Compositio Mathematica **115:** 241–301, 1999.

Ordinary p-adic étale cohomology groups attached to towers of elliptic modular curves

MASAMI OHTA
Department of Mathematics, Tokai University, Hiratsuka, Kanagawa, 259-12, Japan

(Received 21 January 1997; accepted in final form 2 September 1997)

Abstract. Fix a prime number $p \geqslant 5$ and a positive integer N prime to p. We consider the projective limits of p-adic étale cohomology groups of the modular curves $X_1(Np^r)$ and $Y_1(Np^r)$ $(r \geqslant 1)$, which are denoted by $ES_p(N)_{\mathbf{Z}_p}$ and $GES_p(N)_{\mathbf{Z}_p}$, respectively. Let $e^{*\prime}$ be the projector to the direct sum of the ω^i-eigenspaces of the ordinary part, for $i \not\equiv 0, -1 \bmod p-1$. Our main result states that $e^{*\prime}GES_p(N)_{\mathbf{Z}_p}$ has a good p-adic Hodge structure, which can be described in terms of Λ-adic modular forms, extending the previously known result for $e^{*\prime}ES_p(N)_{\mathbf{Z}_p}$. We then apply the method of Harder and Pink to the Galois representation on $e^{*\prime}ES_p(N)_{\mathbf{Z}_p}$ to construct large unramified Abelian p-extensions over cyclotomic $\mathbf{Z}_p$-extensions of Abelian number fields.

Mathematics Subject Classifications (1991): 11F33, 11F67.

Key words: Eichler–Shimura cohomology, Λ-adic modular forms, cyclotomic fields.

Introduction

Let $\Gamma = \Gamma_1(M)$ be the usual congruence subgroup of $\mathrm{SL}_2(\mathbf{Z})$. For each integer $d \geqslant 0$, we have the well-known Eichler–Shimura isomorphisms

$$H^1_P(\Gamma, S^d(\mathbf{C})) \cong S_{d+2}(\Gamma) \oplus \overline{S_{d+2}(\Gamma)}, \tag{i}$$

$$H^1(\Gamma, S^d(\mathbf{C})) \cong M_{d+2}(\Gamma) \oplus \overline{S_{d+2}(\Gamma)}. \tag{ii}$$

Here, $S^d(\mathbf{C})$ is $\mathbf{C}^{\oplus(d+1)}$ on which Γ acts via the symmetric tensor representation of degree d, H^1_P means the parabolic cohomology, and other symbols are the standard ones. It follows that the cokernel of the natural mapping $i_{\mathbf{C}} : H^1_P(\Gamma, S^d(\mathbf{C})) \hookrightarrow H^1(\Gamma, S^d(\mathbf{C}))$ is isomorphic to the space of Eisenstein series of weight $d+2$ with respect to Γ, and the exact sequence

$$0 \to H^1_P(\Gamma, S^d(\mathbf{C})) \xrightarrow{i_{\mathbf{C}}} H^1(\Gamma, S^d(\mathbf{C})) \to \mathrm{Coker}\,(i_{\mathbf{C}}) \to 0,$$

canonically splits as modules over the Hecke algebra. In this sense, the 'difference' between $H^1_P(\Gamma, S^d(\mathbf{C}))$ and $H^1(\Gamma, S^d(\mathbf{C}))$ is well-understood. However, if we take the integral structure in consideration, replacing $\mathbf{C}$ by $\mathbf{Z}$ or $\mathbf{Z}_p$, the situation becomes subtle. Namely, the exact sequence

$$0 \to H^1_P(\Gamma, S^d(\mathbf{Z}_p)) \xrightarrow{i_{\mathbf{Z}_p}} H^1(\Gamma, S^d(\mathbf{Z}_p)) \to \mathrm{Coker}(i_{\mathbf{Z}_p}) \to 0,$$

(Kb. 6) INTERPRINT: S.A. PIPS Nr.: 148970 MATHKAP
comp4193.tex; 21/07/1995; 13:12; v.7; p.1

usually does not split as modules over the Hecke algebra. In fact, when $M = 1$ and d is even, Harder and Pink [HP] started with the fact that the special value of the Riemann zeta function appears as the 'denominator of the Eisenstein cohomology class', and then used it to construct and study large enough unramified Abelian p-extensions of $\mathbf{Q}(\zeta_p)$.

In our previous work [O2], we have shown that there is a good p-adic analogue of (i) for a subspace of the 'p-adic Eichler–Shimura cohomology group'. We fix a prime number $p \geqslant 5$, and a complete subfield K of $\mathbf{C}_p$ whose ring of integers we denote by $\mathfrak{o}$. Let N be a positive integer prime to p, and set

$$ES_p(N)_{\mathfrak{o}} := \left(\varprojlim_{r \geqslant 1} H^1(\overline{X_1(Np^r)}, \mathbf{Z}_p) \right) \widehat{\otimes}_{\mathbf{Z}_p} \mathfrak{o}$$

using the modular curves $X_1(Np^r)$ over $\mathbf{Q}$ attached to $\Gamma_1(Np^r)$, and the étale cohomology groups of their base extensions to $\overline{\mathbf{Q}}$. The Hecke operator $T^*(p)$ acts on this space, and we can consider the associated idempotent e^* of Hida. Let $e^{*\prime}$ be the projector to the direct sum of the ω^i-eigenspaces for $i \not\equiv 0, -1 \bmod p-1$ of $e^* ES_p(N)_{\mathfrak{o}}$ with respect to an action of the group $(\mathbf{Z}/p\mathbf{Z})^\times$, ω being the Teichmüller character. Both $e^* ES_p(N)_{\mathfrak{o}}$ and $e^{*\prime} ES_p(N)_{\mathfrak{o}}$ are known to be free modules of finite rank over the Iwasawa algebra $\Lambda_{\mathfrak{o}} \cong \mathfrak{o}[[T]]$. On the other hand, let $S(N; \Lambda_{\mathfrak{o}})$ be the space of $\Lambda_{\mathfrak{o}}$-adic cusp forms of level N. We can also define idempotents e and e' from the Hecke operator $T(p)$ in a similar manner. Let I_p be the inertia group of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$, and put

$$\mathfrak{A}_{\infty,\mathfrak{o}} := e^{*\prime} ES_p(N)_{\mathbf{Z}_p}^{I_p} \widehat{\otimes}_{\mathbf{Z}_p} \mathfrak{o},$$
$$\mathfrak{B}_{\infty,\mathfrak{o}} := e^{*\prime} ES_p(N)_{\mathfrak{o}} / \mathfrak{A}_{\infty,\mathfrak{o}}.$$

Then the main result of [O2] states that, when K is sufficiently large, we have canonical isomorphisms

$$\begin{aligned} \mathfrak{B}_{\infty,\mathfrak{o}} &\cong e' S(N; \Lambda_{\mathfrak{o}})(-1), \\ \mathfrak{A}_{\infty,\mathfrak{o}} &\cong \mathrm{Hom}_{\Lambda_{\mathfrak{o}}}(\mathfrak{B}_{\infty,\mathfrak{o}}, \Lambda_{\mathfrak{o}}). \end{aligned} \tag{I}$$

Note that these isomorphisms preserve the integral structure. The purpose of the present paper is to pursue the same subject for the following bigger group, called the *generalized p-adic Eichler–Shimura cohomology group of level N*:

$$GES_p(N)_{\mathfrak{o}} := \left(\varprojlim_{r \geqslant 1} H^1(\overline{Y_1(Np^r)}, \mathbf{Z}_p) \right) \widehat{\otimes}_{\mathbf{Z}_p} \mathfrak{o}.$$

Here, $Y_1(Np^r)$ is the canonical model of the open curve $\Gamma_1(Np^r)\backslash H$ over $\mathbf{Q}$. Thus there is a natural injective homomorphism $i_{\Lambda_{\mathfrak{o}}}\colon ES_p(N)_{\mathfrak{o}} \hookrightarrow GES_p(N)_{\mathfrak{o}}$ and we

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

want to understand (the ordinary part of) the nature of this mapping. Let $M(N;\Lambda_{\mathfrak{o}})$ be the space of $\Lambda_{\mathfrak{o}}$-adic modular forms of level N. We can define the idempotents e^* and $e^{*\prime}$ (resp. e and e') acting on $GES_p(N)_{\mathfrak{o}}$ (resp. $M(N;\Lambda_{\mathfrak{o}})$) in the same way as above. The following theorem is our main result of this paper, which gives a p-adic analogue of (ii) for $e^{*\prime}GES_p(N)_{\mathfrak{o}}$, and extends (I):

THEOREM. *$e^*GES_p(N)_{\mathfrak{o}}$ is a free $\Lambda_{\mathfrak{o}}$-module of finite rank. Thus we have $e^{*\prime}GES_p(N)^{I_p}_{\mathbf{Z}_p} = \mathfrak{A}_{\infty,\mathbf{Z}_p}$ and when K contains all the roots of unity, there is a canonical isomorphism*

$$e^{*\prime}GES_p(N)_{\mathfrak{o}}/\mathfrak{A}_{\infty,\mathfrak{o}} \xrightarrow{\sim} e'M(N;\Lambda_{\mathfrak{o}})(-1). \tag{II}$$

The idea of the proof of this theorem is basically the same as that of (I). Namely, we let $M_k(\Gamma;\mathbf{Z})$ be the subspace of $M_k(\Gamma)$ consisting of elements having q-expansions with coefficients in $\mathbf{Z}$ at $i\infty$ and set $M_k(\Gamma;R) := M_k(\Gamma;\mathbf{Z})\otimes_{\mathbf{Z}} R$ for any ring R. We consider the space

$$\mathfrak{M}^*_k(N;\mathfrak{o}) := \varprojlim_{r\geqslant 1}\left\{f\in M_k(\Gamma_1(Np^r);\mathbf{C}_p) \mid f \mid \begin{bmatrix} 0 & -1\\ Np^r & 0\end{bmatrix}\in M_k(\Gamma_1(Np^r);\mathfrak{o})\right\},$$

where the projective limit is taken with respect to the natural trace mappings. Again, we have idempotents e^* and $e^{*\prime}$ attached to $T^*(p)$ acting on this space and, as in the case of cusp forms, we have a canonical isomorphism $e\,M(N;\Lambda_{\mathfrak{o}})\cong e^*\mathfrak{M}^*_k(N;\mathfrak{o})$, for each integer $k\geqslant 2$. The main part of the proof consists in showing that there is a canonical isomorphism

$$e^{*\prime}GES_p(N)_{\mathfrak{o}}/\mathfrak{A}_{\infty,\mathfrak{o}} \xrightarrow{\sim} e^{*\prime}\mathfrak{M}^*_2(N;\mathfrak{o})(-1), \tag{II*}$$

which together with the above isomorphism gives (II).

Our results reduce the study of the 'difference' between $e^{*\prime}ES_p(N)_{\mathfrak{o}}$ and $e^{*\prime}GES_p(N)_{\mathfrak{o}}$ to that between $e'S(N;\Lambda_{\mathfrak{o}})$ and $e'M(N;\Lambda_{\mathfrak{o}})$, which is much simpler. Indeed, we can analyse the latter using the $\Lambda_{\mathfrak{o}}$-adic Eisenstein series. To state the result, let us assume that $p\nmid\varphi(N)$, and fix an even primitive Dirichlet character χ defined modulo Np whose restriction to $(\mathbf{Z}/p\mathbf{Z})^\times$ is neither ω^0 nor ω^{-1}. Let $\mathfrak{r}$ be the ring generated by the values of χ over $\mathbf{Z}_p$. Then taking the χ-eigenspaces, we get from $i_{\Lambda_{\mathfrak{r}}}$ an exact sequence

$$0\to e^*ES_p(N)^{(\chi)}_{\mathfrak{r}} \xrightarrow{i^{(\chi)}_{\Lambda_{\mathfrak{r}}}} e^*GES_p(N)^{(\chi)}_{\mathfrak{r}} \to \mathrm{Coker}(i^{(\chi)}_{\Lambda_{\mathfrak{r}}})\to 0.$$

Further localizing this sequence at the 'Eisenstein maximal ideal' of the p-adic Hecke algebra acting on $e^*GES_p(N)^{(\chi)}_{\mathfrak{r}}$, we obtain an exact sequence which we

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

simply write $0 \to X \to Y \xrightarrow{\pi} Z \to 0$ (see 5.2 of the text for details). The following theorem asserts that the 'denominator of the p-adic Eisenstein cohomology class' is essentially the p-adic L-function

THEOREM. *Z is a free module of rank one over $\Lambda_{\mathfrak{r}}$. The above exact sequence of $\Lambda_{\mathfrak{r}}$-modules canonically splits when tensored with the quotient field $\mathcal{L}$ of $\Lambda_{\mathfrak{r}}$. If $s\colon Z \otimes_{\Lambda_{\mathfrak{r}}} \mathcal{L} \to Y \otimes_{\Lambda_{\mathfrak{r}}} \mathcal{L}$ gives the splitting, then we have*

$$\pi(Y \cap s(Z)) = \begin{cases} G(T, \chi\omega^2)\cdot Z & \text{when } \chi \neq \omega^{-2}, \\ Z & \text{when } \chi = \omega^{-2}. \end{cases}$$

Here, $G(T, \chi\omega^2)$ is a twist of the Iwasawa power series giving the Kubota–Leopoldt p-adic L-function; precisely $G(u^s - 1, \chi\omega^2) = L_p(-s-1, \chi\omega^2)$, with a suitable choice of a topological generator u of $1 + p\mathbf{Z}_p$.

After this theorem, we can directly apply the method of [HP], replacing the classical Eichler–Shimura cohomology group by the above X (and hence $\mathbf{Z}_p$ by $\Lambda_{\mathfrak{r}}$). As a consequence, we can give a fairly explicit construction of large enough unramified Abelian p-extensions over cyclotomic $\mathbf{Z}_p$-extensions of Abelian number fields, under some assumptions. In the particular case where χ ranges over even powers of the Teichmüller character, this result gives a new (and simple) proof of the Mazur–Wiles theorem [MW1] (the Iwasawa main conjecture) for such characters.

The organization of this paper is as follows: The first four sections are devoted to the proof of our main theorem. In doing this, we need tools which are well-known for studying cusp forms; but could not be found in the literature to treat modular forms. We thus supply them in Sections 1–3. In Section 1, we study the structure of the ordinary generalized p-adic Eichler–Shimura cohomology groups and the ordinary p-adic Hecke algebras attached to modular forms. In particular, we show that they are controllable (in the sense of Hida's theory) via the action of the Iwasawa algebra. In Section 2, we study the spaces $e\,M(N;\Lambda_{\mathfrak{o}})$ and $e^*\mathfrak{M}_k^*(N;\mathfrak{o})$. Aside from the knowledge of similar spaces corresponding to cusp forms, we need the explicit description of enough $\Lambda_{\mathfrak{o}}$-adic Eisenstein series here.

In our study [O2] of cusp forms, an essential role was played by the Jacobians of modular curves; especially their 'good quotients' and the associated p-divisible groups. In the present treatment of modular forms, rather than cusp forms, we need the corresponding theory for the *generalized Jacobians* (of reduced cuspidal moduli) of modular curves. In Section 3, we collect some general facts about generalized Jacobians for later use. After these three preliminary sections, we carry out the construction of our p-adic period mapping (II) in Section 4, and complete the proof of the main theorem. As in the case of cusp forms, a hard point here is the surjectivity of (II)*. We get over this difficulty by reducing the problem to an integrality property of the residues of ordinary modular forms (of weight 2), with the aid of the known result for cusp forms.

Section 5 is an application of our cohomology theory to the theory of cyclotomic fields. The second theorem above is proved in Subsection 5.2 and with this we can proceed in a completely parallel way, as in [HP], to construct large unramified Abelian p-extensions.

Notation and conventions

Since this paper is a continuation of the previous work [O2], we use the same terminology as in loc. cit. In particular

- $H := \{z \in \mathbf{C} \mid \mathrm{Im}(z) > 0\}$.
- $\Gamma_1(M)$ and $\Gamma_0(M)$ denote the usual congruence subgroups of $\mathrm{SL}_2(\mathbf{Z})$ defined by

$$\Gamma_1(M) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbf{Z}) \mid \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \bmod M{\cdot}M_2(\mathbf{Z}) \right\},$$

$$\Gamma_0(M) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbf{Z}) \mid \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \bmod M{\cdot}M_2(\mathbf{Z}) \right\}.$$

- $\mathbf{C}_p :=$ (the completion of $\overline{\mathbf{Q}}_p$).
- We fix embeddings of $\overline{\mathbf{Q}}$ into $\mathbf{C}$ and $\mathbf{C}_p$, once and for all.
- If A is a module over a ring R, and r (resp. I) is an element (resp. an ideal) of R, we often write A/r (resp. A/I) for A/rA (resp. A/IA).

1. Generalized p-adic Eichler–Shimura cohomology groups and p-adic Hecke algebras

1.1. GENERALIZED p-ADIC EICHLER–SHIMURA COHOMOLOGY GROUPS

As in [O2], we fix a prime number $p \geqslant 5$, and a complete subfield K of $\mathbf{C}_p$, with its ring of integers $\mathfrak{o}$. We also fix a postive integer N not divisible by p. We set

$$N_r := Np^r \quad \text{and} \quad \Gamma_r := \Gamma_1(N_r) \quad \text{for } r \geqslant 1 \tag{1.1.1}$$

and write

$$X_r := X_1(N_r), \qquad Y_r := Y_1(N_r) \tag{1.1.2}$$

for the canonical models of $\Gamma_r\backslash H \cup \mathbf{P}^1(\mathbf{Q})$ and $\Gamma_r\backslash H$ over $\mathbf{Q}$, respectively. (As in [O2], the cusp $i\infty$ is a $\mathbf{Q}$-rational point of X_r.)

For any commutative ring R with unity, we put $S^d(R) := R^{\oplus(d+1)}$ and let

$$\rho_d : \mathrm{GL}_2(R) \to \mathrm{GL}(S^d(R)) \tag{1.1.3}$$

be the symmetric tensor representation of degree $d (\geqslant 0)$, realized as in Shimura [Sh] 8.2. To this representation, we can associate a twisted constant p-adic étale sheaf

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

$F_{S^d(\mathbf{Z}_p)}$ on Y_r; and we have canonical isomorphisms between étale cohomology groups and classical group cohomologies:

$$\begin{aligned} &H^1(\overline{Y}_r, F_{S^d(\mathbf{Z}_p)}) \cong H^1(\Gamma_r, S^d(\mathbf{Z}_p)), \\ &H^1(\overline{X}_r, j_{r*}F_{S^d(\mathbf{Z}_p)}) \cong H^1_P(\Gamma_r, S^d(\mathbf{Z}_p)), \end{aligned} \tag{1.1.4}$$

where the bar means the base change from $\mathbf{Q}$ to $\overline{\mathbf{Q}}$, $j_r\colon Y_r \hookrightarrow X_r$ is the injection morphism, and H^1_P is the parabolic cohomology (cf. [O2] 1.2). We will frequently identify the groups in both hand sides.

DEFINITION (1.1.5). We set

$$GES_p(N)_{\mathbf{Z}_p} := \varprojlim_{r\geqslant 1} H^1(\overline{Y}_r, \mathbf{Z}_p),$$

$$GES_p(N)_{\mathfrak{o}} := GES_p(N)_{\mathbf{Z}_p} \widehat{\otimes}_{\mathbf{Z}_p} \mathfrak{o},$$

the projective limit being taken relative to the trace mappings. We call these groups the *generalized p-adic Eichler–Shimura cohomology groups of level N over $\mathbf{Z}_p$ or $\mathfrak{o}$*, respectively. Similarly, using $H^1(\overline{X}_r, \mathbf{Z}_p)$ instead of $H^1(\overline{Y}_r, \mathbf{Z}_p)$, we define the *p-adic Eichler–Shimura cohomology groups* $ES_p(N)_{\mathbf{Z}_p}$ and $ES_p(N)_{\mathfrak{o}}$ ([O2] (1.2.13)).

As in [O1] 7.3 and 7.4, the Hecke operators $T^*(n)$ and $T^*(q,q)$ act on the groups in (1.1.4) and (1.1.5). Especially, we have Hida's idempotent

$$e^* := \lim_{n\to\infty} T^*(p)^{n!} \tag{1.1.6}$$

acting on these groups.

1.2. SOME LEMMAS

We write U_r for the multiplicative group $1 + p^r\mathbf{Z}_p$ for $r \geqslant 1$. For the moment, we fix integers $s \geqslant r \geqslant 1$ and $d \geqslant 0$. Set

$$\Phi^r_s := \Gamma_r \cap \Gamma_0(p^s). \tag{1.2.1}$$

Thus $\Gamma_r \supseteq \Phi^r_s \rhd \Gamma_s$, and we have the following disjoint decomposition:

$$\Gamma_r = \coprod_{0\leqslant j\leqslant p^{s-r}-1} \xi_j \Phi^r_s \quad \text{with } \xi_j := \begin{bmatrix} 1 & 0 \\ N_r j & 1 \end{bmatrix}; \quad \text{and} \tag{1.2.2}$$

$$\Phi^r_s = \coprod_{\alpha\in U_r/U_s} \sigma_\alpha \Gamma_s$$

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

with

$$\Gamma_r \ni \sigma_\alpha \equiv \begin{bmatrix} \alpha^{-1} & * \\ 0 & \alpha \end{bmatrix} \bmod p^s \cdot M_2(\mathbf{Z}). \tag{1.2.3}$$

Let Y_s^r be the canonical model of $\Phi_s^r \backslash H$ over $\mathbf{Q}$ so that $Y_s \to Y_s^r \to Y_r$ is defined over $\mathbf{Q}$. Then it is known that the following diagram commutes:

$$\begin{array}{ccccc} H^1(\overline{Y}_s, F_{S^d(\mathbf{Z}_p)}) & \xrightarrow{\text{Tr}} & H^1(\overline{Y}_s^r, F_{S^d(\mathbf{Z}_p)}) & \xrightarrow{\text{Tr}} & H^1(\overline{Y}_r, F_{S^d(\mathbf{Z}_p)}) \\ \downarrow \wr & & \downarrow \wr & & \downarrow \wr \\ H^1(\Gamma_s, S^d(\mathbf{Z}_p)) & \xrightarrow[\text{Cor}]{} & H^1(\Phi_s^r, S^d(\mathbf{Z}_p)) & \xrightarrow[\text{Cor}]{} & H^1(\Gamma_r, S^d(\mathbf{Z}_p)) \end{array} \tag{1.2.4}$$

where Tr (resp. Cor) means the trace mapping (resp. the corestriction), and the vertical isomorphisms are given by (1.1.4) (and similarly for Φ_s^r); cf. [O1] (2.5.4). The Hecke operators as in 1.1 act compatibly on these groups. For example, the operator $T^*(p^t)$ on $H^1(\Phi_s^r, S^d(\mathbf{Z}_p))$ is described as follows: First we have

$$\Phi_s^r \begin{bmatrix} 1 & 0 \\ 0 & p^t \end{bmatrix} \Phi_s^r = \coprod_{0 \leqslant i \leqslant p^t - 1} \beta_i \Phi_s^r \quad \text{with } \beta_i := \begin{bmatrix} 1 & 0 \\ N_s i & p^t \end{bmatrix}. \tag{1.2.5}$$

$T^*(p^t)$ then sends a cohomology class $cl(u)$ of a 1-cocycle u to $cl(u')$ where

$$u'(\gamma) = \sum_{i=0}^{p^t-1} \rho_d(\beta_i) u(\gamma_i) \quad \text{for } \gamma \in \Phi_s^r$$

$$\text{if } \gamma^{-1}\beta_i = \beta_{i'}\gamma_i^{-1} \quad \text{with } \gamma_i \in \Phi_s^r. \tag{1.2.6}$$

We have a similar diagram as (1.2.4) after applying the operator $e^* = \lim_{n\to\infty} T^*(p)^{n!}$. The following two lemmas are variants of Hida's results in [H3], for which we give direct proof for the convenience of the reader.

LEMMA (1.2.7) (cf. [H3] Lemma 4.6). *$e^*H^1(\Gamma_r, S^d(\mathbf{Z}_p))$ and $e^*H^1(\Phi_s^r, S^d(\mathbf{Z}_p))$ are free $\mathbf{Z}_p$-modules.*

Proof. We give the proof only for the latter group. It is finitely generated over $\mathbf{Z}_p$. Take an integer M so large that p^M annihilates its torsion subgroup. Then from the long exact sequence of cohomology groups obtained from:

$$0 \to S^d(\mathbf{Z}_p) \xrightarrow{p^M} S^d(\mathbf{Z}_p) \to S^d(\mathbf{Z}/p^M\mathbf{Z}) \to 0,$$

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

we have a surjective homomorphism

$$H^0(\Phi_s^r, S^d(\mathbf{Z}/p^M\mathbf{Z})) \to H^1(\Phi_s^r, S^d(\mathbf{Z}_p))_{\text{tors}}.$$

Now it is easy to see that the endomorphism of $H^0(\Phi_s^r, S^d(\mathbf{Z}/p^M\mathbf{Z})) = S^d(\mathbf{Z}/p^M\mathbf{Z})^{\Phi_s^r}$ defined by $m \mapsto \sum_{i=0}^{p^t-1} \rho_d(\beta_i)m$ is compatible with $T^*(p^t)$ on $H^1(\Phi_s^r, S^d(\mathbf{Z}/p^M\mathbf{Z}))$. If $t \geqslant M$, we see that

$$\rho_d(\beta_i) = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ N_s i & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ (N_s i)^d & 0 & \cdots & 0 \end{bmatrix}.$$

It follows that if $t > M$ and t is divisible by M, then $\sum_{i=0}^{p^t-1} \rho_d(\beta_i)m = 0$, which proves our assertion. □

In general, if Γ and Γ' are congruence subgroups of $\mathrm{SL}_2(\mathbf{Z})$ and $\Gamma' \supseteq \alpha\Gamma\alpha^{-1}$ with $\alpha \in \mathrm{GL}_2(\mathbf{Q})$, we can define the operator

$$\text{‘}\mid \alpha\text{’} : H^1(\Gamma', S^d(R)) \to H^1(\Gamma, S^d(R)) \tag{1.2.8}$$

by the formula

$$cl(u') \mid \alpha = cl(u) \quad \text{with } u(\gamma) = \rho_d(\alpha^{-1})u'(\alpha\gamma\alpha^{-1}) \quad \text{for all } \gamma \in \Gamma, \tag{1.2.9}$$

provided that R is a **Q**-algebra, or $\alpha^{-1} \in M_2(\mathbf{Z})$. This operator preserves the parabolic part; and coincides with the usual operator ‘$\mid \alpha$’ (cf. (1.5.1) below) on modular forms via the Eichler–Shimura isomorphism when $\det(\alpha) > 0$.

LEMMA (1.2.10) (cf. [H3] Lemma 4.3 and page 570). *Put* $\delta := \begin{bmatrix} 1 & 0 \\ 0 & p^{s-r} \end{bmatrix}$. *Then we clearly have* $\delta^{-1}\Phi_s^r\delta \subseteq \Gamma_r$; *and the following diagram commutes:*

$$\begin{array}{ccc} H^1(\Phi_s^r, S^d(\mathbf{Z}_p)) & \xrightarrow{\text{Cor}} & H^1(\Gamma_r, S^d(\mathbf{Z}_p)) \\ \downarrow {\scriptstyle T^*(p^{s-r})} & \swarrow {\scriptstyle \text{‘}|\delta^{-1}\text{’}} & \downarrow {\scriptstyle T^*(p^{s-r})} \\ H^1(\Phi_s^r, S^d(\mathbf{Z}_p)) & \xrightarrow[\text{Cor}]{} & H^1(\Gamma_r, S^d(\mathbf{Z}_p)). \end{array}$$

Proof. Take $cl(u) \in H^1(\Phi_s^r, S^d(\mathbf{Z}_p))$ and let $\mathrm{Cor}(cl(u)) \mid \delta^{-1} =: cl(u')$. Then a simple calculation shows that, for any $\gamma \in \Phi_s^r$, $u'(\gamma) = \sum_{j=0}^{p^{s-r}-1} \rho_d(\delta\xi_j)u(\gamma_j)$

if $\gamma^{-1}\delta\xi_j = \delta\xi_{j'}\gamma_j^{-1}$ with $\gamma_j \in \Phi_s^r$ for each index j. Since $\delta\xi_j$ is equal to β_j with $t = s - r$, the upper triangle commutes. The commutativity of the lower triangle can be proved in a similar manner. □

COROLLARY (1.2.11). *The corestriction:* $e^*H^1(\Phi_s^r, S^d(\mathbf{Z}_p)) \to e^*H^1(\Gamma_r, S^d(\mathbf{Z}_p))$ *is an isomorphism.*

We can let U_1/U_s act on $e^*H^1(\Gamma_s, S^d(\mathbf{Z}_p))$ by $\alpha \mapsto$ ' $| \sigma_\alpha^{-1}$' with $\sigma_\alpha \in \mathrm{SL}_2(\mathbf{Z})$ satisfying $\sigma_\alpha \equiv \begin{bmatrix} \alpha^{-1} & * \\ 0 & \alpha \end{bmatrix}$ mod $p^s \cdot M_2(\mathbf{Z})$ (for the moment; later we will use different action of U_1).

