COMPOSITIO MATHEMATICA

EHUD DE SHALIT

On certain Galois representations related to the modular curve $X_1(p)$

Compositio Mathematica, tome 95, n° 1 (1995), p. 69-100

<http://www.numdam.org/item?id=CM_1995__95_1_69_0>

Compositio Mathematica **95**: 69–100, 1995.

On certain Galois representations related to the modular curve $X_1(p)$

EHUD DE SHALIT
Department of Mathematics, Hebrew University, Giv'at-Ram, Jerusalem 91904, Israel

Received 7 June 1993; accepted in final form 9 December 1993

0.1. Hida's deformation

Let p be a prime number, $p \geqslant 5$, and X_0 the modular curve $X_0(p)$ over $\mathbb{Q}$. Let $J_0 = J_0(p)$ be its Jacobian, and $V = \mathrm{Hom}(J_0[p^\infty], \mathbb{Q}_p/\mathbb{Z}_p)$ the p-adic (contravariant) Tate module of J_0. V is a representation module for $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Hida [Hi] introduced and studied an important *deformation* $\mathbf{V}$ of V, obtained from the ordinary parts of the Tate modules of $J_1(p^n)$ passing to the limit over n. This big representation space $\mathbf{V}$ is a module over the Iwasawa algebra $\Lambda = \mathbb{Z}_p[[\Gamma]]$, where $\Gamma = 1 + p\mathbb{Z}_p$ acts through the so-called "diamond operators". $\mathbf{V}$ is finitely generated and free over Λ, and V is identified with its Γ-coinvariants (loc. cit., Proposition 5.5).

Hida's original approach relied on Eichler-Shimura cohomology. Mazur and Wiles ([M-W2]) studied the geometry behind Hida's construction, and proved that the restriction of $\mathbf{V}$ to a decomposition group at p, has a 2-step filtration with well-understood graded pieces. (This was taken up by Hida too.)

0.2. The work of Greenberg and Stevens

Recently, Greenberg and Stevens [G-S] realized the relevance of $\mathbf{V}$ to a conjecture of Mazur, Tate and Teitelbaum [M-T-T] about the "$\mathscr{L}$-invariant" of (modular) elliptic curves with split multiplicative reduction at p. We want to review certain ideas used in their proof of this conjecture, because they are central to our paper too, and to subsequent work [dS2].

We shall assume that the elliptic curve in question has a prime conductor p. This restriction, whether here or in 0.1 above, is not essential. We stick to it to simplify the notation and highlight the main points.

Thus let E be an elliptic curve of conductor p, and assume without loss of generality that it is *contained* in $J_0(p)$ (one calls such an E a *strong* Weil curve; others are isogenous to it). E has multiplicative reduction at p, and we assume that this reduction is *split*. (In terms of the newform of weight 2 corresponding to E, this is equivalent to the pth Fourier coefficient a_p

being equal to 1.) Let $q \in \mathbb{Q}_p^\times$ be the Tate-period of E. The *$\mathscr{L}$-invariant* $\mathscr{L}_p(E)$ is defined to be $\log_p(q)/\mathrm{ord}_p(q)$, where $\log_p$ is normalized by $\log_p(p) = 0$, and ord_p by $\mathrm{ord}_p(p) = 1$. Clearly $\mathscr{L}_p(E)$ is an isogeny invariant.

Since we assumed that $a_p = 1$, the p-adic L function of E, $L_p(E, s)$ vanishes at $s = 1$ (see [M-T-T]). The conjecture of Mazur, Tate and Teitelbaum, proved by Greenberg and Stevens, predicted the relation

$$L_p'(E, 1) = \mathscr{L}_p(E) \cdot \Lambda_\infty(E, 1). \tag{1}$$

Here $\Lambda_\infty(E, 1)$, the algebraic part of the special value of the *classical* L-function of E at $s = 1$, is a certain rational number expressed in terms of modular symbols.

REMARK. Both sides of (1) vanish if $E(\mathbb{Q})$ is infinite. In this case Mazur, Tate and Teitelbaum made further conjectures in the style of Birch and Swinnerton-Dyer about the leading term in the Taylor expansion of $L_p(E, s)$ at $s = 1$, but the methods of Greenberg and Stevens are far short of treating them.

Let $V(E) = \mathrm{Hom}(E[p^\infty], \mathbb{Q}_p/\mathbb{Z}_p)$. As a representation of the decomposition group $\mathscr{G}_p$ at a prime of $\bar{\mathbb{Q}}$ above p, $V(E)$ is naturally filtered, because E is ordinary. Denote the filtration by

$$0 \to U(E) \to V(E) \to W(E) \to 0.$$

Then $U(E) \approx \mathbb{Z}_p$ and $W(E) \approx \mathbb{Z}_p(-1)$ as $\mathscr{G}_p$-modules.

The idea of Greenberg and Stevens was to interpret q as a certain *restriction* on *filtered deformations* of $V(E)$. This is done as follows. Passing to the p-adic completion of $\mathbb{Q}_p^\times$, the period q maps to $(\mathbb{Q}_p^\times)\hat{} \approx H^1(\mathbb{Q}_p, \mathbb{Z}_p(1))$. This last space is isomorphic to $\mathbb{Z}_p^2$ via $(\mathrm{ord}_p, \log_p)$. Thus $\mathscr{L}_p(E)$ determines a line l in $H^1(\mathbb{Q}_p, \mathbb{Z}_p(1))$.

An infinitesimal deformation of $V(E)$ *with its filtration* (as a representation for the local Galois group at p) is a commutative exact diagram of $\mathscr{G}_p$-modules

$$\begin{array}{ccccccc} 0 & \to & \tilde{U}(E) & \to & \tilde{V}(E) & \to & \tilde{W}(E) \to 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \to & U(E) & \to & V(E) & \to & W(E) \to 0 \end{array}$$

where the modules in the top row are endowed with an action of $\mathbb{Z}_p[\varepsilon]$, $\varepsilon^2 = 0$, commuting with Galois, and the vertical arrows are surjective and identify $U(E)$ (resp. $V(E)$, $W(E)$) with the ε-coinvariants of $\tilde{U}(E)$ (resp.

$\tilde{V}(E)$, $\tilde{W}(E)$). We further demand that $\tilde{U}(E)$ and $\tilde{W}(E)$ be free of rank 1 over $\mathbb{Z}_p[\varepsilon]$. By local class field theory, the left column of such a diagram defines a linear functional on $H^1(\mathbb{Q}_p, \mathbb{Z}_p(1))$. A standard diagram chasing proves that this functional must vanish on the line l. One extracts from here a certain relation that must hold between $\mathscr{L}_p(E)$ and the representation of $\mathscr{G}_p$ on $\tilde{U}(E)$. For precise definitions and details see [G-S] Section 3, and in particular Theorem 3.14.

Now $V(E)$ is a quotient of V, so $\mathbf{V}$, in view of the results of Hida and Mazur-Wiles quoted in 0.1, supplies us with a concrete filtered deformation of $V(E)$. The information that it carries about $\mathscr{L}_p(E)$ was translated by Greenberg and Stevens to prove (1). This translation procedure is far from trivial, but involves a different circle of ideas, in particular the study of a 2-variable p-adic L function associated with E, with a functional equation.

0.3. Description of the main results of this work

Following the brief review of the work of Greenberg and Stevens, let us explain what we intend to do. Our final goal is to prove a "refinement" of (1), conjectured by Mazur and Tate in [M-T] (the "refined conjecture"at the bottom of p. 712). The present paper deals with the first half of the project.

We shall (a) establish a "refined" analogue of Hida's deformation (Theorem 1, §2.10), (b) prove an analogue of the theorem of Mazur and Wiles (Propositions 3.2 and 3.7), and (c) draw the information that this "refined deformation" carries about the projection of $q/p^{\mathrm{ord}(q)}$ to $\mathbb{F}_p^\times$ (Theorem 2, §3.6, and Theorem 3, §3.10). Note that this projection is precisely the part lost by taking logarithms in making $\mathscr{L}_p(E)$, hence the adjectives "refined" or "exponentiated" that are used in conjunction with the conjectures of Mazur and Tate. Note also that the quantity we are after is highly sensitive to isogenies. In fact, in contrast to [G-S], all that we do below is "trivial up to isogeny".

The second half of our project, involving the construction of a "two-variable" theta-element with a functional equation (see [M-T], p. 173 for the one-variable theta element, called there the modular element), and a proof of the conjecture of Mazur and Tate, will be given in another paper [dS2].

Finally, let us stress that restricting to prime conductor, or to elliptic curves (i.e. eigenforms of weight 2 with coefficients in $\mathbb{Q}$) should not be considered serious limitations. In fact although, as explained above, we stick to prime level, we shall treat all of $J_0(p)$ at once, and instead of the q of E, we shall consider the full p-adic period matrix of $J_0(p)$. Generalizations to higher weight, however, introduce an interesting challenge.

Throughout, compatibility with the action of the ring of Hecke operators is important, both to test the naturality of our maps, and to allow later on the deduction of results pertaining to individual elliptic curves.

0.4. We shall use the following conventions. If A is a group or a group scheme, and r an endomorphism of A, $A[r]$ will denote its kernel, and $A^* = \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$ the Pontrjagin dual of A, in a category where it makes sense. If A comes equipped with a Galois group action, we put the usual contragradient action on A^*, i.e. for $\alpha \in A^*$, $a \in A$ and $\sigma \in \mathrm{Galois}$, $(\sigma\alpha)(a) = \alpha(\sigma^{-1}(a))$. If A comes equipped with a ring of endomorphisms $\mathbf{T}$ (e.g. Hecke operators), we put the dual action on A^*, i.e. $(T\alpha)(a) = \alpha(Ta)$. If $\mathbf{T}$ and Galois commute in their action on A, they will commute in their action on A^*.

Let $r = l^n$ be the highest power of a prime $l \neq 2, 3$ dividing $p - 1$. Let $\Delta = \mathbb{F}_p^\times = \mu_r \times \mu_{r'}$, $(r, r') = 1$, $R = \mathbb{Z}/r\mathbb{Z}$, $\mathbf{\Lambda} = R[\Delta]$, $\Lambda' = R[\mu_{r'}]$, and $\Lambda = R[\mu_r]$. Then Λ is a local R-algebra, and Λ' is étale over R. We have $\mathbf{\Lambda} = \Lambda \otimes \Lambda'$, and Λ is a direct summand (as an R-algebra) of $\mathbf{\Lambda}$, since R is a direct summand of Λ' (the corresponding idempotent is $(1/r')\,\Sigma_{\zeta \in \mu_{r'}} \langle \zeta \rangle$). If $\mathbf{I}$ is the augmentation ideal in $\mathbf{\Lambda}$, then $\mathbf{I} = I \otimes \Lambda' \oplus \Lambda \otimes I'$, where I and I' are the augmentation ideals in Λ and Λ' respectively. Observe that I is nilpotent and $I/I^2 = R \otimes \mu_r = R(1) \approx R$, but $I' = I'^2$, so $\mathbf{I}/\mathbf{I}^2 = I/I^2$. Define

$$V = J_0[r]^*, \qquad \mathbf{V} = J_1[r][I']^*,$$

where $J_1 = \mathrm{Jac}(X_1)$, $X_1 = X_1(p)_{/\mathbb{Q}}$. The group Δ acts on J_1 via the "diamond operators" (Δ is the Galois group of the cover X_1/X_0), and on $\mathbf{V}$ it acts through μ_r, hence $\mathbf{V}$ is a Λ-module. These should be thought of as the "refined" versions of the V and $\mathbf{V}$ described above. The fact that $\mathrm{Spec}(\Lambda)$ is connected guarantees that the resulting deformation theory is not trivial. The natural map from $\mathbf{V}$ to V is almost surjective—the cokernel is the dual of the r-torsion in the Shimura subgroup, and is small and well controlled. In particular, when we localize at a non-Eisenstein prime of the Hecke algebra, it disappears. Moreover, one can show that "away from the Eisenstein primes" V is the I-coinvariants of $\mathbf{V}$. An even better strategy, which will eventually allow us to include the Eisenstein primes in the discussion, is to replace V and $\mathbf{V}$ by $V^\#$ and $\mathbf{V}^\#$, which are obtained from the generalized Jacobians of X_0 and X_1 with respect to the modulus consisting of the cusps (each counted with multiplicity one). We call this modulus the (reduced) cuspidal modulus. See [Se] for generalized Jacobians, which show up once more, in a different context, in this work. In the rest of the introduction we shall ignore the complication coming from the $^\#$-ed modules, and consider only V and $\mathbf{V}$.

Having defined our modules, we shall analyze regular models of X_1 over $\mathbb{Z}_p$ and over the ring of integers of $K = \mathbb{Q}_p(\zeta)$ (ζ is a primitive pth root of unity), and study the Néron models of J_1 over the same fields. We shall construct a 2-step filtration of $\mathbf{V}$ as a representation of $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$,

$$0 \to \mathbf{U} \to \mathbf{V} \to \mathbf{W} \to 0. \tag{2}$$

Of the graded pieces of this filtration, $\mathbf{W}$ will be dual to the kernel of I' in the r-torsion of the *generalized* Jacobian of the Igusa curve $\mathrm{Ig}(p)$, with respect to the modulus of the supersingular points. This piece will therefore be unramified. The other piece $\mathbf{U}$ will be dual to $\mathbf{W}$ under the "twisted Weil pairing" of [M-W2], p.243, a pairing which is only defined over K. As a result, the inertia group $\mathrm{Gal}(K/\mathbb{Q}_p)$ will act on it through the "geometric inertia group action" ([M-W2], p. 236). The eigenvalue of Frobenius in its action on $\mathbf{W}$ will be related to Atkin's U_p-operator on J_1 (compare [M-W1], Ch. 2, §9).

