Iwasawa's Main Conjecture for elliptic curves over anticyclotomic $\mathbb{Z}_p$-extensions

M. Bertolini*
H. Darmon†

February 19, 2003

Contents

*Partially supported by GNSAGA (INdAM), M.U.R.S.T., and the EC.
†Partially supported by CICMA and by an NSERC research grant.

Introduction

Let E be an elliptic curve over $\mathbb{Q}$, let p be an ordinary prime for E, and let K be an imaginary quadratic field. Write K_∞/K for the anticyclotomic $\mathbb{Z}_p$-extension of K and set $G_\infty = \mathrm{Gal}(K_\infty/K)$.

Following a construction of sec. 2 of [BD1] which is recalled in section 1, one attaches to the data (E, K, p) an anticyclotomic p-adic L-function $L_p(E, K)$ which belongs to the Iwasawa algebra $\Lambda := \mathbb{Z}_p[\![G_\infty]\!]$. This element, whose construction was inspired by a formula proved in [Gr1], is known, thanks to work of Zhang ([Zh] §1.4), to interpolate special values of the complex L-function of E/K twisted by characters of G_∞.

Let $\mathrm{Sel}(K_\infty, E_{p^\infty})^\vee$ be the Pontrjagin dual of the p-primary Selmer group attached to E over K_∞, equipped with its natural Λ-module structure, as defined in section 2. It is a compact Λ-module; write $\mathcal{C}$ for its characteristic power series, which is well-defined up to units in Λ.

Let N_0 denote the conductor of E, set $N = pN_0$ if E has good ordinary reduction at p, and set $N = N_0$ if E has multiplicative reduction at p so that p divides N_0 exactly. It will be assumed throughout that the discriminant of K is prime to N, so that K determines a factorisation

$$N = pN^+N^-,$$

where N^+ (resp. N^-) is divisible only by primes different from p which are split (resp. inert) in K.

The main goal of the present work is to prove (under the mild technical assumption 6 on (E, K, p) given at the end of this introduction) theorem 1 below, a weak form of the Main Conjecture of Iwasawa Theory for elliptic curves in the ordinary and anticyclotomic setting.

Theorem 1 *Assume that N^- is the square-free product of an odd number of primes. The characteristic power series $\mathcal{C}$ divides the p-adic L-function $L_p(E, K)$.*

The hypothesis on N^- made in theorem 1 arises naturally in the anticyclotomic setting, and some justification for it is given at the end of the introduction.

Denote by $L_p(E, K, s)$ the p-adic Mellin transform of the measure defined by the element $L_p(E, K)$ of Λ. Let r be the rank of the Mordell-Weil group $E(K)$. The next result follows by combining theorem 1 with standard techniques of Iwasawa theory.

Corollary 2 $\mathrm{ord}_{s=1} L_p(E, K, s) \geq r$.

A program of study of $L_p(E, K, s)$ in the spirit of the work of Mazur, Tate and Teitelbaum [MTT] is outlined in [BD1], and partially carried out in [BD2]–[BD5]. In particular, section 4 of [BD1] formulates a conjecture predicting the exact order of vanishing of $L_p(E, K, s)$ at $s = 1$. More precisely, set $E^+ = E$ and let E^- be the elliptic curve over $\mathbb{Q}$ obtained by twisting E by K. Write $r^\pm$ for the rank of $E^\pm(\mathbb{Q})$, so that $r = r^+ + r^-$. Set $\tilde{r}^\pm = r^\pm + \delta^\pm$, where

$$\delta^\pm = \begin{cases} 1 & \text{if } E^\pm \text{ has split multiplicative reduction at } p, \\ 0 & \text{otherwise.} \end{cases}$$

Finally set $\rho := \max(\tilde{r}^+, \tilde{r}^-)$ and $\tilde{r} := \tilde{r}^+ + \tilde{r}^-$. Conjecture 4.2 of [BD1] predicts that

$$\mathrm{ord}_{s=1} L_p(E, K, s) = 2\rho = \tilde{r} + |\tilde{r}^+ - \tilde{r}^-|. \tag{1}$$

This conjecture indicates that $L_p(E, K, s)$ vanishes to order strictly greater than r, if either $\tilde{r} > r$ or if $\tilde{r}^+ \neq \tilde{r}^-$. The first source of extra vanishing is accounted for by the phenomenon of exceptional zeroes arising when p is a prime of split multiplicative reduction for E over K, which was discovered by Mazur, Tate and Teitelbaum in the cyclotomic setting [MTT]. The second source of extra vanishing is specific to the anticyclotomic setting, and may be accounted for by certain predictable degeneracies in the anticyclotomic p-adic height, related to the fact that $\mathrm{Sel}(K_\infty, E_{p^\infty})^\vee$ fails to be semisimple as a module over Λ when $r^+ \neq r^-$. (Cf. for example [BD$\frac{1}{2}$].)

A more careful study of the Λ-module structure of $\mathrm{Sel}(K_\infty, E_{p^\infty})$, which in the good ordinary reduction case is carried out in [BD0] and [BD$\frac{1}{2}$], yields the following refinement of corollary 2 which is consistent with the conjectured equality (1).

Corollary 3 *If p is a prime of good ordinary reduction for E, then*

$$\mathrm{ord}_{s=1} L_p(E, K, s) \geq 2\rho.$$

Let $\mathcal{O}$ be a finite extension of $\mathbb{Z}_p$, and let $\chi : G_\infty \longrightarrow \mathcal{O}^\times$ be a finite order character, extended by $\mathbb{Z}_p$-linearity to a homomorphism of Λ to $\mathcal{O}$. If M is any Λ-module, write

$$M^\chi = M \otimes_\chi \mathcal{O},$$

where the tensor product is taken over Λ via the map χ.

Let $Ш_p(E/K_\infty)$ denote the p-primary part of the Shafarevich-Tate group of E over K_∞. A result of Zhang ([Zh], §1.4) generalising a formula of Gross established in [Gr1] in the special case where N is prime and χ is unramified, relates $\chi(L_p(E, K))$ to a non-zero multiple of the classical L-value $L(E/K, \chi, 1)$ (where one views χ as a complex-valued character by choosing an embedding of $\mathcal{O}$ into $\mathbb{C}$). Theorem 1 combined with Zhang's formula leads to the following corollary, a result which lends some new evidence for the classical Birch and Swinnerton-Dyer conjecture.

Corollary 4 *If $L(E/K, \chi, 1) \neq 0$, then $E(K_\infty)^\chi$ and $Ш_p(E/K_\infty)^\chi$ are finite.*

Remarks:
1. The restriction that χ be of p-power conductor is not essential for the method that is used in this work, so that it should be possible, with little extra effort, to establish corollary 4 for arbitrary anticyclotomic χ, and for

the χ-part of the full Shafarevich-Tate group and not just its p-primary part, using the techniques in the proof of theorem 1.

2. Corollary 4 was also proved in [BD2] by a different, more restrictive method which requires the assumption that p is a prime of *multiplicative reduction* for E/K which is inert in K. Hence, in contrast with the previous remark, the method of [BD2] cannot be used to obtain the finiteness of the full Shafarevich-Tate group of E, but only of its p-primary part for a finite set of primes p.

3. The non-vanishing of $L(E/K, \chi, 1)$ seems to occur fairly often. For example, Vatsal has shown ([Va1], theorem 1.4) that $L(E/K, \chi, 1)$ is non-zero for almost all χ when χ varies over the anticyclotomic characters of p-power conductor for a fixed p.

Another immediate consequence of theorem 1 is that $\mathrm{Sel}(K_\infty, E_{p^\infty})$ is a cotorsion Λ-module whenever $L_p(E, K)$ is not identically 0, so that in particular one has

Corollary 5 *If $L_p(E, K)$ is non-zero, then the Mordell-Weil group $E(K_\infty)$ is finitely generated.*

Remark: The non-vanishing of $L_p(E, K)$ has been established by Vatsal. See for example theorem 1.1 of [Va2] which even gives a precise formula for the associated μ-invariant.

Assumptions:

Let E_p be the mod p representation of $G_{\mathbb{Q}}$ attached to E. For simplicity, it is assumed throughout the paper that (E, K, p) satisfies the following conditions.

Assumption 6 *1. The prime p is ≥ 5.*

2. The Galois representation attached to E_p has image isomorphic to $\mathbf{GL}_2(\mathbb{F}_p)$.

3. The prime p does not divide the minimal degree of a modular parametrisation $X_0(N_0) \longrightarrow E$.

4. For all primes ℓ such that ℓ^2 divides N, and p divides $\ell + 1$, the module E_p is an irreducible I_ℓ-module.

Remarks:
1. Note that these assumptions are satisfied by all but finitely many primes once E is fixed, provided that E has no complex multiplications. They are imposed to simplify the argument and could probably be relaxed. This is unlike the condition in theorem 1 which – although it may appear less natural to the uninitiated – is an essential feature of the situation being studied. Indeed, for square-free N^-, the restriction on the parity of the number of primes appearing in its factorisation is equivalent to requiring that the sign in the functional equation of $L(E, K, \chi, s)$, for χ a ramified character of G_∞, is equal to 1. Without this condition, the p-adic L-function $L_p(E, K, s)$ would vanish identically. See [BD1] for a discussion of this case where it becomes necessary to interpolate the first derivatives $L'(E, K, \chi, 1)$.

2. The analogue of theorem 1 for the cyclotomic $\mathbb{Z}_p$-extension has been proved by Kato. Both the proof of theorem 1 and Kato's proof of the cyclotomic counterpart are based on Kolyvagin's theory of Euler systems.

3. The original "Euler system" argument of Kolyvagin relies on the presence of a systematic supply of algebraic points on E - the so-called *Heegner points* defined over K and over abelian extensions of K. As can be seen from corollaries 4 and 5, the situation in which we have placed ourselves precludes the existence of a non-trivial norm-compatible system of points in $E(K_\infty)$. One circumvents this difficulty by resorting to the theory of congruences between modular forms and the Ceednik-Drinfeld interchange of invariants, which, for each $n \geq 1$, realises the Galois representation E_{p^n} in the p^n-torsion of the Jacobian of certain Shimura curves for which the Heegner point construction becomes available. By varying the Shimura curves, a compatible collection of cohomology classes in $H^1(K_\infty, E_{p^n})$ is produced, a collection which can be related to special values of L-functions and is sufficient to control the Selmer group $\mathrm{Sel}(K_\infty, E_{p^\infty})$. It should be noted that this geometric approach to the theory of Euler Systems produces ramified cohomology classes in $H^1(K_\infty, E_{p^n})$ directly without resorting to classes defined over auxiliary ring class field extensions of K_∞; in particular, Kolyvagin's derivative operators make no appearance in the argument. In the terminology of [MR], the strategy of this article produces a "Kolyvagin system" without passing through an Euler system in the sense of [Ru]. This lends some support for the suggestion made in [MR] that Kolyvagin systems are the more fundamental objects of study.

Acknowledgements: It is a pleasure to thank Professor Ihara for some useful information on his work, as well as Kevin Buzzard, Ben Howard and the anonymous referees for many helpful comments which led to some corrections and significant improvements in the exposition.

1 p-adic L-functions

1.1 Modular forms on quaternion algebras

Let N^- be an arbitrary square-free integer which is the product of an odd number of primes, and let N^+ be any integer prime to N^-. Let p be a prime which does not divide N^+N^- and write $N = pN^+N^-$. Let B be the definite quaternion algebra ramified at all the primes dividing N^-, and let R be an Eichler $\mathbb{Z}[1/p]$-order of level N^+ in B. The algebra B is unique up to isomorphism, and the Eichler order R is unique up to conjugation by $B^\times$, by strong approximation (cf. [Vi], chapitre III, §4 and §5).

Denote by $\mathcal{T}$ the Bruhat-Tits tree of $B_p^\times/\mathbb{Q}_p^\times$, where

$$B_p := B \otimes \mathbb{Q}_p \simeq M_2(\mathbb{Q}_p).$$

The set $\mathcal{V}(\mathcal{T})$ of vertices of $\mathcal{T}$ is indexed by the maximal $\mathbb{Z}_p$-orders in B_p, two vertices being adjacent if their intersection is an Eichler order of level p. Let $\vec{\mathcal{E}}(\mathcal{T})$ denote the set of ordered edges of $\mathcal{T}$, i.e., the set of ordered pairs (s,t) of adjacent vertices of $\mathcal{T}$. If $e = (s,t)$, the vertex s is called the *source* of e and the vertex t is called its *target*; they are denoted by $s(e)$ and $t(e)$ respectively.

The tree $\mathcal{T}$ is endowed with a natural left action of $B_p^\times/\mathbb{Q}_p^\times$ by isometries corresponding to conjugation of maximal orders by elements of $B_p^\times$. This action is transitive on both $\mathcal{V}(\mathcal{T})$ and $\vec{\mathcal{E}}(\mathcal{T})$. Let $R^\times$ denote the group of invertible elements of R. The group $\Gamma := R^\times/\mathbb{Z}[1/p]^\times$ – a discrete subgroup of $B_p^\times/\mathbb{Q}_p^\times$ in the p-adic topology – acts naturally on $\mathcal{T}$ and the quotient $\mathcal{T}/\Gamma$ is a finite graph.

Definition 1.1 *A modular form (of weight two) on $\mathcal{T}/\Gamma$ is a $\mathbb{Z}_p$-valued function f on $\vec{\mathcal{E}}(\mathcal{T})$ satisfying*

$$f(\gamma e) = f(e), \quad \textit{for all } \gamma \in \Gamma.$$

Denote by $S_2(\mathcal{T}/\Gamma)$ the space of such modular forms. It is a free $\mathbb{Z}_p$-module of finite rank. More generally, if Z is any ring, denote by $S_2(\mathcal{T}/\Gamma, Z)$ the space of Γ-invariant functions on $\vec{\mathcal{E}}(\mathcal{T})$ with values in Z.

Duality. Let $e_1, \ldots, e_s$ be a set of representatives for the orbits of Γ acting on $\vec{\mathcal{E}}(\mathcal{T})$, and let w_j be the cardinality of the finite group $\mathrm{Stab}_\Gamma(e_j)$. The space $S_2(\mathcal{T}/\Gamma)$ is endowed with a $\mathbb{Z}_p$-bilinear pairing defined by

$$\langle f_1, f_2\rangle = \sum_{i=1}^{s} w_i f_1(e_i) f_2(e_i). \tag{2}$$

This pairing is non-degenerate so that it identifies $S_2(\mathcal{T}/\Gamma) \otimes \mathbb{Q}_p$ with its $\mathbb{Q}_p$-dual.

Hecke operators. Let $\ell \neq p$ be a prime which does not divide p. Choose an element M_ℓ of reduced norm ℓ in the $\mathbb{Z}[1/p]$-order R that was used to define Γ. The double coset $\Gamma M_\ell \Gamma$ decomposes as a disjoint union of left cosets:

$$\Gamma M_\ell \Gamma = \gamma_1 \Gamma \cup \cdots \cup \gamma_t \Gamma. \tag{3}$$

Here $t = \ell + 1$ (resp. ℓ, 1) if ℓ does not divide N^+N^- (resp. divides N^+, N^-). The function $f_{|\ell}$ defined on $\vec{\mathcal{E}}(\mathcal{T})$ by the rule

$$f_{|\ell}(e) = \sum_{i=1}^{t} f(\gamma^{-1} e) \tag{4}$$

is independent of the choice of M_ℓ or of the representatives $\gamma_1, \ldots, \gamma_t$, and the assignment $f \mapsto f_{|\ell}$ is a linear endomorphism of $S_2(\mathcal{T}/\Gamma)$, called the ℓ-th Hecke operator at ℓ and denoted T_ℓ if ℓ does not divide N, and U_ℓ if ℓ divides N^+N^-.

Associated to the prime p there is a Hecke operator denoted U_p and defined by the rule

$$(U_p f)(e) = \sum_{s(e')=t(e)} f(e'). \tag{5}$$

The Hecke operators T_ℓ (with $\ell \not| N$) are called the *good* Hecke operators. They are self-adjoint for the pairing on $S_2(\mathcal{T}/\Gamma)$ defined in (2):

$$\langle T_\ell f_1, f_2\rangle = \langle f_1, T_\ell f_2\rangle. \tag{6}$$

Oldforms and Newforms. Let $S_2(\mathcal{V}/\Gamma, Z)$ denote the space of Γ-invariant Z-valued functions on $\mathcal{V}(\mathcal{T})$, equipped with a Z-valued bilinear pairing as in (2) with edges replaced by vertices. There are two natural "degeneracy maps" $s^*, t^* : S_2(\mathcal{V}/\Gamma) \longrightarrow S_2(\mathcal{T}/\Gamma)$ defined by

$$s^*(f)(e) = f(s(e)), \quad t^*(f)(e) = f(t(e)).$$

A form $f \in S_2(\mathcal{T}/\Gamma, Z)$ is said to be p-old if there exist Γ-invariant functions f_1 and f_2 on $\mathcal{V}(\mathcal{T})$ such that

$$f = s^*(f_1) + t^*(f_2). \tag{7}$$

A form which is orthogonal to the oldforms (i.e., is orthogonal to the image of s^* and t^*) is said to be p-new. The form f is p-new if and only if f is *harmonic* in the sense that it satisfies

$$s_*(f)(v) := \sum_{s(e)=v} f(e) = 0, \quad t_*(f)(v) := \sum_{t(e)=v} f(e) = 0, \quad \forall v \in \mathcal{V}(\mathcal{T}). \tag{8}$$

This can be seen by noting that s_* and t_* are the adjoints of the maps s^* and t^* respectively.

p-isolated forms. Let $\mathbb{T}$ be the Hecke algebra acting on the space $S_2(\mathcal{T}/\Gamma)$. A form f in this space is called an *eigenform* if it is a simultaneous eigenvector for all the Hecke operators, i.e.,

$$\begin{aligned} T_\ell(f) &= a_\ell(f) f, \quad \text{for all } \ell \not| N, \\ U_\ell(f) &= \alpha_\ell(f) f, \quad \text{for all } \ell | N, \end{aligned}$$

where the eigenvalues $a_\ell(f)$ and $\alpha_\ell(f)$ belong to $\mathbb{Z}_p$. Such an eigenform determines a maximal ideal $\mathfrak{m}_f$ of $\mathbb{T}$ by the rule

$$\mathfrak{m}_f := \langle p, T_\ell - a_\ell(f), \quad U_\ell - \alpha_\ell(f) \rangle .$$

Definition 1.2 *The eigenform f is said to be p-*isolated *if the completion of $S_2(\mathcal{T}/\Gamma)$ at $\mathfrak{m}_f$ is a free $\mathbb{Z}_p$-module of rank one.*

In other words, f is p-isolated if there are no non-trivial congruences between f and other modular forms in $S_2(\mathcal{T}/\Gamma)$. Note that this is really a property of the mod p eigenform in $S_2(\mathcal{T}/\Gamma, \mathbb{F}_p)$ associated to f, or of the maximal ideal $\mathfrak{m}_f$, so that it makes sense to say that $\mathfrak{m}_f$ is p-isolated if it is attached to (the reduction of) a p-isolated eigenform.

The Jacquet-Langlands correspondence. The complex vector space $S_2(\mathcal{H}/\Gamma_0(N))$ of classical modular forms of weight 2 on $\mathcal{H}/\Gamma_0(N))$ is similarly endowed with an action of Hecke operators, which will also be denoted by the symbols T_ℓ, U_ℓ and U_p by abuse of notation. Let ϕ be an eigenform on $\Gamma_0(N)$ which arises from a newform ϕ_0 of level N_0. It is a simultaneous eigenfunction for all the good Hecke operators T_ℓ. Assume that it is also an eigenfunction for the Hecke operator U_p. Write a_ℓ for the eigenvalue of T_ℓ acting on ϕ, and α_p for the eigenvalue of U_p acting on ϕ.

Remark: If p does not divide N_0, so that ϕ is not new at p, then the eigenvalue α_p is a root of the polynomial $x^2 - a_p x + p$, where a_p is the eigenvalue of T_p acting on ϕ_0. If p divides N_0, then $\phi = \phi_0$ and the eigenvalue α_p is equal to 1 (resp -1) if the abelian variety attached to ϕ by the Eichler-Shimura construction has split (resp. non-split) multiplicative reduction at p.

Proposition 1.3 *Let ϕ be as above. Then there exists an eigenform f in $S_2(\mathcal{T}/\Gamma, \mathbb{C})$ satisfying*

$$\begin{aligned} &T_\ell f = a_\ell(\phi) f \text{ for all } \ell \not| N, \\ &U_\ell f = \alpha_\ell(\phi) f \text{ for all } \ell | N^+, \qquad U_p f = \alpha_p(\phi) f. \end{aligned} \tag{9}$$

The form f with these properties is unique up to multiplication by a non-zero complex number. Conversely, given an eigenform $f \in S_2(\mathcal{T}/\Gamma, \mathbb{C})$, there exists an eigenform $\phi \in S_2(\mathcal{H}/\Gamma_0(N))$ satisfying (9).

Proof: Suppose first that p divides N_0, so that ϕ is a newform on $\Gamma_0(N)$. Let R_0 be an Eichler $\mathbb{Z}$-order of level pN^+ in the definite quaternion algebra of discriminant N^-. Write $\hat{R}_0 = R_0 \otimes \hat{\mathbb{Z}} = \prod_\ell R_0 \otimes \mathbb{Z}_\ell$, and $\hat{B} := \hat{R}_0 \otimes \mathbb{Q}$. The Jacquet-Langlands correspondence (which, in this case, can be established using the Eichler trace formula as in [Ei]; see also [JL] and the dicussion in chapter 5 of [DT]) implies the existence of a unique function

$$f : B^\times \backslash \hat{B}^\times / \hat{R}_0^\times \longrightarrow \mathbb{C} \tag{10}$$

satisfying $T_\ell f = a_\ell f$ for all $\ell \not| N$, and $U_p f = \alpha_p f$. (Where the operators T_ℓ and U_p are the general Hecke operators defined in terms of double cosets as in [Sh].) Strong approximation identifies the double coset space appearing in (10) with the space $R^\times \backslash B_p^\times/(R_0)_p^\times$. The transitive action of $B_p^\times$ on the set of maximal orders in B_p by conjugation yields an action of $B_p^\times$ on $\mathcal{T}$ by isometries, for which the subgroup $(R_0)_p^\times$ is equal to the stabiliser of a certain oriented edge. In this way $B_p^\times/(R_0)_p^\times$ is identified with $\vec{\mathcal{E}}(\mathcal{T})$, and f can thus be viewed as an element of $S_2(\mathcal{T}/\Gamma, \mathbb{C})$.

If p does not divide N_0, let a_p denote the eigenvalue of T_p acting on ϕ_0, and let R_0 denote now the Eichler order of level N^+ in the quaternion algebra B. As before, to the form ϕ_0 is associated a unique function

$$f_0 : B^\times \backslash \hat{B}^\times/\hat{R}_0^\times \longrightarrow \mathbb{C} \tag{11}$$

satisfying $T_\ell f = a_\ell f$ for all $\ell \not| N_0$. As before, strong approximation makes it possible to identify f_0 with a Γ-invariant function on $\mathcal{V}(\mathcal{T})$. In this description, the action of T_p on f_0 is given by the formula

$$T_p(f_0(v)) = \sum_w f_0(w),$$

where the sum is taken over the $p+1$ vertices w of $\mathcal{T}$ which are adjacent to v. Define functions $f_s, f_t : \vec{\mathcal{E}}(\mathcal{T}) \longrightarrow \mathbb{C}$ by the rules:

$$f_s(e) = f_0(s(e)), \qquad f_t(e) = f_0(t(e)).$$

The forms f_s and f_t both satisfy $T_\ell(g) = a_\ell g$ for all $\ell \not| N$, and span the two-dimensional eigenspace of forms with this property. A direct calculation reveals that

$$U_p f_s = p f_t, \quad U_p f_t = -f_s + a_p f_t.$$

The function $f = f_s - \alpha_p f_t$ satisfies $U_p f = \alpha_p f$, and is, up to scaling, the unique eigenform in $S_2(\mathcal{T}/\Gamma, \mathbb{C})$ with this property.

The converse is proved by essentially reversing the argument above: to an eigenform $f \in S_2(\mathcal{T}/\Gamma, \mathbb{C})$ is associated a function on the adelic coset space attached to $B^\times$ as in (10); the Jacquet-Langlands correspondence (applied now in the reverse direction) produces the desired $\phi \in S_2(\mathcal{H}/\Gamma_0(N))$.

The Shimura-Taniyama conjecture. Let E be an elliptic curve as in the introduction. For each prime ℓ which does not divide N, set

$$a_\ell = \ell + 1 - \#E(\mathbb{F}_\ell).$$

If E has good ordinary reduction at p, let $\alpha_p \in \mathbb{Z}_p$ be the unique root of the polynomial $x^2 - a_p x + p$ which is a p-adic unit. Set $\alpha_p = 1$ (resp. -1) if E has split (resp. non-split) multiplicative reduction at p. The following theorem is a consequence of the Shimura-Taniyama conjecture in view of proposition 1.3.

Proposition 1.4 *There exists an eigenform f in $S_2(\mathcal{T}/\Gamma)$ satisfying*

$$T_\ell f = a_\ell f, \text{ for all } \ell \not| N \quad U_p f = \alpha_p f,$$

$$f \notin pS_2(\mathcal{T}/\Gamma).$$

The form f with these properties is unique up to multiplication by a scalar in $\mathbb{Z}_p^\times$.

Proof: Proposition 1.3 shows that there exists a form $f \in S_2(\mathcal{T}/\Gamma, \mathbb{C})$ satisfying the conclusion of proposition 1.4. The eigenvalues a_ℓ belong to $\mathbb{Z}$, and, since E is ordinary at p, the eigenvalue α_p belongs to the ring of integers $\mathcal{O}$ of a quadratic extension of $\mathbb{Q}$ in which p splits completely. Hence, the form f can be chosen to lie in $S_2(\mathcal{T}/\Gamma, \mathcal{O})$. After applying the unique embedding of $\mathcal{O}$ into $\mathbb{Z}_p$ which sends α_p to a p-adic unit, and rescaling f appropriately, one obtains a form in $S_2(\mathcal{T}/\Gamma)$ satisfying the conclusion of proposition 1.4.

1.2 p-adic Rankin L-functions

An eigenform f in $S_2(\mathcal{T}/\Gamma)$ is said to be *ordinary* if the eigenvalue α_p of U_p acting on f is a p-adic unit. This section recalls the definition of the p-adic Rankin L-function attached to an ordinary form on $\mathcal{T}/\Gamma$ and a quadratic algebra $K \subset B$.

If A is any $\mathbb{Z}$-algebra, let

$$A_\ell = A \otimes \mathbb{Z}_\ell, \quad \hat{A} = A \otimes \hat{\mathbb{Z}} = \prod_\ell A_\ell. \tag{12}$$

Let K be a quadratic algebra of discriminant prime to N which embeds in B. Since B is definite of discriminant N^-, the algebra K is an imaginary quadratic field in which all prime divisors of N^- are inert. Let $\mathcal{O}_K$ denote the ring of integers of K and let $\mathcal{O} = \mathcal{O}_K[1/p]$ be the maximal $\mathbb{Z}[1/p]$-order in K.

Let $\tilde{G}_\infty$ denote the group

$$\tilde{G}_\infty = \hat{K}^\times/(\hat{\mathbb{Q}}^\times \prod_{\ell \neq p} \mathcal{O}_\ell^\times K^\times) \tag{13}$$

Fix an embedding

$$\Psi : K \longrightarrow B \quad \text{satisfying} \quad \Psi(K) \cap R = \Psi(\mathcal{O}). \tag{14}$$

Such a Ψ exists if and only if all the primes dividing N^+ are split in K. By passing to the adelisation the embedding Ψ induces a map

$$\hat{\Psi} : \tilde{G}_\infty \longrightarrow B^\times \backslash \hat{B}^\times / \left(\hat{\mathbb{Q}}^\times \prod_{\ell \neq p} R_\ell^\times \right). \tag{15}$$

By strong approximation ([Vi], chapitre III, §4), the double coset space appearing on the right has a fundamental region contained in $B_p^\times \subset \hat{B}^\times$. In fact, strong approximation yields a canonical identification

$$\eta : B^\times \backslash \hat{B}^\times / \left(\hat{\mathbb{Q}}^\times \prod_{\ell \neq p} R_\ell^\times \right) \longrightarrow \Gamma \backslash B_p^\times / \mathbb{Q}_p^\times. \tag{16}$$

The modular form $f \in S_2(\mathcal{T}/\Gamma)$ determines a pairing between $\tilde{G}_\infty$ and $\vec{\mathcal{E}}(\mathcal{T})$ by the rule

$$[\sigma, e]_f := f(\eta \hat{\Psi}(\sigma) e) \in \mathbb{Z}_p. \tag{17}$$

The embedding Ψ induces an embedding of $K_p^\times$ into $B_p^\times$ and hence yields an action of $K_p^\times/\mathbb{Q}_p^\times$ on $\mathcal{T}$. This action fixes a single vertex if p is inert in K, and no vertex if p is split in K. Let

$$U_n := (1 + p^n \mathcal{O}_K \otimes \mathbb{Z}_p)^\times / (1 + p^n \mathbb{Z}_p)^\times \tag{18}$$

denote the standard compact subgroup of $K_p^\times/\mathbb{Q}_p^\times$ of level n. Choose a sequence $e_1, e_2, \ldots, e_n, \ldots$ of consecutive edges on $\mathcal{T}$ satisfying

$$\mathrm{Stab}_{K_p^\times/\mathbb{Q}_p^\times}(e_j) = U_j, \quad j = 1, \ldots, n, \ldots. \tag{19}$$

Since α_p is a p-adic unit, the pairing defined by equation (17) can be used to define a $\mathbb{Z}_p$-valued distribution $\tilde{\nu}_f$ on $\tilde{G}_\infty$ by the rule

$$\tilde{\nu}_f(\sigma U_j) := \alpha_p^{-j}[\sigma, e_j]_f, \tag{20}$$

for all compact open subsets of $\tilde{G}_\infty$ of the form σU_j with $\sigma \in \tilde{G}_\infty$. The distribution relation for $\tilde{\nu}_f$ is ensured by the fact that f is an eigenform for the U_p operator with eigenvalue α_p. The distribution $\tilde{\nu}_f$ gives rise to an element $\tilde{\mathcal{L}}_f$ in the completed integral group ring $\mathbb{Z}_p[\![\tilde{G}_\infty]\!]$ by the rule

$$(\tilde{\mathcal{L}}_f)_n := \sum_{g \in \tilde{G}_n} \tilde{\nu}_f(gU_n) \cdot g,$$

where $\tilde{G}_n := \tilde{G}_\infty/U_n$ so that $\tilde{G}_\infty$ is the inverse limit of the finite groups $\tilde{G}_n$.