LEMMA (1.2.12). *The corestriction induces an isomorphism*

$$e^*H^1(\Gamma_s, S^d(\mathbf{Z}_p))_{U_r/U_s} \xrightarrow{\sim} e^*H^1(\Gamma_r, S^d(\mathbf{Z}_p)),$$

where the subscript means the coinvariant.

Proof. By the corollary above, it is enough to show that the mapping induced from the corestriction $H^1(\Gamma_s, S^d(\mathbf{Z}_p))_{U_r/U_s} \to H^1(\Phi_s^r, S^d(\mathbf{Z}_p))$, is an isomorphism.

For this, let $\mathcal{N}$ be the Pontryagin dual of $S^d(\mathbf{Z}_p)$. Let $(\ , \ )$ be the canonical pairing between $S^d(\mathbf{Z}_p)$ and $\mathcal{N}$, and consider $\mathcal{N}$ as a Φ_s^r-module by $(x, y) = (\gamma x, \gamma y)$ for $\gamma \in \Phi_s^r$. Denoting by $\mathcal{F}_\mathcal{N}$ the sheaf on $\Phi_s^r\backslash H$ (or its pull-back to $\Gamma_s\backslash H$) attached to $\mathcal{N}$, the Poincaré duality implies that the Pontryagin dual of the mapping above is identified with the canonical mapping

$$H_c^1(\Phi_s^r\backslash H, \mathcal{F}_\mathcal{N}) \to H_c^1(\Gamma_s\backslash H, \mathcal{F}_\mathcal{N})^{U_r},$$

But from the argument of [O1] 7.3, we may interpret this as the natural mapping

$$\mathrm{Hom}_{\Phi_s^r}(D_0, \mathcal{N}) \to \mathrm{Hom}_{\Gamma_s}(D_0, \mathcal{N})^{U_r},$$

where D_0 is the degree 0 part of the free Abelian group on $\mathbf{P}^1(\mathbf{Q})$, the set of cusps of Γ_s or Φ_s^r. This is clearly an isomorphism because $U_r/U_s \cong \Phi_s^r/\Gamma_s$ ($\alpha \leftrightarrow \sigma_\alpha$). □

1.3. PASSING TO THE PROJECTIVE LIMIT

We denote by $\Lambda_{\mathbf{Z}_p}$ (resp. $\Lambda_\mathfrak{o}$) the completed group algebra of U_1 over $\mathbf{Z}_p$ (resp. $\mathfrak{o}$), and write

$$\iota : U_1 \hookrightarrow \Lambda_{\mathbf{Z}_p} \subseteq \Lambda_\mathfrak{o}, \tag{1.3.1}$$

for the obvious inclusion. As usual, we fix a topological generator u of U_1, and identify $\Lambda_{\mathbf{Z}_p}$ (resp. $\Lambda_\mathfrak{o}$) with the formal power series ring $\mathbf{Z}_p[[T]]$ (resp. $\mathfrak{o}[[T]]$) via $\iota(u) \leftrightarrow 1 + T$. We put

$$\omega_{r,d} := \iota(u^{p^{r-1}}) - u^{dp^{r-1}} = (1+T)^{p^{r-1}} - u^{dp^{r-1}}, \tag{1.3.2}$$

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

for integers $r \geqslant 1$ and $d \geqslant 0$.

Now set

$$\mathfrak{X}_{d,\mathbf{Z}_p} := \varprojlim_{r\geqslant 1} e^* H^1(\overline{Y}_r, F_{S^d(\mathbf{Z}_p)}) \cong \varprojlim_{r\geqslant 1} e^* H^1(\Gamma_r, S^d(\mathbf{Z}_p)) \tag{1.3.3}$$

where the projective limits are taken relative to the trace mappings and the corestrictions, respectively. We also set

$$\mathfrak{X}_{d,\mathfrak{o}} := \mathfrak{X}_{d,\mathbf{Z}_p} \widehat{\otimes}_{\mathbf{Z}_p} \mathfrak{o}. \tag{1.3.4}$$

Thus, $\mathfrak{X}_{0,\mathfrak{o}} = e^* GES_p(N)_{\mathfrak{o}}$. As we explained before (1.2.12), we may consider $\mathfrak{X}_{d,\mathbf{Z}_p}$ as a $\Lambda_{\mathbf{Z}_p}$-module and, hence, $\mathfrak{X}_{d,\mathfrak{o}}$ as a $\Lambda_{\mathfrak{o}} = \Lambda_{\mathbf{Z}_p} \widehat{\otimes}_{\mathbf{Z}_p} \mathfrak{o}$-module also.

THEOREM (1.3.5). *For each $d \geqslant 0$, $\mathfrak{X}_{d,\mathfrak{o}}$ is a free $\Lambda_{\mathfrak{o}}$-module of rank*

$$\mathrm{rank}_{\Lambda_{\mathfrak{o}}} e^* ES_p(N)_{\mathfrak{o}} + \frac{p-1}{2} \sum_{0<t|N} \varphi(t)\varphi\left(\frac{N}{t}\right) =: r(N),$$

where φ is the Euler function. Moreover, via the natural projection, we have an isomorphism

$$\mathfrak{X}_{d,\mathfrak{o}}/\omega_{r,0} \xrightarrow{\sim} e^* H^1(\overline{Y}_r, F_{S^d(\mathbf{Z}_p)}) \otimes_{\mathbf{Z}_p} \mathfrak{o} \cong e^* H^1(\Gamma_r, S^d(\mathfrak{o}))$$

for each $r \geqslant 1$.

Proof. For integers $s_1 \geqslant s_2 \geqslant r \geqslant 1$, we have a commutative diagram:

$$\begin{array}{ccccccc}
e^*H^1(\Gamma_{s_1},S^d(\mathbf{Z}_p)) & \xrightarrow{\omega_{r,0}} & e^*H^1(\Gamma_{s_1},S^d(\mathbf{Z}_p)) & \xrightarrow{\mathrm{Cor}} & e^*H^1(\Gamma_r,S^d(\mathbf{Z}_p)) & \longrightarrow & 0 \\
{\scriptstyle\mathrm{Cor}}\downarrow & & {\scriptstyle\mathrm{Cor}}\downarrow & & \| & & \\
e^*H^1(\Gamma_{s_2},S^d(\mathbf{Z}_p)) & \xrightarrow[\omega_{r,0}]{} & e^*H^1(\Gamma_{s_2},S^d(\mathbf{Z}_p)) & \xrightarrow[\mathrm{Cor}]{} & e^*H^1(\Gamma_r,S^d(\mathbf{Z}_p)) & \longrightarrow & 0
\end{array}$$

with exact horizontal lines by (1.2.12). Thus taking the projective limit, we obtain an isomorphism $\mathfrak{X}_{d,\mathbf{Z}_p}/\omega_{r,0} \xrightarrow{\sim} e^* H^1(\Gamma_r, S^d(\mathbf{Z}_p))$. Especially, $\mathfrak{X}_{d,\mathbf{Z}_p}$ is a finitely generated $\Lambda_{\mathbf{Z}_p}$-module.

Now $e^* H^1(\Gamma_r, S^d(\mathbf{Z}_p))$ is free over $\mathbf{Z}_p$ by (1.2.7); and let us now compute its rank. First, we already know that the $\mathbf{Z}_p$-rank of $e^* H^1_P(\Gamma_r, S^d(\mathbf{Z}_p))$ is equal to $p^{r-1}\mathrm{rank}_{\Lambda_{\mathbf{Z}_p}} e^* ES_p(N)_{\mathbf{Z}_p}$ by [O2] (1.4.3). On the other hand, the operator '$/\begin{bmatrix} 0 & -1 \\ N_r & 0 \end{bmatrix}$' interchanges $T(p)$ and $T^*(p)$ on $H^1(\Gamma_r, S^d(\mathbf{Q}_p))$ and, hence, $e^* H^1(\Gamma_r, S^d(\mathbf{Q}_p))/e^* H^1_P(\Gamma_r, S^d(\mathbf{Q}_p))$ has the same dimension as $e H^1(\Gamma_r, S^d$

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

$(\mathbf{Q}_p))/e\,H^1_P(\Gamma_r, S^d(\mathbf{Q}_p))$, where e is the idempotent attached to $T(p)$. It then follows from [H3] Lemma 5.3 (which we recall in (2.3.2) below) and Corollary 5.6 that the common dimension of these spaces is $(\varphi(p^r)/2)\sum_{0<t|N}\varphi(t)\varphi(N/t)$. (We will give another proof of this dimension formula in 4.3.) We therefore see that $\mathfrak{X}_{d,\mathbf{Z}_p}/\omega_{r,0}$ is a free $\mathbf{Z}_p$-module of rank $p^{r-1}r(N)$ for each $r \geqslant 1$. Using the well-known structure theorem of finitely generated $\Lambda_{\mathbf{Z}_p}$-modules, we easily see that $\mathfrak{X}_{d,\mathbf{Z}_p}$ is free of rank $r(N)$ over $\Lambda_{\mathbf{Z}_p}$.

This proves our result when $\mathfrak{o} = \mathbf{Z}_p$; and the general case follows from this. □

1.4. SPECIALIZATI ONS OF $e^*GES_p(N)_{\mathfrak{o}}$.

Recall that we have the *specialization mapping*

$$sp_{r,d} : GES_p(N)_{\mathfrak{o}} \to H^1(\Gamma_r, S^d(\mathfrak{o})) \tag{1.4.1}$$

for each integers $r \geqslant 1$ and $d \geqslant 0$ (cf. [O2] 1.3). It commutes with the Hecke operators $T^*(n)$ and $T^*(q,q)$. In view of this, from now on, we change the U_1-module structure of $H^1(\Gamma_r, S^d(\mathfrak{o}))$ newly defining the action of $\alpha \in U_1$ by $\alpha^d \cdot `\,|\,\sigma_\alpha^{-1}$'. The resulting new $\Lambda_{\mathfrak{o}}$-module structure of $\mathfrak{X}_{d,\mathfrak{o}}$ is the twist of the previous one by the character: $U_1 \ni \alpha \mapsto \alpha^d$ and, hence, (1.3.5) remains valid if we replace $\omega_{r,0}$ by $\omega_{r,d}$ in the statement. The specialization mapping above is then a homomorphism of $\Lambda_{\mathfrak{o}}$-modules (loc. cit.).

One can prove the following theorem in a similar manner as in [O2] (1.4.3). (From (1.3.5), we know that the both sides below are free $\mathfrak{o}$-modules of the same rank and, hence, we only need to show the surjectivity of $sp_{r,d}$ when $\mathfrak{o} = \mathbf{Z}_p$.) But a much more general result had been obtained by Ash and Stevens, cf. [AS], Theorem 5.1.

THEOREM (1.4.2). For each $r \geqslant 1$ and $d \geqslant 0$, $sp_{r,d}$ induces an isomorphism

$$e^*GES_p(N)_{\mathfrak{o}}/\omega_{r,d} \xrightarrow{\sim} e^*H^1(\Gamma_r, S^d(\mathfrak{o})).$$

Now when $s \geqslant r \geqslant 1$, for the same reason as [O2] (1.4.4), the following triangle commutes:

$$\begin{array}{ccc} GES_p(N)_{\mathfrak{o}} & \xrightarrow{sp_{s,d}} & H^1(\Gamma_s, S^d(\mathfrak{o})) \\ & {\scriptstyle sp_{r,d}}\searrow & \downarrow{\scriptstyle \mathrm{Cor}} \\ & & H^1(\Gamma_r, S^d(\mathfrak{o})). \end{array} \tag{1.4.3}$$

From this, we obtain the following corollary:

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

COROLLARY (1.4.4). *For each integer* $d \geqslant 0$, *the mappings* $sp_{r,d}$ *induce an isomorphism of* $\Lambda_{\mathfrak{o}}$*-modules* $e^*GES_p(N)_{\mathfrak{o}} \xrightarrow{\sim} \mathfrak{X}_{d,\mathfrak{o}}$.

1.5. p-ADIC HECKE ALGEBRAS

As usual, we denote by $M_k(\Gamma)$ (resp. $S_k(\Gamma)$) the space of holomorphic modular forms (resp. cusp forms) with respect to a congruence subgroup Γ of $\mathrm{SL}_2(\mathbf{Z})$. In this paper, we consider only forms of weight $k \geqslant 2$. For $f \in M_k(\Gamma)$ and $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{GL}_2(\mathbf{R})$ with positive determinant, we set

$$(f \mid \gamma)(z) := \det(\gamma)(cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right). \tag{1.5.1}$$

DEFINITION (1.5.2). We denote by $\mathcal{H}_k(\Gamma_r;\mathbf{Z})$ the $\mathbf{Z}$-subalgebra of $\mathrm{End}_{\mathbf{C}}(M_k(\Gamma_r))$ generated by all the Hecke operators $T(n)$ and $T(q,q)$. Similarly we define $\mathcal{H}_k^*(\Gamma_r;\mathbf{Z}) \subseteq \mathrm{End}_{\mathbf{C}}(M_k(\Gamma_r))$ using $T^*(n)$ and $T^*(q,q)$ (cf. [O1] 7.3). The Hecke algebras corresponding to $S_k(\Gamma_r)$ are denoted by $h_k(\Gamma_r;\mathbf{Z})$ and $h_k^*(\Gamma_r;\mathbf{Z})$, respectively. For any commutative ring R with unity, we set $\mathcal{H}_k(\Gamma_r;R) := \mathcal{H}_k(\Gamma_r;\mathbf{Z}) \otimes_{\mathbf{Z}} R$ and likewise for other algebras.

If we put

$$\tau_r := \begin{bmatrix} 0 & -1 \\ N_r & 0 \end{bmatrix} \quad \text{for } r \geqslant 1, \tag{1.5.3}$$

then we have

$$\begin{aligned} `\mid \tau_r\text{'} \circ T(n) &= `\mid \tau_r\text{'} \circ T^*(n), \\ `\mid \tau_r\text{'} \circ T(q,q) &= `\mid \tau_r\text{'} \circ T^*(q,q), \end{aligned} \tag{1.5.4}$$

both on $M_k(\Gamma_r)$ and $S_k(\Gamma_r)$. Thus $\mathcal{H}_k(\Gamma_r;R)$ and $\mathcal{H}_k^*(\Gamma_r;R)$ are canonically isomorphic via the correspondence: $T(n) \leftrightarrow T^*(n)$ and $T(q,q) \leftrightarrow T^*(q,q)$.

We set

$$\begin{aligned} \mathcal{H}_k(N;R) &:= \varprojlim_{r \geqslant 1} \mathcal{H}_k(\Gamma_r;R), \\ \mathcal{H}_k^*(N;R) &:= \varprojlim_{r \geqslant 1} \mathcal{H}_k^*(\Gamma_r;R), \end{aligned} \tag{1.5.5}$$

relative to the natural homomorphisms ($T(n) \mapsto T(n)$ and $T(q,q) \mapsto T(q,q)$ etc.); and we define $h_k(N;R)$ and $h_k^*(N;R)$ in a similar manner. The element of $\mathcal{H}_k(N;R)$ corresponding to the sequence of $T(n) \in \mathcal{H}_k(\Gamma_r;R)$ will be denoted by the same symbol $T(n)$; and similarly for $T^*(n)$, etc.

Via the Eichler–Shimura isomorphism, we may identify $\mathcal{H}_k(\Gamma_r;\mathbf{Z})$ and $\mathcal{H}_k^*(\Gamma_r;\mathbf{Z})$ with the subalgebras of $\mathrm{End}_{\mathbf{Q}}(H^1(\Gamma_r, S^d(\mathbf{Q})))$ defined in the same way as (1.5.2), where $k = d+2$. By (1.2.7), we may consider $\mathfrak{X}_{d,\mathfrak{o}}$ as an $e^*\mathcal{H}_{d+2}^*(N;\mathfrak{o})$-module.

Now we let $(\mathbf{Z}/N_r\mathbf{Z})^\times \ni q$ mod N_r act on $\mathcal{H}_2(\Gamma_r;R)$ (resp. $\mathcal{H}_2^*(\Gamma_r;R)$) as multiplication by $T(q,q)$ (resp. $T^*(q,q)$). Thus if we set

$$\mathcal{Z}_N := \varprojlim_{r\geqslant 1} (\mathbf{Z}/N_r\mathbf{Z})^\times \cong (\mathbf{Z}/N\mathbf{Z})^\times \times \mathbf{Z}_p^\times, \tag{1.5.6}$$

$\mathcal{H}_2(N;R)$ and $\mathcal{H}_2^*(N;R)$ are naturally equipped with the structure of $R[[\mathcal{Z}_N]]$-(and, hence, $R[[U_1]]$-)algebras.

Remember that e (resp. e^*) stands for the idempotent attached to $T(p)$ (resp. $T^*(p)$). The following result is essentially due to Hida; the corresponding assertion for $h_k(N;\mathfrak{o})$ and $h_k^*(N;\mathfrak{o})$ being well-known:

THEOREM-DEFINITION (1.5.7). (i) *Via the natural correspondence* $T(n) \leftrightarrow T(n)$ *and* $T(q,q) \leftrightarrow T(q,q)$, *we have isomorphisms of algebras* $e\mathcal{H}_2(N;\mathfrak{o}) \cong e\mathcal{H}_k(N;\mathfrak{o})$, *for all* $k \geqslant 2$*; and similarly we have* $e^*\mathcal{H}_2^*(N;\mathfrak{o}) \cong e^*\mathcal{H}_k^*(N;\mathfrak{o})$.

In what follows, we identify these isomorphic algebras, and write them $e\mathcal{H}(N;\mathfrak{o})$ *and* $e^*\mathcal{H}^*(N;\mathfrak{o})$, *respectively. We make the same convention for* $e\,h(N;\mathfrak{o})$ *and* $e^*h^*(N;\mathfrak{o})$.

(ii) $e\mathcal{H}(N;\mathfrak{o})$ *and* $e^*\mathcal{H}^*(N;\mathfrak{o})$ *are free* $\Lambda_\mathfrak{o}$*-modules of finite rank. The rank is given by*

$$\mathrm{rank}_{\Lambda_\mathfrak{o}}\, e\,h(N;\mathfrak{o}) + \frac{p-1}{2} \sum_{0<t|N} \varphi(t)\varphi\left(\frac{N}{t}\right).$$

(iii) *Via the natural correspondence, we have isomorphisms*

$$e\mathcal{H}(N;\mathfrak{o})/\omega_{r,d} \xrightarrow{\sim} e\mathcal{H}_{d+2}(\Gamma_r;\mathfrak{o}),$$
$$e^*\mathcal{H}^*(N;\mathfrak{o})/\omega_{r,d} \xrightarrow{\sim} e^*\mathcal{H}_{d+2}^*(\Gamma_r;\mathfrak{o}),$$

for every integers $r \geqslant 1$ *and* $d \geqslant 0$.

Unfortunately, in [H3], Hida proves the result only for the Hecke algebras attached to cusp forms. Thus we outline the proof for the convenience of the reader. We may assume that $\mathfrak{o}$ is finite over $\mathbf{Z}_p$.

Let $k = d+2 \geqslant 2$. As we noted above, we can consider $\mathfrak{X}_{d,\mathfrak{o}}$ as an $e^*\mathcal{H}_k^*(N;\mathfrak{o})$-module. Moreover, by (1.3.5), this is in fact a faithful $e^*\mathcal{H}_k^*(N;\mathfrak{o})$-module. We then obtain an injective homomorphism: $e^*\mathcal{H}_k^*(N;\mathfrak{o}) \hookrightarrow \mathrm{End}_{\Lambda_\mathfrak{o}}(\mathfrak{X}_{d,\mathfrak{o}}) \cong M_{r(N)}(\Lambda_\mathfrak{o})$, the matrix algebra of size $r(N)$ over $\Lambda_\mathfrak{o}$. It is easy to see that this mapping is continuous and, hence, we may identify $e^*\mathcal{H}_k^*(N;\mathfrak{o})$ with the $\mathfrak{o}$-subalgebra of

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

$\mathrm{End}_{\Lambda_\mathfrak{o}}(\mathfrak{X}_{d,\mathfrak{o}})$ topologically generated by all $T^*(n)$ and $T^*(q,q)$. The assertion (i) then follows from (1.4.4). It also follows that $e^*\mathcal{H}^*(N;\mathfrak{o})$ is finite over $\Lambda_\mathfrak{o}$.

The freeness in (ii) is more difficult and so we follow Hida's method. Consider $M_k(\Gamma_r)$ as a subspace of $\mathbf{C}[[q]]$ via the usual q-expansion and let

$$\begin{aligned} &M_k(\Gamma_r;\mathbf{Z}) := M_k(\Gamma_r)\cap\mathbf{Z}[[q]],\\ &M_k(\Gamma_r;R) := M_k(\Gamma_r;\mathbf{Z})\otimes_\mathbf{Z} R\hookrightarrow \mathbf{Z}[[q]]\otimes_\mathbf{Z} R. \end{aligned}\tag{1.5.8}$$

We then set

$$\begin{aligned} &M^j(\Gamma_r;\mathfrak{o}) := \oplus_{k=2}^j M_k(\Gamma_r;K)\cap\mathfrak{o}[[q]] \quad (j\geqslant 2),\\ &M^\infty(\Gamma_r;\mathfrak{o}) := \textstyle\bigcup_{j\geqslant 2} M^j(\Gamma_r;\mathfrak{o}) \ \text{ in } \ \mathfrak{o}[[q]], \end{aligned}\tag{1.5.9}$$

and let $\overline{M}(\Gamma_r;\mathfrak{o})$ denote the completion of $M^\infty(\Gamma_r;\mathfrak{o})$ with respect to the natural norm on $\mathfrak{o}[[q]]$. Then Hida proved that this subset of $\mathfrak{o}[[q]]$ is *independent* of $r\geqslant 1$ ([H2] Corollary 1.2) and we write $\overline{M}(N;\mathfrak{o})$ for this space.

We denote by $\mathcal{H}^j(\Gamma_r;\mathfrak{o})$ and $\mathcal{H}^{*j}(\Gamma_r;\mathfrak{o})$ the Hecke algebras for $M^j(\Gamma_r;\mathfrak{o})$ defined similarly as before. Then by the above-mentioned result, the algebras

$$\varprojlim_{j\geqslant 2}\mathcal{H}^j(\Gamma_r;\mathfrak{o}),\qquad \varprojlim_{j\geqslant 2}\mathcal{H}^{*j}(\Gamma_r;\mathfrak{o}),\tag{1.5.10}$$

are seen to be 'independent of $r\geqslant 1$' in the obvious sense ([H2] (1.15 a)), which we denote by $\mathcal{H}'(N;\mathfrak{o})$ and $\mathcal{H}^{*\prime}(N;\mathfrak{o})$, respectively. These are $\Lambda_\mathfrak{o}$-algebras in a natural manner.

Now from the inclusion $M_k(\Gamma_r;\mathfrak{o})\hookrightarrow\overline{M}(N;\mathfrak{o})$ we get homomorphisms

$$\begin{aligned} &\rho_{r,k}: e\mathcal{H}'(N;\mathfrak{o})\twoheadrightarrow e\mathcal{H}_k(\Gamma_r;\mathfrak{o}),\\ &\rho_{\infty,k}: e\mathcal{H}'(N;\mathfrak{o})\twoheadrightarrow e\mathcal{H}_k(N;\mathfrak{o}) = e\mathcal{H}(N;\mathfrak{o}), \end{aligned}\tag{1.5.11}$$

as in [H3] Section 1. Clearly, $\rho_{\infty,k}$ is independent of k and, hence, we write it ρ_∞. Similarly, we obtain a homomorphism

$$\rho_\infty^*: e^*\mathcal{H}^{*\prime}(N;\mathfrak{o})\twoheadrightarrow e^*\mathcal{H}^*(N;\mathfrak{o}).\tag{1.5.12}$$

By virtue of [H2], Theorem 3.1, $e^*\mathcal{H}^{*\prime}(N;\mathfrak{o})$ is free of finite rank over $\Lambda_\mathfrak{o}$. Let us now look at the homomorphisms induced from ρ_∞^*:

$$e^*\mathcal{H}^{*\prime}(N;\mathfrak{o})/\omega_{1,n}\twoheadrightarrow e^*\mathcal{H}^*(N;\mathfrak{o})/\omega_{1,n}\quad (n\geqslant 0).\tag{1.5.13}$$

These algebras act on $e^*H^1(\Gamma_1,S^n(\mathfrak{o}))\cong e^*GES_p(N)_\mathfrak{o}/\omega_{1,n}$ by (1.4.2). But by [H2] Corollary 3.2, we know that

$$e^*\mathcal{H}^{*\prime}(N;\mathfrak{o})/\omega_{1,n}\xrightarrow{\sim} e^*\mathcal{H}^*_{n+2}(\Gamma_1;\mathfrak{o})\ \text{ for }\ n\geqslant p-1.\tag{1.5.14}$$

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

It follows that this isomorphism must factor through $e^*\mathcal{H}^*(N;\mathfrak{o})/\omega_{1,n}$, showing that (1.5.13) is an isomorphism whenever $n \geqslant p-1$. The freeness in question then follows from the above-quoted theorem and [H3] Lemma 6.3; and it also follows that ρ^*_∞ and ρ_∞ are isomorphisms.

As for (iii), we have a natural surjective homomorphism: $e^*\mathcal{H}^*(N;\mathfrak{o})/\omega_{r,d} \twoheadrightarrow e^*\mathcal{H}^*_k(\Gamma_r;\mathfrak{o})$ by (1.4.2). Thus it is enough to show that these two *free* $\mathfrak{o}$-modules have the same rank.

For this, we recall the well-known duality: In general, let

$$m_k(\Gamma_r;\mathfrak{o}) := \{f \in M_k(\Gamma_r;K) \mid a(n;f) \in \mathfrak{o} \text{ for all } n \geqslant 1\}, \tag{1.5.15}$$

where $a(n;f)$ denotes the coefficient of q^n in f. Then the pairing

$$(\ ,\ ) : m_k(\Gamma_r;\mathfrak{o}) \times \mathcal{H}_k(\Gamma_r;\mathfrak{o}) \to \mathfrak{o}, \tag{1.5.16}$$

given by $(f,t) := a(1; f \mid t)$ sets up a perfect duality of free $\mathfrak{o}$-modules (cf. [H2] Proposition 2.1).

From this, (1.5.14), and the remark after it, we have

$$r := \operatorname{rank}_{\Lambda_\mathfrak{o}} e^*\mathcal{H}^*(N;\mathfrak{o}) = \operatorname{rank}_\mathfrak{o} e\mathcal{H}_l(\Gamma_1;\mathfrak{o}) = \operatorname{rank}_\mathfrak{o} e\, m_l(\Gamma_1;\mathfrak{o}), \tag{1.5.17}$$

for $l \geqslant p+1$. By [H3] Lemma 5.3, we see that

$$r = \dim_K\ e\, S_l(\Gamma_1;K) + \frac{p-1}{2} \sum_{0<t|N} \varphi(t)\varphi\left(\frac{N}{t}\right). \tag{1.5.18}$$

Similarly, we have

$$\begin{aligned}&\operatorname{rank}_\mathfrak{o} e^*\mathcal{H}^*_k(\Gamma_r;\mathfrak{o})\\ &\quad = \dim_K eS_k(\Gamma_r;K) + \frac{\varphi(p^r)}{2} \sum_{0<t|N} \varphi(t)\varphi\left(\frac{N}{t}\right).\end{aligned} \tag{1.5.19}$$

Since we already know that

$$\begin{aligned}\dim_K e\, S_k(\Gamma_r;K) &= p^{r-1}\operatorname{rank}_{\Lambda_\mathfrak{o}} e\, h(N;\mathfrak{o})\\ &= p^{r-1}\dim_K e\, S_l(\Gamma_1;K)\end{aligned} \tag{1.5.20}$$

the assertion (iii) follows. The formula of the rank in (ii) is also clear.