Finally, we shall draw the information that our "refined deformation" carries about $q/p^{\mathrm{ord}(q)}$, except that we do it for the full p-adic period pairing of J_0, and we do not "project" to E, if an E as in the introduction exists (see [dS2] §6 to see how this is done).

0.5. Comparison with [M-W2]

Our analysis clearly relies on the results of Mazur-Wiles. The difference is in two aspects. First, since we deal with r-torsion rather than p-torsion, we cannot "decompose" our modules with respect to characters of μ_r (we can, and we do, isolate the identity character on μ_r). In fact, that is the whole point! Otherwise, we would not get any interesting deformation. Thus, we shall not be able, and not want, to discard the part on which Δ acts trivially, coming from J_0 (as Mazur and Wiles do in [M-W2]). Accordingly, we shall deal with the special fiber of the Néron model as a whole, and not just with its "abelian variety part". This is why we get *generalized* Jacobians. We emphasize that our deformation is captured exactly in the *extension class* of the Jacobian of $\mathrm{Ig}(p)$ by the toric part of the generalized Jacobian.

Another curious difference between our results, and those of [M-W2], concerns the question, Which of the graded pieces in the filtration of $\mathbf{V}$ is unramified? In [M-W2] the analogue of $\mathbf{U}$ is unramified. This is because in the filtration that they define on the p-divisible group of J_1 the *quotient* is unramified. This is a general fact about ordinary p-divisible groups: first comes the "kernel of reduction", and the quotient is unramified. In our work $\mathbf{W}$ is unramified. This is because in the filtration that we define on $J_1[r]$, the *submodule* $J_1[r]^{\mathrm{sub}}$ is unramified. Here too, this can be traced to

a general fact about the l-divisible group of a Néron model over a p-adic discrete valuation ring ($l \neq p$): the "partie fixe" (under inertia, to use Grothendieck's terminology [Groth]) of the l-divisible group is a *sub*group.

In contrast to [M-W2], we do not encounter problems arising from points of order p lying in the kernel of reduction, since p does not divide r. No "ordinariness" assumption intervenes in our work. On the other hand, the obstruction to splitting that we face, having to do with the generalized Jacobian of $\mathrm{Ig}(p)$ with respect to the supersingular modulus, is irrelevant to [M-W2], because the inclusion of the p-divisible group of J_0 in the p-divisible group of J_1 does split up to isogeny.

1. The deformation modules V and $V^{\#}$

1.1 Let the notation be as in 0.4. Let Σ be the Shimura subgroup of J_0([M], §II.11). Then we have an exact sequence

$$0 \to \Sigma \to J_0 \to J_1. \tag{1}$$

Let $\mathbf{T}_0$ be the subring of $\mathrm{End}(J_{0/\mathbb{Q}})$ generated over $\mathbb{Z}$ by the Hecke operators T_q (q prime $\neq p$) and U_p. Let $\mathbf{T}_1$ be the subring of $\mathrm{End}(J_{1/\mathbb{Q}})$ generated by T_q, U_p, and the diamond operators $\langle a \rangle$, for $a \in \Delta$. To avoid misunderstanding, we emphasize that if T is a Hecke correspondence on a modular curve, we let T denote also the endomorphism of its Jacobian that is induced by *Picard* functoriality. Thus, in the notation of [M-W1], Ch. 2, §5, $T_q = T_q^*$ etc., *contrary* to the convention used there. This is necessary because we shall study the map $J_0 \to J_1$ induced by Picard functoriality, and we need this map to be Hecke compatible.†

Both $\mathbf{T}_0$ and $\mathbf{T}_1$ are commutative, finite and flat over $\mathbb{Z}$, and $\mathbf{T}_1$ contains $\mathbb{Z}[\Delta/\langle \pm 1 \rangle]$ as a subring. Since Σ is finite and Hecke stable, we may identify the Hecke ring in $\mathrm{End}(J_0)$ with that in $\mathrm{End}(J_0/\Sigma)$, so we get a surjection from $\mathbf{T}_1$ to $\mathbf{T}_0$.

Let r be the maximal power of a prime $l \neq 2, 3$ dividing $p - 1$, and (notation as in 0.4)

$$V = J_0[r]^*, \qquad \mathbf{V} = J_1[r][I']^*. \tag{2}$$

†This remark is slightly misleading. Since $T^* = T_*$ on $J_0(p)$, we *could* have worked with the T_* and the maps $J_0 \to J_1$ would still be Hecke compatible. But in the presence of an auxiliary level of type $\Gamma_1(a)$, it will become important to consider the endomorphisms induced by Picard functoriality. A reflection of the same problem is present in [M-W1], Ch. 2, §9. In general (i.e. with an auxiliary $\Gamma_1(a)$ level), only U_p^* preserves what we call below $J^{\text{ét}}$ — loc. cit. Proposition 3, and not U_{p^*} — loc. cit. Proposition 1. However, in the case of $J_1(p)$ ($a = 1$) it is easily checked that in the diagram of Proposition 1 [M-W1] p. 253, U_{p^*} too preserves the Jacobian of the Igusa curve $J^{\text{ét}} = \beta_0(\mathrm{Pic}^0(\mathrm{Igusa}(p)_{/k})$, in the notation used there.

Then we have an exact sequence of Hecke and Galois modules

$$\mathbf{V} \to V \to \Sigma[r]^* \to 0. \tag{3}$$

In particular, $\mathbf{V}$ is a Λ-module.

1.2. Eisenstein ideals

Let $J_0^\#$ (resp. $J_1^\#$) be the generalized Jacobian of X_0 (resp. X_1) with respect to the (reduced) cuspidal modulus. It is an extension of J_0 (resp. J_1) by $D_0 = \mathbb{G}_m$ (resp. a $(p-2)$ dimensional torus D_1) defined over $\mathbb{Q}$. Since the Hecke correspondences on X_0 (resp. X_1) preserve the cusps, they define endomorphisms of $J_0^\#$ (resp. $J_1^\#$). Let $\mathbf{T}_0^\#$ (resp. $\mathbf{T}_1^\#$) be the rings generated by them. For $i = 0$ or 1, $\mathbf{T}_i^\#$ maps to $\mathrm{End}(D_i)$ (by restriction) and we let $\mathbf{I}_i^\#$ be the kernel of this homomorphism. On the other hand, $\mathbf{T}_i^\#$ maps surjectively onto $\mathbf{T}_i$ and we let $\mathbf{I}_i$ denote the image of $\mathbf{I}_i^\#$ under this map. We call $\mathbf{I}_i$ the *Eisenstein ideal* in $\mathbf{T}_i$. Any prime ideal in $\mathrm{spec}(\mathbf{T}_i)$ containing it is called an *Eisenstein prime.*

EXAMPLE. $\mathbf{I}_0$ contains, and in fact is generated by, $T_q - q - 1$, for $q \neq p$, and $U_p - 1$. Indeed, we have to show the same thing for $\mathbf{I}_0^\#$ (caution: the symbol T_q or U_p stands for different operators in different Hecke rings...). But $\mathrm{End}(D_0) = \mathbb{Z}$ is faithfully represented on the tangent space to D_0, whose *dual* may be identified with the line spanned by the unique (normalized) Eisenstein series of weight 2 for $\Gamma_0(p)$. It is well known that this Eisenstein series is annihilated by $T_q - q - 1$ and $U_p - 1$. Since $\mathbf{T}_0^\#/\mathbf{I}_0^\# = \mathbb{Z}$, these elements generate $\mathbf{I}_0^\#$. Thus $\mathbf{I}_0$ coincides with the Eisenstein ideal as defined in [M].

EXAMPLE. $\mathbf{I}_1$ contains $(T_q - 1 - \langle q\rangle q)(T_q - \langle q\rangle - q)$ for any $q \neq p$ (this follows from [M-W1], p. 238 by arguments similar to the above).

1.3 PROPOSITION. *The natural map of $J_0^\#$ into $J_1^\#$ (induced by Pic functoriality) is injective on r-torsion. Furthermore (for any natural number r) $J_0^\#[r] = J_1^\#[r]^\Delta$. If we let*

$$V^\# = J_0^\#[r]^*, \qquad \mathbf{V}^\# = J_1^\#[r][I']^*, \tag{4}$$

and denote by I the augmentation ideal in Λ, we get an isomorphism

$$\mathbf{V}^\# \otimes_\Lambda (\Lambda/I) \approx V^\#. \tag{5}$$

Proof. The proof is based on the identifications

$$J_1[r] = H^1_{\text{ét}}(X_1(p)_{/\bar{\mathbb{Q}}}, \mu_r), \quad J_1^\#[r] = H^1_{\text{ét,c}}(Y_1(p)_{/\bar{\mathbb{Q}}}, \mu_r)$$

($Y_1(p)$ = the *affine* part of $X_1(p)$) (see [Mi] III.1.30). Thus

$$\begin{aligned}\mathrm{Hom}(J_1^{\#}[r], R) &= \mathrm{Hom}(H^1_{\text{ét},c}(Y_1(p)_{/\bar{\mathbb{Q}}}, \mu_r), R)\\ &= H^1_{\text{ét}}(Y_1(p)_{/\bar{\mathbb{Q}}}, R) \quad \text{(Poincaré duality)}\\ &= H^1_{\text{sing}}(Y_1(p)(\mathbb{C}), R) \quad \text{(Artin's comparison theorem)}\\ &= H^1(\Gamma_1(p), R) \quad \text{(since } \Gamma_1(p) \text{ contains no elliptic elements).}\end{aligned}$$

Under these identifications the action of $\langle d\rangle$, $d \in \Delta$, on $J_1^{\#}[r]^*$ corresponds to the following action of Δ on $H^1(\Gamma_1(p), R)$. First, identify Δ with $\Gamma_0(p)/\Gamma_1(p)$ as usual, sending $\langle d\rangle$ to the class of a matrix γ whose *lower right* corner is d mod p. Next, if ψ is a 1-cocycle of $\Gamma_1(p)$ in R (i.e. a homomorphism), and $\gamma \in \Gamma_0(p)$, $\gamma\psi$ is the 1-cocycle $(\gamma\psi)_\sigma = \psi_{\gamma^{-1}\sigma\gamma}$. This defines an action of $\Gamma_0(p)/\Gamma_1(p) = \Delta$. We now invoke Shapiro's lemma

$$H^1(\Gamma_1(p), R) \approx H^1(\Gamma_0(p), \Lambda). \tag{6}$$

It can be checked that the Λ action on the left gets translated to the "obvious" Λ structure on the right, coming from the action on the coefficients. This is a well-defined action because $\Gamma_0(p)$ acts on Λ via the *abelian* quotient Δ, thereby in a manner that commutes with Λ's own action on itself, rendering the cohomology group a Λ-structure.

Now as Δ is cyclic, $\mathbf{I}$ is principal, say $\mathbf{I} = \alpha\Lambda$, with $\alpha = \langle d\rangle - 1$, d a generator of Δ. The l-cohomological dimension of $\Gamma_0(p)$ is 1, because $l \neq 2, 3$, and $\bar{\Gamma}_0(p)$ ($\bar{\Gamma} = \Gamma/\langle \pm 1\rangle$) is a free product of cyclic groups of orders 2 or 3, corresponding to elliptic conjugacy classes, and a free group. From the exact sequence $0 \to \mathbf{I} \to \Lambda \to R \to 0$ we get that

$$H^1(\Gamma_0(p), \mathbf{I}) \to H^1(\Gamma_0(p), \Lambda) \to H^1(\Gamma_0(p), R) \to 0 \tag{7}$$

is exact. From the exact sequence $0 \to \Lambda[\alpha] \to \Lambda \to \mathbf{I} \to 0$ we get that multiplication by α maps $H^1(\Gamma_0(p), \Lambda)$ surjectively onto $H^1(\Gamma_0(p), \mathbf{I})$, hence we may identify the image of $H^1(\Gamma_0(p), \mathbf{I})$ in $H^1(\Gamma_0(p), \Lambda)$ with $\mathbf{I}H^1(\Gamma_0(p), \Lambda)$. We conclude that there exists an isomorphism

$$H^1(\Gamma_0(p), \Lambda)/\mathbf{I}H^1(\Gamma_0(p), \Lambda) \approx H^1(\Gamma_0(p), R). \tag{8}$$

Since r is odd, $H^1(\Gamma_0(p), R) = H^1(\bar{\Gamma}_0(p), R)$. Now, even if $\bar{\Gamma}_0(p)$ has elliptic elements, they are of order prime to r, so an argument similar to the string of equalities at the beginning of the proof shows that $H^1(\bar{\Gamma}_0(p), R) = V^{\#}$, and (5) follows.

