As in [Co-Va 1, 3.3], we define the Jacobian of M_H^* (resp., N_H^*) to be the abelian variety over F

$$J(M_H^*) := \mathrm{Pic}^\circ(M_H^*/F) = \mathrm{Res}_{F(\mathcal{M}_H)/F}\left(\mathrm{Pic}^\circ(M_H^*/F(\mathcal{M}_H))\right)$$
$$J(N_H^*) := \mathrm{Pic}^\circ(N_H^*/F) = \mathrm{Res}_{F(\mathcal{N}_H)/F}\left(\mathrm{Pic}^\circ(N_H^*/F(\mathcal{N}_H))\right)$$

(recall that $F(\mathcal{M}_H)$ (resp., $F(\mathcal{N}_H)$) denotes the field of constants of M_H^* (resp., of N_H^*)).

As $\mathrm{Pic}^\circ(-/F)$ is both covariant and contravariant for finite flat morphisms of proper smooth curves over $\mathrm{Spec}(F)$, each diagram (1.9.1) induces morphisms of abelian varieties

$$[HgH']_* = [H'g^{-1}H]^* : J(M_H^*) \longrightarrow J(M_{H'}^*), \qquad [HgH']^* = [H'g^{-1}H]_* : J(M_{H'}^*) \longrightarrow J(M_H^*) \tag{1.16.1}$$

(and similarly for N_H^*). Each Jacobian $J(M_H^*)$ has a canonical principal polarization. It follows from (1.16.1) that the corresponding Rosati involution ι acts by

$$\iota\left([HgH]_*\right) = [HgH]^* = [Hg^{-1}H]_*, \qquad \iota\left([HgH]^*\right) = [HgH]_* = [Hg^{-1}H]^*. \tag{1.16.2}$$

One can consider (1.16.2) as a "motivic" version of (1.11.3).

We let the Hecke correspondences act on the Jacobians *covariantly*. As $[\cdot g] \circ [\cdot g'] = [\cdot g'g]$, the map

$$\begin{array}{ccc} \mathbf{Z}[H\backslash\widehat{B}^*/H]^{\mathrm{op}} & \longrightarrow & \mathrm{End}(J(M_H^*)) \\ [HgH] & \mapsto & [HgH]_* \end{array} \tag{1.16.3}$$

is a ring homomorphism (recall that the multiplication on $\mathbf{Z}[H\backslash\widehat{B}^*/H]$ used here is the opposite of the one considered in [Co-Va 1, 3.4, 3.11]).

The space $\Gamma((M_H^*)^{\mathrm{an}}, \Omega^{\mathrm{an}})$ is canonically isomorphic to the cotangent space $(T_0 J(M_H^*)^{\mathrm{an}})^\vee$ of the complex torus $J(M_H^*)^{\mathrm{an}}$ at the origin. For each Hecke correspondence $[HgH'] : M_H^* - - - \succ M_{H'}^*$, the induced map

$$[HgH']^* : \Gamma((M_{H'}^*)^{\mathrm{an}}, \Omega^{\mathrm{an}}) \longrightarrow \Gamma((M_H^*)^{\mathrm{an}}, \Omega^{\mathrm{an}})$$

corresponds to the dual of the differential of the morphism

$$[HgH']_* : J(M_H^*) \longrightarrow J(M_{H'}^*)$$

at the origin.

(1.17) The "physical" Hecke algebra. In the situation of (1.12.1), the spherical Hecke algebra

$$\mathbf{T}_H^S := \mathbf{Z}[H^S\backslash G(\mathbf{A}_f)^S/H^S] \subset \mathbf{Z}[H\backslash\widehat{B}^*/H]$$

is commutative; we let it act on the Jacobian $J(M_H^*)$ by the rule (1.16.3), which defines a ring homomorphism

$$\theta : \mathbf{T}_H^S = \left(\mathbf{T}_H^S\right)^{\mathrm{op}} \subset \mathbf{Z}[H\backslash\widehat{B}^*/H]^{\mathrm{op}} \longrightarrow \mathrm{End}(J(M_H^*)). \tag{1.17.1}$$

As a ring, $\mathbf{T}_H^S$ is generated by the double cosets $[Hb_vH]$ and $[H\varpi_v^{\pm 1}H]$ ($v \notin S$), where b_v is as in 1.12. For each $v \notin S$, the endomorphisms

$$T(v) := \theta([Hb_vH]), \qquad [\varpi_v^{\pm 1}] := \theta([H\varpi_v^{\pm 1}H])$$

of $J(M_H^*)$ induce the eponymous endomorphisms of $\Gamma((M_H^*)^{\mathrm{an}}, \Omega^{\mathrm{an}})$ (which were defined in 1.12)) via the contravariant action on the cotangent space at the origin. In other words, the action of $\mathbf{T}_H^S$ on $\mathcal{S}_2^H \xrightarrow{\sim} \Gamma((M_H^*)^{\mathrm{an}}, \Omega^{\mathrm{an}})$ factors through the morphism θ. Similarly, we let $T(v)$ and $[\varpi_v^{\pm 1}]$ act on the spaces W, W_{dR} and W_ℓ defined in 1.12 by contravariant functoriality, i.e. by $[Hb_vH]^*$ and $[H\varpi_v^{\pm 1}H]^*$.

The commutative ring

$$\mathbf{T} := \theta\left(\mathbf{T}_H^S\right) \subset \mathrm{End}(J(M_H^*))$$

(the "physical" Hecke algebra) is a free $\mathbf{Z}$-module of finite rank, generated (as a ring) by the endomorphisms $T(v)$ and $[\varpi_v^{\pm 1}]$ (for $v \notin S$). It follows from (1.16.2) that

$$(\forall v \notin S) \qquad \iota\,(T(v)) = [\varpi_v^{-1}]\,T(v), \qquad \iota\left([\varpi_v^{\pm 1}]\right) = [\varpi_v^{\mp 1}], \tag{1.17.2}$$

hence $\mathbf{T}$ is a commutative subring of $\mathrm{End}(J(M_H^*))$ stable by the Rosati involution ι. The positivity property of this involution implies ([Mu, §21]) that the $\mathbf{Q}$-algebra $\mathbf{T} \otimes \mathbf{Q}$ is isomorphic to a finite product of number fields

$$\mathbf{T} \otimes \mathbf{Q} \xrightarrow{\sim} \prod_{j \in J} L_j, \qquad J = J_1 \cup J_2,$$

where each factor L_j is ι-stable and

$$\begin{aligned} &(\forall j \in J_1) \qquad L_j \text{ is totally real and } \iota \text{ acts trivially on } L_j \\ &(\forall j \in J_2) \qquad L_j \text{ is a CM field and } \iota \text{ acts on } L_j \text{ by complex conjugation.} \end{aligned} \tag{1.17.3}$$

For each $j \in J$, we denote by θ_j the ring homomorphism

$$\theta_j : \mathbf{T}_H^S \xrightarrow{\theta} \mathbf{T} \subset \mathbf{T} \otimes \mathbf{Q} \twoheadrightarrow L_j. \tag{1.17.4}$$

The image of θ_j is an order in L_j and $\mathbf{T}$ has finite index in $\prod_j \mathrm{Im}(\theta_j)$.

If $\pi = \sigma_2 \otimes \pi_f$ is an irreducible cuspidal unitary representation of $B_{\mathbf{A}}^*$ satisfying $\pi_f^H \neq 0$, then $\mathbf{T}_H^S$ acts on π_f^H through a ring homomorphism $\lambda_\pi : \mathbf{T}_H^S \longrightarrow \mathbf{C}$, which factors as

$$\lambda_\pi : \mathbf{T}_H^S \xrightarrow{\theta_j} L_j \overset{\sigma}{\hookrightarrow} \mathbf{C},$$

for a unique pair $(j, \sigma) \in J \times \mathrm{Hom}(L_j, \mathbf{C})$. The strong multiplicity one theorem for automorphic representations of $B_{\mathbf{A}}^*$ ([Ge], VI.2) implies that

$$\left[\pi = \sigma_2 \otimes \pi_f \neq \pi' = \sigma_2 \otimes \pi'_f,\ \pi_f^H \neq 0 \neq \pi_f'^H \implies \lambda_\pi \neq \lambda_{\pi'}.\right] \tag{1.17.5}$$

The canonical map $J(M_H^*) \longrightarrow J(N_H^*)$ (induced by the projection $M_H^* \longrightarrow N_H^*$) is T_H^S-equivariant and surjective; it follows that $T_H^S \otimes \mathbf{Q}$ acts on $J(N_H^*) \otimes \mathbf{Q}$ (in the category of abelian varieties up to isogeny) by a certain quotient of $\mathbf{T} \otimes \mathbf{Q}$.

Let ℓ be a prime number. For each prime $\mathscr{L} \mid \ell$ of L_j, denote by $V_{\mathscr{L}}(\theta_j)$ the $\mathscr{L}$-adic Galois representation of $G_{F,S}$ associated to $JL(\pi)$ (which is a Hilbert modular form of parallel weight $(2, \ldots, 2)$ over F). This is a two-dimensional, absolutely irreducible ([Tay, Prop. 3.1]) representation of $G_{F,S}$ over $(L_j)_{\mathscr{L}}$, characterized by the property

$$(\forall v \notin S) \qquad \det(1 - X\,\mathrm{Fr}(v)_{\mathrm{geom}} \mid V_{\mathscr{L}}(\theta_j)) = 1 - \theta_j(T(v))X + \omega_\pi(v)(Nv)X^2.$$

(1.18) Proposition (Decomposition of $J(M_H^*)$ and $J(N_H^*)$ up to isogeny). (i) *For each pair $(j, \sigma) \in J \times \mathrm{Hom}(L_j, \mathbf{C})$ there exists a unique irreducible cuspidal unitary representation $\pi = \sigma_2 \otimes \pi_f$ of $B_{\mathbf{A}}^*$ satisfying $\pi_f^H \neq 0$, $\lambda_\pi = \sigma \circ \theta_j$. We denote $\pi = \pi(\sigma \circ \theta_j)$.*

(ii) *For each prime number ℓ, the $\mathbf{T} \otimes \mathbf{Q}_\ell[G_F]$-module $W_\ell = H^1_{et}(M_H^* \otimes_F \overline{F}, \mathbf{Q}_\ell)$ is isomorphic to*

$$W_\ell \xrightarrow{\sim} \bigoplus_{j \in J} \Big(\bigoplus_{\mathscr{L} \mid \ell} V_{\mathscr{L}}(\theta_j) \Big)^{a_j},$$

where $a_j = \dim_{\mathbf{C}}(\pi(\sigma \circ \theta_j)_f^H) \geq 1$, $\mathscr{L}$ runs through all primes of L_j above ℓ, and $\mathbf{T}$ acts on $V_{\mathscr{L}}(\theta_j)$ via θ_j and the embedding $L_j \hookrightarrow (L_j)_{\mathscr{L}}$.

(iii) *There exists a $\mathbf{T}$-linear isogeny $u : J(M_H^*) \longrightarrow \prod_{j \in J} A_j^{a_j}$ defined over F, where each $a_j \geq 1$ is as in (ii), A_j is an abelian variety over F of dimension $\dim(A_j) = [L_j : \mathbf{Q}]$ satisfying $\mathcal{O}_{L_j} = \mathrm{End}_F(A_j)$ (hence A_j is*

F-simple) on which $\mathbf{T}$ acts via θ_j, $H^1_{et}(A_j \otimes_F \overline{F}, \mathbf{Q}_\ell)$ is isomorphic to $\bigoplus_{\mathscr{L}|\ell} V_{\mathscr{L}}(\theta_j)$ as an $\mathbf{T} \otimes \mathbf{Q}_\ell[G_F]$-module and there is an equality of L-series (Euler factor by Euler factor)

$$L(A_j/F, s) = \prod_{\sigma: L_j \hookrightarrow \mathbf{C}} L(\pi(\sigma \circ \theta_j), s - 1/2).$$

The abelian variety A_j is unique up to an $\mathcal{O}_{L_j}$-linear isogeny.
(iv) *If $j, j' \in J$, $j \neq j'$, then A_j is not isogeneous (over F) to $A_{j'}$.*
(v) *For each $j \in J_1$ (resp., $j \in J_2$) and each polarization of A_j defined over F, the corresponding Rosati involution acts on $L_j = \mathrm{End}_F(A_j) \otimes \mathbf{Q}$ trivially (resp., by the complex conjugation).*
(vi) *There exists a $\mathbf{T}$-linear isogeny $u_1 : J(N_H^*) \longrightarrow \prod_{j \in J_1} A_j^{a_j}$ (defined over F) fitting into a commutative diagram (in which the right vertical arrow is the canonical projection)*

$$\begin{array}{ccc} J(M_H^*) & \xrightarrow{u} & \prod_{j \in J} A_j^{a_j} \\ \big\downarrow & & \big\downarrow \\ J(N_H^*) & \xrightarrow{u_1} & \prod_{j \in J_1} A_j^{a_j}. \end{array}$$

Proof. All statements are well-known, but as we are not aware of a good reference, we sketch the argument. In (i), the uniqueness is a consequence of (1.17.5). In order to prove the existence of π, note that $W = H^1(M_H^*, \mathbf{Q})$ is a faithful $\mathbf{T} \otimes \mathbf{Q}$-module, hence it is isomorphic to

$$W \xrightarrow{\sim} \bigoplus_{j \in J} L_j^{\oplus b_j} \qquad (b_j > 0). \tag{1.18.1}$$

Both comparison isomorphisms

$$W \otimes_{\mathbf{Q}} \mathbf{C} \xrightarrow{\sim} W_{\mathbf{C}} \oplus \overline{W_{\mathbf{C}}}, \qquad W_{\mathrm{dR}} \otimes_{F,\tau_1} \mathbf{C} \xrightarrow{\sim} W_{\mathbf{C}}$$

(where $W_{\mathbf{C}} = \Gamma((M_H^*)^{\mathrm{an}}, \Omega^{\mathrm{an}})$ and $W_{\mathrm{dR}} = H^1_{\mathrm{dR}}(M_H^*/F)$) are $\mathbf{T} \otimes \mathbf{C}$-linear. As $\tau_1(F) \subset \mathbf{R}$, the second one implies that the $\mathbf{T} \otimes \mathbf{C}$-modules $W_{\mathbf{C}}$ and $\overline{W_{\mathbf{C}}}$ are isomorphic, which yields an isomorphism of $\mathbf{T} \otimes \mathbf{C}$-modules

$$W_{\mathbf{C}} \xrightarrow{\sim} \bigoplus_{j \in J} (L_j \otimes_{\mathbf{Q}} \mathbf{C})^{\oplus a_j}, \qquad a_j = b_j/2 > 0.$$

The isomorphism

$$L_j \otimes_{\mathbf{Q}} \mathbf{C} \xrightarrow{\sim} \prod_{\sigma: L_j \hookrightarrow \mathbf{C}} \mathbf{C}, \qquad a \otimes z \mapsto (\sigma(a)z)_\sigma$$

implies that each morphism $\sigma \circ \theta_j$ occurs as λ_π in $W_{\mathbf{C}}$, with multiplicity $a_j > 0$. In other words, $\pi(\sigma \circ \theta_j)$ exists and

$$\dim_{\mathbf{C}} \pi(\sigma \circ \theta_j)_f^H = a_j.$$

(ii) As W_ℓ is a semi-simple $\mathbf{Q}_\ell[G_F]$-module ([Fa, Satz 3]), it is sufficient to show that the traces of $\mathrm{Fr}(v)_{\mathrm{geom}}$ ($v \notin S$) acting on both sides coincide, which follows from the $\mathbf{T} \otimes \mathbf{Q}_\ell$-linear comparison isomorphism $W \otimes_{\mathbf{Q}} \mathbf{Q}_\ell \xrightarrow{\sim} W_\ell$ and the formulas (1.14.2) and (1.18.1).
(iii) The existence of a $\mathbf{T}$-linear isogeny $J(M_H^*) \longrightarrow \prod_{j \in J} A_j^{a_j}$ (defined over F) such that $L_j \hookrightarrow \mathrm{End}_F(A_j) \otimes \mathbf{Q}$, $\mathbf{T}$ acts on A_j via θ_j and $H^1_{et}(A_j \otimes_F \overline{F}, \mathbf{Q}_\ell)$ is isomorphic to $\bigoplus_{\mathscr{L}|\ell} V_{\mathscr{L}}(\theta_j)$ follows from (ii) and Faltings' isogeny theorem [Fa, Satz 4] (formerly known as Tate's conjecture). The endomorphism ring $\mathrm{End}_F(A_j)$ contains $\mathrm{Im}(\theta_j)$, which is an order in L_j. Replacing A_j by the F-isogeneous abelian variety $\mathrm{Hom}_{\mathrm{Im}(\theta_j)}(\mathcal{O}_{L_j}, A_j)$ (see [Co, Ch. 10] for a discussion of the formalism of $\mathcal{O}$-transforms), we may assume that $\mathrm{End}_F(A_j)$ contains $\mathcal{O}_{L_j}$.

Fix a prime number ℓ which splits in $L_j/\mathbf{Q}$. If $\mathscr{L}$ and $\mathscr{L}'$ are distinct primes above ℓ in L_j, then the $\mathbf{Q}_\ell[G_F]$-modules $V_{\mathscr{L}}(\theta_j)$ and $V_{\mathscr{L}'}(\theta_j)$ are not isomorphic, as L_j is generated (as a field extension of $\mathbf{Q}$) by the traces $\theta_j(T(v))$ and determinants $\omega_\pi(v)$ of the Frobenius elements $\mathrm{Fr}(v)_{\mathrm{geom}}$ ($v \notin S$) acting on $V_{\mathscr{L}}(\theta_j)$ (as well as on $V_{\mathscr{L}'}(\theta_j)$), and the two embeddings $L_j \hookrightarrow (L_j)_{\mathscr{L}}$, $L_j \hookrightarrow (L_j)_{\mathscr{L}'}$ are distinct. Absolute irreducibility of $V_{\mathscr{L}}(\theta_j)$ yields an inclusion

$$L_j \otimes_{\mathbf{Q}} \mathbf{Q}_\ell \hookrightarrow \mathrm{End}_F(A_j) \otimes_{\mathbf{Q}} \mathbf{Q}_\ell = \mathrm{End}_{\mathbf{Q}_\ell[G_F]}\Big(\bigoplus_{\mathscr{L}|\ell} V_{\mathscr{L}}(\theta_j)\Big) = \bigoplus_{\mathscr{L}|\ell} \mathbf{Q}_\ell, \tag{1.18.2}$$

which must be an equality, by comparing the dimensions of the two flank terms; this proves that $L_j = \mathrm{End}_F(A_j) \otimes \mathbf{Q}$. As $\mathcal{O}_{L_j} \subset \mathrm{End}_F(A_j)$, we must have $\mathrm{End}_F(A_j) = \mathcal{O}_{L_j}$; as its endomorphism ring is an integral domain, the abelian variety A_j is F-simple. The statement about the local L-factor $L_v(A_j/F, s)$ follows from (1.15.2) (resp., the discussion following (1.15.2)) if $v \in S$ (resp., if $v \notin S$), combined with (i) and (ii), since $L_v(h^1(M_H^*), s) = L_v(J(M_H^*), s)$. The uniqueness of A_j (up to an $\mathcal{O}_{L_j}$-linear isogeny) follows from Faltings' isogeny theorem and the equality in (1.18.2).

(iv) The same argument as in the proof of (iii) shows that, if ℓ is a prime number split in both L_j and $L_{j'}$ and $\mathscr{L}, \mathscr{L}'$ are primes above ℓ in $L_j, L_{j'}$, respectively, (not necessarily distinct), then the $\mathbf{Q}_\ell[G_F]$-modules $V_{\mathscr{L}}(\theta_j)$ and $V_{\mathscr{L}'}(\theta_{j'})$ are not isomorphic, hence A_j is not isogeneous to $A_{j'}$ (over F).

(v) As $\mathrm{End}_F(A_j)$ is commutative, the Rosati involution does not depend on the polarization. For the canonical polarization, the statement follows from (1.17.3).

(vi) $\mathbf{T}_H^S \otimes \mathbf{Q}$ acts on $J(N_H^*) \otimes \mathbf{Q}$ through a certain quotient $\mathbf{T}' \otimes \mathbf{Q}$ of $\mathbf{T} \otimes \mathbf{Q}$, which is necessarily isomorphic to $\prod_{j \in J'}$, for some subset $J' \subset J$. As $\Gamma((N_H^*)^{\mathrm{an}}, \Omega^{\mathrm{an}}) \xrightarrow{\sim} \mathcal{S}_2^{H\widehat{F}^*}$ consists precisely of those automorphic forms from $\mathcal{S}_2^H$ which have trivial central character, the formula (1.17.2) implies that the Rosati involution acts trivially on $\mathbf{T}' \otimes \mathbf{Q}$, hence $J' \subset J_1$. The arguments used in the proof of (i), (ii) show that $J(N_H^*)$ is $\mathbf{T}$-linearly isogeneous to $\prod_{j \in J'} A_j^{a_j'}$, where

$$(\forall j \in J')\,(\forall \sigma : L_j \hookrightarrow \mathbf{C}) \qquad a_j' = \dim_{\mathbf{C}} \pi(\sigma \circ \theta_j)_f^{H\widehat{F}^*} > 0.$$

In particular, for each pair $(j, \sigma) \in J' \times \mathrm{Hom}(L_j, \mathbf{C})$, the representation $\pi(\sigma \circ \theta_j)$ satisfies $\pi(\sigma \circ \theta_j)_f^{H\widehat{F}^*} \neq 0$, hence it has trivial central character, which in turn implies that

$$a_j' = \dim_{\mathbf{C}} \pi(\sigma \circ \theta_j)_f^{H\widehat{F}^*} = \dim_{\mathbf{C}} \pi(\sigma \circ \theta_j)_f^{H} = a_j.$$

Conversely, if $j \in J_1$, then the existence of the Weil pairing implies that $G_{F,S}$ acts on $\Lambda^2 V_{\mathscr{L}}(\theta_j)$ by the cyclotomic character ([Cas, Cor. 5.5]; [Ri, Lemma 4.5.1]), hence $\omega_\pi = 1$. It follows that $J' = J_1$.

(1.19) The maps $M_H^* \longrightarrow J(M_H^*)$ and $N_H^* \longrightarrow J(N_H^*)$. In the classical case $B = M_2(\mathbf{Q})$, the class of the divisor (∞) in $\mathrm{Pic}(M_H^*)$ has the following properties: its pull-back to each irreducible component of $M_H^* \otimes_{\mathbf{Q}} \overline{\mathbf{Q}}$ has degree one and there exists an integer $m \geq 1$ such that each Hecke operator $[HbH]_*$ acts on the class of $m(\infty)$ by multiplication by its degree. Indeed, we can take any m that annihilates the cuspidal group $C(M_H^*) \subset \mathrm{Pic}(M_H^*)$, which is defined as the subgroup generated by the divisors whose pull-backs to each irreducible component of $M_H^* \otimes_{\mathbf{Q}} \overline{\mathbf{Q}}$ have degree zero and are supported at the cusps. The group $C(M_H^*)$ is finite by the theorem of Manin-Drinfeld [Dr].

For $B \neq M_2(\mathbf{Q})$, Zhang [Zh 1, Introduction] (see also [Co-Va 1, 3.5]) constructed a certain class $\xi(M_H^*) \in \mathrm{Pic}(M_H^*/F) \otimes \mathbf{Q}$ ("the Hodge class") such that the degree of the pull-back of $\xi(M_H^*)$ to each irreducible component of $M_H^* \otimes_F \overline{F}$ is equal to one. More precisely, $\xi(M_H^*)$ is constructed, for a suitable integer $m \geq 1$, as $\widetilde{\xi(M_H^*)} = \widetilde{m\xi(M_H^*)} \otimes 1/m$, where $\widetilde{m\xi(M_H^*)} \in \mathrm{Pic}(M_H^*/F)$ has degree m on each irreducible component of $M_H^* \otimes_F \overline{F}$ and each Hecke operator $[HbH]_*$ acts on it by multiplication by its degree ([Co-Va 1], Remark 3.7).

In general, if

$$M_H^* \otimes_F \overline{F} = \coprod_\alpha \mathcal{C}_\alpha$$

is the decomposition into irreducible components, let $m\delta_\alpha \in \mathrm{Pic}(\mathcal{C}_\alpha)$ be the pull-back to $\mathrm{Pic}(\mathcal{C}_\alpha)$ of the class of $m(\infty)$ (resp., of $m\widetilde{\xi(M_H^*)}$) if $B = M_2(\mathbf{Q})$ (resp., if $B \neq M_2(\mathbf{Q})$). We denote by

$$\iota : M_H^* \longrightarrow J(M_H^*)$$

the morphism (defined over F), which is characterized by the formula

$$(\forall \alpha)\,(\forall P \in \mathcal{C}_\alpha(\overline{F})) \qquad \iota(P) = m(P) - m\delta_\alpha.$$

The same discussion applies to the curves N_H^*; we obtain a morphism

$$\iota : N_H^* \longrightarrow J(N_H^*).$$

2. CM points

In this section we recall basic properties of CM points on the curves M_H and N_H. We follow the notation and conventions of Sect. 1.

(2.1) Let K be a totally imaginary quadratic extension of F such that each prime $v \in S_B$ either ramifies or is inert in K/F. This assumption implies that there exists an F-embedding (= an injective homomorphism of F-algebras) $t : K \hookrightarrow B$; we fix such an embedding and denote by $t_v : K \otimes_F F_v \hookrightarrow B_v$ (resp., by $\widehat{t} : \widehat{K} \hookrightarrow \widehat{B}$) the induced embedding of the completions (resp., of the finite adèles). As in 1.1, we fix an embedding $\overline{K} \hookrightarrow \mathbf{C}$ extending $\tau_1 : F \longrightarrow \mathbf{R}$.

(2.2) Lemma. (i) *There exists a unique point $z \in \mathbf{C}$ with $\mathrm{Im}(z) > 0$, which is fixed by the action of $t(K^*) \subset B^* \subset B_{\tau_1}^* \xrightarrow{\sim} GL_2(\mathbf{R})$.*
(ii) *We have $\{\lambda \in B^* \mid \lambda(z) = z\} = t(K^*)$.*

Proof. Easy exercise.

(2.3) Definition. *The set of* **CM-points by** *K on the curve M_H (resp., on N_H) is the set*

$$CM(M_H, K) = \{x = [z, b] \in M_H(\mathbf{C}) \mid b \in \widehat{B}^*\}$$
$$CM(N_H, K) = \{x = [z, b] \in N_H(\mathbf{C}) \mid b \in \widehat{B}^*\} = \text{ the image of } CM(M_H, K) \text{ in } N_H(\mathbf{C})$$

(these sets do not depend on the choice of t, as two different F-embeddings of K into B are conjugate by an element of B^*, by the Skolem-Noether theorem).

(2.4) The Galois action on CM-points. The reciprocity law [De, 3.9], [Mi 2, II.5.1] (with the sign corrected, [Mi 3, 1.10]) states that $CM(M_H, K) \subset M_H(K^{ab})$ and that the Galois action of $\mathrm{Gal}(K^{ab}/K)$ on $CM(M_H, K)$ is described, via the reciprocity map $\mathrm{rec}_K : \widehat{K}^* \longrightarrow \mathrm{Gal}(K^{ab}/K)$, by the following formula:

$$(\forall a \in \widehat{K}^*) \qquad \mathrm{rec}_K(a)\,[z, b] = [z, \widehat{t}(a)b].$$

(2.5) Proposition. *Denote by $K(x) \subset K^{ab}$ the field of definition over K of a CM point (by K) $x = [z, b]$ on the curve M_H (resp., on N_H). Then the reciprocity map rec_K induces an isomorphism $\mathrm{rec}_K : K^*\backslash\widehat{K}^*/\widehat{t}^{-1}(bHb^{-1}) \xrightarrow{\sim} \mathrm{Gal}(K(x)/K)$ (resp., $\mathrm{rec}_K : K^*\backslash\widehat{K}^*/\widehat{t}^{-1}(bH\widehat{F}^*b^{-1}) \xrightarrow{\sim} \mathrm{Gal}(K(x)/K)$).*

Proof. If $x = [z, b] \in CM(M_H, K)$ and $a \in \widehat{K}^*$, then we deduce from 2.4 and Lemma 2.2(ii) that

$$\begin{aligned}
\mathrm{rec}_K(a)\,[z, b] = [z, b] &\iff (\exists \lambda \in B^*)\,(\exists h \in H) \qquad (z, \widehat{t}(a)b) = (\lambda(z), \lambda bh) \in (\mathbf{C} - \mathbf{R}) \times \widehat{B}^* \\
&\iff (\exists \mu \in K^*)\,(\exists h \in H) \qquad \widehat{t}(a)b = t(\mu)bh \\
&\iff a \in K^* \cdot \widehat{t}^{-1}(bHb^{-1}).
\end{aligned}$$

The proof for $x \in CM(N_H, K)$ is similar.

(2.6) Ring class fields of K

(2.6.1) From now on, we shall consider only CM points on the curves N_H. For such a point $x = [z, b]$, the formula from Proposition 2.5 can be restated as an isomorphism

$$\mathrm{rec}_K : \widehat{K}^*/K^*\widehat{F}^*Z \xrightarrow{\sim} \mathrm{Gal}(K(x)/K),$$

where $Z = \widehat{t}^{-1}(bH\widehat{\mathcal{O}}_F^* b^{-1}) \subset \widehat{\mathcal{O}}_K^*$ is an open (compact) subgroup of $\widehat{\mathcal{O}}_K^*$ containing $\widehat{\mathcal{O}}_F^*$.