2. $\Lambda_{\mathfrak{o}}$-adic modular forms and projective systems of modular forms

2.1. $\Lambda_{\mathfrak{o}}$-ADIC MODULAR FORMS

As in [O2], we write $\widehat{U_1/U_r}$ for the set of $\overline{\mathbf{Q}}^{\times}$-valued characters of U_1/U_r (identified with the characters of U_1 trivial on U_r), and put

$$\widehat{U}_{1,f} := \bigcup_{r \geqslant 1} \widehat{U_1/U_r}. \tag{2.1.1}$$

When $\varepsilon \in \widehat{U}_{1,f}$, we denote by $\mathfrak{o}_\varepsilon$ (resp. K_ε) the ring generated by the values of ε over $\mathfrak{o}$ (resp. K), and define an element $P_{\varepsilon,d} \in \Lambda_{\mathbf{Z}_p\varepsilon}$ by

$$P_{\varepsilon,d} := \iota(u) - \varepsilon(u)u^d = T - (\varepsilon(u)u^d - 1), \tag{2.1.2}$$

for each integer $d \geqslant 0$. Also, we define an integer $r_\varepsilon \geqslant 1$ by $\mathrm{Ker}(\varepsilon) = U_{r_\varepsilon}$.

Let $\mathcal{L}_K$ be the quotient field of $\Lambda_{\mathfrak{o}}$. If $\mathcal{F} = \sum_{n=0}^{\infty} a(n;\mathcal{F})q^n \in \Lambda_{\mathfrak{o}}[[q]] \otimes_{\Lambda_{\mathfrak{o}}} \mathcal{L}_K \subset \mathcal{L}_K[[q]]$, we set

$$\mathcal{F}_{\varepsilon,d} := \sum_{n=0}^{\infty} a(n;\mathcal{F})(\varepsilon(u)u^d - 1) \cdot q^n \in K_\varepsilon[[q]], \tag{2.1.3}$$

whenever the right-hand side is meaningful and note that this is the case except possibly for finitely many pairs of ε and d.

For $\varepsilon \in \widehat{U_1/U_r}$, we set

$$\begin{aligned} &M_k(\Gamma_r, \varepsilon; \mathfrak{o}_\varepsilon) \\ &\quad := \{ f \in M_k(\Gamma_r; \mathfrak{o}_\varepsilon) \mid f \mid \sigma_\alpha = \varepsilon(\alpha) f \ \text{ for all } \ \alpha \in U_1 \}. \end{aligned} \tag{2.1.4}$$

Here, σ_α is an element of Γ_1 congruent to $\begin{bmatrix} \alpha^{-1} & * \\ 0 & \alpha \end{bmatrix}$ mod $p^r \cdot M_2(\mathbf{Z})$, and the operator '$\mid \sigma_\alpha$' is deduced from (1.5.1) (see [O2] 2.1 for further explanation about such symbols).

We are now going to define and study the spaces of $\Lambda_{\mathfrak{o}}$-adic modular forms. As in [O2], for the reason that will be clear later, it is convenient for us to start with such forms of a *fixed weight.*

DEFINITION (2.1.5). For each integer $k = d + 2 \geqslant 2$, we define two types of spaces of $\Lambda_{\mathfrak{o}}$-*adic modular forms of weight k and level* N by

$$\begin{aligned} &M_k(N; \Lambda_{\mathfrak{o}}) \\ &\quad := \{ \mathcal{F} \in \Lambda_{\mathfrak{o}}[[q]] \mid \mathcal{F}_{\varepsilon,d} \in M_k(\Gamma_{r_\varepsilon}, \varepsilon; \mathfrak{o}_\varepsilon) \ \text{ for all } \ \varepsilon \in \widehat{U}_{1,f} \}, \\ &M_k'(N; \Lambda_{\mathfrak{o}}) \\ &\quad := \{ \mathcal{F} \in \Lambda_{\mathfrak{o}}[[q]] \mid \mathcal{F}_{\varepsilon,d} \in M_k(\Gamma_{r_\varepsilon}, \varepsilon; \mathfrak{o}_\varepsilon) \ \text{ for almost all } \ \varepsilon \in \widehat{U}_{1,f} \}. \end{aligned}$$

These spaces are $\Lambda_{\mathfrak{o}}$-modules in the obvious manner.

If $\mathcal{F} = \sum_{n=0}^{\infty} a(n;\mathcal{F})q^n$ belongs to either one of these spaces, we set $\mathcal{F} \mid T(p) := \sum_{n=0}^{\infty} a(np;\mathcal{F})q^n$. Then it is clear that $(\mathcal{F} \mid T(p))_{\varepsilon,d} = \mathcal{F}_{\varepsilon,d} \mid T(p)$ whenever $\mathcal{F}_{\varepsilon,d} \in M_k(\Gamma_{r_\varepsilon}, \varepsilon; \mathfrak{o}_\varepsilon)$; and hence $\mathcal{F} \mid T(p)$ belongs to the same space. One can define the idempotent $e = \lim_{n\to\infty} T(p)^{n!}$ on each of the spaces above. The spaces $S_k(N;\Lambda_{\mathfrak{o}})$ of $\Lambda_{\mathfrak{o}}$-adic cusp forms are defined similarly; and we already know that $e\,S_k(N;\Lambda_{\mathfrak{o}})$ is independent of $k \geqslant 2$ (cf. [O2] (2.5.5)). *Let us henceforth denote this space by* $e\,S(N;\Lambda_{\mathfrak{o}})$. Later, we will show that $e\,M_k(N;\Lambda_{\mathfrak{o}}) = e\,M'_k(N;\Lambda_{\mathfrak{o}})$; and that this is independent of $k \geqslant 2$.

2.2. PROJECTIVE SYSTEMS OF MODULAR FORMS

Let τ_r be as in (1.5.3), and put

$$M_k^*(\Gamma_r;\mathfrak{o}) := \{f \in M_k(\Gamma_r;\mathbf{C}_p) \mid f \mid \tau_r \in M_k(\Gamma_r;\mathfrak{o})\}. \tag{2.2.1}$$

If we denote by $\mathrm{Tr}_r\colon M_k(\Gamma_{r+1};\mathbf{C}_p) \to M_k(\Gamma_r;\mathbf{C}_p)$ the natural trace mapping, then one can show that it sends $M_k^*(\Gamma_{r+1};\mathfrak{o})$ to $M_k^*(\Gamma_r;\mathfrak{o})$ as in [O2] 2.3.

DEFINITION (2.2.2). For each $k \geqslant 2$, we set

$$\mathfrak{M}_k^*(N;\mathfrak{o}) := \varprojlim_{r\geqslant 1} M_k^*(\Gamma_r;\mathfrak{o})$$

the projective limit being taken relative to Tr_r.

Since $M_k(\Gamma_r;\mathfrak{o})$ is stable under all $T(n)$ and $T(q,q)$, one sees from (1.5.4) that $M_k^*(\Gamma_r;\mathfrak{o})$ is stable under all $T^*(n)$ and $T^*(q,q)$. Also, Tr_r commutes with these operators. It follows that we can consider $\mathfrak{M}_k^*(N;\mathfrak{o})$ as a module over $\mathcal{H}_k^*(N;\mathfrak{o})$ (1.5.5). We can then consider $e^*\mathfrak{M}_k^*(N;\mathfrak{o})$ as a module over $e^*\mathcal{H}^*(N;\mathfrak{o})$ or $\Lambda_{\mathfrak{o}}$ (cf. (1.5.7)).

THEOREM (2.2.3). *For each* $k = d + 2 \geqslant 2$, *we have an isomorphism of* $\Lambda_{\mathfrak{o}}$-*modules* $e\,M_k(N;\Lambda_{\mathfrak{o}}) \cong e^*\mathfrak{M}_k^*(N;\mathfrak{o})$, *given explicitly as follows:*

If $\mathcal{F} \in e\,M_k(N;\Lambda_{\mathfrak{o}})$, *we send this element to* $\mathbf{f} = (f_r)_{r\geqslant 1} \in e^*\mathfrak{M}_k^*(N;\mathfrak{o})$ *defined by*

$$f_r := \frac{1}{p^{r-1}}\left(\sum_{\varepsilon\in\widehat{U_1/U_r}} \mathcal{F}_{\varepsilon,d} \mid T(p)^{-r}\right) \mid \tau_r^{-1}.$$

If $\mathbf{f} = (f_r)_{r\geqslant 1} \in e^*\mathfrak{M}_k^*(N;\mathfrak{o})$, *we send this element to the unique* $\mathcal{F} \in e\,M_k(N;\Lambda_{\mathfrak{o}})$ *satisfying*

$$\mathcal{F}_{\varepsilon,d} = \sum_{\alpha\in U_1/U_r} \varepsilon(\alpha)(f_r \mid \tau_r \mid T(p)^r \mid \sigma_\alpha^{-1}),$$

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

for all $\varepsilon \in \widehat{U_{1,f}}$. *Here,* r *is any integer such that* $r \geqslant r_\varepsilon$.

Proof. The proof given for cusp forms ([O2] 2.4) works without any change in the present case and, hence, we do not repeat it here. □

Via this theorem and the canonical isomorphism: $e\,\mathcal{H}(N;\mathfrak{o}) \cong e^*\mathcal{H}^*(N;\mathfrak{o})$ $(T(n) \leftrightarrow T^*(n), T(q,q) \leftrightarrow T^*(q,q))$, we henceforth consider $e\,M_k(N;\Lambda_\mathfrak{o})$ as an $e\,\mathcal{H}(N;\mathfrak{o})$-module. One easily checks that the resulting $\Lambda_\mathfrak{o}$-module structure coincides with the obvious one and also that

$$\begin{aligned}(\mathcal{F} \mid T(n))_{\varepsilon,d} &= \mathcal{F}_{\varepsilon,d} \mid T(n),\\ (\mathcal{F} \mid T(q,q))_{\varepsilon,d} &= \mathcal{F}_{\varepsilon,d} \mid T(q,q),\end{aligned} \tag{2.2.4}$$

for all $\mathcal{F} \in e\,M_k(N;\Lambda_\mathfrak{o})$ and $\varepsilon \in \widehat{U_{1,f}}$.

2.3. $\Lambda_\mathfrak{o}$-ADIC EISENSTEIN SERIES

Let u, v and c be positive integers; and let χ and ψ be Dirichlet characters defined modulo u and v, respectively. Then we set

$$\begin{aligned}&E_k(\chi,\psi;c)\\ &:= \delta(\psi)L_\infty(1-k,\chi) + \sum_{n=1}^{\infty}\left(\sum_{0<t|n}\chi(t)\psi\left(\frac{n}{t}\right)t^{k-1}\right)q^{cn},\end{aligned} \tag{2.3.1}$$

where $L_\infty(s,\chi)$ is the Dirichlet L-function; and $\delta(\psi)$ is $1/2$ if ψ is the trivial character, and 0 otherwise. When χ is a Dirichlet character modulo u, we denote by χ_1 the character modulo $\mathrm{LCM}(u,p)$ induced from χ. We then have $L_\infty(s,\chi_1) = (1-\chi(p)p^{-s})L_\infty(s,\chi)$.

Let $\mathrm{Eis}_k(\Gamma_r)$ be the orthogonal complement of $S_k(\Gamma_r)$ in $M_k(\Gamma_r)$ with respect to the Petersson metric.

LEMMA (2.3.2) ([H3] Lemma 5.3 and its proof). *Suppose that* $k \geqslant 2$ *and* $r \geqslant 1$, *and let* $\mathrm{Eis}_k(\Gamma_r;\mathbf{Q})$ *be the set of all elements of* $\mathrm{Eis}_k(\Gamma_r)$ *having* $\mathbf{Q}$-*rational* q-*expansions. Then* $\mathrm{Eis}_k(\Gamma_r;\mathbf{Q})$ *spans* $\mathrm{Eis}_k(\Gamma_r)$; *and the idempotent* e *attached to* $T(p)$ *acting on* $\mathrm{Eis}_k(\Gamma_r;\mathbf{Q}) \otimes_\mathbf{Q} \mathbf{C}_p$ *leaves* $\mathrm{Eis}_k(\Gamma_r;\mathbf{Q})$ *stable. The series* $E_k(\chi_1,\psi;c)$ *with* χ, ψ *and* c *satisfying the following three conditions give a basis of* $e\,\mathrm{Eis}_k(\Gamma_r)$:

(i) $\chi\psi(-1) = (-1)^k$ *and* cuv *divides* N_r;
(ii) χ *and* ψ *are primitive Dirichlet characters modulo* u *and* v, *respectively;*
(iii) v *and* c *are prime to* p.

Moreover, we have

$$\dim_\mathbf{C} e\,\mathrm{Eis}_k(\Gamma_r) = \frac{\varphi(p^r)}{2}\sum_{0<t|N}\varphi(t)\varphi\left(\frac{N}{t}\right).$$

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

We are going to construct enough elements of $e\,M_k(N;\Lambda_\circ)/e\,S_k(N;\Lambda_\circ)$ using this lemma. To do this, we first recall well-known facts about p-adic L-functions (cf. Washington [Wa] Section 7.2): Let θ be an even primitive Dirichlet character of the first kind. Then there is a unique element

$$F(T,\theta) \in \begin{cases} \Lambda_{\mathbf{Z}_{p_\theta}} & \text{if } \theta \neq \mathbf{1}, \\ \frac{1}{(1+T)-u}\Lambda_{\mathbf{Z}_p} & \text{if } \theta = \mathbf{1}, \end{cases} \tag{2.3.3}$$

such that $F(u^s-1,\theta) = L_p(s,\theta)$, the Kubota–Leopoldt p-adic L-function attached to θ. Here, and henceforth, we denote by $\mathbf{1}$ the trivial character.

We may consider an $\varepsilon \in \widehat{U_{1,f}}$ as a (primitive) Dirichlet character of the second kind. It is then known that, moreover, we have

$$F(\varepsilon(u)u^s-1,\theta) = L_p(s,\theta\varepsilon^{-1}). \tag{2.3.4}$$

We set

$$G(T,\theta) := F(u^{-1}(1+T)^{-1}-1,\theta), \tag{2.3.5}$$

so that we have

$$G(\varepsilon(u)u^d-1,\theta) = L_p(1-k,\theta\varepsilon) = L_\infty(1-k,(\theta\varepsilon\omega^{-k})_1), \tag{2.3.6}$$

for $k = d+2 \geqslant 2$. Here, ω is the Teichmüller character; and, as in [Wa], we consider $\theta\varepsilon\omega^{-k}$ as a primitive Dirichlet character.

On the other hand, we can write every $a \in \mathbf{Z}_p^\times$ as

$$a = \omega(a)\langle a\rangle, \tag{2.3.7}$$

with $\langle a\rangle \in U_1$. If t is a positive integer prime to p, we set

$$A_t(T) := t(1+T)^{s(t)} = t\sum_{i=0}^{\infty}\binom{s(t)}{i}T^i \quad \text{if } \langle t\rangle = u^{s(t)}. \tag{2.3.8}$$

Then using the same convention as above, we have

$$A_t(\varepsilon(u)u^d-1) = t^{d+1}\varepsilon\omega^{-d}(t), \tag{2.3.9}$$

for any $\varepsilon \in \widehat{U_{1,f}}$.

THEOREM–DEFINITION (2.3.10). *Let θ and ψ be primitive Dirichlet characters defined modulo u and v, respectively; and let c be a positive integer. We assume that $\theta\psi(-1)=1$; v and c are prime to p; and cuv divides $N_1 = Np$. Set*

$$\mathcal{E}(\theta,\psi;c) := \delta(\psi)G(T,\theta\omega^2) + \sum_{n=1}^{\infty}\left(\sum_{\substack{0<t|n\\ p\nmid t}}\theta(t)\psi\left(\frac{n}{t}\right)A_t(T)\right)\cdot q^{cn}.$$

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

Then, for any $\varepsilon \in \widehat{U_{1,f}}$ *and* $d \geqslant 0$*, we have*

$$\mathcal{E}(\theta, \psi; c)_{\varepsilon,d} = E_{d+2}((\theta\varepsilon\omega^{-d})_1, \psi; c).$$

Whenever $\mathfrak{o}$ *contains the values of* θ *and* ψ*, we have:* $\mathcal{E}(\theta, \psi; c) \in \bigcap_{k\geqslant 2} e\,M_k(N; \Lambda_{\mathfrak{o}})$ *unless* $\theta = \omega^{-2}$ *and* $\psi = \mathbf{1}$*; and* $((1+T) - u^{-2})\mathcal{E}(\omega^{-2}, \mathbf{1}; c)$ *has the same property.*

When θ, ψ *and* c *satisfying the above conditions vary, and* $\mathfrak{o}$ *contains the values of all* θ *and* ψ*, we obtain* $((p-1)/2) \sum_{0<t|N} \varphi(t)\varphi(N/t)$ *such* $\Lambda_{\mathfrak{o}}$-adic Eisenstein series *which are linearly independent over* $\Lambda_{\mathfrak{o}}$ *modulo* $e\,S(N; \Lambda_{\mathfrak{o}})$.

Proof. First note that $\theta\omega^2$ is of the first kind. Then from (2.3.6) and (2.3.9), we see that $\mathcal{E}(\theta, \psi; c)_{\varepsilon,d}$ coincides with $E_k((\theta\varepsilon\omega^{-d})_1, \psi; c)$ with $k = d+2$ for every $d \geqslant 0$ and $\varepsilon \in \widehat{U_{1,f}}$. It is clear that, under our assumption, $\theta\varepsilon\omega^{-d}$, ψ and c satisfy the conditions (i)–(iii) of (2.3.2). Now assume that K contains the values of θ and ψ. Then we have shown that $E_k((\theta\varepsilon\omega^{-d})_1, \psi; c)$ belongs to $e\,M_k(\Gamma_r; K_\varepsilon)$. But it is well known that the Nebentypus character of this form is (the one induced from) $(\theta\varepsilon\omega^{-d})_1\psi$. We conclude that $\mathcal{E}(\theta, \psi; c)_{\varepsilon,d} \in e\,M_k(\Gamma_r, \varepsilon; \mathfrak{o}_\varepsilon) \otimes_{\mathfrak{o}_\varepsilon} K_\varepsilon$ for all $\varepsilon \in \widehat{U_{1,f}}$ and $d \geqslant 0$. This proves the first part of the theorem.

That the number of the $\Lambda_{\mathfrak{o}}$-adic Eisenstein series is given by the above formula is a special case of (2.3.2); and the linear independence follows by looking at the specialization. □

2.4. THE STRUCTURE OF $e\,M_k(N; \Lambda_{\mathfrak{o}})$

Let $\varepsilon \in \widehat{U_1/U_r}$ be a character whose values are contained in $\mathfrak{o}$. We then denote by $\mathcal{H}_k(\Gamma_r, \varepsilon; \mathfrak{o})$ the $\mathfrak{o}$-subalgebra of $\mathrm{End}_{\mathfrak{o}}(M_k(\Gamma_r, \varepsilon; \mathfrak{o}))$ generated by all $T(n)$ and $T(q,q)$. We also set

$$m_k(\Gamma_r, \varepsilon; \mathfrak{o}) := \{f \in M_k(\Gamma_r, \varepsilon; \mathfrak{o}) \otimes_{\mathfrak{o}} K \mid a(n; f) \in \mathfrak{o} \ \text{ for all } \ n \geqslant 1\}. \tag{2.4.1}$$

We can define a pairing

$$(\ ,\ ) : m_k(\Gamma_r, \varepsilon; \mathfrak{o}) \times \mathcal{H}_k(\Gamma_r, \varepsilon; \mathfrak{o}) \to \mathfrak{o}, \tag{2.4.2}$$

as in (1.5.16), which gives a perfect duality of free $\mathfrak{o}$-modules. It follows from (1.5.7) (iii) that we have a canonical isomorphism

$$e\,\mathcal{H}(N; \mathfrak{o})/P_{\varepsilon,d} \xrightarrow{\sim} e\mathcal{H}_{d+2}(\Gamma_r, \varepsilon; \mathfrak{o}), \tag{2.4.3}$$

for all $d \geqslant 0$ and ε as above. We therefore have the equalities:

$$\mathrm{rank}_{\mathfrak{o}}\, e\,m_k(\Gamma_r, \varepsilon; \mathfrak{o}) = \mathrm{rank}_{\mathfrak{o}}\, e\,M_k(\Gamma_r, \varepsilon; \mathfrak{o}) = \mathrm{rank}_{\Lambda_{\mathfrak{o}}}\, e\,\mathcal{H}(N; \mathfrak{o}). \tag{2.4.4}$$

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

Now the purpose of this subsection is to prove the following

THEOREM-DEFINITION (2.4.5) *The subspace* $e\,M_k(N;\Lambda_{\mathfrak{o}})$ *of* $\Lambda_{\mathfrak{o}}[[q]]$ *is independent of* $k \geqslant 2$. *Moreover, it is a free* $\Lambda_{\mathfrak{o}}$*-module whose rank is equal to* $\mathrm{rank}_{\Lambda_{\mathfrak{o}}}\, e\,\mathcal{H}(N;\mathfrak{o})$. We hereafter denote this space by $e\,M(N;\Lambda_{\mathfrak{o}})$.

For the proof, we follow the method of Hida [H4] 7.3. As usual, put $k = d+2 \geqslant 2$.

LEMMA (2.4.6) $e\,M'_k(N;\Lambda_{\mathfrak{o}})$ *is a finite and free* $\Lambda_{\mathfrak{o}}$*-module.*

Proof. We first show that, if $\mathfrak{o}_0$ is the ring of integers of a finite extension K_0 of K, then $e\,M'_k(N;\Lambda_{\mathfrak{o}_0}) = e\,M'_k(N;\Lambda_{\mathfrak{o}}) \otimes_{\mathfrak{o}} \mathfrak{o}_0$. (The same holds for $e\,M_k(N;\Lambda_{\mathfrak{o}})$.) For this, we assume for the moment that K_0 is a Galois extension of K whose Galois group is $\{\sigma_1,\ldots,\sigma_m\}$. Let $\{\omega_1,\ldots,\omega_m\}$ be a basis of $\mathfrak{o}_0$ over $\mathfrak{o}$. Then we may write every $\mathcal{F} \in e\,M'_k(N;\Lambda_{\mathfrak{o}_0})$ as $\mathcal{F} = \sum_{i=1}^m \omega_i\mathcal{F}_i$ with $\mathcal{F}_i \in \Lambda_{\mathfrak{o}}[[q]]$. If we let $\mathrm{Gal}(K_0/K)$ act on the coefficients of $\Lambda_{\mathfrak{o}_0}[[q]] = \mathfrak{o}_0[[T,q]]$, then it is easy to see that each $\mathcal{F}^{\sigma_j}$ is an element of $e\,M'_k(N;\Lambda_{\mathfrak{o}_0})$. Since the matrix $(\omega_i^{\sigma_j})_{1\leqslant i,j\leqslant m}$ is invertible, we can express $\mathcal{F}_i$ as a linear combination of $\mathcal{F}^{\sigma_j}$'s. This shows that $\mathcal{F}_i \in e\,M'_k(N;\Lambda_{\mathfrak{o}_0}) \cap \Lambda_{\mathfrak{o}}[[q]] = e\,M'_k(N;\Lambda_{\mathfrak{o}})$ and, hence, $e\,M'_k(N;\Lambda_{\mathfrak{o}_0}) \subseteq e\,M'_k(N;\Lambda_{\mathfrak{o}}) \otimes_{\mathfrak{o}} \mathfrak{o}_0$. The converse inclusion is obvious.

In the general case, we let K_1 be the Galois closure of K_0/K, and denote by $\mathfrak{o}_1$ its ring of integers. We then obtain the desired equality by taking the $\mathrm{Gal}(K_1/K_0)$-invariants from the equality: $e\,M'_k(N;\Lambda_{\mathfrak{o}_1}) = e\,M'_k(N;\Lambda_{\mathfrak{o}}) \otimes_{\mathfrak{o}} \mathfrak{o}_1$.

After this remark, the proof goes as that of [H4] 7.3 Theorem 1 as follows:

- Let $\{\mathcal{F}_1,\ldots,\mathcal{F}_r\} \subseteq e\,M'_k(N;\Lambda_{\mathfrak{o}})$ be a maximal set of $\Lambda_{\mathfrak{o}}$-linearly independent elements. This is a finite set; and in fact r is bounded by $\mathrm{rank}_{\Lambda_{\mathfrak{o}}} e\mathcal{H}(N;\mathfrak{o})$ by (2.4.4). Then there is a nonzero $D(T) \in \Lambda_{\mathfrak{o}}$ such that $e\,M'_k(N;\Lambda_{\mathfrak{o}}) \subseteq (1/D(T))(\Lambda_{\mathfrak{o}}\mathcal{F}_1 + \cdots + \Lambda_{\mathfrak{o}}\mathcal{F}_r)$.
- We may therefore take an $\varepsilon \in \widehat{U_{1,f}}$ so that $\mathcal{F}_{\varepsilon,d} \in e\,M_k(\Gamma_{r_\varepsilon},\varepsilon;\mathfrak{o}_\varepsilon)$ for *all* $\mathcal{F} \in e\,M'_k(N;\Lambda_{\mathfrak{o}})$. By the first remark, we may assume that $\mathfrak{o}_\varepsilon = \mathfrak{o}$ to prove our lemma.
- One sees that

$$P_{\varepsilon,d}\cdot e\,M'_k(N;\Lambda_{\mathfrak{o}}) = \{\mathcal{F} \in e\,M'_k(N;\Lambda_{\mathfrak{o}}) \mid \mathcal{F}_{\varepsilon,d} = 0\}.$$

(Note here that the corresponding assertion for $e\,M_k(N;\Lambda_{\mathfrak{o}})$ is far from being trivial.) Thus the correspondence $\mathcal{F} \mapsto \mathcal{F}_{\varepsilon,d}$ gives an injection

$$e\,M'_k(N;\Lambda_{\mathfrak{o}})/P_{\varepsilon,d} \hookrightarrow e\,M_k(\Gamma_{r_\varepsilon},\varepsilon;\mathfrak{o}).$$

If $\{\mathcal{F}_1,\ldots,\mathcal{F}_r\} \subseteq e\,M'_k(N;\Lambda_{\mathfrak{o}})$ gives an $\mathfrak{o}$-basis of $e\,M'_k(N;\Lambda_{\mathfrak{o}})/P_{\varepsilon,d}$ when reduced modulo $P_{\varepsilon,d}$, then it is a free basis of $e\,M'_k(N;\Lambda_{\mathfrak{o}})$ over $\Lambda_{\mathfrak{o}}$. □

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

LEMMA (2.4.7). $e\,M'_k(N;\Lambda_{\mathfrak{o}}) \subseteq \Lambda_{\mathfrak{o}}[[q]]$ *is independent of* $k \geqslant 2$*. Moreover, its* $\Lambda_{\mathfrak{o}}$*-rank is equal to* $\mathrm{rank}_{\Lambda_{\mathfrak{o}}} e\mathcal{H}(N;\mathfrak{o})$.

Proof. It follows from the proof of the lemma above that

$$\mathrm{rank}_{\Lambda_{\mathfrak{o}}} e\,M'_k(N;\Lambda_{\mathfrak{o}}) \leqslant \mathrm{rank}_{\Lambda_{\mathfrak{o}}} e\mathcal{H}(N;\mathfrak{o}).$$

However, $e\,M'_k(N;\Lambda_{\mathfrak{o}})$ contains $e\,S(N;\Lambda_{\mathfrak{o}})$, which is $\Lambda_{\mathfrak{o}}$-free, and the $\Lambda_{\mathfrak{o}}$-adic Eisenstein series constructed in (2.3.10). Therefore, we have

$$\mathrm{rank}_{\Lambda_{\mathfrak{o}}} e\,M'_k(N;\Lambda_{\mathfrak{o}}) \geqslant \mathrm{rank}_{\Lambda_{\mathfrak{o}}} e\,S(N;\Lambda_{\mathfrak{o}}) + \frac{p-1}{2}\sum_{0<t|N} \varphi(t)\varphi\left(\frac{N}{t}\right).$$

By (1.5.7) (ii) and [O2] (2.5.3), the right-hand side is equal to $\mathrm{rank}_{\Lambda_{\mathfrak{o}}} e\mathcal{H}(N;\mathfrak{o})$. This proves our assertion concerning the rank.