Let Δ denote the torsion subgroup of $\tilde{G}_\infty$, and let

$$G_\infty = \tilde{G}_\infty/\Delta \simeq \mathbb{Z}_p. \tag{21}$$

Write $\mathcal{L}_f$ for the natural image of $\tilde{\mathcal{L}}_f$ in the Iwasawa algebra

$$\Lambda = \mathbb{Z}_p[\![G_\infty]\!] \simeq \mathbb{Z}_p[\![T]\!],$$

and denote by ν_f the associated measure on G_∞. Note that a different choice of edges e_j satisfying (19) has the effect of multiplying $\mathcal{L}_f$ by an element of G_∞, so that $\mathcal{L}_f$ is only well-defined up to multiplication by such elements.

Functional equations. The Iwasawa algebra is equipped with the involution $\theta \mapsto \theta^*$ sending any $\sigma \in G_\infty$ to σ^{-1}. Let $\epsilon = \pm 1$ be the sign in the functional equation of the classical L-function $L(E/\mathbb{Q}, s)$ attached to $E/\mathbb{Q}$. Conjecturally, the value of ϵ determines the parity of the rank of $E/\mathbb{Q}$. More precisely, this rank should be even if $\epsilon = 1$, and odd if $\epsilon = -1$. Set $\epsilon_p = \epsilon$ if E does not have split multiplicative reduction over $\mathbb{Q}_p$, and set $\epsilon_p = -\epsilon$ otherwise. The sign ϵ_p is interpreted in [MTT] as the sign in the functional equation for the Mazur-Swinnerton-Dyer p-adic L-function attached to $E/\mathbb{Q}$. While this L-function differs markedly from the p-adic Rankin L-function considered in this article, one still has

Lemma 1.5 *The equality*

$$\mathcal{L}_f^* = \epsilon_p \mathcal{L}_f$$

holds in Λ, up to multiplication by an element of G_∞.

Proof: See proposition 2.13 and equation (11) of [BD1].

Definition 1.6 *The anticyclotomic Rankin L-function attached to f and K is the element $L_p(f,K)$ of Λ defined by*

$$L_p(f,K) = \mathcal{L}_f \mathcal{L}_f^*.$$

Remark: 1. Note that $L_p(f,K)$ is a well-defined element of Λ, since multiplying $\mathcal{L}_f$ by $\sigma \in G_\infty$ has the effect of multiplying $\mathcal{L}_f^*$ by σ^{-1}. Thus the ambiguity in the definition of $\mathcal{L}_f$ arising from the choice of end in $\mathcal{T}$ satisfying (19) is cancelled out.

2. Definition 1.6 extends naturally, *mutatis mutandis*, to any eigenform g in $S_2(\mathcal{T}/\Gamma, Z)$, where Z is any ring in which the eigenvalue of U_p acting on g is invertible. In this case the anticyclotomic Rankin L-function $L_p(g,K)$ is simply an element of the completed group ring $Z[\![G_\infty]\!]$.

Let $\mu_{f,K}$ be the $\mathbb{Z}_p$-valued measure on G_∞ associated to $L_p(f,K)$. The function $L_p(f,K,s)$ is defined to be the p-adic Mellin transform of $\mu_{f,K}$:

$$L_p(f,K,s) := \int_{G_\infty} g^{s-1} d\mu_{f,K}(g).$$

where $g^{s-1} := \exp((s-1)\log(g))$, and $\log : G_\infty \to \mathbb{Q}_p$ is a choice of p-adic logarithm.

Interpolation properties. Let ϕ be the normalised eigenform on $\Gamma_0(N)$ attached to f via the Jacquet-Langlands correspondence of proposition 1.3, and let $\Omega_f = \langle \phi, \phi \rangle$ denote the Peterson scalar product of ϕ with itself. It is known (cf. [Zh], sec. 1.4) that the measure $\mu_{f,K}$ on G_∞ satisfies the following p-adic interpolation property:

$$|\int_{\tilde{G}_\infty} \chi(g) d\mu_{f,K}(g)|^2 \doteq L(f,K,\chi,1)/(\sqrt{\mathrm{Disc}(K)}\Omega_f),$$

for all ramified finite order characters χ of $\tilde{G}_\infty$. Here the values of χ and $\mu_{f,K}$ are viewed as complex numbers by fixing an embedding of $\bar{\mathbb{Q}}_p$ in $\mathbb{C}$, and the absolute value taken on the left-hand side is the complex one. The symbol $\doteq$ indicates an equality up to a simple algebraic fudge factor expressed as a product of terms comparatively less important than the quantities explicitly described in the formulas. Note in particular that dividing $L(f, K, \chi, 1)$ by the complex period Ω_f yields an algebraic number.

Elliptic curves. If E is an elliptic curve as in the introduction, let f_E be the modular form in $S_2(\mathcal{T}/\Gamma)$ attached to it by proposition 1.4. The p-adic L-function attached to E and K is defined by:

$$L_p(E, K) := L_p(f_E, K), \quad L_p(E, K, s) := L_p(f_E, K, s). \tag{22}$$

Remark: Note that $L_p(E, K)$ is only well-defined up to multiplication by a unit in $\mathbb{Z}_p^\times$, since the same is true of the form f_E attached to it by proposition 1.4.

2 Selmer Groups

2.1 Galois representations and cohomology

Let f be an ordinary eigenform in $S_2(\mathcal{T}/\Gamma)$ with coefficients in $\mathbb{Z}_p$, and let K be a quadratic imaginary field in which all primes dividing N^- (resp. N^+) are inert (resp. split). To these two objects a p-adic L-function $L_p(f, K)$ was attached in section 1. This section introduces an invariant of a more arithmetic nature – the so called *Selmer group* attached to f and K.

Galois representations. To f is attached a continous representation of the Galois group $G_{\mathbb{Q}}$:

$$V_f \simeq \mathbb{Q}_p^2,$$

satisfying

$$\operatorname{trace}((\mathrm{Frob}_\ell)_{|V_f}) = a_\ell(f), \quad \text{for all } \ell \not| N. \tag{23}$$

This representation is constructed by invoking proposition 1.3 to associate to f a classical eigenform $\phi \in S_2(\mathcal{H}/\Gamma_0(N))$ with the same Hecke eigenvalues as f at the good primes. The representation V_f arises in the Jacobian of $J_0(N)$ using the well-known constrction of Eichler and Shimura ([DDT], sec. 3.1).

The action of the compact group $G_{\mathbb{Q}}$ is continous for the p-adic topology on V_f and hence preserves a $\mathbb{Z}_p$-lattice T_f. Let

$$A_f = V_f/T_f \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^2 \tag{24}$$

be the divisible $G_{\mathbb{Q}}$-module attached to f, and let $A_{f,n} := A_f[p^n]$ denote the p^n-torsion submodule of A_f. It will be occasionally convenient to denote A_f by $A_{f,\infty}$. Likewise write $T_{f,n} = T_f/p^nT_f$ and set $T_{f,\infty} := T_f$. Note that for $n < \infty$, the modules $A_{f,n}$ and $T_{f,n}$ are isomorphic as $G_{\mathbb{Q}}$-modules, but the $A_{f,n}$ fit naturally into an inductive system while the $T_{f,n}$ are part of a projective system. It is therefore useful to maintain the notational distinction between the two.

The fact that f is ordinary at p implies that $A_{f,n}$ is ordinary, in the sense that it has a quotient $A_{f,n}^{(1)}$ which is free of rank one over $\mathbb{Z}/p^n\mathbb{Z}$ and on which the inertia group I_p at p acts trivially. The kernel of the natural projection $A_{f,n} \longrightarrow A_{f,n}^{(1)}$ is a free module of rank one over $\mathbb{Z}/p^n\mathbb{Z}$, denoted $A_{f,n}^{(p)}$, on which I_p acts via the the p-adic cyclotomic character

$$\epsilon : G_{\mathbb{Q}} \longrightarrow \mathbb{Z}_p^\times$$

describing the action of $G_{\mathbb{Q}}$ on the p-power roots of unity.

In our treatment of the Selmer group attached to f and K, it is convenient to make the following technical assumption on f:

Assumption 2.1 *The Galois representation $A_{f,1}$ is surjective. Furthermore, for all ℓ dividing N_0 exactly, the Galois representation $A_{f,1}$ has a unique one-dimensional subspace $A_{f,1}^{(\ell)}$ on which $\mathrm{Gal}(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$ acts via ϵ or $-\epsilon$.*

Remark: 1. Note that assumption 2.1 is automatically satisfied for ℓ if $A_{f,1}$ is ramified at ℓ, because $A_{f,n}$ arises from the Tate module of an abelian variety which acquires purely toric reduction over the quadratic unramified extension of $\mathbb{Q}_\ell$. If $A_{f,1}$ is unramified at ℓ, then the Frobenius element at ℓ acts on $A_{f,1}$ with eigenvalues ± 1 and $\pm \ell$, and the condition in assumption 2.1 stipulates that p should not divide $\ell^2 - 1$.

2. For the same reason as explained in remark 1, the maximal submodule $A_{f,n}^{(\ell)}$ on which $G_{\mathbb{Q}_\ell}$ acts via $\pm\epsilon$ is free of rank one over $\mathbb{Z}/p^n\mathbb{Z}$.

Lemma 2.2 *Suppose that E satisfies assumption 6 of the introduction. Then assumption 2.1 is satisfied by the modular form f attached to E.*

Proof: Note that in this case T_f is simply isomorphic to the Tate module of E. The assumption that p does not divide the degree of the modular parametrisation of E implies that the newform on $\Gamma_0(N_0)$ attached to E is p-isolated. By Ribet's level-lowering theorem [Ri2], it follows that the Galois representation attached to $A_{f,1}$ is ramified at all primes dividing N_0, and hence lemma 2.2 follows from remark 1 after the statement of assumption 2.1.

$\mathbb{Z}_p$-extensions. Class field theory identifies the group $\tilde{G}_\infty$ of (13) with the Galois group of the maximal abelian extension $\tilde{K}_\infty$ of K which is unramified outside of p and which is of "dihedral type" over $\mathbb{Q}$. The subfield $K_\infty := \tilde{K}_\infty^\Delta$ is called the *anticyclotomic $\mathbb{Z}_p$-extension* of K. Its Galois group over K is identified with the group $G_\infty \simeq \mathbb{Z}_p$ of equation (21). Let K_m be the m-th layer of K_∞/K, so that $\mathrm{Gal}(K_m/K) \simeq \mathbb{Z}/p^m\mathbb{Z}$.

Galois Cohomology. For each $m \in \mathbb{N}$ and $n \in \mathbb{N} \cup \{\infty\}$, let $H^1(K_m, A_{f,n})$ and $H^1(K_m, T_{f,n})$ denote the usual continuous Galois cohomology groups of $\mathrm{Gal}(\bar{K}_m/K_m)$ with values in these modules. (Note that

$$H^1(K_m, A_f) := \varinjlim_n H^1(K_m, A_{f,n}), \qquad H^1(K_m, T_f) := \varprojlim_n H^1(K_m, T_{f,n}).)$$

To study the behaviour of these groups as K_m varies over the finite layers of the anticyclotomic $\mathbb{Z}_p$-extension, it is convenient to introduce the groups

$$H^1(K_\infty, A_{f,n}) := \varinjlim_m H^1(K_m, A_{f,n}), \qquad \hat{H}^1(K_\infty, T_{f,n}) = \varprojlim_m H^1(K_m, T_{f,n}),$$

where the direct limit is taken with respect to the natural restriction maps, and the inverse limit is taken with respect to the norm (corestriction) maps. The compatible actions of the group rings $\mathbb{Z}_p[G_m]$ on the groups $H^1(K_m, A_{f,n})$ and $H^1(K_m, T_{f,n})$ yield an action of the Iwasawa algebra $\Lambda = \mathbb{Z}_p[\![G_\infty]\!]$ on both of the groups $H^1(K_\infty, A_{f,n})$ and $\hat{H}^1(K_\infty, T_{f,n})$.

Local cohomology groups. For each rational prime ℓ, set

$$K_{m,\ell} := K_m \otimes \mathbb{Q}_\ell = \oplus_{\lambda|\ell} K_{m,\lambda},$$

where the direct sum is taken over all primes λ of K_m dividing ℓ, and write for any G_{K_m}-module X:

$$H^1(K_{m,\ell}, X) := \oplus_{\lambda|\ell} H^1(K_{m,\lambda}, X).$$

Set

$$H^1(K_{\infty,\ell}, A_{f,n}) = \lim_{\overrightarrow{m}} H^1(K_{m,\ell}, A_{f,n}), \quad \hat{H}^1(K_{\infty,\ell}, T_{f,n}) = \lim_{\overleftarrow{m}} H^1(K_{m,\ell}, T_{f,n})$$

for the local counterparts of $H^1(K_\infty, A_{f,n})$ and $\hat{H}^1(K_\infty, T_{f,n})$. The Iwasawa algebra Λ acts naturally on these modules in a manner which is compatible with the restriction maps. For each rational prime ℓ, write

$$H^1(I_{m,\ell}, A_{f,n}) := \oplus_{\lambda|\ell} H^1(I_{m,\lambda}, A_{f,n}),$$

where $I_{m,\lambda}$ denotes the inertia group at λ.

Tate duality. Let ℓ be a rational prime, and let $n \in \mathbb{N} \cup \{\infty\}$. The finite Galois modules $T_{f,n} = A_{f,n}$ are isomorphic to their own Kummer duals: the Weil pairing gives rise to a canonical $G_{\mathbb{Q}}$-equivariant pairing

$$T_{f,n} \times A_{f,n} \longrightarrow \mathbb{Z}/p^n\mathbb{Z}(1) = \mu_{p^n}.$$

Combining this with the cup product pairing in cohomology gives rise to the collection of local Tate pairings at the primes above ℓ over the finite layers K_m in K_∞:

$$\langle\ ,\ \rangle_{m,\ell} : H^1(K_{m,\ell}, T_{f,n}) \times H^1(K_{m,\ell}, A_{f,n}) \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p, \tag{25}$$

which gives rise, after passing to the limit with m, to a perfect pairing

$$\langle\ ,\ \rangle_\ell : \hat{H}^1(K_{\infty,\ell}, T_{f,n}) \times H^1(K_{\infty,\ell}, A_{f,n}) \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p.$$

These pairings satisfy the rule

$$\langle \lambda\kappa, s\rangle_\ell = \langle \kappa, \lambda^* s\rangle_\ell,$$

for all $\lambda \in \Lambda$, and hence give an isomorphism of Λ-modules

$$\hat{H}^1(K_{\infty,\ell}, T_{f,n}) \longrightarrow H^1(K_{\infty,\ell}, A_{f,n})^\vee,$$

where the Pontrjagin dual $X^\vee$ of a Λ-module X is itself endowed with a Λ-module structure by the rule

$$\lambda f(x) := f(\lambda^* x), \quad \text{for all } \lambda \in \Lambda, f \in X^\vee, x \in X.$$

2.2 Finite/singular structures

Let $\ell \not| N$ be a rational prime. The *singular part* of $H^1(K_{m,\ell}, A_{f,n})$ is the group

$$H^1_{\text{sing}}(K_{m,\ell}, A_{f,n}) := H^1(I_\ell, A_{f,n})^{G_{K_\ell}}.$$

There is a natural map arising from restriction – the so-called *residue map* –

$$\partial_\ell : H^1(K_{m,\ell}, A_{f,n}) \longrightarrow H^1_{\text{sing}}(K_{m,\ell}, A_{f,n}).$$

Let $H^1_{\text{fin}}(K_{m,\ell}, A_{f,n})$ denote the kernel of ∂_ℓ. The classes in $H^1_{\text{fin}}(K_{m,\ell}, A_{f,n})$ are sometimes called the *finite* or *unramified classes*.

Of course, identical definitions can be made in which $A_{f,n}$ is replaced by $T_{f,n}$. By passing to the limit as $m \longrightarrow \infty$ (taking either a direct or an inverse limit) the definition of the residue map ∂_ℓ extends both to $H^1(K_{\infty,\ell}, A_{f,n})$ and to $\hat{H}^1(K_{\infty,\ell}, T_{f,n})$ and the groups

$$H^1_{\text{fin}}(K_{\infty,\ell}, A_{f,n}), \qquad \hat{H}^1_{\text{fin}}(K_{\infty,\ell}, T_{f,n}),$$

$$H^1_{\text{sing}}(K_{\infty,\ell}, A_{f,n}), \qquad \hat{H}^1_{\text{sing}}(K_{\infty,\ell}, T_{f,n})$$

are defined in the natural way.

Let ℓ be a prime dividing N_0 exactly. Recall in this case (in view of assumption 2.1) the distinguished line $A^{(\ell)}_{f,n}$ consisting of elements on which $G_{\mathbb{Q}_\ell}$ acts via $\pm\epsilon$. The *ordinary part* of $H^1(K_{\infty,\ell}, A_{f,n})$ is defined to be the group

$$H^1_{\text{ord}}(K_{\infty,\ell}, A_{f,n}) := H^1(K_{\infty,\ell}, A^{(\ell)}_{f,n}).$$

Finally, at the prime p, set

$$H^1_{\text{ord}}(K_{\infty,p}, A_{f,n}) := \text{res}_p^{-1}\left(H^1(I_{\infty,p}, A^{(p)}_{f,n})\right),$$

where $\text{res}_p : H^1(K_{\infty,p}, A_{f,n}) \longrightarrow H^1(I_{\infty,p}, A_{f,n})$ is induced from the restriction maps at the (finitely many) primes of K_∞/K above p.

Proposition 2.3 *If ℓ is a prime not dividing N, the groups $H^1_{\text{fin}}(K_{\infty,\ell}, A_{f,n})$ and $\hat{H}^1_{\text{fin}}(K_{\infty,\ell}, T_{f,n})$ are annihilators of each other under the local Tate pairing $\langle\ ,\ \rangle_\ell$. The same is true of $H^1_{\text{ord}}(K_{\infty,\ell}, A_{f,n})$ and $\hat{H}^1_{\text{ord}}(K_{\infty,\ell}, T_{f,n})$ for $\ell \| N$. In particular, $H^1_{\text{fin}}(K_{\infty,\ell}, A_{f,n})$ and $\hat{H}^1_{\text{sing}}(K_{\infty,\ell}, T_{f,n})$ are the Pontryagin duals of each other.*

Proof: The result over the finite layers K_m follows from standard properties of the local Tate pairing, and is then deduced over K_∞ by passage to the limit.

Proposition 2.3 yields a perfect pairing of Λ-modules (denoted by the same symbols $\langle\ ,\ \rangle_\ell$ by abuse of notation)

$$\langle\ ,\ \rangle_\ell : \hat{H}^1_{\mathrm{sing}}(K_{\infty,\ell}, T_{f,n}) \times H^1_{\mathrm{fin}}(K_{\infty,\ell}, A_{f,n}) \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p.$$

The following lemma makes explicit the structure of the local cohomology groups $\hat{H}^1(K_{\infty,\ell}, T_{f,n})$ and $H^1(K_{\infty,\ell}, A_{f,n})$.

Lemma 2.4 *Suppose that ℓ is a rational prime which does not divide N. If ℓ is split in $K/\mathbb{Q}$, then*

$$\hat{H}^1_{\mathrm{sing}}(K_{\infty,\ell}, T_{f,n}) = 0, \quad H^1_{\mathrm{fin}}(K_{\infty,\ell}, A_{f,n}) = 0.$$

Proof: Because $(\ell) = \lambda_1\lambda_2$ is split in $K/\mathbb{Q}$, the frobenius element attached to λ_1 topologically generates a subgroup of finite index in G_∞. Hence $K_{\infty,\ell}$ is isomorphic to a direct sum of a finite number of copies of the unramified $\mathbb{Z}_p$-extension of $\mathbb{Q}_\ell$. Since $A_{f,n}$ is of exponent p^n, any unramified cohomology class in $H^1(K_{m,\ell}, A_{f,n})$ becomes trivial after restriction to $H^1(K_{m',\ell}, A_{f,n})$ for m' sufficiently large. This implies the second assertion; the first follows from the non-degeneracy of the local Tate pairing.

The primes ℓ which are inert in $K/\mathbb{Q}$ exhibit a markedly different behaviour, because they split completely in the anticyclotomic tower. It is the presence of such primes which accounts for some of the essential differences between the anticyclotomic theory and the more familiar Iwasawa theory of the cyclotomic $\mathbb{Z}_p$-extension.

Lemma 2.5 *If ℓ does not divide N and is inert in $K/\mathbb{Q}$, then*

$$\hat{H}^1_{\mathrm{sing}}(K_{\infty,\ell}, T_{f,n}) \simeq H^1_{\mathrm{sing}}(K_\ell, T_{f,n}) \otimes \Lambda,$$

and

$$H^1_{\mathrm{fin}}(K_{\infty,\ell}, A_{f,n}) \simeq \mathrm{Hom}(H^1_{\mathrm{sing}}(K_\ell, T_{f,n}) \otimes \Lambda, \mathbb{Q}_p/\mathbb{Z}_p).$$

Proof: Since ℓ is inert in K and $K_\infty/\mathbb{Q}$ is an extension of dihedral type, the frobenius element at ℓ in $\mathrm{Gal}(K_\infty/\mathbb{Q})$ is of order two and hence ℓ splits completely in K_∞/K. The choice of a prime λ_m of K_m above ℓ thus determines an isomorphism $H^1(K_{m,\ell}, T_{f,n}) \longrightarrow H^1(K_\ell, T_{f,n}) \otimes \mathbb{Z}_p[G_m]$. Choosing a compatible sequence of primes λ_m of K_m which lie above each other, one obtains an isomorphism

$$\hat{H}^1(K_{\infty,\ell}, T_{f,n}) \simeq H^1(K_\ell, T_{f,n}) \otimes \Lambda,$$

from the definition of the completed group ring Λ. The first isomorphism of the lemma now follows by passing to the singular parts of the cohomology, while the second is a consequence of proposition 2.3.

Admissible primes. A rational prime ℓ is said to be *n-admissible* relative to f if it satisfies the following conditions:

1. ℓ does not divide $N = pN^+N^-$;
2. ℓ is inert in $K/\mathbb{Q}$;
3. p does not divide $\ell^2 - 1$;
4. p^n divides $\ell + 1 - a_\ell$ or $\ell + 1 + a_\ell$.

A 1-admissible prime will simply be called *admissible* (so that in particular any n-admissible prime is admissible).

Note that if ℓ is n-admissible, the module $T_{f,n}$ is unramified at ℓ and the Frobenius element over $\mathbb{Q}$ at ℓ acts semisimply on this module with eigenvalues $\pm\ell$ and ± 1 which are distinct modulo p. From this a direct calculation shows that:

Lemma 2.6 *The local cohomology groups $H^1_{\mathrm{sing}}(K_\ell, T_{f,n})$ and $H^1_{\mathrm{fin}}(K_\ell, T_{f,n})$ are both isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$.*

Proof: The group $H^1_{\mathrm{sing}}(K_\ell, T_{f,n})$ is identified with $H^1(I_\ell, T_{f,n})^{G_{K_\ell}}$. Since $T_{f,n}$ is unramified at ℓ, this first cohomology group is identified with a group of homomorphisms, which necessarily factor through the tame inertia group at ℓ. The Frobenius element over K at (ℓ) acts on this tame inertia group as multiplication by ℓ^2, while it acts on $T_{f,n}$ with eigenvalues ℓ^2 and 1. The result follows from this, in light of the fact that p does not divide $\ell^2 - 1$. Similarly, the group $H^1_{\mathrm{fin}}(K_\ell, A_{f,n})$ is identified with the G_{K_ℓ}-coinvariants of $A_{f,n}$ which are also isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$.

Lemma 2.7 *The local groups $\hat{H}^1_{\mathrm{sing}}(K_{\infty,\ell}, T_{f,n})$ and $\hat{H}^1_{\mathrm{fin}}(K_{\infty,\ell}, T_{f,n})$ are each free of rank one over $\Lambda/p^n\Lambda$.*

Proof: Since ℓ is inert in $K/\mathbb{Q}$, lemma 2.5 implies that $\hat{H}^1(K_{\ell,\infty}, T_{f,n})$ is isomorphic to $H^1(K_\ell, T_{f,n}) \otimes \Lambda$. The result now follows from lemma 2.6.

Remark:
1. Note that the n-admissible primes are not the primes appearing in Kolyvagin's study of the Selmer groups of elliptic curves, where the condition that p^n divides $\ell + 1$ was imposed.

2. The notion of admissible prime introduced here is similar to the one introduced in [BD0], def. 2.20, the main difference arising from the fact that the local cohomology groups $H^1_{\mathrm{fin}}(K_\ell, A_{f,n})$ and $H^1_{\mathrm{sing}}(K_\ell, T_{f,n})$ are both free of rank one (and not two) over $\mathbb{Z}/p^n\mathbb{Z}$.

2.3 Definition of the Selmer group

Let ℓ be a prime not dividing N. Composing restriction from K_∞ to $K_{\infty,\ell}$ with ∂_ℓ yields residue maps on the global cohomology groups, still denoted ∂_ℓ by an abuse of notation,

$$\partial_\ell \;:\; H^1(K_\infty, A_{f,n}) \to H^1_{\mathrm{sing}}(K_{\infty,\ell}, A_{f,n}), \tag{26}$$

$$\partial_\ell \;:\; \hat{H}^1(K_\infty, T_{f,n}) \to \hat{H}^1_{\mathrm{sing}}(K_{\infty,\ell}, T_{f,n}). \tag{27}$$

Note that if ℓ is split in $K/\mathbb{Q}$, the residue map of (27) is 0 by lemma 2.4.

If $\partial_\ell(\kappa) = 0$ for $\kappa \in H^1(K_\infty, A_{f,n})$ (resp. $\hat{H}^1(K_\infty, T_{f,n})$), let

$$v_\ell(\kappa) \in H^1_{\mathrm{fin}}(K_{\infty,\ell}, A_{f,n}) \quad (\text{resp. } \hat{H}^1_{\mathrm{fin}}(K_{\infty,\ell}, T_{f,n}))$$

denote the natural image of κ under the restriction map at ℓ.

Definition 2.8 *The* Selmer group $\mathrm{Sel}_{f,n}$ *attached to f, n and K_∞ is the group of elements s in $H^1(K_\infty, A_{f,n})$ satisfying*

1. *$\partial_\ell(s) = 0$ for all rational primes ℓ not dividing N.*
2. *The class s is ordinary at the primes $\ell | N^- p$.*
3. *The class s is trivial at the primes $\ell | N^+$.*

Caveat: Note that the group $\mathrm{Sel}_{f,n}$ depends on the value of N, hence on the modular form f itself, and not just on the Galois representation $A_{f,n}$ attached to it. The same remark holds for the *compactified Selmer group* $\hat{H}^1_S(K_\infty, T_{f,n})$ defined below:

Definition 2.9 *Let S be a square-free integer which is relatively prime to N. The* compactified Selmer group $\hat{H}^1_S(K_\infty, T_{f,n})$ *attached to f, S and K_∞ is the group of elements κ in $\hat{H}^1(K_\infty, T_{f,n})$ satisfying*

1. *$\partial_\ell(\kappa) = 0$ for all rational primes ℓ not dividing SN;*
2. *The class κ is ordinary at the primes $\ell | N^- p$.*
3. *The class κ is arbitrary at the primes ℓ dividing N^+, and at the primes dividing S.*

Global reciprocity. Let $\kappa \in \hat{H}^1(K_\infty, T_{f,n})$ and let $s \in H^1(K_\infty, A_{f,n})$ be global cohomology classes. For each rational prime q, let κ_q and s_q denote the restrictions of these cohomology classes to the (semi-)local cohomology group attached to the prime q. The global reciprocity law of class field theory implies that

$$\sum_q \langle \kappa_q, s_q \rangle_q = 0, \tag{28}$$

where the sum is taken over all the rational primes. In particular, if κ belongs to $\hat{H}^1_S(K_\infty, T_{f,n})$ and s belongs to $\mathrm{Sel}_{f,n}$, then since the local conditions defining these two groups are orthogonal at the primes not dividing S, and since s has trivial residue at the primes dividing S, formula (28) becomes:

$$\sum_{q|S} \langle \partial_q(\kappa), v_q(s) \rangle_q = 0.$$

Of particular interest is the following special case:

Proposition 2.10 *Suppose that κ belongs to $\hat{H}^1_\ell(K_\infty, A_{f,n})$. Then*

$$\langle \partial_\ell(\kappa), v_\ell(s) \rangle_\ell = 0,$$

for all $s \in \mathrm{Sel}_{f,n}$.

The strategy of the proof of theorem 1 is to produce, for sufficiently many primes ℓ that are inert in K, cohomology classes $\kappa(\ell) \in \hat{H}^1_\ell(K_\infty, A_{f,n})$ whose residue $\partial_\ell(\kappa(\ell))$ can be related to the p-adic L-function $L_p(f, K)$ constructed in section 1. Thanks to proposition 2.10, the elements $\partial_\ell(\kappa(\ell))$ yield relations in a presentation for $\mathrm{Sel}_{f,n}^\vee$.

3 Some Preliminaries

3.1 Λ-modules

If X is any module over a ring R, let $\mathrm{Fitt}_R(X)$ denote the Fitting ideal of X over R. If $R = \Lambda$ and X is finitely generated, let $\mathrm{Char}(X)$ denote the characteristic ideal attached to X.