The injectivity of the map from $J_0^{\#}[r]$ to $J_1^{\#}[r]$ then follows by duality. What really happens here is that the Shimura subgroup dies in J_1, but survives in D_1, the toric part of $J_1^{\#}$. □

2. The filtration on V and $\mathbf{V}^{\#}$, and structure over Λ

2.1. In Section 1 (2) and (4) we defined Hecke modules $\mathbf{V}$ and $\mathbf{V}^{\#}$, which carry a commuting $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ action, and which we view as *deformations* of the corresponding V and $V^{\#}$ (despite the fact that for V, the map from $\mathbf{V}$ to V is not quite surjective). Of course, V and $\mathbf{V}$ are submodules of $V^{\#}$ and $\mathbf{V}^{\#}$ respectively. From many respects, the # modules are better behaved than the ones obtained from the ordinary Jacobians. This is already evident if we compare Section 1 (5) to Section 1 (3).

In this section we define a 2-step filtration on all of our four modules. This filtration will be stable under Hecke and the *local* Galois group at p. Once again, it will be better behaved for the # modules.

2.2. Let us start with V. Let S be the set of supersingular elliptic curves in characteristic p. Then $|S| = 1 + \mathrm{genus}(X_0(p))$, and X_0 has a well-known semi-stable model $\mathscr{X}_0$ over $\mathbb{Z}$, whose special fiber at p consists of two projective lines $\mathbb{P}_1^{\text{ét}}$ and $\mathbb{P}_1^{\mu}$ intersecting transversally at $|S|$ points which are in a natural bijection with S. In terms of the moduli problem $[\Gamma_0(p)]$ (see [K-M]), the smooth points of $\mathbb{P}_1^{\text{ét}}$ classify ordinary elliptic curves with an étale subgroup scheme of order p, and those of $\mathbb{P}_1^{\mu}$ elliptic curves with a connected subgroup scheme of multiplicative type (i.e. whose Cartier dual is étale) of order p. The intersection points are defined over $\mathbb{F}_{p^2}$. As a 2-dimensional scheme $\mathscr{X}_0$ is not regular (unless $p \equiv 1 \bmod 12$), but its singular points, which belong to the special fiber above p, and correspond to supersingular elliptic curves with j-invariant 0 or 1728, are *inconsequential* in the sense of [M-W1], p. 230. In the desingularization $\tilde{\mathscr{X}}_0$ of $\mathscr{X}_0$, the singular points are replaced by a string of (one or two) $\mathbb{P}^1$'s.

Let $N = \mathbb{Z}[S]$ and let N_0 be the augmentation subgroup of N. Let k be the quadratic unramified extension of $\mathbb{Q}_p$. The Galois group $\mathrm{Gal}(k/\mathbb{Q}_p)$ acts on S via the action of $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$. Hence N and N_0 are Galois modules for the local Galois group. The Jacobian J_0 has a rigid analytic uniformization by the torus $\mathrm{Hom}(N_0, \mathbb{G}_m)$. In fact, there exists a symmetric non-degenerate *period pairing*

$$Q: N_0 \times N_0 \to \mathbb{Q}_p^{\times} \tag{1}$$

(not only Q, but even $\mathrm{ord}_p \circ Q$ is nondegenerate) which induces an inclusion

$q: N_0 \to \mathrm{Hom}(N_0, \mathbb{Q}_p^\times)$, and an isomorphism of rigid analytic spaces over k

$$J_0 \approx \mathrm{Hom}(N_0, \mathbb{G}_m)/q(N_0). \tag{2}$$

For all this, see [dS1] and [dS3]. (Something has to be said to justify the fact that (1) is into $\mathbb{Q}_p^\times$ and not merely into $k^\times$. Thus the two sides of (2) are defined over $\mathbb{Q}_p$. The isomorphism between them is only defined over k, where J_0 attains *split* multiplicative reduction. However, as Galois modules $J_0(\bar{\mathbb{Q}}_p) \approx \mathrm{Hom}(N_0, \bar{\mathbb{Q}}_p^\times)/q(N_0)$ *over* $\mathbb{Q}_p$ if we let $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ act on $h \in \mathrm{Hom}(N_0, \bar{\mathbb{Q}}_p^\times)$ as $\sigma(h) = \sigma \circ h \circ \sigma^{-1}$.) It follows that we have a short exact sequence of $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$-modules

$$0 \to \mathrm{Hom}(N_0, \mu_r) \to J_0[r] \to N_0/rN_0 \to 0. \tag{3}$$

Dualizing, and setting $U = (N_0/rN_0)^*$ and $W = \mathrm{Hom}(N_0, \mu_r)^*$, we get our first filtration

$$0 \to U \to V \to W \to 0. \tag{4}$$

Alternatively, the Néron model $\mathscr{J}_0$ of J_0 over $\mathbb{Z}_p$ is semi-abelian. Let $\mathscr{J}_0(\mathcal{O}_L)^0$ denote its points in (the ring of integers of) an unramified extension L of $\mathbb{Q}_p$, which specialize to the connected componnt $(\mathscr{J}_{0/\mathbb{F}_p})^0$ of the special fiber. Since $(p, r) = 1$, the map on r-torsion

$$\mathscr{J}_0(\mathcal{O}_L)^0[r] \to (\mathscr{J}_{0/\mathbb{F}_p})^0(\kappa_L)[r]$$

is an isomorphism (κ_L is the residue field of L). In the model (2) the points in $\mathscr{J}_0(\mathcal{O}_L)^0$ correspond to $\mathrm{Hom}(N_0, U(L))$, where $U(L)$ are the units of the local field L. Their reduction corresponds to $\mathrm{Hom}(N_0, \kappa_L^\times)$.

Raynaud gave a characterization of $\mathscr{J}_0(\mathcal{O}_L)^0$ in terms of Cartier divisors on the regular scheme $\tilde{\mathscr{X}}_0$. We refer to [A], §1.20–1.21 for a concise description of his results, and to [B-L-R] (§9.5/4, see also §9.2/13) for full proofs. Raynaud's theorem says that $\mathscr{J}_0(\mathcal{O}_L)^0$ classifies line bundles $\mathscr{L}$ on $\tilde{\mathscr{X}}_0$ defined over L, whose restriction to each irreducible component of the special fiber is of degree 0. More generally, the functors $\mathscr{J}_0^0$ and $\mathrm{Pic}^0_{\tilde{\mathscr{X}}_0/\mathcal{O}_K}$ on $\mathcal{O}_K$-schemes, coincide. It follows that $(\mathscr{J}_{0/\mathbb{F}_p})^0$ classifies divisors δ supported (without loss of generality) on the smooth part of $\tilde{\mathscr{X}}_{0/\mathbb{F}_p}$, which are of degree 0 on each irreducible component, modulo divisors of functions. By a "function" on the reducible curve $\tilde{\mathscr{X}}_{0/\mathbb{F}_p}$ we mean a collection of functions, one for each component, which agree at the intersection points, and get there finite non-zero values.

In either language, of line bundles or of divisors, we can now make the isomorphism $(\mathscr{J}_{0/\mathbb{F}_p})^0(\kappa_L) \approx \mathrm{Hom}(N_0, \kappa_L^\times)$ explicit as follows. For simplicity, let us assume that $p \equiv 1 \bmod 12$. The modifications in the remaining cases are straightforward. Let $\sigma^{\text{ét}}$, σ^{μ} be sections over the two components of the special fiber trivializing $\mathscr{L}$. Taking the ratios of the σ's at the intersection points, labeled by S, we get a homomorphism from N to $\mathbb{G}_m$, whose restriction to N_0 is well defined (i.e. independent of the trivializing sections), and completely determines the restriction of $\mathscr{L}$ to the special fiber.

Thus $\mathrm{Hom}(N_0, \mu_r)$ is just the part of $J_0[r]$ which specializes to the connected component $(\mathscr{J}_{0/\mathbb{F}_p})^0$. In the language of [Groth], this is the "partie fixe", and also the "partie torique". On the other hand, N_0/rN_0 is the kernel of r in the group of connected components of the Néron model over a *sufficiently ramified* extension of $\mathbb{Q}_p$ (e.g., any extension over which all the r-torsion in J_0 is defined).

2.3. We now repeat the same analysis for the generalized Jacobian $J_0^\#$. For a treatment of Néron models of generalized Jacobians, see the last chapter of [B-L-R]. From the rigid analytic point of view, the Manin-Drinfeld uniformization of Jacobians of Mumford curves [M-D] can be nicely extended to generalized Jacobians, using a larger class of p-adic theta functions. In the case of $X_0(p)$ this was done in [dS3].

The two cusps $c^{\text{ét}}$ and c^{μ} of X_0 (represented by 0 and $i\infty$ under the usual complex uniformization) specialize to the corresponding components in $\mathscr{X}_0$. Let $\mathscr{J}_0^\#$ be the Néron model of $J_0^\#$ over $\mathbb{Z}_p$. Then $(\mathscr{J}^\#_{0/\mathbb{F}_p})^0$ consists of classes of divisors δ supported on the smooth part of $\tilde{\mathscr{X}}_{0/\mathbb{F}_p}$ and away from the cusps, which are of degree 0 in every irreducible component, *modulo* divisors of functions which give the same (finite, nonzero) value to the two cusps. We identify $(\mathscr{J}^\#_{0/\mathbb{F}_p})^0$ with $\mathrm{Hom}(N, \mathbb{G}_{m/\mathbb{F}_p})$ in the following way. Given a divisor δ as above, we may first assume, if p is not 1 mod 12, that δ does not pass through the components of $\tilde{\mathscr{X}}_{0/\mathbb{F}_p}$ obtained by blowing up the singular points of the arithmetical surface $\mathscr{X}_0$. Then δ corresponds to a pair of functions $(f^{\text{ét}}, f^{\mu})$ as above, but this time we normalize them to have the same value at the two cusps. The map $s \mapsto f^{\text{ét}}(s)/f^{\mu}(s)$ $(s \in S)$ defines a well-defined homomorphism from N to $\mathbb{G}_m$, that depends only on the class of δ in the generalizaed Jacobian.

The group of connected components of $\mathscr{J}^\#_{0/\mathbb{F}_p}$ is the same as that of $\mathscr{J}_{0/\mathbb{F}_p}$. We conclude that we have a short exact sequence of $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$-modules

$$0 \to \mathrm{Hom}(N, \mu_r) \to J_0^\#[r] \to N_0/rN_0 \to 0 \tag{5}$$

as in (3), with a similar interpretation regarding the Néron model.

We can arrive at the same conclusion from the rigid-analytic uniformization of $J_0^\#$. It was shown in [dS3] how to extend the period pairing Q to a pairing

of $N \times N_0$ into $\mathbb{Q}_p^\times$, and how to get a corresponding uniformization of rigid analytic spaces over k

$$J_0^\# = \mathrm{Hom}(N, \mathbb{G}_m)/q(N_0). \tag{6}$$

Now (5) follows from (6) easily.

Dualizing, and making the obvious definitions $V^\# = J_0^\#[r]^*$, $U^\# = U$, $W^\# = \mathrm{Hom}(N, \mu_r)^*$, we get from (5) the exact sequence

$$0 \to U^\# \to V^\# \to W^\# \to 0.$$

2.4. Similar analysis applies to X_1 and J_1 except that the picture is more complicated. First, J_1 only attains semi-abelian reduction over $K^+ = \mathbb{Q}_p(\zeta + \zeta^{-1})$ (ζ = a primitive pth root of 1). In fact, we shall work over $K = \mathbb{Q}_p(\zeta)$. Second, when we pass to $J_1^\#$ there are $p-1$ cusps, so the toric part is bigger.

Let $\mathscr{X}_1$ be the model of $X_1(p)$ over $\mathcal{O}_K$ discussed in [M-W1], p. 246 (Example 1 of §8, with $n = 1$, $a = 1$), or in [W] §5. In the language of [K-M], it corresponds to the moduli problem [bal. $\Gamma_1(p)$]. Its special fiber is reduced, and consists of two smooth components, $\Sigma^{\text{ét}}$ and Σ^μ, intersecting transversally at a set of points which is in bijection with S. The two components $\Sigma^{\text{ét}}$ and Σ^μ, are both isomorphic to the *Igusa curve* $\mathrm{Ig}(p)$ over $\mathbb{F}_p$. In fact, the involution w_ζ of X_1 extends to an involution of $\mathscr{X}_1$ which interchanges them. For more details, and proofs of the statements made here see [W] §5 and [M-W1]. Our notation is borrowed from there too.