We have also shown that $e\,M'_k(N;\Lambda_{\mathfrak{o}})\otimes_{\Lambda_{\mathfrak{o}}}\mathcal{L}_K$ is spanned over $\mathcal{L}_K$ by $e\,S(N;\Lambda_{\mathfrak{o}})$ and the $\Lambda_{\mathfrak{o}}$-adic Eisenstein series in (2.3.10). It is therefore independent of $k \geqslant 2$ and, hence, so is $e\,M'_k(N;\Lambda_{\mathfrak{o}}) = (e\,M'_k(N;\Lambda_{\mathfrak{o}}) \otimes_{\Lambda_{\mathfrak{o}}} \mathcal{L}_K) \cap \Lambda_{\mathfrak{o}}[[q]]$. □

In the following, we write $e\,M'(N;\Lambda_{\mathfrak{o}})$ for the common space in the lemma above.

LEMMA (2.4.8). *Let* $\varepsilon \in \widehat{U_1/U_r}$ *take values in* $\mathfrak{o}$*. Then for any* $g \in e\,M_k(\Gamma_r,\varepsilon;\mathfrak{o})$*, there is an* $\mathcal{F} \in e\,M'(N;\Lambda_{\mathfrak{o}})$ *such that* $\mathcal{F}_{\varepsilon,d} = g$*.*

Proof (cf. [H4] p. 215). We consider $\mathcal{E}(\omega^{-2},\mathbf{1};1)$ given in (2.3.10). Its 'constant term' is $G(T,\mathbf{1})/2$, and we recall that $G(u^s-1,\mathbf{1}) = \zeta_p(-s-1)$ ((2.3.4), (2.3.5)), where ζ_p is the p-adic Riemann zeta function. Put $\mathcal{E}' := ((1+T)-u^{-2})\mathcal{E}(\omega^{-2},\mathbf{1};1)$, which belongs to $e\,M_l(N;\Lambda_{\mathfrak{o}})$ for all $l \geqslant 2$. Then $\mathcal{E}'\,|_{T=u^{-2}-1}= (2u^2)^{-1}(p^{-1}-1)\log_p u =: C$ is a constant which is in fact a p-adic unit. Let $\mathcal{E}''$ be the element of $\Lambda_{\mathfrak{o}}[[q]]$ obtained from $C^{-1}\mathcal{E}'$ by the change of variable $T \mapsto \varepsilon(u)^{-1}u^{-k}(1+T)-1$.

Now for g as above, it is easy to see that $g\cdot\mathcal{E}'' \in \Lambda_{\mathfrak{o}}[[q]]$ belongs to $M'_l(N;\Lambda_{\mathfrak{o}})$ for any $l \geqslant k+2$; and also that $(g\cdot\mathcal{E}'')_{\varepsilon,d} = g$. It follows that $\mathcal{F} := e(g\cdot\mathcal{E}'')$ has the desired property. □

Theorem (2.4.5) would follow from what we said above, and the following lemma:

LEMMA (2.4.9). $e\,M_k(N;\Lambda_{\mathfrak{o}}) = e\,M'(N;\Lambda_{\mathfrak{o}})$.

Proof (cf. [H4] loc. cit.). Assume otherwise and take an element $\mathcal{F} \in e\,M'(N;\Lambda_{\mathfrak{o}}) - e\,M_k(N;\Lambda_{\mathfrak{o}})$. Then there is an $\varepsilon \in \widehat{U_{1,f}}$ such that $\mathcal{F}_{\varepsilon,d} \notin e\,M_k(\Gamma_{r_\varepsilon},\varepsilon;\mathfrak{o}_\varepsilon)$. It follows from this and (2.4.8) that

$$\mathrm{rank}_{\mathfrak{o}_\varepsilon} e\,M'(N;\Lambda_{\mathfrak{o}_\varepsilon})/P_{\varepsilon,d} > \mathrm{rank}_{\mathfrak{o}_\varepsilon} e\,M_k(\Gamma_{r_\varepsilon},\varepsilon;\mathfrak{o}_\varepsilon) = \mathrm{rank}_{\Lambda_{\mathfrak{o}}} e\,\mathcal{H}(N;\mathfrak{o})$$

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

which contradicts (2.4.7). □

As a consequence of (2.2.3) and (2.4.5), we record:

COROLLARY (2.4.10). *For any k and $k' \geqslant 2$, $e^*\mathfrak{M}_k^*(N;\mathfrak{o})$ and $e^*\mathfrak{M}_{k'}^*(N;\mathfrak{o})$ are canonically isomorphic as $e^*\mathcal{H}^*(N;\mathfrak{o})$-modules; and these are free $\Lambda_\mathfrak{o}$-modules of finite rank.*

2.5. SPECIALIZATIONS

As for the specializations of $e\,M(N;\Lambda_\mathfrak{o})$, we obtain the following result immediately from the argument of 2.4:

PROPOSITION (2.5.1). *Let $\varepsilon \in \widehat{U_{1,f}}$ take values in $\mathfrak{o}$. Then for every integer $k = d+2 \geqslant 2$, the correspondence: $\mathcal{F} \mapsto \mathcal{F}_{\varepsilon,d}$ gives an isomorphism:*

$$e\,M(N;\Lambda_\mathfrak{o})/P_{\varepsilon,d} \xrightarrow{\sim} e\,M_k(\Gamma_{r_\varepsilon},\varepsilon;\mathfrak{o}).$$

Next, for $\varepsilon \in \widehat{U_1/U_r}$ with values in $\mathfrak{o}$, we set

$$M_k^*(\Gamma_r,\varepsilon;\mathfrak{o}) := \{f \in M_k(\Gamma_r;\mathbf{C}_p) \mid \ f \mid \tau_r \in M_k(\Gamma_r,\varepsilon;\mathfrak{o})\}. \tag{2.5.2}$$

We can then define

$$p_\varepsilon : e^*\mathfrak{M}_k^*(N;\mathfrak{o}) \to e^*M_k^*(\Gamma_{r_\varepsilon},\varepsilon;\mathfrak{o}) \tag{2.5.3}$$

by $p_\varepsilon((f_r)_{r\geqslant 1}) := \sum_{\alpha\in U_1/U_{r_\varepsilon}} \varepsilon(\alpha) f_{r_\varepsilon} \mid \sigma_\alpha$, which factors through $e^*\mathfrak{M}_k^*(N;\mathfrak{o})/P_{\varepsilon,d}$. One then obtains the following result in the same manner as in the case of cusp forms (cf. [O2] (2.6.4)):

PROPOSITION (2.5.4). *Let the notation be as above. Then we have the following commutative diagram:*

$$\begin{array}{ccc}
e^*\mathfrak{M}_k^*(N;\mathfrak{o}) & \xrightarrow[(2.2.3)]{\sim} & e\,M(N;\Lambda_\mathfrak{o}) \\
\downarrow{\scriptstyle \text{can}} & & \downarrow{\scriptstyle \text{can}} \\
e^*\mathfrak{M}_k^*(N;\mathfrak{o})/P_{\varepsilon,d} & \xrightarrow[(2.2.3)]{\sim} & e\,M(N;\Lambda_\mathfrak{o})/P_{\varepsilon,d} \\
\downarrow{\scriptstyle p_\varepsilon} & & \wr\downarrow{\scriptstyle (2.5.1)} \\
e^*M_k^*(\Gamma_{r_\varepsilon},\varepsilon;\mathfrak{o}) & \xrightarrow{\sim} & e\,M_k(\Gamma_{r_\varepsilon},\varepsilon;\mathfrak{o}),
\end{array}$$

if we define the bottom horizontal arrow by $f \mapsto f \mid \tau_{r_\varepsilon} \mid T(p)^{r_\varepsilon}$. In particular, p_ε induces an isomorphism $e^*\mathfrak{M}_k^*(N;\mathfrak{o})/P_{\varepsilon,d} \xrightarrow{\sim} e^*M_k^*(\Gamma_{r_\varepsilon},\varepsilon;\mathfrak{o})$.

In concluding this section, we add the following remark:

Remark (2.5.5). Set $e\,m(N;\Lambda_\mathfrak{o}) := (e\,M(N;\Lambda_\mathfrak{o}) \otimes_{\Lambda_\mathfrak{o}} \mathcal{L}_K) \cap (\mathcal{L}_K + q\Lambda_\mathfrak{o}[[q]])$. Then we can show that the pairing $e\,m(N;\Lambda_\mathfrak{o}) \times e\mathcal{H}(N;\mathfrak{o}) \to \Lambda_\mathfrak{o}$ defined by $(\mathcal{F},t) := a(1;\mathcal{F} \mid t)$ sets up a perfect duality of free $\Lambda_\mathfrak{o}$-modules; and also that $e\,M(N;\Lambda_\mathfrak{o})$ is a faithful $e\mathcal{H}(N;\mathfrak{o})$-module. Especially, we can identify $e\mathcal{H}(N;\mathfrak{o})$ with the $\Lambda_\mathfrak{o}$-subalgebra of $\mathrm{End}_{\Lambda_\mathfrak{o}}(e\,M(N;\Lambda_\mathfrak{o}))$ generated by all $T(n)$. This point of view was taken up as the definition of $e\mathcal{H}(N;\mathfrak{o})$ in [H4].

3. Preliminaries on generalized Jacobians

3.1. GENERALIZED JACOBIANS

In this section, we recall and study some properties of generalized Jacobians of Rosenlicht and Serre. Basic references are Serre [Se] and Bosch–Lütkebohmert–Raynaud [BLR].

For simplicity, we assume that our base field F is of characteristic 0; and consider only the generalized Jacobians of *reduced* moduli. Now let Y be a geometrically connected and smooth curve over F, and X its smooth compactification. We consider $C := X - Y$ as the reduced closed subscheme of X. We henceforth assume that C is nonempty.

Recall that, for an F-scheme S, an invertible sheaf on X_S (the base change of X from F to S) rigidified along C_S is a pair $(\mathcal{L},\alpha)$, where $\mathcal{L}$ is an invertible sheaf on X_S and α is an isomorphism: $\mathcal{O}_{C_S} \xrightarrow{\sim} \mathcal{L}\mid_{C_S}$. The functor

$$(\mathrm{Pic}_{X/F},C) : (\mathrm{Sch}/F)^0 \to (\mathrm{Sets}) \tag{3.1.1}$$

assigning to each $S \in (\mathrm{Sch}/F)^0$ the set of isomorphism classes of $(\mathcal{L},\alpha)$ as above, is represented by a commutative group scheme locally of finite presentation over F. We denote this group scheme by P_Y. Its identity component

$$P_Y^0 =: GJ_Y \tag{3.1.2}$$

is the *generalized Jacobian* of X with the modulus C.

For any F-scheme S and $s \in Y(S)$, we may consider s as a section of Y_S over S and, hence, also as an effective relative Cartier divisor D_s of degree 1 on X_S over S. The correspondence: $s \mapsto (\mathcal{O}_X(D_s)$ together with its canonical rigidification) gives an F-morphism

$$\iota_Y : Y \to P_Y, \tag{3.1.3}$$

the *canonical morphism* of Y to P_Y. If we fix a rational point $x_0 \in Y(F)$, we also have a morphism

$$\iota_{Y,x_0} : Y \to GJ_Y, \tag{3.1.4}$$

by $\iota_{Y,x_0}(s) = \iota_Y(s) - \iota_Y(x_{0,S})$ for $s \in Y(S)$ as above, where $x_{0,S}$ is the base change of the section x_0 to S. We may consider ι_Y and ι_{Y,x_0} as rational mappings from X to P_Y and GJ_Y, respectively; and they enjoy the universal property of 'Albanese type' ([BLR] 10.3 Theorem 2, [Se] V n°9 Théorème 2).

Let P_X be the usual Picard scheme of X over F, and $J_X := P_X^0$ the usual Jacobian variety of X. Then there is a natural homomorphism 'forgetting the rigidification': $P_Y \to P_X$ and, hence, also $GJ_Y \to J_X$. We have a natural exact sequence of commutative group schemes over F:

$$0 \to V_X^* \to V_C^* \to P_Y \to P_X \to 0, \tag{3.1.5}$$

where V_X^* (resp. V_C^*) represents the functor $(\mathrm{Sch}/F)^0 \to (\mathrm{Sets})$ which associates each S with the group $\Gamma(X_S, \mathcal{O}_{X_S}^*)$ (resp. $\Gamma(C_S, \mathcal{O}_{C_S}^*)$) ([BLR] 8.1). We recall that the middle arrow sends $u \in \Gamma(C_S, \mathcal{O}_{C_S}^*)$ to the pair $(\mathcal{O}_{X_S}$ (the multiplication by u)) $\in P_Y(S)$. In our situation, we clearly have $\Gamma(X_S, \mathcal{O}_{X_S}^*) = \Gamma(S, \mathcal{O}_S^*)$ and, hence, $V_X^* = \mathbf{G}_m$. On the other hand, it is also clear that $V_C^* = R_{C/F}(\mathbf{G}_m)$, the Weil restriction of $\mathbf{G}_m$. Thus, if we set

$$T_Y := \mathrm{Ker}(P_Y \to P_X) = \mathrm{Ker}(GJ_Y \to J_X), \tag{3.1.6}$$

we have a canonical isomorphism

$$T_Y \cong \mathrm{Coker}(\mathbf{G}_m \to R_{C/F}(\mathbf{G}_m)), \tag{3.1.7}$$

where the morphism corresponds to the natural $\Gamma(S, \mathcal{O}_S^*) \to \Gamma(C_S, \mathcal{O}_{C_S}^*)$.

We denote by $\mathrm{Cot}(P_Y) = \mathrm{Cot}(GJ_Y)$ the cotangent space at the origin of P_Y or GJ_Y, and identify it with the space of translation invariant differential forms on P_Y or GJ_Y. We also identify it with the F-dual of the Lie algebra $\mathrm{Lie}(P_Y) = \mathrm{Lie}(GJ_Y)$. Let $F[\varepsilon]$ be the ring of dual numbers over F, and set $S[\varepsilon] := S \otimes_F F[\varepsilon]$ for an F-scheme S. Let $\mathcal{O}_{X[\varepsilon]}(1\,\mathrm{on}\,C[\varepsilon])^*$ be the subsheaf of $\mathcal{O}_{X[\varepsilon]}^*$ whose sections take value 1 on $C[\varepsilon]$, and define $\mathcal{O}_X(1\,\mathrm{on}\,C)^*$ in a similar manner. Then the exact sequence of sheaves on X:

$$0 \to \mathcal{O}_X(-C) \to \mathcal{O}_{X[\varepsilon]}(1\,\mathrm{on}\,C[\varepsilon])^* \to \mathcal{O}_X(1\,\mathrm{on}\,C)^* \to 0, \tag{3.1.8}$$

yields the canonical isomorphism

$$H^1(X, \mathcal{O}_X(-C)) \cong \mathrm{Ker}(P_Y(F[\varepsilon]) \to P_Y(F)) = \mathrm{Lie}(P_Y). \tag{3.1.9}$$

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

With these notations, we have the following important compatibility (Deligne [D] 2.3; one can prove this in a similar manner as Mazur [M] §2 e)): The diagram

$$\begin{array}{ccc} \mathrm{Lie}(P_Y)^\vee & \xrightarrow{\iota_Y^*} & H^0(Y, \Omega^1_{Y/F}) \\ \downarrow \wr & & \uparrow \mathrm{can} \\ H^1(X, \mathcal{O}_X(-C))^\vee & \xrightarrow[\mathrm{Serre}]{\sim} & H^0(X, \Omega^1_{X/F}(C)), \end{array} \tag{3.1.10}$$

commutes, where the superscript '$\vee$' means the F-dual, and the bottom horizontal arrow comes from the Serre duality. (It is Proposition 5 of [Se] V n°10 that the image of ι_Y^* is $H^0(X, \Omega^1_{X/F}(C))$.)

Next assume that all the points of C are F-rational. Let $C = \{c_1, \ldots, c_k\}$ and let $i_j : \mathrm{Spec}(F) \to X$ correspond to c_j. Then the exact sequence

$$0 \to \mathcal{O}_X(-C) \to \mathcal{O}_X \to \oplus_{j=1}^k i_{j*}(F) \to 0, \tag{3.1.11}$$

obtained by 'evaluation at c_j' gives the exact sequence

$$0 \to F \xrightarrow{\mathrm{diag}} \oplus_{c_j \in C} F \to H^1(X, \mathcal{O}_X(-C)) \to H^1(X, \mathcal{O}_X) \to 0. \tag{3.1.12}$$

On the other hand, $R_{C/F}(\mathbf{G}_m)$ is the product of k copies of $\mathbf{G}_m$, which are indexed by C in this case.

LEMMA (3.1.13). (i) *The notation being as above, the following diagram commutes:*

$$\begin{array}{ccccccccccc} 0 & \to & F & \xrightarrow{\mathrm{diag}} & \oplus_{c_j \in C} F & \to & H^1(X, \mathcal{O}_X(-C)) & \to & H^1(X, \mathcal{O}_X) & \to & 0 \\ & & \downarrow & & \downarrow & & (3.1.9) \downarrow \wr & & \downarrow \wr & & \\ 0 & \to & \mathrm{Lie}(\mathbf{G}_m) & \to & \prod_{c_j \in C} \mathrm{Lie}(\mathbf{G}_m) & \to & \mathrm{Lie}(P_Y) & \to & \mathrm{Lie}(P_X) & \to & 0, \end{array}$$

if we define the left two isomorphisms in a natural manner ($F \ni 1$ is sent to $1 + \varepsilon \in \mathrm{Ker}(\mathbf{G}_m(F[\varepsilon]) \to \mathbf{G}_m(F))$, which corresponds to $X d/dX$ if $\mathbf{G}_m = \mathrm{Spec}(F[X, X^{-1}])$). Here, the bottom horizontal sequence is obtained from (3.1.5).

(ii) *The F-dual of the sequence* (3.1.12) *is identified with*

$$0 \to H^0(X, \Omega^1_{X/F}) \to H^0(X, \Omega^1_{X/F}(C)) \xrightarrow{\oplus_j \mathrm{Res}_{c_j}} \oplus_{c_j \in C} F \xrightarrow{\mathrm{sum}} F \to 0$$

via the Serre duality, the middle arrow being the mapping 'taking residues at c_j'.

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

Proof. As for the first assertion, it is enough to show the commutativity of the middle square. Thus take and fix $(a_j)_{1\leqslant j\leqslant k} \in \oplus_{c_j\in C} F = H^0(X, \oplus_{j=1}^{k} i_{j*}(F))$. Its image in $H^1(X, \mathcal{O}_X(-C))$ is the class of the $\mathcal{O}_X(-C)$-torsor consisting of local sections of $\mathcal{O}_X$ whose values at c_j are a_j. Take an open affine covering $\{U_i\}$ of X so that this torsor admits a section p_i on each U_i. Then the image of the above class in $H^1(X, \mathcal{O}_{X[\varepsilon]}(1 \text{ on } C[\varepsilon])^*)$ is represented by the Čech 1-cocycle $\{1+(p_j\,|_{U_i\cap U_j} - p_i\,|_{U_i\cap U_j})\varepsilon \in \Gamma(U_i\cap U_j, \mathcal{O}_{X[\varepsilon]}(1 \text{ on } C[\varepsilon])^*)\}$. On the other hand, if we start with $(a_j)_{1\leqslant j\leqslant k}$ and go anticlockwise, then we get $(\mathcal{L}, \alpha) \in P_Y(F[\varepsilon])$ with $\mathcal{L} = \mathcal{O}_{X[\varepsilon]}$ and α given by multiplication by $(1 + a_j\varepsilon)_{1\leqslant j\leqslant k}$. It is easy to see that this corresponds to the above cohomology class, which proves the first assertion. The second assertion follows from the explicit description of the Serre duality ([Se] II n°8). □

3.2. FUNCTORIALITY OF GENERALIZED JACOBIANS

Let Y_1 and Y_2 be smooth and geometrically irreducible curves over F and let X_i and C_i have the same meaning as in 3.1 for Y_i ($i = 1, 2$). We assume that we are given an F-morphism

$$f : X_1 \to X_2 \text{ such that } f^{-1}(C_2) = C_1 \text{ (set theoretically)}. \tag{3.2.1}$$

Its restriction to Y_1 will be also denoted by f.

For an isomorphism class of $(\mathcal{L}, \alpha)$ in $P_{Y_2}(S)$, we can naturally attach its pull-back $(f_S^*(\mathcal{L}), (f_S|_{C_{1,S}})^*(\alpha))$. This correspondence yields homomorphisms of F-group schemes

$$f^* : \begin{cases} P_{Y_2} \to P_{Y_1}, \\ GJ_{Y_2} \to GJ_{Y_1}. \end{cases} \tag{3.2.2}$$

Also, from the 'Albanese type' universality referred to in 3.1, we see that there are unique F-homomorphisms

$$f_* : \begin{cases} P_{Y_1} \to P_{Y_2}, \\ GJ_{Y_1} \to GJ_{Y_2}, \end{cases} \tag{3.2.3}$$

such that the following diagram commutes:

$$\begin{array}{ccc} Y_1 & \xrightarrow{\iota_{Y_1}} & P_{Y_1} \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f_*} \\ Y_2 & \xrightarrow[\iota_{Y_2}]{} & P_{Y_2}. \end{array} \tag{3.2.4}$$

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

From this, we clearly have the commutative diagram

$$
\begin{array}{ccc}
H^0(X_1, \Omega^1_{X_1/F}(C_1)) & \xleftarrow{\sim} & \mathrm{Cot}(P_{Y_1}) \\
{\scriptstyle f^*}\uparrow & & \uparrow{\scriptstyle \mathrm{Cot}(f_*)} \\
H^0(X_2, \Omega^1_{X_2/F}(C_2)) & \xleftarrow[\sim]{} & \mathrm{Cot}(P_{Y_2}),
\end{array}
\tag{3.2.5}
$$

where the vertical arrows are obtained by pulling back differentials.

As for (3.2.2), we have the following commutative diagram:

$$
\begin{array}{ccc}
H^0(X_1, \Omega^1_{X_1/F}(C_1)) & \xleftarrow{\sim} & \mathrm{Cot}(P_{Y_1}) \\
{\scriptstyle \mathrm{trace}}\downarrow & & \downarrow{\scriptstyle \mathrm{Cot}(f^*)} \\
H^0(X_2, \Omega^1_{X_2/F}(C_2)) & \xleftarrow[\sim]{} & \mathrm{Cot}(P_{Y_2}).
\end{array}
\tag{3.2.6}
$$

In fact, the compatibility (3.1.10) easily reduces this to the commutativity of the diagram below when F is algebraically closed:

$$
\begin{array}{ccc}
H^0(X_1, \Omega^1_{X_1/F}(C_1))^\vee & \xrightarrow[\mathrm{Serre}]{\sim} & H^1(X_1, \mathcal{O}_{X_1}(-C_1)) \\
{\scriptstyle (\mathrm{trace})^\vee}\uparrow & & \uparrow{\scriptstyle \mathrm{can}} \\
H^0(X_2, \Omega^1_{X_2/F}(C_2))^\vee & \xrightarrow[\sim]{\mathrm{Serre}} & H^1(X_2, \mathcal{O}_{X_2}(-C_2)).
\end{array}
\tag{3.2.7}
$$

This amounts to the formula in Lemme 4 (cf. also remark 1) on the subsequent page) of [Se] II n°12, via the explicit description of the Serre duality.

Next, we look at the torus parts of the generalized Jacobians. For this, we assume that both C_1 and C_2 consist of F-rational points; and write $C_1 = \{c_1, \ldots, c_k\}$ and $C_2 = \{d_1, \ldots, d_l\}$. Then, from the definitions, we see that the following diagram commutes:

$$
\begin{array}{ccccccc}
\mathbf{G}_m & \longrightarrow & \prod_{c_i \in C_1} \mathbf{G}_m & \longrightarrow & GJ_{Y_1} & \longrightarrow & J_{X_1} \\
\| & & \uparrow & & \uparrow{\scriptstyle f^*} & & \uparrow{\scriptstyle f^*} \\
\mathbf{G}_m & \longrightarrow & \prod_{d_j \in C_2} \mathbf{G}_m & \longrightarrow & GJ_{Y_2} & \longrightarrow & J_{X_2},
\end{array}
\tag{3.2.8}
$$

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

where the horizontal arrows come from (3.1.5), and the middle left morphism is given by: $\mathbf{G}_m \xrightarrow{\text{diag}} \prod_{c_i \in f^{-1}(d_j)} \mathbf{G}_m$ on the jth factor of $\prod_{d_j \in C_2} \mathbf{G}_m$. Also, we have the following commutative diagram:

$$\begin{array}{ccccccc} \mathbf{G}_m & \longrightarrow & \prod_{c_i \in C_1} \mathbf{G}_m & \longrightarrow & GJ_{Y_1} & \longrightarrow & J_{X_1} \\ \Big\downarrow{\scriptstyle \deg(f)} & & \Big\downarrow & & \Big\downarrow{\scriptstyle f^*} & & \Big\downarrow{\scriptstyle f^*} \\ \mathbf{G}_m & \longrightarrow & \prod_{d_j \in C_2} \mathbf{G}_m & \longrightarrow & GJ_{Y_2} & \longrightarrow & J_{X_2}. \end{array} \tag{3.2.9}$$

Here, the left vertical morphism is $x \mapsto x^{\deg(f)}$. The middle left morphism sends $x \in \mathbf{G}_m(S)$ in the ith factor to $x^{e(c_i/d_j)}$ in the jth factor, if $f(c_i) = d_j$ and the ramification index of c_i over d_j is $e(c_i/d_j)$. To see this, we only need to check the commutativity of the middle square. Since we are in characteristic zero, it is enough to prove that the square obtained by taking 'Cot' is commutative. In view of (3.2.5) and (3.1.13), this reduces to the obvious commutativity:

$$\begin{array}{ccc} \oplus_{c_i \in C_1} F & \xleftarrow{\oplus_i \mathrm{Res}_{c_i}} & H^0(X_1, \Omega^1_{X_1/F}(C_1)) \\ \Big\uparrow & & \Big\uparrow{\scriptstyle f^*} \\ \oplus_{d_j \in C_2} F & \xleftarrow[\oplus_j \mathrm{Res}_{d_j}]{} & H^0(X_2, \Omega^1_{X_2/F}(C_2)) \end{array} \tag{3.2.10}$$

where the left arrow sends a in the jth factor to $\oplus_{c_i \in f^{-1}(d_j)} e(c_i/d_j)a$.