(2.6.2) In the special case when $H = \widehat{R}^*$, for an $\mathcal{O}_F$-order $R \subset B$, then $Z = \widehat{\mathcal{O}}^*$ for some $\mathcal{O}_F$-order $\mathcal{O} \subset K$. Such an order is necessarily of the form $\mathcal{O}_c = \mathcal{O}_F + c\mathcal{O}_K$, where $c \subset \mathcal{O}_F$ is a non-zero ideal of $\mathcal{O}_F$. The corresponding abelian extension $K[c]/K$ satisfying

$$\mathrm{rec}_K : \widehat{K}^*/K^*\widehat{F}^*\widehat{\mathcal{O}}_c^* \xrightarrow{\sim} \mathrm{Gal}(K[c]/K)$$

is called the **ring class field of K of conductor** c (note that Zhang [Zh 2] uses the same terminology, but Cornut and Vatsal [Co-Va 1,2] consider a slightly more general class of extensions).

If $c, c' \subset \mathcal{O}_F$ are non-zero ideals, then we have

$$\widehat{\mathcal{O}}_c^* \cdot \widehat{\mathcal{O}}_{c'}^* = \widehat{\mathcal{O}}_{\gcd(c,c')}^*, \qquad K^*\widehat{F}^*\widehat{\mathcal{O}}_c^* \cap K^*\widehat{F}^*\widehat{\mathcal{O}}_{c'}^* \supseteq K^*\widehat{F}^*\widehat{\mathcal{O}}_{\mathrm{lcm}(c,c')}^*, \tag{2.6.2.1}$$

hence

$$K[c] \cap K[c'] = K[\gcd(c, c')], \qquad K[c]\,K[c'] \subseteq K[\mathrm{lcm}(c, c')].$$

(2.6.3) Each prime of K not dividing $c\mathcal{O}_K$ is unramified in $K[c]/K$. If ℓ is a prime of F which does not divide c and which is inert in K/F, then $\ell\mathcal{O}_K$ splits completely in $K[c]/K$ and each prime above ℓ is totally tamely ramified in $K[c\ell]/K[c]$.

(2.6.4) In general, if $Z \subset \widehat{\mathcal{O}}_K^*$ is an open subgroup containing $\widehat{\mathcal{O}}_F^*$, we denote by $K_Z \subset K^{ab}$ the finite abelian extension of K satisfying

$$\mathrm{rec}_K : \widehat{K}^*/K^*\widehat{F}^*Z \xrightarrow{\sim} \mathrm{Gal}(K_Z/K).$$

It follows from the last paragraph in 1.4 and from Proposition 2.5 that we have

$$\bigcup_Z K_Z = \bigcup_c K[c] =: K[\infty], \qquad CM(N_H, K) \subset N_H(K[\infty]).$$

(2.6.5) The reciprocity map rec_K is compatible with the action of $\mathrm{Gal}(K/F) = \{1, \rho\}$ (where ρ denotes the complex conjugation on $\overline{K} \subset \mathbf{C}$) on both sides. As

$$(\forall a \in \widehat{K}^*) \qquad a \cdot \rho(a) \in \widehat{F}^*,$$

it follows that K_Z/F is a Galois extension and the conjugation action of ρ on $\mathrm{Gal}(K_Z/K)$ is given by $\rho g \rho^{-1} = g^{-1}$. In other words,

$$\mathrm{Gal}(K_Z/F) \xrightarrow{\sim} \mathrm{Gal}(K_Z/K) \rtimes \{1, \rho\}$$

is a generalized dihedral group.

(2.7) We shall now describe the Galois group

$$\mathrm{Gal}(K_{Z'}/K_Z) \xrightarrow{\sim} K^*\widehat{F}^*Z/K^*\widehat{F}^*Z', \tag{2.7.1}$$

where $Z' \subset Z \subset \widehat{\mathcal{O}}_K^*$ are two open subgroups containing $\widehat{\mathcal{O}}_F^*$. We use the elementary fact that, whenever A and $B \supset C$ are subgroups of some abelian group, then the obvious inclusion maps give rise to an exact sequence

$$0 \longrightarrow \frac{A \cap B}{A \cap C} \longrightarrow \frac{B}{C} \longrightarrow \frac{AB}{AC} \longrightarrow 0,$$

from which we deduce

$$\begin{aligned}
&\widehat{F}^* \cap \widehat{\mathcal{O}}_K^* = \widehat{\mathcal{O}}_F^* \implies \widehat{F}^* \cap Z = \widehat{F}^* \cap Z' = \widehat{\mathcal{O}}_F^* \implies Z/Z' \xrightarrow{\sim} \widehat{F}^* Z/\widehat{F}^* Z' \\
&F^* \cap (\mathcal{O}_K^* \cap Z) = F^* \cap (\mathcal{O}_K^* \cap Z') = \mathcal{O}_F^* \implies (\mathcal{O}_K^* \cap Z)/(\mathcal{O}_K^* \cap Z') \xrightarrow{\sim} F^*(\mathcal{O}_K^* \cap Z)/F^*(\mathcal{O}_K^* \cap Z')
\end{aligned} \tag{2.7.2}$$

and, by taking $A = K^*$, $B = \widehat{F}^* Z$, $C = \widehat{F}^* Z'$, an exact sequence

$$0 \longrightarrow \frac{K^* \cap \widehat{F}^* Z}{K^* \cap \widehat{F}^* Z'} \longrightarrow \frac{Z}{Z'} \longrightarrow \mathrm{Gal}(K_{Z'}/K_Z) \longrightarrow 0. \tag{2.7.3}$$

The next step is to determine the abelian group $K^* \cap \widehat{F}^* Z$ (and its counterpart for Z' instead of Z).

(2.8) Proposition. *Put* $G = \mathrm{Gal}(K/F) = \{1, \rho\}$.
(i) $\mathrm{Ker}\left(N_{K/F} : \mathcal{O}_K^* \longrightarrow \mathcal{O}_F^*\right) = (\mathcal{O}_K^*)_{\mathrm{tors}}$.
(ii) *There is an isomorphism* $(K^* \cap \widehat{F}^* \widehat{\mathcal{O}}_K^*)/F^* \mathcal{O}_K^* \xrightarrow{\sim} \mathrm{Ker}(\mathrm{Pic}(\mathcal{O}_F) \longrightarrow \mathrm{Pic}(\mathcal{O}_K))$.
(iii) *([Wa, Thm. 10.3]) The abelian group* $\mathrm{Ker}(\mathrm{Pic}(\mathcal{O}_F) \longrightarrow \mathrm{Pic}(\mathcal{O}_K))$ *naturally injects into* $H^1(G, O_K^*)$. *The order of the abelian group* $H^1(G, O_K^*)$ *is equal to* 1 *or* 2.

Proof. (i) As K is a CM field and F its maximal real subfield, the group $\mathrm{Ker}(N_{K/F} : \mathcal{O}_K^* \longrightarrow \mathcal{O}_F^*)$ is finite, hence contained in $(\mathcal{O}_K^*)_{\mathrm{tors}}$. On the other hand, each root of unity $\zeta \in (\mathcal{O}_K^*)_{\mathrm{tors}}$ satisfies $\zeta \cdot \rho(\zeta) = 1$.
(ii) If $\beta \in K^* \cap \widehat{F}^* \widehat{\mathcal{O}}_K^*$, then, for each non-archimedean prime v of F, there exists $\alpha_v \in F_v^*$ such that $\mathrm{ord}_w(\beta) = \mathrm{ord}_w(\alpha_v)$, for all primes w above v in K. Let I be the ideal of $\mathcal{O}_F$ with divisor equal to $\sum_v \mathrm{ord}_v(\alpha_v)\,[v]$; then $I\mathcal{O}_K = (\beta)$. It follows that the map

$$\beta \mapsto \text{ the class of } I\mathcal{O}_K$$

defines a homomorphism

$$(K^* \cap \widehat{F}^* \widehat{\mathcal{O}}_K^*)/F^* \mathcal{O}_K^* \longrightarrow \mathrm{Ker}(\mathrm{Pic}(\mathcal{O}_F) \longrightarrow \mathrm{Pic}(\mathcal{O}_K)),$$

the inverse of which is given by $I \mapsto \beta$, if $I\mathcal{O}_K = (\beta)$.
(iii) The exact sequence

$$0 \longrightarrow P_K \longrightarrow I_K \longrightarrow \mathrm{Pic}(\mathcal{O}_K) \longrightarrow 0$$

(where P_K (resp., I_K) denotes the group of principal (resp., of all) fractional ideals of K) and its counterpart over F give rise to a commutative diagram with exact rows

$$\begin{array}{ccccccccc}
0 & \longrightarrow & P_F & \longrightarrow & I_F & \longrightarrow & \mathrm{Pic}(\mathcal{O}_F) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & P_K^G & \longrightarrow & I_K^G & \longrightarrow & \mathrm{Pic}(\mathcal{O}_K)^G & \longrightarrow & H^1(G, P_K).
\end{array}$$

The Snake Lemma then implies that the group $\mathrm{Ker}(\mathrm{Pic}(\mathcal{O}_F) \longrightarrow \mathrm{Pic}(\mathcal{O}_K))$ injects into $\mathrm{Coker}(P_F \longrightarrow P_K^G)$. On the other hand, the cohomology sequence of

$$0 \longrightarrow \mathcal{O}_K^* \longrightarrow K^* \longrightarrow P_K \longrightarrow 0$$

yields an exact sequence

$$0 \longrightarrow \mathcal{O}_F^* \longrightarrow F^* \longrightarrow P_K^G \longrightarrow H^1(G, \mathcal{O}_K^*) \longrightarrow 0,$$

hence $\mathrm{Coker}(P_F \longrightarrow P_K^G) \xrightarrow{\sim} H^1(G, \mathcal{O}_K^*)$. The abelian group $H^1(G, \mathcal{O}_K^*)$ is a quotient of the finite cyclic group $\mathrm{Ker}(N_{K/F} : \mathcal{O}_K^* \longrightarrow \mathcal{O}_F^*) = (\mathcal{O}_K^*)_{\mathrm{tors}}$; on the other hand, it is annihilated by $|G| = 2$, which implies that $|H^1(G, \mathcal{O}_K^*)| \leq 2$.

(2.9) Proposition. *If $Z' \subset Z$ are open subgroups of $\widehat{\mathcal{O}}_K^*$ containing $\widehat{\mathcal{O}}_F^*$, then the natural inclusions give rise to an exact sequence*

$$0 \longrightarrow \frac{\mathcal{O}_K^* \cap Z}{\mathcal{O}_K^* \cap Z'} \longrightarrow \frac{K^* \cap \widehat{F}^* Z}{K^* \cap \widehat{F}^* Z'} \longrightarrow U_{Z,Z'} \longrightarrow 0,$$

in which $|U_{Z,Z'}| \leq |\mathrm{Ker}(\mathrm{Pic}(\mathcal{O}_F) \longrightarrow \mathrm{Pic}(\mathcal{O}_K))| \leq 2$.

Proof. Injectivity of the first arrow follows from the second isomorphism in (2.7.2) and the equality

$$F^*(\mathcal{O}_K^* \cap Z) \cap \widehat{F}^* Z' = F^*(\mathcal{O}_K^* \cap Z \cap \widehat{F}^* Z') = F^*(\mathcal{O}_K^* \cap Z \cap \widehat{\mathcal{O}}_F^* Z') = F^*(\mathcal{O}_K^* \cap Z').$$

Define $U_{Z,Z'}$ to be the cokernel of this injective map. Assume first that $\mathrm{Ker}(\mathrm{Pic}(\mathcal{O}_F) \longrightarrow \mathrm{Pic}(\mathcal{O}_K)) = 0$; then $K^* \cap \widehat{F}^* \widehat{\mathcal{O}}_K^* = F^* \mathcal{O}_K^*$, by Proposition 2.8(ii), which implies that

$$K^* \cap \widehat{F}^* Z = F^* \mathcal{O}_K^* \cap \widehat{F}^* Z = F^*(\mathcal{O}_K^* \cap \widehat{F}^* Z) = F^*(\mathcal{O}_K^* \cap \widehat{\mathcal{O}}_F^* Z) = F^*(\mathcal{O}_K^* \cap Z)$$

(and similarly for Z'), hence $U_{Z,Z'} = 0$.
If $\mathrm{Ker}(\mathrm{Pic}(\mathcal{O}_F) \longrightarrow \mathrm{Pic}(\mathcal{O}_K)) \neq 0$, then there exists $\beta \in K^*$ such that $K^* \cap \widehat{F}^* \widehat{\mathcal{O}}_K^* = F^* \mathcal{O}_K^* \cup \beta F^* \mathcal{O}_K^*$, by Proposition 2.8(ii)-(iii); thus

$$K^* \cap \widehat{F}^* Z = F^*(\mathcal{O}_K^* \cap Z) \cup F^*(\beta \mathcal{O}_K^* \cap \widehat{F}^* Z).$$

If $u, u' \in \mathcal{O}_K^*$ satisfy $\beta u, \beta u' \in \widehat{F}^* Z$, then $u'/u \in \mathcal{O}_K^* \cap \widehat{F}^* Z = \mathcal{O}_K^* \cap Z$, which shows that $|U_{Z,Z'}| \leq 2$.

(2.10) Proposition. *Let $I_0 \subset \mathcal{O}_K$ be the non-zero ideal $I_0 := \mathrm{lcm}\,\{(u-1) \mid u \in (\mathcal{O}_K^*)_{\mathrm{tors}}, u \neq 1\}$. If $c \subset \mathcal{O}_F$ is a non-zero ideal such that $c\mathcal{O}_K \nmid I_0$ and $Z \subset \widehat{\mathcal{O}}_c^*$ is a subgroup, then $K^* \cap \widehat{F}^* Z = F^*$ and $\mathcal{O}_K^* \cap Z = \mathcal{O}_F^*$.*

Proof. It is enough to consider the case $Z = \widehat{\mathcal{O}}_c^*$. Assume that $\beta \in K^* \cap \widehat{F}^* \widehat{\mathcal{O}}_c^*$, $\beta = ab$, $a \in \widehat{F}^*$, $b \in \widehat{\mathcal{O}}_c^*$. Then we have

$$u := \beta/\rho(\beta) = b/\rho(b) \in K^* \cap \widehat{\mathcal{O}}_c^* \subset \mathcal{O}_K^*.$$

More precisely,

$$u \in \mathrm{Ker}\left(N_{K/F} : \mathcal{O}_K^* \longrightarrow \mathcal{O}_F^*\right) \cap \left(\widehat{\mathcal{O}}_c^*\right)^{1-\rho} \subseteq (\mathcal{O}_K^*)_{\mathrm{tors}} \cap \mathrm{Ker}\left(\widehat{\mathcal{O}}_K^* \longrightarrow (\mathcal{O}_K/c\mathcal{O}_K)^*\right);$$

the condition $c\mathcal{O}_K \nmid I_0$ then implies that $u = 1$, hence $\beta \in F^*$. It follows that $K^* \cap \widehat{F}^* \widehat{\mathcal{O}}_c^* = F^*$ and $\mathcal{O}_F^* \subset \mathcal{O}_c^* \subset \mathcal{O}_K^* \cap \widehat{F}^* \widehat{\mathcal{O}}_c^* \subset \mathcal{O}_K^* \cap F^* = \mathcal{O}_F^*$.

(2.11) Corollary. *If $Z' \subset Z \subset \widehat{\mathcal{O}}_K^*$ are open subgroups containing $\widehat{\mathcal{O}}_F^*$ such that $Z \subset \widehat{\mathcal{O}}_c^*$, for some non-zero ideal $c \subset \mathcal{O}_F$ satisfying $c\mathcal{O}_K \nmid I_0$, then the Galois group $\mathrm{Gal}(K_{Z'}/K_Z)$ is isomorphic to Z/Z'.*

Proof. Combine (2.7.3) with Propositions 2.9-10.

3. The main result

We follow the notations defined in Sect. 1-2.

(3.1) Fix the following data:

(3.1.1) An open compact subgroup $H \subset \widehat{B}^*$.

(3.1.2) An F-simple quotient A_j ($j \in J_1$) of $J(N_H^*)$ satisfying $\mathrm{End}_F(A_j) = \mathcal{O}_{L_j}$ and a non-trivial $\mathbf{T}$-linear morphism $J(N_H^*) \longrightarrow A_j$ (defined over F). Denote by ι_j the composite morphism

$$\iota_j : N_H^* \xrightarrow{\iota} J(N_H^*) \longrightarrow A_j.$$

(3.1.3) A totally imaginary quadratic extension K of F such that each prime $v \in S_B$ either ramifies or is inert in K/F.
(3.1.4) An F-embedding $t : K \hookrightarrow B$.
(3.1.5) A CM point $x = [z, b] \in CM(N_H, K)$; denote by $K(x)$ its field of definition over K.
(3.1.6) A character $\alpha : \mathrm{Gal}(K(x)/K) \longrightarrow \mathcal{O}_L^*$, where L is a number field containing the totally real field $L_j = \mathrm{End}_F(A_j) \otimes \mathbf{Q}$.

We denote

$$e_\alpha = \sum_{\sigma \in \mathrm{Gal}(K(x)/K)} \alpha^{-1}(\sigma)\, \sigma \in \mathcal{O}_L[\mathrm{Gal}(K(x)/K)]$$

and, for any $\mathcal{O}_L[\mathrm{Gal}(K(x)/K)]$-module M,

$$M^{(\alpha)} = \{m \in M \mid \forall \sigma \in \mathrm{Gal}(K(x)/K) \quad \sigma(m) = \alpha(\sigma)m\}.$$

The character α factors through an injective character

$$\beta : \mathrm{Gal}(K(\alpha)/K) \hookrightarrow \mathcal{O}_L^*,$$

where $K(\alpha) = K(x)^{\mathrm{Ker}(\alpha)} \subset K(x)$.

(3.2) Theorem. *Given the data (3.1.1-6), put $y_j = \iota_j(x) \otimes 1 \in A_j(K(x)) \otimes_{\mathcal{O}_{L_j}} \mathcal{O}_L$. Assume that the following condition is satisfied:*
($\star$) The abelian variety A_j does not acquire complex multiplication over any totally imaginary quadratic extension K' of F contained in $K(\alpha)$.
If $e_\alpha(y_j) \notin \Big(A_j(K(x)) \otimes_{\mathcal{O}_{L_j}} \mathcal{O}_L\Big)_{\mathrm{tors}}$, then the following abelian groups (more precisely, $\mathcal{O}_L$-modules) are finite:

$$\Big(A_j(K(x)) \otimes_{\mathcal{O}_{L_j}} \mathcal{O}_L\Big)^{(\alpha)}/\mathcal{O}_L \cdot e_\alpha(y_j), \qquad \Big(Ш(A_j/K(x)) \otimes_{\mathcal{O}_{L_j}} \mathcal{O}_L\Big)^{(\alpha)}$$
$$\Big(A_j(K(x)) \otimes_{\mathcal{O}_{L_j}} \mathcal{O}_L\Big)^{(\alpha^{-1})}/\mathcal{O}_L \cdot \rho(e_\alpha(y_j)), \qquad \Big(Ш(A_j/K(x)) \otimes_{\mathcal{O}_{L_j}} \mathcal{O}_L\Big)^{(\alpha^{-1})}$$

(where the complex conjugation ρ acts on $A_j(K(x)) \otimes_{\mathcal{O}_{L_j}} \mathcal{O}_L$ by $\rho \otimes \mathrm{id}$).

(3.3) Previously known results in this direction ([Ko], [Ko-Lo 1,2], [Be-Da], [Ho 1,2], [Be], [Ti], [Zh 3]) use several additional hypotheses which ensure, among other things, that there is a "geometric" formula relating $\rho(y_j)$ to y_j. Our main observation is that the Euler system argument does not require such a geometric relation.

(3.4) As explained in 6.2.1 below, the condition ($\star$) can be reformulated as follows: the Hilbert modular forms that occur in the factorization of $L(A_j/F, s)$ do not have CM by K'.

(3.5) It will be convenient to rephrase Theorem 3.2 and its proof in terms of the abelian variety

$$A = A_j \otimes_{\mathcal{O}_{L_j}} \mathcal{O}_L, \qquad \mathcal{O}_L \hookrightarrow \mathrm{End}_F(A)$$

(see [Con, §7] for the general formalism of such tensor products). We have

$$y_j \in A_j(K(x)) \otimes_{\mathcal{O}_{L_j}} \mathcal{O}_L = A(K(x)), \qquad e_\alpha(y_j) = e_\beta(y) \in A(K(\alpha)),$$

where

$$e_\beta = \sum_{\sigma \in \mathrm{Gal}(K(\alpha)/K)} \beta^{-1}(\sigma)\, \sigma \in \mathcal{O}_L[\mathrm{Gal}(K(\alpha)/K)], \qquad y = \mathrm{Tr}_{K(x)/K(\alpha)}(y_j) \in A(K(\alpha)).$$

Fix a maximal ideal $\mathfrak{p} \subset \mathcal{O}_L$ and a sufficiently large integer $M >> 0$ such that the ideal $\mathfrak{p}^M$ is principal. Fixing its generator (which will be, by abuse of language, also denoted by $\mathfrak{p}^M$), the Galois cohomology of

$$0 \longrightarrow A[\mathfrak{p}^M] \longrightarrow A(\overline{F}) \xrightarrow{\mathfrak{p}^M} A(\overline{F}) \longrightarrow 0$$

gives rise to the usual descent sequence

$$0 \longrightarrow A(K(\alpha))/\mathfrak{p}^M \xrightarrow{\delta} S \longrightarrow Ш(A/K(\alpha))[\mathfrak{p}^M] \longrightarrow 0,$$

where we have denoted by $S = Sel(A/K(\alpha), \mathfrak{p}^M)$ the classical Selmer group for the $\mathfrak{p}^M$-descent on A.
In order to prove Theorem 3.2, it will be enough to show, assuming that $e_\beta(y) \notin A(K(\alpha))_{\mathrm{tors}}$, that

$$(\exists C(\mathfrak{p}) \geq 0)\,(\forall M >> 0) \qquad \mathfrak{p}^{C(\mathfrak{p})} \cdot \left(S^{(\beta)}/\mathcal{O}_L \cdot \delta(e_\beta(y)) \right) = 0. \tag{3.5.1}$$

$$\text{For all but finitely many } \mathfrak{p}, \qquad C(\mathfrak{p}) = 0. \tag{3.5.2}$$

(3.6) Let us briefly outline the proof of (3.5.1), the main steps of which follow [Be-Da]. We denote $\mathcal{O}_\mathfrak{p} = \mathcal{O}_{L,\mathfrak{p}}$ and use temporarily the notation "$X \doteq Y$" (resp., "$x \dot{\in} X$") as a shorthand for $\mathfrak{p}^C X = \mathfrak{p}^C Y$ (resp., for $\mathfrak{p}^C x \in X$), where C is a suitable constant, independent of M.

(3.6.1) The Euler system. The first step is to construct an Euler system, by letting various Hecke operators act on the CM point x. Applying Kolyvagin's derivative and e_β, one obtains the derived cohomology classes

$$\kappa_1 = \text{a suitable multiple of } \delta(e_\beta(y)) \in S^{(\beta)}, \qquad \kappa_{\ell_1 \cdots \ell_r} \in S^{(\beta)}_{\{\ell_1,\ldots,\ell_r\}} \subset H^1(K(\alpha), A[\mathfrak{p}^M])(\beta),$$

where $\ell_1, \ldots, \ell_r$ are distinct primes of F, inert in K/F, which satisfy "Kolyvagin's condition" modulo a sufficiently high power of $\mathfrak{p}$. The subscript $\ell_1, \ldots, \ell_r$ indicates that the class $\kappa_{\ell_1 \cdots \ell_r}$ satisfies the "Selmer" local conditions only at primes distinct from $\ell_1, \ldots, \ell_r$.

(3.6.2) The Weil pairing. Fix a polarization $\varphi : A_j \longrightarrow \widehat{A}_j$ defined over F; it gives rise to the Weil pairing

$$T_p(A_j) \times T_p(A_j) \longrightarrow \mathbf{Z}_p(1)$$

(where p is the residual characteristic of $\mathfrak{p}$). This extends naturally (see 5.19 below) to an $\mathcal{O}_\mathfrak{p}$-bilinear pairing

$$T_\mathfrak{p}(A) \times T_\mathfrak{p}(A) \longrightarrow \mathcal{O}_\mathfrak{p}(1),$$

whose reduction modulo $\mathfrak{p}^M$

$$(\ ,\ )_M : A[\mathfrak{p}^M] \times A[\mathfrak{p}^M] \longrightarrow \mathcal{O}_\mathfrak{p}/\mathfrak{p}^M(1)$$

is skew-symmetric, and its kernel is killed by $\deg(\varphi)$.

(3.6.3) The first annihilation relation. For simplicity, assume that $\beta \neq \overline{\beta} := \beta^{-1}$. Let $s \in S^{(\beta)}$. For each Kolyvagin prime ℓ, we have a class $\kappa_\ell \in S^{(\beta)}_{\{\ell\}}$ and its complex conjugate ${}^\rho\kappa_\ell \in S^{(\overline{\beta})}_{\{\ell\}}$. Applying the reciprocity law of global class field theory

$$\left(\forall a \in H^2(K(\alpha), \mathcal{O}_\mathfrak{p}/\mathfrak{p}^M(1))\right) \qquad \sum_v \mathrm{inv}_v(a_v) = 0 \in \mathcal{O}_\mathfrak{p}/\mathfrak{p}^M$$

to the cup product $a = s \cup {}^\rho\kappa_\ell$, we obtain the relation

$$\sum_v \mathrm{inv}_v(s_v \cup ({}^\rho\kappa_\ell)_v) = 0 \in \mathcal{O}_\mathfrak{p}/\mathfrak{p}^M, \tag{3.6.3.1}$$

to which only the primes of $K(\alpha)$ above ℓ contribute. Fixing one such a prime, say, λ, and using the fundamental relation 5.18 between the localizations $(\kappa_1)_\lambda, (\kappa_\ell)_\lambda$, one can rewrite (3.6.3.1) as

$$[K(\alpha):K]\ (s_\lambda,(\kappa_1)_\lambda)_M = 0 \in \mathcal{O}_\mathfrak{p}/\mathfrak{p}^M(1), \tag{3.6.3.2}$$

where one considers the localizations $s_\lambda, (\kappa_1)_\lambda$ as elements of

$$H^1_{ur}(K(\alpha)_\lambda, A[\mathfrak{p}^M]) \xrightarrow{\sim} A[\mathfrak{p}^M] \quad (\xrightarrow{\sim} (\mathcal{O}_\mathfrak{p}/\mathfrak{p}^M)^2),$$

by using evaluation at the Frobenius element $\mathrm{Fr}(\lambda)$.
The assumption $e_\beta(y) \notin A_{\mathrm{tors}}$ implies that

$$\langle \kappa_1 \rangle \ \ (= \mathcal{O}_L \cdot \kappa_1) \doteq \mathcal{O}_\mathfrak{p}/\mathfrak{p}^M.$$

An application of the Čebotarev density theorem then shows that one can choose a Kolyvagin prime ℓ in such a way that

$$\langle (\kappa_1)_\lambda \rangle \doteq \mathcal{O}_\mathfrak{p}/\mathfrak{p}^M$$

(inside $H^1_{ur}(K(\alpha)_\lambda, A[\mathfrak{p}^M]) \xrightarrow{\sim} A[\mathfrak{p}^M]$). As the pairing $(\ ,\ )_M$ on $A[\mathfrak{p}^M]$ is almost symplectic, the annihilation relation (3.6.3.2) yields

$$s_\lambda \doteq \langle (\kappa_1)_\lambda \rangle^\perp \doteq \langle (\kappa_1)_\lambda \rangle. \tag{3.6.3.3}$$

If we put

$$\widetilde{S}^{(\beta)} = \{ s \in S^{(\beta)} \mid s_\lambda = 0 \},$$

then we deduce from (3.6.3.3) that

$$S^{(\beta)} \doteq \langle \kappa_1 \rangle \oplus \widetilde{S}^{(\beta)}.$$

(3.6.4) The second annihilation relation. Let $s \in \widetilde{S}^{(\beta)}$. In order to complete the proof of (3.5.1), we must show that $s \doteq 0$. If $\ell' \neq \ell$ is another Kolyvagin prime and λ' a prime above ℓ' in $K(\alpha)$, then the reciprocity law applied to the cup product $s \cup {}^\rho\kappa_{\ell\ell'}$

$$\sum_v \mathrm{inv}_v(s_v \cup ({}^\rho\kappa_{\ell\ell'})_v) = 0 \in \mathcal{O}_\mathfrak{p}/\mathfrak{p}^M$$

simplifies to

$$[K(\alpha):K]\ (s_{\lambda'},(\kappa_\ell)_{\lambda'})_M = 0 \in \mathcal{O}_\mathfrak{p}/\mathfrak{p}^M(1). \tag{3.6.4.1}$$

As $(\kappa_1)_\lambda$ (resp., $(\kappa_\ell)_\lambda$) is unramified (resp., totally ramified) at λ, we have

$$\langle (\kappa_1)_\lambda, (\kappa_\ell)_\lambda \rangle \doteq (\mathcal{O}_\mathfrak{p}/\mathfrak{p}^M)^2 \subset H^1(K(\alpha)_\lambda, A[\mathfrak{p}^M]),$$

hence

$$\langle \kappa_1, \kappa_\ell \rangle \doteq (\mathcal{O}_\mathfrak{p}/\mathfrak{p}^M)^2 \subset S^{(\beta)}_{\{\ell\}}.$$

Another application of the Čebotarev density theorem shows that one can choose ℓ' in such a way that

$$\langle (\kappa_1)_{\lambda'}, (\kappa_\ell)_{\lambda'} \rangle \doteq (\mathcal{O}_\mathfrak{p}/\mathfrak{p}^M)^2 = H^1_{ur}(K(\alpha)_{\lambda'}, A[\mathfrak{p}^M]) \xrightarrow{\sim} A[\mathfrak{p}^M] \tag{3.6.4.2}$$

and

$$\langle s_{\lambda'} \rangle \doteq \langle s \rangle. \tag{3.6.4.3}$$

The first annihilation relation (3.6.3.2) applies with ℓ' instead of ℓ, hence

$$s_{\lambda'} \dot{\in} \langle (\kappa_1)_{\lambda'} \rangle^{\perp}.$$

On the other hand, the second annihilation relation (3.6.4.1) yields

$$s_{\lambda'} \dot{\in} \langle (\kappa_\ell)_{\lambda'} \rangle^{\perp},$$

thus

$$s_{\lambda'} \dot{\in} \langle (\kappa_1)_{\lambda'}, (\kappa_\ell)_{\lambda'} \rangle^{\perp} \doteq A[\mathfrak{p}^M]^{\perp} \doteq 0,$$

by (3.6.4.2), which in turns implies that $s \doteq 0$, by (3.6.4.3). This finishes the proof that $\widetilde{S}^{(\beta)} \doteq 0$, hence $S^{(\beta)} \doteq \langle \kappa_1 \rangle = \langle \delta(e_\beta(y)) \rangle$.