Let $\mathscr{J}_1$ be the Néron model of J_1 over $\mathcal{O}_K$. The connected component of the special fiber $\mathscr{J}_{1/\mathbb{F}_p}$ is a semi-abelian variety. Let $\tilde{\mathscr{X}}_1$ be the desingulaization of $\mathscr{X}_1$. Its special fiber is semi-stable. By the above-mentioned theorem of Raynaud, the connected component $(\mathscr{J}_{1/\mathbb{F}_p})^0$ of $\mathscr{J}_{1/\mathbb{F}_p}$ consists of classes of divisors δ which are supported on the smooth part of $\tilde{\mathscr{X}}_{1/\mathbb{F}_p}$ and are of degree 0 on every irreducible component, *modulo* divisors of functions ("functions" have the same meaning as above). As in the case of X_0, the singularities of $\mathscr{X}_1$ are inconsequential, and every class is represented by a δ not passing through the $\mathbb{P}^1$'s which arise from the resolution of the singularities of $\mathscr{X}_1$. By pull-back to $\Sigma^{\text{ét}}$ and Σ^μ we get a surjective map from $(\mathscr{J}_{1/\mathbb{F}_p})^0$ to $J^{\text{ét}} \times J^\mu$, the product of the corresponding Jacobians, which are each isomorphic to the Jacobian of $\mathrm{Ig}(p)$, and are interchanged by the involution w_ζ. (Mazur and Wiles [M-W1] call $J^{\text{ét}} \times J^\mu$ the abelian-variety part of the Néron model, and denote it $av(J_1)$.) The kernel of this map is the toric part, and as above it is isomorphic to $\mathrm{Hom}(N_0, \mathbb{G}_m)$. We have established the existence of an exact sequence

$$0 \to \mathrm{Hom}(N_0, \mu_r) \to (\mathscr{J}_{1/\mathbb{F}_p})^0[r] \to J^{\text{ét}}[r] \times J^\mu[r] \to 0. \tag{7}$$

REMARK. There is another way to obtain (7), avoiding the study of any model of X_1. Consider the exact sequence of abelian varieties over K^+

$$0 \to J_0/\Sigma \to J_1 \to A_1 \to 0,$$

and the corresponding sequence of Néron models over $\mathcal{O}_{K^+}$. Langlands' theorem ([M-W1], Ch. 3, §2, Prop. 2) shows that A_1 acquires good reduction over K^+. It follows that J_1 has semi-abelian reduction. By Theorem 4 of [B-L-R] §7.5, the sequence of Néron models is exact, and this gives (7).

DEFINITION. Let $J_1[r]^{\text{sub}}$ be the pre-image in $(\mathcal{J}_{1/\mathbb{F}_p})^0[r]$ of $J^{\text{ét}}[r] \times \{0\}$. Let $J_1[r]^{\text{quot}} = J_1[r]/J_1[r]^{\text{sub}}$.

PROPOSITION. *$J_1[r]^{\text{sub}}$ is identified with the r-torsion in the generalized Jacobian of* Ig(p) *with respect to the (reduced) modulus consisting of the set S of supersingular points.*

Proof. By definition we have an exact sequence

$$0 \to \text{Hom}(N_0, \mu_r) \to J_1[r]^{\text{sub}} \to J^{\text{ét}}[r] \to 0.$$

A class in $(\mathcal{J}_{1/\mathbb{F}_p})^0$ maps to $J^{\text{ét}}$ if and only if it contains a divisor δ supported on (the smooth part of) $\Sigma^{\text{ét}}$. It is furthermore a divisor of a function in the above sense if an f can be found which is constant on Σ^{μ}, has the divisor δ on $\Sigma^{\text{ét}}$, and agrees at the intersections. Thus the pre-image of $J^{\text{ét}}$ in $(\mathcal{J}_{1/\mathbb{F}_p})^0$ classifies divisors prime to S on $\Sigma^{\text{ét}} = \text{Ig}(p)$ modulo divisors of functions which are constant along S, and this is precisely the generalized Jacobian. $J_1[r]^{\text{sub}}$ is simply the r-torsion in it. □

2.5. PROPOSITION. (i) *$J_1[r]^{\text{sub}}$ is a* $\text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$*-submodule of $J_1[r]$, stable under the Hecke algebra* $\mathbf{T}_1$.

(ii) *Let $\mathcal{J}_1'$ be the Néron model of $J_{1/\mathbb{Q}_p}$ over $\mathbb{Z}_p$. From the universal property of Néron models we get a map $\mathcal{J}_1' \times_{\mathbb{Z}_p} \mathcal{O}_K \to \mathcal{J}_1$, which induces a map of special fibers $\mathcal{J}'_{1/\mathbb{F}_p} \to \mathcal{J}_{1/\mathbb{F}_p}$. Then $J_1[r]^{\text{sub}}$ is the image of $(\mathcal{J}'_{1/\mathbb{F}_p})^0[r]$ under this map.*

(iii) *Fix a primitive* pth *root of unity ζ. Then the twisted Weil pairing of* [M-W2] §6, *defined by*

$$[x, y] = \langle x, w_\zeta y \rangle \in \mu_r \tag{8}$$

where $\langle \cdot, \cdot \rangle$ is the usual Weil pairing, sets $J_1[r]^{\text{sub}}$ and $J_1[r]^{\text{quot}}$ in duality.

(iv) *$J_1[r]^{\text{quot}}$ is an extension of the r-torsion in the group of connected components of the Néron model of J_1 over a sufficiently ramified extension of K, by $J^{\mu}[r]$.*

Proof. We start with part (ii). Let H_p be the subgroup of $\text{GL}_2(\mathbb{F}_p)$ consisting of matrices whose left column is ${}^t(\pm 1, 0)$ (but where no restriction is put on the lower right entry). Let $\mathcal{X}_1'$ be the model of X_1 over $\mathbb{Z}_p$ corresponding, in

the notation of [M-W1] §8, to this H_p. In the language of [K-M] it corresponds to the moduli problem (non-balanced) $[\Gamma_1(p)]$. This $\mathscr{X}'_1$ may not be regular, but again it has at worst inconsequential singularities. Its special fiber consists of two irreducible components. One, which we call $\Sigma'^{\text{ét}}$, is reduced, and its normalization is Ig(p). The other, which we call Σ'^{μ}, is the j-line with multiplicity $(p-1)/2$. See [K-M], p. 417. The two components intersect at $|S|$ points, which are in bijection with S. The natural map $\mathscr{X}_1 \to \mathscr{X}'_1 \times_{\mathbb{Z}_p} \mathcal{O}_K$ identifies $\Sigma'^{\text{ét}}$ with $\Sigma^{\text{ét}}$. We may now compute the connected component of the special fiber $(\mathscr{J}'_{1/\mathbb{F}_p})^0$ using the model $\mathscr{X}'_1$ as we did over K before. The result is that we obtain an extension of $J^{\text{ét}}$ by a connected affine algebraic group, whose multiplicative part is $\text{Hom}(N_0, \mathbb{G}_m)$, but which has a unipotent part as well. In fact, the argument given in the previous proposition for the Néron model over K shows that $(\mathscr{J}'_{1/\mathbb{F}_p})^0$ is precisely the generalized Jacobian of Ig(p) with respect to the non-reduced modulus which consists of the supersingular points with multiplicity $(p-1)/2$. Note that the unipotent part of the generalized Jacobian contributes nothing to the r-torsion in the special fiber because $(r, p) = 1$.

At any rate, since the map between Néron models is induced from the map between regular models, (ii) follows.

Part (i) follows from (ii), because we may identify $J_1[r]^{\text{sub}}$ with $(\mathscr{J}'_{1/\mathbb{F}_p})^0[r]$, and now we are considering Néron models over $\mathbb{Q}_p$, not over K. Note that $J_1[r]^{\text{sub}}$, and therefore its abelian-variety quotient $J^{\text{ét}}[r]$, are stable under *all* the Hecke operators, including U_p, despite the fact that U_p does not define a correspondence on the Igusa curve $\Sigma^{\text{ét}}$. Compare [M-W1] Prop. 3, Ch. 2, §9.

Let us prove (iii). $\text{Hom}(N_0, \mu_r)$ is stable under w_ζ. By a theorem of Groethendieck it is orthogonal to the whole kernel of r on the connected component $\mathscr{J}_1(\mathcal{O}_L)^0[r]$ under the Weil pairing ([Groth], "Théorème d'orthogonalité" IX.2.4), hence also under the twisted Weil pairing. It follows that the twisted Weil pairing, when restricted to $\mathscr{J}_1(\mathcal{O}_L)^0[r]$, factors through $J^{\text{ét}}[r] \times J^{\mu}[r]$ (see (7)). But here w_ζ evidently interchanges $J^{\text{ét}}$ with J^{μ}. Since the Weil pairing pairs $J^{\text{ét}}[r]$ trivially with $J^{\mu}[r]$, the twisted Weil pairing pairs $J^{\text{ét}}[r]$ trivially with itself. It follows that $J_1[r]^{\text{sub}}$ is a maximal isotropic submodule for the twisted pairing, which is of course a non-degenerate pairing into μ_r. Part (iii) follows from here.

Part (iv) is clear from the definition. □

2.6. We make a digression to explain the relation between the filtrations on $J_0[r]$ and $J_1[r]$. Consider the following diagram of Galois modules

$$\begin{array}{ccccccccc} 0 & \to & \text{Hom}(N_0, \mu_r) & \to & J_0[r] & \to & N_0/rN_0 & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & J_1[r]^{\text{sub}} & \to & J_1[r] & \to & J_1[r]^{\text{quot}} & \to & 0 \end{array} \tag{9}$$

where the middle vertical arrow is induced from Section 1 (1), hence its kernel

is $\Sigma[r]$. The left vertical arrow is induced from the map between $\mathscr{J}_0(\mathscr{O}_L)^0[r]$ and $\mathscr{J}_1'(\mathscr{O}_L)^0[r]$, where L is a large enough unramified extension of $\mathbb{Q}_p$. As before, the superscript 0 denotes sections reducing to the connected component of the special fiber. From the description of the filtration of $J_0[r]$ given in Section 2.2, it is clear that the left vertical arrow in (9) identifies $\mathrm{Hom}(N_0, \mu_r)$ with the same module inside $J_1[r]^{\mathrm{sub}}$ (see (7)), and is therefore injective. This is not new. The Shimura subgroup in fact gets mapped injectively into the group of connected components, and surjectively onto those connected components which are defined over $\mathbb{Q}_p$. See [M], Ch. II, §11.

The right vertical arrow is induced by the first two. Now, as mentioned above, $J_1[r]^{\mathrm{quot}}$ has a filtration

$$0 \to J^{\mu}[r] \to J_1[r]^{\mathrm{quot}} \to \Phi_1[r] \to 0 \tag{10}$$

where Φ_1 is the group of connected components of the special fiber of the Néron model of J_1 over a sufficiently ramified extension M of K. Now it can be checked that, since r divides $(p-1)/2$, the map on connected components $N_0/rN_0 = \Phi_0[r] \to \Phi_1[r]$ is identically zero. Nevertheless, we have

PROPOSITION. $\Sigma[r]$ *maps isomorphically onto the kernel of the right vertical arrow in* (9).

First proof. Recall that $J_0[r]/\Sigma[r]$ and $J_1[r]^{\mathrm{sub}}$ are both subgroups of $J_1[r]$ stable under U_p. Furthermore, on $H = (J_0[r]/\Sigma[r]) \cap J_1[r]^{\mathrm{sub}}$ the involution w_ζ acts like $-U_p$ because this is true on J_0 (where all the w_ζ are equal to w_p). Thus H is stable under w_ζ. But clearly w_ζ interchanges $J^{\text{ét}}$ and J^{μ} in its action on the connected component of the Néron model, so H must be contained in the toric part $\mathrm{Hom}(N_0, \mu_r)$ (see (7)). This proves our assertion.

Second proof. Instead of using U_p, one may use Mazur's result on the "multiplicity-one" of the mod l representations obtained from J_0. We leave the details to the reader. □

2.7. Since R is a direct summand of Λ', taking invariants under the diamond operators $\langle a \rangle$, for $a \in \mu_r$, (i.e., taking the kernel of I') is an operation that preserves exact sequences. Write $\mathbf{U} = J_1[r][I']^{\mathrm{quot}*}$, $\mathbf{W} = J_1[r][I']^{\mathrm{sub}*}$. Then we get a diagram

$$\begin{array}{ccccccc}
0 & \to & \mathbf{U} & \to & \mathbf{V} & \to & \mathbf{W} \to 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \to & U & \to & V & \to & W \to 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & \Sigma[r]^* = \Sigma[r]^* & \to & 0 & &
\end{array} \tag{11}$$

with exact rows and columns. This diagram is *dual* to (9).

Finally, we wish to extend the analysis of $J_1[r]$ carried out in Section 2.4 to $J_1^{\#}[r]$, the r-torsion in the generalized Jacobian of X_1 with respect to the (reduced) cuspidal modulus C. The set of cusps is the union $C^{\text{ét}} \cup C^{\mu}$ of the cusps above $c^{\text{ét}}$ and those above c^{μ}. Each contains $(p-1)/2$ cusps, on which Δ acts transitively. In the model $\mathscr{X}_1$ over $\mathcal{O}_K$, the cusps reduce (mod π_K) *injectively*, those in $C^{\text{ét}}$ to the cusps of the Igusa curve $\Sigma^{\text{ét}}$, and those in C^{μ} to the cusps of the Igusa curve Σ^{μ}. The two groups of cusps are interchanged by the involution w_{ζ}.