3.3. ÉTALE COHOMOLOGY GROUPS AND GENERALIZED JACOBIANS

In this subsection, all the cohomology groups will be the étale cohomology. Let X, Y and C be as in 3.1; and indicate by bar the base extension from F to its algebraic closure $\overline{F}$. Then the 'Kummer theory' provides us with the canonical isomorphism

$$H^1_c(\overline{Y}, \boldsymbol{\mu}_n) \cong {}_nGJ_Y(\overline{F}), \tag{3.3.1}$$

for any positive integer n, where the subscript '${}_n$' in the right-hand side means the kernel of multiplication by n ([SGA4] XVIII 1.6.4). This in turn gives us an isomorphism

$$H^1_c(\overline{Y}, \mathbf{Z}_p(1)) \cong T_p(GJ_Y), \tag{3.3.2}$$

T_p being the usual p-adic Tate module. Combining these with the Poincaré duality, we obtain the following canonical isomorphisms:

$$\begin{aligned} H^1(\overline{Y}, \mathbf{Z}/n\mathbf{Z}) &\cong \mathrm{Hom}({}_nGJ_Y(\overline{F}), \mathbf{Z}/n\mathbf{Z}), \\ H^1(\overline{Y}, \mathbf{Z}_p) &\cong \mathrm{Hom}(T_p(GJ_Y), \mathbf{Z}_p). \end{aligned} \tag{3.3.3}$$

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

Now we consider the situation as in 3.2. We then first see that the diagram:

$$\begin{array}{ccc} H^1(\overline{Y}_1, \mathbf{Z}_p) & \xrightarrow{\sim} & \mathrm{Hom}(T_p(GJ_{Y_1}), \mathbf{Z}_p) \\ {\scriptstyle \mathrm{Tr}_f}\downarrow & & \downarrow{\scriptstyle \mathrm{Hom}(f^*, \mathbf{Z}_p)} \\ H^1(\overline{Y}_2, \mathbf{Z}_p) & \xrightarrow[\sim]{} & \mathrm{Hom}(T_p(GJ_{Y_2}), \mathbf{Z}_p), \end{array} \tag{3.3.4}$$

commutes, where the left vertical arrow is the trace mapping with respect to f. This indeed follows from the well-known fact that the Poincaré dual of Tr_f is the canonical mapping: $H_c^1(\overline{Y}_2, \mathbf{Z}_p(1)) \to H_c^1(\overline{Y}_1, \mathbf{Z}_p(1))$. The commutativity of the following diagram seems less obvious to us:

$$\begin{array}{ccc} H^1(\overline{Y}_1, \mathbf{Z}_p) & \xrightarrow{\sim} & \mathrm{Hom}(T_p(GJ_{Y_1}), \mathbf{Z}_p) \\ {\scriptstyle \mathrm{can}}\uparrow & & \uparrow{\scriptstyle \mathrm{Hom}(f_*, \mathbf{Z}_p)} \\ H^1(\overline{Y}_2, \mathbf{Z}_p) & \xrightarrow[\sim]{} & \mathrm{Hom}(T_p(GJ_{Y_2}), \mathbf{Z}_p). \end{array} \tag{3.3.5}$$

For this, we show the commutativity of the diagram

$$\begin{array}{ccc} H^1(\overline{Y}_1, \mathbf{Z}/n\mathbf{Z}) & \xrightarrow{\sim} & \mathrm{Hom}({}_nGJ_{Y_1}(\overline{F}), \mathbf{Z}/n\mathbf{Z}) \\ {\scriptstyle \mathrm{can}}\uparrow & & \uparrow{\scriptstyle \mathrm{Hom}(f_*, \mathbf{Z}/n\mathbf{Z})} \\ H^1(\overline{Y}_2, \mathbf{Z}/n\mathbf{Z}) & \xrightarrow[\sim]{} & \mathrm{Hom}({}_nGJ_{Y_2}(\overline{F}), \mathbf{Z}/n\mathbf{Z}) \end{array} \tag{3.3.6}$$

for any positive integer n. We may assume that $F = \overline{F}$ and, hence, drop the bar for the simplicity of the notation in the following. We fix an F-rational point x_1 of Y_1 and put $x_2 := f(x_1)$, so that the diagram

$$\begin{array}{ccc} Y_1 & \xrightarrow{\iota_{Y_1, x_1}} & GJ_{Y_1} \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f_*} \\ Y_2 & \xrightarrow[\iota_{Y_2, x_2}]{} & GJ_{Y_2} \end{array} \tag{3.3.7}$$

commutes. Consider the exact sequence

$$0 \to {}_nGJ_{Y_i} \to GJ_{Y_i} \xrightarrow{n} GJ_{Y_i} \to 0 \tag{3.3.8}$$

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

of commutative group schemes over F for $i = 1$ or 2. We can then view (the middle) GJ_{Y_i} as an ${}_nGJ_{Y_i}$-torsor on (the right) GJ_{Y_i}, which determines a cohomology class in $H^1(GJ_{Y_i}, {}_nGJ_{Y_i})$. (Note that ${}_nGJ_{Y_i}$ is a constant group scheme under our assumption.) Now take $u \in \mathrm{Hom}({}_nGJ_{Y_i}(F), \mathbf{Z}/n\mathbf{Z})$. Changing the structural group by u, we obtain a $\mathbf{Z}/n\mathbf{Z}$-torsor $GJ_{Y_i} \overset{{}_nGJ_{Y_i}}{\wedge} \mathbf{Z}/n\mathbf{Z}$ (the contracted product via u) on GJ_{Y_i}; and then taking its inverse image under ι_{Y_i,x_i}, we get a cohomology class in $H^1(Y_i, \mathbf{Z}/n\mathbf{Z})$. In this way, we obtain a mapping

$$\varphi_i : \mathrm{Hom}({}_nGJ_{Y_i}(F), \mathbf{Z}/n\mathbf{Z}) \to H^1(Y_i, \mathbf{Z}/n\mathbf{Z}). \tag{3.3.9}$$

It is then known that $-\varphi_i$ is inverse to one of the horizontal mappings in (3.3.6) ([SGA4$^{1/2}$] Arcata VI (2.3.3)). Therefore, starting with $u \in \mathrm{Hom}({}_nGJ_{Y_2}(F), \mathbf{Z}/n\mathbf{Z})$, it is enough to show that the two $\mathbf{Z}/n\mathbf{Z}$-torsors on

$$GJ_{Y_1}\colon (f_*)^*(GJ_{Y_2} \overset{{}_nGJ_{Y_2}}{\wedge} \mathbf{Z}/n\mathbf{Z})$$
$$\cong (f_*)^* GJ_{Y_2} \overset{{}_nGJ_{Y_2}}{\wedge} \mathbf{Z}/n\mathbf{Z} \quad \text{and} \quad GJ_{Y_1} \overset{{}_nGJ_{Y_1}}{\wedge} \mathbf{Z}/n\mathbf{Z}$$

are isomorphic; the latter being defined by ${}_nGJ_{Y_1}(F) \xrightarrow{f_*} {}_nGJ_{Y_2}(F) \xrightarrow{u} \mathbf{Z}/n\mathbf{Z}$. But we have the following obvious commutative diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & {}_nGJ_{Y_1} & \longrightarrow & GJ_{Y_1} & \xrightarrow{n} & GJ_{Y_1} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f_*} & & \downarrow{\scriptstyle f_*} & & \downarrow{\scriptstyle f_*} & & \\
0 & \longrightarrow & {}_nGJ_{Y_2} & \longrightarrow & GJ_{Y_2} & \xrightarrow[n]{} & GJ_{Y_2} & \longrightarrow & 0.
\end{array} \tag{3.3.10}$$

Since the multiplication by n on GJ_{Y_2} is étale, $(f_*)^*GJ_{Y_2}$ is represented by the fibre product $GJ_{Y_2} \times_{GJ_{Y_2}} GJ_{Y_1}$ obtained from the right square above. We thus have a morphism: $GJ_{Y_1} \to (f_*)^*GJ_{Y_2}$ over GJ_{Y_1}, which commutes with the action of ${}_nGJ_{Y_1}$ and ${}_nGJ_{Y_2}$ via f_*. We conclude that there is a morphism of $\mathbf{Z}/n\mathbf{Z}$-torsors: $GJ_{Y_1} \overset{{}_nGJ_{Y_1}}{\wedge} \mathbf{Z}/n\mathbf{Z} \to (f_*)^*GJ_{Y_2} \overset{{}_nGJ_{Y_2}}{\wedge} \mathbf{Z}/n\mathbf{Z}$, which is automatically an isomorphism. This completes the proof of the commutativity of (3.3.6) and (3.3.5).

3.4. MODULAR GENERALIZED JACOBIANS AND HECKE OPERATORS

Suppose that we are given a congruence subgroup Γ of $\mathrm{SL}_2(\mathbf{Z})$ and an $\alpha \in \mathrm{GL}_2(\mathbf{Q})$ with positive determinant. If we set $\Gamma' := \Gamma \cap \alpha^{-1}\Gamma\alpha$, then we have the following morphisms of Riemann surfaces:

$$\Gamma\backslash H \xleftarrow{\mathrm{can}} \Gamma'\backslash H \xrightarrow{\alpha} \Gamma\backslash H, \tag{3.4.1}$$

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

where the left (resp. the right) arrow is the natural projection (resp. given by $z \bmod \Gamma' \mapsto \alpha(z) \bmod \Gamma$). Assume that we are given a model of this situation

$$Y \xleftarrow{p} Y' \xrightarrow{q} Y, \tag{3.4.2}$$

all defined over a subfield F of **C**. This extends to a diagram between smooth compactifications over F

$$X \xleftarrow{p} X' \xrightarrow{q} X. \tag{3.4.3}$$

As before, we set $C := X - Y$ and $C' := X' - Y'$. Then using (3.2.2) and (3.2.3), we can define endomorphisms of GJ_Y over F in two ways:

$$T := q_* \circ p^*, \qquad T^* := p_* \circ q^*. \tag{3.4.4}$$

Now we have canonical isomorphisms:

$$\mathrm{Cot}(GJ_Y) \otimes_F \mathbf{C} \underset{(3.1.10)}{\cong} H^0(X, \Omega^1_{X/F}(C)) \otimes_F \mathbf{C} \cong M_2(\Gamma), \tag{3.4.5}$$

the latter being the usual one: $f\,dq/q \leftrightarrow f$. Let

$$\Gamma\alpha\Gamma = \coprod_i \Gamma\beta_i = \coprod_j \gamma_j\Gamma, \tag{3.4.6}$$

be disjoint. Then, from the commutativity of (3.2.5) and (3.2.6), one easily derives the following:

LEMMA (3.4.7). *Via* (3.4.5), *the endomorphism* $\mathrm{Cot}(T)$ *(resp.* $\mathrm{Cot}(T^*)$*) corresponds to the usual operator* '$\mid [\Gamma\alpha\Gamma]$' *(resp.* '$\mid [\Gamma\alpha\Gamma]^*$'*) on* $M_2(\Gamma)$*; that is,*

$$f \mid [\Gamma\alpha\Gamma] = \sum_i f \mid \beta_i, \qquad f \mid [\Gamma\alpha\Gamma]^* = \sum_j f \mid \gamma_j^{-1}.$$

EXAMPLE (3.4.8). We assume that Γ is $\Gamma_1(M)$ and that Y is the canonical model of $\Gamma\backslash H$ over **Q**.

(i) Let $\alpha := \begin{bmatrix} 1 & 0 \\ 0 & l \end{bmatrix}$ with a prime number l. Then we can take F to be **Q**, and obtain endomorphisms of GJ_Y defined over **Q** by (3.4.4). They will be denoted by $T(l)$ and $T^*(l)$, respectively.

(ii) Let q be a positive integer prime to M. If we take α to be an element of $\mathrm{SL}_2(\mathbf{Z})$ congruent to $\begin{bmatrix} q^{-1} & * \\ 0 & q \end{bmatrix}$ mod $M \cdot M_2(\mathbf{Z})$, we again obtain **Q**-endomorphisms of GJ_Y, which will be denoted by $T(q,q)$ and $T^*(q,q)$, respectively.

(iii) Let $\alpha = \begin{bmatrix} 0 & -1 \\ M & 0 \end{bmatrix} =: \tau$. In this case, we get an involution of GJ_Y defined over $\mathbf{Q}(e^{2\pi i/M})$.

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

By (3.4.7), the endomorphisms in (i) and (ii) above induce the operators of the same name on $\mathrm{Cot}(GJ_Y) \otimes_{\mathbf{Q}} \mathbf{C} \cong M_2(\Gamma)$. Thus the subalgebra of $\mathrm{End}_{\mathbf{Q}}(GJ_Y)$ generated by all $T(l)$ and $T(q,q)$ (resp. $T^*(l)$ and $T^*(q,q)$) is canonically isomorphic to the Hecke algebra over $\mathbf{Z}$ attached to $M_2(\Gamma)$ of the same sort. By (3.3.4) and (3.3.5), the isomorphisms in (3.3.3) are also compatible with $T(l)$ and $T^*(l)$ etc. Similarly, the automorphism defined in (iii) corresponds to '$|\ \tau$' on $M_2(\Gamma)$. Conjugation by this involution interchanges $T(l)$ and $T^*(l)$; and also $T(q,q)$ and $T^*(q,q)$ (cf. (1.5.4)).

Finally, we wish to write down the effect of the endomorphisms T and T^* above on the torus part T_Y (3.1.6) of GJ_Y. This is equivalent to describe the induced endomorphisms of the Tate module $T_p(T_Y)$. However, for later use via (3.3.3), it is rather convenient to describe the adjoint action on the dual group. To do this, let us denote by $\mathbf{Z}_p[C]$ the free $\mathbf{Z}_p$-module generated by the elements of $C(\overline{\mathbf{Q}})$, the latter being identified with $\Gamma\backslash\mathbf{P}^1(\mathbf{Q})$. It is clear from (3.1.7) that we have an exact sequence

$$0 \to \mathbf{Z}_p(1) \xrightarrow{\text{diag}} \mathbf{Z}_p[C](1) \to T_p(T_Y) \to 0. \tag{3.4.9}$$

The pairing

$$\mathbf{Z}_p[C] \times \mathbf{Z}_p[C] \to \mathbf{Z}_p; \left(\sum_{c\in C(\overline{\mathbf{Q}})} a_c\cdot c, \sum_{c\in C(\overline{\mathbf{Q}})} b_c\cdot c \right) := \sum_{c\in C(\overline{\mathbf{Q}})} a_c b_c \tag{3.4.10}$$

obviously gives a perfect duality of $\mathbf{Z}_p$-modules. In the following, we identify $\mathrm{Hom}(\mathbf{Z}_p[C], \mathbf{Z}_p)$ with $\mathbf{Z}_p[C]$ by this pairing. We therefore obtain from (3.4.9) the exact sequence:

$$0 \to \mathrm{Hom}(T_p(T_Y), \mathbf{Z}_p) \to \mathbf{Z}_p[C](-1) \xrightarrow{\text{sum}} \mathbf{Z}_p(-1) \to 0. \tag{3.4.11}$$

PROPOSITION (3.4.12). *The notation being as above, T_Y is stable under T and T^*; and* $\mathrm{Hom}(T, \mathbf{Z}_p)$ *and* $\mathrm{Hom}(T^*, \mathbf{Z}_p)$ *on* $\mathrm{Hom}(T_p(T_Y), \mathbf{Z}_p)$ *are induced from the $\mathbf{Z}_p$-linear endomorphisms of $\mathbf{Z}_p[C]$ determined by* (i) *and* (ii) *below via* (3.4.11), *respectively.*

(i) $\mathbf{Z}_p[C] \supset C(\overline{\mathbf{Q}}) \ni c \mapsto \sum_j \gamma_j^{-1} \cdot c$,
(ii) $\mathbf{Z}_p[C] \supset C(\overline{\mathbf{Q}}) \ni c \mapsto \sum_i \beta_i \cdot c$.

(Thus they look like T^* and T, respectively!)

Proof. We may fix an isomorphism: $\mathbf{Z}_p(1) \cong \mathbf{Z}_p$, and neglect the Tate twist to prove our proposition. Define a $\mathbf{Z}_p$-linear endomorphism t^* of $\mathbf{Z}_p[C]$ by

$$C(\overline{\mathbf{Q}}) \ni c \mapsto \sum_{d\in q^{-1}(c)} e(d/p(d)) \cdot p(d),$$

where the sum ranges over all $d \in C'(\overline{\mathbf{Q}})$ such that $q(d) = c$. Then by (3.2.8) and (3.2.9), it induces the action of T^* on $T_p(T_Y)$ via (3.4.9). If we define an endomorphism $t^\vee$ of $\mathbf{Z}_p[C]$ by $(t^*(c), c') = (c, t^\vee(c'))$, we have

$$t^\vee(c') = \sum_{d \in p^{-1}(c')} e(d/c') \cdot q(d).$$

A simple group theoretical argument shows that this coincides with the endomorphism given by (ii), which proves our assertion for T^*.

The proof of the assertion for T (which actually will not be used in what follows) is similar. □

4. The p-adic Hodge structure of $e^{*\prime}GES_p(N)_o$

4.1. GOOD QUOTIENTS OF MODULAR GENERALIZED JACOBIANS

We now return to the situation of 1.1. We set

$$C_r := X_r - Y_r \tag{4.1.1}$$

(the reduced cuspidal subscheme of X_r), and write

$$GJ_r := GJ_{Y_r}, \qquad J_r := J_{X_r}, \qquad T_r := T_{Y_r} \tag{4.1.2}$$

for the generalized Jacobian of X_r with the modulus C_r, the Jacobian of X_r, and the torus part of GJ_r, respectively. They are all defined over $\mathbf{Q}$. The purpose of this subsection is to construct certain quotient of GJ_r following Mazur and Wiles [MW1] and Tilouine [Ti].

Recall that $\Phi_r^{r-1} = \Gamma_{r-1} \cap \Gamma_0(p^r)$, and Y_r^{r-1} is the canonical model of $\Phi_r^{r-1}\backslash H$ over $\mathbf{Q}$ (1.2). We have natural morphisms

$$Y_r \xrightarrow{\pi_r} Y_r^{r-1} \xrightarrow{\rho_r} Y_{r-1}. \tag{4.1.3}$$

(Here, $\Phi_1^0 = \Gamma_1(N) \cap \Gamma_0(p)$ and $Y_0 = Y_1(N)$.) We define the quotient group schemes

$$\alpha_r : GJ_r \to Q_r, \tag{4.1.4}$$

inductively as follows: First we define

$$Q_1 := GJ_1/\pi_1^*(GJ_{Y_1^0}). \tag{4.1.5}$$

If we have already constructed α_{r-1}: $GJ_{r-1} \to Q_{r-1}$ ($r \geqslant 2$), we put

$$\begin{aligned} K_r &:= \mathrm{Ker}(\alpha_{r-1} \circ \rho_{r*} : GJ_{Y_r^{r-1}} \to Q_{r-1}), \\ Q_r &:= GJ_r/(\pi_r^*(K_r))^0. \end{aligned} \tag{4.1.6}$$

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

Note that we are taking quotients by *connected* subgroup schemes.

Recall also that we have canonical isomorphisms (3.4.5):

$$\mathrm{Cot}(GJ_r)\otimes_{\mathbf{Q}}\mathbf{C}\cong H^0(X_r,\Omega^1_{X_r/\mathbf{Q}}(C_r))\otimes_{\mathbf{Q}}\mathbf{C}\cong M_2(\Gamma_r). \tag{4.1.7}$$

PROPOSITION (4.1.8). *The notation being as above, the image of*

$$\mathrm{Cot}(\alpha_r):\mathrm{Cot}(Q_r)\otimes_{\mathbf{Q}}\mathbf{C}\hookrightarrow\mathrm{Cot}(GJ_r)\otimes_{\mathbf{Q}}\mathbf{C},$$

corresponds, via (4.1.7)*, to the following subspace of* $M_2(\Gamma_r)$*, for each* $r\geqslant 1$:

$$\oplus_{i=1}^{r}\oplus_{\varepsilon}\{f\in M_2(\Gamma_i)\mid f\mid\sigma_a=\varepsilon(a)f\ \text{ for all }\ a\in(\mathbf{Z}/N_i\mathbf{Z})^{\times}\}=:\mathcal{M}_r.$$

Here, the inner sum ranges over all the Dirichlet characters mod N_i *whose conductors are divisible by* p^i*, and* $\sigma_a\in\mathrm{SL}_2(\mathbf{Z})$ *is congruent to* $\begin{bmatrix}a^{-1}&*\\0&a\end{bmatrix}$ mod $N_i\cdot M_2(\mathbf{Z})$.

Proof. We proceed by induction on r. First note that the kernel of π_r^*: $GJ_{Y_r^{r-1}}\to GJ_r$ is finite. For $r=1$, we have a commutative diagram with exact horizontal lines:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Cot}(Q_1)_{\mathbf{C}} & \xrightarrow{\mathrm{Cot}(\alpha_1)} & \mathrm{Cot}(GJ_1)_{\mathbf{C}} & \xrightarrow{\mathrm{Cot}(\pi_1^*)} & \mathrm{Cot}(GJ_{Y_1^0})_{\mathbf{C}} & \longrightarrow & 0\\
 & & & & \downarrow\wr & & \downarrow\wr & & \\
 & & & & M_2(\Gamma_1) & \xrightarrow[\text{trace}]{} & M_2(\Phi_1^0) & \longrightarrow & 0,
\end{array}$$

by (3.2.6), where the subscript '$\mathbf{C}$' means '$\otimes_{\mathbf{Q}}\mathbf{C}$'. The trace mapping is given by $M_2(\Gamma_1)\ni f\mapsto\sum_a f\mid\sigma_a$ (resp. $2^{-1}\sum_a f\mid\sigma_a$) if $N\geqslant 3$ (resp. otherwise), the sum ranging over all $a\in(\mathbf{Z}/p\mathbf{Z})^{\times}\hookrightarrow(\mathbf{Z}/N_1\mathbf{Z})^{\times}$. Our assertion for $r=1$ therefore follows.

Next suppose that $r>1$. We have an exact sequence

$$0\longrightarrow\mathrm{Cot}(Q_r)\xrightarrow{\mathrm{Cot}(\alpha_r)}\mathrm{Cot}(GJ_r)\longrightarrow\mathrm{Cot}(K_r)\longrightarrow 0,$$

and also a commutative diagram

$$\begin{array}{ccccc}
\mathrm{Cot}(GJ_r)_{\mathbf{C}} & \xrightarrow{\mathrm{Cot}(\pi_r^*)} & \mathrm{Cot}(GJ_{Y_r^{r-1}})_{\mathbf{C}} & \xleftarrow{\mathrm{Cot}(\rho_{r*})} & \mathrm{Cot}(GJ_{r-1})_{\mathbf{C}}\\
\downarrow\wr & & \downarrow\wr & & \downarrow\wr\\
M_2(\Gamma_r) & \xrightarrow[\text{trace}]{} & M_2(\Phi_r^{r-1}) & \xleftarrow[\text{can}]{} & M_2(\Gamma_{r-1}),
\end{array}$$

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

by (3.2.5) and (3.2.6). But by the induction hypothesis, there is a commutative diagram with exact horizontal lines

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Cot}(Q_{r-1})_{\mathbf{C}} & \xrightarrow{\mathrm{Cot}(\alpha_{r-1}\circ\rho_{r*})} & \mathrm{Cot}(GJ_{Y_r^{r-1}})_{\mathbf{C}} & \longrightarrow & \mathrm{Cot}(K_r)_{\mathbf{C}} & \longrightarrow & 0 \\ & & \downarrow \wr & & \downarrow \wr & & & & \\ 0 & \longrightarrow & \mathcal{M}_{r-1} & \xrightarrow[\text{can}]{} & M_2(\Phi_r^{r-1}). & & & & \end{array}$$

Combining these, we conclude that $f \in M_2(\Gamma_r) \cong \mathrm{Cot}(GJ_r)_{\mathbf{C}}$ lies in the image of $\mathrm{Cot}(Q_r)_{\mathbf{C}}$ if and only if its trace to $M_2(\Phi_r^{r-1})$ belongs to $\mathcal{M}_{r-1}$. Our result follows easily from this. □

COROLLARY (4.1.9). Ker$(\alpha_r) = (\pi_r^*(K_r))^0$ *is stable under all* $T(l)$ *and* $T(q,q)$ (cf. (3.4.8) for these endomorphisms of GJ_r).

Proof. It is enough to prove that Lie(Ker(α_r)) is stable under such operators. By (4.1.8) and the remark after (3.4.8), we are reduced to show that $\mathcal{M}_r$ is stable under the Hecke operators $T(l)$ and $T(q,q)$, which is clear. □

It follows that the action of the Hecke algebra $\mathcal{H}_2(\Gamma_r; \mathbf{Z})$ on GJ_r (cf. the remark after (3.4.8)) induces a homomorphism: $\mathcal{H}_2(\Gamma_r; \mathbf{Z}) \to \mathrm{End}_{\mathbf{Q}}(Q_r)$ for each $r \geqslant 1$.

Let B_r be the 'good quotient' of J_r defined in a same manner as above ([Ti] Section 2). Here, as before, we assume that the kernel of the quotient homomorphism: $J_r \to B_r$ is connected. Then, from the construction, it is easy to see that there is a unique **Q**-homomorphism: $Q_r \to B_r$ making the following square commutative:

$$\begin{array}{ccc} GJ_r & \xrightarrow{\alpha_r} & Q_r \\ \downarrow & & \downarrow \\ J_r & \longrightarrow & B_r. \end{array} \tag{4.1.10}$$

It is also easy to see that the kernel of this homomorphism is a quotient of T_r and, hence, it is a torus.

4.2. p-DIVISIBLE GROUPS ATTACHED TO MODULAR GENERALIZED JACOBIANS

We have seen in 1.5 that $e\mathcal{H}(N; \mathfrak{o})$ and $e^*\mathcal{H}^*(N; \mathfrak{o})$ are naturally equipped with the structure of $\mathfrak{o}[[\mathcal{Z}_N]]$-algebras (cf. (1.5.6) and (1.5.7)). Especially, we can decompose them as:

$$\begin{aligned} e\mathcal{H}(N; \mathfrak{o}) &= \oplus_{i \bmod p-1}\, e\mathcal{H}(N; \mathfrak{o})^{(i)}, \\ e^*\mathcal{H}^*(N; \mathfrak{o}) &= \oplus_{i \bmod p-1}\, e^*\mathcal{H}^*(N; \mathfrak{o})^{(i)}, \end{aligned} \tag{4.2.1}$$

where the superscript '$^{(i)}$' means the ω^i-eigenspace with respect to the action of $(\mathbf{Z}/p\mathbf{Z})^\times \subset \mathcal{Z}_N$.

DEFINITION (4.2.2). As in [O2], we denote by e' (resp. $e^{*\prime}$) the idempotent of $e\mathcal{H}(N;\mathfrak{o})$ (resp. $e^*\mathcal{H}^*(N;\mathfrak{o})$) corresponding to the projector to $\oplus_{i\not\equiv 0,-1} e\mathcal{H}(N;\mathfrak{o})^{(i)}$ (resp. $\oplus_{i\not\equiv 0,-1} e^*\mathcal{H}^*(N;\mathfrak{o})^{(i)}$). We use the same symbol to denote its homomorphic image to other algebras (e.g. $e\mathcal{H}_k(\Gamma_r;\mathfrak{o})$ (resp. $e^*\mathcal{H}_k^*(\Gamma_r;\mathfrak{o})$) via (1.5.7) (iii)).

See [O2] (3.2.7) for the reason why we have to exclude the ω^0- and the ω^{-1}-eigenspaces. (Actually, the argument of this subsection works without excluding the ω^{-1}-eigenspace.)

In general, if G is a group scheme over a scheme S which is an extension of an abelian scheme by a torus, then the kernels of multiplication by p^n: $({}_{p^n}G)$ form a p-divisible group over S. We denote this p-divisible group by $G(p)$.

PROPOSITION (4.2.3). *The quotient homomorphism α_r induces an isomorphism of p-divisible groups over* $\mathbf{Q}$: $e'\cdot GJ_r(p) \xrightarrow{\sim} e'\cdot Q_r(p)$.

Proof. Write L_r (resp. L'_r) for the kernel of $GJ_r \to Q_r$ (resp. $J_r \to B_r$); and let L''_r be the kernel of the natural surjective homomorphism: $L_r \to L'_r$. Then we know that $e'\cdot {}_{p^n}L'_r(\overline{\mathbf{Q}}) = \{0\}$ ([Ti]; cf. also [O2] 3.2). It follows that we have an isomorphism: $e'\cdot {}_{p^n}L''_r(\overline{\mathbf{Q}}) \xrightarrow{\sim} e'\cdot {}_{p^n}L_r(\overline{\mathbf{Q}})$ for each $n \geqslant 1$. To prove that $e'\cdot L_r(p)$ is trivial, it is enough to show that $T(p)$ has no unit eigenvalue on $T_p(L''_r)^{(i)} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ when $i \not\equiv 0 \bmod p-1$. But since L''_r is isomorphic to a subgroup scheme of the torus T_r, this is equivalent to saying that the same holds for $(\mathrm{Lie}(L''_r) \otimes_{\mathbf{Q}} \mathbf{Q}_p)^{(i)}$. Thus, we need to show that, for $i \not\equiv 0 \bmod p-1$, $T(p)$ has no (p-adic) unit eigenvalue on $(\mathrm{Cot}(L''_r) \otimes_{\mathbf{Q}} \mathbf{C})^{(i)}$, which is isomorphic to a quotient of $(M_2(\Gamma_r)/\mathcal{M}_r)^{(i)}$ by (4.1.8). This is a consequence of Hida [H1] Proposition 4.1. □

Next, let us denote by w_r the automorphism of GJ_r induced by $\tau_r = \begin{bmatrix} 0 & -1 \\ N_r & 0 \end{bmatrix}$ (3.4.8). It is defined over $\mathbf{Q}(\zeta_{N_r})$, where ζ_{N_r} is a primitive N_rth root of unity. If $\sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta_{N_r})/\mathbf{Q})$ and $\zeta_{N_r}^\sigma = \zeta_{N_r}^a$ with a positive integer a, then we have

$$w_r^\sigma = w_r \circ T(a,a) = T^*(a,a) \circ w_r. \tag{4.2.4}$$

We define

$$Q_r^* := GJ_r/w_r(\mathrm{Ker}(\alpha_r)). \tag{4.2.5}$$

From the above relation, we see that $w_r(\mathrm{Ker}(\alpha_r))$ is $\mathbf{Q}$-rational; and hence Q_r^* is defined over $\mathbf{Q}$. We also see that there is a natural homomorphism: $\mathcal{H}_2^*(\Gamma_r;\mathbf{Z}) \to \mathrm{End}_{\mathbf{Q}}(Q_r^*)$. We thus obtain the following obvious corollary:

COROLLARY (4.2.6). *The quotient homomorphism induces an isomorphism of p-divisible groups over* $\mathbf{Q}$: $e^{*\prime}\cdot GJ_r(p) \xrightarrow{\sim} e^{*\prime}\cdot Q_r^*(p)$.