4. The Euler system

Assume that we are in the situation of 3.1.

(4.1) According to Proposition 2.5, the field of definition $K(x)$ of x over K is characterized by the isomorphism

$$\mathrm{rec}_K : \widehat{K}^*/K^*\widehat{F}^*Z \xrightarrow{\sim} \mathrm{Gal}(K(x)/K), \qquad Z = \widehat{t}^{-1}(bH\widehat{\mathcal{O}}_F^* b^{-1}).$$

It follows from the first formula in (2.6.2.1) that there exists a smallest non-zero ideal $c(x) \subset \mathcal{O}_F$ (with respect to divisibility) such that $Z \supseteq \widehat{\mathcal{O}}^*_{c(x)}$. Equivalently, $K[c(x)]$ is the smallest ring class field of K (with respect to inclusion) containing $K(x)$.

(4.2) Fix S as in 1.12. The decomposition (1.12.1) implies that we have

$$Z = Z_S Z^S, \qquad Z_S \subset \prod_{v \in S} \mathcal{O}^*_{K,v}, \qquad Z^S = \prod_{v \notin S} Z_v, \qquad (\forall v \notin S) \quad Z_v = t_v^{-1}(b_v H_v \mathcal{O}^*_{F,v} b_v^{-1}) \subset \mathcal{O}^*_{K,v},$$

where we have denoted, slightly abusively,

$$\mathcal{O}_{K,v} = \mathcal{O}_K \otimes_{\mathcal{O}_F} \mathcal{O}_{F,v} = \bigoplus_{w|v} \mathcal{O}_{K,w}.$$

For each $v \notin S$, we have

$$\mathrm{ord}_v(c(x)) = 0 \iff Z_v = \mathcal{O}^*_{K,v}.$$

(4.3) Definition. *Let $\mathscr{S} = \bigcup_{r \geq 0} \mathscr{S}_r$ be the following set of square-free ideals of $\mathcal{O}_F$: $\mathscr{S}_0 = \{(1)\}$,*

$$\mathscr{S}_1 = \{\ell \subset \mathcal{O}_F \mid \ell \text{ is a maximal ideal inert in } K/F,\ \ell \notin S,\ \ell \nmid (p)c(x),\ \ell\mathcal{O}_K \nmid I_0\},$$
$$(\forall r > 1) \quad \mathscr{S}_r = \{\ell_1 \cdots \ell_r \mid \ell_j \in \mathscr{S}_1 \text{ distinct}\},$$

where $I_0 \subset \mathcal{O}_K$ is the ideal defined in Proposition 2.10.

(4.4) Definition. *For each $\mathfrak{n} \in \mathscr{S}$, let $h(\mathfrak{n}) \in \widehat{B}^*$ be the following element: $h((1)) = 1$. For each $\ell \in \mathscr{S}_1$, we have $H_\ell = R(\ell)^*$, for a maximal $\mathcal{O}_{F,\ell}$-order $R(\ell) \subset B_\ell$; let $h(\ell) \in R(\ell) \cap B_\ell^* \subset B_\ell^* \subset \widehat{B}^*$ be any element satisfying $\mathrm{ord}_\ell(nr(h(\ell))) = 1$. Finally, for $\mathfrak{n} = \ell_1 \cdots \ell_r$ ($r > 1$, $\ell_j \in \mathscr{S}_1$), we put $h(\mathfrak{n}) = h(\ell_1) \cdots h(\ell_r) \in \prod_{j=1}^r B^*_{\ell_j} \subset \widehat{B}^*$. Having defined $h(\mathfrak{n})$, we define CM points*

$$(\forall \mathfrak{n} \in \mathscr{S}) \qquad x(\mathfrak{n}) := [z, bh(\mathfrak{n})] \in CM(N_H, K).$$

(4.5) Proposition. *For each $\mathfrak{n} \in \mathscr{S}$, the field of definition $K(x(\mathfrak{n}))$ is contained in $K[c(x)\mathfrak{n}]$ and the reciprocity map induces an isomorphism*

$$\mathrm{rec}_K : \widehat{K}^*/K^*\widehat{F}^*Z(\mathfrak{n}) \xrightarrow{\sim} \mathrm{Gal}(K(x(\mathfrak{n}))/K),$$

where

$$Z(\mathfrak{n}) = \widehat{t}^{-1}(bh(\mathfrak{n})H\widehat{\mathcal{O}}_F^* h(\mathfrak{n})^{-1}b^{-1}) = Z \cap \widehat{\mathcal{O}}_{\mathfrak{n}}^* = Z_S \prod_{\ell|\mathfrak{n}} Z(\mathfrak{n})_\ell \prod_{\ell \notin S(\mathfrak{n})} Z_\ell, \qquad S(\mathfrak{n}) = S \cup \{\ell \in \mathscr{S}_1,\, \ell \mid \mathfrak{n}\}.$$

The quotient $Z/Z(\mathfrak{n})$ is naturally isomorphic to

$$Z/Z(\mathfrak{n}) \xrightarrow{\sim} \prod_{\ell|\mathfrak{n}} Z_\ell/Z(\mathfrak{n})_\ell, \qquad Z_\ell/Z(\mathfrak{n})_\ell \xrightarrow{\sim} \frac{(\mathcal{O}_K/\ell\mathcal{O}_K)^*}{(\mathcal{O}_F/\ell\mathcal{O}_F)^*};$$

in particular, each group $Z_\ell/Z(\mathfrak{n})_\ell$ (for $\ell \in \mathscr{S}_1, \ell \mid \mathfrak{n}$) is cyclic of order $N\ell + 1$.

Proof. The isomorphism comes from Proposition 2.5. As $h(\mathfrak{n}) = 1$ for each $v \nmid \mathfrak{n}$, the abelian group $Z(\mathfrak{n})$ decomposes as required, with $Z(\mathfrak{n})_v = Z_v$ for each $v \nmid S(\mathfrak{n})$ and

$$(\forall \ell \mid \mathfrak{n},\, \ell \in \mathscr{S}_1) \qquad Z(\mathfrak{n})_\ell = t_\ell^{-1}(b_\ell h(\ell) R(\ell)^* h(\ell)^{-1} b_\ell^{-1}).$$

Applying Proposition 4.7(iv) below with $E = F_\ell$, $R = R(\ell) \subset B_\ell \xrightarrow{\sim} M_2(F_\ell)$, $i = \mathrm{Ad}(b_\ell)^{-1} \circ t_\ell : K \otimes_F F_\ell \hookrightarrow B_\ell \xrightarrow{\sim} M_2(F_\ell)$ and $r = 1$ implies that $Z(\mathfrak{n}) = Z \cap \widehat{\mathcal{O}}_{\mathfrak{n}}^*$ and

$$Z_\ell/Z(\mathfrak{n})_\ell \xrightarrow{\sim} \frac{(\mathcal{O}_K/\ell\mathcal{O}_K)^*}{(\mathcal{O}_F/\ell\mathcal{O}_F)^*}.$$

Finally, it follows from $Z \supseteq \widehat{\mathcal{O}}_{c(x)}^*$ that $Z(\mathfrak{n}) \supseteq \widehat{\mathcal{O}}_{c(x)}^* \cap \widehat{\mathcal{O}}_{\mathfrak{n}}^* = \widehat{\mathcal{O}}_{c(x)\mathfrak{n}}^*$, hence $K(x(\mathfrak{n})) \subseteq K[c(x)\mathfrak{n}]$.

(4.6) Proposition. *Let v be a non-archimedean prime of F which does not divide $c(x)$.*
(i) *If $\mathfrak{n} \in \mathscr{S}$ and $v \nmid \mathfrak{n}$, then each prime of K above v is unramified in $K(x(\mathfrak{n}))/K$.*
(ii) *If $\mathfrak{n} \in \mathscr{S}$, $v \nmid \mathfrak{n}$ and v is inert in K/F, then $v\mathcal{O}_K$ splits completely in $K(x(\mathfrak{n}))/K$.*
(iii) *If $\mathfrak{n}\ell \in \mathscr{S}_{r+1}$ ($\ell \in \mathscr{S}_1$, $\mathfrak{n} \in \mathscr{S}_r$, $r \geq 0$), then each prime of $K(x(\mathfrak{n}))$ above ℓ is totally tamely ramified in $K(x(\mathfrak{n}\ell))/K(x(\mathfrak{n}))$.*

Proof. (i) As $K(x(\mathfrak{n})) \subseteq K[c(x)\mathfrak{n}]$ and $v \nmid c(x)\mathfrak{n}$, the prime v is unramified in $K(x(\mathfrak{n}))/K$.
(ii) The decomposition group of $v\mathcal{O}_K$ in the extension $K(x(\mathfrak{n}))/K$ is equal to the image of the composite map

$$K_v^* := (K \otimes_F F_v)^* \longrightarrow \widehat{K}^* \longrightarrow \widehat{K}^*/K^*\widehat{F}^* Z(\mathfrak{n}),$$

which factors through $K_v^*/\mathcal{O}_{K,v}^* F_v^* = 0$, as $v\mathcal{O}_K$ is unramified in this extension.
(iii) The inertia group of this extension at any prime λ of $K(x(\mathfrak{n}))$ above ℓ is equal to the image of the composite map

$$f : \mathcal{O}_{K(x(\mathfrak{n})),\lambda}^* \xrightarrow{f_1} \mathcal{O}_{K,\ell}^* \xrightarrow{f_2} \frac{(\mathcal{O}_K/\ell\mathcal{O}_K)^*}{(\mathcal{O}_F/\ell\mathcal{O}_F)^*} = Z(\mathfrak{n}\ell)/Z(\mathfrak{n}) \xrightarrow{f_3} \mathrm{Gal}(K(x(\mathfrak{n}\ell))/K(x(\mathfrak{n}))).$$

The arrow f_1 (given by the norm map) is surjective, since λ is unramified in $K(x(\mathfrak{n}))/K$, and the arrows f_2 and f_3 are given by the canonical projections (cf. (2.7.3)). It follows that f is surjective, hence λ is totally ramified; the ramification is tame, as $[K(x(\mathfrak{n}\ell)) : K(x(\mathfrak{n}))]$ divides $N\ell + 1$, which is prime to $N\lambda$.

(4.7) Proposition. *Let E be a finite extension of $\mathbf{Q}_p$, E' the unique unramified quadratic extension of E and π a common uniformizer of E and E'. Let $R \subset M_2(E)$ be a maximal $\mathcal{O}_E$-order and $i : E' \hookrightarrow M_2(E)$ an E-embedding. For $r \geq 1$, put $\mathcal{O}_{E',r}^* := \mathrm{Ker}\,(\mathcal{O}_{E'}^* \longrightarrow (\mathcal{O}_{E'}/\pi^r)^*)$.*
(i) *R^* is a maximal compact subgroup of $M_2(E)^* = GL_2(E)$.*
(ii) *$(\forall \gamma \in GL_2(E)) \quad i^{-1}(\gamma R^* \gamma^{-1}) \subset \mathcal{O}_{E'}^*$.*
(iii) *If $i^{-1}(R^*) = \mathcal{O}_{E'}^*$ and if $g \in R$ satisfies $\mathrm{ord}_\pi(\det(g)) = 1$, then, for each integer $r \geq 1$, the map of sets*

$$i_r : \mathcal{O}_{E'}^*/\mathcal{O}_E^*\mathcal{O}_{E',r}^* \longrightarrow R^*/(R^* \cap g^r R^* g^{-r})$$

induced by i is bijective.
(iv) *Under the assumptions of (iii), we have, for each $r \geq 1$,*

$$i^{-1}(g^r R^* g^{-r}) = i^{-1}(R^* \cap g^r R^* g^{-r}) = \mathcal{O}_E^* \mathcal{O}_{E',r}^*,$$

hence the reduction modulo π^r induces an isomorphism of abelian groups

$$\frac{i^{-1}(R^*)}{i^{-1}(g^r R^* g^{-r})} \xrightarrow{\sim} \frac{\mathcal{O}_{E'}^*}{\mathcal{O}_E^* \mathcal{O}_{E',r}^*} \xrightarrow{\sim} \frac{(\mathcal{O}_{E'}/\pi^r \mathcal{O}_{E'})^*}{(\mathcal{O}_E/\pi^r \mathcal{O}_E)^*}.$$

In particular, reduction modulo π induces an isomorphism

$$\frac{i^{-1}(R^*)}{i^{-1}(gR^* g^{-1})} \xrightarrow{\sim} k_{E'}^*/k_E^*,$$

where k_E and $k_{E'}$ denote the residue fields of E and E', respectively.

Proof. Without loss of generality, we can assume that $R = M_2(\mathcal{O}_E)$ and $g = \begin{pmatrix} 1 & 0 \\ 0 & \pi \end{pmatrix}$. In this case (i) is well-known and (ii) follows from the properness of the map i (which implies that $i^{-1}(\gamma R^* \gamma^{-1})$ is a compact subgroup of E'^*, hence is contained in $\mathcal{O}_{E'}^*$). In order to prove (iii) and (iv), note first that we have, for each $r \geq 0$,

$$i^{-1}(g^r R^* g^{-r}) \overset{(ii)}{=} \mathcal{O}_{E'}^* \cap i^{-1}(g^r R^* g^{-r}) = i^{-1}(R^*) \cap i^{-1}(g^r R^* g^{-r}) = i^{-1}(R^* \cap g^r R^* g^{-r}).$$

On the other hand, the intersection $R_r := R \cap g^r R g^{-r}$ is equal to the Eichler order (of level π^r)

$$R_r = \Big\{ \begin{pmatrix} a & b \\ \pi^r c & d \end{pmatrix} \Big| \, a, b, c, d \in \mathcal{O}_E \Big\} \subset M_2(\mathcal{O}_E) = R,$$

which implies that $i^{-1}(R_r)$ is an $\mathcal{O}_E$-order in $\mathcal{O}_{E'}$, hence $i^{-1}(R_r) = \mathcal{O}_E + \pi^{c(r)} \mathcal{O}_{E'}$, for some $c(r) \geq 0$. As $i^{-1}(R^*) = \mathcal{O}_{E'}^*$, we must have $i^{-1}(R) = \mathcal{O}_{E'}$. For $r \geq 1$, the $\mathcal{O}_E$-module $i^{-1}(R)/i^{-1}(R_r) \xrightarrow{\sim} \mathcal{O}_E/\pi^{c(r)}$ injects into $R/R_r \xrightarrow{\sim} \mathcal{O}_E/\pi^r$, hence $c(r) \leq r$. If $c(r) < r$, then $i(\pi^{r-1} \mathcal{O}_{E'}) \subseteq R_r$, which implies that $i(\mathcal{O}_{E'}) \subseteq R \cap \pi^{1-r} R_r = R_1$. In other words, i induces a k_E-embedding of $k_{E'}$ into the ring $\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, b, d \in k_E \}$, which is impossible. This contradiction proves that $c(r) = r$, hence

$$i^{-1}(R^* \cap g^r R^* g^{-r}) = i^{-1}(R_r^*) = i^{-1}(R_r \cap R^*) = (\mathcal{O}_E + \pi^r \mathcal{O}_{E'}) \cap \mathcal{O}_{E'}^* = (\mathcal{O}_E + \pi^r \mathcal{O}_{E'})^* = \mathcal{O}_E^* \mathcal{O}_{E',r}^*.$$

The remaining statements in (iii) and (iv) follow automatically.

(4.8) Proposition (The norm relation). *Let $\mathfrak{n}\ell \in \mathscr{S}_{r+1}$ ($\ell \in \mathscr{S}_1$, $\mathfrak{n} \in \mathscr{S}_r$, $r \geq 0$).*
(i) *$K(x(\mathfrak{n}\ell))/K(x(\mathfrak{n}))$ is a cyclic extension of degree $(N\ell + 1)/u(r)$, where $u(r) = 1$ for $r > 0$ and $u(0) = (K^* \cap \widehat{F}^* Z : F^*)$ ($= (\mathcal{O}_K^* \cap Z : \mathcal{O}_F^*)$ or $2\,(\mathcal{O}_K^* \cap Z : \mathcal{O}_F^*)$).*
(ii) *We have an equality of divisors on $N_H^* \otimes_F \overline{F}$*

$$T(\ell)\, x(\mathfrak{n}) = u(r) \sum_{\sigma \in \mathrm{Gal}(K(x(\mathfrak{n}\ell))/K(x(\mathfrak{n})))} \sigma(x(\mathfrak{n}\ell)),$$

where $T(\ell)\, x(\mathfrak{n}) = [Hb_\ell H]_*(x(\mathfrak{n}))$ (which is also equal to $[Hb_\ell H]^*(x(\mathfrak{n}))$, as we work with the curve N_H^*).
(iii) *The following equality holds in $J(N_H^*)(K(x(\mathfrak{n})))$:*

$$T(\ell)\, (\iota(x(\mathfrak{n}))) = u(r)\, \mathrm{Tr}_{K(x(\mathfrak{n}\ell))/K(x(\mathfrak{n}))}(\iota(x(\mathfrak{n}\ell))).$$

Proof. (i) We apply (2.7.3) to the extension $K(x(\mathfrak{n}\ell))/K(x(\mathfrak{n})) = K_{Z(\mathfrak{n}\ell)}/K_{Z(\mathfrak{n})}$. As $\mathfrak{n}\ell\mathcal{O}_K \nmid I_0$, Proposition 2.10 implies that $K^* \cap \widehat{F}^* Z(\mathfrak{n}\ell) = F^*$. If $r > 0$, then $K^* \cap \widehat{F}^* Z(\mathfrak{n}) = F^*$ as well, hence a combination of (2.7.3) with Proposition 4.5 yields an isomorphism

$$\frac{(\mathcal{O}_K/\ell\mathcal{O}_K)^*}{(\mathcal{O}_F/\ell\mathcal{O}_F)^*} \xrightarrow{\sim} \mathrm{Gal}(K(x(\mathfrak{n}\ell))/K(x(\mathfrak{n}))).$$

If $r = 0$ ($\iff \mathfrak{n} = (1)$), then the same argument shows that the kernel of the natural surjection

$$\frac{(\mathcal{O}_K/\ell\mathcal{O}_K)^*}{(\mathcal{O}_F/\ell\mathcal{O}_F)^*} \longrightarrow \mathrm{Gal}(K(x(\mathfrak{n}\ell))/K(x(\mathfrak{n})))$$

has order equal to $u(0) = (K^* \cap \widehat{F}^* Z : F^*)$, which is in turn equal to $(\mathcal{O}_K^* \cap Z : \mathcal{O}_F^*)$ or $2(\mathcal{O}_K^* \cap Z : \mathcal{O}_F^*)$, thanks to Proposition 2.9.
(ii) By definition, the divisor $T(\ell)\, x(\mathfrak{n})$ contains $x(\mathfrak{n}\ell)$. Proposition 4.7(iii) for $r = 1$ together with the proof of (i) imply that $T(\ell)\, x(\mathfrak{n})$ coincides with the orbit of $x(\mathfrak{n}\ell)$ under the action of $\mathrm{Gal}(K(x(\mathfrak{n}\ell))/K(x(\mathfrak{n})))$, with each point counted with multiplicity $u(r)$.
(iii) This is a consequence of (ii) and the fact that $T(\ell)$ acts on the class of $m(\infty)$ (resp., on $\widetilde{m\xi(N_H^*)}$) by multiplication by $\deg T(\ell) = N\ell + 1$.

(4.9) Proposition (The congruence relation). *Let $\mathfrak{n}\ell \in \mathscr{S}_{r+1}$ ($\ell \in \mathscr{S}_1$, $\mathfrak{n} \in \mathscr{S}_r$, $r \geq 0$). For each prime $\lambda \mid \ell$ above ℓ in $K(\mathfrak{n}\ell)$ the following congruence holds:*

$$x(\mathfrak{n}\ell) \equiv \mathrm{Fr}(\ell)_{\mathrm{arith}}\, x(\mathfrak{n}) \equiv \mathrm{Fr}(\ell)_{\mathrm{geom}}\, x(\mathfrak{n}) \pmod{\lambda}$$

(considered as an equality in $\mathbf{N}_H^*(\kappa(\lambda))$).

Proof. Firstly, $\kappa(\lambda)/\kappa(\ell)$ is a quadratic extension, by Proposition 4.6(ii)-(iii), hence the actions of $\mathrm{Fr}(\ell)_{\mathrm{arith}}$ and $\mathrm{Fr}(\ell)_{\mathrm{geom}}$ on $\kappa(\lambda)$ coincide. Combining this remark with the congruence relation (1.14.3), we deduce that the reduction modulo λ of each point in the support of $T(\ell)\, x(\mathfrak{n})$ (in particular, of $x(\mathfrak{n}\ell)$) is equal to the reduction of $\mathrm{Fr}(\ell)_{\mathrm{arith}}\, x(\mathfrak{n})$.

(4.10) Proposition-Definition. *For each $\mathfrak{n} \in \mathscr{S}$, define the subfield $K(x(\mathfrak{n}))' \subseteq K(x(\mathfrak{n}))$ by*

$$K(x(\mathfrak{n}))' = \begin{cases} K(x), & \mathfrak{n} = (1) \\ K(x(\ell_1)) \cdots K(x(\ell_r)), & \mathfrak{n} = \ell_1 \cdots \ell_r \ (r \geq 1,\ \ell_i \in \mathscr{S}_1) \end{cases}$$

and put $G(\mathfrak{n}) = \mathrm{Gal}(K(x(\mathfrak{n}))'/K(x))$.
(i) *For each $\ell \in \mathscr{S}_1$, the group $G(\ell)$ is cyclic, of order $(N\ell + 1)/u(0)$.*
(ii) *For each $\mathfrak{n} = \ell_1 \cdots \ell_r \in \mathscr{S}_r$, the canonical map $G(\mathfrak{n}) \longrightarrow G(\ell_1) \times \cdots \times G(\ell_r)$ is an isomorphism.*
(iii) *For each $\mathfrak{n} \in \mathscr{S}_r$ ($r \geq 0$), we have $[K(x(\mathfrak{n})) : K(x(\mathfrak{n}))'] = u(r)u(0)^{r-1}$.*

Proof. (i) This is a special case of Proposition 4.8(i).
(ii) The case $r = 0$ is trivial. For $r \geq 1$ the statement follows from Lemma 4.11 below, applied to $G = Z/Z(\mathfrak{n}) = Z/Z(\ell_1 \cdots \ell_r)$, $G_j = Z(\mathfrak{n}/\ell_j)/Z(\mathfrak{n})$, $\widetilde{G}_j = Z(\ell_j)/Z(\mathfrak{n})$, $A = (K^* \cap \widehat{F}^* Z)/F^*$ (we use (2.7.3) and Proposition 2.10 to view $A \subset G$, and then use Proposition 2.10 again for $\widetilde{G}_i \cap A = 0$).
(iii) The case $r = 0$ is again trivial. For $r \geq 1$ we have

$$[K(x(\mathfrak{n})) : K(x(\mathfrak{n}))'] = |A|^{r-1} = u(0)^{r-1},$$

by the proof of Lemma 4.11.

(4.11) Lemma. *Let $G = G_1 \oplus \cdots \oplus G_r$ ($r \geq 1$) be a finite abelian group, $A \subset G$ a subgroup and $\pi : G \longrightarrow G/A$ the canonical projection. Assume that, for each $i = 1, \ldots, r$, we have $\widetilde{G}_i \cap A = 0$, where $\widetilde{G}_i = \bigoplus_{j \neq i} G_i \subset G$. Then the canonical homomorphism*

$$\pi(G)/\bigcap_{i=1}^{r} \pi(\widetilde{G}_i) \longrightarrow \bigoplus_{i=1}^{r} \pi(G)/\pi(\widetilde{G}_i)$$

is an isomorphism.

Proof. There is nothing to prove if $r = 1$, so we can assume that $r > 1$. As the homomorphism in question is injective and $|\pi(\widetilde{G}_i)| = |\widetilde{G}_i| = |G|/|G_i|$ (since $\widetilde{G}_i \cap \mathrm{Ker}(\pi) = 0$ by assumption), it is enough to show that

$$\left|\bigcap_{i=1}^{r} \pi(\widetilde{G}_i)\right| \stackrel{?}{=} |\pi(G)| \prod_{i=1}^{r} \frac{|\pi(\widetilde{G}_i)|}{|\pi(G)|} = \frac{|G|}{|A|} \prod_{i=1}^{r} \frac{|A|}{|G_i|} = |A|^{r-1}.$$

Denote, for any subset $I \subset \{1, \dots, r\}$,

$$G_I = \bigoplus_{i \in I} G_i \subset G, \qquad I^0 = \{1, \dots, r\} - I, \qquad \widetilde{G}_I = G_{I^0}.$$

Applying the Snake Lemma to the commutative diagrams with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \widetilde{G}_i & \longrightarrow & G & \xrightarrow{\pi_i} & G_i & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \wr} & & \downarrow{\scriptstyle \pi} & & \downarrow & & \\ 0 & \longrightarrow & \pi(\widetilde{G}_i) & \longrightarrow & \pi(G) & \longrightarrow & \pi(G)/\pi(\widetilde{G}_i) & \longrightarrow & 0 \end{array}$$

(where $\pi_i : G \longrightarrow G_i$, $i = 1, \dots, r$, denotes the natural projection with kernel $\widetilde{G}_i$) and

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \widetilde{G}_{\{1,\dots,k\}} & \longrightarrow & \widetilde{G}_{\{1,\dots,k-1\}} & \xrightarrow{\pi_k} & G_k & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha_k} & & \downarrow{\scriptstyle \alpha_{k-1}} & & \downarrow{\scriptstyle \pi} & & \\ 0 & \longrightarrow & \bigcap_{i=1}^{k} \pi(\widetilde{G}_i) & \longrightarrow & \bigcap_{i=1}^{k-1} \pi(\widetilde{G}_i) & \longrightarrow & \pi(G)/\pi(\widetilde{G}_k) & & \end{array}$$

$(k = 2, \dots, r)$, we obtain isomorphisms $A \xrightarrow{\sim} \pi_i(A)$ $(i = 1, \dots, r)$, inclusions

$$\mathrm{Ker}(\alpha_r) \subseteq \mathrm{Ker}(\alpha_{r-1}) \subseteq \cdots \subseteq \mathrm{Ker}(\alpha_1) = 0$$

and exact sequences

$$0 \longrightarrow \pi_k(A) \longrightarrow \mathrm{Coker}(\alpha_k) \longrightarrow \mathrm{Coker}(\alpha_{k-1}) \longrightarrow 0 \qquad\qquad (k = 2, \dots, r),$$

which imply, by induction, the desired equality

$$\left|\bigcap_{i=1}^{r} \pi(\widetilde{G}_i)\right| = |\mathrm{Coker}(\alpha_r)| = \prod_{i=2}^{r} |\pi_i(A)| = |A|^{r-1}.$$

(4.12) Definition of the Euler system. *For each $\mathfrak{n} \in \mathscr{S}_r$ $(r \geq 0)$, define the point $y(\mathfrak{n}) \in A(K(x(\mathfrak{n}))') = A_j(K(x(\mathfrak{n}))') \otimes_{\mathcal{O}_{L_j}} \mathcal{O}_L$ by*

$$y(\mathfrak{n}) = \frac{u(0)}{u(r)} \mathrm{Tr}_{K(x(\mathfrak{n}))/K(x(\mathfrak{n}))'} \iota(x(\mathfrak{n})) \otimes 1$$

(in particular, $y((1)) = \iota(x) \otimes 1 \in A(K(x))$).

(4.13) Proposition (The Euler system relations). *Let $\mathfrak{n}\ell \in \mathscr{S}_{r+1}$ $(\ell \in \mathscr{S}_1$, $\mathfrak{n} \in \mathscr{S}_r$, $r \geq 0)$. Then:*
(i) $\mathrm{Tr}_{K(x(\mathfrak{n}\ell))'/K(x(\mathfrak{n}))'} y(\mathfrak{n}\ell) = a_\ell\, y(\mathfrak{n})$, *where $a_\ell = \theta(T(\ell)) \in \mathcal{O}_{L_j}$ is the eigenvalue of the Hecke operator $T(\ell)$ acting on A_j.*
(ii) *For each prime $\lambda' \mid \ell$ above ℓ in $K(x(\mathfrak{n}\ell))'$, we have*

$$y(\mathfrak{n}\ell) \equiv u(0)\, \mathrm{Fr}(\ell)_{\mathrm{arith}}\, y(\mathfrak{n}) \equiv u(0)\, \mathrm{Fr}(\ell)_{\mathrm{geom}}\, y(\mathfrak{n}) \pmod{\lambda'}.$$

Proof. (i) This follows from Proposition 4.8(iii).
(ii) As $m(\infty)$ (resp., $\widetilde{m\xi(N_H^*)}$) is defined over F, it follows from (the proof of) Proposition 4.9 that we have, for each prime $\lambda \mid \lambda'$ above λ' in $K(x(\mathfrak{n}\ell))$,

$$\iota(x(\mathfrak{n}\ell)) \equiv \mathrm{Fr}(\ell)_{\mathrm{arith}}\,\iota(x(\mathfrak{n})) \equiv \mathrm{Fr}(\ell)_{\mathrm{geom}}\,\iota(x(\mathfrak{n}))\ (\mathrm{mod}\,\lambda),$$

hence (using Proposition 4.10(iii))

$$y(\mathfrak{n}\ell) \equiv \frac{u(0)}{u(r+1)}\,[K(x(\mathfrak{n}\ell)) : K(x(\mathfrak{n}\ell))']\,(\iota(x(\mathfrak{n}\ell)) \otimes 1) \equiv u(0)^{r+1}\,\iota(x(\mathfrak{n}\ell)) \otimes 1\ (\mathrm{mod}\,\lambda)$$

and, similarly,

$$y(\mathfrak{n}) \equiv u(0)^r\,\iota(x(\mathfrak{n})) \otimes 1\ (\mathrm{mod}\,\lambda),$$

which proves the desired congruence.