Let $\mathscr{J}_1^{\#}$ be the Néron model of $J_1^{\#}$ over $\mathcal{O}_K$. It is an extension of $\mathscr{J}_1$ by the torus D_1 (defined over $\mathcal{O}_K$). Similarly, the connected component of its special fiber is an extension of $(\mathscr{J}_{1/\mathbb{F}_p})^0$ by $D_{1/\mathbb{F}_p}$. Now $(\mathscr{J}_{1/\mathbb{F}_p}^{\#})^0$ classifies divisors δ on $\tilde{\mathscr{X}}_{1/\mathbb{F}_p}$, relatively prime to C and the singular points, which are of degree 0 on every irreducible component, *modulo* divisors of functions f which get a constant finite non-zero value along C. (See Section 2.3 for the notion of a "function" on the reducible scheme $\tilde{\mathscr{X}}_{1/\mathbb{F}_p}$.) Once again, since the singularities of $\mathscr{X}_1$ are inconsequential, we may assume that δ is supported on $\Sigma^{\text{ét}} \cup \Sigma^{\mu}$. When we restrict to those divisors supported in the smooth locus of $\Sigma^{\text{ét}}$ (and away from $C^{\text{ét}}$), we see that the divisors by which we have to mod out are divisors of functions f for which there exists an α such that f restricted to $\Sigma^{\mu} \cup C^{\text{ét}}$ gets the constant value α. We therefore define

DEFINITION. $J_1^{\#}[r]^{\text{sub}} = r$-torsion in the group

$$\frac{\{\delta \mid \delta \text{ is a divisor of degree 0 on } \Sigma^{\text{ét}}, \text{ disjoint from } S \cup C^{\text{ét}}\}}{\{(f) \mid \exists \alpha \neq 0, \infty \text{ s.t. } f|_{S \cup C^{\text{ét}}} = \alpha\}}. \tag{12}$$

However, this group is nothing but the generalized Jacobian of Ig(p) with respect to the modulus $S \cup C^{\text{ét}}$. It admits a filtration

$$0 \to \text{Hom}(\mathbb{Z}[S \cup C^{\text{ét}}]_0, \mu_r) \to J_1^{\#}[r]^{\text{sub}} \to J^{\text{ét}}[r] \to 0. \tag{13}$$

Under the map of $J_1^{\#}[r]$ to $J_1[r]$, whose kernel is $D_1[r] = \text{Hom}(\mathbb{Z}[C]_0, \mu_r)$, $J_1^{\#}[r]^{\text{sub}}$ maps to $J_1[r]^{\text{sub}}$ with kernel $\text{Hom}(\mathbb{Z}[C^{\text{ét}}], \mu_r)$. The inclusion of $\text{Hom}(\mathbb{Z}[C^{\text{ét}}], \mu_r)$ in $\text{Hom}(\mathbb{Z}[C]_0, \mu_r)$ is obtained from the exact sequence

$$0 \to \mathbb{Z}[C^{\mu}]_0 \to \mathbb{Z}[C]_0 \to \mathbb{Z}[C^{\text{ét}}] \to 0. \tag{14}$$

A similar sequence gives the inclusion

$$\text{Hom}(\mathbb{Z}[C^{\text{ét}}], \mu_r) \subseteq \text{Hom}(\mathbb{Z}[S \cup C^{\text{ét}}]_0, \mu_r).$$

PROPOSITION. *Let* $J_1^{\#}[r]^{\text{quot}} = J_1^{\#}[r]/J_1^{\#}[r]^{\text{sub}}$. *Define, as before*

$$\mathbf{U}^{\#} = (J_1^{\#}[r][I']^{\text{quot}})^*, \qquad \mathbf{W}^{\#} = (J_1^{\#}[r][I']^{\text{sub}})^*.$$

Then we have a commutative diagram with exact rows and surjective vertical arrows

$$\begin{array}{ccccccccc} 0 & \to & \mathbf{U}^{\#} & \to & \mathbf{V}^{\#} & \to & \mathbf{W}^{\#} & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & U^{\#} & \to & V^{\#} & \to & W^{\#} & \to & 0. \end{array} \tag{15}$$

Proof. To prove the surjectivity of the vertical arrows recall that the middle one is surjective by Proposition 1.3. The map between the W's is therefore surjective also. The following lemma concludes the proof of the surjectivity.

LEMMA. *The map* $J_0^{\#}[r]^{\text{quot}} \to J_1^{\#}[r]^{\text{quot}}$ *is injective.*

Proof. Let

$$B = \operatorname{Coker}(J_0^{\#}[r] \to J_1^{\#}[r]) \quad \textit{and} \quad A = \operatorname{Coker}(J_0^{\#}[r]^{\text{sub}} \to J_1^{\#}[r]^{\text{sub}}).$$

From the snake lemma we see that we have to prove that the natural map $A \to B$ is injective. Consider the commutative diagrams with exact rows and columns

$$\begin{array}{ccccccccc} & & & & 0 & \to & \Sigma[r] & \dashrightarrow & \\ & & & & \downarrow & & \downarrow & & \\ 0 & \to & \operatorname{Hom}(\mathbb{Z}, \mu_r) & \to & J_0^{\#}[r] & \to & J_0[r] & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & \operatorname{Hom}(\mathbb{Z}[C]_0, \mu_r) & \to & J_1^{\#}[r] & \to & J_1[r] & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & \dashrightarrow & \operatorname{Hom}(\mathbb{Z}[C^{\text{ét}}]_0 \times \mathbb{Z}[C^{\mu}]_0, \mu_r) & \to & B & \to & J_1[r]/\operatorname{im} J_0[r] & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array} \tag{16}$$

and

$$\begin{array}{ccccccc} & & 0 & & 0 & & 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 \to & & \mathrm{Hom}(\mathbb{Z}, \mu_r) & \to & J_0^{\#}[r]^{\mathrm{sub}} & \to & J_0[r]^{\mathrm{sub}} \to 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 \to & \mathrm{Hom}(\mathbb{Z}[C^{\text{ét}}], \mu_r) & \to & J_1^{\#}[r]^{\mathrm{sub}} & \to & J_1[r]^{\mathrm{sub}} \to 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 \to & \mathrm{Hom}(\mathbb{Z}[C^{\text{ét}}]_0, \mu_r) & \to & A & \to & J^{\text{ét}}[r] & \to 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ & & 0 & & 0 & & 0 \end{array} \tag{17}$$

from which we get the following diagram with exact rows

$$\begin{array}{ccccccc} 0 \to & & \mathrm{Hom}(\mathbb{Z}[C^{\text{ét}}]_0, \mu_r) & & \to A \to & J^{\text{ét}}[r] & \to 0 \\ & & \downarrow & & \downarrow & \downarrow & \\ 0 \to & \mathrm{Hom}(\mathbb{Z}[C^{\text{ét}}]_0 \times \mathbb{Z}[C^{\mu}]_0, \mu_r)/\Sigma[r] & \to & B & \to & J_1[r]/\mathrm{im}\, J_0[r] & \to 0 \end{array} \tag{18}$$

Proposition 2.6 asserts that the right vertical arrow is injective. On the other hand, $\Sigma[r]$ is invariant under the $w_\zeta (= w_p)$ involution, which acts on it via multiplication by -1. If an element h of $\mathrm{Hom}(\mathbb{Z}[C^{\text{ét}}]_0 \times \mathbb{Z}[C^{\mu}]_0, \mu_r)$, which is obtained from $\Sigma[r]$ via the connecting homomorphism in (16), also vanishes on $\mathbb{Z}[C^{\mu}]_0$, it vanishes as well on $w_\zeta(\mathbb{Z}[C^{\mu}]_0) = \mathbb{Z}[C^{\text{ét}}]_0$, so $h = 0$ identically. This proves the injectivity of the left vertical arrow in (18), hence of the map $A \to B$. □

2.8. PROPOSITION. $\mathbf{U}^{\#}$ *is free over* Λ, *and we have an isomorphism*

$$U^{\#} \approx \mathbf{U}^{\#} \otimes_{\Lambda} (\Lambda/I). \tag{19}$$

Proof. We proved a similar statement for $\mathbf{V}^{\#}$ in Proposition 1.3. Our proof here is more subtle, because the arguments of Section 1.3, involving Eichler-Shimura cohomology, are not well-adapted to the study of the filtration introduced in Section 2. We proceed in several steps.

Step 1. $\mathbf{V}^{\#} \approx (\Lambda/I) \oplus \Lambda^{2m}$, where $m = \mathrm{genus}(X_0)$, as Λ-modules.

Proof. In Section 1.3 we got the isomorphism

$$\mathbf{V}^{\#} \approx H^1(\Gamma_0, \Lambda)[I'] = H^1(\Gamma_0, \Lambda) = H^1(\bar{\Gamma}_0, \Lambda) = Z^1/B^1$$

where Z^1 and B^1 denote cocycles and coboundaries respectively. Furthermore, $\bar{\Gamma}_0$ is a free product of cyclic subgroups of orders 2 or 3, one for each elliptic conjugacy class, and a free group on $2m+1$ generators. Let T denote the normal subgroup of $\bar{\Gamma}_0$ generated by the elliptic elements. Then $\bar{\Gamma}_0/T \approx \pi_1(Y_0)$ is free of rank $2m+1$. We may choose $\gamma_0, \ldots, \gamma_{2m}$ in $\bar{\Gamma}_0$ so that $\gamma_i \in \Gamma_1$ for $1 \leqslant i \leqslant 2m$, and the images of the $2m+1$ elements mod T generate $\pi_1(Y_0)$. It follows that the projection of γ_0 to Δ generates Δ, so $(\gamma_0 - 1)\Lambda = \mathrm{I}$. Observe that T acts trivially on Λ since $(r, 6) = 1$. A cocycle in Z^1 is therefore a homomorphism when restricted to T, and since $(r, 6) = 1$, it vanishes on generators of T, hence on all of T. Now Z^1 and B^1 are Λ-modules, so $Z^1 \approx \Lambda^{2m+1}$ via $z \mapsto (z(\gamma_i))_{0 \leqslant i \leqslant 2m}$. Since $\bar{\Gamma}_0$ acts on Λ via its quotient μ_r, B^1 is identified with $I \times 0 \times \cdots \times 0$, and the structure of H^1 follows (although non-canonically).

Step 2. Choose a set of generators $v_0, v_1, \ldots, v_{2m}$ for $\mathbf{V}^\#$ over Λ compatible with the decomposition of Step 1. Let u_i be the image of v_i in

$$V^\# = \mathrm{Hom}(\bar{\Gamma}_0, R) = \mathrm{Hom}(J_0^\#[r], R).$$

Now giving a homomorphism u in $V^\#$ is the same as giving X, a cyclic cover of X_0 of degree dividing r, which is unramified outside the cusps, together with a generator of the Galois group of X/X_0. Such a u comes from V if and only if X/X_0 is everywhere unramified. From the rigid analytic interpretation of $U = \mathrm{Hom}(N_0, R)$ it is clear that u belongs to U if and only if X is a Mumford curve. Indeed, N_0 is canonically the abelianization of the (free, rank m) subgroup $\tilde{\Gamma}$ of $\mathrm{PGL}_2(k)$ giving the p-adic Schottky uniformization of X_0. Finite quotients of $\tilde{\Gamma}$ are in one-to-one correspondence with unramified coverings of X_0 by Mumford curves.

Consider in particular the unique cyclic cover X of degree r between X_0 and X_1. Any u corresponding to it should vanish on Γ_1, hence on γ_i for $i \geqslant 1$, and should provide an isomorphism of $R \otimes (\bar{\Gamma}_0/\Gamma_1) = R \otimes \Delta = \mu_r$ with R. Hence we may assume that u_0 is this u (note that u_0 corresponds to an everywhere unramified cover of X_0 because it lies in the parabolic cohomology — its restriction to the standard parabolic subgroup P is trivial because $P \subseteq \Gamma_1$). We conclude that u_0 in fact lies in V, but *not* in U, because it is well known that no subcover of $X_1 \to X_0$ except for X_0 itself is a Mumford curve.

For the same reason, the projection of u_0 to $W \subseteq W^\#$ is of order r. *A fortiori*, the projection of $\Lambda/I = \Lambda/I \cdot v_0$ to $\mathbf{W}^\#$ is an isomorphism and $\mathbf{U}^\#$ is mapped injectively into $\Lambda^{2m} = \oplus \Lambda v_i$ $(1 \leqslant i \leqslant 2m)$, when we mod out by $(\Lambda/I)v_0$.

Step 3. We conclude by a counting argument. The rank over R of $U^\# = U = \mathrm{Hom}(N_0, R)$ is m. Changing the original bases we may assume that $U^\#$ has $u_1, \ldots, u_m$ for a basis over R. Choose $x_1, \ldots, x_m$ in $\mathbf{U}^\# \subseteq \Lambda^{2m} = \oplus \Lambda v_i$ lifting the u_i. Mod I, the vectors x_i look like the first m standard basis vectors v_i. It

easily follows that the sum $\Sigma \Lambda x_i$ is a direct sum, isomorphic to Λ^m. Indeed, the first $m \times m$ minor in the $m \times 2m$ matrix (λ_{ij}) giving $x_i = \Sigma \lambda_{ij} v_j$ is congruent to 1 mod I, hence so is its determinant. Since I is a nilpotent ideal, this minor is invertible as a matrix over Λ.