Proposition 3.1 *Let X be a finitely generated Λ-module and let $\mathcal{L}$ be an element of Λ. Suppose that $\varphi(\mathcal{L})$ belongs to $\mathrm{Fitt}_{\mathcal{O}}(X \otimes_\varphi \mathcal{O})$, for all homomorphisms $\varphi : \Lambda \longrightarrow \mathcal{O}$, where $\mathcal{O}$ is a discrete valuation ring. Then $\mathcal{L}$ belongs to $\mathrm{Char}(X)$.*

Proof: If X is not Λ-torsion, then $\mathrm{Fitt}_\Lambda(X) = 0$. Since

$$\mathrm{Fitt}_{\mathcal{O}}(X \otimes_\varphi \mathcal{O}) = \varphi(\mathrm{Fitt}_\Lambda(X)),$$

it follows that $\varphi(\mathcal{L}) = 0$ for all φ. This implies (by the Weierstrass preparation theorem, for example) that $\mathcal{L} = 0$. Hence one may assume without loss of generality that X is a Λ-torsion module. In that case the structure theory of Λ-modules ensures the existence of an exact sequence of Λ-modules:

$$X \xrightarrow{j} \oplus_i \Lambda/(g_i) \longrightarrow C \longrightarrow 0, \tag{29}$$

where C and $\ker j$ are finite Λ-modules and the g_i are non-zero distinguished polynomials or powers of p. By definition, $g := \prod_i g_i$ is a generator of $\mathrm{Char}(X)$. Since C is finite, its Λ-Fitting ideal can be generated by two elements ι_1 and ι_2 having no common irreducible factors. By tensoring the exact sequence (29) with $\mathcal{O}$ one finds that

$$\varphi(\iota_i)\mathrm{Fitt}_{\mathcal{O}}(X \otimes_\varphi \mathcal{O}) \subset (\varphi(g)), \quad \text{for } i = 1, 2.$$

It follows by assumption that $\varphi(g)$ divides $\varphi(\iota_i\mathcal{L})$ for all φ. Hence (as can be seen by using the Weierstrass preparation theorem) g divides $\iota_i\mathcal{L}$ for $i = 1, 2$, and therefore g divides $\mathcal{L}$.

3.2 Controlling the Selmer group

Suppose now that $A_{f,1}$ satisfies the irreducibility condition 2 of assumption 6.

Theorem 3.2 *Let s be a non-zero element of $H^1(K, A_{f,1})$. There exist infinitely many n-admissible primes ℓ relative to f such that $\partial_\ell(s) = 0$ and $v_\ell(s) \neq 0$.*

Proof: Let $\mathbb{Q}(A_{f,n})$ be the extension of $\mathbb{Q}$ fixed by the kernel of the Galois representation $A_{f,n}$. It is unramified at the primes not dividing N. Since the discriminant of K is assumed to be prime to N, the fields $\mathbb{Q}(A_{f,n})$ and K are linearly disjoint. Letting M denote the compositum of these fields, there is therefore a natural inclusion

$$\mathrm{Gal}(M/\mathbb{Q}) = \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(A_{f,n})/\mathbb{Q}) \subset \{1, \tau\} \times \mathrm{Aut}_{\mathbb{Z}/p^n\mathbb{Z}}(A_{f,n}),$$

so that elements of $\mathrm{Gal}(M/\mathbb{Q})$ can be labelled by certain pairs (τ^j, T) with $j \in \{0, 1\}$ and $T \in \mathrm{Aut}_{\mathbb{Z}/p^n\mathbb{Z}}(A_{f,n})$. Let M_s be the extension of M cut out by the image $\bar{s}$ of s under restriction to $H^1(M, A_{f,1}) = \mathrm{Hom}(\mathrm{Gal}(\bar{M}/M), A_{f,1})$. Assume without loss of generality that s belongs to a specific eigenspace for the action of τ, so that

$$\tau s = \delta s, \text{ for some } \delta \in \{1, -1\}.$$

Under this assumption, the extension M_s is Galois over $\mathbb{Q}$, not merely over K. In fact, by the assumption that $A_{f,1}$ is an irreducible $G_{\mathbb{Q}}$-module, $\mathrm{Gal}(M_s/\mathbb{Q})$ is identified with the semi-direct product

$$\mathrm{Gal}(M_s/\mathbb{Q}) = A_{f,1} \rtimes \mathrm{Gal}(M/\mathbb{Q}), \tag{30}$$

where the quotient $\mathrm{Gal}(M/\mathbb{Q})$ acts on the abelian normal subgroup $A_{f,1}$ of $\mathrm{Gal}(M_s/\mathbb{Q})$ by the rule

$$(\tau^j, T)(v) = \delta^j \bar{T} v. \tag{31}$$

Here $\bar{T}$ denotes the natural image of T in $\mathrm{Aut}_{\mathbb{F}_p}(A_{f,1})$. By part 2 of assumption 6 on the Galois representation $A_{f,1}$, the group $\mathrm{Gal}(M_s/\mathbb{Q})$ contains an element of the form (v, τ, T), where

1. The automorphism T has eigenvalues δ and λ, where $\lambda \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ is not equal to $\pm 1 \bmod p$ and has order prime to p. (Note that here the assumption that $p > 3$ is needed.)

2. The vector $v \in A_{f,1}$ is non-zero and belongs to the δ-eigenspace for $\bar{T}$.

Let $\ell \not| N$ be a rational prime which is unramified in $M_s/\mathbb{Q}$ and satisfies

$$\mathrm{Frob}_\ell(M_s/\mathbb{Q}) = (v, \tau, T). \tag{32}$$

By the Chebotarev density theorem, there exist infinitely many such primes. In fact, the set of such primes has positive density. The fact, immediate from (32), that $\mathrm{Frob}_\ell(M/\mathbb{Q}) = (\tau, T)$ implies that ℓ is an admissible prime. To see that $v_\ell(s) \neq 0$, choose a prime λ of M above ℓ, and let d be the (necessarily even) degree of the corresponding residue field extension. Then

$$\mathrm{Frob}_\lambda(M_s/M) = (v, \tau, T)^d = v + \delta\bar{T}v + \bar{T}^2 v + \cdots + \delta\bar{T}^{d-1}v = dv.$$

Let $\bar{s}$ denote the image of s in

$$H^1(M, A_{f,1}) = \mathrm{Hom}(\mathrm{Gal}(\bar{M}/M), A_{f,1})$$

under restriction. Since d is prime to p by property 1 of T, it follows that $\bar{s}(\mathrm{Frob}_\lambda(M_s/M)) = d\bar{s}(v) \neq 0$, so that the restriction at λ of $\bar{s}$ is non-zero. Hence, so is $v_\ell(s)$, a fortiori.

Global cohomology groups. Following [BD0], definition 2.22, a finite set S of primes is said to be *n-admissible* relative to f if

1. All $\ell \in S$ are n-admissible relative to f.

2. The map $\mathrm{Sel}(K, A_{f,n}) \longrightarrow \oplus_{\ell \in S} H^1_{\mathrm{fin}}(K_\ell, A_{f,n})$ is injective.

A direct argument based on theorem 3.2 shows that n-admissible sets exist. (See also the proof of lemma 2.23 of [BD0].) In fact, any finite collection of n-admissible primes can be enlarged to an n-admissible set.

Proposition 3.3 *If S is an n-admissible set, then the group $\hat{H}^1_S(K_\infty, T_{f,n})$ is free of rank $\#S$ over $\Lambda/p^n\Lambda$.*

Proof: The fact that $H^1_S(K_m, T_{f,n})$ is free over $\mathbb{Z}/p^n\mathbb{Z}[G_m]$ is essentially theorem 3.2 of [BD0], whose proof carries over, mutatis mutandis, to the present context with its slightly modified notion of admissible prime. Proposition 3.3 follows by passing to the limit as $m \longrightarrow \infty$.

Theorem 3.4 *Let $\mathfrak{m}_\Lambda$ denote the maximal ideal of Λ. Then*

1. *The natural map from $H^1(K, A_{f,1}) \to H^1(K_\infty, A_{f,n})[\mathfrak{m}_\Lambda]$ induced by restriction is an isomorphism.*
2. *If S is an n-admissible set, the natural map from $\hat{H}^1_S(K_\infty, T_{f,n})/\mathfrak{m}_\Lambda$ to $H^1(K, T_{f,1})$ induced by corestriction is injective.*

Proof: Let I_Λ denote the augmentation ideal of Λ. The inflation-restriction sequence from K to K_m gives the exact sequence

$$\begin{aligned} H^1(K_m/K, A_{f,n}^{G_{K_m}}) &\longrightarrow H^1(K, A_{f,n}) \xrightarrow{j} H^1(K_m, A_{f,n})[I_\Lambda] \longrightarrow \\ &\longrightarrow H^2(K_m/K, A_{f,n}^{G_{K_m}}). \end{aligned}$$

By part 2 of assumption 6 in the introduction, the module $A_{f,n}^{G_{K_m}}$ is trivial. (Otherwise, the Galois representation attached to $A_{f,n}$ would have solvable image, contradicting the hypotheses that were made in the introduction.) Hence the map j is an isomorphism. Taking the G_K-cohomology of the exact sequence

$$0 \longrightarrow A_{f,1} \longrightarrow A_{f,n} \xrightarrow{p} A_{f,n-1} \longrightarrow 0$$

and using the fact that $A_{f,1}^{G_K} = 0$ once again, shows that the natural map

$$H^1(K, A_{f,1}) \longrightarrow H^1(K, A_{f,n})[p] \tag{33}$$

is an isomorphism. It follows that the natural map

$$H^1(K, A_{f,1}) \longrightarrow H^1(K_m, A_{f,n})[\mathfrak{m}_\Lambda]$$

is an isomorphism as well. Part 1 of theorem 3.4 follows by taking the direct limit as $m \longrightarrow \infty$.

Part 2 of theorem 3.4 follows directly from proposition 3.3.

3.3 Rigid pairs

Let $W_f := \mathrm{ad}_0(A_{f,1}) = \mathrm{Hom}_0(A_{f,1}, A_{f,1})$ be the adjoint representation attached to $A_{f,1}$, i.e., the vector space of trace zero endomorphisms of $A_{f,1}$. It is a three-dimensional $\mathbb{F}_p$-vector space endowed with a natural action of $G_{\mathbb{Q}}$

arising from the conjugation of endomorphisms. Write $W_f^* := \mathrm{Hom}(W_f, \mu_p)$ for the Kummer dual of W_f.

Recall that $A_{f,1}$ is ordinary at p, so that there is an exact sequence of I_p-modules

$$0 \longrightarrow A_{f,1}^{(p)} \longrightarrow A_{f,1} \longrightarrow A_{f,1}^{(1)} \longrightarrow 0$$

where $A_{f,1}^{(p)}$ represents the subspace on which I_p acts via the cyclotomic character ϵ, and $A_{f,1}^{(1)}$ represents the I_p-coinvariants of $A_{f,1}$. Let

$$W_f^{(p)} := \mathrm{Hom}(A_{f,1}^{(1)}, A_{f,1}^{(p)}).$$

It is an I_p-submodule of W_f; let $W_f^{(1)} := W_f/W_f^{(p)}$. The classes in $H^1(\mathbb{Q}_p, W_f)$ whose restriction at p belong to $H^1(I_p, W_f^{(p)})$ are called *ordinary* at p.

Likewise, if ℓ is a prime which divides N exactly, recall the submodules $A_{f,1}^{(\ell)}$ and $A_{f,1}^{(1)}$ on which $G_{\mathbb{Q}_\ell}$ acts by $\pm\epsilon$ and ± 1 respectively. (These submodules are well-defined, by virtue of assumption 2.1.) Set

$$W_f^{(\ell)} := \mathrm{Hom}(A_{f,1}^{(1)}, A_{f,1}^{(\ell)}).$$

The classes in $H^1(\mathbb{Q}, W_f)$ whose restriction at ℓ belongs to $H^1(\mathbb{Q}_\ell, W_f^{(\ell)})$ are called *ordinary* at ℓ.

If ℓ is an admissible prime for f, the eigenvalues of Frob_ℓ acting on the Galois representation $A_{f,1}$ are ± 1 and $\pm\ell$. Recall also that $\ell^2 \neq 1$ belongs to $\mathbb{F}_p^\times$. Therefore, the eigenvalues of Frob_ℓ acting on W_f (resp. W_f^*) are the distinct elements 1, ℓ, and ℓ^{-1} (resp. ℓ, 1 and ℓ^2) of $\mathbb{F}_p^\times$. Let $W_f^{(\ell)}$ and $W_f^{*(\ell)}$ denote the one-dimensional $\mathbb{F}_p$-subspace on which Frob_ℓ acts with eigenvalue ℓ. The classes in $H^1(\mathbb{Q}, W_f)$ whose restriction at ℓ belong to $H^1(\mathbb{Q}_\ell, W_f^{(\ell)})$ are called *ordinary* at ℓ. (In [Ram], section 3, these classes are referred to as *null cocycles.*) Note that $H^1(\mathbb{Q}_\ell, W_f)$ decomposes as a direct sum of two one-dimensional $\mathbb{F}_p$-subspaces,

$$H^1(\mathbb{Q}_\ell, W_f) = H^1_{\mathrm{fin}}(\mathbb{Q}_\ell, W_f) \oplus H^1_{\mathrm{ord}}(\mathbb{Q}_\ell, W_f^{(\ell)}),$$

where

$$H^1_{\mathrm{fin}}(\mathbb{Q}_\ell, W_f) := H^1(\mathbb{Q}_\ell^{nr}/\mathbb{Q}_\ell, W_f)$$

is the space of unramified cocycles. A similar remark holds for W_f^*.

Let S be a square-free product of admissible primes for f.

Definition 3.5 *The* S-Selmer group *attached to* W_f*, denoted* $\mathrm{Sel}_S(\mathbb{Q}, W_f)$*, is the subspace of cohomology classes* $\xi \in H^1(\mathbb{Q}, W_f)$ *satisfying*

1. *For all* ℓ *which do not divide* NS*, the image of* ξ *in* $H^1(\mathbb{Q}_\ell, W_f)$ *belongs to* $H^1_{\mathrm{fin}}(\mathbb{Q}_\ell, W_f)$*.*

2. *The class* ξ *is ordinary at the primes* ℓ *dividing* NS *exactly.*

3. *The class* ξ *belongs to the kernel of the restriction to* $H^1(I_\ell, W_f)$ *if* ℓ *is a prime such that* ℓ^2 *divides* N^+*.*

Similar definitions can be made for $\mathrm{Sel}_S(\mathbb{Q}, W_f^*)$. Note that $H^1(\mathbb{Q}_\ell, W_f^{(\ell)})$ and $H^1(\mathbb{Q}_\ell, W_f^{*(\ell)})$ are orthogonal to each other under the local Tate pairing.

Proposition 3.6 *The modular form* f *is* p*-isolated if and only if* $\mathrm{Sel}_1(\mathbb{Q}, W_f)$ *is trivial.*

Proof: Let R denote the universal ring attached to deformations ρ of the Galois representation $A_{f,1}$, satisfying

1. The determinant of ρ is the cyclotomic character describing the action of $G_{\mathbb{Q}}$ on the p-power roots of unity.

2. ρ is unramified outside NS.

3. ρ is ordinary at p, i.e., the restriction of ρ to I_p is of the form $\begin{pmatrix} \epsilon & * \\ 0 & 1 \end{pmatrix}$.

4. For all ℓ dividing N^+N^-S exactly, the restriction of ρ to a decomposition group at ℓ is ordinary, i.e., is of the form $\begin{pmatrix} \epsilon & * \\ 0 & 1 \end{pmatrix}$.

The ring R is a complete local Noetherian $\mathbb{Z}_p$-algebra with residue field $\mathbb{F}_p$. Let $\mathfrak{m}$ denote the maximal ideal of R. Standard results of deformation theory (cf. lemma 2.39 and secs. 2.6 and 2.7 of [DDT],) identify $\mathfrak{m}/(p, \mathfrak{m}^2)$ with the Pontryagin dual of $\mathrm{Sel}_S(\mathbb{Q}, W_f)$. It follows that $R = \mathbb{Z}_p$ if and only if $\mathrm{Sel}_S(\mathbb{Q}, W_f)$ is trivial. Taking $S = 1$, a calculation as in [W], sec. 3 shows that the ring R surjects onto the ring $\mathbb{T}_f$ of Hecke operators acting on the space $S_2(\mathcal{T}/\Gamma)$, completed at the maximal ideal attached to f. A deep result of Wiles ([W], [DDT] theorem 3.42) asserts that this surjection is an isomorphism. Hence the fact that $R = \mathbb{Z}_p$ is equivalent to the fact that $\mathbb{T}_f = \mathbb{Z}_p$, which in turn is equivalent to the fact that the modular form f is p-isolated.

If S is a square-free product of admissible primes for $A_{f,1}$, let $\mathrm{Sel}_{(S)}(\mathbb{Q}, W_f)$ denote the Selmer group defined in the same way as $\mathrm{Sel}_S(\mathbb{Q}, W_f)$ above, but with no condition imposed at the primes of S. Let $\mathrm{Sel}_{[S]}(\mathbb{Q}, W_f)$ denote the subgroup of $\mathrm{Sel}_S(\mathbb{Q}, W_f)$ consisting of classes that are trivial at the primes in S. These notations can be combined: thus, if S_1, S_2, S_3 are pairwise coprime square-free products of admissible primes, the group $\mathrm{Sel}_{S_1(S_2)[S_3]}(\mathbb{Q}, W_f)$ is given the obvious meaning. Similar definitions can be made with W_f replaced by W_f^*. Note that the Selmer groups $\mathrm{Sel}_{(S)}(\mathbb{Q}, W_f)$ and $\mathrm{Sel}_{[S]}(\mathbb{Q}, W_f^*)$ are dual Selmer groups in the sense of [DDT], section 2.3, and the same is true of $\mathrm{Sel}_S(\mathbb{Q}, W_f)$ and $\mathrm{Sel}_S(\mathbb{Q}, W_f^*)$.

Proposition 3.7 *If f is p-isolated, and ℓ is an admissible prime for f, then $\mathrm{Sel}_{(\ell)}(\mathbb{Q}, W_f)$ and $\mathrm{Sel}_{(\ell)}(\mathbb{Q}, W_f^*)$ are one-dimensional $\mathbb{F}_p$-vector spaces.*

Proof: It follows from a direct calculation of orders of local cohomology groups, combined with theorem 2.18 of [DDT], that the groups $\mathrm{Sel}_1(\mathbb{Q}, W_f)$ and $\mathrm{Sel}_1(\mathbb{Q}, W_f^*)$ have the same cardinality. By proposition 3.6, both these groups are trivial. Applying theorem 2.18 of [DDT] once more, and using the fact that p divides $(\ell+1)^2 - a_\ell^2$, one finds that

$$\#\mathrm{Sel}_{(\ell)}(\mathbb{Q}, W_f)/\#\mathrm{Sel}_{[\ell]}(\mathbb{Q}, W_f^*) = p.$$

Hence $\mathrm{Sel}_{(\ell)}(\mathbb{Q}, W_f)$ is one-dimensional over $\mathbb{F}_p$. The same argument, with W_f and W_f^* interchanged, shows that $\mathrm{Sel}_{(\ell)}(\mathbb{Q}, W_f^*)$ is one-dimensional as well.

Suppose that f is p-isolated so that the conclusion of proposition 3.7 holds. If $\ell \neq \ell_1$ is any admissible prime, write

$$v_\ell : \mathrm{Sel}_{(\ell_1)}(\mathbb{Q}, W_f) \longrightarrow H^1_{\mathrm{fin}}(\mathbb{Q}_\ell, W_f), \quad v_\ell^* : \mathrm{Sel}_{(\ell_1)}(\mathbb{Q}, W_f^*) \longrightarrow H^1_{\mathrm{fin}}(\mathbb{Q}_\ell, W_f^*)$$

for the natural maps induced from restriction at ℓ.

Proposition 3.8 *1. If $\mathrm{Sel}_{\ell_1}(\mathbb{Q}, W_f) \neq 0$, and v_{ℓ_2} and $v_{\ell_2}^*$ are both non-zero, then $\mathrm{Sel}_{\ell_1\ell_2}(\mathbb{Q}, W_f) = 0$.*

2. *If* $\mathrm{Sel}_{\ell_1}(\mathbb{Q}, W_f) = 0$*, and* v_{ℓ_2} *is* 0*, then either* $\mathrm{Sel}_{\ell_1\ell_2}(\mathbb{Q}, W_f) = 0$ *or* $\mathrm{Sel}_{\ell_2}(\mathbb{Q}, W_f)$ *is one-dimensional.*

Proof: 1. Since ℓ_1 is admissible, we may invoke proposition 3.7 and let ξ_1 and ξ_1^* be generators of $\mathrm{Sel}_{(\ell_1)}(\mathbb{Q}, W_f)$ and $\mathrm{Sel}_{(\ell_1)}(\mathbb{Q}, W_f^*)$ respectively. Note that ξ_1 belongs to $\mathrm{Sel}_{\ell_1}(\mathbb{Q}, W_f)$ (ie., the restiction of ξ_1 at ℓ_1 is ordinary) since $\mathrm{Sel}_{\ell_1}(\mathbb{Q}, W_f) \neq 0$. A calculation using theorem 2.18 of [DDT] shows that $\mathrm{Sel}_{\ell_1}(\mathbb{Q}, W_f)$ and $\mathrm{Sel}_{\ell_1}(\mathbb{Q}, W_f^*)$ have the same dimension, and hence ξ_1^* also belongs to $H^1_{\ell_1}(\mathbb{Q}, W_f^*)$.

By theorem 2.18 of [DDT],

$$\#\mathrm{Sel}_{\ell_1(\ell_2)}(\mathbb{Q}, W_f)/\#\mathrm{Sel}_{\ell_1[\ell_2]}(\mathbb{Q}, W_f^*) = p.$$

The assumption that $v_{\ell_2}(\xi_1^*) \neq 0$ implies that $\#\mathrm{Sel}_{\ell_1[\ell_2]}(\mathbb{Q}, W_f^*) = 0$. Hence $\mathrm{Sel}_{\ell_1(\ell_2)}(\mathbb{Q}, W_f) = \mathrm{Sel}_{\ell_1}(\mathbb{Q}, W_f)$ is one-dimensional and spanned by ξ_1. Now the assumption that $v_{\ell_2}(\xi_1) \neq 0$ shows that $\mathrm{Sel}_{\ell_1\ell_2}(\mathbb{Q}, W_f) = 0$.

2. It is convenient to distinguish two cases:
a) If $\mathrm{Sel}_{\ell_2}(\mathbb{Q}, W_f) = 0$, then the space $\mathrm{Sel}_{(\ell_1)\ell_2}$ is one-dimensional by theorem 2.18 of [DDT]. The assumption that $v_{\ell_2}(\xi_1) = 0$ shows that in fact ξ_1 generates $\mathrm{Sel}_{(\ell_1)\ell_2}(\mathbb{Q}, W_f)$. But ξ_1 does not belong to $\mathrm{Sel}_{\ell_1(\ell_2)}(\mathbb{Q}, W_f)$ since if it did it would also belong to $\mathrm{Sel}_{\ell_1}(\mathbb{Q}, W_f)$ which is trivial by assumption. Hence

$$\mathrm{Sel}_{\ell_1\ell_2}(\mathbb{Q}, W_f) = \mathrm{Sel}_{(\ell_1)\ell_2}(\mathbb{Q}, W_f) \cap \mathrm{Sel}_{\ell_1(\ell_2)}(\mathbb{Q}, W_f) = 0.$$

b) If $\mathrm{Sel}_{\ell_2}(\mathbb{Q}, W_f) \neq 0$, it is necessarily one-dimensional since it lies in the one-dimensional space $\mathrm{Sel}_{(\ell_2)}(\mathbb{Q}, W_f)$.

Definition 3.9 *A pair* (ℓ_1, ℓ_2) *of admissible primes is said to be a* rigid pair *if the Selmer group* $\mathrm{Sel}_{\ell_1\ell_2}(\mathbb{Q}, W_f)$ *is trivial.*

In addition to theorem 3.2 guaranteeing the existence of a plentiful supply of n-admissible primes sufficient to control the Selmer group $\mathrm{Sel}_{f,n}$, there arises the need for the somewhat more technical theorems 3.10 and 3.11 below guaranteeing the existence of a large supply of rigid pairs of n-admissible primes in certain favorable circumstances.

Theorem 3.10 *Suppose that* f *is a* p*-isolated eigenform in* $S_2(\mathcal{T}/\Gamma)$*, and let* ℓ_1 *be an admissible prime for* f*. Let* s *be a non-zero class in* $H^1(K, A_{f,1})$*. For any* n*, there exist infinitely many* n*-admissible primes* ℓ_2 *such that*

1. $\partial_{\ell_2}(s) = 0$ *and* $v_{\ell_2}(s) \neq 0$.

2. Either (ℓ_1, ℓ_2) *is a rigid pair, or* $\mathrm{Sel}_{\ell_2}(\mathbb{Q}, W_f)$ *is one-dimensional.*

Proof: Assume as in the proof of theorem 3.2 that s belongs to a fixed eigenspace for complex conjugation, so that $\tau s = \delta s$ for some $\delta \in \{1, -1\}$. Write $M = K(A_{f,n})$ and let M_s be the Galois extension of M cut out by s as in the proof of theorem 3.2.

The fact that f is p-isolated implies, by proposition 3.7, that the Selmer groups $\mathrm{Sel}_{(\ell_1)}(\mathbb{Q}, W_f)$ and $\mathrm{Sel}_{(\ell_1)}(\mathbb{Q}, W_f^*)$ are one-dimensional over $\mathbb{F}_p$. Let ξ and ξ^* denote as before generators of these spaces. The image $\bar{\xi}$, $\bar{\xi}^*$ of ξ, ξ^* in $H^1(M, W_f) = \mathrm{Hom}(G_M, W_f)$ and $H^1(M, W_f^*)$ cuts out extensions M_ξ and M_{ξ^*} of M whose Galois groups are identified, via $\bar{\xi}$ and $\bar{\xi}^*$, with W_f and W_f^* respectively.

Let M_{s,ξ,ξ^*} denote the compositum of M_s, M_ξ, and M_{ξ^*} over M. Since the Galois representations $A_{f,1}$, W_f and W_f^* are absolutely irreducible and pairwise non-isomorphic, the Galois group of M_{s,ξ,ξ^*} over $\mathbb{Q}$ is isomorphic to the semi-direct product

$$\mathrm{Gal}(M_{s,\xi,\xi^*}/\mathbb{Q}) = (A_{f,1} \times W_f \times W_f^*) \rtimes \mathrm{Gal}(M/\mathbb{Q}),$$

where the action of the quotient $\mathrm{Gal}(M/\mathbb{Q})$ on the abelian normal subgroup $(A_{f,1} \times W_f \times W_f^*)$ is given by

$$(\tau^j, T)(v, w, w^*) = (\delta^j \bar{T} v, \bar{T} w \bar{T}^{-1}, \bar{T} w^* \bar{T}^{-1} \det(T)).$$

Case 1: Suppose that ξ belongs to $\mathrm{Sel}_{\ell_1}(\mathbb{Q}, W_f)$, so that ξ^* belongs also to $\mathrm{Sel}_{\ell_1}(\mathbb{Q}, W_f^*)$. The group $\mathrm{Gal}(M_{s,\xi,\xi^*}/\mathbb{Q})$ contains an element of the form (v, w, w^*, τ, T), where

1. The transformation T acting on $A_{f,n}$ has eigenvalues δ and λ, were λ is an element of $(\mathbb{Z}/p^n\mathbb{Z})^\times$ of order prime to p which is $\neq \pm 1$.

2. The vector v belongs to the unique line in $A_{f,1}$ on which T acts by δ.

3. The vector w (resp. w^*) belongs to the unique line in W_f (resp. W_f^*) which is fixed by T.

Let ℓ_2 be a rational prime satisfying

$$\mathrm{Frob}_{\ell_2}(M_{s,\xi,\xi^*}/\mathbb{Q}) = (v, w, w^*, \tau, T). \qquad (34)$$

There are infinitely many such primes ℓ_2, by the Chebotarev density theorem. Now, note that

1. By the same reasoning as in the proof of theorem 3.2, the prime ℓ_2 is n-admissible and $v_{\ell_2}(s) \neq 0$.

2. A similar argument shows that $v_{\ell_2}(\xi) \neq 0$ and $v_{\ell_2}(\xi^*) \neq 0$. From this it follows, by part 1 of proposition 3.8, that $\mathrm{Sel}_{\ell_1\ell_2}(\mathbb{Q}, W_f) = 0$. Hence (ℓ_1, ℓ_2) is a rigid pair, and theorem 3.10 follows.

Case 2: Suppose that ξ does not belong to $\mathrm{Sel}_{\ell_1}(\mathbb{Q}, W_f)$, so that ξ^* also does not belong to $\mathrm{Sel}_{\ell_1}(\mathbb{Q}, W_f^*)$. Keeping the notations of case 1, let ℓ_2 be a rational prime satisfying

$$\mathrm{Frob}_{\ell_2}(M_{s,\xi,\xi^*}/\mathbb{Q}) = (v, 0, 0, \tau, T). \tag{35}$$

There are infinitely such primes ℓ_2, by the Chebotarev density theorem. Note that the prime ℓ_2 is n-admissible and $v_{\ell_2}(s) \neq 0$, and that $v_{\ell_2}(\xi)$ and $v_{\ell_2}(\xi^*)$ both vanish. It follows from part 2 of proposition 3.8 that either $\mathrm{Sel}_{\ell_1\ell_2}(\mathbb{Q}, W_f)$ is trivial – i.e., (ℓ_1, ℓ_2) is a rigid pair – or that $\mathrm{Sel}_{\ell_2}(\mathbb{Q}, W_f)$ is one-dimensional.