5. The derivative classes

We continue to use the notation of Sect. 1-4.

(5.1) Fix a prime number p, a prime ideal $\mathfrak{p} \subset \mathcal{O}_L$ above p and a prime element $\varpi \in \mathcal{O}_{\mathfrak{p}} = \mathcal{O}_{L,\mathfrak{p}}$. Set $M_0 = \mathrm{ord}_{\mathfrak{p}}(u(0))$.

(5.2) The set $\mathscr{S}_1(M)$ of "Kolyvagin primes"

(5.2.1) Definition. *For each integer $M \geq 1$, define $\mathscr{S}_1(M)$ to be the set of maximal ideals $\ell \subset \mathcal{O}_F$ satisfying the following conditions:*

$$\ell \nmid (p)c(x)d_{K/F}, \qquad \ell\mathcal{O}_K \nmid I_0, \qquad \ell \notin S,$$

and the conjugacy class of the arithmetic Frobenius $\mathrm{Fr}(\ell)_{\mathrm{arith}}$ in the Galois group $\mathrm{Gal}(K(x)(A[\mathfrak{p}^{M+M_0}])/F)$ coincides with the conjugacy class of the complex conjugation ρ. We also define

$$\mathscr{S}_0(M) = \{(1)\}, \qquad \mathscr{S}_r(M) = \{\ell_1 \cdots \ell_r \mid \ell_i \in \mathscr{S}_1(M) \text{ distinct}\} \qquad (r > 1).$$

(5.2.2) If $\ell \nmid (p)c(x)d_{K/F}$ and $\ell \notin S$, then the extension $K(x)(A[\mathfrak{p}^{M+M_0}])/F$ is unramified at ℓ, so it makes sense to consider the conjugacy class of $\mathrm{Fr}(\ell)_{\mathrm{arith}}$.

(5.2.3) By the Čebotarev density theorem, the set $\mathscr{S}_1(M)$ has positive density.

(5.2.4) If $\ell \in \mathscr{S}_1(M)$, then ℓ is inert in K/F. In particular, $\mathscr{S}_1(M) \subseteq \mathscr{S}_1$ (hence $\mathscr{S}_r(M) \subseteq \mathscr{S}_r$ for each $r \geq 0$).

(5.2.5) If $\ell \in \mathscr{S}_1(M)$, then $u(0) \mid (N\ell + 1)$ (by Proposition 4.8(i)) and

$$1 - a_\ell X + (N\ell)X^2 = \det(1 - \mathrm{Fr}(\ell)_{\mathrm{arith}} X \mid T_{\mathfrak{p}}A) \equiv \det(1 - \rho X \mid T_{\mathfrak{p}}A) = 1 - X^2\ (\mathrm{mod}\,\mathfrak{p}^{M+M_0}),$$

which implies that the following congruences hold in $\mathcal{O}_L$:

$$a_\ell \equiv 0\ (\mathrm{mod}\,\mathfrak{p}^{M+M_0}), \qquad N\ell + 1 \equiv 0\ (\mathrm{mod}\,u(0)\mathfrak{p}^M).$$

(5.3) From now on, we fix a sufficiently large integer $M >> 0$ divisible by the order of $\mathfrak{p}$ in the ideal class group of $\mathcal{O}_L$, and a generator of the principal ideal $\mathfrak{p}^M$ (also to be denoted $\mathfrak{p}^M$, by abuse of notation).

(5.4) Definition. *For each $\ell \in \mathscr{S}_1(M)$, fix a generator σ_ℓ of the cyclic group $G(\ell) = \mathrm{Gal}(K(x(\ell))/K(x))$ and define*

$$\mathrm{Tr}_\ell = \sum_{i=0}^{|G(\ell)|-1} \sigma_\ell^i, \qquad D_\ell = \sum_{i=0}^{|G(\ell)|-1} i\sigma_\ell^i \in \mathbf{Z}[G(\ell)];$$

these elements satisfy

$$(\sigma_\ell - 1)D_\ell = |G(\ell)| - \mathrm{Tr}_\ell = (N\ell + 1)/u(0) - \mathrm{Tr}_\ell.$$

For each $\mathfrak{n} = \ell_1 \cdots \ell_r \in \mathscr{S}_r(M)$ ($\ell_i \in \mathscr{S}_1(M)$), define

$$D_{\mathfrak{n}} = D_{\ell_1} \cdots D_{\ell_r} \in \mathbf{Z}[G(\ell_1)] \otimes \cdots \otimes \mathbf{Z}[G(\ell_r)] = \mathbf{Z}[G(\mathfrak{n})].$$

(5.5) Lemma. *For each $\mathfrak{n} \in \mathscr{S}_r(M)$, the image of the point $D_{\mathfrak{n}}y(\mathfrak{n}) \in A(K(x(\mathfrak{n}))')$ in $A(K(x(\mathfrak{n}))') \otimes \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^M$ (which will be denoted by $(D_{\mathfrak{n}}y(\mathfrak{n}) \pmod{\mathfrak{p}^M})$) is contained in $\left(A(K(x(\mathfrak{n}))') \otimes \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^M\right)^{G(\mathfrak{n})}$.*

Proof. If $\mathfrak{n} = \ell_1 \cdots \ell_r$, then we have, for each $i = 1, \ldots, r$,

$$(\sigma_{\ell_i} - 1)\, D_{\mathfrak{n}}\, y(\mathfrak{n}) = (N\ell_i + 1)/u(0)\, D_{\mathfrak{n}/\ell_i}\, y(\mathfrak{n}) - a_{\ell_i}\, D_{\mathfrak{n}/\ell_i}\, y(\mathfrak{n}/\ell_i) \in \mathfrak{p}^M A(K(x(\mathfrak{n}))').$$

(5.6) As $\mathfrak{p}^M$ is principal, the exact sequence of G_F-modules

$$0 \longrightarrow A[\mathfrak{p}^M] \longrightarrow A(\overline{\mathbf{Q}}) \xrightarrow{\mathfrak{p}^M} A(\overline{\mathbf{Q}}) \longrightarrow 0$$

induces, for each extension K' of F, the cohomology sequence

$$0 \longrightarrow A(K') \otimes \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^M \xrightarrow{\delta} H^1(K', A[\mathfrak{p}^M]) \longrightarrow H^1(K', A)[\mathfrak{p}^M] \longrightarrow 0.$$

Kolyvagin's **derivative classes** $[c(\mathfrak{n})]$ (which will be constructed in 5.7-9 below) are natural lifts of the classes $\delta(D_{\mathfrak{n}}y(\mathfrak{n}) \pmod{\mathfrak{p}^M})$ under the restriction maps [(1)]

$$\mathrm{res} : H^1(K(x), A[\mathfrak{p}^M]) \longrightarrow H^1(K(x(\mathfrak{n}))', A[\mathfrak{p}^M])^{G(\mathfrak{n})} \tag{5.6.1}$$

(of course, there is nothing to do if $\mathfrak{n} = (1)$, in which case one defines $[c((1))] = \delta(y((1))) = \delta(\iota(x) \otimes 1)$).

(5.7) In order to construct such cohomology classes $[c(\mathfrak{n})] \in H^1(K(x), A[\mathfrak{p}^M])$ (where $\mathfrak{n} = \ell_1 \cdots \ell_r \in \mathscr{S}_r$), we fix a point $z(\mathfrak{n}) \in A(\overline{\mathbf{Q}})$ satisfying $\mathfrak{p}^M z(\mathfrak{n}) = D_{\mathfrak{n}}y(\mathfrak{n}) \in A(K(x(\mathfrak{n}))')$. The cohomology class $\delta(D_{\mathfrak{n}}y(\mathfrak{n}) \pmod{\mathfrak{p}^M}) \in H^1(K(x(\mathfrak{n}))', A[\mathfrak{p}^M])$ is then represented by the 1-cocycle

$$(g \mapsto (g-1)z(\mathfrak{n})) \in Z^1(\mathrm{Gal}(\overline{\mathbf{Q}}/K(x(\mathfrak{n}))'), A[\mathfrak{p}^M]).$$

Note that the formula $g \mapsto (g-1)z(\mathfrak{n})$ makes sense even for $g \in \mathrm{Gal}(\overline{\mathbf{Q}}/K(x))$; it defines a 1-cocycle in $Z^1(\mathrm{Gal}(\overline{\mathbf{Q}}/K(x)), A(\overline{\mathbf{Q}}))$.

Denote by

$$\mathrm{pr} : \mathrm{Gal}(\overline{\mathbf{Q}}/K(x)) \longrightarrow \mathrm{Gal}(K(x(\mathfrak{n}))'/K(x)) = G(\mathfrak{n})$$

the natural surjection. We are going to define a 1-cocycle

$$d'(\mathfrak{n}) \in Z^1(G(\mathfrak{n}), A(K(x(\mathfrak{n}))'))$$

such that the 1-cocycle

$$c(\mathfrak{n}) : g \mapsto (\inf(d'(\mathfrak{n})))(g) + (g-1)z(\mathfrak{n}) = d'(\mathfrak{n})(\mathrm{pr}(g)) + (g-1)z(\mathfrak{n}) \in Z^1(\mathrm{Gal}(\overline{\mathbf{Q}}/K(x), A(\overline{\mathbf{Q}}))$$

will have values in $A[\mathfrak{p}^M]$. Its cohomology class $[c(\mathfrak{n})] \in H^1(K(x), A[\mathfrak{p}^M])$ will then satisfy

$$\mathrm{res}([c(\mathfrak{n})]) = \delta(D_{\mathfrak{n}}y(\mathfrak{n}) \pmod{\mathfrak{p}^M}).$$

In order to construct $d'(\mathfrak{n})$, we apply the following Lemma to $G = G(\mathfrak{n})$, $G_i = G(\ell_i)$, $\sigma_i = \sigma_{\ell_i}$, $X = A(K(x(\mathfrak{n}))')$.

[(1)] As the kernel (resp., cokernel) of the map res is equal (resp., injects) to $H^i(G(\mathfrak{n}), A(K(x(\mathfrak{n}))')[\mathfrak{p}^M])$ for $i = 1$ (resp., $i = 2$) and the torsion submodule $A(K[\infty])_{\mathrm{tors}}$ over $K[\infty] = \bigcup K[c]$ is finite (cf. [Ne-Sch, 2.2]), one sees directly, without any calculation, that such natural lifts exist if we multiply the points $y(\mathfrak{n})$ by the square of any fixed element of $\mathcal{O}_L - \{0\}$ which annihilates $A(K[\infty])_{\mathrm{tors}}$.

(5.8) Lemma. *Let $G = G_1 \times \cdots \times G_r$ be a finite product of finite cyclic groups G_i. For each G-module X, the evaluation of 1-cocycles at fixed generators $\sigma_i \in G_i$ induces an isomorphism of abelian groups*

$$\begin{aligned} Z^1(G,X) &\xrightarrow{\sim} \{(x_1,\ldots,x_r) \in X^r \mid (\forall i,j=1,\ldots,r)\,(1+\sigma_i+\cdots+\sigma_i^{|G_i|-1})x_i = 0,\ (\sigma_i-1)x_j = (\sigma_j-1)x_i\} \\ z &\mapsto (z(\sigma_1),\ldots,z(\sigma_r)). \end{aligned}$$

Proof. Easy exercise.

(5.9) Proposition-Definition. *If $\mathfrak{n} = \ell_1 \cdots \ell_r \in \mathscr{S}_r(M)$ ($r \geq 1$, $\ell_i \in \mathscr{S}_1(M)$), then:*
(i) *The elements*

$$x_i = D_{\mathfrak{n}/\ell_i}\left(\frac{a_{\ell_i}}{\mathfrak{p}^M}\, y(\mathfrak{n}/\ell_i) - \frac{N\ell_i+1}{u(0)\mathfrak{p}^M}\, y(\mathfrak{n})\right) \in A(K(x(\mathfrak{n}))') \qquad\qquad (i=1,\ldots,r)$$

satisfy

$$(\forall i,j=1,\ldots,r) \qquad \mathrm{Tr}_{\ell_i}\, x_i = 0, \qquad (\sigma_{\ell_i}-1)x_j = (\sigma_{\ell_j}-1)x_i.$$

(ii) *There exists a unique 1-cocycle $d'(\mathfrak{n}) \in Z^1(G(\mathfrak{n}), A(K(x(\mathfrak{n}))')$ satisfying*

$$(\forall i=1,\ldots,r) \qquad d'(\mathfrak{n})(\sigma_{\ell_i}) = x_i.$$

(iii) *The cohomology class of $d'(\mathfrak{n})$ lies in $H^1(G(\mathfrak{n}), A(K(x(\mathfrak{n}))'))[\mathfrak{p}^M]$; more precisely, we have*

$$(\forall i=1,\ldots,r) \qquad \mathfrak{p}^M d'(\mathfrak{n})(\sigma_{\ell_i}) = -(\sigma_{\ell_i}-1)D_{\mathfrak{n}}y(\mathfrak{n}).$$

(iv) *Define $d(\mathfrak{n}) = \inf(d'(\mathfrak{n})) \in Z^1(\mathrm{Gal}(\overline{\mathbf{Q}}/K(x)), A(\overline{\mathbf{Q}}))$, i.e. $d(\mathfrak{n})(g) = d'(\mathfrak{n})(\mathrm{pr}(g))$.*
(v) *Define $d((1)) = 0 \in Z^1(\mathrm{Gal}(\overline{\mathbf{Q}}/K(x)), A(\overline{\mathbf{Q}}))$.*

Proof. (i) Firstly, the congruences 5.2.5 show that $a_{\ell_i}/\mathfrak{p}^M$ and $(N\ell_i+1)/u(0)\mathfrak{p}^M$ are contained in $\mathcal{O}_L$, so the definition of x_i makes sense. Secondly, the relation 4.13(i) together with 4.10(i) imply that we have

$$\mathrm{Tr}_{\ell_i}\, x_i = D_{\mathfrak{n}/\ell_i}\left(\frac{a_{\ell_i}}{\mathfrak{p}^M}\,|G(\ell_i)| - \frac{N\ell_i+1}{u(0)\mathfrak{p}^M}\, a_{\ell_i}\right) y(\mathfrak{n}/\ell_i) = 0$$

and, if $i \neq j$,

$$\begin{aligned} (\sigma_{\ell_i}-1)x_j &= D_{\mathfrak{n}/\ell_i\ell_j}\left(\frac{N\ell_i+1}{u(0)} - \mathrm{Tr}_{\ell_i}\right)\left(\frac{a_{\ell_j}}{\mathfrak{p}^M}\, y(\mathfrak{n}/\ell_j) - \frac{N\ell_j+1}{u(0)\mathfrak{p}^M}\, y(\mathfrak{n})\right) = \\ &= D_{\mathfrak{n}/\ell_i\ell_j}\left(-\frac{(N\ell_i+1)(N\ell_j+1)}{u(0)^2\mathfrak{p}^M}\, y(\mathfrak{n}) + \frac{(N\ell_i+1)a_{\ell_j}}{u(0)\mathfrak{p}^M}\, y(\mathfrak{n}/\ell_j) + \frac{(N\ell_j+1)a_{\ell_i}}{u(0)\mathfrak{p}^M}\, y(\mathfrak{n}/\ell_i) - \frac{a_{\ell_i}a_{\ell_j}}{\mathfrak{p}^M}\, y(\mathfrak{n}/\ell_i\ell_j)\right) = \\ &= (\sigma_{\ell_j}-1)x_i. \end{aligned}$$

(ii) This follows from (i) and Lemma 5.8.
(iii) We compute, using again 4.10(i) and 4.13(i), that

$$\mathfrak{p}^M d'(\mathfrak{n})(\sigma_{\ell_i}) = D_{\mathfrak{n}/\ell_i}\,(a_{\ell_i}\, y(\mathfrak{n}/\ell_i) - (N\ell_i+1)/u(0)\, y(\mathfrak{n})) = -D_{\mathfrak{n}/\ell_i}(\sigma_{\ell_i}-1)D_{\ell_i}\, y(\mathfrak{n}) = -(\sigma_{\ell_i}-1)D_{\mathfrak{n}}y(\mathfrak{n}).$$

As $d'(\mathfrak{n})$ is a 1-cocycle, it follows that $\mathfrak{p}^M d'(\mathfrak{n})$ is a coboundary.

(5.10) Proposition-Definition. *Let $\mathfrak{n} = \ell_1 \cdots \ell_r \in \mathscr{S}_r(M)$ ($r \geq 0$, $\ell_i \in \mathscr{S}_1(M)$). The 1-cocycle $c(\mathfrak{n}) \in Z^1(\mathrm{Gal}(\overline{\mathbf{Q}}/K(x)), A(\overline{\mathbf{Q}}))$, defined by the formula*

$$c(\mathfrak{n}) : g \mapsto d(\mathfrak{n})(g) + (g-1)z(\mathfrak{n}),$$

has the following properties:
(i) $c(\mathfrak{n}) \in Z^1(\mathrm{Gal}(\overline{\mathbf{Q}}/K(x)), A[\mathfrak{p}^M])$.
(ii) *The cohomology class $[c(\mathfrak{n})] \in H^1(K(x), A[\mathfrak{p}^M])$ does not depend on the choice of $z(\mathfrak{n})$.*
(iii) *The image of $[c(\mathfrak{n})]$ under the restriction map (5.6.1) is equal to*

$$\mathrm{res}([c(\mathfrak{n})]) = \delta(D_{\mathfrak{n}} y(\mathfrak{n}) \pmod{\mathfrak{p}^M}) \in H^1(K(x(\mathfrak{n}))', A[\mathfrak{p}^M]).$$

(iv) *The image of $[c(\mathfrak{n})]$ in $H^1(K(x), A(\overline{\mathbf{Q}}))$ is equal to $[d(\mathfrak{n})]$.*

Proof. (i) As $c(\mathfrak{n})$ is a 1-cocycle, it is sufficient to check that $\mathfrak{p}^M c(\mathfrak{n})(g) = 0$, for each element of $\mathrm{Ker}(\mathrm{pr}) = \mathrm{Gal}(\overline{\mathbf{Q}}/K(x(\mathfrak{n}))')$ and for each $g \in \mathrm{pr}^{-1}(\sigma_{\ell_i})$ ($i = 1, \ldots, r$). If $g \in \mathrm{Ker}(\mathrm{pr})$, then

$$\mathfrak{p}^M c(\mathfrak{n})(g) = (g-1) D_{\mathfrak{n}} y(\mathfrak{n}) = 0.$$

If $\mathrm{pr}(g) = \sigma_{\ell_i}$, then we have, by Proposition 5.9(iii),

$$\mathfrak{p}^M c(\mathfrak{n})(g) = -(\sigma_{\ell_i} - 1) D_{\mathfrak{n}} y(\mathfrak{n}) + (g-1) D_{\mathfrak{n}} y(\mathfrak{n}) = 0.$$

(ii) Two choices of $z(\mathfrak{n})$ differ by an element of $A[\mathfrak{p}^M]$.
(iii) For each element $g \in \mathrm{Gal}(\overline{\mathbf{Q}}/K(x(\mathfrak{n}))')$, we have

$$(\mathrm{res}(c(\mathfrak{n}))(g) = (g-1)z(\mathfrak{n}) = \delta(D_{\mathfrak{n}} y(\mathfrak{n}) \pmod{\mathfrak{p}^M}))(g).$$

(iv) The cohomology class of $(g-1)z(\mathfrak{n})$ vanishes in $H^1(K(x), A(\overline{\mathbf{Q}}))$.

(5.11) We now investigate the **localizations**

$$[c(\mathfrak{n})_v] \in H^1(K(x)_v, A[\mathfrak{p}^M]), \qquad [d(\mathfrak{n})_v] \in H^1(K(x)_v, A(\overline{\mathbf{Q}}))[\mathfrak{p}^M] = H^1(K(x)_v, A)[\mathfrak{p}^M]$$

of the cohomology classes $[c(\mathfrak{n})]$ and $[d(\mathfrak{n})]$ at various primes v of $K(x)$.

(5.12) Proposition (Localization outside $\mathfrak{n}$). *Let v be a non-archimedean prime of $K(x)$ lying above a prime v_F of F. Denote by $\widetilde{A}_v$ the special fibre at v of the Néron model of $A \otimes_F K(x)$ over $\mathcal{O}_{K(x)}$, by $\pi_0(\widetilde{A}_v)$ the $\mathcal{O}_L$-module of the connected components of $\widetilde{A}_v$, and define*

$$C_{1,v}(\mathfrak{p}) = \min\{c \geq 0 \mid \mathfrak{p}^c \cdot \pi_0(\widetilde{A}_v)_{\mathfrak{p}} = 0\}.$$

If $v_F \nmid \mathfrak{n}$, then

$$\mathfrak{p}^{C_{1,v}(\mathfrak{p})} \cdot [d(\mathfrak{n})_v] = 0.$$

In particular, if $v_F \nmid \mathfrak{n}$ and $v \notin S$, then $[d(\mathfrak{n})_v] = 0$.

Proof. If $v_F \nmid \mathfrak{n}$, then v is unramified in $K(x(\mathfrak{n}))'/K(x)$, hence the cohomology class $[d(\mathfrak{n})_v]$ is inflated from an element of the cohomology group $H^1_{ur}(K(x)_v, A)[\mathfrak{p}^M]$, which is isomorphic to $H^1(\kappa(v), \pi_0(\widetilde{A}_v))[\mathfrak{p}^M]$, where $\kappa(v)$ denotes the residue field of v ([Mi 1, I.3.8]). This implies that the annihilator of $\pi_0(\widetilde{A}_v)_{\mathfrak{p}}$ kills $[d(\mathfrak{n})_v]$. If, in addition, $v \notin S$, then A has good reduction at v_F, $A \otimes_F K(x)$ has good reduction at v and $\pi_0(\widetilde{A}_v) = 0$.

(5.13) If $\ell \in \mathscr{S}_1(M)$, fix primes $w \mid v \mid \lambda \mid \ell$ in the fields

$$K(x(\ell)) \supset K(x) \supset K \supset F,$$

respectively (of course, λ is unique and w is uniquely determined by v, by Proposition 4.6). We denote by $\mathrm{Fr}(v) = \mathrm{Fr}(v)_{\mathrm{geom}}$ etc. the various **geometric** Frobenius elements.

The assumption $\ell \in \mathscr{S}_1(M)$ implies that $\mathrm{Fr}(v) = \mathrm{Fr}(\lambda) = \mathrm{Fr}(\ell)^2$ acts trivially on $A[\mathfrak{p}^M]$, hence the evaluation map

$$\begin{aligned} \mathrm{ev}_{\mathrm{Fr}(v)} : H^1_{ur}(K(x)_v, A[\mathfrak{p}^M]) = \mathrm{Hom}(\langle \mathrm{Fr}(v)\rangle, A(K(x)_v)[\mathfrak{p}^M]) &\xrightarrow{\sim} A(K(x)_v)[\mathfrak{p}^M] \\ f &\mapsto f(\mathrm{Fr}(v)) \end{aligned}$$

is an isomorphism.

(5.14) Proposition. *If $\ell \in \mathscr{S}_1(M)$ and if $v \mid \ell$ is a prime of $K(x)$ above ℓ, then all maps in the following diagram are isomorphisms and the diagram is commutative.*

$$\begin{array}{ccccc} A(K(x)_v) \otimes_{\mathcal{O}_L} \mathcal{O}_L/\mathfrak{p}^M & \xrightarrow{\delta_v} & H^1_{ur}(K(x)_v, A[\mathfrak{p}^M]) = \mathrm{Hom}(\langle \mathrm{Fr}(v)\rangle, A(K(x)_v)[\mathfrak{p}^M]) & \xrightarrow{\mathrm{ev}_{\mathrm{Fr}(v)}} & A(K(x)_v)[\mathfrak{p}^M] \\ \downarrow{\scriptstyle \mathrm{red}_v} & & & & \downarrow{\scriptstyle \mathrm{red}_v} \\ \widetilde{A}_v(\kappa(v)) \otimes_{\mathcal{O}_L} \mathcal{O}_L/\mathfrak{p}^M & & \xrightarrow{(a_\ell \mathrm{Fr}(\ell) - (N\ell+1))/\mathfrak{p}^M N\ell = ((N\ell+1) - a_\ell \mathrm{Fr}(\ell))/\mathfrak{p}^M} & & \widetilde{A}_v(\kappa(v))[\mathfrak{p}^M] \end{array}$$

Proof. The map δ_v is an isomorphism, as A has good reduction at ℓ and $v \nmid p$. The evaluation map $\mathrm{ev}_{\mathrm{Fr}(v)}$ is an isomorphism, by 5.13. Both vertical maps are isomorphisms, as the kernel of the surjective reduction map $\mathrm{red}_v : A(K(x)_v) \longrightarrow \widetilde{A}_v(\kappa(v))$ is a pro-$char(\kappa(v))$-group and $v \nmid p$. It remains to show that the diagram is commutative (which will imply that the bottom horizontal map is also an isomorphism). As the composite map

$$f : A(K(x)_v)[\mathfrak{p}^\infty] \hookrightarrow A(K(x)_v) \twoheadrightarrow A(K(x)_v) \otimes_{\mathcal{O}_L} \mathcal{O}_L/\mathfrak{p}^M$$

is surjective, it is sufficient to compute $\mathrm{ev}_{\mathrm{Fr}(v)} \circ \delta_v \circ f(P)$ for $P \in A(K(x)_v)[\mathfrak{p}^\infty]$. If we fix a point $Q \in A(\overline{K(x)_v})$ such that $\mathfrak{p}^M Q = P$, then

$$\begin{aligned} \mathrm{ev}_{\mathrm{Fr}(v)} \circ \delta_v \circ f(P) = (\mathrm{Fr}(v) - 1)(Q) = (\mathrm{Fr}(\ell)^2 - 1)(Q) = \frac{a_\ell \mathrm{Fr}(\ell) - (N\ell+1)}{N\ell}(Q) = \\ = \frac{a_\ell \mathrm{Fr}(\ell) - (N\ell+1)}{\mathfrak{p}^M N\ell}(P) = \frac{(N\ell+1) - a_\ell \mathrm{Fr}(\ell)}{\mathfrak{p}^M}(P), \end{aligned}$$

as

$$N\ell \equiv -1 \ (\mathrm{mod}\, \mathfrak{p}^M), \qquad Q \in A(K(x)_v)[\mathfrak{p}^\infty] \qquad \text{and} \qquad \mathrm{Fr}(\ell)^{-2} - a_\ell \mathrm{Fr}(\ell)^{-1} + N\ell = 0 \quad \text{on} \quad T_{\mathfrak{p}}(A).$$

(5.15) In the situation of 5.13 we identify the $\mathcal{O}_L/\mathfrak{p}^M$-modules

$$\frac{H^1(K(x)_v, A[\mathfrak{p}^M])}{H^1_{ur}(K(x)_v, A[\mathfrak{p}^M])} = \frac{H^1(K(x)_v, A[\mathfrak{p}^M])}{\mathrm{Im}(\delta_v)} \xrightarrow{\sim} H^1(K(x)_v, A)[\mathfrak{p}^M].$$

The evaluation at the fixed generator $\sigma_\ell \in G(\ell)$ defines an isomorphism

$$\begin{aligned} \mathrm{ev}_{\sigma_\ell} : \frac{H^1(K(x)_v, A[\mathfrak{p}^M])}{H^1_{ur}(K(x)_v, A[\mathfrak{p}^M])} &\xrightarrow{\sim} H^1(K(x)_v^{ur}, A[\mathfrak{p}^M])^{\mathrm{Fr}(v)=1} = \mathrm{Hom}(I_v^t, A[\mathfrak{p}^M])^{\mathrm{Fr}(v)=1} = \\ = \mathrm{Hom}(I_v^t, A[\mathfrak{p}^M]) &\xleftarrow{\sim} \mathrm{Hom}(G(\ell), A(K(x)_v)[\mathfrak{p}^M]) \xrightarrow{\mathrm{ev}_{\sigma_\ell}} A(K(x)_v)[\mathfrak{p}^M] \end{aligned}$$

(where $G(\ell)$ is identified with the quotient $\mathrm{Gal}(K(x(\ell))_w K(x)_v^{ur}/K(x)_v^{ur})$ of the tame inertia group I_v^t at v). We denote by $\Phi_v = \mathrm{ev}_{\sigma_\ell}^{-1} \circ \mathrm{ev}_{\mathrm{Fr}(v)}$ the isomorphism defined by the following commutative diagram:

$$\begin{array}{ccc} H^1_{ur}(K(x)_v, A[\mathfrak{p}^M]) & \xrightarrow{\Phi_v} & \frac{H^1(K(x)_v, A[\mathfrak{p}^M])}{H^1_{ur}(K(x)_v, A[\mathfrak{p}^M])} \\ \Big\downarrow{\scriptstyle \mathrm{ev}_{\mathrm{Fr}(v)}} & & \Big\downarrow{\scriptstyle \mathrm{ev}_{\sigma_\ell}} \\ A(K(x)_v)[\mathfrak{p}^M] & = & A(K(x)_v)[\mathfrak{p}^M] \end{array}$$

As $N\ell \equiv -1 \pmod{\mathfrak{p}^M}$, the conjugation action of $\mathrm{Fr}(\ell)$ on $I_v^t \otimes \mathcal{O}_L/\mathfrak{p}^M$ is given by multiplication by -1. In particular,

$$\Phi_v \circ \mathrm{Fr}(\ell) = -\mathrm{Fr}(\ell) \circ \Phi_v. \tag{5.15.1}$$