But the rank over R of $\mathbf{U}^\#$ is the rank of $J_1^\#[r][I']^{\text{quot}}$, which is

$$\text{rk}(J_1^\#[r][I']) - \text{rk}(J_1^\#[r][I']^{\text{sub}}).$$

Denote by X the unique cover of X_0 of degree r, dominated by X_1 (as above). Since $[X_1 : X] = r'/2$ is relatively prime to r, it is easy to see that $J_1^\#[r][I'] = J_X^\#[r]$, where by $J_X^\#$ we of course mean the generalized Jacobian of X with respect to its cuspidal modulus. Now X has a regular model similar to the one constructed for X_0 or X_1 over $\mathbb{Z}_p[\zeta_p]$. Also, X is an unramified cover of X_0, and has $2r$ cusps. We compute

$$\text{rk}\, J_X^\#[r] = 2(\text{genus}(X)) + 2r - 1 = r(2m - 2) + 2r + 1 = 2rm + 1$$

$$\text{rk}\, J_X^\#[r]^{\text{sub}} = \text{rk}\, J_X^{\text{ét}}[r] + \text{rk}\, \mathbb{Z}[S_X \cup C_X^{\text{ét}}]_0 = 2\,\text{genus}(\text{Ig}_X(p)) + m + r.$$

Here the subscript X refers to the objects related to the regular model of X. For example, Ig_X is the quotient of Ig by the action of $\mu_{r'}$. But

$$2\,\text{genus}(\text{Ig}_X(p)) + m = \text{genus}(X),$$

so we get $\text{rk}\, \mathbf{U}^\# = rm$. Since we already found a copy of Λ^m in $\mathbf{U}^\#$, it follows that $\mathbf{U}^\# = \oplus \Lambda x_i \approx \Lambda^m$, and, incidently, that $\mathbf{W}^\# \approx \Lambda/I \oplus \Lambda^m$.

Finally, (19) follows from the freeness of $\mathbf{U}^\#$ and from the analogous result for the full $\mathbf{V}^\#$. □

2.9. COROLLARY. *We have*

$$I\mathbf{U}^\#/I^2\mathbf{U}^\# \approx \mathbf{U}^\#/I\mathbf{U}^\# \approx U^\# = U. \qquad (20)$$ □

The first isomorphism in (20) is non-canonical. It depends on choosing a generator for Δ. Nevertheless, it is an isomorphism for both the Hecke action and the Galois group action, facts that will be crucial later on.

2.10. For future reference we gather the main results of Sections 1 and 2 in the following theorem.

THEOREM 1. *Let p be a prime, and $r = l^n$ the maximal power of a prime $l \neq 2, 3$ dividing $p - 1$. Then we have a commutative diagram of Hecke and* $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$*-modules, with surjective vertical arrows*

$$\begin{array}{ccccccccc} 0 & \to & \mathbf{U}^{\#} & \to & \mathbf{V}^{\#} & \to & \mathbf{W}^{\#} & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & U^{\#} & \to & V^{\#} & \to & W^{\#} & \to & 0. \end{array}$$

In this diagram $U^{\#} = \mathrm{Hom}(N_0, R)$, $W^{\#} = \mathrm{Hom}(N, \mu_r)^*$. $\mathbf{W}^{\#}$ is dual to the kernel of I' on the r-torsion in the generalized Jacobian of $\mathrm{Ig}(p)$*, where "generalized" is with respect to the modulus consisting of the $(p-1)/2$ cusps of* $\mathrm{Ig}(p)$ *and the supersingular points (each counted with multiplicity* 1*).*

As Λ-modules $\mathbf{U}^{\#} \approx \Lambda^m$, $\mathbf{V}^{\#} \approx \Lambda/I \oplus \Lambda^{2m}$, and $\mathbf{W}^{\#} \approx \Lambda/I \oplus \Lambda^m$. The bottom row is identified with the top row $\otimes \Lambda/I$. □

3. Galois structure and consequences for the Q-pairing

3.1. For any R-module M we denote by $M(1)$ or by $M(\chi)$ the module $M \otimes_R \mu_r$. M and $M(\chi)$ are isomorphic, even as $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ modules, in case M is equipped with a Galois action, but non-canonically. We think of χ as the mod-r cyclotomic character, although since $r \mid p - 1$, it is trivial.

Let

$$\tilde{U}^{\#} = \mathbf{U}^{\#}/I^2\mathbf{U}^{\#}, \tag{1}$$

and similarly for W and V. Consider the commutative diagram of $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$-Hecke-modules with exact rows and columns

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & U^{\#} \otimes_R I/I^2 & \to & V_0^{\#} & \to & W_0^{\#} & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & \tilde{U}^{\#} & \to & \tilde{V}^{\#} & \to & \tilde{W}^{\#} & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & U^{\#} & \to & V^{\#} & \to & W^{\#} & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array} \tag{2}$$

Here the bottom two rows repeat the diagram of Theorem 1, except that we work mod I^2 everywhere. The first row is defined by the diagram. Note that by Corollary 2.9 (20) the kernel of $\tilde{U}^\# \to U^\#$ is isomorphic to $U^\#$, but more canonically it is $U^\# \otimes_{\Lambda/I} I/I^2$. To identify it with $U^\#$ we need to fix a generator d of Δ, by means of which we can identify $I/I^2 = R \otimes \Delta$ with $\Lambda/I = R$, sending $d - 1 \bmod I^2$ to 1.

3.2. Let us examine the Galois action on

$$\tilde{W}^\#(1) = \mathrm{Hom}(J_1^\#[r][I']^{\mathrm{sub}}, \mu_r) \otimes_\Lambda \Lambda/I^2.$$

It is evidently unramified, so we only have to specify the action of Frob_p, the (absolute) Frobenius automorphism. For the next result compare Proposition 3 in Chapter 2, Section 9 of [M-W1].

PROPOSITION. *The Hecke operator U_p is invertible in its action on $\mathbf{V}^\#$, and therefore on any of the modules in Theorem* 1 *or* (2) *above. On $\tilde{W}^\#(1)$ we have the identity*

$$\mathrm{Frob}_p = U_p. \tag{3}$$

Proof. The first statement is clear, since U_p acts invertibly on $V^\#$, which is the I-coinvariants of $\mathbf{V}^\#$, and I is a nilpotent ideal. According to the conventions explained in 0.4, it is definitely enough to show that on $J_1^\#[r]^{\mathrm{sub}}$ we have

$$\mathrm{Frob}_p^{-1} = U_p (= U_p^*, \text{ induced by Pic functoriality}).$$

Let $x = (E, P)$ be a point of X_1. Then $U_p^*(E, P) = \Sigma(E', P')$ where the sum is over all pairs having a subgroup C' of order p not containing P' such that $(E, P) \approx (E'/C', P' \bmod C')$. Clearly $E' \approx E'/E'[p] = E'/(C' + \langle P' \rangle) = E/\langle P \rangle$ for such a pair. For P' we may take any pth root of P, mod $\langle P \rangle$. There are p possibilities.

Now look at the Zariski closure of the point x in $\tilde{\mathscr{X}}_1$, and assume (recalling the definition of $J_1^\#[r]^{\mathrm{sub}}$) that its specialization falls in $\Sigma^{\text{ét}}$. Then P does not reduce to 0, and therefore it generates (in the special fiber) the kernel of Verschiebung, and $E' = E^{(p^{-1})}$. We claim that P' reduces to $P^{(p^{-1})}$. Indeed, applying Frob_p to E' is like dividing E by the kernel of p, a homomorphism that sends P' to P (all in the special fiber).

We get that in the special fiber U_p^* has the same effect on divisors of degree 0 *passing through* $\Sigma^{\text{ét}}$ as $\mathrm{Ver}_p = p \cdot \mathrm{Frob}_p^{-1}$. Since $p \equiv 1 \bmod r$, this proves our proposition. □

Let ϕ be the unramified character of $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ with values in (the group of units of) the *image* of the Hecke algebra $\mathbf{T}_1^{\#}$ in $\mathrm{End}(\mathbf{V}^{\#})$, defined by $\phi(\mathrm{Frob}_p) = U_p$. If M is a Galois and Hecke module over R, let $M(\chi\phi^{-1})$ be the module $M(\chi)$ on which $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ acts via the original action twisted by the character ϕ^{-1}. This is well defined because the actions of Galois and Hecke commute.

Since the homomorphisms in (2) preserve the Hecke action we may apply $-(\chi\phi^{-1})$ to the whole diagram. When we do so, the right column (of the W's) acquires the trivial Galois action. Apply the long exact sequence in Galois cohomology. We write a portion of the resulting diagram.

$$\begin{array}{ccc} H^0(\mathbb{Q}_p, \tilde{W}^{\#}(\chi\phi^{-1})) & \longrightarrow & H^1(\mathbb{Q}_p, \tilde{U}^{\#}(\chi\phi^{-1})) \\ \downarrow & & \downarrow \\ H^0(\mathbb{Q}_p, W^{\#}(\chi\phi^{-1})) & \xrightarrow{\check{q}_R} & H^1(\mathbb{Q}_p, U^{\#}(\chi\phi^{-1})) \\ & & \downarrow{\scriptstyle \delta} \\ & & H^2(\mathbb{Q}_p, U^{\#}(\chi\phi^{-1}) \otimes_R I/I^2) \end{array} \tag{4}$$

Now the arrow between the H^0 terms on the left is surjective, because the modules carry the trivial Galois action. Thus we conclude

$$\delta \circ \check{q}_R = 0. \tag{5}$$

Our purpose is to identify the modules participating in (4), and to make the homomorphisms $\check{q}_R$ and δ explicit using Kummer theory and local class field theory.

3.3. LEMMA. *We have the following canonical identifications (as Hecke modules; the Galois action is trivialized after we take cohomology)*

(i) $H^0(\mathbb{Q}_p, W^{\#}(\chi\phi^{-1})) = W^{\#}(\chi\phi^{-1}) = N \otimes R$.
(ii) $H^1(\mathbb{Q}_p, U^{\#}(\chi\phi^{-1})) = N_0^{\vee} \otimes \mathbb{Q}_p^{\times} \otimes R$, *where* $N_0^{\vee} = \mathrm{Hom}(N_0, \mathbb{Z})$.
(iii) $H^2(\mathbb{Q}_p, U^{\#}(\chi\phi^{-1}) \otimes_R I/I^2) = N_0^{\vee} \otimes R \otimes_R (I/I^2)$.

Proof. (i) $W^{\#}(\chi\phi^{-1}) = \mathrm{Hom}(N, \mu_r)^*(1)$ with trivial Galois action
$= \mathrm{Hom}(\mathrm{Hom}(N, \mu_r), \mu_r) = N \otimes R$.
(ii) $H^1(\mathbb{Q}_p, U^{\#}(\chi\phi^{-1})) = H^1(\mathbb{Q}_p, \mathrm{Hom}(N_0, \mu_r)(\phi^{-1}))$

The effect of the twist by ϕ^{-1} on $\mathrm{Hom}(N_0, \mu_r)$ is to trivialize the Galois action

(on N_0, Frob_p and U_p act the same, via the quadratic unramified character). We may therefore write

$$= \mathrm{Hom}(N_0, H^1(\mathbb{Q}_p, \mu_r))$$
$$= \mathrm{Hom}(N_0, \mathbb{Q}_p^\times \otimes R) \text{ (Kummer theory)} = N_0^\vee \otimes \mathbb{Q}_p^\times \otimes R.$$

(iii) It is enough to prove that $H^2(\mathbb{Q}_p, U^\#(\chi\phi^{-1})) = N_0^\vee \otimes R$. But as in (ii) we get

$$H^2(\mathbb{Q}_p, \mathrm{Hom}(N_0, \mu_r)(\phi^{-1})) = \mathrm{Hom}(N_0, H^2(\mathbb{Q}_p, \mu_r)) = \mathrm{Hom}(N_0, R). \qquad \square$$

3.4. LEMMA. *Via identifications* (i) *and* (ii) *made in Lemma* 3.3, *the map* $\check{q}_R$ *of* (4) *is* (*up to a sign, depending on how one normalizes the connecting homomorphism*) *the map "*$\check{q} \bmod r$*" where* $\check{q}: N \to N_0^\vee \otimes \mathbb{Q}_p^\times$ *is the map obtained from the p-adic period pairing* $Q: N \times N_0 \to \mathbb{Q}_p^\times$. (See §2.3 and [dS3].)

REMARK. Previously (§2(6)), we called q the dual map $N_0 \to N^\vee \otimes \mathbb{Q}_p^\times$ obtained from Q. Of course, either q or $\check{q}$ completely determines Q, and vice versa. In terms of 1-motives we are considering *dual* 1-motives: previously we talked about the 1-motive given by $J_0^\#$. Now we talk about the 1-motive given by J_0 plus the map of $\mathbb{Z}$ into it sending 1 to the class of the divisor c^μ-$c^{\text{ét}}$. The restriction of Q to N_0 is symmetric and defines the self-dual 1-motive J_0.

Proof. The proof is a standard application of Kummer theory. See [G-S] (3.12) for a similar situation. We have to consider the exact sequence (5) of Section 2.3, twisted by $\chi\phi^{-1}$ and dualized, and compute its connecting homomorphism. Since the effect of ϕ^{-1} is to trivialize the Galois action on N and N_0 in their appearances in this exact sequence, instead of carrying the notation $-(\phi^{-1})$ everywhere, we shall *pretend* that N and N_0 have trivial Galois actions (i.e. replace $J_0^\#$ by its "quadratic twist" which has a *totally split* reduction over $\mathbb{Q}_p$).