Theorem 3.11 *Suppose that f is a p-isolated eigenform in $S_2(\mathcal{T}/\Gamma)$, and let ℓ_1 be an admissible prime for f. Let s be a non-zero class in $H^1(K, A_{f,1})$. Suppose further that $\mathrm{Sel}_{\ell_1}(\mathbb{Q}, W_f)$ is one-dimensional over $\mathbb{F}_p$. Then there exist infinitely many n-admissible primes ℓ_2 such that*

1. *$\partial_{\ell_2}(s) = 0$ and $v_{\ell_2}(s) \neq 0$.*

2. *(ℓ_1, ℓ_2) is a rigid pair.*

Proof: This follows directly from the analysis of case 1 in the proof of theorem 3.10.

Congruences between modular forms. Let ℓ_1, ℓ_2 be distinct n-admissible primes relative to f, such that p^n divides $\ell_1+1-\epsilon_1 a_{\ell_1}(f)$ and $\ell_2+1-\epsilon_2 a_{\ell_2}(f)$, for ϵ_1 and ϵ_2 equal to ± 1. Let B' be the definite quaternion algebra of discriminant $\mathrm{Disc}(B)\ell_1\ell_2$, let R' be an Eichler $\mathbb{Z}[1/p]$-order of level N^+ in B' and let $\Gamma' := (R')^\times/\mathbb{Z}[1/p]^\times$. The theory of congruences between modular forms yields the following proposition:

Proposition 3.12 *There exists an eigenform $g \in S_2(\mathcal{T}/\Gamma', \mathbb{Z}/p^n\mathbb{Z})$ such that the equalities modulo p^n hold:*

$$T_q g \equiv a_q(f) g \quad (q \not| N\ell_1\ell_2), \qquad U_q g \equiv a_q(f) g \quad (q|N), \tag{36}$$

$$U_{\ell_1} g \equiv \epsilon_1 g, \quad U_{\ell_2} g \equiv \epsilon_2 g.$$

If furthermore the pair (ℓ_1, ℓ_2) is a rigid pair, then g can be lifted to an eigenform with coefficients in $\mathbb{Z}_p$ satisfying (36) above. This form is p-isolated.

Proof: The existence of the mod p^n eigenform g, which relies on the concepts and notations introduced in sections 5 and 9, is given in theorem 9.3. This g corresponds to a surjective algebra homomorphism $f_{\ell_2,\ell_1} : \mathbb{T}_{\ell_2,\ell_1} \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$, where $\mathbb{T}_{\ell_2,\ell_1}$ is the Hecke algebra defined in the proof of theorem 9.3. If (ℓ_1, ℓ_2) is a rigid pair, this algebra is isomorphic to $\mathbb{Z}_p$ and therefore f_{ℓ_2,ℓ_1} lifts to characteristic 0 so that g can be lifted (uniquely) to a form in $S_2(\mathcal{T}/\Gamma')$.

4 The Euler System Argument

4.1 The Euler system

Section 7 describes the construction of certain global cohomology classes

$$\kappa(\ell) \in \hat{H}^1_\ell(K_\infty, T_{f,n}),$$

indexed by the n-admissible primes ℓ attached to f. The proof of theorem 1 relies crucially on the existence of these classes and on their behaviour under localisation described in theorems 4.1 and 4.2 below. Both theorems are instances of explicit reciprocity laws relating these explicit cohomology classes to special values of L-functions, and form the technical heart of the proof of theorem 1.

Observe that when ℓ is an n-admissible prime, the local cohomology group $\hat{H}^1(K_{\infty,\ell}, T_{f,n})$ decomposes as a direct sum

$$\begin{aligned} \hat{H}^1(K_{\infty,\ell}, T_{f,n}) &= \hat{H}^1_{\mathrm{fin}}(K_{\infty,\ell}, T_{f,n}) \oplus \hat{H}^1_{\mathrm{ord}}(K_{\infty,\ell}, T_{f,n}) \\ &= \hat{H}^1_{\mathrm{fin}}(K_{\infty,\ell}, T_{f,n}) \oplus \hat{H}^1_{\mathrm{sing}}(K_{\infty,\ell}, T_{f,n}). \end{aligned}$$

The map ∂_ℓ is simply the projection onto the second factor, while v_ℓ can be extended naturally to a map

$$v_\ell : \hat{H}^1(K_{\infty,\ell}, T_{f,n}) \longrightarrow \hat{H}^1_{\rm fin}(K_{\infty,\ell}, T_{f,n}) = \hat{H}^1(K_{\infty,\ell}, T_{f,n})/\hat{H}^1_{\rm ord}(K_{\infty,\ell}, T_{f,n})$$

defined as the projection onto the first factor.

Theorem 4.1 *If ℓ is an n-admissible prime, then $v_\ell(\kappa(\ell)) = 0$. The equality*

$$\partial_\ell(\kappa(\ell)) = \mathcal{L}_f \pmod{p^n}$$

holds in $\hat{H}^1_{\rm sing}(K_{\infty,\ell}, T_{f,n}) \simeq \Lambda/p^n\Lambda$, up to multiplication by elements of $\mathbb{Z}_p^\times$ and G_∞.

Note that the ambiguity in the statement of theorem 4.1 is unavoidable, since the identification of $H^1_{\rm sing}(K_{\infty,\ell}, T_{f,n})$ with $\Lambda/p^n\Lambda$, and the element $\mathcal{L}_f$, are both only defined up to multiplication by elements in $\mathbb{Z}_p^\times$ and G_∞.

Theorem 4.1 is proved in section 8.

The second theorem describes the localisation of $\kappa(\ell_1)$ at an n-admissible prime ℓ_2 which is different from ℓ_1. Recall the discrete subgroup Γ' of $\mathbf{PSL}_2(\mathbb{Q}_p)$ and the $\mathbb{Z}/p^n\mathbb{Z}$-valued eigenform g in $S_2(\mathcal{T}/\Gamma', \mathbb{Z}/p^n\mathbb{Z})$ attached to f and (ℓ_1, ℓ_2) in proposition 3.12.

Theorem 4.2 *The equality*

$$v_{\ell_2}(\kappa(\ell_1)) = \mathcal{L}_g$$

holds in $\hat{H}^1_{\rm fin}(K_{\infty,\ell_2}, T_{f,n}) \simeq \Lambda/p^n\Lambda$, up to multiplication by elements of $\mathbb{Z}_p^\times$ and G_∞.

Theorem 4.2 is proved in section 9.

Since the definition of g is symmetric in ℓ_1 and ℓ_2, one obtains the following reciprocity formula for the classes $\kappa(\ell)$:

Corollary 4.3 *For all pairs of n-admissible primes ℓ_1, ℓ_2 attached to f, the equality*

$$v_{\ell_1}(\kappa(\ell_2)) = v_{\ell_2}(\kappa(\ell_1))$$

holds in $\Lambda/p^n\Lambda$, up to multiplication by elements of $\mathbb{Z}_p^\times$ and G_∞.

4.2 The argument

To an ordinary eigenform $f \in S_2(\mathcal{T}/\Gamma)$ with coefficients in $\mathbb{Z}_p$ one has associated two invariants: the p-adic L-function $L_p(f,K) \in \Lambda$ (section 1) and the Selmer group $\mathrm{Sel}_{f,n}$ (section 2). This section explains the proof of theorem 1. In our approach based on congruences between modular forms, it is indispensable to prove the following generalisation which is stronger insofar as it applies to all p-isolated modular eigenforms in $S_2(\mathcal{T}/\Gamma)$ with coefficients in $\mathbb{Z}_p$ satisfying assumption 2.1.

Theorem 4.4 *Let f be an ordinary eigenform in $S_2(\mathcal{T}/\Gamma)$ with coefficients in $\mathbb{Z}_p$ which is p-isolated, and satisfies assumption 2.1. The characteristic power series of* $\mathrm{Sel}_{f,\infty}^\vee$ *divides the p-adic L-function $L_p(f,K)$.*

Proof: By proposition 3.1, it suffices to show that

$$\varphi(\mathcal{L}_f)^2 \text{ belongs to } \mathrm{Fitt}_{\mathcal{O}}(\mathrm{Sel}_{f,\infty}^\vee \otimes_\varphi \mathcal{O}), \tag{37}$$

for all homomorphisms φ of Λ into a discrete valuation ring $\mathcal{O}$. For this it is enough to show that

$$\varphi(\mathcal{L}_f)^2 \text{ belongs to } \mathrm{Fitt}_{\mathcal{O}}(\mathrm{Sel}_{f,n}^\vee \otimes_\varphi \mathcal{O}), \quad \text{for all } n \geq 1. \tag{38}$$

Fix $\mathcal{O}$, φ, and n. Write π for a uniformiser of $\mathcal{O}$, and let $e := \mathrm{ord}_\pi(p)$ be the ramification degree of $\mathcal{O}$ over $\mathbb{Z}_p$. Write

$$t_f := \mathrm{ord}_\pi(\varphi(\mathcal{L}_f)).$$

Assume without loss of generality that

1. $t_f < \infty$. (Otherwise, $\varphi(\mathcal{L}_f) = 0$ and (38) is trivially verified.)

2. The group $\mathrm{Sel}_{f,n}^\vee \otimes \mathcal{O}$ is non-trivial. (Otherwise, its Fitting ideal is equal to $\mathcal{O}$ and (38) is trivially verified.)

Theorem 4.4 (or rather, equation (38)) is proved by induction on t_f.

We begin by describing the construction of certain cohomology classes attached to an admissible prime ℓ. Let ℓ be any $(n+t_f)$-admissible prime, and enlarge $\{\ell\}$ to an $(n+t_f)$-admissible set S. Let

$$\kappa(\ell) \in \hat{H}^1_\ell(K_\infty, T_{f,n+t_f}) \subset \hat{H}^1_S(K_\infty, T_{f,n+t_f})$$

be the cohomology class attached to ℓ as in section 4.1, and denote by $\kappa_\varphi(\ell)$ the natural image of this class in

$$\mathcal{M} := \hat{H}^1_S(K_\infty, T_{f,n+t_f}) \otimes_\varphi \mathcal{O}.$$

Note that this module is free over $\mathcal{O}/p^{(n+t_f)}$, by proposition 3.3. By theorem 4.1,

$$\mathrm{ord}_\pi(\kappa_\varphi(\ell)) \leq \mathrm{ord}_\pi(\partial_\ell \kappa_\varphi(\ell)) = \mathrm{ord}_\pi(\varphi(\mathcal{L}_f)) = t_f,$$

so that $t := \mathrm{ord}_\pi(\kappa_\varphi(\ell)) \leq t_f$. Choose an element $\tilde{\kappa}_\varphi(\ell) \in \mathcal{M}$ satisfying

$$\pi^t \tilde{\kappa}_\varphi(\ell) = \kappa_\varphi(\ell).$$

Note that $\tilde{\kappa}_\varphi(\ell)$ is well defined modulo the π^t-torsion subgroup of $\mathcal{M}$, which is contained in the kernel of the natural homomorphism

$$\hat{H}^1_S(K_\infty, T_{f,n+t_f}) \otimes_\varphi \mathcal{O} \longrightarrow \hat{H}^1_S(K_\infty, T_{f,n}) \otimes_\varphi \mathcal{O}.$$

To remove this ambiguity, let $\kappa'_\varphi(\ell)$ be the natural image of the class $\tilde{\kappa}_\varphi(\ell)$ in $\hat{H}^1_S(K_\infty, T_{f,n}) \otimes \mathcal{O}$. The key properties of the class $\kappa'_\varphi(\ell)$ are summarised in lemmas 4.5 and 4.6 below.

Lemma 4.5 *The class $\kappa'_\varphi(\ell)$ enjoys the following properties:*

1. $\mathrm{ord}_\pi(\kappa'_\varphi(\ell)) = 0$.
2. $\partial_q \kappa'_\varphi(\ell) = 0$, *for all* $q \not| \ell N^-$.
3. $v_\ell(\kappa'_\varphi(\ell)) = 0$.
4. $\mathrm{ord}_\pi(\partial_\ell \kappa'_\varphi(\ell)) = t_f - t$.

Proof: The first property follows from the fact that $\mathrm{ord}_\pi(\kappa_\varphi(\ell)) = t$. The second is a direct consequence of the fact that $\kappa(\ell)$ belongs to $\hat{H}^1_\ell(K_\infty, T_{f,n+t_f})$, while the third and fourth follow from theorem 4.1.

Lemma 4.6 *The element $\partial_\ell(\kappa'_\varphi(\ell))$ belongs to the kernel of the natural homomorphism*

$$\eta_\ell : \hat{H}^1_{\mathrm{sing}}(K_{\infty,\ell}, T_{f,n}) \otimes_\varphi \mathcal{O} \longrightarrow \mathrm{Sel}^\vee_{f,n} \otimes_\varphi \mathcal{O}.$$

Proof: Let I_φ denote the kernel of φ. By the global reciprocity law of class field theory, the class $\tilde{\kappa}_\varphi(\ell)$ satisfies

$$\sum_{q|S}\langle \partial_q(\tilde{\kappa}_\varphi(\ell)), s_q\rangle_q = 0, \tag{39}$$

for all $s \in \mathrm{Sel}_{f,n+t_f}[I_\varphi]$. (Here, s_q simply denotes the natural image of s in $H^1_{\mathrm{fin}}(K_{q,\infty}, A_{f,n+t_f})$.) On the other hand, $\pi^t\tilde{\kappa}_\varphi(\ell) = \kappa_\varphi(\ell)$ has trivial residue at all the primes $q \neq \ell$. Hence, for such primes, the element $\partial_q(\tilde{\kappa}_\varphi(\ell))$ annihilates

$$\pi^t H^1_{\mathrm{fin}}(K_{\infty,q}, A_{f,n+t_f})[I_\varphi] \supset H^1_{\mathrm{fin}}(K_{\infty,q}, A_{f,n})[I_\varphi].$$

Hence, if s belongs to $\mathrm{Sel}_{f,n}[I_\varphi]$, the terms in the sum (39) corresponding to the primes $q \neq \ell$ are zero. Hence so is the term corresponding to ℓ. It follows that $\partial_\ell(\kappa'_\varphi(\ell))$ annihilates the image of $\mathrm{Sel}_{f,n}[I_\varphi]$ in $H^1_{\mathrm{fin}}(K_{\infty,\ell}, A_{f,n})$, as was to be shown.

We now turn to the proof of (38), in the case where $t_f = 0$, which provides the basis for the induction argument.

Proposition 4.7 *If $t_f = 0$, (i.e., $\mathcal{L}_f$ is a unit) then $\mathrm{Sel}^\vee_{f,n}$ is trivial.*

Proof: Since $\mathcal{L}_f$ is a unit, theorem 4.1 implies that $\partial_\ell(\kappa_\varphi(\ell))$ generates $\hat{H}^1_{\mathrm{sing}}(K_{\infty,\ell}, T_{f,n}) \otimes_\varphi \mathcal{O}$, for all n-admissible primes ℓ. Hence the map η_ℓ of lemma 4.6 is trivial for all such primes. This is enough to conclude that $\mathrm{Sel}^\vee_{f,n}$ is trivial. For otherwise, Nakayama's lemma implies that the group

$$\mathrm{Sel}^\vee_{f,n}/\mathfrak{m}_\Lambda = (\mathrm{Sel}_{f,n}[\mathfrak{m}_\Lambda])^\vee$$

is non-zero. Let s be a non-trivial element of $\mathrm{Sel}_{f,n}[\mathfrak{m}_\Lambda]$. By part 1 of theorem 3.4, s can be viewed as an element of $H^1(K, A_{f,1})$. Invoking theorem 3.2, choose an n-admisible prime ℓ such that $v_\ell(s) \neq 0$. The non-degeneracy of the local Tate pairing implies that η_ℓ is non-zero, a contradiction.

Turning now to the general case of equation (38), let Π be the set of rational primes ℓ satisfying the following conditions:

1. ℓ is $(n + t_f)$-admissible.

2. The quantity $t = \mathrm{ord}_\pi(\kappa_\varphi(\ell))$ is minimal, among all primes satisfying condition 1.

Note that the set Π is non-empty, by theorem 3.2. Let t be the common value of $\mathrm{ord}_\pi(\kappa_\varphi(\ell))$ for $\ell \in \Pi$.

Lemma 4.8 *One has $t < t_f$.*

Proof: Suppose not. Then $\mathrm{ord}_\pi(\kappa_\varphi(\ell)) = t_f$, for all $(n+t_f)$-admissible primes ℓ. Let s be a non-zero element of $H^1(K, A_{f,1}) \cap \mathrm{Sel}_{f,n}$, which exists by theorem 3.4. Invoking theorem 3.2, choose an $(n+t_f)$-admissible prime ℓ such that $v_\ell(s) \neq 0$. By lemma 4.5, the natural image of $\partial_\ell(\kappa'_\varphi(\ell))$ in $H^1(K_\ell, T_{f,1}) \otimes_\varphi \mathcal{O}$ is non zero. By lemma 4.6, it is also orthogonal to $v_\ell(s)$ with respect to the local Tate pairing, contradicting the fact that the vectors $\partial_\ell(\kappa'_\varphi(\ell))$ and $v_\ell(s)$ are both supposed to be non-zero and that the Tate pairing is a perfect duality between these two one-dimensional vector spaces over $\mathcal{O}/\pi$.

Lemma 4.9 *There exist primes $\ell_1, \ell_2 \in \Pi$ such that (ℓ_1, ℓ_2) is a rigid pair.*

Proof: Choose any ℓ_1 in Π, and let s denote the natural image of $\kappa'_\varphi(\ell_1)$ in

$$\begin{aligned} \hat{H}^1_S(K_\infty, T_{f,n}) \otimes_\varphi \mathcal{O}/(\pi) &= \left(\hat{H}^1_S(K_\infty, T_{f,n})/\mathfrak{m}_\Lambda\right) \otimes (\mathcal{O}/\pi) \\ &\subset H^1(K, T_{f,1}) \otimes (\mathcal{O}/\pi), \end{aligned}$$

where the last inclusion (cf. part 2 of theorem 3.4) is induced from the corestriction map and the natural projection $T_{f,n} \longrightarrow T_{f,1}$. Observe that the class s is a non-zero element of $H^1(K, T_{f,1}) \otimes (\mathcal{O}/\pi)$ which satisfies $\partial_q(s) = 0$ for all $q \not| \ell_1 N$. Invoking theorem 3.10, choose an $n + t_f$-admissible prime ℓ_2 such that

1. $v_{\ell_2}(s) \neq 0$, and
2. either (ℓ_1, ℓ_2) is a rigid pair, or $\mathrm{Sel}_{\ell_2}(\mathbb{Q}, W_f)$ is one-dimensional.

The reader will note that:

$$t = \mathrm{ord}_\pi(\kappa_\varphi(\ell_1)) \leq \mathrm{ord}_\pi(\kappa_\varphi(\ell_2)) \leq \mathrm{ord}_\pi(v_{\ell_1}(\kappa_\varphi(\ell_2))). \qquad (40)$$

The first inequality holds by the minimality assumption made in the choice of the prime ℓ_1. The second inequality is a consequence of the fact that v_{ℓ_1}

is a homomorphism. By the reciprocity law of corollary 4.3, and the choice of ℓ_2,

$$\mathrm{ord}_\pi(v_{\ell_1}(\kappa_\varphi(\ell_2))) = \mathrm{ord}_\pi(v_{\ell_2}(\kappa_\varphi(\ell_1))) = \mathrm{ord}_\pi(\kappa_\varphi(\ell_1)). \tag{41}$$

(To see the second equality, note that the inequality

$$\mathrm{ord}_\pi(v_{\ell_2}(\kappa_\varphi(\ell_1))) \geq \mathrm{ord}_\pi(\kappa_\varphi(\ell_1))$$

is clear, and that strict inequality holds precisely when $v_{\ell_2}(s) = 0$.) Combining (40) and (41), it follows that that the inequalities must be equalities throughout, so that

$$t = \mathrm{ord}_\pi(\kappa_\varphi(\ell_1)) = \mathrm{ord}_\pi(\kappa_\varphi(\ell_2)).$$

Hence ℓ_2 belongs to Π. If (ℓ_1, ℓ_2) is a rigid pair, we are done. Otherwise, the group $\mathrm{Sel}_{\ell_2}(\mathbb{Q}, W_f)$ is one-dimensional. In that case one can repeat the argument above, with ℓ_1 replaced by ℓ_2, invoking this time theorem 3.11 instead of 3.10 to obtain a pair (ℓ_2, ℓ_3) satisfying the conclusion of lemma 4.9. This completes the proof of the lemma.

Let (ℓ_1, ℓ_2) be a rigid pair of $(n + t_f)$-admissible primes in Π, whose existence is guaranteed by lemma 4.9. By theorem 4.2, note that $t = t_g = \mathrm{ord}_\pi(\varphi(\mathcal{L}_g))$, where g is the p-isolated eigenform in $S_2(\mathcal{T}/\Gamma')$ attached to f and (ℓ_1, ℓ_2) through proposition 3.12.

Let $\mathrm{Sel}_{[\ell_1\ell_2]}$ denote the subgroup of $\mathrm{Sel}_{f,n}$ consisting of classes which are locally trivial at the primes dividing ℓ_1 and ℓ_2. By definition, there is a natural exact sequence of Λ-modules

$$0 \longrightarrow S^f_{\ell_1\ell_2} \longrightarrow \mathrm{Sel}^\vee_{f,n} \longrightarrow \mathrm{Sel}^\vee_{[\ell_1\ell_2]} \longrightarrow 0, \tag{42}$$

where $S^f_{\ell_1\ell_2}$ denotes the kernel of the natural surjection of duals of Selmer groups. Note the natural surjection given by local Tate duality:

$$\eta_f : (\hat{H}^1_{\mathrm{sing}}(K_{\infty,\ell_1}, A_{f,n}) \oplus \hat{H}^1_{\mathrm{sing}}(K_{\infty,\ell_2}, A_{f,n})) \longrightarrow S^f_{\ell_1\ell_2}$$

induced from the inclusion

$$(S^f_{\ell_1\ell_2})^\vee \subset H^1_{\mathrm{fin}}(K_{\infty,\ell_1}, A_{f,n}) \oplus H^1_{\mathrm{fin}}(K_{\infty,\ell_2}, A_{f,n}).$$

The domain of η_f is isomorphic to $(\Lambda/p^n\Lambda)^2$, by lemma 2.7. Let η_f^φ denote the map induced from η_f after tensoring by $\mathcal{O}$ via φ. The domain of η_f^φ is isomorphic to $(\mathcal{O}/p^n\mathcal{O})^2$. By lemma 4.6, the kernel of η_f^φ contains the vectors $(\partial_{\ell_1}\kappa'_\varphi(\ell_1), 0)$ and $(0, \partial_{\ell_2}\kappa'_\varphi(\ell_2))$ in

$$\left(\hat{H}^1_{\mathrm{sing}}(K_{\infty,\ell_1}, A_{f,n}) \oplus \hat{H}^1_{\mathrm{sing}}(K_{\infty,\ell_2}, A_{f,n})\right) \otimes_\varphi \mathcal{O} \simeq (\mathcal{O}/p^n\mathcal{O})^2.$$

By part 3 of lemma 4.5,

$$t_f - t_g = \mathrm{ord}_\pi(\partial_{\ell_1}\kappa'_\varphi(\ell_1)) = \mathrm{ord}_\pi(\partial_{\ell_2}\kappa'_\varphi(\ell_2)).$$

Hence

$$\pi^{2(t_f - t_g)} \text{ belongs to the Fitting ideal of } S^f_{\ell_1\ell_2} \otimes_\varphi \mathcal{O}. \tag{43}$$

One may repeat the above argument with the modular form g. Thus we have an exact sequence similar to (42) but involving g instead of f:

$$0 \longrightarrow S^g_{\ell_1\ell_2} \longrightarrow \mathrm{Sel}^\vee_{g,n} \longrightarrow \mathrm{Sel}^\vee_{[\ell_1\ell_2]} \longrightarrow 0, \tag{44}$$

as well as a surjection given by local Tate duality:

$$\eta_g : (\hat{H}^1_{\mathrm{fin}}(K_{\infty,\ell_1}, A_{f,n}) \oplus \hat{H}^1_{\mathrm{fin}}(K_{\infty,\ell_2}, A_{f,n})) \longrightarrow S^g_{\ell_1\ell_2}.$$

By global reciprocity, the kernel of the map η_g^φ obtained from η_g after tensoring by $\mathcal{O}$ via φ contains the elements

$$(v_{\ell_1}\kappa'_\varphi(\ell_1), v_{\ell_2}\kappa'_\varphi(\ell_1)) = (0, v_{\ell_2}\kappa'_\varphi(\ell_1))$$

as well as $(v_{\ell_1}\kappa'_\varphi(\ell_2), 0)$. But

$$\mathrm{ord}_\pi(v_{\ell_2}\kappa'_\varphi(\ell_1)) = \mathrm{ord}_\pi(v_{\ell_1}\kappa'_\varphi(\ell_2)) = t_g - t = 0.$$

It follows from this that the module $S_g \otimes_\varphi \mathcal{O}$ is trivial, and the natural surjection

$$\mathrm{Sel}^\vee_{g,n} \otimes_\varphi \mathcal{O} \longrightarrow \mathrm{Sel}^\vee_{[\ell_1\ell_2]} \otimes_\varphi \mathcal{O} \text{ is an isomorphism.} \tag{45}$$

Recall that, by lemma 4.8,

$$t_g < t_f,$$

and that the eigenform g satisfies all the hypotheses of theorem 4.4, including assumption 2.1, in light of the fact that ℓ_1 and ℓ_2 are admissible. One is thus in a position to invoke the induction hypothesis to conclude that

$$\varphi(\mathcal{L}_g)^2 \text{ belongs to the Fitting ideal of } \mathrm{Sel}_{g,n}^\vee \otimes_\varphi \mathcal{O}. \tag{46}$$

The theory of Fitting ideals implies that

$$\begin{aligned}
\pi^{2t_f} &= \pi^{2(t_f-t_g)}\pi^{2t_g} \\
&\in \mathrm{Fitt}_\mathcal{O}(S^f_{\ell_1\ell_2}\otimes\mathcal{O})\mathrm{Fitt}_\mathcal{O}(\mathrm{Sel}^\vee_{g,n}\otimes\mathcal{O}), \quad \text{by (43) and (46)} \\
&= \mathrm{Fitt}_\mathcal{O}(S^f_{\ell_1\ell_2}\otimes\mathcal{O})\mathrm{Fitt}_\mathcal{O}(\mathrm{Sel}^\vee_{[\ell_1\ell_2]}\otimes\mathcal{O}), \quad \text{by (45)} \\
&\subset \mathrm{Fitt}_\mathcal{O}(\mathrm{Sel}^\vee_{f,n}\otimes\mathcal{O}), \quad \text{by (42)}.
\end{aligned}$$

Hence (38) is proved: $\varphi(\mathcal{L}_f)^2$ belongs to the Fitting ideal of $\mathrm{Sel}^\vee_{f,n}\otimes_\varphi\mathcal{O}$. Theorem 4.4 follows.

5 Shimura curves

The construction and the properties of the Euler System used in the argument of section 4 are based on the geometry over $\mathbb{Z}$ of certain Shimura curves, which is reviewed in this section.

Let M be a positive integer, and let $M = M^+M^-$ be an integer decomposition of M such that M^- is a squarefree product (possibly empty) of an even number of prime factors. Following [Ro] and [BD1], one may attach to such a decomposition a Shimura curve X_{M^+,M^-}. If M^- is equal to 1, X_{M^+,M^-} is the classical modular curve $X_0(M)$ of level M. In the general case, X_{M^+,M^-} is the Shimura curve with level M^+-structure associated to the indefinite quaternion algebra of discriminant M^-.

5.1 The moduli definition

The curve $X = X_{M^+,M^-}$ has the following moduli interpretations.
Models over $\mathbb{Z}[\frac{1}{M}]$
Let $\mathcal{B}$ be the indefinite quaternion algebra over $\mathbb{Q}$ of discriminant M^-. Fix a maximal order $\mathcal{R}_{\max}$ in $\mathcal{B}$, and an Eichler order $\mathcal{R}$ of level M^+ contained in $\mathcal{R}_{\max}$. Write $\mathcal{F} = \mathcal{F}_{\mathbb{Z}[\frac{1}{M}]}$ for the functor from the category of schemes

over $\mathbb{Z}[\frac{1}{M}]$ to the category of sets which associates to a scheme S the set of isomorphism classes of triples (A, ι, C), where:

1. A is an abelian scheme over S of relative dimension 2,
2. $\iota : \mathcal{R}_{\max} \to \mathrm{End}(A)$ is an action of $\mathcal{R}_{\max}$ on A,
3. C is a level M^+-structure on A, that is, a subgroup scheme of A of order $(M^+)^2$ which is stable and cyclic for the action of $\mathcal{R}_{\max}$.

If M^- is strictly greater than 1, the functor $\mathcal{F}$ is coarsely representable by a smooth projective scheme $X_{\mathbb{Z}[\frac{1}{M}]}$ over $\mathbb{Z}[\frac{1}{M}]$, with smooth fibers. Let $\mathcal{H}_\infty$ be the complex upper half plane, and let $\mathcal{R}_1^\times$ be the group of norm 1 elements in $\mathcal{R}$. Fix an embedding of $\mathcal{B}$ in $M_2(\mathbb{R})$, and write $\Gamma_{\infty,1}$ for the natural image of $\mathcal{R}_1^\times$ in $\mathbf{PGL}_2(\mathbb{R})$. The group $\Gamma_{\infty,1}$ acts discontinuously (on the right) on $\mathcal{H}_\infty$, and the complex points $X(\mathbb{C})$ of the generic fiber $X = X_{\mathbb{Q}}$ are identified with the Riemann surface $\mathcal{H}_\infty/\Gamma_{\infty,1}$. For more information, see [BC], chapter III and [Bu].

If M^- is equal to 1, then $\mathcal{B}$ is isomorphic to the split quaternion algebra $M_2(\mathbb{Q})$, and one may assume that $\mathcal{R}_{\max}$ corresponds to the standard maximal order $M_2(\mathbb{Z})$. A triple (A, i, C) as above is then of the form $(E\times E, \iota, C_E\times C_E)$ where E is an elliptic curve, C_E is a level M-structure on E, and the action ι is the natural matrix action of $M_2(\mathbb{Z})$ on $E \times E$. Thus, the functor $\mathcal{F}$ is coarsely representable by the affine modular curve $Y_0(M)_{\mathbb{Z}[\frac{1}{M}]}$. The projective completion $X_0(M)_{\mathbb{Z}[\frac{1}{M}]}$ of $Y_0(M)_{\mathbb{Z}[\frac{1}{M}]}$, obtained by adding a finite set of cusps, is a moduli space for generalized elliptic curves with level M-structure. See [DR] and [Bu].