(5.16) Proposition. *If $\mathfrak{n}\ell \in \mathscr{S}_{r+1}(M)$ ($\mathfrak{n} \in \mathscr{S}_r(M)$, $\ell \in \mathscr{S}_1(M)$, $r \geq 0$) and if $v \mid \ell$ is a prime of $K(x)$ above ℓ, then the localization*

$$[d(\mathfrak{n}\ell)_v] \in H^1(K(x)_v, A)[\mathfrak{p}^M] \xleftarrow{\sim} \frac{H^1(K(x)_v, A[\mathfrak{p}^M])}{H^1_{ur}(K(x)_v, A[\mathfrak{p}^M])}$$

is equal to

$$[d(\mathfrak{n}\ell)_v] = -\Phi_v\left(\mathrm{Fr}(\ell)\,[c(\mathfrak{n})_v]\right).$$

Proof. The commutative diagram

$$\begin{array}{ccc} H^1(K(x(\ell))_w/K(x)_v, A(K(x(\ell))_w))[\mathfrak{p}^M] & \xrightarrow{\mathrm{red}_w} & H^1(G(\ell), \widetilde{A}_v(\kappa(w)))[\mathfrak{p}^M] \\ \Big\downarrow & & \| \\ H^1(K(x(\ell))_w K(x)_v^{ur}/K(x)_v^{ur}, A(\overline{K(x)_v}))[\mathfrak{p}^M] & & \mathrm{Hom}(G(\ell), \widetilde{A}_v(\kappa(v))[\mathfrak{p}^M]) \\ \Big\downarrow & & \Big\uparrow{\scriptstyle \wr \mathrm{red}_v} \\ H^1(K(x)_v^{ur}, A(\overline{K(x)_v}))[\mathfrak{p}^M] & & \mathrm{Hom}(G(\ell), A(K(x)_v)[\mathfrak{p}^M]) \\ \Big\uparrow{\scriptstyle \wr} & & \Big\downarrow{\scriptstyle \wr} \\ H^1(K(x)_v^{ur}, A[\mathfrak{p}^M]) & = & \mathrm{Hom}(I_v^t, A(K(x)_v)[\mathfrak{p}^M]) \end{array}$$

implies that

$$\begin{aligned} \mathrm{red}_v \circ \mathrm{ev}_{\sigma_\ell}\left([d(\mathfrak{n}\ell)_v]\right) = \mathrm{red}_v\left([d'(\mathfrak{n}\ell)_v](\sigma_\ell)\right) = \mathrm{red}_v\left(D_{\mathfrak{n}}\left(\frac{a_\ell}{\mathfrak{p}^M}\, y(\mathfrak{n}) - \frac{N\ell+1}{u(0)\mathfrak{p}^M}\, y(\mathfrak{n}\ell)\right)\right) \overset{4.12(ii)}{=\!=} \\ = D_{\mathfrak{n}}\left(\frac{a_\ell}{\mathfrak{p}^M} - \frac{(N\ell+1)\mathrm{Fr}(\ell)}{\mathfrak{p}^M}\right) \mathrm{red}_v\, y(\mathfrak{n}) = \left(\frac{a_\ell\,\mathrm{Fr}(\ell) - (N\ell+1)}{\mathfrak{p}^M}\right) \mathrm{Fr}(\ell)\,\mathrm{red}_v(D_{\mathfrak{n}} y(\mathfrak{n})) \overset{5.14}{=\!=} \\ = -\mathrm{Fr}(\ell)\,\mathrm{red}_v\left(\mathrm{ev}_{\mathrm{Fr}(v)} \circ \delta_v(D_{\mathfrak{n}} y(\mathfrak{n}) \pmod{\mathfrak{p}^M})\right) \end{aligned}$$

(where we have used the fact that $\mathrm{Fr}(\ell)^2 = \mathrm{Fr}(\lambda) = \mathrm{Fr}(v)$ acts trivially on $\kappa(v)$ and $K(x)_v$). As the reduction map $\mathrm{red}_v : A(K(x)_v)[\mathfrak{p}^M] \longrightarrow \widetilde{A}_v(\kappa(v))[\mathfrak{p}^M]$ is an isomorphism, it follows that

$$[d(\mathfrak{n}\ell)_v] = -\mathrm{ev}_{\sigma_\ell}^{-1} \circ \mathrm{ev}_{\mathrm{Fr}(v)}\left(\mathrm{Fr}(\ell)\,[c(\mathfrak{n})_v]\right) = -\Phi_v\left(\mathrm{Fr}(\ell)\,[c(\mathfrak{n})_v]\right).$$

(5.17) If $\ell \in \mathscr{S}_1(M)$, fix a prime v_α of $K(\alpha)$ above ℓ. As $\ell\mathcal{O}_K$ splits completely in $K(x)/K$ (by Proposition 4.6(ii)), we have, for each prime $v \mid v_\alpha$ of $K(x)$, natural identifications $K(\alpha)_{v_\alpha} = K(x)_v$ and isomorphisms

$$\begin{aligned} &\mathrm{ev}_{\mathrm{Fr}(v_\alpha)} : H^1_{ur}(K(\alpha)_{v_\alpha}, A[\mathfrak{p}^M]) \xrightarrow{\sim} A(K(\alpha)_{v_\alpha})[\mathfrak{p}^M] \\ &\mathrm{ev}_{\sigma_\ell} : H^1(K(\alpha)_{v_\alpha}, A[\mathfrak{p}^M])/H^1_{ur}(K(\alpha)_{v_\alpha}, A[\mathfrak{p}^M]) \xrightarrow{\sim} A(K(\alpha)_{v_\alpha})[\mathfrak{p}^M] \\ &\Phi_{v_\alpha} = \mathrm{ev}_{\sigma_\ell}^{-1} \circ \mathrm{ev}_{\mathrm{Fr}(v_\alpha)} : H^1_{ur}(K(\alpha)_{v_\alpha}, A[\mathfrak{p}^M]) \xrightarrow{\sim} H^1(K(\alpha)_{v_\alpha}, A[\mathfrak{p}^M])/H^1_{ur}(K(\alpha)_{v_\alpha}, A[\mathfrak{p}^M]). \end{aligned}$$

(5.18) Proposition. *If $\mathfrak{n}\ell \in \mathscr{S}_{r+1}(M)$ ($\mathfrak{n} \in \mathscr{S}_r(M)$, $\ell \in \mathscr{S}_1(M)$, $r \geq 0$) and if $v_\alpha \mid \ell$ is a prime of $K(\alpha)$ above ℓ, then the localization*

$$\left[\left(\mathrm{cor}_{K(x)/K(\alpha)}\, d(\mathfrak{n}\ell)\right)_{v_\alpha}\right] \in H^1(K(\alpha)_{v_\alpha}, A)[\mathfrak{p}^M] \xleftarrow{\sim} \frac{H^1(K(\alpha)_{v_\alpha}, A[\mathfrak{p}^M])}{H^1_{ur}(K(\alpha)_{v_\alpha}, A[\mathfrak{p}^M])}$$

is equal to

$$\left[\left(\mathrm{cor}_{K(x)/K(\alpha)}\, d(\mathfrak{n}\ell)\right)_{v_\alpha}\right] = -\Phi_v\left(\mathrm{Fr}(\ell)\ \left[\left(\mathrm{cor}_{K(x)/K(\alpha)}\, c(\mathfrak{n})\right)_{v_\alpha}\right]\right).$$

Proof. This follows from Proposition 5.16 and the fact that

$$(\forall X = A, A[\mathfrak{p}^M])\ (\forall c \in H^1(K(x), X)) \qquad \left(\mathrm{cor}_{K(x)/K(\alpha)}\,(c)\right)_{v_\alpha} = \sum_{v|v_\alpha} \mathrm{cor}_{K(x)_v/K(\alpha)_{v_\alpha}}\,(c_v) = \sum_{v|v_\alpha} c_v.$$

(5.19) The Weil pairings. The Weil pairing

$$(\ ,\ )_{A_j} : T_p(A_j) \times T_p(\widehat{A_j}) \longrightarrow \mathbf{Z}_p(1)$$

is G_F-equivariant and satisfies

$$(\forall f \in \mathrm{End}_F(A_j) = \mathcal{O}_{L_j}) \qquad (f(x), y)_{A_j} = (x, \widehat{f}(y))_{A_j}.$$

Fix a polarization $\varphi : A_j \longrightarrow \widehat{A_j}$ defined over F. As the corresponding Rosati involution acts trivially on $\mathcal{O}_{L_j}$ (by Proposition 1.18(v)), the induced skew-symmetric pairing

$$T_p(A_j) \times T_p(A_j) \longrightarrow \mathbf{Z}_p(1), \qquad x, y \mapsto (x, \varphi(y))_{A_j}$$

factors through $T_p(A_j) \otimes_{\mathcal{O}_{L_j}} T_p(A_j)$ and preserves the decomposition

$$T_p(A_j) = \bigoplus_{P|p} T_P(A_j),$$

where P runs through all primes of L_j above p. Denote by

$$(\ ,\ )_{\mathfrak{p}_j} : T_{\mathfrak{p}_j}(A_j) \otimes_{\mathcal{O}_{\mathfrak{p}_j}} T_{\mathfrak{p}_j}(A_j) \longrightarrow \mathbf{Z}_p(1)$$

its $\mathfrak{p}_j$-component, where $\mathfrak{p}_j = \mathfrak{p} \cap \mathcal{O}_{L_j}$ and $\mathcal{O}_{\mathfrak{p}_j} = \mathcal{O}_{L_j, \mathfrak{p}_j}$.
Fix a generator $d \in \mathscr{D}^{-1}_{\mathcal{O}_{\mathfrak{p}_j}/\mathbf{Z}_p}$ of the inverse different; the map

$$\lambda : \mathcal{O}_{\mathfrak{p}_j} \xrightarrow{\sim} \mathrm{Hom}_{\mathbf{Z}_p}(\mathcal{O}_{\mathfrak{p}_j}, \mathbf{Z}_p), \qquad x \mapsto (y \mapsto \mathrm{Tr}_{\mathcal{O}_{\mathfrak{p}_j}/\mathbf{Z}_p}(dxy))$$

is a symmetric isomorphism of $\mathcal{O}_{\mathfrak{p}_j}$-modules. The composition of the two maps

$$\begin{aligned} T_{\mathfrak{p}_j}(A_j) \longrightarrow \mathrm{Hom}_{\mathcal{O}_{\mathfrak{p}_j}}(T_{\mathfrak{p}_j}(A_j), \mathrm{Hom}_{\mathbf{Z}_p}(\mathcal{O}_{\mathfrak{p}_j}, \mathbf{Z}_p(1))) &\xrightarrow{\mathrm{Hom}(\mathrm{id}, \lambda^{-1})} \mathrm{Hom}_{\mathcal{O}_{\mathfrak{p}_j}}(T_{\mathfrak{p}_j}(A_j), \mathcal{O}_{\mathfrak{p}_j}(1)) \\ x \ \mapsto\ (y \ \mapsto\ (a \ \mapsto\ (x, ay)_{\mathfrak{p}_j})) & \end{aligned}$$

defines, by adjunction, a skew-symmetric $\mathcal{O}_{\mathfrak{p}_j}$-bilinear G_F-equivariant pairing

$$(\ ,\ )_j : T_{\mathfrak{p}_j}(A_j) \times T_{\mathfrak{p}_j}(A_j) \longrightarrow \mathcal{O}_{\mathfrak{p}_j}(1)$$

characterized by the property

$$(\forall x, y \in T_{\mathfrak{p}_j}(A_j))\ (\forall a \in \mathcal{O}_{\mathfrak{p}_j}) \qquad \mathrm{Tr}_{\mathcal{O}_{\mathfrak{p}_j}/\mathbf{Z}_p}(da(x, y)_j) = (x, ay)_{\mathfrak{p}_j} = (ax, y)_{\mathfrak{p}_j}.$$

On tensoring with $\mathcal{O}_{\mathfrak{p}} = \mathcal{O}_{L,\mathfrak{p}}$, we obtain a skew-symmetric $\mathcal{O}_{\mathfrak{p}}$-bilinear G_F-equivariant pairing on $T_{\mathfrak{p}}(A) = T_{\mathfrak{p}_j}(A_j) \otimes_{\mathcal{O}_{\mathfrak{p}_j}} \mathcal{O}_{\mathfrak{p}}$:

$$(\ , \ ) : T_{\mathfrak{p}}(A) \times T_{\mathfrak{p}}(A) \longrightarrow \mathcal{O}_{\mathfrak{p}}(1)$$
$$x \otimes a,\ y \otimes b \ \mapsto \ ab(x,y)_j \qquad\qquad (x, y \in T_{\mathfrak{p}_j}(A_j);\ a, b \in \mathcal{O}_{\mathfrak{p}}).$$

The adjoint map $T_{\mathfrak{p}}(A) \longrightarrow \mathrm{Hom}_{\mathcal{O}_{\mathfrak{p}}}(T_{\mathfrak{p}}(A), \mathcal{O}_{\mathfrak{p}}(1))$ is injective and its cokernel is killed by $\deg(\varphi)$. Reducing $(\ , \ )$ modulo $\mathfrak{p}^M$ yields a skew-symmetric $\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^M$-bilinear G_F-equivariant pairing

$$(\ , \ )_M : A[\mathfrak{p}^M] \times A[\mathfrak{p}^M] \longrightarrow \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^M(1), \tag{5.19.1}$$

whose kernel is killed by $\deg(\varphi)$. This implies that, for each $\mathcal{O}_{\mathfrak{p}}$-submodule $Y \subset A[\mathfrak{p}^M]$ isomorphic to $\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^{M-c}$, we have

$$2\deg(\varphi)\,\mathfrak{p}^c\, Y^{\perp} \subseteq Y. \tag{5.19.2}$$

(5.20) Proposition. *In the situation of 5.16, let v_α be the prime of $K(\alpha)$ induced by v and $\zeta_v \in K(\alpha)_{v_\alpha} = K(x)_v$ be a root of unity whose image under the reciprocity map $rec_v : K(x)_v^* \longrightarrow G_{K(x)_v}^{ab}$ induces $\sigma_\ell \in \mathrm{Gal}(K(x(\ell))_w/K(x)_v)$. Then we have, for each $x \in H^1_{ur}(K(\alpha)_{v_\alpha}, A[\mathfrak{p}^M])$,*

$$\zeta_v \otimes \mathrm{inv}_{v_\alpha}\Big(x \cup \big(\mathrm{cor}_{K(x)/K(\alpha)}\, c(\mathfrak{n}\ell)\big)_{v_\alpha}\Big) = -\Big(\mathrm{ev}_{\mathrm{Fr}(v_\alpha)}(x), \mathrm{Fr}(\ell)\,\mathrm{ev}_{\mathrm{Fr}(v_\alpha)}\big(\mathrm{cor}_{K(x)/K(\alpha)}\, c(\mathfrak{n})\big)_{v_\alpha}\Big)_M \in \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^M(1),$$

where $\cup$ denotes the cup product

$$H^1(K(\alpha)_{v_\alpha}, A[\mathfrak{p}^M]) \times H^1(K(\alpha)_{v_\alpha}, A[\mathfrak{p}^M]) \xrightarrow{\cup} H^2(K(\alpha)_{v_\alpha}, \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^M(1)) \xrightarrow{\mathrm{inv}_{v_\alpha}} \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^M$$

induced by the pairing $(\ , \ )_M$.

Proof. Combine Proposition 5.18 with Lemma 5.21 below (using the identification $K(\alpha)_{v_\alpha} = K_\lambda$, where $\lambda = \ell\mathcal{O}_K$).

(5.21) Lemma. *Let $\ell \in \mathscr{S}_1(M)$, $\lambda = \ell\mathcal{O}_K$. If $\zeta \in K_\lambda^*$ is a root of unity of order prime to $N\ell$, then we have, for each $x \in H^1_{ur}(K_\lambda, A[\mathfrak{p}^M])$ and $y \in H^1(K_\lambda, A[\mathfrak{p}^M])$,*

$$\zeta \otimes \mathrm{inv}_\lambda(x \cup y) = (x(\mathrm{Fr}(\lambda)), y(\mathrm{rec}_\lambda(\zeta)))_M \in \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^M(1),$$

where $\mathrm{rec}_\lambda : K_\lambda^* \longrightarrow G_{K_\lambda}^{ab}$ denotes the reciprocity map (normalized in such a way that the geometric Frobenius element $\mathrm{Fr}(\lambda)$ corresponds to a uniformizer).

Proof. We can assume that ζ is a primitive root of unity of order $n = N\lambda - 1$. Denoting by $\delta : K_\lambda^* \otimes \mathbf{Z}/n\mathbf{Z} \xrightarrow{\sim} H^1(K_\lambda, \mu_n)$ the standard Kummer map, then we have

$$x = \delta\zeta \otimes a \otimes \zeta^{\otimes -1} \in H^1_{ur}(K_\lambda, \mu_n) \otimes A[\mathfrak{p}^M] \otimes \mu_n^{\otimes -1} = H^1_{ur}(K_\lambda, A[\mathfrak{p}^M])$$
$$y = \delta u \otimes b \otimes \zeta^{\otimes -1} \in H^1(K_\lambda, \mu_n) \otimes A[\mathfrak{p}^M] \otimes \mu_n^{\otimes -1} = H^1(K_\lambda, A[\mathfrak{p}^M])$$

for some $a, b \in A[\mathfrak{p}^M]$ and $u \in K_\lambda^*$ (recall that G_{K_λ} acts trivially on $A[\mathfrak{p}^M]$, since $\ell \in \mathscr{S}_1(M)$). As the reciprocity map is normalized by letting the uniformizers correspond to geometric Frobenius elements,

$$x(\mathrm{Fr}(\lambda)) = (\delta\zeta)(\mathrm{Fr}(\lambda)) \otimes a \otimes \zeta^{\otimes -1} = \zeta^{-1} \otimes a \otimes \zeta^{\otimes -1} = -a.$$

For each character $\chi \in \mathrm{Hom}_{\mathrm{cont}}(G_{K_\lambda}, \mathbf{Q}/\mathbf{Z}) = H^1(G_{K_\lambda}, \mathbf{Q}/\mathbf{Z})$, we have ([Se 1, Prop. XI.2])

$$(\forall z \in K_\lambda^*) \qquad \chi(\mathrm{rec}_\lambda(z)) = \mathrm{inv}_\lambda(z \cup \delta\chi) = -\mathrm{inv}_\lambda(\delta z \cup \chi) = \mathrm{inv}_\lambda(\chi \cup \delta z), \tag{5.21.1}$$

where $\delta\chi \in H^2(G_{K_\lambda}, \mathbf{Z})$ denotes the coboundary associated to the exact sequence

$$0 \longrightarrow \mathbf{Z} \longrightarrow \mathbf{Q} \longrightarrow \mathbf{Q}/\mathbf{Z} \longrightarrow 0.$$

Using (5.21.1) with $z = \zeta$ and $z = u$, we obtain

$$y(\mathrm{rec}_\lambda(\zeta)) = (\delta u)(\mathrm{rec}_\lambda(\zeta)) \otimes b \otimes \zeta^{\otimes -1} = -(\delta\zeta)(\mathrm{rec}_\lambda(u)) \otimes b \otimes \zeta^{\otimes -1} \ (= \mathrm{ord}_\lambda(u)b)$$
$$\zeta \otimes \mathrm{inv}_\lambda(x \cup y) = \mathrm{inv}_\lambda(\delta\zeta \cup \delta u)\,(a,b)_M \otimes \zeta^{\otimes -1} = (\delta\zeta)(\mathrm{rec}_\lambda(u))\,(a,b)_M \otimes \zeta^{\otimes -1} = (x(\mathrm{Fr}(\lambda)), y(\mathrm{rec}_\lambda(\zeta)))_M\,.$$

6. Linear algebra

In order to simplify the notation, we denote

$$H = K(\alpha), \qquad H_M = H(A[\mathfrak{p}^{M+M_0}]), \qquad T = T_\mathfrak{p}(A), \qquad V = T_\mathfrak{p}(A) \otimes_{\mathcal{O}_\mathfrak{p}} L_\mathfrak{p}$$
$$\Delta = \mathrm{Gal}(H/K), \qquad U_M = \mathrm{Gal}(H_M/H) \subseteq \mathrm{Aut}_{\mathcal{O}_\mathfrak{p}}(A[\mathfrak{p}^{M+M_0}]) \xrightarrow{\sim} GL_2(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^{M+M_0}).$$

(6.1) The constant $C_2(\mathfrak{p})$

(6.1.1) Proposition. (i) *(Bogomolov [Bo])* $Z_p(A/H) := \mathbf{Z}_p^* \cap \mathrm{Im}\left(G_H \longrightarrow \mathrm{Aut}_{\mathbf{Z}_p}(T_p(A)\right)$ *is an open subgroup of* $\mathbf{Z}_p^*$.
(ii) *(Serre [Se 3])* *There exists a constant* $c(A/H)$ *such that the inequality* $(\mathbf{Z}_p^* : Z_p(A/H)) \leq c(A/H)$ *holds for all prime numbers* p.

(6.1.2) Proposition. *Consider the restriction map*

$$\mathrm{res} : H^1(H, A[\mathfrak{p}^M]) \longrightarrow H^1(H_M, A[\mathfrak{p}^M])^{U_M} = \mathrm{Hom}_{U_M}(G_{H_M}^{ab}, A[\mathfrak{p}^M]).$$

There exists an integer $C_2(\mathfrak{p}) \geq 0$ *which is equal to zero for all but finitely many* $\mathfrak{p}$ *and such that* $\mathfrak{p}^{C_2(\mathfrak{p})}\,\mathrm{Ker}(\mathrm{res}) = 0$ *for all* M.

Proof. Proposition 6.1.1(i) implies that there exists $u \in \mathbf{Z}_p^* - \{1\}$ such that

$$(\forall M \geq 0) \qquad u \ (\mathrm{mod}\,\mathfrak{p}^{M+M_0}) \in Z(U_M).$$

It follows from "Sah's Lemma" ([Sa], proof of Prop. 2.7(b)) that $u-1$ kills $H^1(U_M, A[\mathfrak{p}^M]) = \mathrm{Ker}(\mathrm{res})$, hence $\mathfrak{p}^{C_2(\mathfrak{p})}\,\mathrm{Ker}(\mathrm{res}) = 0$ for $C_2(\mathfrak{p}) = \mathrm{ord}_\mathfrak{p}(u-1)$. According to Proposition 6.1.1(ii), we can take $u \not\equiv 1 \ (\mathrm{mod}\,p)$ (hence $C_2(\mathfrak{p}) = 0$) if $p - 1 > c(A/H)$.

(6.2) The constant $C_3(\mathfrak{p})$

(6.2.1) Proposition. *The following conditions are equivalent.*
(i) V *is an absolutely irreducible representation of* G_H.
(ii) $\mathrm{End}_{L_\mathfrak{p}[G_H]}(V) = L_\mathfrak{p}$.
(iii) *For every non-trivial character* $\eta : \mathrm{Gal}(H/F) \longrightarrow \{\pm 1\}$, *the* $L_\mathfrak{p}[G_F]$*-modules* V *and* $V \otimes \eta$ *are not isomorphic.*
(iv) *For every totally imaginary quadratic extension* K' *of* F *contained in* H, *the abelian variety* A_j *does not acquire complex multiplication over* K'.
(v) *For every* K' *as in (iv), every totally imaginary quadratic extension* K_j *of* L_j, *every algebraic Hecke character* $\psi : \mathbf{A}_{K'}^* \longrightarrow K_j^*$ *and every embedding* $\tau : K_j \hookrightarrow \mathbf{C}$, *the L-series* $L(\psi_\tau, s)$ *(where* $\psi_\tau : \mathbf{A}_{K'}^*/K'^* \longrightarrow \mathbf{C}^*$ *is the idèle class character asociated to* ψ *at* τ*) is not equal to any of the L-series* $L(\pi(\sigma \circ \theta_j), s - 1/2)$ *from Proposition 1.18.*

Proof. If F'/F is any quadratic extension, denote by $\eta_{F'/F} : G_F \longrightarrow \{\pm 1\}$ the associated quadratic character with kernel $\mathrm{Ker}(\eta_{F'/F}) = G_{F'}$.
(i) $\Longleftrightarrow$ (ii): Irreducibility of V implies that its restriction to G_H is semi-simple. The equivalence of (i) and (ii) is then well-known ([Cu-Re, Thm. 3.43]).
(ii) $\Longrightarrow$ (iii): According to [Tay], Prop. 3.1 (and using the fact that each complex conjugation acts on $V(f)$ by a matrix with distinct eigenvalues $\pm 1 \in L_\mathfrak{p}$), V is an absolutely irreducible representation of G_F, hence $\mathrm{End}_{L_\mathfrak{p}[G_F]}(V) = L_\mathfrak{p}$, and both conditions (ii) and (iii) are invariant under finite extensions of the field $L_\mathfrak{p}$.

We can assume, therefore, that $L_{\mathfrak{p}}$ contains all roots of unity of order $[H:K]$. The Frobenius reciprocity yields

$$\begin{aligned}\mathrm{End}_{L_{\mathfrak{p}}[G_K]}(V) = \mathrm{Hom}_{L_{\mathfrak{p}}[G_F]}\left(V, \mathrm{Ind}_{G_K}^{G_F}\left(\mathrm{Res}_{G_F}^{G_K}(V)\right)\right) = \mathrm{Hom}_{L_{\mathfrak{p}}[G_F]}\left(V, V\oplus(V\otimes\eta_{K/F})\right) = \\ = L_{\mathfrak{p}}\oplus \mathrm{Hom}_{L_{\mathfrak{p}}[G_F]}\left(V, V\otimes\eta_{K/F}\right).\end{aligned} \tag{6.2.1.1}$$

Irreducibility of V implies that any non-trivial element of $\mathrm{Hom}_{L_{\mathfrak{p}}[G_F]}(V, V\otimes\eta_{K/F})$ is an isomorphism of $L_{\mathfrak{p}}[G_F]$-modules $V \xrightarrow{\sim} V\otimes\eta_{K/F}$, which proves the equivalence (ii) $\iff$ (iii) in the case $H=K$. Similarly,

$$\begin{aligned}\mathrm{End}_{L_{\mathfrak{p}}[G_H]}(V) = \mathrm{Hom}_{L_{\mathfrak{p}}[G_K]}\left(V, \mathrm{Ind}_{G_H}^{G_K}\left(\mathrm{Res}_{G_K}^{G_H}(V)\right)\right) = \mathrm{Hom}_{L_{\mathfrak{p}}[G_K]}\Big(V, \bigoplus_{\chi\in\widehat{\Delta}} V\otimes\chi\Big) = \\ = \bigoplus_{\chi\in\widehat{\Delta}} \mathrm{Hom}_{L_{\mathfrak{p}}[G_K]}(V, V\otimes\chi),\end{aligned} \tag{6.2.1.2}$$

where $\widehat{\Delta} = \mathrm{Hom}(\Delta, L_{\mathfrak{p}}^*)$. Assume that there exists an isomorphism of $L_{\mathfrak{p}}[G_F]$-modules $V \xrightarrow{\sim} V\otimes\eta$, for a non-trivial character $\eta : \mathrm{Gal}(H/F) \longrightarrow \{\pm 1\}$. If $\eta = \eta_{K/F}$, then (6.2.1.1) implies that $\mathrm{End}_{L_{\mathfrak{p}}[G_K]}(V) \neq L_{\mathfrak{p}}$, hence $\mathrm{End}_{L_{\mathfrak{p}}[G_H]}(V) \neq L_{\mathfrak{p}}$. If $\eta \neq \eta_{K/F}$, then the character $\chi := \eta|_{\Delta} \in \widehat{\Delta}$ is non-trivial, hence $\mathrm{End}_{L_{\mathfrak{p}}[G_H]}(V) \neq L_{\mathfrak{p}}$, by (6.2.1.2).
(iii) $\Longrightarrow$ (ii): Assume that $\mathrm{End}_{L_{\mathfrak{p}}[G_H]}(V) \neq L_{\mathfrak{p}}$. If $\mathrm{End}_{L_{\mathfrak{p}}[G_K]}(V) \neq L_{\mathfrak{p}}$, then $V \xrightarrow{\sim} V\otimes\eta_{K/F}$, by (6.2.1.1). If $\mathrm{End}_{L_{\mathfrak{p}}[G_K]}(V) = L_{\mathfrak{p}}$, then V is an absolutely irreducible representation of G_K and, thanks to (6.2.1.2), there exists a non-trivial character $\chi \in \widehat{\Delta}$ and a non-trivial morphism of $L_{\mathfrak{p}}[G_K]$-modules $V \longrightarrow V\otimes\chi$, which is necessarily an isomorphism. As $\det(V) = \det(V)\chi^2$, the values of χ are contained in $\{\pm 1\}$. It follows that χ extends to a character $\chi_F : \mathrm{Gal}(H/F) \longrightarrow \{\pm 1\}$ ($\chi_F \neq 1, \eta_{K/F}$, since $\chi \neq 1$). Applying again the Frobenius reciprocity

$$\begin{aligned}0 \neq \mathrm{Hom}_{L_{\mathfrak{p}}[G_K]}(V\otimes\chi, V) = \mathrm{Hom}_{L_{\mathfrak{p}}[G_F]}\left(V\otimes\chi_F, \mathrm{Ind}_{G_K}^{G_F}\left(\mathrm{Res}_{G_F}^{G_K}(V)\right)\right) = \\ = \mathrm{Hom}_{L_{\mathfrak{p}}[G_F]}\left(V\otimes\chi_F, V\oplus(V\otimes\eta_{K/F})\right),\end{aligned}$$

we deduce that there exists a character $\eta \in \{\chi_F, \chi_F\eta_{K/F}\}$ (hence $\eta \neq 1$) and a morphism of $L_{\mathfrak{p}}[G_F]$-modules $V \longrightarrow V\otimes\eta$, which is necessarily an isomorphism.
(ii) $\Longrightarrow$ (iv): If A_j acquires complex multiplication over K' as in (iv), then $\mathrm{Im}\left(L_{\mathfrak{p}}[G_{K'}] \longrightarrow \mathrm{End}_{L_{\mathfrak{p}}}(V)\right)$ is a commutative subalgebra of $\mathrm{End}_{L_{\mathfrak{p}}}(V) \xrightarrow{\sim} M_2(L_{\mathfrak{p}})$, hence $\mathrm{End}_{L_{\mathfrak{p}}[G_H]}(V) \supseteq \mathrm{End}_{L_{\mathfrak{p}}[G_{K'}]}(V) \supsetneq L_{\mathfrak{p}}$.
(v) $\Longrightarrow$ (iv): This follows from the Main Theorem of Complex Multiplication ([Sh-Ta], [Mi 2, I.5]).
(iv) $\Longrightarrow$ (v): If the L-function $L(\pi(\sigma\circ\theta_j), s-1/2)$ is given by a Hecke character of K', then $\mathrm{Im}(L_{\mathfrak{p}}[G_{K'}] \longrightarrow \mathrm{End}_{L_{\mathfrak{p}}}(V))$ is a commutative subalgebra of $\mathrm{End}_{L_{\mathfrak{p}}}(V) \xrightarrow{\sim} M_2(L_{\mathfrak{p}})$. Faltings' isogeny theorem then implies that $\mathrm{End}_{K'}(A_j)\otimes\mathbf{Q}$ contains a commutative subalgebra bigger than L_j, hence A_j acquires CM over K'.
(v) $\Longrightarrow$ (iii): Assume that $\eta : \mathrm{Gal}(H/F) \longrightarrow \{\pm 1\}$ is a non-trivial character such that the $L_{\mathfrak{p}}[G_F]$-modules V and $V\otimes\eta$ are isomorphic. Then $K' = H^{\mathrm{Ker}(\eta)}$ is a quadratic extension of F and $\mathrm{End}_{L_{\mathfrak{p}}[G_{K'}]}(V) = L_{\mathfrak{p}}\oplus L_{\mathfrak{p}}$, hence V is a semi-simple L-rational abelian representation of $G_{K'}$ with infinite image. This implies, according to [He, Thm. 2] (see also [Se 2, III.2.3, Thm. 2]) that K' is totally imaginary and $G_{K'}$ acts on $V\otimes_{L_{\mathfrak{p}}}\overline{L}_{\mathfrak{p}}$ by $\psi_{\mathfrak{p}}\oplus\psi_{\mathfrak{p}}\circ\rho$, where $\psi_{\mathfrak{p}} : G_{K'} \longrightarrow \overline{L}_{\mathfrak{p}}^*$ is the Galois representation associated to an algebraic Hecke character ψ of K' (cf. [Ne], proof of 12.6.5.2), hence A_j acquires complex multiplication over K'.