Let $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$, $x \in N$, and $y \in N_0$. Let $x_R \in N \otimes R = W^\#(\chi\phi^{-1})$ be the induced homomorphism $\mathrm{Hom}(N, \mu_r) \to \mu_r$. Let y_R be the image of y in $N_0 \otimes R$. Recalling the exact sequence (5) in Section 2.3, and the identification $J_0^\# = \mathrm{Hom}(N, \mathbb{G}_m)/q(N_0)$, let $\bar{x}_R$ be an extension of x_R to a homomorphism from $J_0^\#[r]$ to μ_r. We view $\bar{x}_R$ as a homomorphism from $q(N_0)^{1/r}$ ($\subseteq \mathrm{Hom}(N, \mathbb{G}_m)$) into μ_r, trivial on $q(N_0)$. Since $(\sigma - 1)(\bar{x}_R)$ is trivial on $\mathrm{Hom}(N, \mu_r)$, it induces a homomorphism $N_0 \otimes R \to \mu_r$, and we may evaluate it on y_R. Since $\mu_r \subseteq \mathbb{Q}_p$, Kummer theory supplies us with a certain $\beta(x, y) \in \mathbb{Q}_p^\times \otimes R$, independent of σ, such that

$$[(\sigma - 1)(\bar{x}_R)](y_R) = (\sigma - 1)(\beta(x, y)^{1/r}).$$

By the definition of the connecting homomorphism, $[\check{q}_R(x_R)](y_R) = \beta(x, y)$ (here we have used Lemma 3.3 (i) and (ii)).

To compute $\beta(x, y)$ lift y_R to a $\tilde{y}_R \in J_0^{\#}[r]$ and let $\tilde{y} \in q(N_0)^{1/r} \subseteq \mathrm{Hom}(N, \mathbb{G}_m)$ represent it. Then $q(y) = Q(\cdot, y) \equiv \tilde{y}^r \bmod q(N_0)^r$, and

$$[(\sigma - 1)\tilde{x}_R](y_R) = [(\sigma - 1)\tilde{x}_R](\tilde{y}_R) = \tilde{x}_R[(\sigma^{-1} - 1)(\tilde{y})].$$

Since $\tilde{y}^r$ is in $q(N_0)$, hence invariant under Galois, $(\sigma^{-1} - 1)(\tilde{y})$ is a homomorphism from N to μ_r. On such a homomorphism the extended $\tilde{x}_R$ is simply given by the original x_R and we end up with

$$\begin{aligned}[(\sigma - 1)\tilde{x}_R](y_R) &= x_R[(\sigma^{-1} - 1)(\tilde{y})] = [(\sigma^{-1} - 1)(\tilde{y})](x) \\ &= (\sigma^{-1} - 1)(Q(x, y)^{1/r}) = (1 - \sigma)(Q(x, y)^{1/r}).\end{aligned}$$

We conclude that $\beta(x, y) = Q(x, y)^{-1} \bmod r$th powers, which is the desired result (up to a sign). □

3.5. Consider the left vertical column of (2), twisted:

$$0 \to U^{\#}(\chi\phi^{-1}) \otimes_R I/I^2 \to \tilde{U}^{\#}(\chi\phi^{-1}) \to U^{\#}(\chi\phi^{-1}) \to 0. \tag{6}$$

The local Galois action on $U^{\#}(\chi\phi^{-1}) = \mathrm{Hom}(N_0, \mu_r)(\phi^{-1})$ is trivial, hence the extension in (6) defines a homomorphism P

$$\begin{aligned}P: \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) &\to \mathrm{Hom}(U^{\#}(\chi\phi^{-1}),\ U^{\#}(\chi\phi^{-1}) \otimes_R I/I^2) \\ &= \mathrm{Hom}(N_0^{\vee} \otimes R,\ N_0^{\vee} \otimes R \otimes_R I/I^2),\end{aligned} \tag{7}$$

which we write $P(\sigma) = P_\sigma$. To compute $P_\sigma(u)$ lift $u \in U^{\#}(\chi\phi^{-1})$ to $\tilde{u} \in \tilde{U}^{\#}(\chi\phi^{-1})$, and let $P_\sigma(u) = \sigma(\tilde{u}) - \tilde{u}$.

LEMMA. *Let* $t \in \mathbb{Q}_p^{\times}$, *and let* $\sigma = (t, \mathbb{Q}_p^{ab}/\mathbb{Q}_p)$ *be its local Artin symbol. Then, using the identifications of Lemma* 3.3 (ii) *and* (iii), *for every* $x \otimes 1 \in N_0^{\vee} \otimes R$

$$P_\sigma(x \otimes 1) = \delta(x \otimes t \otimes 1). \tag{8}$$

In other words, P_σ *is obtained by contracting* δ *with* t.

Proof. This is a standard application of local class field theory and Tate duality. See [G-S] Theorem 3.11 for a similar situation. □

REMARK. Choosing a generator d for Δ as above, we may identify P_σ with a $\bar{P}_\sigma \in \mathrm{End}(N_0^{\vee}) \otimes R = \mathrm{End}(N_0) \otimes R$. With such a choice also $\Lambda/I^2 = R[\varepsilon]$, $\varepsilon^2 = 0$ (under $\varepsilon = d - 1 \bmod I^2$) (the ring of dual numbers), and the action of Galois on $\tilde{U}^{\#}(\chi\phi^{-1})$ is via multiplication by $1 + \bar{P}_\sigma\varepsilon$. Thus our $\bar{P}_\sigma$ is the

analogue of "$d\psi/dT$" in [G-S], and their choice of T is the analogue of our choice of ε. The module $\tilde{U}^{\#}(\chi\phi^{-1})$ is the *infinitesimal deformation* of $U^{\#}(\chi\phi^{-1})$.

3.6. THEOREM 2. *Let δ be the map defined by* (8), *i.e. the homomorphism*

$$\delta: N_0^{\vee} \otimes \mathbb{Q}_p^{\times} \otimes R \to N_0^{\vee} \otimes R \otimes_R I/I^2 \tag{9}$$

which corresponds (after we identify $\mathbb{Q}_p^{\times} \otimes R$ with the Galois group of the maximal abelian extension of $\mathbb{Q}_p$ of exponent r via the Artin symbol) to the infinitesimal deformation (6) *as explained above.*

Let $\check{q}_R: N \otimes R \to N_0^{\vee} \otimes \mathbb{Q}_p^{\times} \otimes R$ be the homomorphism obtained from the (extended) p-adic period pairing Q as above.

Then $\delta \circ \check{q}_R = 0$.

Proof. Combine all the preceding lemmas with (5). □

3.7. To go any further we need to know how $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ acts on $\tilde{U}^{\#}$. We know the Galois action on $\tilde{W}^{\#}$, which is unramified (Proposition 3.2). Unfortunately, the dulity with respect to the twisted Weil pairing is only between $\mathbf{U}$ and $\mathbf{W}$ (Proposition 2.5(iii)), and not between $\mathbf{U}^{\#}$ and $\mathbf{W}^{\#}$. If we wished to apply this duality to compute the Galois action on $\tilde{U}^{\#}$ (following [M-W2], end of Section 8—the character called there η is our ϕ), we would have to localize at a prime of the Hecke algebra which is *non-Eisenstein*. Instead, we shall compute the Galois action on $\tilde{U}^{\#}$ directly from the definition.

PROPOSITION. *Let $\langle\cdot\rangle: \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \to \Delta = \mathbb{F}_p^{\times}/\pm 1$ be the character which associates to σ the operator $\langle\sigma\rangle := \langle a_\sigma\rangle$, if $\zeta^{\sigma} = \zeta^{a_\sigma}$ for a primitive pth root of unity ζ. Let ϕ be the unramified character defined in Section* 3.2. *Then* $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ *acts on* $\mathbf{U}^{\#}$ *via* $\langle\cdot\rangle\phi^{-1}$.

REMARK. Identifying the Galois group of the maximal abelian extension of exponent r of $\mathbb{Q}_p$ with $\mathbb{Q}_p^{\times} \otimes R$, the assertion is that the Artin symbol of t acts on $\mathbf{U}^{\#}$ via the Hecke operator $\langle tp^{-\mathrm{ord}(t)}\rangle \cdot U_p^{-\mathrm{ord}(t)}$.

Proof. We have to show that σ acts on $J_1^{\#}[r]^{\mathrm{quot}}$ via $\langle a_\sigma\rangle^{-1}\phi(\sigma)$. It is enough to consider σ's whose restriction to $\mathbb{Q}_p^{ur}$ is Frob_p because they generate the local Galois group. Fix such a σ, so that $\phi(\sigma) = U_p$.

Let $x = (E, P) \in X_1(M)$ (M: a finite extension of $\mathbb{Q}_p$, which we assume contains K, E: an elliptic curve over M, P: a point of order p in $E(M)$). It is enough to prove that the divisor

$$\langle a_\sigma\rangle^* \sigma(x) - U_p^*(x)$$

extends (by Zariski closure) over the scheme $\mathscr{X}_1$ to a divisor meeting the special fiber only in $\Sigma^{\text{ét}}$. Indeed, this is then true for any divisor of degree 0 on X_1, relatively prime to C. Passing to $J_1^{\#}[r]$, we conclude that for any $x \in J_1^{\#}[r]$, the divisor class $\langle a_\sigma \rangle^* \sigma(x) - U_p^*(x)$ is represented by a divisor meeting the special fiber in $\Sigma^{\text{ét}}$, and therefore its image in $J_1^{\#}[r]^{\text{quot}}$ is trivial.

So let $x = (E, P)$ be as above. Then $\langle a_\sigma \rangle^* \sigma(x) = (\sigma E, \langle a_\sigma \rangle^{-1} \sigma P)$. We may assume that E has good ordinary reduction (every class in $J_1^{\#}[r]$ is represented by a divisor not meeting the special fiber of $\mathscr{X}_1$ in the finite collection of points $S \cup C$). The Zariski closure of x is a point $\xi \in \mathscr{X}_1(\mathscr{O}_M)$ written as $\xi = (E, P, Q \bmod \langle P \rangle)$ where E is an elliptic curve over $\mathscr{O}_M$, P and Q sections of order p, and the Weil pairing pairs them to ζ (a fixed pth root of 1): $\langle P, Q \rangle_E = \zeta$. The Zariski closure of $\langle a_\sigma \rangle^* \sigma(x)$ is $\xi' = (E', P', Q' \bmod \langle P' \rangle)$ where $E' = \sigma E$, $P' = \langle a_\sigma \rangle^{-1} \sigma P$, and $Q' = Q \bmod \langle P' \rangle$. Check that $\langle P', Q' \rangle_{E'} = \zeta$!

We have to show that $U_p^*(\xi) - \xi'$ specializes to a divisor supported on $\Sigma^{\text{ét}}$. But

$$U_p^*(\xi) = \sum (\tilde{E}, \tilde{P}, \tilde{Q} \bmod \langle \tilde{P} \rangle)$$

where the sum is over the p triples satisfying: (a) there exists a cyclic subgroup of order p, $\tilde{C} \subseteq \tilde{E}$, not containing $\tilde{P}$, such that $(\tilde{E}/\tilde{C}, \tilde{P} \bmod \tilde{C}) = (E, P)$, (b) $\langle \tilde{P}, \tilde{Q} \rangle_{\tilde{E}} = \zeta$.

For any triple of this sort, $\tilde{E} \approx \tilde{E}/\tilde{E}[p] = \tilde{E}/(\tilde{C} + \langle \tilde{P} \rangle) = E/\langle P \rangle$, and under this isomorphism $\tilde{C} \approx p^{-1}\tilde{C} \bmod \tilde{E}[p] = p^{-1}\tilde{C} \bmod (\tilde{C} + \langle \tilde{P} \rangle) = E[p] \bmod \langle P \rangle$. For $\tilde{P}$ there are p choices, forming a principal homogeneous space under $\tilde{C}$, and $\tilde{Q}$ is determined by (b).

There are two possibilities. If $\tilde{P}$ is not in the kernel of reduction, the triple $(\tilde{E}, \tilde{P}, \tilde{Q} \bmod \langle \tilde{P} \rangle)$ will specialize to $\Sigma^{\text{ét}}$ and may therefore be ignored. (This is always the case if P is not in the kernel of reduction. If P is in the kernel of reduction, $p - 1$ of the p triples will be of this form.) Otherwise, $\tilde{P}$ is in the kernel of reduction, and $\tilde{C}$ is not contained in it, so $\tilde{P}$ is unique. Assume that we are in this case.

Write red for the image under the reduction map. Then $\operatorname{red}(E') = \operatorname{red}(E)^{(p)} = \operatorname{red}(\tilde{E})$. Now $\zeta = \langle \tilde{P}, \tilde{Q} \rangle_{\tilde{E}} = \langle \tilde{P} \bmod \tilde{C}, Q \rangle_E$. If C is the kernel of the dual isogeny $E \to \tilde{E}$, namely $C = \tilde{E}[p]/\tilde{C}$, we get $Q \bmod C = \tilde{Q}$. But C reduces to the kernel of Frobenius, so $\operatorname{red}(Q') = \operatorname{red}(Q)^{(p)} = \operatorname{red}(\tilde{Q})$. Thus the reduction of the triple $(\tilde{E}, \tilde{P}, \tilde{Q} \bmod \langle \tilde{P} \rangle)$ considered here coincides with the reduction of ξ'. □

3.8. COROLLARY. *Consider* $U^{\#}(\chi\phi^{-1}) = N_0 \otimes R$ *(with trivialized Galois action), and its infinitesimal deformation* $\tilde{U}^{\#}(\chi\phi^{-1})$. *Then* $\operatorname{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ *acts on* $\tilde{U}^{\#}(\chi\phi^{-1})$ *via the character* $\langle \cdot \rangle \phi^{-2}$. □

3.9. Λ-*Adic Brandt matrices*

The Hecke ring $\mathbf{T}_0^{\#}$ is faithfully represented on N. When one writes this representation in terms of the canonical basis S of supersingular elliptic curves, one gets the famous Brandt matrices. See [Gr] §§1 and 2. Restrict the Brandt matrices to N_0. Our result that $\mathbf{U}^{\#}$ is free of rank m ($=\operatorname{rank} N_0$) over Λ has the following implication. Since the Hecke operators commute with Λ, they act on $\mathbf{U}^{\#}$ via $m \times m$ matrices with coefficients in Λ, which mod I give the usual Brandt matrices (restricted to N_0). We call these the Λ-adic Brandt matrices, and think of them as deformations of the usual Brandt matrices.