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

Let B_r^* be the quotient of J_r defined in a similar manner as (4.2.5). We then have an exact sequence of commutative group schemes over $\mathbf{Q}$ in which we define N_r:

$$0 \to N_r \to Q_r^* \to B_r^* \to 0. \tag{4.2.7}$$

It is well-known that B_r^* has good reduction over $\mathbf{Q}(\zeta_{p^r})$ at the prime above p. On the other hand, by (3.1.7), T_r splits over $\mathbf{Q}_p(\zeta_{N_r})$, an unramified extension of $\mathbf{Q}_p(\zeta_{p^r})$; and hence so is N_r. Let us now denote by $Q^*_{r/\mathbf{Z}_p[\zeta_{p^r}]}$ the 'Néron lft-model' of Q_r^* over $\mathbf{Z}_p[\zeta_{p^r}]$ ([BLR] 10.1); and similarly for N_r and B_r^*. They exist by [BLR] 10.2 Theorem 2. Since the formation of Néron lft-models commutes with étale base changes, $N^0_{r/\mathbf{Z}_p[\zeta_{p^r}]}$ is a torus which splits over $\mathbf{Z}_p[\zeta_{N_r}]$, by [BLR] 10.1 Example 5. It then follows from the argument of the proof of [BLR] 10.1 Proposition 7 that (4.2.7) extends to an exact sequence of commutative group schemes over $\mathbf{Z}_p[\zeta_{p^r}]$:

$$0 \longrightarrow N^0_{r/\mathbf{Z}_p[\zeta_{p^r}]} \longrightarrow Q^{*0}_{r/\mathbf{Z}_p[\zeta_{p^r}]} \longrightarrow B^*_{r/\mathbf{Z}_p[\zeta_{p^r}]} \longrightarrow 0. \tag{4.2.8}$$

The Hecke algebra $\mathcal{H}_2^*(\Gamma_r;\mathbf{Z})$ acts on these group schemes compatibly; and we can make the following

DEFINITION (4.2.9). We define the p-divisible groups over $\mathbf{Z}_p[\zeta_{p^r}]$ by

$$H_r := e^{*\prime} \cdot N^0_{r/\mathbf{Z}_p[\zeta_{p^r}]}(p),$$
$$\widetilde{G}_r := e^{*\prime} \cdot Q^{*0}_{r/\mathbf{Z}_p[\zeta_{p^r}]}(p), \qquad G_r := e^{*\prime} \cdot B^*_{r/\mathbf{Z}_p[\zeta_{p^r}]}(p),$$

so that we have an exact sequence of p-divisible groups over $\mathbf{Z}_p[\zeta_{p^r}]$

$$0 \longrightarrow H_r \longrightarrow \widetilde{G}_r \longrightarrow G_r \longrightarrow 0.$$

4.3. ORDINARY CUSPIDAL GROUPS

As before, we identify $C_r(\overline{\mathbf{Q}})$ with $\Gamma_r\backslash\mathbf{P}^1(\mathbf{Q})$. The correspondence: $\mathrm{SL}_2(\mathbf{Z}) \ni \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \mapsto a/c \in \mathbf{P}^1(\mathbf{Q})$ gives a bijection:

$$\Gamma_r\backslash\,\mathrm{SL}_2(\mathbf{Z})/U_\infty \xrightarrow{\sim} \Gamma_r\backslash\mathbf{P}^1(\mathbf{Q}), \tag{4.3.1}$$

where $U_\infty = \{\pm\left[\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbf{Z})\}$ is the stabilizer subgroup of the cusp $i\infty$. For a positive integer M, we put

$$A_M := \left\{ \begin{bmatrix} x \\ y \end{bmatrix} \in (\mathbf{Z}/M\mathbf{Z})^{\oplus 2} \mid (x,y) = 1 \text{ in } \mathbf{Z}/M\mathbf{Z} \right\} / \sim \tag{4.3.2}$$

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

where $\left[\begin{smallmatrix} x \\ y \end{smallmatrix}\right] \sim \left[\begin{smallmatrix} x' \\ y' \end{smallmatrix}\right]$ if and only if $y = y'$ and $x \equiv x' \bmod y(\mathbf{Z}/M\mathbf{Z})$. Then it is well known that there are bijections:

$$\Gamma_r \backslash \mathrm{SL}_2(\mathbf{Z})/U_\infty \xrightarrow{\sim} A_{N_r}/\{\pm 1\} \xrightarrow{\sim} (A_N \times A_{p^r})/\{\pm 1\}. \tag{4.3.3}$$

Here, the first arrow sends $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ to the class of $\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right]$ mod N_r, and the second one is induced from the natural mapping:

$$\begin{bmatrix} x \\ y \end{bmatrix} \mapsto \left(\begin{bmatrix} x \\ y \end{bmatrix} \bmod N, \begin{bmatrix} x \\ y \end{bmatrix} \bmod p^r \right).$$

The image of $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbf{Z})$ in the middle (resp. the right) set will be denoted by $\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right]_{N_r}$ $\left(\text{resp.} \left(\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right]_N, \left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right]_{p^r}\right)\right)$. We henceforth identify $C_r(\overline{\mathbf{Q}})$ with the sets in (4.3.3).

There is a natural action of the operator $T(p)^n$ on $\mathbf{Z}_p[C_r]$. Namely, it sends the class of $x \in \mathbf{P}^1(\mathbf{Q})$ to the formal sum of the classes of $(x+i)/p^n \in \mathbf{P}^1(\mathbf{Q})$ for $i = 0, \ldots, p^n - 1$. In view of (3.4.12) (cf. also (4.3.6) below), we denote by e^* the idempotent attached to this $T(p)$ acting on $\mathbf{Z}_p[C_r]$.

PROPOSITION (4.3.4). *Let D_r be the submodule of $\mathbf{Z}_p[C_r]$ generated by all $\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right]_{N_r}$ such that $p \mid c$. Then D_r is stable under $T(p)$, and $e^* D_r = \{0\}$. Moreover, we have an isomorphism $e^*\mathbf{Z}_p[C_r] \xrightarrow{\sim} \mathbf{Z}_p[C_r]/D_r$.*

Proof. Take $\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right]_{N_r} \in A_{N_r}/\{\pm 1\}$ with $p \mid c$. Then since $p \nmid a$, we see that

$$T(p)^n \begin{bmatrix} a \\ c \end{bmatrix}_{N_r} = \sum_{i=0}^{p^n-1} \begin{bmatrix} a + ic \\ p^n c \end{bmatrix}_{N_r}.$$

This shows that D_r is stable under $T(p)$. If $n \geqslant r$ and $p^n \equiv 1 \bmod N$, we have

$$\begin{bmatrix} a + ic \\ p^n c \end{bmatrix}_{N_r} = \left(\begin{bmatrix} a \\ c \end{bmatrix}_N, \begin{bmatrix} a + ic \\ 0 \end{bmatrix}_{p^r} \right).$$

It then follows that

$$T(p)^n \begin{bmatrix} a \\ c \end{bmatrix}_{N_r} = p^{n-r} \sum_{i=0}^{p^r-1} \left(\begin{bmatrix} a \\ c \end{bmatrix}_N, \begin{bmatrix} a + ic \\ 0 \end{bmatrix}_{p^r} \right)$$

and, hence, $e^* = \lim\limits_{k \to \infty} T(p)^{k!}$ annihilates D_r.

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

On the other hand, $\mathbf{Z}_p[C_r]/D_r$ is generated by $\begin{bmatrix} a \\ c \end{bmatrix}_{N_r}$ with $p \nmid c$. Take and fix an n such that $p^n \equiv 1 \bmod N$. We may change a and assume that a is divisible by p^n. We then see that:

$$T(p)^n \begin{bmatrix} a \\ c \end{bmatrix}_{N_r} \equiv \begin{bmatrix} a/p^n \\ c \end{bmatrix}_{N_r} = \begin{bmatrix} a \\ c \end{bmatrix}_{N_r} \mod D_r.$$

It follows that $e^*(\mathbf{Z}_p[C_r]/D_r) = \mathbf{Z}_p[C_r]/D_r$. □

COROLLARY (4.3.5). $\mathrm{rank}_{\mathbf{Z}_p}\, e^*\mathbf{Z}_p[C_r] = \frac{1}{2}\varphi(p^r)\sum_{0<t|N}\varphi(t)\varphi(N/t)$.

Proof. The rank in question is equal to the cardinality of

$$\left\{ \left(\begin{bmatrix} a_1 \\ c_1 \end{bmatrix}_N, \begin{bmatrix} 0 \\ c_2 \end{bmatrix}_{p^r} \right) \in (A_N \times A_{p^r})/\{\pm 1\} \right\}.$$ □

Recall that $H^1(\overline{Y}_r, \mathbf{Z}_p)$ is canonically isomorphic to $\mathrm{Hom}(T_p(GJ_r), \mathbf{Z}_p)$ (3.3.3). We henceforth consider the latter group as a module over $\mathcal{H}_2^*(\Gamma_r; \mathbf{Z}_p)$ through this isomorphism. Thus, as we noted after (3.4.8), for example, the action of $T^*(l) \in \mathcal{H}_2^*(\Gamma_r; \mathbf{Z}_p)$ on $\mathrm{Hom}(T_p(GJ_r), \mathbf{Z}_p)$ is induced from the endomorphism $T^*(l)$ of GJ_r (3.4.8). On the other hand, from (3.4.11), we have an isomorphism

$$\mathrm{Hom}(e^*T_p(T_r), \mathbf{Z}_p) \xrightarrow{\sim} e^*\mathbf{Z}_p[C_r](-1), \tag{4.3.6}$$

by (3.4.12). These groups then inherit the structure of $e^*\mathcal{H}_2^*(\Gamma_r; \mathbf{Z}_p)$-modules. We therefore have the following diagram of $e^*\mathcal{H}_2^*(\Gamma_r; \mathbf{Z}_p)$-modules with exact horizontal lines:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & e^*H^1(\overline{X}_r, \mathbf{Z}_p) & \xrightarrow{\text{can}} & e^*H^1(\overline{Y}_r, \mathbf{Z}_p) & & & & \\
 & & \wr\downarrow & & \wr\downarrow (3.3.3) & & & & \\
0 & \longrightarrow & \mathrm{Hom}(e^*T_p(J_r), \mathbf{Z}_p) & \longrightarrow & \mathrm{Hom}(e^*T_p(GJ_r), \mathbf{Z}_p) & \longrightarrow & e^*\mathbf{Z}_p[C_r](-1) & \longrightarrow & 0.
\end{array} \tag{4.3.7}$$

Here, the left vertical arrow is the usual one (cf. [O2] (3.1.4)). One checks that the square above commutes, in a similar manner as (3.3.5).

Recall also that $e^*\mathcal{H}_2^*(\Gamma_r; \mathbf{Z}_p)$ is a $\mathbf{Z}_p[(\mathbf{Z}/N_r\mathbf{Z})^\times]$-algebra; and that $e^*\mathcal{H}^*(N; \mathbf{Z}_p)$ is a $\mathbf{Z}_p[[\mathcal{Z}_N]]$-algebra (1.5). From now on, we denote by the same letter ι as before the natural mappings

$$\iota : \begin{cases} (\mathbf{Z}/N_r\mathbf{Z})^\times \hookrightarrow \mathbf{Z}_p[(\mathbf{Z}/N_r\mathbf{Z})^\times] \ \ (\to e^*\mathcal{H}_2^*(\Gamma_r; \mathbf{Z}_p)), \\ \mathcal{Z}_N \hookrightarrow \mathbf{Z}_p[[\mathcal{Z}_N]] \ \ (\to e^*\mathcal{H}^*(N; \mathbf{Z}_p)). \end{cases} \tag{4.3.8}$$

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

For $\alpha \in (\mathbf{Z}/N_r\mathbf{Z})^\times$, the action of $\iota(\alpha)$ on $e^*\mathbf{Z}_p[C_r](-1)$ is obtained from (the Tate twist of) the following action:

$$\mathbf{Z}_p[C_r] \supseteq C_r(\overline{\mathbf{Q}}) \ni c \mapsto \sigma_\alpha \cdot c, \tag{4.3.9}$$

where $\sigma_\alpha \in \mathrm{SL}_2(\mathbf{Z})$ is congruent to $\begin{bmatrix} \alpha^{-1} & * \\ 0 & \alpha \end{bmatrix}$ mod $N_r \cdot M_2(\mathbf{Z})$, by (3.4.12).

PROPOSITION (4.3.10). *Consider* $\mathbf{Z}_p[C_r]$ *as a* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$*-module via the natural action on* $C_r(\overline{\mathbf{Q}})$. *Then* (4.3.6) *is an isomorphism of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$*-modules. If* $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}(\zeta_N))$ *satisfies* $\zeta_{p^r}^\sigma = \zeta_{p^r}^\alpha$ *with* $\alpha \in (\mathbf{Z}/p^r\mathbf{Z})^\times \subseteq (\mathbf{Z}/N_r\mathbf{Z})^\times$, σ *acts as* $\iota(\alpha)^{-1}$ *on* $e^*\mathbf{Z}_p[C_r]$.

Proof. It is easy to see that the exact sequence (3.4.9) for Y_r is $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-equivariant; and the pairing (3.4.10) clearly satisfies $(x^\sigma, y^\sigma) = (x, y)$ for all $x, y \in \mathbf{Z}_p[C_r]$ and $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Therefore, (3.4.11) for Y_r is an exact sequence of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-modules. We also see that $T(p)$ on $\mathbf{Z}_p[C_r]$ commutes with the action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$; and hence the first assertion follows.

Next, D_r, being the kernel of e^*, is a Galois submodule of $\mathbf{Z}_p[C_r]$. Thus for the second assertion, with the same notation as above, it suffices to show that

$$\begin{bmatrix} a \\ c \end{bmatrix}_{N_r}^{\sigma} = \sigma_\alpha^{-1} \cdot \begin{bmatrix} a \\ c \end{bmatrix}_{N_r},$$

if $p \nmid c$. Let X be the canonical model over $\mathbf{Q}(\zeta_N)$ of the modular curve attached to $\Gamma(N) \cap \Gamma_1(p^r)$ of which the cusp $i\infty$ is rational over $\mathbf{Q}(\zeta_N)$. $\Gamma_0(p^r)$ normalizes the above group; and it acts as $\mathbf{Q}(\zeta_N)$-automorphisms of X. It follows that all the cusps of the form $\left(\begin{bmatrix} * \\ * \end{bmatrix}_N, \begin{bmatrix} * \\ 0 \end{bmatrix}_{p^r}\right)$ on X_r are $\mathbf{Q}(\zeta_N)$-rational. But a cusp $\begin{bmatrix} a \\ c \end{bmatrix}_{N_r}$ with $p \nmid c$ is obtained from a cusp of the above type by applying τ_r. The formula to be proved results from the well-known property of the automorphism of X_r attached to τ_r (cf. (4.2.4)). $\square$

When $s \geqslant r \geqslant 1$, we have the commutative diagram (3.3.4) for the natural morphism $f_r^s : X_s \to X_r$. But by (3.2.8), the diagram:

$$\begin{array}{ccc} \mathrm{Hom}(T_p(T_s), \mathbf{Z}_p) & \xrightarrow{(3.4.11)} & \mathbf{Z}_p[C_s](-1) \\ {\scriptstyle \mathrm{Hom}(f_r^{s*}, \mathbf{Z}_p)} \downarrow & & \downarrow \\ \mathrm{Hom}(T_p(T_r), \mathbf{Z}_p) & \xrightarrow[(3.4.11)]{} & \mathbf{Z}_p[C_r](-1), \end{array} \tag{4.3.11}$$

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

commutes, if we define the right vertical arrow from the (set theoretical) projection: $C_s(\overline{\mathbf{Q}}) \to C_r(\overline{\mathbf{Q}})$. Thus, taking the projective limits with respect to $\mathrm{Hom}(f_r^{s*}, \mathbf{Z}_p)$ and (4.3.11), (4.3.7) yields the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & e^*ES_p(N)_{\mathbf{Z}_p} & \longrightarrow & e^*GES_p(N)_{\mathbf{Z}_p} & & & & \\ & & \downarrow \wr & & \downarrow \wr & & & & \\ 0 & \longrightarrow & \varprojlim_{r\geqslant 1} \mathrm{Hom}(e^*T_p(J_r), \mathbf{Z}_p) & \longrightarrow & \varprojlim_{r\geqslant 1} \mathrm{Hom}(e^*T_p(GJ_r), \mathbf{Z}_p) & \longrightarrow & \varprojlim_{r\geqslant 1} e^*\mathbf{Z}_p[C_r](-1) & \longrightarrow & 0. \end{array} \tag{4.3.12}$$

Now set

$$\mathcal{C}_p(N)_{\mathbf{Z}_p} := \varprojlim_{r\geqslant 1} e^*\mathbf{Z}_p[C_r], \qquad \mathcal{C}_p(N)_{\mathfrak{o}} := \mathcal{C}_p(N)_{\mathbf{Z}_p} \widehat{\otimes}_{\mathbf{Z}_p} \mathfrak{o}. \tag{4.3.13}$$

These are modules over $\mathbf{Z}_p[[\mathcal{Z}_N]]$ or $\mathfrak{o}[[\mathcal{Z}_N]]$ (and hence over $\Lambda_{\mathbf{Z}_p}$ or $\Lambda_{\mathfrak{o}}$), respectively.

PROPOSITION (4.3.14). *$\mathcal{C}_p(N)_{\mathfrak{o}}$ is a free $\Lambda_{\mathfrak{o}}$-module of rank $((p-1)/2)\sum_{0<t|N} \varphi(t)\varphi(N/t)$. Moreover, for each $r \geqslant 1$, the projection mapping induces an isomorphism $\mathcal{C}_p(N)_{\mathfrak{o}}/\omega_{r,0} \xrightarrow{\sim} e^*\mathbf{Z}_p[C_r] \otimes_{\mathbf{Z}_p} \mathfrak{o} =: e^*\mathfrak{o}[C_r]$.*

Proof. It is enough to prove our assertion when $\mathfrak{o} = \mathbf{Z}_p$. If $\alpha \in U_1$, the action of $\iota(\alpha)$ on $\mathbf{Z}_p[C_r]$ is given by

$$C_r(\overline{\mathbf{Q}}) \ni \left(\begin{bmatrix} a_1 \\ c_1 \end{bmatrix}_N, \begin{bmatrix} a_2 \\ c_2 \end{bmatrix}_{p^r} \right) \mapsto \left(\begin{bmatrix} a_1 \\ c_1 \end{bmatrix}_N, \begin{bmatrix} \alpha^{-1}a_2 \\ \alpha c_2 \end{bmatrix}_{p^r} \right).$$

Therefore, as a $\Lambda_{\mathbf{Z}_p}$-module, $e^*\mathbf{Z}_p[C_r]$ is isomorphic to the submodule of $\mathbf{Z}_p[C_r]$ generated by all the elements of the form $\left(\begin{bmatrix} a_1 \\ c_1 \end{bmatrix}_N, \begin{bmatrix} 0 \\ c_2 \end{bmatrix}_{p^r}\right)$, by (4.3.4). Namely, it is canonically isomorphic to the free $\mathbf{Z}_p$-module generated by $(A_N \times (\mathbf{Z}/p^r\mathbf{Z})^\times)/\{\pm 1\}$ as a $\Lambda_{\mathbf{Z}_p}$-module; the $\Lambda_{\mathbf{Z}_p}$-module structure of the latter being the evident one. Our conclusion is now obvious. □

4.4. THE MAPPING: $e^{*\prime}GES_p(N)_{\mathfrak{o}} \to e^{*\prime}\mathfrak{M}_2^*(N;\mathfrak{o})(-1)$

We now come to our main step. By virtue of what we have said so far, we can proceed in a parallel way as in [O2] 3.3 to construct the mapping above, as follows: Let $\widetilde{G}_r^0$ and $\widetilde{G}_r^{\text{ét}}$ be the connected part and the maximal étale quotient of the p-divisible group $\widetilde{G}_r$ (4.2.9), respectively; and likewise for G_r. Since H_r is of multiplicative type, it is contained in $\widetilde{G}_r^0$ and, hence, $\widetilde{G}_r^{\text{ét}} = G_r^{\text{ét}}$. Put

$$\mathfrak{A}_r := \mathrm{Hom}(T_p(G_r^{\text{ét}}), \mathbf{Z}_p), \begin{cases} \widetilde{\mathfrak{B}}_r := \mathrm{Hom}(T_p(\widetilde{G}_r^0), \mathbf{Z}_p), \\ \mathfrak{B}_r := \mathrm{Hom}(T_p(G_r^0), \mathbf{Z}_p). \end{cases} \tag{4.4.1}$$

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

Then we have an exact sequence of $e^{*\prime}\mathcal{H}_2^*(\Gamma_r;\mathbf{Z}_p)$-modules:

$$0 \to \mathfrak{A}_r \to e^{*\prime}H^1(\overline{Y}_r,\mathbf{Z}_p) \to \widetilde{\mathfrak{B}}_r \to 0, \tag{4.4.2}$$

by (3.3.3) and (4.2.6).

Let I_p be the inertia group of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$, and

$$\kappa : \begin{cases} \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{Z}_p^\times \ \text{ or} \\ \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p) \to \mathbf{Z}_p^\times, \end{cases} \tag{4.4.3}$$

the p-cyclotomic character. Then we have:

$$\begin{aligned} &\mathfrak{A}_r = e^{*\prime}H^1(\overline{Y}_r,\mathbf{Z}_p)^{I_p} = e^{*\prime}H^1(\overline{X}_r,\mathbf{Z}_p)^{I_p}, \\ &I_p \ni \sigma \ \text{ acts as } \ \kappa(\sigma)^{-1}\iota(\kappa(\sigma))^{-1} \ \text{ on } \ \widetilde{\mathfrak{B}}_r. \end{aligned} \tag{4.4.4}$$

In fact, we know by (4.3.10) (resp. [O2] (3.2.11)) that the action of I_p on $\widetilde{\mathfrak{B}}_r/\mathfrak{B}_r$ (resp. $\mathfrak{B}_r$) is as stated as above. But it is easy to see that the exact sequence of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$-modules: $0 \longrightarrow \mathfrak{B}_r \longrightarrow \widetilde{\mathfrak{B}}_r \longrightarrow \widetilde{\mathfrak{B}}_r/\mathfrak{B}_r \longrightarrow 0$ splits when tensored with $\mathbf{Q}_p$, using an appropriate element of $e^{*\prime}\mathcal{H}_2^*(\Gamma_r;\mathbf{Z}_p)$.

From this, we see that (4.4.2) is a split exact sequence of $e^{*\prime}\mathcal{H}_2^*(\Gamma_r;\mathbf{Z}_p)$-modules. The splitting is noncanonical, but can be made functorial when we let r vary. Therefore, if we set

$$\mathfrak{A}_\infty := \varprojlim_{r\geqslant 1} \mathfrak{A}_r, \quad \begin{cases} \widetilde{\mathfrak{B}}_\infty := \varprojlim_{r\geqslant 1} \widetilde{\mathfrak{B}}_r, \\ \mathfrak{B}_\infty := \varprojlim_{r\geqslant 1}, \mathfrak{B}_r, \end{cases} \tag{4.4.5}$$

we have a split exact sequence of $e^{*\prime}\mathcal{H}^*(N;\mathbf{Z}_p)$-modules

$$0 \longrightarrow \mathfrak{A}_\infty \longrightarrow e^{*\prime}GES_p(N)_{\mathbf{Z}_p} \longrightarrow \widetilde{\mathfrak{B}}_\infty \longrightarrow 0. \tag{4.4.6}$$

It follows from (1.3.5) that both $\mathfrak{A}_\infty$ and $\widetilde{\mathfrak{B}}_\infty$ are free $\Lambda_{\mathbf{Z}_p}$-modules. Moreover, we see that, via the projection mappings

$$\mathfrak{A}_\infty/\omega_{r,0} \xrightarrow{\sim} \mathfrak{A}_r, \qquad \widetilde{\mathfrak{B}}_\infty/\omega_{r,0} \xrightarrow{\sim} \widetilde{\mathfrak{B}}_r, \tag{4.4.7}$$

for all $r \geqslant 1$. For each pair of integers $r \geqslant 1$ and $d \geqslant 0$, set

$$\begin{aligned} &\mathfrak{A}_{r,d} := e^{*\prime}H^1(\overline{Y}_r, F_{S^d(\mathbf{Z}_p)})^{I_p}, \\ &\widetilde{\mathfrak{B}}_{r,d} := e^{*\prime}H^1(\overline{Y}_r, F_{S^d(\mathbf{Z}_p)})/\mathfrak{A}_{r,d}. \end{aligned} \tag{4.4.8}$$

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

Then, by (1.4.2), we also see that the specialization mapping $sp_{r,d}$ induces the following isomorphisms:

$$\mathfrak{A}_\infty/\omega_{r,d} \xrightarrow{\sim} \mathfrak{A}_{r,d}, \qquad \widetilde{\mathfrak{B}}_\infty/\omega_{r,d} \xrightarrow{\sim} \widetilde{\mathfrak{B}}_{r,d}. \tag{4.4.9}$$

If we put

$$\mathfrak{A}_{r,\mathfrak{o}} := \mathfrak{A}_r \widehat{\otimes}_{\mathbf{Z}_p} \mathfrak{o}, \qquad \widetilde{\mathfrak{B}}_{r,\mathfrak{o}} := \widetilde{\mathfrak{B}}_r \widehat{\otimes}_{\mathbf{Z}_p} \mathfrak{o}, \tag{4.4.10}$$

for $1 \leqslant r \leqslant \infty$, and similarly for $\mathfrak{A}_{r,d}$ and $\widetilde{\mathfrak{B}}_{r,d}$, (4.4.2), (4.4.6), (4.4.7) and (4.4.9) remain valid for these modules, $e^{*\prime} H^1(\overline{Y}_r, \mathbf{Z}_p) \otimes_{\mathbf{Z}_p} \mathfrak{o}$, and $e^{*\prime} GES_p(N)_\mathfrak{o}$.

From now on, we assume that $\mathfrak{o}$ *contains all the roots of unity*. Then applying the argument of Tate [Ta] Section 4 to the *ordinary* p-divisible group $\widetilde{G}_r$ over $\mathbf{Z}_p[\zeta_{p^r}]$, we have canonical isomorphisms:

$$\begin{aligned}
\mathfrak{A}_{r,\mathfrak{o}} &\cong \mathrm{Lie}((\widetilde{G}^{\text{ét}}_{r/\mathfrak{o}})') = \mathrm{Lie}((\widetilde{G}_{r/\mathfrak{o}})'),\\
\mathfrak{B}_{r,\mathfrak{o}} &\cong \mathrm{Cot}(G^0_{r/\mathfrak{o}})(-1) = \mathrm{Cot}(G_{r/\mathfrak{o}})(-1) \cong e^{*\prime}\mathrm{Cot}(B^*_{r/\mathfrak{o}})(-1),\\
\widetilde{\mathfrak{B}}_{r,\mathfrak{o}} &\cong \mathrm{Cot}(\widetilde{G}^0_{r/\mathfrak{o}})(-1) = \mathrm{Cot}(\widetilde{G}_{r/\mathfrak{o}})(-1) \cong e^{*\prime}\mathrm{Cot}(Q^*_{r/\mathfrak{o}})(-1),
\end{aligned} \tag{4.4.11}$$

where the subscript '$_{/\mathfrak{o}}$' means the base extension from $\mathbf{Z}_p[\zeta_{p^r}]$ to $\mathfrak{o}$, and $(\ )'$ signifies the Cartier dual. From (4.4.2), we obtain the following exact sequence:

$$0 \to \mathrm{Lie}((\widetilde{G}_{r/\mathfrak{o}})') \to e^{*\prime} H^1(\overline{Y}_r, \mathbf{Z}_p) \otimes_{\mathbf{Z}_p} \mathfrak{o} \to \mathrm{Cot}(\widetilde{G}_{r/\mathfrak{o}})(-1) \to 0. \tag{4.4.12}$$

Especially, we have constructed homomorphisms of $e^{*\prime}\mathcal{H}^*_2(\Gamma_r; \mathfrak{o})$-modules:

$$e^{*\prime} H^1(\overline{Y}_r, \mathbf{Z}_p) \otimes_{\mathbf{Z}_p} \mathfrak{o} \to \widetilde{\mathfrak{B}}_{r,\mathfrak{o}} \cong e^{*\prime}\mathrm{Cot}(Q^*_{r/\mathfrak{o}})(-1) \hookrightarrow M_2(\Gamma_r; K)(-1). \tag{4.4.13}$$

PROPOSITION (4.4.14). *The image of the natural mapping:* $e^{*\prime}\mathrm{Cot}(Q^*_{r/\mathfrak{o}}) \hookrightarrow M_2(\Gamma_r; K)$ *is contained in* $e^{*\prime} M^*_2(\Gamma_r; \mathfrak{o}) \cap M_2(\Gamma_r; \mathfrak{o})$.