(6.2.2) Proposition. *If the equivalent conditions (i)-(v) of Proposition 6.2.1 hold, then there exists an integer $C_3(\mathfrak{p}) \geq 0$, which is equal to zero for all but finitely many $\mathfrak{p}$ and which satisfies*

$$\mathrm{Im}\left(\mathcal{O}_{\mathfrak{p}}[G_H] \longrightarrow \mathrm{End}_{\mathcal{O}_{\mathfrak{p}}}(T)\right) \supseteq \mathfrak{p}^{C_3(\mathfrak{p})}\,\mathrm{End}_{\mathcal{O}_{\mathfrak{p}}}(T).$$

Proof. $\mathrm{Im}\left(\mathcal{O}_{\mathfrak{p}}[G_H] \longrightarrow \mathrm{End}_{\mathcal{O}_{\mathfrak{p}}}(T)\right)$ is an $\mathcal{O}_{\mathfrak{p}}$-lattice in the $L_{\mathfrak{p}}$-algebra

$$A = \mathrm{Im}\left(L_{\mathfrak{p}}[G_H] \longrightarrow \mathrm{End}_{L_{\mathfrak{p}}}(V)\right) \subseteq \mathrm{End}_{L_{\mathfrak{p}}}(V).$$

As V is a faithful simple A-module satisfying $\mathrm{End}_A(V) = \mathrm{End}_{L_{\mathfrak{p}}[G_H]}(V) = L_{\mathfrak{p}}$, a theorem of Burnside ([Cu-Re, Thm. 3.32]) implies that $A = \mathrm{End}_{L_{\mathfrak{p}}}(V)$, which proves the existence of $C_3(\mathfrak{p})$.
It remains to show that, for all but finitely many $\mathfrak{p}$, the map $\mathcal{O}_{\mathfrak{p}}[G_H] \longrightarrow \mathrm{End}_{\mathcal{O}_{\mathfrak{p}}}(T)$ is surjective. By the Nakayama Lemma, this amounts to the surjectivity of

$$k[G_H] \longrightarrow \mathrm{End}_k(\overline{T}) \qquad\qquad (k = \mathcal{O}_{\mathfrak{p}}/\mathfrak{p},\ \overline{T} = T/\mathfrak{p}T),$$

which would follow from absolute irreducibility of $\mathrm{Res}^{G_H}_{G_F}(\overline{T})$. We can assume that $p \nmid [H : F]$ (hence $p \neq 2$) and, after replacing L by a finite extension, that L contains all roots of unity of order $[H : K]$ (hence k does, too). According to [Di, Prop. 3.1], for all but finitely many $\mathfrak{p}$, $\overline{T}$ is an absolutely irreducible $k[G_F]$-module, hence $\mathrm{End}_{k[G_F]}(\overline{T}) = k$. For such $\mathfrak{p}$, $\overline{T}$ is a semi-simple $k[G_H]$-module, by Clifford's Theorem ([Cu-Re, Thm. 11.1(i)]; this applies to an arbitrary group G and its normal subgroup H of finite index), hence

$$\mathrm{Res}^{G_H}_{G_F}(\overline{T}) \ \text{ is absolutely irreducible} \iff \mathrm{End}_{k[G_H]}(\overline{T}) = k.$$

The same argument as in the proof of 6.2.1 (ii) $\iff$ (iii) shows that

$$\mathrm{End}_{k[G_H]}(\overline{T}) \neq k \iff (\exists \eta : \mathrm{Gal}(H/F) \longrightarrow \{\pm 1\},\ \eta \neq 1) \qquad \overline{T} \xrightarrow{\sim} \overline{T} \otimes \eta \quad \text{as } k[G_F] - \text{modules}.$$

If this were true for infinitely many $\mathfrak{p}$'s, we could find a common non-trivial character $\eta : \mathrm{Gal}(H/F) \longrightarrow \{\pm 1\}$ for which the congruences

$$(\forall g \in G_F) \qquad \mathrm{Tr}(g \mid T) \equiv \mathrm{Tr}(g \mid T \otimes \eta) \pmod{\mathfrak{p}}$$

held for infinitely many $\mathfrak{p}$, hence

$$(\forall g \in G_F) \qquad \mathrm{Tr}(g \mid V) = \mathrm{Tr}(g \mid V \otimes \eta),$$

which would imply that $V \xrightarrow{\sim} V \otimes \eta$ (by irreducibility of V). This contradiction with 6.2.1(iii) proves that $C_3(\mathfrak{p}) = 0$ for all but finitely many $\mathfrak{p}$.

(6.3) Galois groups

(6.3.1) Let $W' \subset H^1(H, A[\mathfrak{p}^M])$ be an $\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^M$-submodule of finite type. Denote by $W = \mathrm{res}(W') \subset \mathrm{Hom}_{U_M}(G^{ab}_{H_M}, A[\mathfrak{p}^M])$ its image under the restriction map from Proposition 6.1.2, by $W^{\perp} \subset G^{ab}_{H_M}$ the annihilator of W, and set $H_M(W) := (H^{ab}_M)^{W^{\perp}}$. The natural injective map

$$\begin{aligned} G := \mathrm{Gal}(H_M(W)/H) &\hookrightarrow \mathrm{Hom}_{\mathcal{O}_{\mathfrak{p}}}(W, A[\mathfrak{p}^M]) \\ g &\mapsto (\mathrm{ev}_g : w \mapsto w(g)) \end{aligned}$$

is a morphism of $\mathbf{Z}[U_M]$-modules, where $U_M = \mathrm{Gal}(H_M/H) \subset \mathrm{Aut}_{\mathcal{O}_{\mathfrak{p}}}(A[\mathfrak{p}^{M+M_0}])$ acts trivially on W and by conjugation on G. Denote by

$$X = \mathcal{O}_{\mathfrak{p}} \cdot G = \mathcal{O}_{\mathfrak{p}} \cdot \mathrm{Gal}(H_M(W)/H) \subset \mathrm{Hom}_{\mathcal{O}_{\mathfrak{p}}}(W, A[\mathfrak{p}^M])$$

the $\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^M$-submodule of $\mathrm{Hom}_{\mathcal{O}_{\mathfrak{p}}}(W, A[\mathfrak{p}^M])$ generated by the image of G and by

$$j : X \hookrightarrow \mathrm{Hom}_{\mathcal{O}_{\mathfrak{p}}}(W, A[\mathfrak{p}^M])$$

the inclusion map. By construction, j is $\mathcal{O}_{\mathfrak{p}}[U_M]$-linear and the natural map

$$W \longrightarrow \mathrm{Hom}_{\mathcal{O}_{\mathfrak{p}}}(X, A[\mathfrak{p}^M])$$

is injective.

(6.3.2) Proposition. *If the equivalent conditions of Proposition 6.2.1 are satisfied, then*

$$(\forall M,\, W') \qquad \mathfrak{p}^{C_3(\mathfrak{p})}\,\mathrm{Coker}(j) = 0.$$

Proof. This is a special case of Proposition 6.4.3 below, for

$$B = \mathrm{Im}\left(L_{\mathfrak{p}}[G_H] \longrightarrow \mathrm{End}_{L_{\mathfrak{p}}}(V)\right) = \mathrm{End}_{L_{\mathfrak{p}}}(V), \qquad D = L_{\mathfrak{p}},$$
$$\Lambda = \mathrm{Im}\left(\mathcal{O}_{\mathfrak{p}}[G_H] \longrightarrow \mathrm{End}_{\mathcal{O}_{\mathfrak{p}}}(T)\right) \supseteq \mathfrak{p}^{C_3(\mathfrak{p})}\,\mathrm{End}_{\mathcal{O}_{\mathfrak{p}}}(T), \qquad R = \mathcal{O}_{\mathfrak{p}}.$$

(6.3.3) Corollary. *If the equivalent conditions of Proposition 6.2.1 are satisfied, then*

$$\mathfrak{p}^{C_2(\mathfrak{p})+C_3(\mathfrak{p})}\,\mathrm{Coker}\left(j' : X \xrightarrow{j} \mathrm{Hom}_{\mathcal{O}_{\mathfrak{p}}}(W, A[\mathfrak{p}^M]) \xrightarrow{\mathrm{Hom}(\mathrm{res},\mathrm{id})} \mathrm{Hom}_{\mathcal{O}_{\mathfrak{p}}}(W', A[\mathfrak{p}^M])\right) = 0.$$

Proof. It follows from Proposition 6.1.2 that $\mathrm{Coker}(\mathrm{Hom}(\mathrm{res}, \mathrm{id}))$ is killed by $\mathfrak{p}^{C_2(\mathfrak{p})}$.

(6.3.4) Corollary. *If the equivalent conditions of Proposition 6.2.1 are satisfied and if W' is ρ-stable (where $\rho \in G_F = \mathrm{Gal}(\overline{F}/F)$ denotes the complex conjugation with respect to the fixed embedding $\overline{F} \hookrightarrow \mathbf{C}$ extending τ_1), so are W, $H_M(W)$ and X. The maps j, j' are ρ-equivariant and, denoting $(-)^{\pm} = (-)^{\rho=\pm 1}$, we have*

$$2X^+ \subseteq \mathcal{O}_{\mathfrak{p}}G^+ \subseteq X^+$$
$$\mathfrak{p}^{C_2(\mathfrak{p})+C_3(\mathfrak{p})}\,\mathrm{Coker}\left(j' : X^+ \hookrightarrow \mathrm{Hom}_{\mathcal{O}_{\mathfrak{p}}}(W', A[\mathfrak{p}^M])^+\right) = 0$$
$$4 \cdot \mathrm{Coker}\left(\mathrm{Hom}_{\mathcal{O}_{\mathfrak{p}}}(W', A[\mathfrak{p}^M])^+ \longrightarrow \mathrm{Hom}_{\mathcal{O}_{\mathfrak{p}}}((W')^+, A[\mathfrak{p}^M]^+) \oplus \mathrm{Hom}_{\mathcal{O}_{\mathfrak{p}}}((W')^-, A[\mathfrak{p}^M]^-)\right) = 0$$
$$2^4\,\mathfrak{p}^{C_2(\mathfrak{p})+C_3(\mathfrak{p})}\,\mathrm{Coker}\left(\mathcal{O}_{\mathfrak{p}} \cdot 2G^+ \hookrightarrow X^+ \xrightarrow{j'} \mathrm{Hom}_{\mathcal{O}_{\mathfrak{p}}}((W')^+, A[\mathfrak{p}^M]^+) \oplus \mathrm{Hom}_{\mathcal{O}_{\mathfrak{p}}}((W')^-, A[\mathfrak{p}^M]^-)\right) = 0.$$

(6.4) In this section we prove a general abstract version of Proposition 6.3.2.

(6.4.1) Assume that V is a $\mathbf{Q}_p$-vector space of finite dimension, $B \subset \mathrm{End}_{\mathbf{Q}_p}(V)$ a $\mathbf{Q}_p$-subalgebra, $\Lambda \subset B$ a $\mathbf{Z}_p$-order in B and $T \subset V$ a $\mathbf{Z}_p$-lattice such that $\Lambda T = T$. The $\mathbf{Q}_p$-algebra

$$D = \mathrm{End}_B(V)^{\mathrm{op}}$$

acts on V on the right; its action commutes with the left action of B. The ring

$$R = \{x \in D \,|\, Tx \subset T\}$$

is a $\mathbf{Z}_p$-order in D.

(6.4.2) In the situation of 6.4.1, assume that we are given the following data:

- An integer $N \geq 1$.
- A right $(R/p^N R)$-module $W = W_R$.
- A left $(\Lambda/p^N\Lambda)$-module $X = {}_\Lambda X$.
- A $\mathbf{Z}_p$-bilinear pairing
$$\langle\ ,\ \rangle : X \times W \longrightarrow T/p^N T$$
satisfying
$$\langle \lambda x, w\rangle = \lambda\langle x, w\rangle$$
$$\langle x, wr\rangle = \langle x, w\rangle r \qquad (\forall x \in X,\, \forall w \in W,\, \forall r \in R,\, \forall \lambda \in \Lambda)$$
such that the induced homomorphisms
$$i = i_W\ : W_R \longrightarrow \mathrm{Hom}_\Lambda\left({}_\Lambda X, {}_\Lambda(T/p^N T)_R\right)$$
$$j = j_X\ : {}_\Lambda X \longrightarrow \mathrm{Hom}_R\left(W_R, {}_\Lambda(T/p^N T)_R\right)$$
are both *injective* (i is a morphism of right R-modules, while j is a morphism of left Λ-modules).

(6.4.3) Proposition. *Assume that we are given the data 6.4.2 and that B is a semi-simple $\mathbf{Q}_p$-algebra. Then there exists a maximal $\mathbf{Z}_p$-order $R_{\max} \supset R$ of D; fixing $R_{\max}$, then*

$$\Lambda_{\max} := \{b \in B \,|\, bT \cdot R_{\max} \subset T \cdot R_{\max}\}$$

is a maximal $\mathbf{Z}_p$-order in B containing Λ. Let $c, d \in Z(R_{\max})$ be non-zero central elements in $R_{\max}$ such that $c\Lambda_{\max} \subset \Lambda$ and $dR_{\max} \subset R$ (they always exist). Then

$$cd\,\mathrm{Coker}(j) = 0.$$

Proof. We begin by reducing to the case $R = R_{\max}$, $\Lambda = \Lambda_{\max}$. First of all, $R_{\max}$ exists by [Cu-Re, Thm. 26.5] and $\Lambda_{\max}$ is a maximal $\mathbf{Z}_p$-order in B, by [Cu-Re, Thm. 26.20, Thm. 26.23(iii)]. Consider the maps

$$W_R \xrightarrow{i} \mathrm{Hom}_\Lambda\left({}_\Lambda X, {}_\Lambda(T/p^N T)_R\right) \xrightarrow{\gamma} \mathrm{Hom}_\Lambda\left({}_\Lambda X, {}_{\Lambda_{\max}}(TR_{\max}/p^N TR_{\max})_{R_{\max}}\right);$$

then

$$\widetilde{W}_{R_{\max}} := (\gamma \circ i)(W_R) R_{\max}$$

is a right $R_{\max}$-module. Similarly, consider

$${}_\Lambda X \xrightarrow{j} \mathrm{Hom}_R\left(W_R, {}_\Lambda(T/p^N T)_R\right) \xrightarrow{\delta} \mathrm{Hom}_{R_{\max}}\left(\widetilde{W}_{R_{\max}}, {}_{\Lambda_{\max}}(TR_{\max}/p^N TR_{\max})_{R_{\max}}\right)$$

and put

$${}_{\Lambda_{\max}}\widetilde{X} := \Lambda_{\max}(\delta \circ j({}_\Lambda X));$$

this is a left $\Lambda_{\max}$-module and the canonical maps

$$\widetilde{i} : \widetilde{W}_{R_{\max}} \longrightarrow \mathrm{Hom}_{\Lambda_{\max}}\left({}_{\Lambda_{\max}}\widetilde{X}, {}_{\Lambda_{\max}}(TR_{\max}/p^N TR_{\max})_{R_{\max}}\right)$$
$$\widetilde{j} : {}_{\Lambda_{\max}}\widetilde{X} \longrightarrow \mathrm{Hom}_{R_{\max}}\left(\widetilde{W}_{R_{\max}}, {}_{\Lambda_{\max}}(TR_{\max}/p^N TR_{\max})_{R_{\max}}\right)$$

are injective. Assume that the statement has been proved for the maximal orders $R_{\max}, \Lambda_{\max}$ and $c = d = 1$. Then $\widetilde{j}$ is surjective, hence

$$\delta \circ j({}_\Lambda X) \supset c\Lambda_{\max}(\delta \circ j)({}_\Lambda X) = c\,\mathrm{Hom}_{R_{\max}}\left(\widetilde{W}, TR_{\max}/p^N TR_{\max}\right),$$

i.e. c kills $\mathrm{Coker}(\delta \circ j)$. As $(T \cap p^N TR_{\max})d \subset p^N T$, d kills $\mathrm{Ker}(\delta) = \mathrm{Hom}_R(W, (T \cap p^N TR_{\max})/p^N T)$. The exact sequence

$$\mathrm{Ker}(\delta) \longrightarrow \mathrm{Coker}(j) \longrightarrow \mathrm{Coker}(\delta \circ j)$$

then implies that cd kills $\mathrm{Coker}(j)$.

We can assume, therefore, that $R = R_{\max}$ and $\Lambda = \Lambda_{\max}$. The next step is the reduction to the case of a simple $\mathbf{Q}_p$-algebra B. In general there is a finite decomposition $B = \prod e_i B$, where each $e_i B = B_i$ is a simple $\mathbf{Q}_p$-algebra and e_i are the corresponding orthogonal idempotents. Then we have $V = \bigoplus V_i$, $V_i = e_i V$. According to [Cu-Re, Thm. 26.20], $\Lambda = \prod \Lambda_i$, where each $\Lambda_i = e_i \Lambda$ is a maximal $\mathbf{Z}_p$-order in B_i. As $\Lambda T \subset T$, we have $T = \bigoplus T_i$ with $T_i = e_i T$, which implies that $D = \prod D_i$, $D_i = \mathrm{End}_{B_i}(V_i)^{\mathrm{op}}$ and $R = \prod R_i$, $R_i = \{x \in D_i \,|\, T_i x \subset T_i\}$. Similarly, $W = \bigoplus e_i W$ and $X = \bigoplus e_i X$.

This implies that we can assume that B is a simple $\mathbf{Q}_p$-algebra, hence $B = M_n(D)$ for a skew-field $D = \mathrm{End}_B(V)^{\mathrm{op}}$ and $V = D^n$. In this case D has a unique maximal order R; every left or right ideal in R is bilateral and is of the form $\varpi_R^m R = R\,\varpi_R^m$ $(m \geq 0)$, where ϖ_R is a fixed prime element of R ([Cu-Re, Thm. 26.23]).

There is an isomorphism of right R-modules

$$W_R \xrightarrow{\sim} \bigoplus_{i=1}^{k} R/\varpi_R^{n_i} R,$$

where $\varpi_R^{n_i} \mid p^N$ for each i. Using the fact that multiplication by $\varpi_R^{n_i} p^{-N}$ induces an isomorphism between $T \cdot p^N \varpi_R^{-n_i}/p^N T$ and $T/T\varpi_R^{n_i}$, we define a left Λ-module ${}_\Lambda Y$ as the fibre product

$$\begin{array}{ccccc} {}_\Lambda Y & \longrightarrow & & & T^k \\ \downarrow & & & & \downarrow \\ {}_\Lambda X & \xrightarrow{j} & \mathrm{Hom}_R\left(W_R, {}_\Lambda(T/p^N)_R\right) & \xrightarrow{\sim} & \bigoplus_{i=1}^k {}_\Lambda\left(T \cdot p^N \varpi_R^{-n_i}/p^N T\right) \xrightarrow{\sim} \bigoplus_{i=1}^k {}_\Lambda\left(T/T\varpi_R^{n_i}\right) \end{array}$$

The injectivity of i_W implies that Y has the following property:

$$(\forall r_1, \ldots, r_k \in R \text{ s.t. } \exists i\ r_i \in R^*)\,(\exists y_1, \ldots, y_k \in Y) \qquad \sum_{i=1}^{k} y_i r_i \notin T\,\varpi_R \tag{$\star_k$}$$

We shall prove, by induction on k, that any Λ-submodule ${}_\Lambda Y \subset {}_\Lambda(T^k)_R$ satisfying $(\star_k)$ is equal to T^k. This will imply that j_X is surjective, as claimed. Let $k = 1$. If ${}_\Lambda Y$ satisfies $(\star_1)$, then $Y \not\subset T\,\varpi_R$. The lattice T is free over R and, in a suitable R-basis of T, $\Lambda = M_r(R)^{\mathrm{op}}$. As $(Y + T\,\varpi_R)/T\,\varpi_R \subset T/T\,\varpi_R$ is a non-zero $\Lambda/\varpi_R = M_r(R/\varpi_R)$-submodule of the simple Λ/ϖ_R-module $T/T\,\varpi_R$, we have $Y + T\,\varpi_R = T$, hence $Y = T$ by the Nakayama Lemma.
Suppose that $k > 1$ and that any ${}_\Lambda Y'$ satisfying $(\star_{k-1})$ is equal to T^{k-1}. If ${}_\Lambda Y \subset {}_\Lambda(T^k)_R$ satisfies $(\star_k)$, then its image under the projection $pr_k : T^k \longrightarrow T$ on the k-th factor satisfies $(\star_1)$, hence $pr_k(Y) = T$. As Λ is a maximal order in a semi-simple $\mathbf{Q}_p$-algebra, it is hereditary, i.e. T is a projective Λ-module [Cu-Re, Thm. 26.12(ii)]. It follows that the (surjective) projection $pr_k : Y \longrightarrow T$ admits a Λ-linear section $s : T \longrightarrow Y$. For each $i = 1, \ldots, k-1$, the map $T \xrightarrow{s} Y \hookrightarrow T^k \xrightarrow{pr_k} T$ is an element of $\mathrm{End}_\Lambda(T) = R^{\mathrm{op}}$, hence is given by right multiplication by some $a_i \in R$. It follows that

$$Y = \{(xa_1 + y_1, \ldots, xa_{k-1} + y_{k-1}, x) \,|\, x \in T,\, y_1, \ldots, y_{k-1} \in Y \cap \ker(pr_k)\}. \tag{6.4.3.1}$$

If $r_1, \ldots, r_{k-1} \in R$ and $(\exists i)\ r_i \in R^*$, then there exist $y_1, \ldots, y_{k-1} \in Y \cap \ker(pr_k)$ such that

$$\sum_{i=1}^{k-1} y_i r_i = \sum_{i=1}^{k-1} (xa_i + y_i) r_i - x \sum_{i=1}^{k-1} a_i r_i \notin T\,\varpi_R,$$

since Y satisfies $(\star_k)$. This implies that $Y \cap \ker(pr_k)$ satisfies $(\star_{k-1})$, hence $Y \cap \ker(pr_k) = T^{k-1}$ by inductive hypothesis. It follows from (6.4.3.1) that $Y = T^k$, which concludes the proof of the Proposition.

(6.5) Galois groups and Frobenius elements

(6.5.1) In the situation of 6.3.1, assume that W' is ρ-stable. Given an arbitrary element

$$g \in G^+ = \mathrm{Gal}(H_M(W)/H_M)^+,$$

then $h = g^2 = (\rho + 1)g \in 2G^+$. The Čebotarev density theorem implies that there exist infinitely many non-archimedean primes $\mathscr{L}(W)$ of $H_M(W)$ satisfying the following properties:

(6.5.1.1) $\mathscr{L}(W)$ is unramified in $H_M(W)/F$.
(6.5.1.2) $\mathscr{L}(W)$ is prime to $(pu(0))c(x)N(I_0)$ and the prime ℓ of F induced by $\mathscr{L}(W)$ does not lie in S.
(6.5.1.3) $\mathrm{Fr}_{H_M(W)/F}(\mathscr{L}(W)) = \rho g \in \mathrm{Gal}(H_M(W)/F)$.

Denote by ℓ, λ, λ_H and $\mathscr{L}$, respectively, the primes of F, K, H and H_M induced by $\mathscr{L}(W)$.

(6.5.2) Lemma. (i) $\ell \in \mathscr{S}_1(M)$.
(ii) *The prime* $\lambda = \ell\mathcal{O}_K$ *splits completely in* H_M/K.
(iii) $\mathrm{Fr}_{H_M(W)/K}(\mathscr{L}(W)) = (\rho g)^2 = \rho g \rho g = {}^{\rho}g\, g = (\rho+1)g = g^2 = h \in 2G^+$.
(iv) *The decomposition group of* $\mathscr{L}$ *in* H_M/F *is equal to* $\mathrm{Gal}(H_M/F)_{\mathscr{L}} = \{1, \rho\}$. *In particular,* $\rho(\mathscr{L}) = \mathscr{L}$.

Proof. The statements (i) and (ii) follow from (6.5.1.2) and the equalities $\mathrm{Fr}_{H_M/F}(\mathscr{L}) = \rho g|_{H_M} = \rho$, $\mathrm{Fr}_{H_M/K}(\mathscr{L}) = \mathrm{Fr}_{H_M/F}(\mathscr{L})^2 = \rho^2 = 1$. The statement (iii) is clear and (iv) follows from the fact that $\mathrm{Gal}(H_M/F)_{\mathscr{L}}$ is generated by $\mathrm{Fr}_{H_M/F}(\mathscr{L}) = \rho$.