Mod I^2, picking a generator of Δ and identifying Λ/I^2 with $R[\varepsilon]$ as above, the Λ/I^2-adic Brandt matrices can be written as $A + B\varepsilon$, where A and B are in $\operatorname{End}(N_0 \otimes R) = \operatorname{End}(N_0^{\vee} \otimes R)$. With the notation of the remark at the end of Section 3.5, what we have proved is that

$$1 + \bar{P}_{\sigma}\varepsilon = \langle\sigma\rangle\phi^{-2}(\sigma) = \langle tp^{-\operatorname{ord}(t)}\rangle \cdot U_p^{-2\operatorname{ord}(t)} \tag{10}$$

if $\sigma = (t, \mathbb{Q}_p^{ab}/\mathbb{Q}_p)$.

3.10. With some non-canonical choices, we can make our results very explicit, and amenable to computations too.

Let d be a primitive root mod p. Then d mod ± 1 is a generator of the cyclic group Δ, and d mod rth powers a generator of $\Delta \otimes R = \mu_r$. Let $\varepsilon = \langle d\rangle - 1 \in I/I^2 = R\varepsilon$, so that $\Lambda/I^2 = R[\varepsilon]$.

Identify $\mathbb{Q}_p^{\times} \otimes R = R \oplus R$ under ($d^a p^b$ modulo rth powers) $\mapsto (a, b)$.

Fix a basis of N, and a basis of N_0. Of course, a natural basis for N is $S = \{e_0, \ldots, e_m\}$, and for N_0 we can take $\{e_1 - e_0, \ldots, e_m - e_0\}$. We have the dual basis for $U^{\#} = \operatorname{Hom}(N_0, R)$. Choose a basis for $\tilde{U}^{\#}$ as a free $R[\varepsilon]$-module that projects modulo ε to this basis of $U^{\#}$. Write U_p in terms of this basis. It is an $m \times m$ matrix with entries in $R[\varepsilon]$. Clearly $U_p^2 = 1 + B\varepsilon$, and we write

$$B = (U_p^2 - 1)/\varepsilon$$

(a more suggestive notation might have been $\mathrm{d}U_p^2/\mathrm{d}\varepsilon$). Note that B is independent of the choice of a basis for $\tilde{U}^{\#}$, and depends only on the choice of basis for N_0, which is somewhat "natural".

Let $\bar{Q}: N \times N_0 \to \mathbb{Q}_p^{\times} \otimes R = R \oplus R$ be the p-adic period pairing "mod rth powers", and write $\tilde{Q}$ for its first coordinate, and $\operatorname{ord}_p \bar{Q}$ for its second coordinate. These are $m \times (m+1)$ matrices with entries in R. The matrix $\operatorname{ord}_p \bar{Q}$ is a particularly simple one. Indeed, the pairing $\operatorname{ord}_p Q$ is the restriction to $N \times N_0$ of the pairing $N \times N \to \mathbb{Z}$ given (with respect to the

basis S) by a diagonal matrix indexed by S, whose entries are 1, 2 or 3 (if $p \equiv 1 \bmod 12$, this is the identity matrix).

THEOREM 3. *With the choices made above*

$$\tilde{Q} = ((U_p^2 - 1)/\varepsilon) \cdot (\mathrm{ord}_p Q). \tag{11}$$

REMARK. This is the "refined" analogue of Theorem 3.18 in [G-S].

Proof. Compute $\delta: N_0^\vee \otimes \mathbb{Q}_p^\times \otimes R = (N_0^\vee \otimes R)^2 \to N_0^\vee \otimes R\varepsilon = N_0^\vee \otimes R$ using Lemma 3.5 (8) and Corollary 3.8. We get that for α, β in $N_0^\vee$, a, b in R

$$\delta(\alpha \otimes a, \beta \otimes b) = \alpha \otimes a - ((U_p^2 - 1)/\varepsilon)\beta \otimes b. \tag{12}$$

We have used here the fact that in $R[\varepsilon]$, $\langle d^a \rangle - 1 = a(\langle d \rangle - 1)$. The theorem follows now from Theorem 2, since $\check{q}_R$ is given by the matrices $(\tilde{Q}, \mathrm{ord}_p \bar{Q})$. □

In [dS2] we shall show how to obtain from Theorem 3 the "refined" conjecture of Mazur and Tate for elliptic curves of prime conductor.

3.11. *A numerical example*

We end the paper with a numerical example. The data is taken from Antwerp IV. Let $p = 61$, and $l = r = 5$. The modular curve $X_0(61)$ is of genus $m = 4$. The Jacobian $J_0(61)$ has 2 simple factors: an elliptic curve A_1 and an abelian variety A_2 of dimension 3. The U_p operator acts like -1 on A_1 (thus A_1 has non-split multiplicative reduction at 61), and like $+1$ on A_2. It follows that $A_1 \cap A_2$ is a 2-group. In fact, tables of Cremona show that $\#(A_1 \cap A_2) = 4$ (this number is the square of the degree of the strong Weil parametrization $X_0(61) \to A_1$, which turns out to be 2). In particular $J_0[5] = A_1[5] \oplus A_2[5]$. The Eisenstein quotient of $J_0[5]$ is $A_2[5]$. This means that the filtration

$$0 \to \mu_5 \to J_0^\#[5] \to A_1[5] \oplus A_2[5] \to 0$$

splits over $A_1[5]$, but not over $A_2[5]$.

The p-adic period pairing of $J_0^\#$ is determined by the formulas of [dS3]. Let $S = \{e_0, \ldots, e_4\}$ be the five supersingular elliptic curves in characteristic 61. Their j-invariants are $j(e_0) = 9, j(e_1) = -20, j(e_2) = -11$,

and $j(e_3)$, $j(e_4)$ are the two roots of $j^2 - 23j + 24 = 0$. Define the pairing $\langle \cdot, \cdot \rangle : N \times N \to \mathbb{Q}_p^\times / (1 + p\mathbb{Z}_p)$ by

$$\langle e_i, e_j \rangle = (j(e_i) - j(e_j))^{p+1} \quad \text{if } i \neq j$$
$$\langle e_i, e_i \rangle = p \prod_{k \neq i} (j(e_i) - j(e_k))^{-(p+1)}.$$

The resulting matrix is

$$\begin{bmatrix} 61 \cdot 36 & 48 & 34 & 20 & 20 \\ 48 & 61 \cdot 15 & 20 & 30 & 30 \\ 34 & 20 & 61 \cdot 49 & 32 & 32 \\ 20 & 30 & 32 & 61 \cdot 40 & 55 \\ 20 & 30 & 32 & 55 & 61 \cdot 40 \end{bmatrix}.$$

Let us use $d = 2$ as a primitive root modulo 61. Then the matrix $\mathrm{ord}_p \langle e_i, e_j \rangle$ is the identity matrix (this is so whenever $p \equiv 1 \bmod 12$), and the matrix of the "logarithm to base 2" of the "unit part" of the above is

$$\begin{bmatrix} 14 & 10 & 48 & 24 & 24 \\ 10 & 28 & 24 & 29 & 29 \\ 48 & 24 & 38 & 5 & 5 \\ 24 & 29 & 5 & 25 & 37 \\ 24 & 29 & 5 & 37 & 25 \end{bmatrix},$$

which modulo 5 is the matrix

$$\begin{bmatrix} 4 & 0 & 3 & 4 & 4 \\ 0 & 3 & 4 & 4 & 4 \\ 3 & 4 & 3 & 0 & 0 \\ 4 & 4 & 0 & 0 & 2 \\ 4 & 4 & 0 & 2 & 0 \end{bmatrix}.$$

From here it is easy to compute the matrices $\mathrm{ord}_p Q$ and $\tilde{Q}$ that figure out

in Theorem 3. As a basis of N_0 we choose $e_i - e_0$, $1 \leqslant i \leqslant 4$. Then $\mathrm{ord}_p Q$ is the matrix

$$\begin{bmatrix} 4 & 1 & 0 & 0 & 0 \\ 4 & 0 & 1 & 0 & 0 \\ 4 & 0 & 0 & 1 & 0 \\ 4 & 0 & 0 & 0 & 1 \end{bmatrix},$$

and $\tilde{Q}$ is the matrix

$$\begin{bmatrix} 1 & 3 & 1 & 0 & 0 \\ 4 & 4 & 0 & 1 & 1 \\ 0 & 4 & 2 & 1 & 3 \\ 0 & 4 & 2 & 3 & 1 \end{bmatrix}.$$

The structure of the various modules studied in the paper can be also worked out explicitly. The ring Λ is $\mathbb{F}_5[\mu_5]$, and as a generator of the augmentation ideal I we may take $\alpha = \langle 2 \rangle_5 - 1$, where $\langle 2 \rangle_5$ is the projection of $\langle 2 \rangle \in \mathbb{F}_{61}^{\times}$ to μ_5. The ring Λ' is $\mathbb{F}_5[\mu_{12}]$, and as a generator of I' we may take $\alpha' = \langle 2 \rangle_{12} - 1$. The module $\mathbf{V}^{\#}$ is the dual (as a vector space over $\mathbb{F}_5$) of $J_1(61)^{\#}[5][\alpha']$. We have $J_1(61)^{\#}[5][\alpha'] \approx \mathbb{F}_5 \oplus \Lambda^8$. In particular we see that it is of dimension 41 over $\mathbb{F}_5$. The graded pieces $\mathbf{U}^{\#}$ and $\mathbf{W}^{\#}$ are of dimensions 20 and 21 respectively. The module $\tilde{U}^{\#}$ is of dimension 8, and in the filtration given by the left column of diagram (2) each piece is of dimension 4. Since, canonically, $U^{\#} = U = \mathrm{Hom}(N_0, \mathbb{F}_5)$, the endomorphism of $U^{\#}$ induced by the action of $U_p^2 - 1$ on $\tilde{U}^{\#}$ can be expressed as a 4×4 matrix in the basis $\{e_i - e_0\}$. The contents of Theorem 3 is that this matrix is related to the period matrix computed above by (11).

References

[A] Artin, M. Néron models, in: G. Cornell and J. Silverman (eds.) *Arithmetic Geometry*, Springer-Verlag, New York (1986).

[B-L-R] Bosch, S., Lutkebohmert, W. and Raynaud, M., *Néron Models*. Springer-Verlag.

[dS1] de Shalit, E., Kronecker's polynomial, supersingular elliptic curves, and p-adic periods of modular curves. *Contemp. Math.* 165, AMS (1994), 135–148.

[dS2] de Shalit, E., P-adic periods and modular symbols of elliptic curves of prime conductor. To appear in *Invent. Math.*

[dS3] de Shalit, E., On the p-adic periods of $X_0(p)$. To appear in *Math. Ann.*

[G-S] Greenberg, R. and Stevens, G., P-adic L functions and p-adic periods of modular forms, *Invent. Math.* 111 (1993) 407–447.

[Gr] Gross, B., Heights and special values of L series, *Proceedings of the 1985 Montréal conference in Number Theory.* CMS conference proceedings, vol. 7.

[Groth] Grothendieck, A., Modeles de néron et monodromie, in: *SGA 71*, LNM 288, Springer-Verlag (1972).

[Hi] Hida, H., Galois representations into $GL_2(\mathbb{Z}_p[[X]])$ attached to ordinary cusp forms, *Inv. Math.* 85 (1986) 543–613.

[K-M] Katz, N. and Mazur, B., Arithmetic moduli of elliptic curves, *Ann. Math. Stud.* 108. Princeton (1985).

[M-D] Manin, J. and Drinfeld, V. G., Periods of p-adic Schottky groups, *J.f.d. reine u. angew. Math.* 262/3 (1973) 239–247.

[M] Mazur, B., Modular curves and the Eisenstein ideal. *Publ. Math. I.H.E.S.* 47 (1977) 33–186.

[M-T] Mazur, B. and Tate, J., Refined conjectures of the "Birch and Swinnerton-Dyer type", *Duke Math. J.* 54 (1987) 711–750.

[M-T-T] Mazur, B., Tate, J. and Teitelbaum, J., On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer, *Inv. Math.* 84 (1986) 1–48.

[M-W1] Mazur, B. and Wiles, A., Class fields of abelian extensions of $\mathbb{Q}$, *Inv. Math.* 76 (1984) 179–330.

[M-W2] Mazur, B. and Wiles, A., On p-adic analytic families of Galois representations, *Compositio Math.* 59 (1986) 231–264.

[Mi] Milne, J., *Etale Cohomology*, PUP, Princeton (1980).

[Se] Serre, J.-P., *Groupes Algébriques et Corps de Classes*, Hermann, Paris (1959).

[W] Wiles, A., Modular curves and the class group of $\mathbb{Q}(\zeta_p)$, *Inv. Math.* 58 (1980) 1–35.