Models over $\mathbb{Z}_\ell$ for $\ell \mid M^+$

Assume that ℓ is a prime dividing exactly M^+. (This is the only case which is relevant to the arguments of this paper.)

The reader is referred to [Ed], sections 3 and 4, [DR], [KM], and [Bu] for the definition of the variant of the moduli functor $\mathcal{F}$ which can be used in this case. The resulting canonical model $X_{\mathbb{Z}_\ell}$ is a *nodal model* of X, in the sense of [Ed]. That is:

1. $X_{\mathbb{Z}_\ell}$ is proper and flat over $\mathbb{Z}_\ell$, and its generic fiber is X (viewed as a curve over $\mathbb{Q}_\ell$),

2. the irreducible components of the special fiber $X_{\mathbb{F}_\ell}$ of $X_{\mathbb{Z}_\ell}$ are smooth, and the only singularities of $X_{\mathbb{F}_\ell}$ are ordinary double points.

More precisely, the special fiber $X_{\mathbb{F}_\ell}$ consists of two copies of the irreducible curve $(X_{M^+/\ell,M^-})_{\mathbb{F}_\ell}$ intersecting transversally at the supersingular points, which are identified via the Frobenius morphism at ℓ. (Note that $X_{M^+/\ell,M^-}$ has good reduction at ℓ, and a description of $(X_{M^+/\ell,M^-})_{\mathbb{F}_\ell}$ follows from the model $(X_{M^+/\ell,M^-})_{\mathbb{Z}[\frac{1}{M/\ell}]}$ given above.)

Models over $\mathbb{Z}_\ell$ for $\ell \mid M^-$
Assume that M^- is strictly greater than 1. Fix a prime ℓ dividing M^-. As before, one may define a model $X_{\mathbb{Z}_\ell}$ of X over $\mathbb{Z}_\ell$ via moduli. The new moduli functor $\mathcal{F}_{\mathbb{Z}_\ell}$ on schemes over $\mathbb{Z}_\ell$ is defined similarly to $\mathcal{F}_{\mathbb{Z}[\frac{1}{M}]}$, except for the requirement that the action ι be *special* in the sense of [BC], section III.3. The functor $\mathcal{F}_{\mathbb{Z}_\ell}$ is coarsely representable by a scheme $X_{\mathbb{Z}_\ell}$, which is a nodal model of X. A more precise description of $X_{\mathbb{Z}_\ell}$ is given in section 5.2 where, in particular, it is explained that the irreducible components of $X_{\mathbb{F}_\ell}$ are rational curves.

5.2 The Cerednik-Drinfeld theorem

(References: see [JoLi1] and [BC] for details, and [BD3], section 4 for an exposition.)
Assume that M^- is strictly greater than 1, and let ℓ be a prime dividing M^-. Let B be the definite quaternion algebra over $\mathbb{Q}$ of discriminant M^-/ℓ, and let R be an Eichler order in B of level $M^+\ell$. Set $B_\ell = B \otimes \mathbb{Z}_\ell$ and $R_\ell = R \otimes \mathbb{Z}_\ell$, and fix an isomorphism $\kappa_\ell : B_\ell \xrightarrow{\sim} M_2(\mathbb{Q}_\ell)$ mapping R_ℓ onto the standard Eichler order of level ℓ in $M_2(\mathbb{Z}_\ell)$, consisting of matrices which are upper triangular modulo ℓ. Write Γ_ℓ, respectively, $\Gamma_{\ell,1}$ for the image of $R[\frac{1}{\ell}]^\times$, respectively, $R[\frac{1}{\ell}]^\times_1$ in $\mathbf{PGL}_2(\mathbb{Q}_\ell)$, where $R[\frac{1}{\ell}]^\times_1$ is the subgroup of norm 1 elements in $R[\frac{1}{\ell}]^\times$.

Let $\mathbb{C}_\ell$ be a completion of an algebraic closure of $\mathbb{Q}_\ell$, and let $\hat{\mathcal{H}}_\ell$ be the *ℓ-adic upper half plane*, viewed as a formal scheme over $\mathbb{Z}_\ell$. The generic fiber of $\hat{\mathcal{H}}_\ell$ is identified with a rigid analytic space $\mathcal{H}_\ell$ over $\mathbb{Q}_\ell$ whose $\mathbb{C}_\ell$-valued points are

$$\mathcal{H}_\ell(\mathbb{C}_\ell) = \mathbb{P}^1(\mathbb{C}_\ell) - \mathbb{P}^1(\mathbb{Q}_\ell) = \mathbb{C}_\ell - \mathbb{Q}_\ell.$$

The special fiber of $\hat{\mathcal{H}}_\ell$ consists of an infinite sequence of projective lines, intersecting at ordinary double points. The ℓ-adic group $\Gamma_{\ell,1}$ acts discontinously on $\hat{\mathcal{H}}_\ell$ and $\mathcal{H}_\ell$ on the right. The action on $\mathcal{H}_\ell(\mathbb{C}_\ell)$ is given by the rule

$$z\gamma = \frac{az+b}{cz+d}, \quad \text{where } \gamma^{-1} \text{ is represented by } \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

The quotients $\hat{\mathcal{H}}_\ell/\Gamma_{\ell,1}$ and $\mathcal{H}_\ell/\Gamma_{\ell,1}$ exist in the category of formal schemes and of rigid analytic spaces, respectively. Since the irreducible components of the special fiber of $\hat{\mathcal{H}}_\ell$ have finite stabilizer in $\Gamma_{\ell,1}$, it follows that the irreducible components of the special fiber of $\mathcal{H}_\ell/\Gamma_{\ell,1}$ are rational curves.

Write $\hat{X}_{\mathbb{Z}_\ell}$ for the formal completion of $X_{\mathbb{Z}_\ell}$ along its special fiber, where $X_{\mathbb{Z}_\ell}$ is the model of X over $\mathbb{Z}_\ell$ introduced in section 5.1. Let X^{an} be the rigid analytic space over $\mathbb{Q}_\ell$ associated to X. Fix a quadratic unramified extension $\mathbb{Q}_{\ell^2}$ of $\mathbb{Q}_\ell$, and denote by $\mathbb{Z}_{\ell^2}$ the ring of integers of $\mathbb{Q}_{\ell^2}$ and by $\mathbb{F}_{\ell^2}$ its residue field.

Theorem 5.1 *The formal schemes $\hat{X}_{\mathbb{Z}_\ell}$ and $\hat{\mathcal{H}}_\ell/\Gamma_{\ell,1}$ are naturally isomorphic over $\mathbb{Z}_{\ell^2}$. In particular, X^{an} is isomorphic to $\mathcal{H}_\ell/\Gamma_{\ell,1}$ over $\mathbb{Q}_{\ell^2}$, and $X_{\mathbb{F}_\ell}$ is isomorphic to the special fiber of $\hat{\mathcal{H}}_\ell/\Gamma_{\ell,1}$ over $\mathbb{F}_{\ell^2}$.*

Theorem 5.1 can be proved by comparing the moduli definition of $X_{\mathbb{Z}_\ell}$ given in section 5.1 with Drinfeld's interpretation [Dr] of $\hat{\mathcal{H}}_\ell$, where the base-change of $\hat{\mathcal{H}}_\ell$ to the maximal unramified extension of $\mathbb{Z}_\ell$ is identified with the classifying space of certain formal groups of dimension 2 and height 4 which are endowed with an action of the local order $\mathcal{R}_{\max} \otimes \mathbb{Z}_\ell$. To obtain the version of the Cerednik-Drinfeld theorem given here, one must descend the isomorphism obtained from the above comparison to $\mathbb{Z}_\ell$, using the arguments of Jordan and Livné in [JoLi1]; see also [BC], chapter III.

5.3 Character groups

Let ℓ be a prime dividing exactly M, and let $X_{\mathbb{Z}_{\ell^2}}$ be a fixed nodal model of X over the unramified quadratic extension $\mathbb{Z}_{\ell^2}$ of $\mathbb{Z}_\ell$. (It is convenient to extend scalars from $\mathbb{Z}_\ell$ to $\mathbb{Z}_{\ell^2}$, also in view of the isomorphism of theorem 5.1.) The *dual graph* $\mathcal{G}_\ell = \mathcal{G}_\ell(X)$ of X at ℓ is defined to be the finite graph determined by the following properties:

1. the set of vertices $\mathcal{V}(\mathcal{G}_\ell)$ is the set of irreducible (geometric) components of the special fiber $X_{\mathbb{F}_{\ell^2}}$,

2. the set of (unoriented) edges $\mathcal{E}(\mathcal{G}_\ell)$ is the set of singular points of $X_{\mathbb{F}_{\ell^2}}$,
3. two vertices v and v' are joined by an edge e if v and v' intersect at the singular point e.

Let $xy = \ell^{\nu_e}$ be a local equation for $X_{\mathbb{Z}_{\ell^2}}$ at the double point e. The assignment $e \mapsto \nu_e$ equips the graph $\mathcal{G}_\ell$ with a weight function $\nu : \mathcal{E}(\mathcal{G}_\ell) \to \mathbb{N}$.

Fix an orientation on $\mathcal{G}_\ell$, that is, a pair of maps $s, t : \mathcal{E}(\mathcal{G}_\ell) \to \mathcal{V}(\mathcal{G}_\ell)$ such that $s(e)$ and $t(e)$ are the ends of the edge e, called the source and the target of e, respectively.

Let $\mathbb{Z}[\mathcal{V}(\mathcal{G}_\ell)]$ and $\mathbb{Z}[\mathcal{E}(\mathcal{G}_\ell)]$ be the module of formal divisors with integer coefficients supported on $\mathcal{V}(\mathcal{G}_\ell)$ and $\mathcal{E}(\mathcal{G}_\ell)$, respectively. Let $\mathbb{Z}[\mathcal{V}(\mathcal{G}_\ell)]^0$ and $\mathbb{Z}[\mathcal{E}(\mathcal{G}_\ell)]^0$ be the submodule of degree zero divisors in $\mathbb{Z}[\mathcal{V}(\mathcal{G}_\ell)]$ and $\mathbb{Z}[\mathcal{E}(\mathcal{G}_\ell)]$, respectively. Let

$$\partial_* : \mathbb{Z}[\mathcal{E}(\mathcal{G}_\ell)] \to \mathbb{Z}[\mathcal{V}(\mathcal{G}_\ell)]^0$$

be the $\mathbb{Z}$-linear boundary map defined by the rule $\partial_*(e) = t(e) - s(e)$.

Let $J = J(X)$ be the jacobian of X, and let $J_{\mathbb{Z}_{\ell^2}}$ be the Néron model of J over $\mathbb{Z}_{\ell^2}$. Write $J_{\mathbb{F}_{\ell^2}}$ for the special fiber of J, $J^0_{\mathbb{F}_{\ell^2}}$ for the connected component of the origin in $J_{\mathbb{F}_{\ell^2}}$, and $\Phi_\ell = \Phi_\ell(X)$ for the group of connected (geometric) components $J_{\mathbb{F}_{\ell^2}}/J^0_{\mathbb{F}_{\ell^2}}$. Denote by $\mathcal{X}_\ell = \mathcal{X}_\ell(X)$ the *character group* $\mathrm{Hom}(T_{\mathbb{F}_{\ell^2}}, \mathbb{G}_m)$ of J at ℓ, where $T_{\mathbb{F}_{\ell^2}}$ is the maximal torus of $J^0_{\mathbb{F}_{\ell^2}}$.

Proposition 5.2 *The module $\mathcal{X}_\ell$ is isomorphic to the kernel of ∂_*, and hence fits into the exact sequence*

$$0 \to \mathcal{X}_\ell \to \mathbb{Z}[\mathcal{E}(\mathcal{G}_\ell)] \xrightarrow{\partial_*} \mathbb{Z}[\mathcal{V}(\mathcal{G}_\ell)]^0 \to 0.$$

Sketch of proof: The module $\mathcal{X}_\ell$ is canonically identified with the integral homology group $H_1(\mathcal{G}_\ell, \mathbb{Z})$. Since the kernel of the map ∂_* (which depends on the choice of orientation on $\mathcal{G}_\ell$) computes $H_1(\mathcal{G}_\ell, \mathbb{Z})$, the proposition follows. (For more details, see [Ed], section 1.)

The character group $\mathcal{X}_\ell$ for $\ell \mid M^+$

Let $X_{\mathbb{Z}_{\ell^2}}$ be (the base change of) the model of X at a prime ℓ dividing exactly M^+, introduced in section 5.1. Let $\mathcal{S}_\ell = \mathcal{S}_\ell(X)$ be the set of supersingular points of the special fiber $X_{\mathbb{F}_{\ell^2}}$. By the facts recalled in section 5.1, $\mathcal{S}_\ell$ is equal to $\mathcal{E}(\mathcal{G}_\ell)$; furthermore, $\mathcal{V}(\mathcal{G}_\ell)$ contains two elements, say v_1 and v_2. Fix an orientation on $\mathcal{G}_\ell$ so that $s(e) = v_1$ and $t(e) = v_2$ for all edges e.

Proposition 5.3 *The character group $\mathcal{X}_\ell$ is identified with the group $\mathbb{Z}[\mathcal{S}_\ell]^0$ of degree zero divisors with $\mathbb{Z}$-coefficients supported on $\mathcal{S}_\ell$.*

Proof: In view of the above remarks, proposition 5.3 follows directly from proposition 5.2.

The character group $\mathcal{X}_\ell$ for $\ell \mid M^-$
Let $\mathcal{T}_\ell$ be the Bruhat-Tits tree of $\mathbf{PGL}_2(\mathbb{Q}_\ell)$.

Proposition 5.4 *The dual graph $\mathcal{G}_\ell$ is identified with $\mathcal{T}_\ell/\Gamma_{\ell,1}$.*

Proof: It follows from theorem 5.1, using the fact that $\mathcal{T}_\ell$ is identified with the dual graph of the special fiber of the formal scheme $\hat{\mathcal{H}}_\ell$ (see [BC], ch. I).

From now on, fix the following orientation on $\mathcal{E}(\mathcal{G}_\ell)$. Let v_0 be the vertex of $\mathcal{T}_\ell$ corresponding to the local maximal order $M_2(\mathbb{Z}_\ell)$. Say that a vertex of $\mathcal{T}_\ell$ is *even* or *odd* depending on whether its distance from v_0 is even or odd, respectively. Since the elements of $\Gamma_{\ell,1}$ have determinant 1, they send even vertices of $\mathcal{T}_\ell$ to even ones, and odd vertices to odd ones. Thus, there is a well defined notion of even and odd vertex for the quotient graph $\mathcal{G}_\ell$. Define the source and target maps $s, t : \mathcal{E}(\mathcal{G}_\ell) \to \mathcal{V}(\mathcal{G}_\ell)$ so that $s(e)$ is the even vertex of e and $t(e)$ is the odd vertex of e.

Write δ_* for the restriction to $\mathbb{Z}[\mathcal{E}(\mathcal{G}_\ell)]^0$ of the map ∂_* (relative to the above choice of orientation).

Proposition 5.5 *The module $\mathcal{X}_\ell$ fits into the exact sequence*

$$0 \to \mathcal{X}_\ell \to \mathbb{Z}[\mathcal{E}(\mathcal{G}_\ell)]^0 \xrightarrow{\delta_*} \mathbb{Z}[\mathcal{V}(\mathcal{G}_\ell)]^0.$$

Proof: By the choice of orientation made above, the elements of $H_1(\mathcal{G}_\ell, \mathbb{Z})$ belong to $\mathbb{Z}[\mathcal{E}(\mathcal{G}_\ell)]^0$. Proposition 5.5 follows directly from proposition 5.2.

5.4 Hecke operators and the Jacquet-Langlands correspondence

(References: see [Ri1], [Ri2] and [JoLi3].)
Assume that M^- is strictly greater than 1, and let ℓ be a prime dividing M^-. This section is concerned with the study of natural families of Hecke operators acting on the terms of the exact sequence of proposition 5.5. The natural

Hecke algebra acting by Picard functoriality on the jacobian $J = \mathrm{Pic}^0(X)$ induces an action on the character group $\mathcal{X}_\ell$. On the other hand, in order to define an action of Hecke operators on $\mathbb{Z}[\mathcal{E}(\mathcal{G}_\ell)]^0$ and $\mathrm{Im}(\delta_*)$, one must use the interpretation of these modules in terms of double coset spaces provided by lemma 5.6.

Remark: A Hecke correspondence T on X induces endomorphisms T and ξ of J via Picard (contravariant) and Albanese (covariant) functoriality. The reader is referred to the discussion in [Ri2], pp. 445-6 for details on the definitions. Unless stated otherwise, the Hecke actions considered in this section and in the following ones will be induced from the Hecke action on J obtained from Picard functioriality. If $w_{M^+,1}$ denotes the Atkin-Lehner involution defined in [BD1], section 1.5, the relation

$$w_{M^+,1} T w_{M^+,1} = \xi$$

holds. (This can be seen by imitating the arguments in proposition 3.54 of [Sh].) In particular, the Hecke operators corresponding to the primes which do not divide M^+ induce the same endomorphism via Picard and Albanese functoriality. (For the primes dividing M^-, this can also be checked by observing that the corresponding Hecke operators are involutions; in this case, a general property of curves shows that the two functorialities induce the same endomorphism.) In view of the above remarks, the detailed discussion of Hecke actions contained in chapters 3 and 4 of [Ri2] extends to the more general setting of this paper.

Let B, R and κ_ℓ be as in section 5.2, and let $\underline{R}$ be the Eichler order of level M^+ which contains R and is mapped by κ_ℓ to $M_2(\mathbb{Z}_\ell)$. Use the notations of formula (12).

Lemma 5.6 *1. The set $\mathcal{E}(\mathcal{G}_\ell)$ is identified with the double coset space $\hat{R}^\times \backslash \hat{B}^\times / B^\times$.*

2. The set $\mathcal{V}(\mathcal{G}_\ell)$ is identified with the disjoint union $\left(\hat{\underline{R}}^\times \backslash \hat{B}^\times / B^\times\right) \times \{0,1\}$ of the double coset space $\hat{\underline{R}}^\times \backslash \hat{B}^\times / B^\times$ with itself.

Proof: Strong approximation (see [Vi], p. 61) yields the identifications

$$\hat{R}^\times \backslash \hat{B}^\times / B^\times = R_\ell^\times \backslash B_\ell^\times / R[\frac{1}{\ell}]^\times, \quad \hat{\underline{R}}^\times \backslash \hat{B}^\times / B^\times = \underline{R}_\ell^\times \backslash B_\ell^\times / R[\frac{1}{\ell}]^\times.$$

Let $\tilde{\mathcal{G}}_\ell$ be the graph $\mathcal{T}_\ell/\Gamma_\ell$, and let $\vec{\mathcal{E}}(\tilde{\mathcal{G}}_\ell)$ be the set of oriented edges of $\tilde{\mathcal{G}}_\ell$. Using the map κ_ℓ, one obtains the identifications

$$\hat{R}^\times\backslash\hat{B}^\times/B^\times = \vec{\mathcal{E}}(\tilde{\mathcal{G}}_\ell), \quad \hat{\underline{R}}^\times\backslash\hat{B}^\times/B^\times = \mathcal{V}(\tilde{\mathcal{G}}_\ell).$$

To conclude, observe that $\mathcal{E}(\mathcal{G}_\ell)$ is identified with $\vec{\mathcal{E}}(\tilde{\mathcal{G}}_\ell)$ by mapping the unoriented edge $\{v,w\}$ (mod $\Gamma_{\ell,1}$) to the oriented edge (v,w) (mod Γ_ℓ) if v is even, and to (w,v) (mod Γ_ℓ) if v is odd (see [BD4], lemma 2.2 for more details). Moreover, the disjoint union $\mathcal{V}(\tilde{\mathcal{G}}_\ell)\times\{0,1\}$ is identified with $\mathcal{V}(\mathcal{G}_\ell)$ by mapping $(\tilde{v},0)$ to the even lift of $\tilde{v}$ and $(\tilde{v},1)$ to the odd lift of $\tilde{v}$, under the natural projection $\mathcal{V}(\mathcal{G}_\ell)\to\mathcal{V}(\tilde{\mathcal{G}}_\ell)$.

Let

$$\alpha : \hat{R}^\times\backslash\hat{B}^\times/B^\times \to \hat{\underline{R}}^\times\backslash\hat{B}^\times/B^\times$$

be the natural projection induced by the inclusion $R\subset\underline{R}$. Denote by $\hat{w}$ the element of $\hat{B}^\times$ whose local components away from ℓ are equal to 1, and whose local component at ℓ maps by κ_ℓ to the diagonal matrix $\mathrm{diag}(1,\ell)$. Since the Eichler order $S=\hat{w}\hat{\underline{R}}^\times\hat{w}^{-1}\cap B$ of level M^+ contains R, there is a natural projection from $\hat{R}^\times\backslash\hat{B}^\times/B^\times$ to $\hat{S}^\times\backslash\hat{B}^\times/B^\times$. Call β the composition of this projection with the identification of $\hat{S}^\times\backslash\hat{B}^\times/B^\times$ with $\hat{\underline{R}}^\times\backslash\hat{B}^\times/B^\times$ induced by the assignment $\hat{b}\mapsto\hat{w}^{-1}\hat{b}$.

Let

$$\mathcal{X}'_\ell=\mathbb{Z}[\hat{R}^\times\backslash\hat{B}^\times/B^\times]^0, \quad \text{respectively,} \quad \mathcal{X}''_\ell=\mathbb{Z}[\hat{\underline{R}}^\times\backslash\hat{B}^\times/B^\times]^0$$

be the module of degree zero formal divisors with $\mathbb{Z}$-coefficients supported on $\hat{R}^\times\backslash\hat{B}^\times/B^\times$, respectively, on $\hat{\underline{R}}^\times\backslash\hat{B}^\times/B^\times$.

Define a degeneracy map

$$d_* : \mathcal{X}'_\ell \to (\mathcal{X}''_\ell)^2$$

by extending by linearity the rule $d_*(x)=(\beta(x),0)-(0,\alpha(x))$ for x in $\hat{R}^\times\backslash\hat{B}^\times/B^\times$.

Proposition 5.7 *The modules $\mathbb{Z}[\mathcal{E}(\mathcal{G}_\ell)]^0$ and $\mathrm{Im}(\delta_*)$ of proposition 5.5 are identified with $\mathcal{X}'_\ell$ and $(\mathcal{X}''_\ell)^2$, respectively. Moreover, the map δ_* corresponds under these identifications to d_* (up to sign).*

Proof: Lemma 5.6 implies directly that $\mathbb{Z}[\mathcal{E}(\mathcal{G}_\ell)]^0$ and $\mathrm{Im}(\delta_*)$ are identified with $\mathcal{X}'_\ell$ and with a submodule of $\mathbb{Z}[\underline{\hat{R}}^\times\backslash\hat{B}^\times/B^\times]^2$. A more careful study shows that d_* is surjective, and corresponds to δ_* under the above identifications. Proposition 5.7 follows.

Let $\mathbb{T}$ be the Hecke algebra acting faithfully on $\mathcal{X}_\ell$, induced by the Hecke algebra acting on the jacobian J (by Picard functoriality). The module $\mathbb{Z}[\mathcal{E}(\mathcal{G}_\ell)]^0$ is also endowed with a faithful action of an algebra $\mathbb{T}'$ of Hecke correspondences, coming from its double coset description given in lemma 5.6: see [BD1], section 1.5 and also section 1.1. Similarly, the identification of $\mathrm{Im}(\delta_*)$ with $(\mathcal{X}''_\ell)^2$ equips $\mathrm{Im}(\delta_*)$ with the diagonal action of Hecke operators T''_q for q not dividing M/ℓ, and U''_q for q dividing M/ℓ. Moreover, the quotient $\mathrm{Im}(\delta_*)$ of $\mathbb{Z}[\mathcal{E}(\mathcal{G}_\ell)]^0$ is stable for the induced action of $\mathbb{T}'$: denote by $\mathbb{T}''$ the algebra quotient of $\mathbb{T}'$ acting faithfully on it. Write $\tilde{\mathbb{T}}$ for the polynomial ring with $\mathbb{Z}$-coefficients generated by the indeterminates $\tilde{T}_q$, for primes q not dividing M, and $\tilde{U}_q$, for primes q dividing M. Note that the Hecke algebras $\mathbb{T}$, $\mathbb{T}'$ and $\mathbb{T}''$ are natural quotients of $\tilde{\mathbb{T}}$.

Proposition 5.8 1. *The exact sequence of proposition 5.5 is equivariant for the natural actions of* $\tilde{\mathbb{T}}$ *on* $\mathcal{X}_\ell$, $\mathbb{Z}[\mathcal{E}(\mathcal{G}_\ell)]^0$, *and* $\mathrm{Im}(\delta_*)$ *defined above.*

2. *For* $q \neq \ell$, *the* q*-th Hecke operator* $T'_q \in \mathbb{T}'$ $(q \nmid M)$ *or* $U'_q \in \mathbb{T}'$ $(q|M)$ *acts on* $\mathrm{Im}(\delta_*) \simeq (\mathcal{X}''_\ell)^2$ *via the diagonal action induced by the natural* q*-th Hecke operator* T''_q $(q \nmid M)$ *or* $U''_q \in \mathbb{T}'$ $(q|M)$*, respectively, acting on the double coset space* $\mathcal{X}''_\ell$. *Moreover, the induced action of* $U'_\ell \in \mathbb{T}'$ *on* $\mathrm{Im}(\delta_*)$ *is given by the formula* $(x, y) \mapsto (T''_\ell x - y, \ell x)$, *where* T''_ℓ *is the* ℓ*-th Hecke operator acting on* $\mathcal{X}''_\ell$.

3. *The Hecke algebra* $\mathbb{T}'$ *is isomorphic to the Hecke algebra acting on modular forms of level* M *which are new at* M^-/ℓ. *Its quotient* $\mathbb{T}$, *respectively,* $\mathbb{T}''$ *is isomorphic to the Hecke algebra acting on modular forms of level* M *which are new at* M^-, *respectively, which are new at* M^-/ℓ *and old at* ℓ.

Sketch of proof:

Step 1: Recalling that M^- is divisible by an even number of primes, fix a prime m such that $m \neq \ell$ and $m \mid M^-$. Denote by X', respectively, X'' the Shimura curve $X_{M^+\ell m, M^-/\ell m}$, respectively, $X_{M^+m, M^-/\ell m}$. Write $\mathcal{X}_m(X')$, respectively, $\mathcal{X}_m(X'')$ for the character group of X', respectively, X'' at m. These character groups are described in proposition 5.3: one has

$$\mathcal{X}_m(X') = \mathbb{Z}[\mathcal{S}_m(X')]^0, \quad \mathcal{X}_m(X'') = \mathbb{Z}[\mathcal{S}_m(X'')]^0.$$

Let a be the natural projection from X' to X'', and let b be the composition of the Atkin-Lehner involution at ℓ acting on X' with a. They induce a surjective degeneracy map

$$b_* - a_* : \mathcal{X}_m(X') \to \mathcal{X}_m(X'')^2.$$

The module $\mathcal{X}_m(X')$, respectively, $\mathcal{X}_m(X'')$ is equipped with the action of a Hecke algebra induced by the Hecke algebra acting (by Picard functoriality) on $J' = \mathrm{Pic}^0(X')$, respectively, $J'' = \mathrm{Pic}^0(X'')$. Moreover, $\mathcal{X}_m(X'')^2$ is endowed with a quotient Hecke action, induced by the map $b_* - a_*$.

Step 2: The assignment sending a supersingular modulus to its ring of endomorphisms equipped with an orientation sets up a bijection of $\mathcal{S}_m(X')$, respectively, $\mathcal{S}_m(X'')$ onto the set of $B^\times$-conjugacy classes of oriented Eichler orders in B of level $M^+\ell$, respectively, M^+ (see [BD2], section 2). These conjugacy classes are classified by the elements of the double coset space $\hat{R}^\times \backslash \hat{B}^\times / B^\times$, respectively, $\hat{\underline{R}}^\times \backslash \hat{B}^\times / B^\times$ (see [BD3], section 1). One obtains the isomorphisms

$$\mathcal{X}_m(X') \simeq \mathcal{X}'_\ell, \quad \mathcal{X}_m(X'') \simeq \mathcal{X}''_\ell.$$

It can be checked that the above identifications are Hecke equivariant, and that the degeneracy maps d_* and $b_* - a_*$ coincide (up to sign) under these identifications.

Step 3: The previous steps give a geometric interpretation of the sequence of proposition 5.5 in terms of the Shimura curves X, X' and X''. Then, the proof of proposition 5.8 in the special case where $M^- = \ell m$ is a product of two primes is contained in Ribet's paper [Ri2]: see theorem 3.19, 3.20 and 3.21. The details on the general case are provided in [Ri1].

Let us state for future use the exact sequence of character groups considered in the proof of proposition 5.8.

Proposition 5.9 *Let m be a prime $\neq \ell$ which divides M^-. There is a Hecke equivariant exact sequence*

$$0 \to \mathcal{X}_\ell(X_{M^+,M^-}) \to \mathcal{X}_m(X_{M^+\ell m, M^-/\ell m}) \to \mathcal{X}_m(X_{M^+m, M^-/\ell m})^2 \to 0.$$

Remark: The identification of the group $\mathbb{Z}[\mathcal{E}(\mathcal{G}_\ell)]^0$ with $\mathcal{X}_m(X_{M^+\ell m, M^-/\ell m})$ and of $\mathrm{Im}(\delta_*)$ with $\mathcal{X}_m(X_{M^+m, M^-/\ell m})^2$ can be made entirely canonical. The reader should consult [Ri1] for a thorough discussion of this issue.