(6.5.3) In the situation of 6.5.1, the element $\mathrm{Fr}(\mathscr{L}) := \mathrm{Fr}_{H_M(W)/H_M}(\mathscr{L}(W)) \in G$ depends only on $\mathscr{L}$; more precisely, $\mathrm{Fr}(\mathscr{L}) = g^2 = h \in 2G^+$, by Lemma 6.5.2(ii). Its image via the map

$$j' : G^+ \hookrightarrow X^+ \xrightarrow{j} \mathrm{Hom}_{\mathcal{O}_\mathfrak{p}}(W, A[\mathfrak{p}^M])^+ \longrightarrow \mathrm{Hom}_{\mathcal{O}_\mathfrak{p}}(W', A[\mathfrak{p}^M])^+$$

is given by the evaluation map

$$j(\mathrm{Fr}(\mathscr{L}))(w') = \mathrm{res}(w')(\mathrm{Fr}(\mathscr{L})) \qquad\qquad (w' \in W') \tag{6.5.3.1}$$

(6.5.4) The prime $\mathscr{L}$ determines identifications

$$A(H_{\lambda_H})[\mathfrak{p}^M] = A((H_M)_{\mathscr{L}})[\mathfrak{p}^M] = A(H_M)[\mathfrak{p}^M] = A(\overline{F})[\mathfrak{p}^M] \qquad (=: A[\mathfrak{p}^M]).$$

The image of $W' \subset H^1(H, A[\mathfrak{p}^M])$ under the localization map

$$\mathrm{res}_{\lambda_H} : H^1(H, A[\mathfrak{p}^M]) \longrightarrow H^1(H_{\lambda_H}, A[\mathfrak{p}^M])$$

is contained in $H^1_{ur}(H_{\lambda_H}, A[\mathfrak{p}^M])$ and the composite map

$$W' \xrightarrow{\mathrm{res}_{\lambda_H}} H^1_{ur}(H_{\lambda_H}, A[\mathfrak{p}^M]) \xrightarrow{\mathrm{ev}_{\mathrm{Fr}(\lambda_H)}} A[\mathfrak{p}^M]$$

coincides with the map (6.5.3.1)

$$j(\mathrm{Fr}(\mathscr{L})) : w' \mapsto \mathrm{res}(w')(\mathrm{Fr}(\mathscr{L})).$$

We shall use repeatedly the fact that this map is ρ-equivariant (= is contained in $\mathrm{Hom}_{\mathcal{O}_\mathfrak{p}}(W', A[\mathfrak{p}^M])^+$). In order to stress the dependence on $\mathscr{L}$, we shall write

$$w'_{\mathscr{L}} := \mathrm{res}_{\lambda_H}(w') \qquad\qquad (w' \in W').$$

(6.6) Linear and quadratic forms

(6.6.1) Lemma. *Let*

$$f(x) = \sum_{i=1}^n f_i\, x_i, \qquad g(x) = \sum_{1 \le i \le j \le n} g_{ij}\, x_i x_j \qquad\qquad \Big(f_i, g_{ij} \in \mathcal{O}_\mathfrak{p}/\mathfrak{p}^N,\ x = \sum_{i=1}^n x_i e_i \in \bigoplus_{i=1}^n \mathcal{O}_\mathfrak{p}\, e_i = \mathcal{O}_\mathfrak{p}^{\oplus n}\Big)$$

be a linear and a quadratic form, respectively, in $n \ge 1$ *variables, with coefficients in* $\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N$. *Writing* $\mathbf{Z}_p^{\oplus n} = \bigoplus_{i=1}^n \mathbf{Z}_p\, e_i \subset \mathcal{O}_\mathfrak{p}^{\oplus n}$, *we have, for each* $m \in \{0, \dots, N\}$*:*
(i) $f(\mathbf{Z}_p^{\oplus n}) \subseteq \mathfrak{p}^m(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N) \iff (\forall i = 1, \dots, n) \quad f_i \in \mathfrak{p}^m(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N) \iff f(\mathcal{O}_\mathfrak{p}^{\oplus n}) \subseteq \mathfrak{p}^m(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N)$.
(ii) $g(\mathbf{Z}_p^{\oplus n}) \subseteq \mathfrak{p}^m(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N) \iff (\forall 1 \le i \le j \le n) \quad g_{ij} \in \mathfrak{p}^m(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N) \iff g(\mathcal{O}_\mathfrak{p}^{\oplus n}) \subseteq \mathfrak{p}^m(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N)$.
(iii) *If* $U \subsetneq \mathbf{Z}_p^{\oplus n}$ *is a proper* $\mathbf{Z}_p$*-submodule and* $g(\mathbf{Z}_p^{\oplus n}) \not\subset \mathfrak{p}^m(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N)$ $(1 \le m < N - \mathrm{ord}_\mathfrak{p}(2))$, *then*

$$(\exists x \in \mathbf{Z}_p^{\oplus n},\ x \notin U) \qquad g(x) \notin 2\,\mathfrak{p}^m(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N) = \mathfrak{p}^{m+\mathrm{ord}_\mathfrak{p}(2)}(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N).$$

Proof. The statements (i) and (ii) follow from the equalities $f_i = f(e_i)$, $g_{ii} = g(e_i)$, $g_{ij} = g(e_i + e_j) - g(e_i) - g(e_j)$ $(i < j)$.
(iii) There exists an integer $r \ge 1$ and a $\mathbf{Z}_p$-basis $e'_1, \dots, e'_n$ of $\mathbf{Z}_p^{\oplus n}$ such that

$$U \subseteq \bigoplus_{i=1}^{r} p\mathbf{Z}_p\, e'_i \oplus \bigoplus_{j=r+1}^{n} \mathbf{Z}_p\, e'_j.$$

Writing $x = \sum_{i=1}^n x_i e_i = \sum_{i=1}^n x'_i e'_i$, we have

$$g(x) = \sum_{1\le i\le j\le n} g'_{ij}\, x'_i x'_j, \qquad g'_{ii} = g(e'_i), \qquad g'_{ij} = g(e'_i + e'_j) - g(e'_i) - g(e'_j) \quad (i<j).$$

It follows from (ii) that

$$(\exists k \le l) \qquad g'_{kl} \notin \mathfrak{p}^m(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N).$$

We distinguish three cases:

(1) $k \le l \le r$:

if $k=l$, then $x := e'_k \notin U$ and $g(x) = g'_{kk} \notin \mathfrak{p}^m(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N)$. If $k<l$, then $g(e'_k+e'_l)-g(e'_k)-g(e'_l) \notin \mathfrak{p}^m(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N)$, hence there exists $x \in \{e'_k, e'_l, e'_k+e'_l\}$ $(\Longrightarrow x \notin U)$ such that $g(x) \notin \mathfrak{p}^m(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N)$.

(2) $k \le r < l$ and $(\forall i \le j \le r)$ $\quad g'_{ij} \in \mathfrak{p}^m(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N)$:

the congruence

$$(\forall \lambda \in \mathbf{Z}_p) \qquad g(e'_k + \lambda e'_l) = g'_{kk} + \lambda g'_{kl} + \lambda^2 g'_{ll} \equiv \lambda g'_{kl} + \lambda^2 g'_{ll} \ (\mathrm{mod}\, \mathfrak{p}^m(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N))$$

implies that there exists $\lambda \in \{1,2\}$ such that $x := e'_k + \lambda e'_l \notin U$ satisfies $g(x) \notin 2\,\mathfrak{p}^m(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N)$.

(3) $(\forall i \le r)\ (\forall j \ge i) \qquad g'_{ij} \in \mathfrak{p}^m(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N)$:

in this case $k > r$ and we have

$$\Big(\forall y \in \bigoplus_{j=r+1}^{n} \mathcal{O}_\mathfrak{p}\, e'_j\Big) \qquad g(e'_1 + y) \equiv g(y) \ (\mathrm{mod}\, \mathfrak{p}^m(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N)).$$

If $k=l$, then $x := e'_1 + e'_k \notin U$ satisfies $g(x) \equiv g'_{kk} \not\equiv 0 \ (\mathrm{mod}\, \mathfrak{p}^m(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N))$. If $k<l$, then

$$g(e'_1+e'_k+e'_l) - g(e'_1+e'_k) - g(e'_1+e'_l) \equiv g(e'_k+e'_l) - g(e'_k) - g(e'_l) \equiv g'_{kl} \not\equiv 0 \ (\mathrm{mod}\, \mathfrak{p}^m(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N)),$$

hence there exists $x \in \{e'_1+e'_k+e'_l, e'_1+e'_k, e'_1+e'_l\}$ $(\Longrightarrow x \notin U)$ such that $g(x) \notin \mathfrak{p}^m(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N)$.

(6.6.2) Proposition. *Let $a, b, N \ge 0$ be integers such that $a, 2b+\mathrm{ord}_\mathfrak{p}(2) < N$. Let $Z \subset (\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N)^{\oplus 5}$ be a $\mathbf{Z}_p$-submodule satisfying $\mathcal{O}_\mathfrak{p}\cdot Z \supseteq \mathfrak{p}^a(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N) \oplus \big(\mathfrak{p}^b(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N)\big)^{\oplus 4}$. Then there exists an element $z = (z_0, \dots, z_4) \in Z$ $(z_i \in \mathcal{O}_\mathfrak{p}/\mathfrak{p}^N)$ such that*

$$\ell_{\mathcal{O}_\mathfrak{p}}\big((\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N)/(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N)z_0\big) \le a$$
$$\ell_{\mathcal{O}_\mathfrak{p}}\big((\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N)^{\oplus 2}/(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N)(z_1,z_2) + (\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N)(z_3,z_4)\big) \le 2b + \mathrm{ord}_\mathfrak{p}(2)$$

(where $\ell_{\mathcal{O}_\mathfrak{p}}(C)$ denotes the length of a finite $\mathcal{O}_\mathfrak{p}$-module C), hence

$$(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N)z_0 \supseteq \mathfrak{p}^a(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N), \qquad (\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N)(z_1,z_2) + (\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N)(z_3,z_4) \supseteq 2\,\mathfrak{p}^{2b}(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N)^{\oplus 2}.$$

Proof. Fix a set of $\mathbf{Z}_p$-generators $z^{(i)} = (z_0^{(i)}, \dots, z_4^{(i)}) \in Z$ $(1 \le i \le n)$ of Z and set

$$f(x) = \sum_{i=1}^n x_i z_0^{(i)}, \qquad g(x) = \begin{vmatrix} \sum_{i=1}^n x_i z_1^{(i)} & \sum_{i=1}^n x_i z_2^{(i)} \\ \sum_{i=1}^n x_i z_3^{(i)} & \sum_{i=1}^n x_i z_4^{(i)} \end{vmatrix} \qquad \Big(x = \sum_{i=1}^n x_i\, e_i \in \bigoplus_{i=1}^n \mathcal{O}_\mathfrak{p}\, e_i = \mathcal{O}_\mathfrak{p}^{\oplus n}\Big).$$

The assumptions imply that $f(\mathcal{O}_\mathfrak{p}^{\oplus n}) \not\subset \mathfrak{p}^{a+1}(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N)$, hence

$$U := \{x \in \mathbf{Z}_p^{\oplus n} \mid f(x) \in \mathfrak{p}^{a+1}(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N)\}$$

is a proper ($U \subsetneq \mathbf{Z}_p^{\oplus n}$) $\mathbf{Z}_p$-submodule of $\mathbf{Z}_p^{\oplus n}$, by Lemma 6.6.1(i). The assumptions also imply that $g(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N) \not\subset \mathfrak{p}^{2b+1}(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N)$, hence

$$\Big(\exists x = \sum_{i=1}^n x_i e_i \in \mathbf{Z}_p^{\oplus n},\, x \notin U\Big) \qquad g(x) \notin \mathfrak{p}^{2b+1+\mathrm{ord}_\mathfrak{p}(2)}(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N),$$

by Lemma 6.6.1(iii). The element $z = \sum_{i=1}^n x_i\, z^{(i)} \in Z$ then has the desired properties.

7. The main result

We continue to use the notation from Sect. 3-6.

(7.1) Selmer groups

(7.1.1) Let F'/F be a finite extension and Σ an arbitrary set of primes of F'. We denote

$$S_\Sigma(A/F', \mathfrak{p}^M) := \mathrm{Ker}\Big(H^1(F', A[\mathfrak{p}^M]) \longrightarrow \bigoplus_{v \notin \Sigma} H^1(F'_v, A[\mathfrak{p}^M])/\mathrm{Im}(\delta_v)\Big),$$

where

$$\delta_v : A(F'_v) \otimes \mathcal{O}_\mathfrak{p}/\mathfrak{p}^M \hookrightarrow H^1(F'_v, A[\mathfrak{p}^M])$$

denotes the coboundary map arising from the cohomology exact sequence associated to

$$0 \longrightarrow A[\mathfrak{p}^M] \longrightarrow A(\overline{F}) \xrightarrow{\mathfrak{p}^M} A(\overline{F}) \longrightarrow 0.$$

If $v \nmid p\infty$ and if A has good reduction at the prime of F induced by v, then $\mathrm{Im}(\delta_v) = H^1_{ur}(F'_v, A[\mathfrak{p}^M])$. This implies that, if Σ is finite, so is $S_\Sigma(A/F', \mathfrak{p}^M)$.

(7.1.2) The classical Selmer group

$$S(A/F', \mathfrak{p}^M) := S_\emptyset(A/F', \mathfrak{p}^M)$$

sits in the standard exact sequence

$$0 \longrightarrow A(F') \otimes \mathcal{O}_\mathfrak{p}/\mathfrak{p}^M \xrightarrow{\delta} S(A/F', \mathfrak{p}^M) \longrightarrow Ш(A/F')[\mathfrak{p}^M] \longrightarrow 0.$$

The inductive limit $\varinjlim_M S(A/F', \mathfrak{p}^M)$ is an $\mathcal{O}_\mathfrak{p}$-module of co-finite type.

(7.1.3) If F''/F' is a finite Galois extension, then the restriction map induces a canonical homomorphism

$$S(A/F', \mathfrak{p}^M) \longrightarrow S(A/F'', \mathfrak{p}^M)^{\mathrm{Gal}(F''/F')},$$

whose kernel and cokernel are killed by $[F'' : F']$.

(7.1.4) The Tate local duality [Mi 1, I.3.4-5] implies that, for each prime v of F', $\mathrm{Im}(\delta_v)$ is an isotropic subspace of $H^1(F'_v, A[\mathfrak{p}^M])$ with respect to the cup product

$$H^1(F'_v, A[\mathfrak{p}^M]) \times H^1(F'_v, A[\mathfrak{p}^M]) \xrightarrow{\cup} H^2(F'_v, \mathcal{O}_\mathfrak{p}/\mathfrak{p}^M(1)) \xrightarrow{\mathrm{inv}_v} \mathcal{O}_\mathfrak{p}/\mathfrak{p}^M$$

induced by the pairing $(\ ,\ )_M$ from (5.19.1).

(7.1.5) If Σ is a finite set of primes of F', $s \in S(A/F', \mathfrak{p}^M)$ and $c \in S_\Sigma(A/F', \mathfrak{p}^M)$, then the reciprocity law

$$\big(\forall a \in H^2(G_{F'}, \mathcal{O}_\mathfrak{p}/\mathfrak{p}^M(1))\big) \qquad \sum_v \mathrm{inv}_v(a_v) = 0 \in \mathcal{O}_\mathfrak{p}/\mathfrak{p}^M$$

applied to $a = s \cup c$ yields (thanks to 7.1.4)

$$\sum_{v\in\Sigma} \mathrm{inv}_v(s_v \cup c_v) = 0 \in \mathcal{O}_\mathfrak{p}/\mathfrak{p}^M.$$

(7.2) Annihilation relations

(7.2.1) Kolyvagin's classes. As in Sect. 6, we denote $H = K(\alpha)$. For each $\mathfrak{n} = \ell_1 \cdots \ell_r \in \mathscr{S}_r(M)$ ($r \geq 0$, $\ell_i \in \mathscr{S}_1(M)$), we define

$$\kappa_\mathfrak{n} = \varpi^{C_1(\mathfrak{p})}\, e_\beta\left(\mathrm{cor}_{K(x)/H}(c(\mathfrak{n}))\right) \in H^1(H, A[\mathfrak{p}^M])^{(\beta)},$$

where $C_1(\mathfrak{p}) = \max_v C_{1,v}(\mathfrak{p})$ (the constants $C_{1,v}(\mathfrak{p})$ were defined in 5.2). For $r = 0$, the cohomology class $\kappa_1 := \kappa_{(1)}$ is equal to

$$\kappa_1 = \varpi^{C_1(\mathfrak{p})}\, \delta(e_\beta(y)) \in S(A/H, \mathfrak{p}^M)^{(\beta)},$$

where $y = \mathrm{cor}_{K(x)/H}(y_j) \in A(H)$. For $r \geq 1$, Proposition 5.12 implies that

$$\kappa_\mathfrak{n} \in S_{\{v|\mathfrak{n}\}}(A/H, \mathfrak{p}^M)^{(\beta)}.$$

(7.2.2) Assume that $\mathfrak{n} = \ell_1 \cdots \ell_r \in \mathscr{S}_r(M)$ ($r \geq 1$, $\ell_i \in \mathscr{S}_1(M)$). For each $i \in \{1, \ldots, r\}$, fix a prime $\mathscr{L}_i \mid \ell_i$ of H_M such that $\mathrm{Fr}_{H_M/F}(\mathscr{L}_i) = \rho$ (as an element of $\mathrm{Gal}(H_M/F)$, not only as a conjugacy class) and denote by v_i the prime of H induced by $\mathscr{L}_i$. As in 6.5.4, $\mathscr{L}_i$ determines identifications

$$A(H_{v_i})[\mathfrak{p}^M] = A((H_M)_{\mathscr{L}_i})[\mathfrak{p}^M] = A(\overline{F})[\mathfrak{p}^M] \qquad (=: A[\mathfrak{p}^M]),$$

and the localization map

$$W_i' := S_{\{v|(\mathfrak{n}/\ell_i)\}}(A/H, \mathfrak{p}^M) \xrightarrow{\mathrm{res}_{v_i}} H^1_{ur}(H_{v_i}, A[\mathfrak{p}^M]) \xrightarrow{\mathrm{ev}_{\mathrm{Fr}(v_i)}} A[\mathfrak{p}^M]$$

coincides with the evaluation map $w' \mapsto w'_{\mathscr{L}_i} := (\mathrm{res}(w'))(\mathrm{Fr}(\mathscr{L}_i))$.

(7.2.3) Proposition. *In the situation of 7.2.2, assume that the generators $\sigma_{\ell_i} \in G(\ell_i)$ have been chosen in the following compatible manner: there exists a global root of unity $\zeta \in \mu_{p^\infty}(H_M)$ such that, for each $i = 1, \ldots, r$, the image of σ_{ℓ_i} in $G(\ell_i) \otimes \mathcal{O}_\mathfrak{p}/\mathfrak{p}^M$ coincides with the image of ζ under the composite map*

$$\mu_{p^\infty}(H_M) \otimes \mathcal{O}_\mathfrak{p}/\mathfrak{p}^M \longrightarrow \mu_{p^\infty}((H_M)_{\mathscr{L}_i}) \otimes \mathcal{O}_\mathfrak{p}/\mathfrak{p}^M \xleftarrow{\sim} \mu_{p^\infty}(H_{v_i}) \otimes \mathcal{O}_\mathfrak{p}/\mathfrak{p}^M \xrightarrow{\mathrm{rec}_{v_i}\otimes\mathrm{id}} G(\ell_i) \otimes \mathcal{O}_\mathfrak{p}/\mathfrak{p}^M$$

(such a compatible choice always exists). Then we have, for each $s \in S(A/H, \mathfrak{p}^M)^{(\beta)}$, an equality

$$[H : K] \sum_{i=1}^{r} \left(s_{\mathscr{L}_i}, (\kappa_{\mathfrak{n}/\ell_i})_{\mathscr{L}_i}\right)_M = 0$$

in $\mu_{p^\infty}(H_M) \otimes \mathcal{O}_\mathfrak{p}/\mathfrak{p}^M = \mathcal{O}_\mathfrak{p}/\mathfrak{p}^M(1)$.

Proof. Applying 7.1.5 to $F' = H$, $\Sigma = \{v \mid \mathfrak{n}\}$, $\rho(s)$ and $c = \kappa_\mathfrak{n}$, we obtain

$$\sum_{i=1}^{r} \sum_{\sigma\in\Delta} \mathrm{inv}_{\sigma(v_i)}\left(\mathrm{res}_{\sigma(v_i)}(\rho(s)) \cup \mathrm{res}_{\sigma(v_i)}(\kappa_\mathfrak{n})\right) = 0 \in \mathcal{O}_\mathfrak{p}/\mathfrak{p}^M, \tag{7.2.3.1}$$

where $\Delta = \mathrm{Gal}(H/K)$. As

$$(\forall \sigma \in \Delta) \qquad \sigma(\rho(s)) = \beta^{-1}(\sigma)\rho(s), \qquad \sigma(\kappa_\mathfrak{n}) = \beta(\sigma)\kappa_\mathfrak{n},$$

we deduce from (7.2.3.1) the equality

$$[H : K] \sum_{i=1}^{r} \mathrm{inv}_{v_i}\left(\mathrm{res}_{v_i}(\rho(s)) \cup \mathrm{res}_{v_i}(\kappa_\mathfrak{n})\right) = 0 \in \mathcal{O}_\mathfrak{p}/\mathfrak{p}^M. \tag{7.2.3.2}$$

Combined with the formula from Proposition 5.20 (with $\zeta_v = \zeta$), (7.2.3.2) yields

$$[H : K] \sum_{i=1}^{r} \left(\rho(s)_{\mathscr{L}_i}, \mathrm{Fr}(\ell_i)(\kappa_{\mathfrak{n}/\ell_i})_{\mathscr{L}_i}\right)_M = 0 \in \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^M(1).$$

Finally, it follows from

$$\rho(s)_{\mathscr{L}_i} = \rho(s_{\mathscr{L}_i}) = \mathrm{Fr}(\ell_i) s_{\mathscr{L}_i} \in A[\mathfrak{p}^M]$$

that

$$\left((\rho(s)_{\mathscr{L}_i}, \mathrm{Fr}(\ell_i)(\kappa_{\mathfrak{n}/\ell_i})_{\mathscr{L}_i}\right)_M = \left(\mathrm{Fr}(\ell_i) s_{\mathscr{L}_i}, \mathrm{Fr}(\ell_i)(\kappa_{\mathfrak{n}/\ell_i})_{\mathscr{L}_i}\right)_M = \mathrm{Fr}(\ell_i) \left(s_{\mathscr{L}_i}, (\kappa_{\mathfrak{n}/\ell_i})_{\mathscr{L}_i}\right)_M = \\ = -\left(s_{\mathscr{L}_i}, (\kappa_{\mathfrak{n}/\ell_i})_{\mathscr{L}_i}\right)_M .$$

(7.2.4) (i) If we do not choose the generators σ_{ℓ_i} compatibly, then there exist $\zeta \in \mu_{p^\infty}(H_M)$ and $u_1, \ldots, u_r \in \mathbf{Z}_p^*$ such that the image of σ_{ℓ_i} in $G(\ell_i) \otimes \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^M$ is equal to the image of $\zeta \otimes u_i$ $(i = 1, \ldots, r)$. The statement of Proposition 7.2.3 then becomes

$$[H : K] \sum_{i=1}^{r} \left(s_{\mathscr{L}_i}, (\kappa_{\mathfrak{n}/\ell_i})_{\mathscr{L}_i}\right)_M \otimes u_i = 0 \in \mu_{p^\infty}(H_M) \otimes \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^M = \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^M(1).$$

(ii) We shall apply Proposition 7.2.3 only in situations when it is known a priori that

$$(\forall i = 2, \ldots, r) \qquad \left(s_{\mathscr{L}_i}, (\kappa_{\mathfrak{n}/\ell_i})_{\mathscr{L}_i}\right)_M = 0.$$

In such a case one does not have to worry about the compatibility of the σ_{ℓ_i}'s.

(7.3) Theorem. *Assume that the condition (⋆) from Theorem 3.2 holds. If $e_\beta(y) \notin A(H)_{\mathrm{tors}}$, then there exists an integer $C(\mathfrak{p}) \geq 0$ which is equal to zero for all but finitely many $\mathfrak{p}$ and such that*

$$(\forall M >> 0) \qquad \mathfrak{p}^{C(\mathfrak{p})} \left(S(A/H, \mathfrak{p}^M)^{(\beta)}/\mathcal{O}_{\mathfrak{p}} \cdot \kappa_1\right) = 0.$$

(7.4) Thanks to 7.1.2, Theorem 7.3 implies Theorem 3.2 (the statements about the α^{-1}-components follow by applying ρ to the α-components). The proof of Theorem 7.3 will occupy the rest of Sect. 7.

Recall that the constants $C_1(\mathfrak{p}), C_2(\mathfrak{p})$ and $C_3(\mathfrak{p})$ were introduced in 7.2.1, 6.1 and 6.2, respectively. We set

$$C_5(\mathfrak{p}) := \mathrm{ord}_{\mathfrak{p}}([H : K]), \qquad C_6(\mathfrak{p}) := \mathrm{ord}_{\mathfrak{p}}(\deg(\varphi)),$$

where $\varphi : A_j \longrightarrow \widehat{A_j}$ is the isogeny from 5.19. If $\beta^2 \neq 1$, then another constant $C_4(\mathfrak{p})$ will be defined in 7.6.1 below.

The assumption $e_\beta(y) \notin A(H)_{\mathrm{tors}}$ implies that the constant

$$C_0(\mathfrak{p}) := \max\{c \in \mathbf{Z}_{\geq 0} \mid e_\beta(y) \in A(H)_{\mathrm{tors}} + \mathfrak{p}^c A(H)\}$$

is defined (and $C_0(\mathfrak{p}) = 0$ for all but finitely many $\mathfrak{p}$).

In order to simplify the notation, we write $C_i = C_i(\mathfrak{p})$ $(i = 0, \ldots, 6)$. We also denote, for each $\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^M$-module Y and an element $y \in Y$,

$$\exp(y) := \min\{c \in \mathbf{Z}_{\geq 0} \mid \mathfrak{p}^c\, y = 0\}, \qquad \exp(Y) := \max\{\exp(y) \mid y \in Y\}.$$

Using this notation, we have, for $M >> 0$,

$$\exp(\kappa_1) \geq M - C_0 - C_1. \tag{7.4.1}$$

(7.5) Proof of Theorem 7.3 in the case $\beta^2 = 1$. In this case $S := S(A/H, \mathfrak{p}^M)^{(\beta)}$ is ρ-stable; we denote $S^{\pm} := S^{\rho=\pm 1}$. As

$$2\kappa_1 = (1+\rho)\kappa_1 + (1-\rho)\kappa_1, \qquad (1 \pm \rho)\kappa_1 \in S^{\pm},$$

it follows that

$$(\exists \varepsilon \in \{\pm 1\}) \qquad \exp((1+\varepsilon\rho)\kappa_1) \geq M - C_0 - C_1 - \operatorname{ord}_{\mathfrak{p}}(2).$$

Fix such an ε; then $x_\varepsilon := (1+\varepsilon\rho)\kappa_1 \in S^{\varepsilon}$.

(7.5.1) Bounding the exponent of $S^{-\varepsilon}$. Fix $s \in S^{-\varepsilon}$ with maximal $\exp(s)$ and set $x_{-\varepsilon} = s$.

Choosing the first Kolyvagin prime. We apply the discussion from 6.3 and 6.5 to $W' = S$. Set

$$U_{\pm\varepsilon} := \{h \in 2G^+ \mid \exp(j'(h))(x_{\pm\varepsilon}) < \exp(x_{\pm\varepsilon}) - (C_2 + C_3 + 4\operatorname{ord}_{\mathfrak{p}}(2))\}.$$

It follows from Corollary 6.3.4 that $U_{\pm\varepsilon} \subsetneq 2G^+$ are proper subgroups of $2G^+$, hence there exists $h = g^2 \in 2G^+ - (U_\varepsilon \cup U_{-\varepsilon})$. Applying the discussion in 6.5.1 to the element $h = g^2$, choose a prime $\mathscr{L}(W)$ satisfying (6.5.1.1-3). The induced primes $\mathscr{L} \mid \lambda_H \mid \lambda \mid \ell$ of H_M, H, K, F, respectively, satisfy $\ell \in \mathscr{S}_1(M)$ and $\rho(\mathscr{L}) = \mathscr{L}$. The definition of $U_{\pm\varepsilon}$ implies that

$$\exp\left((x_{\pm\varepsilon})_{\mathscr{L}}\right) \geq \exp\left(x_{\pm\varepsilon}\right) - (C_2 + C_3 + 4\operatorname{ord}_{\mathfrak{p}}(2)),$$

hence

$$\exp\left(((1+\varepsilon\rho)\kappa_1)_{\mathscr{L}}\right) \geq M - \sum_{i=0}^{3} C_i - 5\operatorname{ord}_{\mathfrak{p}}(2) \tag{7.5.1.1}$$

$$\exp\left(s_{\mathscr{L}}\right) \geq \exp\left(S^{-\varepsilon}\right) - (C_2 + C_3 + 4\operatorname{ord}_{\mathfrak{p}}(2)). \tag{7.5.1.2}$$

The first annihilation relation. Applying Proposition 7.2.3 with $\mathfrak{n} = \ell$ to s and $\rho(s)$, we obtain (using the ρ-equivariance of the map $w' \mapsto w'_{\mathscr{L}}$) that

$$[H:K]\left(s_{\mathscr{L}}, ((1+\varepsilon\rho)\kappa_1)_{\mathscr{L}}\right)_M = 0 \in \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^M(1). \tag{7.5.1.3}$$

Combining (7.5.1.3) with (7.5.1.1) and (5.19.2), we obtain

$$2^6\,\mathfrak{p}^{C_0+C_1+C_2+C_5+C_6} s_{\mathscr{L}} \in \mathcal{O}_{\mathfrak{p}} \cdot ((1+\varepsilon\rho)\kappa_1)_{\mathscr{L}} \subset A[\mathfrak{p}^M]^{\rho=\varepsilon}.$$

On the other hand, $s_{\mathscr{L}} \in A[\mathfrak{p}^M]^{\rho=-\varepsilon}$ (since $s \in S^{-\varepsilon}$) and $2(A[\mathfrak{p}^M]^{\rho=\varepsilon} \cap A[\mathfrak{p}^M]^{\rho=-\varepsilon}) = 0$, hence

$$2^7\,\mathfrak{p}^{C_0+C_1+C_2+C_5+C_6} s_{\mathscr{L}} = 0.$$

Combined with (7.5.1.2), we obtain

$$\mathfrak{p}^{M_1} S^{-\varepsilon} = 0, \qquad M_1 = C_0 + C_1 + 2C_2 + 2C_3 + C_5 + C_6 + 11\operatorname{ord}_{\mathfrak{p}}(2). \tag{7.5.1.4}$$

In particular, $\mathfrak{p}^{M_1}(1-\varepsilon\rho)\kappa_1 = 0$, hence $2\,\mathfrak{p}^{M_1}\kappa_1 = \mathfrak{p}^{M_1}(1+\varepsilon\rho)\kappa_1$.

(7.5.2) Bounding the exponent of $S^{\varepsilon}/\mathcal{O}_{\mathfrak{p}} \cdot (1+\varepsilon\rho)\kappa_1$. Denote

$$\widetilde{S} = \operatorname{Ker}\left(\operatorname{res}_{\lambda_H} : S \longrightarrow H^1(H_{\lambda_H}, A[\mathfrak{p}^M])\right)$$

and fix $\widetilde{s} \in \widetilde{S}^{\varepsilon} = \widetilde{S}^{\rho=\varepsilon}$ with maximal $\exp(\widetilde{s})$. It follows from Proposition 5.18 combined with (5.15.1) that

$$\exp((1-\varepsilon\rho)\kappa_\ell) \geq \exp\left(f\left(((1-\varepsilon\rho)\kappa_\ell)_{\mathscr{L}}\right)\right) = \exp\left(((1+\varepsilon\rho)\kappa_1)_{\mathscr{L}}\right) \geq M - \sum_{i=0}^{3} C_i - 5\operatorname{ord}_{\mathfrak{p}}(2),$$

where f denotes the map

$$f : H^1(H_{\lambda_H}, A[\mathfrak{p}^M]) \longrightarrow H^1(H_{\lambda_H}, A[\mathfrak{p}^M])/H^1_{ur}(H_{\lambda_H}, A[\mathfrak{p}^M])$$

(cf. 7.6.4 below).