Proof. The proof is similar to that of [O2] (3.3.6), as follows. Let $Y_{r/\mathbf{Z}_p[\zeta_{N_r}]}$ be the normalization of the affine j-line over $\mathbf{Z}_p[\zeta_{N_r}]$ in $Y_r \otimes_{\mathbf{Q}} \mathbf{Q}_p(\zeta_{N_r})$, and $Y^{\text{smooth}}_{r/\mathbf{Z}_p[\zeta_{N_r}]}$ its smooth locus over $\mathbf{Z}_p[\zeta_{N_r}]$. Also, let $GJ_{r/\mathbf{Z}_p[\zeta_{N_r}]}$ be the Néron left-model of GJ_r over $\mathbf{Z}_p[\zeta_{N_r}]$. There is an unramified extension of $\mathbf{Q}_p(\zeta_{N_r})$ over which Y_r admits a rational point x_0. We then obtain the morphism ι_{Y_r,x_0} (3.1.4) over this field, which extends to the base extensions of $Y^{\text{smooth}}_{r/\mathbf{Z}_p[\zeta_{N_r}]}$ and $GJ_{r/\mathbf{Z}_p[\zeta_{N_r}]}$ to its ring of integers. Therefore, further extending the base to $\mathfrak{o}$, we obtain $\iota_{Y_r,x_0}\colon Y^{\text{smooth}}_{r/\mathfrak{o}} \to GJ_{r/\mathfrak{o}}$. Thus, we have the situation as in loc. cit.

$$\mathrm{Spec}(\mathfrak{o}((q))) \to Y^{\text{smooth}}_{r/\mathfrak{o}} \xrightarrow{\iota_{Y_r,x_0}} GJ_{r/\mathfrak{o}} \to Q^*_{r/\mathfrak{o}},$$

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

from which we conclude that the image in question lies in $M_2(\Gamma_r;\mathfrak{o})$. The image also lies in $M_2^*(\Gamma_r;\mathfrak{o})$ because the automorphism w_r of GJ_r over $\mathbf{Q}(\zeta_{N_r})$ extends to $GJ_{r/\mathfrak{o}}$. □

It follows that (4.4.13) gives

$$e^{*\prime}H^1(\overline{Y}_r,\mathbf{Z}_p)\otimes_{\mathbf{Z}_p}\mathfrak{o}\to\widetilde{\mathfrak{B}}_{r,\mathfrak{o}}\to e^{*\prime}M_2^*(\Gamma_r;\mathfrak{o})(-1). \tag{4.4.15}$$

When r varies, the trace mappings of étale cohomology groups and the natural trace mappings of modular forms are compatible, by (3.3.4) and (3.2.6). Taking the projective limit, we finally obtain a homomorphism of $e^{*\prime}\mathcal{H}^*(N;\mathfrak{o})$-modules:

$$e^{*\prime}GES_p(N)_{\mathfrak{o}}\to\widetilde{\mathfrak{B}}_{\infty,\mathfrak{o}}\to e^{*\prime}\mathfrak{M}_2^*(N;\mathfrak{o})(-1). \tag{4.4.16}$$

THEOREM (4.4.17). *The mapping:* $\widetilde{\mathfrak{B}}_{\infty,\mathfrak{o}}\longrightarrow e^{*\prime}\mathfrak{M}_2^*(N;\mathfrak{o})(-1)$ *above is an isomorphism.*

We will complete the proof of this theorem in the next subsection. Let us give here some preliminary remarks. The two modules in question are both free of finite rank over $\Lambda_{\mathfrak{o}}$ and, hence, the mapping above is an isomorphism if it is so after reducing modulo $\omega_{1,0}=T$. So, by (2.5.4) and (4.4.7), we just need to show that the mapping

$$e^{*\prime}\mathrm{Cot}(Q^*_{1/\mathfrak{o}})\longrightarrow e^{*\prime}M_2^*(\Gamma_1;\mathfrak{o}) \tag{4.4.18}$$

is an isomorphism.

For this, we recall that there is a canonical isomorphism: $T_r\otimes_{\mathbf{Q}}K\cong\mathrm{Coker}(\mathbf{G}_m\xrightarrow{\text{diag}}\prod_{c\in C_r(\overline{\mathbf{Q}})}\mathbf{G}_m)$. This trivially extends to the group scheme $\mathrm{Coker}(\mathbf{G}_m\xrightarrow{\text{diag}}\prod_{c\in C_r(\overline{\mathbf{Q}})}\mathbf{G}_m)=:T_{r/\mathfrak{o}}$ over $\mathfrak{o}$ of which $N^0_{r/\mathfrak{o}}$ is a quotient. The Hodge–Tate theory for the associated p-divisible group is of the following very elementary nature: Namely, the diagram

$$\begin{array}{ccccc}
\mathrm{Hom}(T_p(T_{r/\mathfrak{o}}),\mathfrak{o}) & \xrightarrow{\text{can}} & \oplus_{c\in C_r(\overline{\mathbf{Q}})}\mathrm{Hom}(T_p(\mathbf{G}_m),\mathfrak{o}) & \xleftarrow{\sim} & \oplus_{c\in C_r(\overline{\mathbf{Q}})}\mathfrak{o}(-1)\\
\text{Tate}\downarrow\wr & & \downarrow\wr & & \\
\mathrm{Cot}(T_{r/\mathfrak{o}})(-1) & \xrightarrow[\text{can}]{} & \oplus_{c\in C_r(\overline{\mathbf{Q}})}\mathrm{Cot}(\mathbf{G}_m)(-1). & &
\end{array} \tag{4.4.19}$$

commutes if we define the right vertical arrow from $\mathfrak{o}\xrightarrow{\sim}\mathrm{Cot}(\mathbf{G}_m)$ sending 1 to dX/X. (Here and in the diagram, we are of course considering $\mathbf{G}_m$ over $\mathfrak{o}$.) The action of $T^*(p)$ on T_r clearly extends to $T_{r/\mathfrak{o}}$; and the above compatibility means that the isomorphism (4.3.6) when tensored with $\mathfrak{o}$ coincides with the one obtained

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

from the Hodge–Tate theory of $T_{r/\mathfrak{o}}$, via $\mathfrak{o} \cong \mathrm{Cot}(\mathbf{G}_m)$. Consider the following commutative diagram with exact horizontal lines:

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Hom}(T_p(G_r), \mathfrak{o}) & \longrightarrow & \mathrm{Hom}(T_p(\widetilde{G}_r), \mathfrak{o}) & \longrightarrow & \mathrm{Hom}(T_p(H_r), \mathfrak{o}) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mathrm{can}} & & \downarrow{\scriptstyle \mathrm{can}} & & \Vert & & \\
0 & \longrightarrow & \mathfrak{B}_{r,\mathfrak{o}} & \longrightarrow & \widetilde{\mathfrak{B}}_{r,\mathfrak{o}} & \longrightarrow & \mathrm{Hom}(T_p(H_r), \mathfrak{o}) & \longrightarrow & 0 \\
 & & {\scriptstyle (4.4.11)}\downarrow\wr & & \wr\downarrow{\scriptstyle (4.4.11)} & & \downarrow\wr & & \\
0 & \longrightarrow & e^{*\prime}\mathrm{Cot}(B^*_{r/\mathfrak{o}})(-1) & \longrightarrow & e^{*\prime}\mathrm{Cot}(Q^*_{r/\mathfrak{o}})(-1) & \xrightarrow{\mathbf{Res}(-1)} & e^{*\prime}\mathfrak{o}[C_r](-1) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle (4.4.14)} & & & & \\
0 & \longrightarrow & e^{*\prime} S_2^*(\Gamma_r; \mathfrak{o})(-1) & \xrightarrow[\mathrm{can}]{} & e^{*\prime} M_2^*(\Gamma_r; \mathfrak{o})(-1). & & & &
\end{array}
\tag{4.4.20}
$$

Here, the upper horizontal line comes from (4.2.9), and the right vertical arrow is obtained from (4.3.6) through the quotient morphism: $T_r \to N_r$. By the remark above, using (3.1.13) and the compatibility (3.1.10), we now see that the mapping labelled as '$\mathbf{Res}(-1)$' is indeed the Tate twist of the *sum of residues* given by:

$$
\mathbf{Res}(\omega) = \sum_{c \in C_r(\overline{\mathbf{Q}})} \mathrm{Res}_c(\omega) \cdot c, \tag{4.4.21}
$$

for $\omega \in \mathrm{e}^{*\prime}\mathrm{Cot}(Q^*_{r/\mathfrak{o}}) \hookrightarrow H^0(X_r \otimes_{\mathbf{Q}} K, \Omega^1_{X_r \otimes_{\mathbf{Q}} K/K}(C_r))$. Namely, we have proved the *surjectivity* of $\mathbf{Res} : \mathrm{e}^{*\prime}\mathrm{Cot}(Q^*_{r/\mathfrak{o}}) \to e^{*\prime}\mathfrak{o}[C_r]$ via the Hodge–Tate theory. As for (4.4.18), we already know that the mapping: $e^{*\prime}\mathrm{Cot}(B^*_{1/\mathfrak{o}}) \to e^{*\prime}S_2^*(\Gamma_1; \mathfrak{o})$ is an isomorphism ([O2] (3.4.9)). Our Theorem (4.4.17) will therefore follow from the following proposition whose proof we give in the next subsection:

PROPOSITION (4.4.22). *For $f \in e^* M_2^*(\Gamma_r; \mathfrak{o})$, we let $\omega_f := f dq/q$ be the corresponding differential on $X_r \otimes_{\mathbf{Q}} K$. Then $\mathbf{Res}(\omega_f) \in e^* \mathbf{Z}_p[C_r] \otimes_{\mathbf{Z}_p} K$ actually lies in $e^*\mathfrak{o}[C_r]$.*

4.5. COMPLETION OF THE PROOF OF OUR MAIN THEOREM

We begin with an elementary observation: In general, let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbf{Z})$, and fix a cusp $s \in \mathbf{P}^1(\mathbf{Q})$. Then there is a $\rho \in \mathrm{SL}_2(\mathbf{Z})$ such that $\rho(s) = i\infty$. If we denote by $\Gamma(s)$ the stabilizer subgroup of s in Γ, we have

$$
\rho\Gamma(s)\rho^{-1} \cdot \{\pm 1\} = \left\{ \pm \begin{bmatrix} 1 & h \\ 0 & 1 \end{bmatrix}^m \mid m \in \mathbf{Z} \right\} \tag{4.5.1}
$$

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

with a positive integer h. For $f \in M_2(\Gamma)$, its Fourier expansion at s (which depends on the choice of ρ) is given by:

$$f \mid \rho^{-1} = \sum_{n=0}^{\infty} a_n q^{n/h} \quad (q^{1/h} = \mathrm{e}^{2\pi i z/h}), \tag{4.5.2}$$

(cf. [Sh] 2.1). The differential $\omega_f = f\,\mathrm{d}q/q$ satisfies $\omega_f \circ \rho^{-1} = (f \mid \rho^{-1})\,\mathrm{d}q/q$; and it follows easily from this that:

$$\omega_f = h\left(\sum_{n=0}^{\infty} a_n\, \mathrm{e}^{2\pi i(n-1)\rho(z)/h}\right) \mathrm{d}\mathrm{e}^{2\pi i\rho(z)/h}. \tag{4.5.3}$$

Since $\mathrm{e}^{2\pi i\rho(z)/h}$ is a local parameter at s of the Riemann surface $\Gamma\backslash H \cup \mathbf{P}^1(\mathbf{Q})$ ([Sh] 1.5), we conclude that:

$$\mathrm{Res}_s(\omega_f) = ha_0. \tag{4.5.4}$$

We now wish to prove (4.4.22). To do this, we use the algebraic theory of modular forms (Katz [Ka1]). In [O2] 3.6, we reviewed this theory and we now use the same terminology as in loc. cit. Recall that $R^k(B, \Gamma_{00}(M)^{\mathrm{arith}})$ denotes the space of $\Gamma_{00}(M)^{\mathrm{arith}}$ modular forms of weight k ($\in \mathbf{Z}$) over a ring B, which consists of certain functions F on the $\Gamma_{00}(M)^{\mathrm{arith}}$-test objects (E, ω, i) over B-algebras. There is a natural injection

$$M_k(\Gamma_1(M)) \hookrightarrow R^k(\mathbf{C}, \Gamma_{00}(M)^{\mathrm{arith}}). \tag{4.5.5}$$

Namely, if we set

$$\begin{aligned} &E_{2\pi i, 2\pi i z} := \mathbf{C}/2\pi i\mathbf{Z} + 2\pi i z\mathbf{Z}, \\ &i(\zeta_M^n) := \frac{2\pi i n}{M} \quad (\zeta_M = \mathrm{e}^{2\pi i/M}), \end{aligned} \tag{4.5.6}$$

then $F_f \in R^k(\mathbf{C}, \Gamma_{00}(M)^{\mathrm{arith}})$ corresponding to $f \in M_k(\Gamma_1(M))$ satisfies

$$f(z) = F_f(E_{2\pi i, 2\pi i z}, \mathrm{d}u, i) \tag{4.5.7}$$

with u the variable on $\mathbf{C}$. The q-expansion of f (at the cusp $i\infty$) is given by evaluating F_f at the Tate curve; precisely, it is equal to $F_f(\mathrm{Tate}(q), \omega_{\mathrm{can}}, i_{\mathrm{can}})$.

Put $\gamma = \rho^{-1} = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ so that $\gamma(i\infty) = s = \left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right]_{N_r}$. Then we see that

$$\begin{aligned} (f \mid \gamma)(z) &= (cz+d)^{-k} F_f(E_{2\pi i, 2\pi i\gamma(z)}, \mathrm{d}u, i) \\ &= F_f(E_{2\pi i, 2\pi i\gamma(z)}, (cz+d)\,\mathrm{d}u, i). \end{aligned} \tag{4.5.8}$$

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

The multiplication by $(cz+d)^{-1}$ on $\mathbf{C}$ induces an isomorphism:

$$E_{2\pi i, 2\pi iz} \xrightarrow{\times(cz+d)^{-1}} E_{2\pi i, 2\pi i\gamma(z)}. \tag{4.5.9}$$

If we define the $\Gamma_{00}(M)^{\text{arith}}$-structure i' on the left-hand side by

$$i'(\zeta_M^n) := \frac{2\pi i(cz+d)n}{M}, \tag{4.5.10}$$

then this is compatible with i on the right-hand side. We therefore have

$$(f \mid \gamma)(z) = F_f(E_{2\pi i, 2\pi iz}, \mathrm{d}u, i'). \tag{4.5.11}$$

This in turn gives us the following purely algebraic description of the Fourier expansion at s:

$$f \mid \gamma = \sum_{n=0}^{\infty} a_n q^{n/h} = F_f(\mathrm{Tate}(q), \omega_{\text{can}}, i''), \tag{4.5.12}$$

where we define i'' by $i''(\zeta_M) := \zeta_M^d q^{c/M}$ (cf. Katz [Ka2] 2.4). Especially, when B is a subring of $\mathbf{C}_p$, this formula makes sense for $f \in M_k(\Gamma_1(M); B)$ (which is defined as in (1.5.8)); and (4.5.4) remains valid if $k = 2$.

LEMMA (4.5.13). *Let B be a subring of $\mathbf{C}$ or $\mathbf{C}_p$, and take an $f \in M_2(\Gamma_1(M); B)$. Assume that $M = M_1M_2$ with relatively prime positive integers M_1 and M_2; and that $\gamma \in \Gamma_0(M_1)$. Then the Fourier expansion of f at $s = \gamma(i\infty)$ (with respect to $\rho = \gamma^{-1}$) belongs to $B[\zeta_{M_2}, 1/M_2][[q^{1/M_2}]]$.*

Proof. First note that h divides M_2. i'' being as above, we see that the following diagram commutes:

$$\begin{array}{ccc}
\boldsymbol{\mu}_M & \xrightarrow{\quad i'' \quad} & {}_M\mathrm{Tate}(q) \\
\downarrow \wr & & \downarrow \wr \\
\boldsymbol{\mu}_{M_1} \times \boldsymbol{\mu}_{M_2} & \xrightarrow{i_1 \times i_2} & {}_{M_1}\mathrm{Tate}(q) \times {}_{M_2}\mathrm{Tate}(q),
\end{array}$$

if we define i_1 (resp. i_2) by $i_1(\zeta_{M_1}) := \zeta_{M_1}^d$ (resp. $i_2(\zeta_{M_2}) := \zeta_{M_2}^d q^{c/M_2}$). (Here, of course, $\zeta_{M_j} = \mathrm{e}^{2\pi i/M_j} \in \overline{\mathbf{Q}}$.) Thus the $\Gamma_{00}(M)^{\text{arith}}$-test object $(\mathrm{Tate}(q), \omega_{\text{can}}, i'')$ is defined over $B[\zeta_{M_2}, 1/M_2]((q^{1/M_2}))$. By the q-expansion principle, F_f belongs to $R^k(B, \Gamma_{00}(M)^{\text{arith}})$; and hence it takes the value in $B[\zeta_{M_2}, 1/M_2]((q^{1/M_2}))$ when evaluated at the triple above. □

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

Proof of (4.4.22). By (4.3.4), we can take a basis of $e^*\mathbf{Z}_p[C_r]$ of the form

$$\left\{ \begin{bmatrix} a \\ c \end{bmatrix}_{N_r} + d_{a,c} \mid p \nmid c \right\},$$

with a suitable $d_{a,c} \in D_r$ for each $\begin{bmatrix} a \\ c \end{bmatrix}_{N_r}$. It is therefore enough to show that $\mathrm{Res}_{\left[\begin{smallmatrix} a \\ c \end{smallmatrix}\right]_{N_r}}(\omega_f) \in \mathfrak{o}$ whenever $p \nmid c$.

Applying the previous lemma to $g := f \mid \tau_r \in M_2(\Gamma_r; \mathfrak{o})$, we see that: $g \mid \gamma \in \mathfrak{o}[[q^{1/N}]]$ for any $\gamma \in \Gamma_0(p^r)$. It follows from (4.5.4) that $\mathrm{Res}_s(\omega_g) \in \mathfrak{o}$ for each cusp s of the form $\left(\begin{bmatrix} * \\ * \end{bmatrix}_N, \begin{bmatrix} * \\ 0 \end{bmatrix}_{p^r}\right)$. But we clearly have: $\omega_g = \omega_f \circ \tau_r$, and hence $\mathrm{Res}_s(\omega_g) = \mathrm{Res}_{\tau_r(s)}(\omega_f)$. This concludes the proof of (4.4.22). □

We have thus completed the proof of (4.4.17). This, together with (2.2.3) and (2.4.5), also gives the isomorphism (II) in the introduction.

5. Application to the theory of cyclotomic fields

5.1. THE GALOIS REPRESENTATION ON $e^*ES_p(N)_{\mathbf{Z}_p}$

In this subsection, for simplicity, we set

$$\begin{aligned} &\Lambda := \Lambda_{\mathbf{Z}_p}, \ \ \mathcal{L} := \mathcal{L}_{\mathbf{Q}_p} (= (\text{the quotient field of } \Lambda)), \\ &e\,h(N; \mathbf{Z}_p)_{\mathcal{L}} := e\,h(N; \mathbf{Z}_p) \otimes_\Lambda \mathcal{L}, \\ &e^*h^*(N; \mathbf{Z}_p)_{\mathcal{L}} := e^*h^*(N; \mathbf{Z}_p) \otimes_\Lambda \mathcal{L}. \end{aligned} \tag{5.1.1}$$

LEMMA (5.1.2). *$e^*ES_p(N)_{\mathbf{Z}_p} \otimes_\Lambda \mathcal{L}$ is a free $e^*h^*(N; \mathbf{Z}_p)_{\mathcal{L}}$-module of rank 2, and $e\,S(N; \Lambda) \otimes_\Lambda \mathcal{L}$ is a free $e\,h(N; \mathbf{Z}_p)_{\mathcal{L}}$-module of rank 1.*

Proof. The proof is standard, as follows (cf. [H3] Lemma 8.1): Let $Q := (\omega_{1,0}) = (T) \subset \Lambda$, and indicate by the subscript '$_Q$' the localization at Q. By [H3] (cf. (1.5.7) above), we know that $e^*h^*(N; \mathbf{Z}_p)/Q \xrightarrow{\sim} e^*h_2^*(\Gamma_1; \mathbf{Z}_p)$, while we also have $e^*ES_p(N)_{\mathbf{Z}_p}/Q \xrightarrow{\sim} e^*H_P^1(\Gamma_1, \mathbf{Z}_p)$, ([O2] (1.4.3)). But it is well known that $e^*H_P^1(\Gamma_1, \mathbf{Q}_p)$ is a free $e^*h_2^*(\Gamma_1; \mathbf{Q}_p)$-module of rank 2. It follows from Nakayama's lemma that there is a surjective homomorphism:

$$e^*h^*(N; \mathbf{Z}_p)_Q^{\oplus 2} \longrightarrow (e^*ES_p(N)_{\mathbf{Z}_p})_Q,$$

of $e^*h^*(N; \mathbf{Z}_p)_Q$- (and hence Λ_Q-) modules. Since the two Λ_Q-modules above are free of the same rank, the first assertion follows.

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

The second assertion can be proved in a similar manner, using that we have an isomorphism $e\,S(N;\Lambda)/Q \xrightarrow{\sim} e\,S_2(\Gamma_1;\mathbf{Z}_p)$, (cf. [O2] (2.6.1)). □

As for $e^{*\prime}ES_p(N)_{\mathbf{Z}_p}$, we moreover have the following

LEMMA (5.1.3). *$\mathfrak{A}_\infty \otimes_\Lambda \mathcal{L}$ and $\mathfrak{B}_\infty \otimes_\Lambda \mathcal{L}$ are free $e^{*\prime}h^*(N;\mathbf{Z}_p)_\mathcal{L}$-modules of rank* 1.

Proof. Actually, it is known that $\mathfrak{A}_\infty$ itself is a free $e^{*\prime}h^*(N;\mathbf{Z}_p)$-module of rank 1 ([H3], [MW2], [Ti]; cf. also Saby [Sa] Théorème 2.3.5). Then by dualities (cf. [O2] (4.3.1), (2.5.3)), we have isomorphisms $\mathfrak{B}_\infty \cong \mathrm{Hom}_\Lambda(\mathfrak{A}_\infty,\Lambda) \cong e'S(N;\Lambda)$ compatible with the action of $e^{*\prime}h^*(N;\mathbf{Z}_p) \cong e'h(N;\mathbf{Z}_p)$ $(T^*(-) \leftrightarrow T(-))$. The assertion for $\mathfrak{B}_\infty \otimes_\Lambda \mathcal{L}$ follows from the lemma above. (We could also derive this lemma from the main result of [O2].) □

By (5.1.2), fixing an $e^*h^*(N;\mathbf{Z}_p)_\mathcal{L}$-basis of $e^*ES_p(N)_{\mathbf{Z}_p} \otimes_\Lambda \mathcal{L}$, we may regard the Galois representation on $e^*ES_p(N)_{\mathbf{Z}_p}$ as

$$\begin{aligned}\rho_N : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) &\longrightarrow \mathrm{GL}_{e^*h^*(N;\mathbf{Z}_p)}(e^*ES_p(N)_{\mathbf{Z}_p})\\ &\hookrightarrow \mathrm{GL}_2(e^*h^*(N;\mathbf{Z}_p)_\mathcal{L}).\end{aligned} \tag{5.1.4}$$

Especially, we may consider the trace $\mathrm{tr}\,\rho_N(\sigma)$ and the determinant $\det\rho_N(\sigma)$, both belonging to $e^*h^*(N;\mathbf{Z}_p)_\mathcal{L}$, for each $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. The representation ρ_N is unramified outside Np by a well-known result of Igusa.

For a prime number l, we denote by Φ_l a *geometric* Frobenius at l in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ or in $\mathrm{Gal}(\overline{\mathbf{Q}}_l/\mathbf{Q}_l)$.

THEOREM (5.1.5). *If l does not divide Np, we have*

$$\det(1-\rho_N(\Phi_l)X) = 1 - T^*(l)X + lT^*(l,l)X^2.$$

Proof. The proof is also standard: First, we have the congruence relation $T^*(l) = \Phi_l + lT^*(l,l)\Phi_l^{-1}$, on $e^*ES_p(N)_{\mathbf{Z}_p}$ ([O1] (7.6.1)). There is an $\mathcal{L}$-bilinear form, denoted by $\{\ ,\ \}$ in [O2] (4.1.17), on $e^*ES_p(N)_{\mathbf{Z}_p} \otimes_\Lambda \mathcal{L}$. We know that $T^*(n)$ and $T^*(q,q)$ are self-adjoint; and that the adjoint of Φ_l is $lT^*(l,l)\Phi_l^{-1}$, with respect to this pairing ([O2] (4.2.8)). Moreover, this pairing is nondegenerate. Indeed, using the same terminology as in the proof of (5.1.2), the reduction modulo Q of $\{\ ,\ \}$ on $(e^*ES_p(N)_{\mathbf{Z}_p})_Q$ is a nondegenerate $\mathbf{Q}_p$-bilinear form, by [O2] (4.2.5). Thus the correspondence $\xi \mapsto$ (the adjoint of ξ with respect to $\{\ ,\ \}$) gives an anti-automorphism of the $e^*h^*(N;\mathbf{Z}_p)_\mathcal{L}$-algebra $\mathrm{End}_{e^*h^*(N;\mathbf{Z}_p)_\mathcal{L}}(e^*ES_p(N)_{\mathbf{Z}_p} \otimes_\Lambda \mathcal{L}) \cong M_2(e^*h^*(N;\mathbf{Z}_p)_\mathcal{L})$. Considering the regular representation on this algebra, we conclude that Φ_l and $lT^*(l,l)\Phi_l^{-1}$, viewed as elements of $\mathrm{End}_{e^*h^*(N;\mathbf{Z}_p)_\mathcal{L}}(e^*ES_p(N)_{\mathbf{Z}_p} \otimes_\Lambda \mathcal{L})$, have the same characteristic polynomial. The congruence relation above then implies that

$$\det(1-\rho_N(\Phi_l)X)^2 = (1 - T^*(l)X + lT^*(l,l)X^2)^2 \in e^*h^*(N;\mathbf{Z}_p)_\mathcal{L}[X],$$

which proves our assertion. $\square$

It follows from this and the Čebotarev density theorem that $\operatorname{tr}\rho_N$ and $\det\rho_N$ take values in $e^*h^*(N;\mathbf{Z}_p)$.

5.2. SOME PROPERTIES OF p-ADIC EISENSTEIN COHOMOLOGY CLASSES

From now on, until the end of this paper, we assume that

$$(p,\varphi(N))=1, \tag{5.2.1}$$

and fix an *even* and *primitive* Dirichlet character χ of conductor $N_1=Np$ such that

$$\chi\,|_{(\mathbf{Z}/p\mathbf{Z})^\times}=\omega^i \quad \text{with} \quad i\not\equiv 0,-1 \mod p-1. \tag{5.2.2}$$

We let $\mathfrak{r}$ be the ring generated by the values of χ over $\mathbf{Z}_p$, and $\mathfrak{k}$ its quotient field. For any $\mathfrak{r}[(\mathbf{Z}/N_1\mathbf{Z})^\times]$-module M, we mean by $M^{(\chi)}$ the maximal direct summand of M on which $(\mathbf{Z}/N_1\mathbf{Z})^\times$ acts via χ.

Recall that there are natural homomorphisms

$$\begin{aligned}\mathfrak{r}[[\mathcal{Z}_N]] &\longrightarrow e^*\mathcal{H}^*(N;\mathfrak{r}) \twoheadrightarrow e^*h^*(N;\mathfrak{r}),\\ \mathfrak{r}[[\mathcal{Z}_N]] &\longrightarrow e\,\mathcal{H}(N;\mathfrak{r}) \twoheadrightarrow e\,h(N;\mathfrak{r}).\end{aligned} \tag{5.2.3}$$

We may then consider an exact sequence

$$0\longrightarrow e^*ES_p(N)_{\mathfrak{r}}^{(\chi)}\longrightarrow e^*GES_p(N)_{\mathfrak{r}}^{(\chi)}\longrightarrow \mathcal{C}_p(N)_{\mathfrak{r}}^{(\chi)}(-1)\longrightarrow 0, \tag{5.2.4}$$

of $e^*\mathcal{H}^*(N;\mathfrak{r})^{(\chi)}$-modules as well as $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-modules. Note that $T^*(q,q)$ is equal to $\chi(q)\iota(\langle q\rangle)\in\Lambda_{\mathfrak{r}}$ in $e^*\mathcal{H}^*(N;\mathfrak{r})^{(\chi)}$ for each positive integer q prime to N_1.