Corollary 5.10 *(The Jacquet-Langlands correspondence) The subring of the endomorphism ring of J generated by the natural Hecke correspondences on X is identified with the Hecke algebra acting on cusp forms of level M which are new at M^-.*

Proof: By theorem 5.1, combined with the theory of ℓ-adic uniformization of Mumford and Tate (see [GvdP], chapters VI and VIII), $J = \mathrm{Pic}^0(X)$ has purely toric reduction at ℓ. Hence, the Hecke algebra $\mathbb{T}$ acting on $\mathcal{X}_\ell(X)$ is canonically identified with the Hecke algebra acting on J. The result follows from the interpretation of $\mathbb{T}$ given in proposition 5.8.

5.5 Connected components

Let ℓ be a prime dividing M^-, and let Φ_ℓ be the group of connected components of J at ℓ, defined in section 5.3.

Let us begin by reviewing Grothendieck's description of Φ_ℓ. Let

$$\langle\ ,\ \rangle : \mathcal{X}_\ell \times \mathcal{X}_\ell \to \mathbb{Z}$$

be the natural *monodromy pairing* on $\mathcal{X}_\ell$. It is defined to be the restriction to $\mathcal{X}_\ell$, by the embedding of proposition 5.2, of the diagonal pairing on $\mathbb{Z}[\mathcal{E}(\mathcal{G}_\ell)]$ given by the rule

$$\langle e, e' \rangle = \nu_e \delta_{e,e'},$$

where ν_e is the weight of the edge e defined in section 5.3. Let

$$j : \mathcal{X}_\ell \to \mathcal{X}_\ell^\vee$$

be the map induced by the monodromy pairing, where $\mathcal{X}_\ell^\vee$ denotes the $\mathbb{Z}$-dual of $\mathcal{X}_\ell$. Using the notations introduced before proposition 5.8, note that the map j is $\mathbb{T}$-equivariant, provided that the action of $\mathbb{T}$ on the source of j is induced by Albanese functoriality and the action of $\mathbb{T}$ on the target of j is induced by Picard functoriality. The reader is referred to the remark at the beginning of section 5.4, where these two actions are compared, and to [Ri2], pp. 448-9 for an extended discussion.

Proposition 5.11 *The group Φ_ℓ is canonically identified with the cokernel of j, and hence fits into the Hecke-equivariant exact sequence*

$$0 \to \mathcal{X}_\ell \xrightarrow{j} \mathcal{X}_\ell^\vee \xrightarrow{\tau_\ell} \Phi_\ell \to 0.$$

Proof: See theorem 11.5 and 12.5 of [Groth], and section 1 and 2 of [Ed].

Corollary 5.12 *There is a natural map*

$$\mathbb{Z}[\mathcal{V}(\mathcal{G}_\ell)]^0 \xrightarrow{\omega_\ell} \Phi_\ell.$$

Proof: Recall the exact sequence

$$0 \to \mathcal{X}_\ell \xrightarrow{i} \mathbb{Z}[\mathcal{E}(\mathcal{G}_\ell)] \xrightarrow{\partial_*} \mathbb{Z}[\mathcal{V}(\mathcal{G}_\ell)] \to \mathbb{Z} \to 0$$

of proposition 5.2, where the map from $\mathbb{Z}[\mathcal{V}(\mathcal{G}_\ell)]$ to $\mathbb{Z}$ is the degree map. The free $\mathbb{Z}$-modules $\mathbb{Z}[\mathcal{E}(\mathcal{G}_\ell)]$ and $\mathbb{Z}[\mathcal{V}(\mathcal{G}_\ell)]$ can be identified canonically with their $\mathbb{Z}$-duals, by using their distinguished bases. Taking the $\mathbb{Z}$-dual of the above sequence yields

$$0 \to \mathbb{Z} \to \mathbb{Z}[\mathcal{V}(\mathcal{G}_\ell)] \xrightarrow{\partial^*} \mathbb{Z}[\mathcal{E}(\mathcal{G}_\ell)] \xrightarrow{i^\vee} \mathcal{X}_\ell^\vee \to 0,$$

where the map from $\mathbb{Z}$ to $\mathbb{Z}[\mathcal{V}(\mathcal{G}_\ell)]$ is the diagonal embedding, and ∂^* sends a vertex v to $-\sum_{s(e)=v} e$ if v is even, and to $\sum_{t(e)=v} e$ if v is odd. Let j_0 denote the map from $\mathbb{Z}[\mathcal{E}(\mathcal{G}_\ell)]$ to itself induced by the pairing $\langle\ ,\ \rangle$ defined above. Note that the map j of proposition 5.11 is equal to $i^\vee \circ j_0 \circ i$. Since Φ_ℓ is identified with the cokernel of j, the assignment sending an element x of $\mathbb{Z}[\mathcal{V}(\mathcal{G}_\ell)]^0$ to the element $(\tau_\ell \circ i^\vee \circ j_0)(y)$ of Φ_ℓ, where y is chosen so that $\partial_*(y) = x$, defines the sought-for map ω_ℓ.

Using the notations of proposition 5.8, say that a $\tilde{\mathbb{T}}$-module C is *Eisenstein* if the relations

$$\tilde{T}_q c = (q+1)c \quad \text{ for } q \nmid M$$

hold for all c in C.

Proposition 5.13 *The restriction of the map ω_ℓ of prop. 5.12 to* $\mathrm{Im}(\delta_*)$, *viewed as a submodule of $\mathbb{Z}[\mathcal{V}(\mathcal{G}_\ell)]^0$ via prop. 5.5, induces a $\tilde{\mathbb{T}}$-equivariant map*

$$\bar{\omega}_\ell : \mathrm{Im}(\delta_*)/\big((U_\ell')^2 - 1\big) \to \Phi_\ell.$$

Furthermore, the kernel and cokernel of $\bar{\omega}_\ell$ are Eisenstein.

Remark: The proof of proposition 5.13 follows the argument in the proof of theorem 4.3 of [Ri2], where the result is proved in the special case where M^- is the product of two primes. See also the previous work of Jordan and Livné [JoLi2]. For the details on the Hecke compatibility in the statement of proposition 5.13, see chapters 3 and 4 of [Ri2], particularly remark 3.24, and the remark at the beginning of section 5.4.

Sketch of proof: Let j' be the map from $\mathbb{Z}[\mathcal{E}(\mathcal{G}_\ell)]^0$ to its $\mathbb{Z}$-dual $(\mathbb{Z}[\mathcal{E}(\mathcal{G}_\ell)]^0)^\vee$ induced by the pairing $\langle\ ,\ \rangle$ defined before. Similarly, let

$$\langle\!\langle\ ,\ \rangle\!\rangle : \mathbb{Z}[\mathcal{V}(\mathcal{G}_\ell)] \times \mathbb{Z}[\mathcal{V}(\mathcal{G}_\ell)] \to \mathbb{Z}$$

be the pairing defined by the rule $\langle\!\langle v, v' \rangle\!\rangle = \nu_v \delta_{v,v'}$, where the weight ν_v of the vertex v is defined to be the order of the stabilizer in $\Gamma_{\ell,1}$ of any lift of v to $\mathcal{V}(\mathcal{T}_\ell)$. (Note that the quantity ν_e, defined in a more geometric fashion in section 5.3, could equivalently be defined to be the order of the stabilizer in $\Gamma_{\ell,1}$ of any lift of e to $\mathcal{E}(\mathcal{T}_\ell)$.) Let

$$j'' : \mathrm{Im}(\delta_*) \to \mathrm{Im}(\delta_*)^\vee$$

be the map induced by $\langle\!\langle\ ,\ \rangle\!\rangle$. Fix a prime divisor $m \neq \ell$ of M^-, and let Φ'_m, respectively, Φ''_m denote the group of connected components of the Néron model over $\mathbb{Z}_{m^2}$ of the jacobian of $X_{M^+\ell m, M^-/\ell m}$, respectively, of $X_{M^+m, M^-/\ell m}$. The groups Φ'_m and Φ''_m are Eisenstein. This follows from a generalization to Shimura curves of theorem 3.12 of [Ri2], which can be obtained from the results of [Bu] and [JoLi3]. The analogue of proposition 5.11 applied to the character groups at m of $X_{M^+\ell m, M^-/\ell m}$ and $X_{M^+m, M^-/\ell m}$, respectively (see theorem 11.5 and 12.5 of [Groth], and section 1 and 2 of [Ed]), combined with proposition 5.9 and the proof of proposition 5.8, yields the identifications

$$\Phi'_m = (\mathbb{Z}[\mathcal{E}(\mathcal{G}_\ell)]^0)^\vee / j'(\mathbb{Z}[\mathcal{E}(\mathcal{G}_\ell)]^0), \quad \Phi''_m \times \Phi''_m = \mathrm{Im}(\delta_*)^\vee / j''(\mathrm{Im}(\delta_*)).$$

Let

$$j'_0 : \mathrm{Im}(\delta_*) \to \frac{(\mathbb{Z}[\mathcal{E}(\mathcal{G}_\ell)]^0)^\vee}{j'(i(\mathcal{X}_\ell))}$$

be the composition of the isomorphism of $\mathrm{Im}(\delta_*)$ with $\mathbb{Z}[\mathcal{E}(\mathcal{G}_\ell)]^0/i(\mathcal{X}_\ell)$, induced by δ_*, with the map induced by j'. Set

$$\sigma : \mathrm{Im}(\delta_*) \to \mathrm{Im}(\delta_*), \quad (x, y) \mapsto ((\ell+1)x + T''_\ell y, T''_\ell x + (\ell+1)y).$$

One obtains a commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Im}(\delta_*) & \stackrel{j''}{\longrightarrow} & \mathrm{Im}(\delta_*)^\vee & \longrightarrow & \Phi''_m \times \Phi''_m & \longrightarrow & 0 \\
 & & \downarrow^{\sigma} & & \downarrow^{\delta_*^\vee} & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Im}(\delta_*) & \stackrel{j'_0}{\longrightarrow} & \frac{(\mathbb{Z}[\mathcal{E}(\mathcal{G}_\ell)]^0)^\vee}{j'(i(\mathcal{X}_\ell))} & \longrightarrow & \Phi'_m & \longrightarrow & 0,
\end{array}$$

where $\delta_*^\vee$ is induced by the $\mathbb{Z}$-dual of δ_*. Note that $\delta_*^\vee$ is injective, and its cokernel is identified with Φ_ℓ, in view of proposition 5.11. Moreover, the cokernel of σ is identified with $\mathrm{Im}(\delta_*)/((U'_\ell)^2-1)$. For, a calculation shows that the composition of the isomorphism

$$(x,y) \mapsto (-x, T''_\ell x - y)$$

of $\mathrm{Im}(\delta_*)$ with σ gives the action of $(U'_\ell)^2-1$. Proposition 5.13 follows from the snake lemma applied to the above diagram.

Let $X_{\mathbb{Z}_{\ell^2}}$ be (the base change of) the model of X introduced in section 5.1, and let $X_{\mathbb{F}_{\ell^2}}$ be the special fiber of $X_{\mathbb{Z}_{\ell^2}}$. Write

$$D = \sum_P n_P P \in \mathrm{Div}^0(X)$$

for a degree zero divisor on X with integer coefficients, and $\mathrm{Supp}(D)$ for the support of D. Assume that D satisfies the following assumptions:

1. each $P \in \mathrm{Supp}(D)$ is defined over $\mathbb{Q}_{\ell^2}$,

2. each $P \in \mathrm{Supp}(D)$ reduces modulo ℓ to a point $r_\ell(P)$ which belongs to a unique irreducible component of $X_{\mathbb{F}_{\ell^2}}$ (that is, $r_\ell(P)$ is not a double point in $X_{\mathbb{F}_{\ell^2}}$).

Thus, D determines an element

$$r_\ell(D) = \sum_P n_P r_\ell(P)$$

in $\mathbb{Z}[\mathcal{V}(\mathcal{G}_\ell)]^0$. Consider the specialization map

$$\partial_\ell : J(\mathbb{Q}_{\ell^2}) \to \Phi_\ell.$$

Proposition 5.14 *Let $D \in \mathrm{Div}^0(X)$ be a divisor satisfying the above assumptions, and let $[D] \in J(\mathbb{Q}_{\ell^2})$ be the class of D. Then*

$$\partial_\ell([D]) = \omega_\ell(r_\ell(D)).$$

Proof: It follows from Edixhoven's results in [Ed], section 2. (These results are built on Raynaud's description of ∂_ℓ in terms of the minimal model of X over $\mathbb{Z}_{\ell^2}$, given in [Ray].)

5.6 Raising the level and groups of connected components

Let $f : \vec{\mathcal{E}}(\mathcal{T})/\Gamma \to \mathbb{Z}_p$ be a form on $\mathcal{T}/\Gamma$, defined as in section 1. Thus, f is attached to an integer factorization $N = N^+N^-$, where N^- is squarefree and divisible by an odd number of primes and N^+ is divisible by p. (Note that this differs slightly from the notation of section 1, where N was written as pN^+N^- and N^+ was assumed to be prime to p.)

Let m be a distinguished prime divisor of N^-. In what follows, ℓ denotes a prime number which does not divide N. Write $\mathbb{T} = \mathbb{T}_{N^+,N^-}$, respectively, $\mathbb{T}_\ell = \mathbb{T}_{N^+,N^-\ell}$ for the Hecke algebra acting on cusp forms on $\Gamma_0(N)$, respectively, on $\Gamma_0(N\ell)$, which are new at N^-, respectively, at $N^-\ell$. Denote by t_q and u_q, respectively, T_q and U_q the Hecke operators in $\mathbb{T}$, respectively, in $\mathbb{T}_\ell$.

The form f yields a surjective homomorphism

$$f : \mathbb{T} \to \mathbb{Z}/p^n\mathbb{Z}$$

(still denoted by f by an abuse of notation). Write $\mathcal{I}_f$ for the kernel of f, and $\mathfrak{m}_f$ for the unique proper maximal ideal of $\mathbb{T}$ containing $\mathcal{I}_f$.

In view of corollary 5.10, $\mathbb{T}$ can be identified with the m-new quotient of the Hecke algebra $\mathbb{T}_{N^+m,N^-/m}$ acting faithfully on $X_{N^+m,N^-/m}$. Since the character group $\mathcal{X}_m(X_{N^+m,N^-/m})$ arises from the m-new part of $J_{N^+m,N^-/m}$, it follows that $\mathbb{T}$ acts naturally on it (by Picard functoriality).

Theorem 5.15 *Assume:*

1. *$\mathfrak{m}_f$ is residually irreducible,*

2. *the completion* $\mathcal{X}_m(X_{N^+m,N^-/m})_{\mathfrak{m}_f}$ *of* $\mathcal{X}_m(X_{N^+m,N^-/m})$ *at* $\mathfrak{m}_f$ *is free of rank* 1 *over the completed Hecke algebra* $\mathbb{T}_{\mathfrak{m}_f}$,

3. ℓ *is a* n*-admissible prime relative to* f.

Then:

1. *There exists a surjective homomorphism*

$$f_\ell : \mathbb{T}_\ell \to \mathbb{Z}/p^n\mathbb{Z}$$

such that $f_\ell(T_q) = f(t_q)$ *for all* $q \nmid N\ell$, $f_\ell(U_q) = f(u_q)$ *for all* $q \mid N$, *and* $f_\ell(U_\ell) = \epsilon$, *where* $\epsilon = \pm 1$ *is such that* p^n *divides* $\ell + 1 - \epsilon f(t_\ell)$.

2. *Let* $\mathcal{I}_{f_\ell} \subset \mathbb{T}_\ell$ *denote the kernel of the homomorphism* f_ℓ, *and let* Φ_ℓ *denote the group of connected components of the Néron model of* $J_{N^+,N^-\ell}$ *over* $\mathbb{Z}_{\ell^2}$, *defined in section 5.3. There is a group isomorphism*

$$\Phi_\ell/\mathcal{I}_{f_\ell} \simeq \mathbb{Z}/p^n\mathbb{Z}.$$

Remark. Compare the proof of theorem 5.15 with section 7 of [Ri2], in which the special case where M^- is a product of two primes and $\mathcal{I}_f = \mathfrak{m}_f$ is a maximal ideal is treated.

Proof: The second assumption implies the existence of an isomorphism

$$\mathcal{X}_m(X_{N^+m,N^-/m})^2/\mathcal{I}_f \simeq (\mathbb{Z}/p^n\mathbb{Z})^2.$$

Write T'_q and U'_q for the Hecke operators in $\mathbb{T}_{N^+\ell,N^-}$. By proposition 5.9 and proposition 5.8, there is an action of $\mathbb{T}_{N^+\ell,N^-}$ on $\mathcal{X}_m(X_{N^+m,N^-/m})^2$, induced by the diagonal action of t_q for $q \nmid N\ell$ and u_q for $q \mid N$, and such that the Hecke operator U'_ℓ acts via the formula

$$(x, y) \mapsto (t_\ell x - y, \ell x).$$

Since ℓ is n-admissible, t_ℓ is equal modulo $\mathcal{I}_f$ to $\epsilon(\ell + 1)$. By combining this relation with the above formula for the action of U'_ℓ and with the fact that $p \geq 5$, one obtains that $U'_\ell + \epsilon$ is invertible on $\mathcal{X}_m(X_{N^+m,N^-/m})^2/\mathcal{I}_f$, and that the isomorphisms

$$\mathcal{X}_m(X_{N^+m,N^-/m})^2/\langle \mathcal{I}_f, U'_\ell - \epsilon\rangle \simeq \mathcal{X}_m(X_{N^+m,N^-/m})^2/\langle \mathcal{I}_f, (U'_\ell)^2 - 1\rangle \simeq \mathbb{Z}/p^n\mathbb{Z}$$

hold. Hence, the action of $\mathbb{T}_{N^+\ell,N^-}$ on the above quotient is via a surjective homomorphism

$$f_\ell{}' : \mathbb{T}_{N^+\ell,N^-} \to \mathbb{Z}/p^n\mathbb{Z}.$$

Write $\mathcal{I}_{f_\ell{}'}$ for the kernel of $f_\ell{}'$. By proposition 5.13 and the residual irreducibility of $\mathfrak{m}_f$, combined with proposition 5.9 and the remark after it, one finds an isomorphism

$$\Phi_\ell/\mathcal{I}_{f_\ell{}'} \simeq \mathcal{X}_m(X_{N^+m,N^-/m})^2/\langle \mathcal{I}_f, (U'_\ell)^2 - 1\rangle.$$

It follows that $f_\ell{}'$ factors through $\mathbb{T}_\ell$, giving the sought for character f_ℓ, and that $\Phi_\ell/\mathcal{I}_{f_\ell}$ is isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$.

Write $X^{(\ell)}$ for the Shimura curve $X_{N^+,N^-\ell}$, $J^{(\ell)}$ for the jacobian of $X^{(\ell)}$, and $\mathrm{Pic}(X^{(\ell)})$ for the Picard variety of $X^{(\ell)}$. Denote by $\mathcal{X}_\ell$ the character group of $J^{(\ell)}$ at ℓ, and by $\mathrm{Ta}_p(J^{(\ell)})$ the p-adic Tate module of $J^{(\ell)}$. Note that the Hecke algebra $\mathbb{T}_\ell$ acts faithfully on $J^{(\ell)}$.

Lemma 5.16 *Under the assumptions of theorem 5.15, the exponent of the $\mathbb{Z}$-module $\mathrm{Ta}_p(J^{(\ell)})/\mathcal{I}_{f_\ell}$ is equal to p^n.*

Proof: Since $\mathrm{Ta}_p(J^{(\ell)})/\mathcal{I}_{f_\ell}$ is naturally a $\mathbb{T}_\ell/\mathcal{I}_{f_\ell}$-module, and $\mathbb{T}_\ell/\mathcal{I}_{f_\ell}$ is isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$, it follows that the exponent of $\mathrm{Ta}_p(J^{(\ell)})/\mathcal{I}_{f_\ell}$ is at most p^n. On the other hand, the Mumford-Tate theory of ℓ-adic uniformization, combined with the Cerednik-Drinfeld theorem, (see section 5.2 and [GvdP], chapters VI and VIII) shows the existence of a symmetric pairing

$$[\ ,\ ] : \mathcal{X}_\ell \times \mathcal{X}_\ell \to \mathbb{Q}_\ell^\times \tag{47}$$

such that there exists an exact sequence of $\mathbb{T}_\ell[\mathrm{Gal}(\bar{\mathbb{Q}}_{\ell^2}/\mathbb{Q}_{\ell^2})]$-modules

$$0 \to \mathcal{X}_\ell \xrightarrow{\tilde{j}} \mathcal{X}_\ell^\vee \otimes \bar{\mathbb{Q}}_{\ell^2}^\times \to J^{(\ell)}(\bar{\mathbb{Q}}_{\ell^2}) \to 0, \tag{48}$$

where $\mathcal{X}_\ell^\vee$ denotes the $\mathbb{Z}$-dual $\mathrm{Hom}(\mathcal{X}_\ell, \mathbb{Z})$ of $\mathcal{X}_\ell$, and where the map $\tilde{j}$ is induced by $[\ ,\ ]$. The sequence (48) is Hecke-equivariant, provided that the action of $\mathbb{T}_\ell$ on the first term is induced by Albanese functoriality, and the action on the second and third term is induced by Picard functoriality. Note also that the need of extending scalars to $\mathbb{Q}_{\ell^2}$ in (48) arises from the fact that the isomorphism of rigid spaces stated in theorem 5.1 is only defined over $\mathbb{Q}_{\ell^2}$ and not over $\mathbb{Q}_\ell$. The pairing $[\ ,\ ]$ is related to monodromy pairing of section 5.5 by the rule

$$\mathrm{ord}_\ell \circ [\ ,\ ] = \langle\ ,\ \rangle \tag{49}$$

(see [M], theorem 7.6). In view of theorem 5.15, choose an element c of $\Phi_\ell/\mathcal{I}_{f_\ell}$ of order p^n, and lift c to an element $\tilde{c}$ of Φ_ℓ of p-power order $p^{n'}$, with $n' \geq n$. In view of proposition 5.11, fix an element $b \in \mathcal{X}_\ell^\vee$ such that $\tau_\ell(b) = \tilde{c}$, and let a be the element of $\mathcal{X}_\ell$ such that $p^{n'}b = j(a)$. Formula (49) shows that ord_ℓ of the period $\tilde{j}(a) \in \mathcal{X}_\ell^\vee \otimes \tilde{\mathbb{Q}}_\ell^\times$ is divisible by $p^{n'}$. Thanks to the sequence (48), the choice of a $p^{n'}$-root of $\tilde{j}(a)$ determines an element $\tilde{t}$ of $J^{(\ell)}[p^{n'}]$ defined over an unramified extension of $\mathbb{Q}_\ell$, whose natural image in Φ_ℓ is equal to $\tilde{c}$. Writing t for the image of $\tilde{t}$ in $J^{(\ell)}[p^{n'}]/\mathcal{I}_{f_\ell}$, then the natural image of t in $\Phi_\ell/\mathcal{I}_{f_\ell}$ is equal to c. Since

$$\mathrm{Ta}_p(J^{(\ell)})/\mathcal{I}_{f_\ell} = J^{(\ell)}[p^{n'}]/\mathcal{I}_{f_\ell},$$

it follows that t is an element of order $\geq p^n$ in $\mathrm{Ta}_p(J^{(\ell)})/\mathcal{I}_{f_\ell}$. Since the exponent of $\mathrm{Ta}_p(J^{(\ell)})/\mathcal{I}_{f_\ell}$ is at most p^n, this proves lemma 5.16.

Theorem 5.17 *Under the assumptions of theorem 5.15, the Galois representations* $\mathrm{Ta}_p(J^{(\ell)})/\mathcal{I}_{f_\ell}$ *and* $T_{f,n}$ *are isomorphic.*

Proof: Let $\mathfrak{m}_{f_\ell}$ be the maximal ideal in $\mathbb{T}_\ell$ containing $\mathcal{I}_{f_\ell}$. (Thus, $\mathbb{T}_\ell/\mathfrak{m}_{f_\ell}$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.) The proof is naturally divided into two steps. In the first step, one works modulo $\mathfrak{m}_{f_\ell}$, and a known result of [BoLeRi] on the structure of $\mathrm{Ta}_p(J^{(\ell)})/\mathfrak{m}_{f_\ell}$ is invoked.

Step 1. This first step shows that $\mathrm{Ta}_p(J^{(\ell)})/\mathfrak{m}_{f_\ell}$ is isomorphic to $T_{f,1}$. Taking p-torsion in the sequence (48) yields the exact sequence of $\mathbb{T}_\ell[\mathrm{Gal}(\bar{\mathbb{Q}}_{\ell^2}/\mathbb{Q}_{\ell^2})]$-modules

$$0 \to \mathcal{X}_\ell^\vee \otimes \mu_p \to J^{(\ell)}[p] \to \mathcal{X}_\ell/p \to 0. \tag{50}$$

After tensoring (50) with $\mathbb{T}_\ell/\mathfrak{m}_{f_\ell}$, one finds

$$0 \to ((\mathcal{X}_\ell^\vee/\mathfrak{m}_{f_\ell})/\mathcal{Y}) \otimes \mu_p \to J^{(\ell)}[p]/\mathfrak{m}_{f_\ell} \to \mathcal{X}_\ell/\mathfrak{m}_{f_\ell} \to 0, \tag{51}$$

where $\mathcal{Y}$ is a certain submodule of $\mathcal{X}_\ell^\vee/\mathfrak{m}_{f_\ell}$. Taking Galois cohomology over $\mathbb{Q}_{\ell^2}$ of (51) yields an exact sequence

$$\mathcal{X}_\ell/\mathfrak{m}_{f_\ell} \to H^1(\mathbb{Q}_{\ell^2}, ((\mathcal{X}_\ell^\vee/\mathfrak{m}_{f_\ell})/\mathcal{Y}) \otimes \mu_p) \to \tag{52}$$

$$\to H^1(\mathbb{Q}_{\ell^2}, J^{(\ell)}[p]/\mathfrak{m}_{f_\ell}) \to H^1(\mathbb{Q}_{\ell^2}, \mathcal{X}_\ell/\mathfrak{m}_{f_\ell}).$$

Note the identifications

$$H^1(\mathbb{Q}_{\ell^2}, ((\mathcal{X}_\ell^\vee/\mathfrak{m}_{f_\ell})/\mathcal{Y}) \otimes \mu_p) = ((\mathcal{X}_\ell^\vee/\mathfrak{m}_{f_\ell})/\mathcal{Y}) \otimes H^1(\mathbb{Q}_{\ell^2}, \mu_p) =$$

$$((\mathcal{X}_\ell^\vee/\mathfrak{m}_{f_\ell})/\mathcal{Y}) \otimes \mathbb{Q}_{\ell^2}^\times/(\mathbb{Q}_{\ell^2}^\times)^p = (\mathcal{X}_\ell^\vee/\mathfrak{m}_{f_\ell})/\mathcal{Y}, \tag{53}$$

where the last equality follows from the fact that ℓ is an admissible prime and hence $p \not| \ell^2 - 1$. Moreover, $J^{(\ell)}[p]/\mathfrak{m}_{f_\ell} = \mathrm{Ta}_p(J^{(\ell)})/\mathfrak{m}_{f_\ell}$, and

$$H^1(\mathbb{Q}_{\ell^2}, \mathcal{X}_\ell/\mathfrak{m}_{f_\ell}) = \mathrm{Hom}_{\mathrm{unr}}(\mathrm{Gal}(\bar{\mathbb{Q}}_{\ell^2}/\mathbb{Q}_{\ell^2}), \mathcal{X}_\ell/\mathfrak{m}_{f_\ell}) = \mathrm{Hom}(\mathbb{Z}/p\mathbb{Z}, \mathcal{X}_\ell/\mathfrak{m}_{f_\ell})$$

by local class field theory, since $p \not| \ell^2 - 1$. Thus, (52) can be re-written as

$$\mathcal{X}_\ell/\mathfrak{m}_{f_\ell} \to (\mathcal{X}_\ell^\vee/\mathfrak{m}_{f_\ell})/\mathcal{Y} \to H^1(\mathbb{Q}_{\ell^2}, \mathrm{Ta}_p(J^{(\ell)})/\mathfrak{m}_{f_\ell}) \to H^1_{\mathrm{unr}}(\mathbb{Q}_{\ell^2}, \mathcal{X}_\ell/\mathfrak{m}_{f_\ell}). \tag{54}$$

The first map in (54) is induced by the monodromy pairing on $\mathcal{X}_\ell$: this follows from the definition of the sequence (48) which induces (54); see also the proposition on page IV-32 of [Se2], which covers a special case. By proposition 5.11, one obtains the exact sequence

$$0 \to \bar{\Phi}_\ell/\mathfrak{m}_{f_\ell} \to H^1(\mathbb{Q}_{\ell^2}, \mathrm{Ta}_p(J^{(\ell)})/\mathfrak{m}_{f_\ell}) \to H^1_{\mathrm{unr}}(\mathbb{Q}_{\ell^2}, \mathcal{X}_\ell/\mathfrak{m}_{f_\ell}), \tag{55}$$

where $\bar{\Phi}_\ell/\mathfrak{m}_{f_\ell}$ is a quotient of $\Phi_\ell/\mathfrak{m}_{f_\ell}$. By the main result of [BoLeRi], the module $\mathrm{Ta}_p(J^{(\ell)})/\mathfrak{m}_{f_\ell}$ is semisimple over $\mathbb{F}_p[\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})]$, and hence is isomorphic to $k \geq 1$ copies of $T_{f,1}$ by the Eichler-Shimura relations. Hence, $H^1(\mathbb{Q}_{\ell^2}, \mathrm{Ta}_p(J^{(\ell)})/\mathfrak{m}_{f_\ell})$ is isomorphic to $H^1(\mathbb{Q}_{\ell^2}, T_{f,1})^k$. In view of the results of section 2.2, the $\mathbb{F}_p$-vector space $H^1(\mathbb{Q}_{\ell^2}, T_{f,1})^k$ is $2k$-dimensional; furthermore, it can be decomposed as the direct sum of two k-dimensional subspaces, one of which generated by unramified cohomology classes, and the other by ramified cohomology classes. Since $\Phi_\ell/\mathfrak{m}_{f_\ell}$ is 1-dimensional by theorem 5.15, it follows from (55) and the proof of lemma 2.6 that $\bar{\Phi}_\ell/\mathfrak{m}_{f_\ell}$ is equal to $\Phi_\ell/\mathfrak{m}_{f_\ell}$, and that k is equal to 1. Hence $\mathrm{Ta}_p(J^{(\ell)})/\mathfrak{m}_{f_\ell}$ is isomorphic to $T_{f,1}$.