Choosing the second Kolyvagin prime. We apply the discussion from 6.3 and 6.5 to the submodule $W' = S_{\{v|\ell\}}(A/H, \mathfrak{p}^M)^{(\beta)}$. Set $x'_{\varepsilon} = \widetilde{s} \in (W')^{\varepsilon}$ and $x'_{-\varepsilon} = (1-\varepsilon\rho)\kappa_\ell \in (W')^{-\varepsilon}$. The argument as in 7.5.1 shows that there exists a prime $\ell' \in \mathscr{S}_1(M)$ $(\ell' \neq \ell)$ and a prime $\mathscr{L}' \mid \ell'$ of H_M such that $\rho(\mathscr{L}') = \mathscr{L}'$ and

$$\exp\left(((1-\varepsilon\rho)\kappa_\ell)_{\mathscr{L}'}\right) \geq M - \sum_{i=0}^{3} C_i - 5\,\mathrm{ord}_{\mathfrak{p}}(2) - (C_2 + C_3 + 4\,\mathrm{ord}_{\mathfrak{p}}(2)) \tag{7.5.2.1}$$

$$\exp\left(\widetilde{s}_{\mathscr{L}'}\right) \geq \exp\left(\widetilde{S}^{\varepsilon}\right) - (C_2 + C_3 + 4\,\mathrm{ord}_{\mathfrak{p}}(2)). \tag{7.5.2.2}$$

The second annihilation relation. Applying Proposition 7.2.3 with $\mathfrak{n} = \ell\ell'$ to $\widetilde{s}$ and $\rho(\widetilde{s})$, we obtain (using the ρ-equivariance of the map $w' \mapsto w'_{\mathscr{L}'}$ and the assumption $\widetilde{s}_{\mathscr{L}} = 0$) that

$$[H : K]\,(\widetilde{s}_{\mathscr{L}'}, ((1-\varepsilon\rho)\kappa_\ell)_{\mathscr{L}'})_M = 0 \in \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^M(1). \tag{7.5.2.3}$$

Combining (7.5.2.3) with (7.5.2.1) and (5.19.2), we deduce that

$$2^{10}\,\mathfrak{p}^{C_0+C_1+2C_2+2C_3+C_5+C_6}\widetilde{s}_{\mathscr{L}'} \in \mathcal{O}_{\mathfrak{p}} \cdot ((1-\varepsilon\rho)\kappa_\ell)_{\mathscr{L}'} \subset A[\mathfrak{p}^M]^{\rho=-\varepsilon}.$$

On the other hand, $\widetilde{s} \in \widetilde{S}^{\varepsilon}$ implies that $\widetilde{s}_{\mathscr{L}'} \subset A[\mathfrak{p}^M]^{\rho=\varepsilon}$, hence

$$2^{11}\,\mathfrak{p}^{C_0+C_1+2C_2+2C_3+C_5+C_6}\widetilde{s}_{\mathscr{L}'} = 0.$$

Applying (7.5.2.2), we obtain

$$2^{15}\,\mathfrak{p}^{C_0+C_1+3C_2+3C_3+C_5+C_6}\,\widetilde{S}^{\varepsilon} = 0. \tag{7.5.2.4}$$

(7.5.3) Bounding the exponent of $S/\mathcal{O}_{\mathfrak{p}}\,\kappa_1$. As $2H^1_{ur}(H_{\lambda_H}, A[\mathfrak{p}^M])^{\varepsilon}$ is a cyclic $\mathcal{O}_{\mathfrak{p}}$-module, it follows from (7.5.1.1) that

$$2^5\,\mathfrak{p}^{C_0+C_1+C_2+C_3}\left(S^{\varepsilon}/\left(\widetilde{S}^{\varepsilon} + \mathcal{O}_{\mathfrak{p}} \cdot (1+\varepsilon\rho)\kappa_1\right)\right) = 0.$$

Putting this together with (7.5.1.4) and (7.5.2.4), we deduce

$$2^{21}\,\mathfrak{p}^{2C_0+2C_1+4C_2+4C_3+C_5+C_6}\,(S/\mathcal{O}_{\mathfrak{p}}\,\kappa_1) = 0,$$

which finishes the proof of Theorem 7.3 in the case $\beta^2 = 1$.

(7.6) Proof of Theorem 7.3 in the case $\beta^2 \neq 1$. We write $\overline{\beta} := \beta^{-1} \neq \beta$, $S := S(A/H, \mathfrak{p}^M)$ (for $M >> 0$) and, as in 7.5, $C_i := C_i(\mathfrak{p})$ $(i = 0, \ldots, 6)$.

(7.6.1) Lemma-Definition. *Define*

$$C_4(\mathfrak{p}) = \begin{cases} 0, & p \nmid \text{order of } \beta^2 \\ \mathrm{ord}_{\mathfrak{p}}(p)/(p-1), & p \mid \text{order of } \beta^2. \end{cases}$$

(i) $C_4(\mathfrak{p}) \in \mathbf{Z}_{\geq 0}$.
(ii) $C_4(\mathfrak{p}) \leq C_5(\mathfrak{p})/(p-1)$.
(iii) *For each $\mathcal{O}_{\mathfrak{p}}[\Delta]$-module Y (where $\Delta = \mathrm{Gal}(H/K)$),* $\mathfrak{p}^{C_4(\mathfrak{p})}\left(Y^{(\beta)} \cap Y^{(\overline{\beta})}\right) = 0$.

Proof. (i) If p divides the order of β^2, then $L_{\mathfrak{p}}$ contains the values of β^2, hence $L_{\mathfrak{p}} \supset \mathbf{Q}_p(\mu_p)$.

(ii) This is clear.
(iii) $(\exists\sigma\in\Delta)\qquad \beta(\sigma)\neq\overline{\beta}(\sigma)$; then $Y^{(\beta)}\cap Y^{(\overline{\beta})}$ is killed by $\beta^2(\sigma)-1\neq 0$, but

$$\mathrm{ord}_{\mathfrak{p}}(\beta^2(\sigma)-1)=\begin{cases}0, & \beta^2(\sigma)\notin\mu_{p^\infty}\\ \leq \mathrm{ord}_{\mathfrak{p}}(p)/(p-1), & \beta^2(\sigma)\in\mu_{p^\infty}.\end{cases}$$

(7.6.2) Definition. (i) *Fix $t_\pm\in T^\pm=T^{\rho=\pm 1}$ such that $T^\pm=\mathcal{O}_{\mathfrak{p}}\,t_\pm$ and let $t_{\pm,M}$ be the image of $t_\pm$ in $(T/\mathfrak{p}^MT)^\pm=A[\mathfrak{p}^M]^\pm$.*
(ii) *$\exp(t_{\pm,M})\geq M-\mathrm{ord}_{\mathfrak{p}}(2)$; fix $u_\pm\in(\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^M)t_{\pm,M}$ with $\exp(u_\pm)=M-\mathrm{ord}_{\mathfrak{p}}(2)$.*
(iii) *Let W' be as in 6.3.1 and let $f\in\mathrm{Hom}_{\mathcal{O}_{\mathfrak{p}}}(W',A[\mathfrak{p}^M])^+$. Then $2f((W')^\pm)\subset(\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^{M-\mathrm{ord}_{\mathfrak{p}}(2)})u_\pm$; we define the morphisms*

$$f_\pm(W')^\pm\longrightarrow\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^{M-\mathrm{ord}_{\mathfrak{p}}(2)},\qquad(\forall w\in(W')^\pm)\qquad f_\pm(w)u_\pm=2f(w).$$

(iv) *For each $w\in W'$, $2w=(1+\rho)w+(1-\rho)w$, hence*

$$4f(w)=f_+((1+\rho)w)u_++f_-((1-\rho)w)u_-.$$

(7.6.3) Choosing the first Kolyvagin prime. We have

$$\kappa_1\in S^{(\beta)},\qquad\rho(\kappa_1)\in S^{(\overline{\beta})},\qquad\exp(\kappa_1)=\exp(\rho(\kappa_1))\geq M-C_0-C_1.$$

As $\mathfrak{p}^{C_4}\left(S^{(\beta)}\cap S^{(\overline{\beta})}\right)=0$, it follows that the elements $(1\pm\rho)\kappa_1\in S^\pm=S^{\rho=\pm1}$ satisfy

$$\exp((1\pm\rho)\kappa_1)\geq M-C_0-C_1-C_4-\mathrm{ord}_{\mathfrak{p}}(2).\tag{7.6.3.1}$$

Applying Corollary 6.3.4 to $W'=S$, we obtain, as in 7.5.1, primes $\ell\in\mathscr{S}_1(M)$ and $\mathscr{L}\mid\ell$ in H_M such that $\rho(\mathscr{L})=\mathscr{L}$ and

$$\exp\left(((1\pm\rho)\kappa_1))_{\mathscr{L}}\right)\geq\exp((1\pm\rho)\kappa_1)-(C_2+C_3+4\,\mathrm{ord}_{\mathfrak{p}}(2))\geq M-M_2,\tag{7.6.3.2}$$

where

$$M_2=\sum_{i=0}^{4}C_i+5\,\mathrm{ord}_{\mathfrak{p}}(2).$$

As $2\kappa_1=(1+\rho)\kappa_1+(1-\rho)\kappa_1$ and $2(A[\mathfrak{p}^M]^+\cap A[\mathfrak{p}^M]^-)=0$, it follows that

$$\exp\left((\kappa_1)_{\mathscr{L}}\right),\exp\left((\rho(\kappa_1))_{\mathscr{L}}\right)\geq M-M_2-2\,\mathrm{ord}_{\mathfrak{p}}(2).\tag{7.6.3.3}$$

The first annihilation relation. Let $s\in S^{(\beta)}$. Applying Proposition 7.2.3 with $\mathfrak{n}=\ell$, we obtain

$$[H:K]\,(s_{\mathscr{L}},(\kappa_1)_{\mathscr{L}})_M=0\in\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^M(1),$$

hence, using (5.19.2) and (7.6.3.3),

$$2^3\,\mathfrak{p}^{M_2+C_5+C_6}\,s_{\mathscr{L}}=2^8\,\mathfrak{p}^{\sum_{i=0}^{6}C_i}\,s_{\mathscr{L}}\in\mathcal{O}_{\mathfrak{p}}\,(\kappa_1)_{\mathscr{L}}.\tag{7.6.3.4}$$

Set

$$\widetilde{S}=\mathrm{Ker}\Big(S\xrightarrow{(\mathrm{res}_v)}\bigoplus_{v\mid\ell}H^1(H_v,A[\mathfrak{p}^M])\Big);$$

then

$$\widetilde{S}^{(\beta)}=\mathrm{Ker}\left(\mathrm{res}_{\lambda_H}:S^{(\beta)}\longrightarrow H^1(H_{\lambda_H},A[\mathfrak{p}^M])\right),$$

and the inclusion (7.6.3.4) can be reformulated as follows:

$$2^3\,\mathfrak{p}^{M_2+C_5+C_6}\left(S^{(\beta)}/\left(\widetilde{S}^{(\beta)}+\mathcal{O}_\mathfrak{p}\,\kappa_1\right)\right)=2^8\,\mathfrak{p}^{\sum_{i=0}^{6}C_i}\left(S^{(\beta)}/\left(\widetilde{S}^{(\beta)}+\mathcal{O}_\mathfrak{p}\,\kappa_1\right)\right)=0. \tag{7.6.3.5}$$

(7.6.4) Choosing the second Kolyvagin prime. In the exact sequence of $\mathcal{O}_\mathfrak{p}/\mathfrak{p}^M$-modules

$$0\longrightarrow H^1_{ur}(H_{\lambda_H},A[\mathfrak{p}^M])\longrightarrow H^1(H_{\lambda_H},A[\mathfrak{p}^M])\xrightarrow{f}\frac{H^1(H_{\lambda_H},A[\mathfrak{p}^M])}{H^1_{ur}(H_{\lambda_H},A[\mathfrak{p}^M])}\longrightarrow 0,$$

both flank terms are isomorphic to $A[\mathfrak{p}^M]\xrightarrow{\sim}(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^M)^{\oplus 2}$, hence the sequence splits and the middle term is isomorphic, as an $\mathcal{O}_\mathfrak{p}/\mathfrak{p}^M$-module, to $(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^M)^{\oplus 4}$. We know that

$$(\rho(\kappa_1))_{\mathscr{L}}=\rho((\kappa_1)_{\mathscr{L}})\in H^1_{ur}(H_{\lambda_H},A[\mathfrak{p}^M])\xrightarrow{\sim}A[\mathfrak{p}^M],\qquad((1\pm\rho)\kappa_1)_{\mathscr{L}}\in A[\mathfrak{p}^M]^{\pm}$$

and

$$\exp\left(((1\pm\rho)\kappa_1)_{\mathscr{L}}\right)\geq M-M_2.$$

On the other hand, (5.15.1) and Proposition 5.18 imply that

$$f\left(((1\pm\rho)\kappa_\ell)_{\mathscr{L}}\right)=-\Phi_{\lambda_H}\left(((1\mp\rho)\kappa_1)_{\mathscr{L}}\right),$$

hence

$$\exp\left(f\left(((1\pm\rho)\kappa_\ell)_{\mathscr{L}}\right)\right)\geq M-M_2. \tag{7.6.4.1}$$

Set

$$W'=S_{\{v|\ell\}}(A/H,\mathfrak{p}^M),\qquad\widetilde{W}'=\mathrm{Ker}\Big(W'\xrightarrow{(\mathrm{res}_v)}\bigoplus_{v|\ell}H^1(H_v,A[\mathfrak{p}^M])\Big);$$

then

$$(\widetilde{W}')^{(\beta)}=\widetilde{S}^{(\beta)},\qquad(\widetilde{W}')^{(\overline{\beta})}=\widetilde{S}^{(\overline{\beta})},\qquad\kappa_1,\kappa_\ell\in(W')^{(\beta)},\qquad\rho(\kappa_1),\rho(\kappa_\ell)\in(W')^{(\overline{\beta})}.$$

Denote by $U\subseteq W'$ the $\mathcal{O}_\mathfrak{p}/\mathfrak{p}^M$-submodule generated by $(1+\rho)\kappa_1,(1-\rho)\kappa_1,(1+\rho)\kappa_\ell$ and $(1-\rho)\kappa_\ell$. It follows from (7.6.3.2) and (7.6.4.1) that

$$\mathrm{res}_{\lambda_H}(U)\supseteq\mathfrak{p}^{M_2}\,H^1(H_{\lambda_H},A[\mathfrak{p}^M]), \tag{7.6.4.2}$$

hence

$$\mathfrak{p}^{M_2}(U\cap\widetilde{W}')=0 \tag{7.6.4.3}$$

and U contains an $\mathcal{O}_\mathfrak{p}/\mathfrak{p}^M$-submodule isomorphic to $(\mathfrak{p}^{M_2}(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^M))^{\oplus 4}$.

Fix an element $\widetilde{s}\in(\widetilde{W}')^{(\beta)}=\widetilde{S}^{(\beta)}$ with maximal $\exp(\widetilde{s})$; then the argument used in the proof of (7.6.3.1) shows that

$$\exp((1+\rho)\widetilde{s})\geq\exp(\widetilde{s})-C_4-\mathrm{ord}_\mathfrak{p}(2). \tag{7.6.4.4}$$

Define a homomorphism of $\mathcal{O}_\mathfrak{p}/\mathfrak{p}^M$-modules

$$z:\mathrm{Hom}_{\mathcal{O}_\mathfrak{p}}(W',A[\mathfrak{p}^M])^+\longrightarrow\left(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N\right)^{\oplus 5}\qquad\qquad(N=M-\mathrm{ord}_\mathfrak{p}(2))$$

by the formula

$$z(f)=(f_+((1+\rho)\widetilde{s}),\,f_+((1+\rho)\kappa_1),\,f_-((1-\rho)\kappa_1),\,f_+((1+\rho)\kappa_\ell),\,f_-((1-\rho)\kappa_\ell)))$$

and set

$$Z = (z \circ j')(2G^+) = (z \circ j')(2\,\mathrm{Gal}(H_M(W)/H_M)^+),$$

which is a $\mathbf{Z}_p$-submodule of $(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N)^{\oplus 5}$. It follows from (7.6.3.2), (7.6.4.1), (7.6.4.3) and (7.6.4.4) that

$$\mathrm{Im}(z) \supseteq 2\,\mathfrak{p}^{a'}(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N) \oplus (2\,\mathfrak{p}^{M_2}(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N))^{\oplus 4},$$

where

$$N - a' \geq \exp(\widetilde{s}) - (M_2 + C_4 + \mathrm{ord}_\mathfrak{p}(2)).$$

Corollary 6.3.4 implies that

$$\mathcal{O}_\mathfrak{p} \cdot Z \supseteq \mathfrak{p}^a(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N) \oplus \mathfrak{p}^b(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N))^{\oplus 4},$$

where

$$N - a \geq \exp(\widetilde{s}) - (M_2 + C_2 + C_3 + C_4 + 6\,\mathrm{ord}_\mathfrak{p}(2)), \qquad b = M_2 + C_2 + C_3 + 5\,\mathrm{ord}_\mathfrak{p}(2).$$

According to Proposition 6.6.2, there exists an element $h = g^2 \in 2G^+$ such that the corresponding vector

$$(z_0, \ldots, z_4) = (z \circ j')(h) \in (\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N)^{\oplus 5}$$

satisfies

$$z_0 \notin \mathfrak{p}^{a+1}(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N), \qquad \begin{vmatrix} z_1 & z_2 \\ z_3 & z_4 \end{vmatrix} \notin 2\,\mathfrak{p}^{2b+1}(\mathcal{O}_\mathfrak{p}/\mathfrak{p}^N). \tag{7.6.4.5}$$

Applying the discussion from 6.5.1, we choose $\mathscr{L}'(W)$ satisfying (6.5.1.1-3) and not dividing ℓ. We denote by $\mathscr{L}', \lambda'_H, \ell' \in \mathscr{S}_1$ ($\ell' \neq \ell$) the induced primes of H_M, H and F, respectively. By construction, we have

$$2\,((1+\rho)\widetilde{s})_{\mathscr{L}'} = z_0 u_+, \qquad \begin{array}{ll} 2\,((1+\rho)\kappa_1)_{\mathscr{L}'} = z_1 u_+, & 2\,((1-\rho)\kappa_1)_{\mathscr{L}'} = z_2 u_-, \\ 2\,((1+\rho)\kappa_\ell)_{\mathscr{L}'} = z_3 u_+, & 2\,((1-\rho)\kappa_\ell)_{\mathscr{L}'} = z_4 u_-, \end{array}$$

hence

$$4(\kappa_1)_{\mathscr{L}'} = z_1 u_+ + z_2 u_-, \qquad 4(\kappa_\ell)_{\mathscr{L}'} = z_3 u_+ + z_4 u_-.$$

It follows from (7.6.4.5) that

$$\exp\left(((1+\rho)\widetilde{s})_{\mathscr{L}'}\right) \geq M - a \geq \exp(\widetilde{s}) - (M_2 + C_2 + C_3 + C_4 + 5\,\mathrm{ord}_\mathfrak{p}(2)) = \exp(\widetilde{s}) - (b + C_4) \tag{7.6.4.6}$$

and

$$\mathrm{res}_{\lambda'_H}\left(\mathcal{O}_\mathfrak{p}\,\kappa_1 + \mathcal{O}_\mathfrak{p}\,\kappa_\ell\right) \supseteq \mathfrak{p}^{2b} H^1_{ur}(H_{\lambda'_H}, A[\mathfrak{p}^M]) \xrightarrow{\sim} \mathfrak{p}^{2b} A[\mathfrak{p}^M]. \tag{7.6.4.7}$$

The second annihilation relation. Applying Proposition 7.2.3 with $\mathfrak{n} = \ell\ell'$ to the above element $s = \widetilde{s} \in \widetilde{S}^{(\beta)}$, we obtain, as in (7.5.2.3),

$$[H : K]\,(\widetilde{s}_{\mathscr{L}'}, (\kappa_\ell)_{\mathscr{L}'})_M = 0 \in \mathcal{O}_\mathfrak{p}/\mathfrak{p}^M(1).$$

Applying Proposition 7.2.3 with $\mathfrak{n} = \ell'$ to $s = \widetilde{s}$ (i.e., the first annihilation relation with ℓ' instead of ℓ), we obtain

$$[H : K]\,(\widetilde{s}_{\mathscr{L}'}, (\kappa_1)_{\mathscr{L}'})_M = 0 \in \mathcal{O}_\mathfrak{p}/\mathfrak{p}^M(1).$$

Combining these two relations with (7.6.4.7), we deduce that the element $\mathfrak{p}^{2b+C_5}\,\widetilde{s}_{\mathscr{L}'} \in A[\mathfrak{p}^M]$ lies in the kernel of the pairing $(\ ,\ )_M$, hence

$$\mathfrak{p}^{2b+C_5+C_6}\,\widetilde{s}_{\mathscr{L}'} = 0.$$

It follows from (7.6.4.6) that

$$\begin{aligned}\exp\left(\widetilde{S}^{(\beta)}\right) = \exp(\widetilde{s}) \leq \exp\left(((1+\rho)\widetilde{s})_{\mathscr{L}'}\right) + (b + C_4) \leq (2b + C_5 + C_6) + (b + C_4) = \\ = 3b + C_4 + C_5 + C_6 = 3C_0 + 3C_1 + 6C_2 + 6C_3 + 4C_4 + C_5 + C_6 + 30\,\mathrm{ord}_{\mathfrak{p}}(2).\end{aligned}$$

Combined with (7.6.3.5), this relation yields

$$2^{38}\,\mathfrak{p}^{4C_0+4C_1+7C_2+7C_3+5C_4+2C_5+2C_6}\left(S^{(\beta)}/\mathcal{O}_{\mathfrak{p}}\,\kappa_1\right) = 0,$$

which concludes the proof of Theorem 7.3 (hence also the proof of Theorem 3.2) in the case $\beta^2 \neq 1$.

References

[Be] M. Bertolini, *Selmer groups and Heegner points in anticyclotomic $\mathbf{Z}_p$-extensions*, Compositio Math. **99** (1995), 153–182.

[Be-Da] M. Bertolini, H. Darmon, *Kolyvagin's descent and Mordell-Weil groups over ring class fields*, J. Reine Angew. Math. **412** (1990), 63–74.

[Bi] B. Birch, *Heegner points of elliptic curves*, In: Symposia Mathematica, Vol. XV (Convegno di Strutture in Corpi Algebrici, INDAM, Rome, 1973), pp. 441–445. Academic Press, London, 1975.

[Bo] F.A. Bogomolov, *Sur l'algébricité des représentations l-adiques*, C. R. Acad. Sci. Paris Sér. A-B **290** (1980), no. 15, A701–A703.

[Bu] K. Buzzard, *Integral models of certain Shimura curves*, Duke Math. J. **87** (1997), 591–612.

[Ca 1] H. Carayol, *Sur la mauvaise réduction des courbes de Shimura*, Compositio Math. **59** (1986), 151–230.

[Ca 2] H. Carayol, *Sur les représentations ℓ-adiques attachées aux formes modulaires de Hilbert*, Ann. Sci. E.N.S. **19** (1986), 409–469.

[Cas] W. Casselman, *On abelian varieties with many endomorphisms and a conjecture of Shimura's*, Invent. Math. **12** (1971), 225–236.

[Con] B. Conrad, *Gross-Zagier revisited*, in: Heegner points and Rankin L-series, (H. Darmon, S.-W. Zhang, eds.), MSRI Publ. **49**, Cambridge Univ. Press, Cambridge, 2004, pp. 67–163.

[Co] C. Cornut, *Réduction de Familles de Points CMs*, Thesis, Strasbourg, 2000.

[Co-Va 1] C. Cornut, V. Vatsal, *Nontriviality of Rankin-Selberg L-functions and CM points*, to appear in: L-functions and Galois representations (Durham 2004).

[Co-Va 2] C. Cornut, V. Vatsal, *CM points and quaternion algebras*, Documenta Math. **10** (2005), 263-309.

[Cu-Re] C.W. Curtis, I. Reiner, *Methods of Representation Theory, Vol. I*, Wiley, New York, 1990.

[De] P. Deligne, *Travaux de Shimura*, Séminaire Bourbaki, exposé 389, 1970/71, Lect. Notes in Math. **244**, Springer, Berlin, 1971, pp. 123–165.

[De-Ra] P. Deligne, M. Rapoport, *Les schémas de modules de courbes elliptiques*, in: Modular functions of one variable II (Antwerp, 1972), Lect. Notes in Math. **349**, Springer, Berlin, 1973, pp. 143–316.

[Di] M. Dimitrov, *Galois representations modulo p and cohomology of Hilbert modular varieties*, Ann. Sci. E.N.S. **38** (2005), 505–551.

[Dr] V.G. Drinfeld, *Two theorems on modular curves* (Russian), Funkcional. Anal. i Priložen. **7** (1973), 83–84. English translation: Functional Anal. Appl. **7** (1973), 155–156.

[Fa] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366. Erratum: Invent. Math. **75** (1984), 381.

[Ge] S. Gelbart, *Lectures on the Arthur-Selberg trace formula*, Univ. Lect. Series **9**, Amer. Math. Soc., Providence, 1996.

[Gr 1] B.H. Gross, *Kolyvagin's work on modular elliptic curves*, in: L-functions and arithmetic (Durham, 1989; J. Coates, M.J. Taylor, eds.), London Math. Soc. Lect. Note Ser. **153**, Cambridge Univ. Press, Cambridge, 1991, pp. 235–256.

[Gr 2] B.H. Gross, *Heegner points and representation theory*, in: Heegner points and Rankin L-series, (H. Darmon, S.-W. Zhang, eds.), MSRI Publ. **49**, Cambridge Univ. Press, Cambridge, 2004, pp. 37–65.

[He] G. Henniart, *Représentations l-adiques abéliennes*, in: Séminaire de Théorie des Nombres de Paris 1980/81, Progress in Math. **22**, (M.-J. Bertin, ed.), Birkhäuser, Boston, 1982, pp. 107–126.

[Ho 1] B. Howard, *The Heegner point Kolyvagin system*, Compos. Math. **140** (2004), 1439–1472.

[Ho 2] B. Howard, *Iwasawa Theory of Heegner points on abelian varieties of GL_2-type*, Duke Math. J. **124** (2004), 1–45.

[Ja-La] H. Jacquet, R. Langlands, *Automorphic forms on $GL(2)$*, Lect. Notes in Math. **114**, Springer, Berlin-New York, 1970.

[Ka-Ma] N. Katz, B. Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies **108**, Princeton Univ. Press, Princeton, 1985.

[Ko] V. A. Kolyvagin, *Euler systems*, in: The Grothendieck Festschrift II, Progress in Mathematics **87**, Birkhäuser, Boston, Basel, Berlin, 1990, pp. 435–483.

[Ko-Lo 1] V.A. Kolyvagin, D.Yu. Logachev, *Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties* (Russian), Algebra i Analiz **1** (1989), 171–196. English translation: Leningrad Math. J. **1** (1990), 1229–1253.

[Ko-Lo 2] V.A. Kolyvagin, D.Yu. Logachev, *Finiteness of Ш over totally real fields* (Russian), Izv. Akad. Nauk. SSSR, Ser. Math. **55** (1991), 851–876. English translation: Math. USSR-Izv. **39** (1992), 829–853.

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

[Mi 2] J.S. Milne, *Canonical models of (mixed) Shimura varieties and automorphic vector bundles*, in: Automorphic forms, Shimura varieties, and L-functions, Vol. I (Ann Arbor, MI, 1988), Perspect. Math. **10**, Academic Press, Boston, 1990, pp. 283–414,

[Mi 3] J.S. Milne, *The points on a Shimura variety modulo a prime of good reduction*, in: The zeta functions of Picard modular surfaces, (R. Langlands, D. Ramakrishnan, eds.), Univ. Montreal, Montreal, 1992, pp. 151–253.

[Miy] T. Miyake, *Modular forms*, Springer, Berlin, 1989.

[Mu] D. Mumford, *Abelian varieties*, Oxford Univ. Press, London, 1970.

[Ne] J. Nekovář, *Selmer complexes*, to appear in Astérisque. Available at `http://www.math.jussieu.fr/~nekovar/pu/`

[Ne-Sch] J. Nekovář, N. Schappacher, *On the asymptotic behaviour of Heegner points*, Turkish J. of Math. **23** (1999), 549–556.

[Oh] M. Ohta, *On l-adic representations attached to automorphic forms*, Japan. J. Math. **8** (1982), 1–47.

[Ri] K. Ribet, *Galois action on division points of Abelian varieties with real multiplications*, Amer. J. Math. **98** (1976), 751–804.

[Sa] C.-H. Sah, *Automorphisms of finite groups*, J. Algebra **10** (1968), 47–68.

[Se 1] J.-P. Serre, *Corps locaux*, Hermann, Paris, 1962.

[Se 2] J.-P. Serre, *Abelian l-adic representations and elliptic curves*, W. A. Benjamin, New York-Amsterdam, 1968.

[Se 3] J.-P. Serre, *Lettre à Marie-France Vignéras du 10/2/1986*, Collected Papers IV, 38–55.

[Sh 1] G. Shimura, *On canonical models of arithmetic quotients of bounded symmetric domains*, Ann. of Math. **91** (1970), 144–222.

[Sh 2] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton Univ. Press, Princeton, 1971.

[Sh-Ta] G. Shimura, Y. Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, Publ. Math. Soc. Japan **6**, Tokyo, 1961.

[Tay] R. Taylor, *On Galois representations associated to Hilbert modular forms II*, in: Elliptic Curves, Modular Forms and Fermat's Last Theorem, (J. Coates, S.T. Yau, eds.), International Press, Boston, 1995, pp. 185–191.

[Ti] Y. Tian, *Euler systems of CM points on Shimura curves*, Thesis, Columbia University, 2003.

[Ti-Zh] Y. Tian, S.-W. Zhang, in preparation.

[Wa] L.C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Mathematics **83**, Second ed., Springer, New York, 1997.
[Zh 1] S.-W. Zhang, *Heights of Heegner points on Shimura curves*, Ann. of Math. (2) **153** (2001), 27–147.
[Zh 2] S.-W. Zhang, *Gross-Zagier formula for GL_2*, Asian J. Math. **5** (2001), 183–290.

Université Pierre et Marie Curie (Paris 6)
Institut de Mathématiques de Jussieu
Théorie des Nombres, Case 247
4, place Jussieu
F-75252 Paris cedex 05
FRANCE

www: `http://www.math.jussieu.fr/∼nekovar/`