Step 2. It remains to show that $\mathrm{Ta}_p(J^{(\ell)})/\mathcal{I}_{f_\ell}$ is isomorphic to $T_{f,n}$. There is a natural $G_{\mathbb{Q}}$-equivariant projection

$$\mathrm{Ta}_p(J^{(\ell)})/\mathcal{I}_{f_\ell} \xrightarrow{\pi} \mathrm{Ta}_p(J^{(\ell)})/\mathfrak{m}_{f_\ell}. \tag{56}$$

In view of lemma 5.16, let t be an element of order p^n in $\mathrm{Ta}_p(J^{(\ell)})/\mathcal{I}_{f_\ell}$, and let $\bar{t} = \pi(t)$. Since $T_{f,1}$ is irreducible, there is an element $g \in G_{\mathbb{Q}}$ such that $\bar{t}$ and $\bar{t}^g$ are a basis for $\mathrm{Ta}_p(J^{(\ell)})/\mathfrak{m}_{f_\ell}$. Nakayama's lemma shows that $\mathrm{Ta}_p(J^{(\ell)})/\mathcal{I}_{f_\ell}$ is generated by t and t^g. Moreover, since g acts as an automorphism of $\mathrm{Ta}_p(J^{(\ell)})/\mathcal{I}_{f_\ell}$, the order of t^g is equal to the order of t. Finally, using the assumption made in the introduction that the Galois representation $T_{f,1}$ has image isomorphic to $\mathbf{GL}_2(\mathbb{F}_p)$, one checks directly that the submodules generated by t and t^g have trivial intersection, so that $\mathrm{Ta}_p(J^{(\ell)})/\mathcal{I}_{f_\ell}$ is isomorphic to $(\mathbb{Z}/p^n\mathbb{Z})^2$. This implies that $\mathrm{Ta}_p(J^{(\ell)})/\mathcal{I}_{f_\ell}$ is isomorphic to $T_{f,n}$.

Remark:

1. Repeating the argument in the proof of the first step of theorem 5.17, with p^n replacing p and the ideal $\mathcal{I}_{f_\ell}$ replacing $\mathfrak{m}_{f_\ell}$, yields the exact sequence (analogue of (55))

$$0 \to \bar{\Phi}_\ell/\mathcal{I}_{f_\ell} \to H^1(K_\ell, \mathrm{Ta}_p(J^{(\ell)})/\mathcal{I}_{f_\ell}) \to H^1_{\mathrm{unr}}(K_\ell, \mathcal{X}_\ell/\mathcal{I}_{f_\ell}), \tag{57}$$

where $\bar{\Phi}_\ell/\mathcal{I}_{f_\ell}$ is a quotient of $\Phi_\ell/\mathcal{I}_{f_\ell}$. This exact sequence will be of use in the proof of corollary 5.18.

2. In view of remark 1, equations (48) and (53), with $\mathcal{I}_{f_\ell}$ replacing $\mathfrak{m}_{f_\ell}$, show that the natural Kummer map from $J^{(\ell)}(K_\ell)$ to $H^1(K_\ell, \mathrm{Ta}_p(J^{(\ell)})/\mathcal{I}_{f_\ell})$ factors through the map of specialization to connected components from $J^{(\ell)}(K_\ell)$ to $\bar{\Phi}_\ell/\mathcal{I}_{f_\ell}$.

Recall the quadratic imaginary field K introduced in the previous sections. Note that the n-admissible prime ℓ is inert in K by definition, so that the completion K_ℓ is isomorphic to $\mathbb{Q}_{\ell^2}$. Given $m \geq 0$, let $\mathcal{O}_m = \mathbb{Z} + p^{m+1}\mathcal{O}_K$ be the order of K of conductor p^{m+1}. Let $\tilde{K}_m$ be the ring class field of K of conductor p^{m+1}, and let $\tilde{K}_\infty$ be the union of the $\tilde{K}_m$. (The field $\tilde{K}_\infty$ was introduced in section 2.1.) The field $\tilde{K}_m$ can be constructed by adjoining to K the value $j(\mathcal{O}_m)$ of the modular function j (viewed as a function of lattices) on $\mathcal{O}_m$. By the theory of complex multiplication, $\tilde{K}_m$ is an abelian extension of K, which contains the Hilbert class field $\tilde{K}$ of K. The Galois group of $\tilde{K}_m$ over $\tilde{K}$ is cyclic, of order $p^m(p-\epsilon(p))/u$, where $\epsilon(p)$ is equal to 1 or -1 depending on whether p is split or inert in K, respectively, and where u denotes half the order of the group of units of K. Write $\tilde{G}_m$ for the Galois group of $\tilde{K}_m$ over K, and $\tilde{G}_\infty$ for the Galois group of $\tilde{K}_\infty$ over K. By class field theory, the Galois group $\tilde{G}_\infty$ is identified with the group $\tilde{G}_\infty$ defined in section 1.2 in terms of the ideles of K.

Write $\Phi_{\ell,m}$, respectively, $\Phi'_{\ell,m}$ for $\oplus_{\lambda|\ell}\Phi_\lambda$, where the sum is taken over the primes λ of K_m and of $\tilde{K}_m$ dividing ℓ, respectively, and Φ_λ denotes the group of connected components of $J^{(\ell)}$ at λ. Define $\hat{\Phi}_\ell$, respectively, $\tilde{\Phi}_\ell$ to be the inverse limit of the groups $\Phi_{\ell,m}$, respectively, $\Phi'_{\ell,m}$ with respect to the norm maps. Since the prime ℓ is inert in K, it splits completely in $\tilde{K}_\infty/K$. Hence, the choice of a prime of $\tilde{K}_\infty$ above ℓ identifies $\hat{\Phi}_\ell$ with $\Phi_\ell\otimes\mathbb{Z}[\![G_\infty]\!]$, and $\tilde{\Phi}_\ell$ with $\Phi_\ell\otimes\mathbb{Z}[\![\tilde{G}_\infty]\!]$. It follows that the identification of $\Phi_\ell/\mathcal{I}_{f_\ell}$ with $\mathbb{Z}/p^n\mathbb{Z}$ of theorem 5.15 yields isomorphisms

$$\hat{\Phi}_\ell/\mathcal{I}_{f_\ell}\simeq\Lambda/p^n\Lambda,\qquad \tilde{\Phi}_\ell/\mathcal{I}_{f_\ell}\simeq\mathbb{Z}/p^n[\![\tilde{G}_\infty]\!].$$

Write $\hat{J}^{(\ell)}(K_\infty)/\mathcal{I}_{f_\ell}$, respectively, $\hat{J}^{(\ell)}(\tilde{K}_\infty)/\mathcal{I}_{f_\ell}$ for the inverse limit of the modules $J^{(\ell)}(K_{m,\ell})/\mathcal{I}_{f_\ell}$, respectively, $J^{(\ell)}(\tilde{K}_{m,\ell})/\mathcal{I}_{f_\ell}$ with respect to the norm maps. The inverse limit of the maps of specialization to connected components yields the maps

$$\hat{\partial}_\ell:\hat{J}^{(\ell)}(K_\infty)/\mathcal{I}_{f_\ell}\to\hat{\Phi}_\ell/\mathcal{I}_{f_\ell}\simeq\Lambda/p^n, \tag{58}$$

$$\tilde{\partial}_\ell:\hat{J}^{(\ell)}(\tilde{K}_\infty)/\mathcal{I}_{f_\ell}\to\tilde{\Phi}_\ell/\mathcal{I}_{f_\ell}\simeq\mathbb{Z}/p^n[\![\tilde{G}_\infty]\!]. \tag{59}$$

Corollary 5.18 *1. There is an isomorphism*

$$\Phi_\ell/\mathcal{I}_{f_\ell}\to H^1_{\mathrm{sing}}(K_\ell,T_{f,n}),$$

which is canonical up to the choice of an identification of $\mathrm{Ta}_p(J^{(\ell)})/\mathcal{I}_{f_\ell}$ *with* $T_{f,n}$.

2. There is an isomorphism

$$\hat{\Phi}_\ell/\mathcal{I}_{f_\ell} \to \hat{H}^1_{\mathrm{sing}}(K_{\infty,\ell}, T_{f,n}),$$

which is canonical up to the choice of an identification of $\mathrm{Ta}_p(J^{(\ell)})/\mathcal{I}_{f_\ell}$ *with* $T_{f,n}$.

3. There is a commutative diagram

$$\begin{array}{ccc} \hat{J}^{(\ell)}(K_\infty)/\mathcal{I}_{f_\ell} & \longrightarrow & \hat{H}^1(K_\infty, T_{f,n}) \\ \downarrow^{\hat{\partial}_\ell} & & \downarrow^{\partial_\ell} \\ \hat{\Phi}_\ell/\mathcal{I}_{f_\ell} & \longrightarrow & \hat{H}^1_{\mathrm{sing}}(K_{\infty,\ell}, T_{f,n}), \end{array}$$

where the top horizontal arrow arises from the natural Kummer map, the lower horizontal arrow is the isomorphism defined above, and ∂_ℓ is the residue map defined in section 2.2. Furthermore, there is a similar commutative diagram having the group $\hat{J}^{(\ell)}(\tilde{K}_\infty)/\mathcal{I}_{f_\ell}$ as its source.

Proof: By theorem 5.17, $\mathrm{Ta}_p(J^{(\ell)})/\mathcal{I}_{f_\ell}$ is isomorphic to $T_{f,n}$. Hence, by the results of section 2.2, $H^1(K_\ell, \mathrm{Ta}_p(J^{(\ell)})/\mathcal{I}_{f_\ell})$ is free of rank two over $\mathbb{Z}/p^n\mathbb{Z}$; moreover, its submodule of unramified classes has rank one. By theorem 5.15, $\Phi_\ell/\mathcal{I}_{f_\ell}$ is isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$. The exact sequence (57) shows that all the elements of $\bar{\Phi}_\ell/\mathcal{I}_{f_\ell}$ map to ramified classes. It follows that $\bar{\Phi}_\ell/\mathcal{I}_{f_\ell}$ is equal to $\Phi_\ell/\mathcal{I}_{f_\ell}$. Furthermore, the residue map induces a surjection of $\Phi_\ell/\mathcal{I}_{f_\ell}$ onto the rank one group $H^1_{\mathrm{sing}}(K_\ell, T_{f,n})$. This defines the isomorphism stated in part one of corollary 5.18. The second part is a formal consequence of the first. The third part follows from the definition of the isomorphism in part two, combined with the remark 2 after the proof of theorem 5.17.

6 The theory of complex multiplication

(Reference: [BD1], section 2.)

Fix a positive integer M, a rational prime p, and an imaginary quadratic field K of discriminant $-D$, such that $p \mid M$ but $p^2 \nmid M$, and $(M, D) = 1$. Define an integer decomposition

$$M = M^+M^-$$

such that $(M^+, M^-) = 1$, and M^+ is divisible by p and by the primes divisors of M/p which are split in K. Assume that:

1. M^- is squarefree,

2. M^- is the product of an even number of primes.

Let $X = X_{M^+,M^-}$ be the Shimura curve attached in section 5.1 to an Eichler order $\mathcal{R}$ of level M^+ in the indefinite quaternion algebra $\mathcal{B}$ of discriminant M^-. For all $m \geq 0$, there is a point P_m on X, which has complex multiplication by the order $\mathcal{O}_m$ of K of conductor p^{m+1} (introduced after the proof of theorem 5.17). More precisely, let (A_m, ι_m, C_m) be a triple corresponding to P_m via the moduli interpretation of X given in section 5.1. Write $\mathrm{End}(P_m)$ for the ring of endomorphisms of A_m which commute with the action ι_m and respect the level structure C_m. Then,

$$\mathrm{End}(P_m) \simeq \mathcal{O}_m.$$

The point P_m is called a *Heegner point* of level m. By the theory of complex multiplication, P_m is defined over the field $\tilde{K}_m$ (defined after the proof of theorem 5.17). Choose the P_m so that they are *compatible*, in the sense that for all $m \geq 0$, there is an isogeny of degree p^2 from A_m to A_{m+1}, which is equivariant for the actions ι_m and ι_{m+1}, and preserves the level structures C_m and C_{m+1}.

One has the following interpretation of the sequence $\{P_m\}$ in terms of the Bruhat-Tits tree at p. Given a point P on the Shimura curve $X_{M^+/p,M^-}$, corresponding to a triple (A, ι, C), let $\mathcal{T}^{(P)}$ denote the tree of p-isogenies of P. The vertices of $\mathcal{T}^{(P)}$ correspond to points of $X_{M^+/p,M^-}$ representing moduli related to (A, ι, C) by an isogeny of p-power degree. Two vertices of $\mathcal{T}^{(P)}$ are adjacent if the corresponding moduli are related by an isogeny of degree p^2. Thus, the oriented edges of $\mathcal{T}^{(P)}$ are naturally identified with points on X. The tree $\mathcal{T}^{(P)}$ is isomorphic to the Bruhat-Tits tree $\mathcal{T}$, and has a distinguished vertex v_P corresponding to P. There is a unique point P on $X_{M^+/p,M^-}$ such that:

1. $\mathrm{End}(P) \simeq \mathcal{O}_K$,

2. P_0 corresponds to an edge of the tree $\mathcal{T}^{(P)}$, with origin in P.

Then, the points P_m determine a half line of $\mathcal{T}^{(P)}$ originating from P, with no back-trackings.

7 Construction of the Euler System

Notations and assumptions being as in section 5.6, the construction of section 6 yields a compatible family of Heegner points

$$P_m \in X^{(\ell)}(\tilde{K}_m)$$

for all $m \geq 0$ (the notation $X^{(\ell)}$ was defined right before lemma 5.16). View P_m as an element of the Picard group $\mathrm{Pic}(X^{(\ell)})(\tilde{K}_m)$. Since the ideal $\mathcal{I}_{f_\ell}$ is not Eisenstein, the natural inclusion

$$J^{(\ell)}(\tilde{K}_m)/\mathcal{I}_{f_\ell} \to \mathrm{Pic}(X^{(\ell)})(\tilde{K}_m)/\mathcal{I}_{f_\ell}$$

is an isomorphism. Let α_p be the unit root of Frobenius at p. Write P_m^* for the image of $\alpha_p^{-m} P_m$ in $J^{(\ell)}(\tilde{K}_m)/\mathcal{I}_{f_\ell}$. The points P_m^* are norm-compatible. Hence their images by the coboundary maps

$$J^{(\ell)}(\tilde{K}_m)/\mathcal{I}_{f_\ell} \to H^1(\tilde{K}_m, \mathrm{Ta}_p(J^{(\ell)})/\mathcal{I}_{f_\ell})$$

yield a sequence of cohomology classes which are compatible under the corestriction maps. The choice of an isomorphism of $\mathrm{Ta}_p(J^{(\ell)})/\mathcal{I}_{f_\ell}$ with $T_{f,n}$, which exists by theorem 5.17, gives a class $\tilde{\kappa}(\ell)$ in $\hat{H}^1(\tilde{K}_\infty, T_{f,n})$, where $\hat{H}^1(\tilde{K}_\infty, T_{f,n})$ denotes the inverse limit under the corestriction maps of the groups $H^1(\tilde{K}_m, T_{f,n})$. Define $\kappa(\ell)$ in $\hat{H}^1(K_\infty, T_{f,n})$ to be the corestriction from $\tilde{K}_\infty$ to K_∞ of $\tilde{\kappa}(\ell)$. In other words, writing Q_m for the norm from $\tilde{K}_\infty$ to K_∞ of P_m^*, the class $\kappa(\ell)$ is the natural image in $\hat{H}^1(K_\infty, T_{f,n})$ of the sequence Q_m via the coboundary maps.

8 The first explicit reciprocity law

This section is devoted to the proof of theorem 4.1, notations being as in the previous sections. Recall that the class $\kappa(\ell)$ is constructed from a family of points on the Shimura curve $X^{(\ell)}$; hence, it can be viewed as an element of the usual (compactified) Selmer group of $J^{(\ell)}$ over K_∞ relative to the Galois module $\mathrm{Ta}_p(J^{(\ell)})/\mathcal{I}_{f_\ell}$. This shows that $\kappa(\ell)$ belongs to $\hat{H}^1_\ell(K_\infty, T_{f,n})$.

Recall the groups $\hat{\Phi}_\ell$ and $\tilde{\Phi}_\ell$, and the maps $\hat{\partial}_\ell$ and $\tilde{\partial}_\ell$, which were defined in section 5.6 (see equations (58) and (59)).

Lemma 8.1 *Theorem 4.1 is implied by the equality*

$$\tilde{\partial}_\ell(\{P_m^*\}) = \tilde{\mathcal{L}}_f \pmod{p^n}.$$

Remark: Note that the terms in the equality of lemma 8.1 are well defined only up to multiplication by elements of $\mathbb{Z}_p^\times$ and of $\tilde{G}_\infty$.

Proof: The element $\hat{\partial}_\ell(\{Q_m\})$ is mapped to $\partial_\ell(\kappa(\ell))$ by the isomorphism of corollary 5.18. Since $\hat{\partial}_\ell(\{Q_m\})$ is the norm of $\tilde{\partial}_\ell(\{P_m^*\})$, and $\mathcal{L}_f$ is the natural image of $\tilde{\mathcal{L}}_f$ in Λ, the claim follows.

In view of lemma 8.1, one is reduced to studying the specialization of the Heegner points P_m to connected components. To begin with, it is necessary to recall the ℓ-adic description of the point P_m given in section 5 of [BD3], and based on Drinfeld's moduli interpretation of the ℓ-adic upper half plane. Let $\bar{P}_m$ denote the reduction of P_m modulo a fixed prime above ℓ, and let

$$\mathrm{End}(P_m) \to \mathrm{End}(\bar{P}_m)$$

be the map obtained by reduction of endomorphisms. Recall that $\mathrm{End}(P_m)$ is isomorphic to the quadratic order $\mathcal{O}_m$. Moreover, the ring $\mathrm{End}(\bar{P}_m)[\frac{1}{\ell}]$ is isomorphic to $\underline{R}[\frac{1}{\ell}]$, where $\underline{R}$ denotes an Eichler order of level N^+ in the definite quaternion algebra B of discriminant N^-, which can be chosen to be independent of m. Extending scalars by $\mathbb{Z}[\frac{1}{\ell}]$, one obtains an injection

$$\Psi_m^0 : \mathcal{O}_m[\frac{1}{\ell}] \to \underline{R}[\frac{1}{\ell}].$$

It can be shown that Ψ_m^0 is well defined up to conjugation by elements in $\underline{R}[\frac{1}{\ell}]_1^\times$. Therefore, Ψ_m^0 can be identified with an element of the space

$$(\mathrm{Hom}(K,B) \times \mathcal{V}(\mathcal{T}_\ell))/\Gamma_{\ell,1},$$

by mapping Ψ_m^0 to the pair (Ψ_m, v_m), where Ψ_m is the extension of scalars of Ψ_m^0, and v_m is the vertex of $\mathcal{T}_\ell$ corresponding to the unique maximal order of B_ℓ containing $\Psi_m(\mathcal{O}_m)$. The embedding Ψ_m induces an action of $K_\ell^\times$ on $\mathcal{H}_\ell$, having two fixed points which belong to $K_\ell - \mathbb{Q}_\ell$, and which are conjugate by the generator of $\mathrm{Gal}(K_\ell/\mathbb{Q}_\ell)$. Then, P_m is identified with the image in $\mathcal{H}_\ell/\Gamma_{\ell,1}$ of one of these two points, via the isomorphism of theorem 5.1. (A suitable condition of normalization specifies which point corresponds to P_m, but this will not be of use here.) Let

$$r_\ell : \mathcal{H}_\ell(\mathbb{C}_\ell)/\Gamma_{\ell,1} \longrightarrow \mathcal{V}(\mathcal{G}_\ell) \cup \mathcal{E}(\mathcal{G}_\ell) = (\mathcal{V}(\mathcal{T}_\ell) \cup \mathcal{E}(\mathcal{T}_\ell))/\Gamma_{\ell,1}$$

be the reduction map (see for example chapter I of [BC], and also sections 1 and 6 of [BD3]). Here $\mathcal{G}_\ell$ is the dual graph $\mathcal{T}_\ell/\Gamma_{\ell,1}$ of $X^{(\ell)}$ at ℓ. Given P in $X^{(\ell)}(\mathbb{C}_\ell)$, viewed as a point in $\mathcal{H}_\ell(\mathbb{C}_\ell)/\Gamma_{\ell,1}$, $r_\ell(P)$ is equal to a vertex v if the reduction of P modulo ℓ lands in the single irreducible component of the fiber $X^{(\ell)}_{\mathbb{F}_{\ell^2}}$ corresponding to v, and $r_\ell(P)$ is equal to an edge e if P reduces to the singular point corresponding to e. The above description of P_m in terms of an ℓ-adic argument in $\mathcal{H}_\ell$ shows that the image of P_m by r_ℓ is equal to the vertex $v_m \pmod{\Gamma_{\ell,1}}$. This follows from the $\mathbf{GL}_2(\mathbb{Q}_\ell)$-equivariance of the reduction map, combined with the fact that P_m corresponds to a fixed point for the action of $\Psi_m(K_\ell^\times)$ on $\mathcal{H}_\ell(\mathbb{C}_\ell)$ and v_m is the unique fixed point for the action of $\Psi_m(K_\ell^\times)$ on $\mathcal{V}(\mathcal{T}_\ell) \cup \mathcal{E}(\mathcal{T}_\ell)$. Hence, the reduction of P_m modulo ℓ lands in the single irreducible component of the fiber $X^{(\ell)}_{\mathbb{F}_{\ell^2}}$ defined by v_m $\pmod{\Gamma_{\ell,1}}$. Furthermore, by proposition 5.14, $v_m \pmod{\Gamma_{\ell,1}}$ computes the image of P_m in the group of connected components $\Phi_{\ell,m}/\mathcal{I}_{f_\ell}$.

On the other hand, recalling that p divides the level of the order $\underline{R}$, strong approximation (see [Vi], p. 61) gives an identification

$$(\mathrm{Hom}(K, B) \times \mathcal{V}(\mathcal{T}_\ell))/\Gamma_{\ell,1} = (\mathrm{Hom}(K, B) \times \vec{\mathcal{E}}(\mathcal{T}_p))/\Gamma_p$$

where, in the notations of section 1.1, $\mathcal{T}_p = \mathcal{T}$ and $\Gamma_p = \Gamma$. The compatibility condition on the Heegner points P_m translates in the condition that they may be represented by pairs (Ψ, e_m) in $\mathrm{Hom}(K, B) \times \vec{\mathcal{E}}(\mathcal{T}_p)$, where Ψ arises from an embedding

$$\Psi^0 : \mathcal{O}_K[1/p] \to \underline{R}[1/p]$$

which does not depend on m, and where the e_m determine a half line with no back-trackings in $\mathcal{T}_p$. The results of [BD3], section 5 show that the action of $\tilde{G}_\infty$ on the P_m is compatible with the action of $\tilde{G}_\infty$ on the edges e_m, which was defined in section 1.2 using the embedding Ψ. Fix a prime λ_∞ of $\tilde{K}_\infty$ above ℓ, and set $\lambda_m = \lambda_\infty \cap \tilde{K}_m$. For $\sigma \in \tilde{G}_\infty$, write $\partial_{\lambda_m}(P_m^\sigma)$ for the natural image of P_m^σ in the group of connected components $\Phi_{\lambda_m}/\mathcal{I}_{f_\ell} \simeq \mathbb{Z}/p^n\mathbb{Z}$. The use of proposition 5.14 described above, together with the identification coming from strong approximation, shows that the map ∂_{λ_m} on the points P_m^σ can be viewed as a function

$$\vec{\mathcal{E}}(\mathcal{T}_p)/\Gamma_p \longrightarrow \mathbb{Z}/p^n\mathbb{Z}.$$

By multiplicity one, this function is equal modulo p^n to the eigenform f introduced in section 5.6 (up to multiplication by an element of $(\mathbb{Z}/p^n\mathbb{Z})^\times$). By comparing with definition (17), one finds that the equality

$$\partial_{\lambda_m}(P_m^\sigma) = [\sigma, e_m]_f \pmod{p^n} \tag{60}$$

holds for a suitable choice of λ_∞. (Note that the possible choices of λ_∞ are permuted by $\tilde{G}_\infty$. Similarly, the choices of embedding Ψ and of a sequence of edges in the definition of the p-adic L-function given in section 1.2 show that $\tilde{\mathcal{L}}_f$ is well defined only up to multiplication by elements of $\tilde{G}_\infty$.) It follows from (60) that

$$\partial_{\lambda_m}(\sigma P_m^*) = \alpha_p^{-m}[\sigma, e_m]_f \pmod{p^n}.$$

In view of equation (20) and of the definition of $\tilde{\mathcal{L}}_f$, this concludes the proof.

9 The second explicit reciprocity law

This section is devoted to the proof of theorem 4.2. Recall that ℓ_1 and ℓ_2 are distinct n-admissible primes relative to f, such that p^n divides $\ell_1 + 1 - \epsilon_1 a_{\ell_1}(f)$ and $\ell_2 + 1 - \epsilon_2 a_{\ell_2}(f)$, with ϵ_1 and ϵ_2 equal to ± 1. Let $\mathbb{T}_{\ell_1}$ be the Hecke algebra acting on $X^{(\ell_1)}$. As in the previous sections, equip $J^{(\ell_1)}$ with the action of $\mathbb{T}_{\ell_1}$ induced by Picard functoriality. Since f is p-isolated, the assumptions of theorem 5.15 are satisfied in the current setting. Thus, by theorem 5.17, $\mathrm{Ta}_p(J^{(\ell_1)})/\mathcal{I}_{f_{\ell_1}}$ is isomorphic to $T_{f,n}$ as a Galois module. Fix such an isomorphism. Then, the map

$$J^{(\ell_1)}(K_{\ell_2})/\mathcal{I}_{f_{\ell_1}} \to H^1(K_{\ell_2}, \mathrm{Ta}_p(J^{(\ell_1)})/\mathcal{I}_{f_{\ell_1}})$$

arising from Kummer theory yields a map

$$J^{(\ell_1)}(K_{\ell_2})/\mathcal{I}_{f_{\ell_1}} \to H^1(K_{\ell_2}, T_{f,n}). \tag{61}$$

The image of (61) is equal to $H^1_{\mathrm{fin}}(K_{\ell_2}, T_{f,n})$, since $T_{f,n}$ is unramified at ℓ_2 and ℓ_2 is a prime of good reduction for $J^{(\ell_1)}$. Since $p \neq \ell_2$, the map induced by reduction modulo ℓ_2

$$J^{(\ell_1)}(K_{\ell_2})/\mathcal{I}_{f_{\ell_1}} \to J^{(\ell_1)}(\mathbb{F}_{\ell_2^2})/\mathcal{I}_{f_{\ell_1}} \tag{62}$$

is an isomorphism. Hence, by composing the inverse of (62) with (61), and fixing an identification of $H^1_{\mathrm{fin}}(K_{\ell_2}, T_{f,n})$ with $\mathbb{Z}/p^n\mathbb{Z}$ (use lemma 2.6), one obtains a surjective map

$$J^{(\ell_1)}(\mathbb{F}_{\ell_2^2})/\mathcal{I}_{f_{\ell_1}} \to \mathbb{Z}/p^n\mathbb{Z}. \tag{63}$$

Let $\mathcal{S}_{\ell_2} \subset X^{(\ell_1)}(\mathbb{F}_{\ell_2^2})$ denote the set of supersingular points of $X^{(\ell_1)}$ in characteristic ℓ_2, and let $\mathrm{Div}(\mathcal{S}_{\ell_2})$, respectively, $\mathrm{Div}^0(\mathcal{S}_{\ell_2})$ be the module of formal divisors, respectively, degree zero formal divisors with $\mathbb{Z}$-coefficients supported on $\mathcal{S}_{\ell_2}$.

One may define two different actions of $\mathbb{T}_{\ell_1}$ on $\mathrm{Div}(\mathcal{S}_{\ell_2})$ and $\mathrm{Div}^0(\mathcal{S}_{\ell_2})$, by using either Picard or Albanese functoriality (see the remark at the beginning of section 5.4, which explains that these two actions differ by an Atkin-Lehner involution $w_{N^+,1}$). The latter action is the usual action defined on supersingular points, and is more natural if one views the supersingular points as being points in $X^{(\ell_1)}(\mathbb{F}_{\ell_2^2})$. The former action is more natural when viewing divisors on supersingular points as giving rise to points in $\mathrm{Pic}(X^{(\ell_1)})(\mathbb{F}_{\ell_2^2})$ and $J^{(\ell_1)}(\mathbb{F}_{\ell_2^2})$, on which the action of $\mathbb{T}_{\ell_1}$ was defined via Picard functoriality. Since f_{ℓ_1} is an eigenform for $w_{N^+,1}$, which acts via multiplication by ± 1, the choice of a specific Hecke action makes no difference for the purpose of establishing the $\mathbb{T}_{\ell_1}$-equivariance of the maps defined below; let us make the convention that the Hecke action on supersingular points be the Albanese one.

Since the inclusion of $\mathrm{Div}^0(\mathcal{S}_{\ell_2})$ in $\mathrm{Div}(\mathcal{S}_{\ell_2})$ induces an identification of $\mathrm{Div}^0(\mathcal{S}_{\ell_2})/\mathcal{I}_{f_{\ell_1}}$ with $\mathrm{Div}(\mathcal{S}_{\ell_2})/\mathcal{I}_{f_{\ell_1}}$ (use the fact that $\mathcal{I}_{f_{\ell_1}}$ is not Eisenstein), one obtains a natural map

$$\mathrm{Div}(\mathcal{S}_{\ell_2}) \to J^{(\ell_1)}(\mathbb{F}_{\ell_2^2})/\mathcal{I}_{f_{\ell_1}}. \tag{64}$$

The composition of (64) with the surjection (63) yields a map

$$\gamma : \mathrm{Div}(\mathcal{S}_{\ell_2}) \to \mathbb{Z}/p^n\mathbb{Z}.$$

Write T_q ($q \nmid N\ell_1$) and U_q ($q \mid N\ell_1$) for the q-th Hecke operator in $\mathbb{T}_{\ell_1}$, and $\bar{T}_q$ and $\bar{U}_q$ for the natural image of T_q and U_q, respectively, in $\mathbb{T}_{\ell_1}/\mathcal{I}_{f_{\ell_1}} = \mathbb{Z}/p^n\mathbb{Z}$. Thus, the following equalities modulo p^n hold: $\bar{T}_q \equiv a_q(f)$ for $q \nmid N\ell_1$, $\bar{U}_q \equiv a_q(f)$ for $q \mid N$, and $\bar{U}_{\ell_1} \equiv \epsilon_1$.

Lemma 9.1 *The relations*

$$\gamma(T_q x) = \bar{T}_q \gamma(x) \quad (q \nmid N\ell_1\ell_2), \qquad \gamma(U_q x) = \bar{U}_q \gamma(x) \quad (q \mid N\ell_1),$$

$$\gamma(T_{\ell_2} x) = \bar{T}_{\ell_2}\gamma(x), \quad \gamma(\mathrm{Frob}_{\ell_2} x) = \epsilon_2 \gamma(x)$$

hold for $x \in \mathrm{Div}(\mathcal{S}_{\ell_2})$.

Proof: As observed in the proof of lemma 2.6, $H^1_{\mathrm{fin}}(K_{\ell_2}, T_{f,n})$ is identified with the module $T_{f,n}/(\mathrm{Frob}^2_{\ell_2} - 1)T_{f,n}$ of $G_{K_{\ell_2}}$-coinvariants of $T_{f,n}$. Therefore, the map γ is defined by sending a point x to the image of $((\mathrm{Frob}^2_{\ell_2} - 1)/p^n)x$ in $T_{f,n}/(\mathrm{Frob}^2_{\ell_2} - 1)T_{f,n}$. The first two identities are a direct consequence of this description of γ. As for the last two identities, note that the Eichler-Shimura relations identify T_{ℓ_2} with the correspondence $\mathrm{Frob}_{\ell_2} + \mathrm{Frob}^\vee_{\ell_2}$, where $\mathrm{Frob}^\vee_{\ell_2}$ denotes the transpose of Frob_{ℓ_2}. Furthermore, on points defined over $\mathbb{F}_{\ell_2^2}$, one has $\mathrm{Frob}^\vee_{\ell_2} x = \ell_2 \mathrm{Frob}_{\ell_2} x$, and hence $T_{\ell_2} x = (\ell_2 + 1)\mathrm{Frob}_{\ell_2} x$. The claim follows from the fact that Frob_{ℓ_2} acts on $T_{f,n}$ with eigenvalues ϵ_2 and $\epsilon_2\ell_2$, which implies that Frob_{ℓ_2} acts as ϵ_2 on the quotient $T_{f,n}/(\mathrm{Frob}^2_{\ell_2} - 1)T_{f,n}$.

Proposition 9.2 *The map* γ *is surjective.*

Proof: Recall that p divides exactly N^+, and that the Shimura curve $X = X^{(\ell_1)}$ was defined in section 5.1 in terms of an Eichler order $\mathcal{R}$ of level N^+ in the indefinite quaternion algebra $\mathcal{B}$ of discriminant $N^-\ell_1$. Let $J = J^{(\ell_1)}$ be the jacobian of X. Write $J(\mathbb{F}_{\ell_2^2})^{ss}$ for the subgroup of $J(\mathbb{F}_{\ell_2^2})$ generated by divisors supported on supersingular points. Since the map (63) is surjective, it is enough to show that the natural image of $J(\mathbb{F}_{\ell_2^2})^{ss}$ in the group $J(\mathbb{F}_{\ell_2^2})/\mathcal{I}_{f_{\ell_1}}$ is equal to the whole group. Let $\Gamma^{(\ell_2)}$ denote the group of norm one elements in $\mathcal{R}[1/\ell_2]^\times/\{\pm 1\}$. Let $\tilde{X}$ be the Shimura curve defined in the same way as X but imposing an extra $\Gamma_1(p)$-level structure. Let $\tilde{\Gamma}^{(\ell_2)}$ be the finite index subgroup of $\Gamma^{(\ell_2)}$ consisting of elements which are congruent to the standard unipotent matrices modulo p. Write $\tilde{J}(\mathbb{F}_{\ell_2^2})$ for the $\mathbb{F}_{\ell_2^2}$-points of the jacobian of $\tilde{X}$, and $\tilde{J}(\mathbb{F}_{\ell_2^2})^{ss}$ for the subgroup generated by divisors supported on supersingular points. Since $\tilde{\Gamma}^{(\ell_2)}$ is torsion-free, the results of [I2] (see in particular remark G, page 19) establish a canonical isomorphism

$$\tilde{J}(\mathbb{F}_{\ell_2^2})/\tilde{J}(\mathbb{F}_{\ell_2^2})^{ss} \simeq (\tilde{\Gamma}^{(\ell_2)})^{ab}, \tag{65}$$

where $(\tilde{\Gamma}^{(\ell_2)})^{ab}$ denotes the abelianization of $\tilde{\Gamma}^{(\ell_2)}$. By fixing an embedding of $\mathcal{B}$ in $M_2(\mathbb{Q}_{\ell_2})$, one obtains an action of $\tilde{\Gamma}^{(\ell_2)}$ on the Bruhat-Tits tree $\mathcal{T}_{\ell_2}$. Let v_0 be the vertex of $\mathcal{T}_{\ell_2}$ such that the stabilizer $\tilde{\Gamma}_{v_0}^{(\ell_2)}$ of v_0 in $\tilde{\Gamma}^{(\ell_2)}$ is the subgroup of integral elements (relative to the fixed embedding of $\tilde{\Gamma}^{(\ell_2)}$ in $M_2(\mathbb{Q}_{\ell_2})$). Let e_0 be the edge originating from v_0 such that the stabilizer $\tilde{\Gamma}_{e_0}^{(\ell_2)}$ of e_0 is the subgroup of $\tilde{\Gamma}_{v_0}^{(\ell_2)}$ whose elements are upper triangular modulo ℓ_2 relative to this embedding. Write v_1 for the target of e_0. Note that $\tilde{\Gamma}_{v_0}^{(\ell_2)}$, respectively, $\tilde{\Gamma}_{e_0}^{(\ell_2)}$ can be identified with the discrete subgroup of $\mathbf{SL}_2(\mathbb{R})$ which defines the Shimura curve $\tilde{X}$, respectively, the Shimura curve $\tilde{X}_0(\ell_2)$ defined in the same way as $\tilde{X}$, but with an extra $\Gamma_0(\ell_2)$-level structure imposed. The group $\tilde{\Gamma}^{(\ell_2)}$ acts on the tree $\mathcal{T}_{\ell_2}$ with the closed edge attached to e_0 as a fundamental region. Hence the exact cohomology sequence in proposition 13 of sec. II.2.8 of [Se1], in the case $i=1$, $M=\mathbb{F}_p$ and $G=\tilde{\Gamma}^{(\ell_2)}$ becomes

$$\begin{aligned} 0 \longrightarrow \ & \mathrm{Hom}(\tilde{\Gamma}^{(\ell_2)}, \mathbb{F}_p) \longrightarrow \mathrm{Hom}(\tilde{\Gamma}_{v_0}^{(\ell_2)}, \mathbb{F}_p) \oplus \mathrm{Hom}(\tilde{\Gamma}_{v_1}^{(\ell_2)}, \mathbb{F}_p) \\ \xrightarrow{d} \ & \mathrm{Hom}(\tilde{\Gamma}_{e_0}^{(\ell_2)}, \mathbb{F}_p). \end{aligned} \tag{66}$$

The modules appearing as the source and target of d are identified by duality with two copies or one copy of the p-torsion in the jacobian of $\tilde{X}$ and $\tilde{X}_0(\ell_2)$, respectively. Moreover, the map d corresponds under these identifications to the map denoted α_p in the statement of theorem 2, p. 451 of [DT]. This theorem (the analogue of Ihara's lemma in the setting of Shimura curves) states that the action of $G_{\mathbb{Q}}$ on the kernel of d factors through an abelian quotient of $G_{\mathbb{Q}}$. View f_{ℓ_1} as a mod p^n modular form (with trivial character) on $\tilde{X}$, and write $\tilde{\mathcal{I}}_{f_{\ell_1}}$ for the associated ideal in the Hecke algebra $\tilde{\mathbb{T}}_{\ell_1}$. Let $\tilde{\mathfrak{m}}_{f_{\ell_1}}$ be the maximal ideal of $\tilde{\mathbb{T}}_{\ell_1}$ containing $\tilde{\mathcal{I}}_{f_{\ell_1}}$. Since $\tilde{\mathfrak{m}}_{f_{\ell_1}}$ corresponds to an irreducible mod p Galois representation, it follows from the sequence (66) that $\mathrm{Hom}(\tilde{\Gamma}^{(\ell_2)}, \mathbb{F}_p)[\mathfrak{m}_{f_{\ell_1}}]$ is trivial, and therefore that $(\tilde{\Gamma}^{(\ell_2)})^{ab}/\tilde{\mathfrak{m}}_{f_{\ell_1}}$ is trivial. By Nakayama's lemma, this shows that

$$(\tilde{\Gamma}^{(\ell_2)})^{ab}/\tilde{\mathcal{I}}_{f_{\ell_1}} = 0. \tag{67}$$

Equation (65) then implies that the natural image of $\tilde{J}(\mathbb{F}_{\ell_2^2})^{ss}$ in $\tilde{J}(\mathbb{F}_{\ell_2^2})/\tilde{\mathcal{I}}_{f_{\ell_1}}$ fills the whole group. Finally, the cokernel of the natural map

$$\tilde{J}^{(\ell_1)}(\mathbb{F}_{\ell_2^2}) \to J^{(\ell_1)}(\mathbb{F}_{\ell_2^2}) \tag{68}$$

can be identified with an abelian quotient of the (finite) image of $\Gamma_0(p)$ in $\mathbf{SL}_2(\mathbb{Z}/p\mathbb{Z})$, and hence has order dividing $p-1$; see for example the results of chapter 7 of [Co], particularly in pages 107 and 110. It follows in particular that the composition of the map (68) with the projection from $J^{(\ell_1)}(\mathbb{F}_{\ell_2^2})$ to $J^{(\ell_1)}(\mathbb{F}_{\ell_2^2})/p^n$ is surjective. When combined with the fact that $\tilde{J}(\mathbb{F}_{\ell_2^2})^{ss}$ maps surjectively to $\tilde{J}(\mathbb{F}_{\ell_2^2})/\tilde{\mathcal{I}}_{f_{\ell_1}}$ (as noted after equation (67)), this implies that $J(\mathbb{F}_{\ell_2^2})^{ss}$ maps surjectively to $J(\mathbb{F}_{\ell_2^2})/\mathcal{I}_{f_{\ell_1}}$, as was to be shown.

Remark: The proof of proposition 9.2 relies crucially on the analogue of Ihara's lemma proved in [DT]. In turn, proposition 9.2 provides the key step in the proof of theorem 9.3, a raising the level result which is a theorem of [DT] (extended to mod p^n modular forms).

Following the notations of proposition 3.12, let B' be the definite quaternion algebra of discriminant $N^-\ell_1\ell_2$, R' an Eichler $\mathbb{Z}[1/p]$-order of level N^+ in B, and Γ' the group $(R')^\times/\mathbb{Z}[1/p]^\times$. The next result contains the part of the statement of proposition 3.12 that remains to be proved.

Theorem 9.3 *There exists an eigenform $g \in S_2(\mathcal{T}/\Gamma', \mathbb{Z}/p^n\mathbb{Z})$ such that*

$$T_q g = a_q(f) g \quad (q \not| N\ell_1\ell_2), \qquad U_q g = a_q(f) g \quad (q|N),$$

$$U_{\ell_1} g = \epsilon_1 g, \quad U_{\ell_2} g = \epsilon_2 g.$$

Proof: Write $\mathbb{T}_{\ell_1} = \mathbb{T}_{N^+,N^-\ell_1}$ for the Hecke algebra acting on cusp forms on $\Gamma_0(N\ell_1)$ which are new at $N^-\ell_1$, and $\mathbb{T}_{\ell_2,\ell_1} = \mathbb{T}_{N^+\ell_2,N^-\ell_1}$ for the Hecke algebra acting on cusp forms on $\Gamma_0(N\ell_1\ell_2)$ which are new at $N^-\ell_1$. By theorem 5.15, there is a mod p^n modular form

$$f_{\ell_1} : \mathbb{T}_{\ell_1} \to \mathbb{Z}/p^n\mathbb{Z}$$

such that $f_{\ell_1}(T_q) = f(t_q)$ for all $q \nmid N\ell_1$, $f_{\ell_1}(U_q) = f(u_q)$ for all $q \mid N$, and $f_{\ell_1}(U_{\ell_1}) = \epsilon_1 f_{\ell_1}$. Recall from the proof of theorem 5.15 that the homomorphism f_{ℓ_1} arises from the group of connected components at ℓ_1 attached to the Shimura curve $X^{(\ell_1)} = X_{N^+, N^- \ell_1}$. Consider now the Shimura curve $X^{(\ell_2,\ell_1)} := X_{N^+\ell_2, N^-\ell_1}$, on which the elements of $\mathbb{T}_{\ell_2,\ell_1}$ act as correspondences. By proposition 5.3, the character group $\mathcal{X}_{\ell_2}$ of $X^{(\ell_2,\ell_1)}$ at ℓ_2 is identified with the module $\mathrm{Div}^0(\mathcal{S}_{\ell_2})$ defined at the beginning of this section; here $\mathcal{S}_{\ell_2}$ is viewed as the set of supersingular points in $X^{(\ell_2,\ell_1)}(\mathbb{F}_{\ell_2^2})$ by the results of section 5.1. Furthermore, the action of $\mathbb{T}_{\ell_2,\ell_1}$ on $\mathcal{X}_{\ell_2}$ induced from the action on $\mathrm{Pic}^0(X^{(\ell_2,\ell_1)})$ defined by Picard functoriality is compatible with the standard (Albanese) action of $\mathbb{T}_{\ell_2,\ell_1}$ via correspondences on the set of supersingular points (see [Ri2], p. 445). The results of [Wa] on the endomorphisms of supersingular abelian surfaces, combined with strong approximation, yield a $\mathbb{T}_{\ell_2,\ell_1}$-compatible identification of $\mathcal{S}_{\ell_2}$ with $\vec{\mathcal{E}}(\mathcal{T})/\Gamma'$. (Note that $\mathcal{X}_{\ell_2} = \mathrm{Div}^0(\mathcal{S}_{\ell_2})$ pertains to the ℓ_2-new part of the jacobian $J^{(\ell_2,\ell_1)}$ of $X^{(\ell_2,\ell_1)}$, being $\mathcal{X}_{\ell_2}$ the character group of the maximal torus of $J^{(\ell_2,\ell_1)}$ over $\mathbb{F}_{\ell_2^2}$.) Therefore, the map γ defined above can also be viewed as a $\mathbb{Z}/p^n\mathbb{Z}$-valued map on $\vec{\mathcal{E}}(\mathcal{T})/\Gamma'$, whose values are not contained in any proper subgroup of $\mathbb{Z}/p^n\mathbb{Z}$, by proposition 9.2. This map defines the sought-for modular form g on Γ', as can be seen by appealing to lemma 9.1. More precisely, let T_q^* (for q not dividing $N\ell_1\ell_2$) and U_q^* (for q dividing $N\ell_1\ell_2$) denote the Hecke operators in $\mathbb{T}_{\ell_2,\ell_1}$. (Note the discrepancy between the notations for the Hecke operators used in this proof and those used in the statement of proposition 3.12, which are also reproduced in the statement of theorem 9.3; in this proof, and throughout the section, the symbols T_q and U_q are used to indicate the Hecke operators in $\mathbb{T}_{\ell_1}$.) Since the Hecke operators at $q \neq \ell_2$ in $\mathbb{T}_{\ell_1}$ and $\mathbb{T}_{\ell_2,\ell_1}$ act in the same way on γ and g, respectively, lemma 9.1 implies directly the relations of theorem 9.3 for all $q \neq \ell_2$:

$$T_q^* g = T_q \gamma = a_q(f) g \quad (q \not| N\ell_1\ell_2), \qquad U_q g = U_q \gamma = a_q(f) g \quad (q | N\ell_1),$$

(in particular one has $T_{\ell_1}^* g = \epsilon_1 g$). As for the operator $U_{\ell_2}^*$, it is known that $U_{\ell_2}^* x = \mathrm{Frob}_{\ell_2} x$ for $x \in \mathcal{S}_{\ell_2}$ (see [Ri2], proposition 3.8). Hence, lemma 9.1 yields

$$(U_q^* g)(x) = \gamma(Frob_{\ell_2} x) = \epsilon_2 g(x).$$

This concludes the proof.

The proof of theorem 9.3 implies the following result.

Corollary 9.4 *Under the indentification of $\mathcal{S}_{\ell_2}$ with $\vec{\mathcal{E}}(\mathcal{T})/\Gamma'$, the map γ corresponds to an eigenform $g \in S_2(\mathcal{T}/\Gamma', \mathbb{Z}/p^n\mathbb{Z})$ satisfying the conclusions of theorem 9.3.*

Consider the sequence $\{P_m\}$ of Heegner points $P_m \in X^{(\ell_1)}(\tilde{K}_m)$, constructed in section 6. Fix a prime λ_∞ of $\tilde{K}_\infty$ above ℓ_2, and let $\lambda_m = \lambda_\infty \cap \tilde{K}_m$. Since ℓ_2 is inert in K, the point P_m reduces modulo λ_m to a supersingular point $\bar{P}_m \in X^{(\ell_1)}(\mathbb{F}_{\lambda_m})$. Identifying $\mathbb{F}_{\lambda_m}$ with $\mathbb{F}_{\ell_2^2}$, $\bar{P}_m$ can be viewed as an element of $\mathcal{S}_{\ell_2}$. Identifying $\mathcal{S}_{\ell_2}$ with $\vec{\mathcal{E}}(\mathcal{T})/\Gamma'$, the sequence $\{\bar{P}_m\}$ can be described by a sequence of consecutive edges $\{e_m\}$ in $\vec{\mathcal{E}}(\mathcal{T})$, modulo Γ', in such a way that the map $\mathrm{End}(P_m) \to \mathrm{End}(\bar{P}_m)$ of reduction of endomorphisms modulo λ_m induces by extension of scalars an embedding

$$\Psi : K \to B',$$

which is independent of m. Then, the natural Galois action of $\tilde{G}_\infty$ on the P_m is compatible with the action of $\tilde{G}_\infty$ on the e_m via Ψ, which was defined in section 1.2. Writing

$$\tilde{\mathcal{L}}_{g,m} := \alpha_p^{-m} \sum_{\sigma \in \tilde{G}_m} g(\overline{\sigma P}_m) \cdot \sigma^{-1} \in \mathbb{Z}/p^n\mathbb{Z}[\tilde{G}_m],$$

it follows that the sequence $\{\tilde{\mathcal{L}}_{g,m}\}$ defines an element of $\mathbb{Z}/p^n\mathbb{Z}[\![\tilde{G}_\infty]\!]$, equal to $\tilde{\mathcal{L}}_g$. Define the local cohomology groups

$$H^1_{\mathrm{fin}}(\tilde{K}_{m,\ell_2}, T_{f,n}) := \oplus_{\lambda|\ell_2} H^1_{\mathrm{fin}}((\tilde{K}_m)_\lambda, T_{f,n}),$$

where the sum is taken over all the primes of $\tilde{K}_m$ dividing ℓ_2, and

$$\hat{H}^1_{\mathrm{fin}}(\tilde{K}_{\infty,\ell_2}, T_{f,n}) := \varprojlim_m H^1_{\mathrm{fin}}(\tilde{K}_{m,\ell_2}, T_{f,n}),$$

where the inverse limit is taken with respect to the natural corestriction maps. The fixed identification of $H^1_{\mathrm{fin}}(K_{\ell_2}, T_{f,n})$ with $\mathbb{Z}/p^n\mathbb{Z}$, together with the choice of the prime λ_∞, yields the identifications

$$H^1_{\mathrm{fin}}(\tilde{K}_{m,\ell_2}, T_{f,n}) = \mathbb{Z}/p^n[\tilde{G}_m], \qquad \hat{H}^1_{\mathrm{fin}}(\tilde{K}_{\infty,\ell_2}, T_{f,n}) = \mathbb{Z}/p^n[\![\tilde{G}_\infty]\!].$$

In view of corollary 9.4 and the definition of the map γ, the image of P_m^* in $H^1_{\mathrm{fin}}(\tilde{K}_{m,\ell_2}, T_{f,n})$ corresponds to $\tilde{\mathcal{L}}_{g,m} \pmod{p^n}$, and the image of the compatible sequence $\{P_m^*\}$ in $\hat{H}^1_{\mathrm{fin}}(\tilde{K}_{\infty,\ell_2}, T_{f,n})$ corresponds to $\tilde{\mathcal{L}}_g \pmod{p^n}$, under the above identifications. Recall the class $\tilde{\kappa}(\ell_1)$, defined in section 7 as the image of the sequence $\{P_m^*\}$ in $\hat{H}^1(\tilde{K}_\infty, T_{f,n})$ by the coboundary map. The value $v_{\ell_2}(\tilde{\kappa}(\ell_1))$ at ℓ_2 of $\tilde{\kappa}(\ell_1)$ is naturally an element of $\hat{H}^1_{\mathrm{fin}}(\tilde{K}_{\infty,\ell_2}, T_{f,n})$, and is equal to the image of $\{P_m^*\}$, and hence to $\tilde{\mathcal{L}}_g \pmod{p^n}$. Since $\mathcal{L}_g$ is the image in Λ of $\tilde{\mathcal{L}}_g$, and $\kappa(\ell_1)$ is the corestriction from $\tilde{K}_\infty$ to K_∞ of $\tilde{\kappa}(\ell_1)$, theorem 4.2 follows.

Remark: The result proved in this section can be viewed as a generalization of the main result of [BD5]. The proof given here follows closely the approach in [Va2], avoiding the study of certain groups of connected components which was involved in the methods of [BD5].

References

[BC] J-F. Boutot, H. Carayol, *Uniformisation p-adique des courbes de Shimura: les théorèmes de Cerednik et de Drinfeld*, Astérisque 196-197 (1991) pp. 45-158.

[BD0] M. Bertolini, H. Darmon, *Derived heights and generalized Mazur-Tate regulators* Duke Math. J. **76** (1994), no. 1, 75–111.

[BD$\frac{1}{2}$] M. Bertolini, H. Darmon, *Derived p-adic heights.* Amer. J. Math. **117** (1995), no. 6, 1517–1554.

[BD1] M. Bertolini and H. Darmon, *Heegner points on Mumford-Tate curves.* Invent. Math. **126** (1996) 413–456.

[BD2] M. Bertolini and H. Darmon, *A rigid-analytic Gross-Zagier formula and arithmetic applications.* Annals of Math. **146** (1997) 111-147.

[BD3] M. Bertolini and H. Darmon, *Heegner points, p-adic L-functions, and the Cerednik-Drinfeld uniformization.* Invent. Math. **131** (1998), no. 3, 453–491.

[BD4] M. Bertolini and H. Darmon, *p-adic periods, p-adic L-functions and the p-adic uniformization of Shimura curves*, Duke Math. J. **98** (1999), no. 2, 305–334.

[BD5] M. Bertolini and H. Darmon, *Euler systems and Jochnowitz congruences*, Amer. J. Math. **121**, n. 2 (1999) 259-281.

[BLR] S. Bosch, W. Lütkebohmert, and M. Raynaud, Néron Models, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3 Folge - Band 21, Springer-Verlag, 1990.

[BoLeRi] N. Boston, H. Lenstra, K. Ribet, *Quotients of groups rings arising form two-dimensional representations,* C. R. Acad. Sci. Paris **312**, Série I (1991) 323–328.

[Bu] K. Buzzard, *Integral models of certain Shimura curves,* Duke Math. J. **87**, no. 3 (1998), 591–612.

[Co] C. Cornut, *Réduction de familles de points CM,* PhD Thesis, Université Louis Pasteur, Strasbourg, 2000.

[Dag] H. Daghigh, *Modular forms, quaternion algebras, and special values of L-functions*, McGill University PhD thesis, 1997.

[Da] H. Darmon, *A refined conjecture of Mazur-Tate type for Heegner points.* Invent. Math. **110** (1992), no. 1, 123–146.

[DDT] H. Darmon, F. Diamond, and R. Taylor, *Fermat's Last Theorem*, Current Developments in Mathematics Vol. **1**, International Press, 1995, pp. 1–154.

[DR] P. Deligne and M. Rapoport, *Les schémas de modules des courbes elliptiques,* LNM **349**, Springer-Verlag, New York, 1973, 143-316.

[Dr] V.G. Drinfeld, *Coverings of p-adic symmetric regions*, (in Russian), Funkts. Anal. Prilozn. 10, 29-40, 1976. Transl. in Funct. Anal. Appl. 10, 107-115, 1976.

[DT] Diamond, Fred; Taylor, Richard. *Nonoptimal levels of mod ℓ modular representations.* Invent. Math. **115** (1994), no. 3, 435-462.

[Ed] B. Edixhoven, Appendix in [BD2].

[Ei] M. Eichler, *The basis problem for modular forms and the traces of the Hecke operators.* Modular functions of one variable, I (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), pp. 75–151. Lecture Notes in Math., Vol. 320, Springer, Berlin, 1973.

[Gr1] B.H. Gross, *Heights and the special values of L-series.* Number theory (Montreal, Que., 1985), 115–187, CMS Conf. Proc., 7, Amer. Math. Soc., Providence, RI, 1987.

[Gr2] B.H. Gross, D.B. Zagier, *Heegner points and derivatives of L-series.* Invent. Math. **84** (1986), no. 2, 225–320.

[Groth] A. Grothendieck, *Groupes de Monodromie en Géométrie Algébrique,* SGA VII, LNM **288**, Springer-Verlag, New York, 1972.

[GvdP] L. Gerritzen, M. van der Put, Schottky Groups and Mumford Curves, Springer Lecture Notes **817**, 1980.

[I1] Y. Ihara, *On congruence monodromy problems,* Lect. Notes Univ. Tokyo **1** (1968).

[I2] Y. Ihara, *Shimura curves over finite fields and their rational points,* Contemporary Math. **245** (1999) 15-23.

[JL] H. Jacquet; R.P. Langlands. Automorphic forms on $\mathbf{GL}(2)$. Lecture Notes in Mathematics, Vol. **114**. Springer-Verlag, Berlin-New York, 1970.

[JoLi1] B.W. Jordan, R. Livné, *Local diophantine properties of Shimura curves,* Math. Ann. **270** (1985) 235-248.

[JoLi2] B.W. Jordan, R. Livné, *On the Néron mdel of Jacobians of Shimura curves,* Compositio Math. **60** (1986) 227-236.

[JoLi3] B.W. Jordan, R. Livné, *Integral Hodge theory and congruences between modular forms,* Duke Math. J. **80** (1995) 419-484.

[KM] N. Katz and B. Mazur, *Arithmetic moduli of elliptic curves,* Annals of Math. Studies 108, Princeton University Press, Princeton, NJ (USA), 1985.

[M] Y.I. Manin, *p-adic automorphic functions*, J. Soviet Math. **5** (1976) 279–333.

[Ma1] B. Mazur, *On the arithmetic of special values of L functions*, Invent. Math.**55** (1979), no. 3, 207–240.

[MR] B. Mazur and K. Rubin, *Kolyvagin systems*, preprint.

[MTT] B. Mazur, J. Tate, J. Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer.* Invent. Math. **84** (1986), no. 1, 1–48.

[Ram] R. Ramakrishna, *Lifting Galois representations.* Invent. Math. **138** (1999), no. 3, 537–562.

[Ray] M. Raynaud, *Spécialization du foncteur de Picard,* Publ. Math., Inst. Hautes Etud. Sc. **38** (1970) 27-76.

[Ri1] K. Ribet, *Bimodules and abelian surfaces,* Adv. Stud. Pure Math. **17** (1989) 359-407.

[Ri2] K. Ribet, *On modular representation of* $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms,* Invent. Math. **100** (1990) 431-476.

[Ro] D. Roberts, Shimura curves analogous to $X_0(N)$, Harvard PhD. Thesis, 1989.

[Ru] K. Rubin, Euler Systems. Annals of Mathematics Studies **147**, 227+xi pp., Princeton: Princeton University Press.

[Se1] J-P. Serre, Trees, translated from the French by John Stilwell, Springer, 1980.

[Se2] J-P. Serre, Abelian ℓ-Adic Representations and Elliptic Curves, Addison-Wesley, 1989.

[Sh] G. Shimura, Introduction to the arithmetic theory of automorphic functions. Reprint of the 1971 original. Publications of the Mathematical Society of Japan, 11. Kanô Memorial Lectures, 1. Princeton University Press, Princeton, NJ, 1994.

[Va1] V. Vatsal, *Uniform distribution of Heegner points,* Invent. Math. **148**, (2002) 1–48.

[Va2] V. Vatsal, *Special values of anticyclotomic L-functions,* Duke Math Journal, to appear.

[Vi] M-F. M-F. Vigneras, *Arithmétique des algèbres des quaternions,* LNM 800, Springer.

[Wa] W. Waterhouse, *Abelian varieties over finite fields,* Ann. Sci. Ec. Nor. Sup., Série **4** (1969) 521-560.

[W] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem,* Ann. Math. **141** (1995) 443-551.

[Zh] S. Zhang, *Gross-Zagier formula for* GL_2, Asian J. Math. **5** (2001), no. 2, 183–290.