DEFINITION (5.2.5). *We define the Eisenstein ideal $\mathcal{I}^*$ (resp. I^*) of $e^*\mathcal{H}^*(N;\mathfrak{r})^{(\chi)}$ (resp. $e^*h^*(N;\mathfrak{r})^{(\chi)}$) as the ideal generated by all $T^*(l)-1-\chi(l)l\iota(\langle l\rangle)$ ($l\nmid N_1$) and $T^*(l)-1$ ($l\mid N_1$) with prime numbers l. Similarly, we define the Eisenstein ideals $\mathcal{I}$ and I of $e\mathcal{H}(N;\mathfrak{r})^{(\chi)}$ and $e\,h(N;\mathfrak{r})^{(\chi)}$, respectively.*

In 2.3, we considered $\Lambda_{\mathfrak{o}}$-adic Eisenstein series. Using the same notation as in (2.3.10), we easily see that for $\mathcal{E}(\theta,\psi;c)\in e\,M(N;\Lambda_{\mathfrak{o}})$,

$$\mathcal{E}(\theta,\psi;c)\mid T(q,q)=\theta\psi(q)\iota(\langle q\rangle)\mathcal{E}(\theta,\psi;c) \quad \text{if} \quad (q,N_1)=1, \tag{5.2.6}$$

unless $\theta=\omega^{-2}$ and $\psi=\mathbf{1}$; and similarly for $((1+T)-u^{-2})\mathcal{E}(\omega^{-2},\mathbf{1};c)$. Thus $(e\,M(N;\Lambda_{\mathfrak{o}})^{(\chi)}/e\,S(N;\Lambda_{\mathfrak{o}})^{(\chi)})\otimes_{\Lambda_{\mathfrak{o}}}\mathcal{L}_K$ is spanned over $\mathcal{L}_K$ by $\mathcal{E}(\theta,\psi):=$

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

$\mathcal{E}(\theta,\psi;1)$ when θ and ψ run through the Dirichlet characters satisfying $\theta\psi = \chi$ and also the conditions in (2.3.10). For such $\Lambda_{\mathfrak{o}}$-adic Eisenstein series, we have

$$\begin{aligned}\mathcal{E}(\theta,\psi) \mid T(n) &= \left(\sum_{\substack{0<t\mid n\\ p\nmid t}} \theta(t)\psi\left(\frac{n}{t}\right) A_t(T)\right)\mathcal{E}(\theta,\psi)\\ &= \left(\sum_{\substack{0<t\mid n\\ p\nmid t}} \theta(t)\psi\left(\frac{n}{t}\right) t\iota(\langle t\rangle)\right)\mathcal{E}(\theta,\psi),\end{aligned} \tag{5.2.7}$$

for all positive integers n. It follows that there is a surjective $\Lambda_{\mathfrak{r}}$-algebra homomorphism: $e\mathcal{H}(N;\mathfrak{r})^{(\chi)} \twoheadrightarrow \Lambda_{\mathfrak{r}}$ sending $T(n)$ to

$$A_n(T,\chi) := \sum_{\substack{0<t\mid n\\ p\nmid t}} \chi(t)t\iota(\langle t\rangle) \tag{5.2.8}$$

(the eigenvalue of $\mathcal{E}(\chi,\mathbf{1})$) whose kernel is $\mathcal{I}$. Especially, $\mathcal{I}$ (resp. $\mathcal{I}^*$) is a proper ideal of $e\mathcal{H}(N;\mathfrak{r})^{(\chi)}$ (resp. $e^*\mathcal{H}^*(N;\mathfrak{r})^{(\chi)}$). Set

$$\begin{aligned}&\mathfrak{M} := (\mathcal{I},p,T); \quad \mathfrak{m} := (I,p,T),\\ &\mathfrak{M}^* := (\mathcal{I}^*,p,T); \quad \mathfrak{m}^* := (I^*,p,T),\end{aligned} \tag{5.2.9}$$

so that $\mathfrak{M}$ and $\mathfrak{M}^*$ are maximal ideals. We consider the localizations at $\mathfrak{M}^*$:

$$\begin{aligned}X &:= e^*ES_p(N)^{(\chi)}_{\mathfrak{r},\mathfrak{M}^*},\\ Y &:= e^*GES_p(N)^{(\chi)}_{\mathfrak{r},\mathfrak{M}^*},\\ Z &:= \mathcal{C}_p(N)^{(\chi)}_{\mathfrak{r},\mathfrak{M}^*}(-1).\end{aligned} \tag{5.2.10}$$

Note that $X = e^*ES_p(N)^{(\chi)}_{\mathfrak{r},\mathfrak{m}^*}$ if $\mathfrak{m}^*$, or equivalently I^*, is a proper ideal and $X = 0$ otherwise. As usual, we identify the Dirichlet characters with characters of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.

LEMMA (5.2.11). (i) *Z is a free $\Lambda_{\mathfrak{r}}$-module of rank 1, and $T^*(n)$ acts as multiplication by $A_n(T,\chi)$ on it.*

(ii) $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}(\zeta_N)) \ni \sigma$ *acts on Z as multiplication by* $(\chi\omega)^{-1}(\sigma)\langle\kappa(\sigma)\rangle^{-1}\iota(\langle\kappa(\sigma)\rangle^{-1}) \in \Lambda_{\mathfrak{r}}^{\times}$.

Proof. Since Z is a direct summand of $\mathcal{C}_p(N)_{\mathfrak{r}}(-1)$, it is a free $\Lambda_{\mathfrak{r}}$-module by (4.3.14). We want to show that $Z \otimes_{\Lambda_{\mathfrak{r}}} \mathcal{L}_{\mathfrak{k}}$ is one-dimensional over $\mathcal{L}_{\mathfrak{k}}$. Suppose otherwise.

By our main theorem, $\mathcal{C}_p(N)^{(\chi)}_{\mathfrak{o}}$ is isomorphic to $e\,M(N;\Lambda_{\mathfrak{o}})^{(\chi)}/e\,S(N;\Lambda_{\mathfrak{o}})^{(\chi)}$, and $T^*(n)$ on the former corresponds to $T(n)$ on the latter. Our assumption then implies that there is a pair $(\theta, \psi) \neq (\chi, \mathbf{1})$ as above such that $e^*\mathcal{H}^*(N; \mathfrak{r})^{(\chi)}_{\mathfrak{M}^*}$ admits a homomorphism to $\Lambda_{\mathfrak{r}'}$, sending $T^*(l)$ to $\theta(l)l\iota(\langle l\rangle) + \psi(l)$ for each prime $l \nmid N_1$, where $\mathfrak{r}'$ is the ring generated by the values of θ and ψ over $\mathfrak{r}$. Reducing modulo the maximal ideal of $\Lambda_{\mathfrak{r}'}$, we see that there is an automorphism τ of the residue field of $\mathfrak{r}$, and the congruence $(\chi\omega)^\tau(l) + 1 \equiv \theta\omega(l) + \psi(l)$ holds for all primes $l \nmid N_1$. Since $\psi \neq \mathbf{1}$, we must have $\psi \equiv (\chi\omega)^\tau$, by our assumption (5.2.1). However, the conductor of ψ was assumed to be prime to p, and this contradicts to the assumption (5.2.2). Thus, $\mathrm{rank}_{\Lambda_{\mathfrak{r}}} Z = 1$, and it is clear from the preceding argument that the action of the Hecke operators is as stated as above.

The second assertion is a direct consequence of (4.3.10). □

Now let us look at the commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & X\widehat{\otimes}_{\mathfrak{r}}\mathfrak{o} & \longrightarrow & Y\widehat{\otimes}_{\mathfrak{r}}\mathfrak{o} & \xrightarrow{\ \pi\ } & Z\widehat{\otimes}_{\mathfrak{r}}\mathfrak{o} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & e\,S(N;\Lambda_{\mathfrak{o}})^{(\chi)}_{\mathfrak{M}} & \xrightarrow[\text{can}]{} & e\,M(N;\Lambda_{\mathfrak{o}})^{(\chi)}_{\mathfrak{M}} & \xrightarrow[\text{ct}]{} & \Lambda_{\mathfrak{o}}. & &
\end{array} \qquad (5.2.12)$$

Here, the right (resp. the left) vertical arrow comes from our main theorem (resp. [O2]), and the mapping ct sends each $\mathcal{F} \in e\,M(N;\Lambda_{\mathfrak{o}})^{(\chi)}_{\mathfrak{M}}$ to its 'constant term' $a(0;\mathcal{F})$. (We have neglected the Tate twist by fixing an isomorphism: $\mathbf{Z}_p(-1) \cong \mathbf{Z}_p$.) The vertical arrows commute with the Hecke operators in the sense that $T^*(-)$ on the upper modules correspond to $T(-)$ on the lower modules.

LEMMA (5.2.13). *The notation being as above, there is an isomorphism of* $\Lambda_{\mathfrak{o}}$-*modules:* $Z\widehat{\otimes}_{\mathfrak{r}}\mathfrak{o} \xrightarrow{\sim} \Lambda_{\mathfrak{o}}$ *together with which* (5.2.12) *remains commutative.*

Proof. Clearly, $e\,S(N;\Lambda_{\mathfrak{o}})^{(\chi)}_{\mathfrak{M}}$ lies in the kernel of ct. Since the cokernels of the middle left horizontal arrows are canonically isomorphic, there is a unique $\Lambda_{\mathfrak{o}}$-homomorphism: $Z\widehat{\otimes}_{\mathfrak{r}}\mathfrak{o} \to \Lambda_{\mathfrak{o}}$ with which the resulting square commutes.

By the lemma above, it remains to show that ct is surjective. Reducing modulo (T), (2.5.1) further reduces the problem to the surjectivity of the constant term mapping: $e\,M_2(\Gamma_1;\mathfrak{o})^{(\chi)}_{\mathfrak{M}} \to \mathfrak{o}$. Here, of course, we are considering the localization $e\,M_2(\Gamma_1;\mathfrak{o})^{(\chi)}_{\mathfrak{M}}$ through $e\mathcal{H}(N;\mathfrak{r})/T \xrightarrow{\sim} e\mathcal{H}_2(\Gamma_1;\mathfrak{r})$ (1.5.7); i.e. it is the localization of $e\,M_2(\Gamma_1;\mathfrak{o})^{(\chi)}$ at the 'Eisenstein prime' of $e\mathcal{H}_2(\Gamma_1;\mathfrak{r})^{(\chi)}$.

By (4.4.22) and the argument preceding it, we know that the mapping:

$$e^*M_2^*(\Gamma_1;\mathfrak{o})^{(\chi)} \to e^*\mathfrak{o}[C_1]^{(\chi)}$$

given by $f \mapsto \mathbf{Res}(\omega_f)$ is surjective. But by (4.3.4), $e^*\mathfrak{o}[C_1]^{(\chi)}$ contains an element of the form

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

$$\frac{1}{g}\sum_{\alpha\in(\mathbf{Z}/N_1\mathbf{Z})^\times}\chi^{-1}(\alpha)\begin{bmatrix}0\\ \alpha\end{bmatrix}_{N_1}+d,$$

with $d\in D_1$, where g is the order of χ. It follows that there is an $f\in e^*M_2^*(\Gamma_1;\mathfrak{o})^{(\chi)}$ such that $\mathrm{Res}_0(\omega_f)\in\mathfrak{o}^\times$. If we set $f':=f\mid\tau_1$, then this belongs to $e\,M_2(\Gamma_1;\mathfrak{o})^{(\chi)}$, and we have $a(0;f')=\mathrm{Res}_{i\infty}(\omega_{f'})=\mathrm{Res}_0(\omega_f)\in\mathfrak{o}^\times$. On the other hand, we have: $e\mathcal{H}_2(\Gamma_1;\mathfrak{r})^{(\chi)}=e\mathcal{H}_2(\Gamma_1;\mathfrak{r})^{(\chi)}_{\mathfrak{M}}\oplus R$ with R a direct sum of local rings. Accordingly, we have a decomposition $e\,M_2(\Gamma_1;\mathfrak{o})^{(\chi)}=e\,M_2(\Gamma_1;\mathfrak{o})^{(\chi)}_{\mathfrak{M}}\oplus M$. If $f'=f_{\mathfrak{M}}+f''$ under this decomposition, then it is clear from (2.3.2) that $a(0;f'')=0$. Consequently, the constant term of $f_{\mathfrak{M}}\in e\,M_2(\Gamma_1;\mathfrak{o})^{(\chi)}_{\mathfrak{M}}$ is a unit. □

THEOREM (5.2.14). *The exact sequence*

$$0\longrightarrow X\otimes_{\Lambda_\mathfrak{r}}\mathcal{L}_\mathfrak{k}\longrightarrow Y\otimes_{\Lambda_\mathfrak{r}}\mathcal{L}_\mathfrak{k}\stackrel{\pi}{\longrightarrow}Z\otimes_{\Lambda_\mathfrak{r}}\mathcal{L}_\mathfrak{k}\longrightarrow 0,$$

uniquely splits as $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$- *and* $e^*\mathcal{H}^*(N;\mathfrak{r})^{(\chi)}_{\mathfrak{M}^*}$*-modules. If* $s\colon Z\otimes_{\Lambda_\mathfrak{r}}\mathcal{L}_\mathfrak{k}\to Y\otimes_{\Lambda_\mathfrak{r}}\mathcal{L}_\mathfrak{k}$*, gives the splitting, then we have*

$$\pi(Y\cap s(Z))=\begin{cases}G(T,\chi\omega^2)\cdot Z & \text{if }\ \chi\neq\omega^{-2},\\ Z & \text{if }\ \chi=\omega^{-2}.\end{cases}$$

Proof. We already know that the exact sequence (4.4.6) splits as $e^{*\prime}\mathcal{H}^*(N;\mathbf{Z}_p)$-modules. By our main theorem and (5.1.2), we have an isomorphism commuting with the Hecke operators in the same sense as above

$$Y\otimes_{\Lambda_\mathfrak{r}}\mathcal{L}_K\cong(e\,M(N;\Lambda_\mathfrak{o})^{(\chi)}_{\mathfrak{M}}\otimes_{\Lambda_\mathfrak{o}}\mathcal{L}_K)\oplus(e\,S(N;\Lambda_\mathfrak{o})^{(\chi)}_{\mathfrak{M}}\otimes_{\Lambda_\mathfrak{o}}\mathcal{L}_K).$$

Therefore, the common kernel of all $T^*(n)-A_n(T,\chi)$ is a one-dimensional $\mathcal{L}_K$-subspace of $Y\otimes_{\Lambda_\mathfrak{r}}\mathcal{L}_K$, which is mapped isomorphically onto $Z\otimes_{\Lambda_\mathfrak{r}}\mathcal{L}_K$. The first part of our theorem follows from this.

On the other hand, by (5.2.13), we have a commutative diagram

$$\begin{array}{ccccc}
Y\widehat{\otimes}_\mathfrak{r}\mathfrak{o} & \stackrel{\pi}{\longrightarrow} & Z\widehat{\otimes}_\mathfrak{r}\mathfrak{o} & \longrightarrow & 0\\
\downarrow & & \downarrow\wr & & \\
e\,M(N;\Lambda_\mathfrak{o})^{(\chi)}_{\mathfrak{M}} & \underset{\mathrm{ct}}{\longrightarrow} & \Lambda_\mathfrak{o} & \longrightarrow & 0,
\end{array}$$

and the left vertical arrow has a section commuting with the Hecke operators. Since $A_p(T,\chi)=1$, the image of $Y\widehat{\otimes}_\mathfrak{r}\mathfrak{o}\cap s(Z\widehat{\otimes}_\mathfrak{r}\mathfrak{o})$ in $e\,M(N,\Lambda_\mathfrak{o})^{(\chi)}_{\mathfrak{M}}$ is $\Lambda_\mathfrak{o}\cdot\mathcal{E}(\chi,\mathbf{1})$ when $\chi\neq\omega^{-2}$ and, hence, we see that $\pi(Y\widehat{\otimes}_\mathfrak{r}\mathfrak{o}\cap s(Z\widehat{\otimes}_\mathfrak{r}\mathfrak{o}))=G(T,\chi\omega^2)\cdot Z\widehat{\otimes}_\mathfrak{r}\mathfrak{o}$,

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

in this case. This proves the latter part of the theorem when $\chi \neq \omega^{-2}$. Since the 'constant term' of $((1+T) - u^{-2})\mathcal{E}(\omega^{-2}, \mathbf{1})$ is a unit in $\Lambda_{\mathbf{Z}_p}$, a similar argument implies the remaining assertion. □

COROLLARY (5.2.15). *If $\chi \neq \omega^{-2}$ and $I^* = \mathfrak{m}^* = e^*h^*(N;\mathfrak{r})^{(\chi)}$, then $G(T, \chi\omega^2) \in \Lambda_{\mathfrak{r}}$ is a unit.*

COROLLARY (5.2.16). *Suppose that $\chi \neq \omega^{-2}$ and that $\mathfrak{m}^* \neq e^*h^*(N;\mathfrak{r})^{(\chi)}$. Then there is a* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$*- and $e^*h^*(N;\mathfrak{r})^{(\chi)}_{\mathfrak{m}^*}$-submodule V of $X/G(T, \chi\omega^2)$ enjoying the following properties:*

(i) *V is isomorphic to $\Lambda_{\mathfrak{r}}/(G(T, \chi\omega^2))$ as a $\Lambda_{\mathfrak{r}}$-module.*
(ii) $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}(\zeta_N)) \ni \sigma$ *acts on V as multiplication by $(\chi\omega)^{-1}(\sigma)\langle\kappa(\sigma)\rangle^{-1}\iota(\langle\kappa(\sigma)\rangle^{-1})$.*
(iii) *$T^*(n)$ acts on V as multiplication by $A_n(T, \chi)$.*

Proof. Write U for $Y \cap s(Z)$. Then we clearly have $G(T, \chi\omega^2) \cdot Y \subseteq X + U$. Therefore, for any $y \in Y$, we can express $G(T, \chi\omega^2)y$ as $x + v$ with unique $x \in X$ and $v \in U$. The correspondence $y \mapsto x$ gives an injective homomorphism

$$Y/(X+U) \hookrightarrow X/G(T, \chi\omega^2).$$

On the other hand, π induces an isomorphism

$$Y/(X+U) \xrightarrow{\sim} Z/\pi(U) \cong \Lambda_{\mathfrak{r}}/(G(T, \chi\omega^2)).$$

The action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}(\zeta_N))$ (resp. the Hecke operators) on $Z/\pi(U)$ is as stated in (ii) (resp. (iii)) by (5.2.11). □

COROLLARY (5.2.17) (cf. Wiles [Wi] Theorem 4.1). *Under the same assumption as above, there is a surjective $\Lambda_{\mathfrak{r}}$-algebra homomorphism $e^*h^*(N;\mathfrak{r})^{(\chi)}_{\mathfrak{m}^*}/I^* \twoheadrightarrow \Lambda_{\mathfrak{r}}/(G(T, \chi\omega^2))$, sending each $T^*(n)$ to $A_n(T, \chi)$.*

5.3. MODULAR CONSTRUCTION OF UNRAMIFIED ABELIAN p-EXTENSIONS

In this final subsection, we follow the method of Harder and Pink [HP] (cf. also Kurihara [Ku]). We keep the notation and the assumption of 5.2 and, moreover, assume that $\chi \neq \omega^{-2}$ and $\mathfrak{m}^* \neq e^*h^*(N;\mathfrak{r})^{(\chi)}$ (otherwise the situation is uninteresting to us in view of (5.2.15); cf. also (5.3.19) below). We henceforth write

$$\mathfrak{h}^* := e^*h^*(N;\mathfrak{r})^{(\chi)}_{\mathfrak{m}^*} \tag{5.3.1}$$

for the simplicity of notation. We now look into the Galois representation

$$\rho\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_{\mathfrak{h}^*}(X) \hookrightarrow \mathrm{GL}_2(\mathfrak{h}^* \otimes_{\Lambda_{\mathfrak{r}}} \mathcal{L}_{\mathfrak{k}}). \tag{5.3.2}$$

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

We already know that

$$\det \rho(\sigma) = (\chi\omega)^{-1}(\sigma)\langle\kappa(\sigma)\rangle^{-1}\iota(\langle\kappa(\sigma)\rangle^{-1}), \tag{5.3.3}$$

by (5.1.5).

Set

$$X_+ := X^{I_p}. \tag{5.3.4}$$

Then I_p acts on X/X_+ via the character: $\sigma \mapsto \omega^{-i-1}(\sigma)\langle\kappa(\sigma)\rangle^{-1}\iota(\langle\kappa(\sigma)\rangle^{-1})$ by (4.4.4), and this action factors through $\mathrm{Gal}(\mathbf{Q}(\mu_{p^\infty})/\mathbf{Q}) = \delta \times \mathrm{Gal}(\mathbf{Q}(\mu_{p^\infty})/\mathbf{Q}(\mu_p))$ with $\delta \cong \mathrm{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q})$. δ thus acts on X/X_+ through the nontrivial character ω^{-i-1}. Take and fix a $\sigma_0 \in I_p$ such that $\xi := \omega^{-i-1}(\sigma_0)$ is a nontrivial $(p-1)$st root of unity. We let X_- be the ξ-eigenspace of X with respect to the action of σ_0, so that we have a direct sum decomposition:

$$X = X_- \oplus X_+, \tag{5.3.5}$$

of $\mathfrak{h}^*$-modules.

By (5.1.3), $X_- \otimes_{\Lambda_\mathfrak{r}} \mathcal{L}_\mathfrak{k}$ and $X_+ \otimes_{\Lambda_\mathfrak{r}} \mathcal{L}_\mathfrak{k}$ are free $\mathfrak{h}^* \otimes_{\Lambda_\mathfrak{r}} \mathcal{L}_\mathfrak{k}$-modules of rank 1. We can therefore express ρ 'matricially' as

$$\rho(\sigma) = \begin{bmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{bmatrix}, \tag{5.3.6}$$

with $a(\sigma) \in \mathrm{End}_{\mathfrak{h}^*}(X_-) \hookrightarrow \mathfrak{h}^* \otimes_{\Lambda_\mathfrak{r}} \mathcal{L}_\mathfrak{k}$ and $d(\sigma) \in \mathrm{End}_{\mathfrak{h}^*}(X_+) \hookrightarrow \mathfrak{h}^* \otimes_{\Lambda_\mathfrak{r}} \mathcal{L}_\mathfrak{k}$, etc. Note that $a(\sigma), d(\sigma)$ and $b(\sigma)c(\sigma') \in \mathfrak{h}^* \otimes_{\Lambda_\mathfrak{r}} \mathcal{L}_\mathfrak{k}$ are independent of the choice of the basis. Note also that we have

$$\rho(\sigma) = \begin{bmatrix} \det \rho(\sigma) & 0 \\ * & 1 \end{bmatrix} \quad \text{if } \sigma \in I_p. \tag{5.3.7}$$

To apply the method of Harder and Pink, it is convenient to consider an auxiliary ideal J^* of $\mathfrak{h}^*$ which is, by definition, generated by $T^*(l) - 1 - \chi(l)l\iota(\langle l\rangle)$ for all prime numbers l prime to Np. By the definition of X_-, $\rho(I_p)$ contains an element $\begin{bmatrix} \xi & 0 \\ 0 & 1 \end{bmatrix}$ with a nontrivial $(p-1)$st root of unity ξ. Using (5.1.5), one can then prove the following two lemmas in the same way as in [HP] 3.1.4 and 3.1.5. See also [Ku] Section 3 for a similar argument.

LEMMA (5.3.8). *For any* $\sigma, \sigma' \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, $a(\sigma) - \det \rho(\sigma)$, $d(\sigma) - 1$ *and* $b(\sigma)c(\sigma')$ *belong to* J^*.

LEMMA (5.3.9). J^* *is generated by either* $\{a(\sigma) - \det \rho(\sigma) \mid \sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})\}$ *or* $\{d(\sigma) - 1 \mid \sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})\}$.

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

Let

$$B \subseteq \mathrm{Hom}_{\mathfrak{h}^*}(X_+, X_-), \qquad C \subseteq \mathrm{Hom}_{\mathfrak{h}^*}(X_-, X_+), \tag{5.3.10}$$

be the $\mathfrak{h}^*$-*submodules* generated by all $b(\sigma)$ or $c(\sigma)$, respectively. We may consider BC as an ideal of $\mathfrak{h}^*$ contained in J^*. Let $\tilde{a}(\sigma), \tilde{d}(\sigma) \in \mathfrak{h}^*/BC$ and $\tilde{b}(\sigma) \in B/(BC)B$ be the elements obtained from $a(\sigma)$ etc. by reducing modulo BC. Then we can define *representations* of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ by

$$\varphi_1(\sigma) := \begin{bmatrix} \tilde{a}(\sigma) & \tilde{b}(\sigma) \\ 0 & \tilde{d}(\sigma) \end{bmatrix}, \qquad \varphi_2(\sigma) := \begin{bmatrix} \tilde{a}(\sigma) & 0 \\ 0 & \tilde{d}(\sigma) \end{bmatrix}. \tag{5.3.11}$$

LEMMA (5.3.12). *We have* $\tilde{a}(\sigma) = \det \rho(\sigma) \bmod BC$, *and* $\tilde{d}(\sigma) = 1$, *for all* $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.

Proof. $\tilde{d}$ is a homomorphism of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ to $(\mathfrak{h}^*/BC)^\times$ unramified outside N, by (5.3.7). Let A be the field corresponding to its kernel. Since the kernel of the homomorphism: $(\mathfrak{h}^*/BC)^\times \twoheadrightarrow (\mathfrak{h}^*/\mathfrak{m}^*)^\times$ is a pro-p group, it follows from class field theory that the composite of $\mathrm{Gal}(A/\mathbf{Q}) \hookrightarrow (\mathfrak{h}^*/BC)^\times \to (\mathfrak{h}^*/\mathfrak{m}^*)^\times$ is still injective. It is thus enough to show that $d(\sigma) \equiv 1 \bmod \mathfrak{m}^*$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.

But by (5.1.5) and the Čebotarev density theorem, we see that

$$a(\sigma) + d(\sigma) \equiv 1 + (\chi\omega)^{-1}(\sigma) \mod \mathfrak{m}^*.$$

Since $(\chi\omega)^{-1}$ ramifies at p by (5.2.2), we must have $d(\sigma) \equiv 1 \bmod \mathfrak{m}^*$. □

From this and (5.3.9), we obtain

COROLLARY (5.3.13). $BC = J^*$.

For $l \nmid Np$, $T^*(l) - 1 - \chi(l)l\iota(\langle l\rangle) \in J^*$ is not a zero divisor in $\mathfrak{h}^*$, and hence we have:

COROLLARY (5.3.14). *B and C are faithful $\mathfrak{h}^*$-modules.*

Reducing φ_1 and φ_2 modulo I^*, we obtain the representations

$$\psi_1(\sigma) := \begin{bmatrix} \overline{\det \rho}(\sigma) & \bar{b}(\sigma) \\ 0 & 1 \end{bmatrix}, \qquad \psi_2(\sigma) := \begin{bmatrix} \overline{\det \rho}(\sigma) & 0 \\ 0 & 1 \end{bmatrix} \tag{5.3.15}$$

with $\bar{b}(\sigma) = b(\sigma) \bmod I^*B$, etc. Let K and k be the subfields of $\overline{\mathbf{Q}}$ corresponding to the kernels of ψ_1 and ψ_2, respectively. By (5.3.7), p does not ramify in the extension K/k. Let F be the field corresponding to $\chi\omega$, and F_∞ the cyclotomic $\mathbf{Z}_p$-extension

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

of F. Then it is easy to see that: $F_\infty \supseteq k \supseteq F$. Since p totally ramifies in F_∞/F, $\mathrm{Gal}(K/k)$ is isomorphic to $\mathrm{Gal}(K_\infty/F_\infty)$ if we set

$$K_\infty := K \cdot F_\infty. \tag{5.3.16}$$

As usual, we have a direct product decomposition:

$$\mathrm{Gal}(F_\infty/\mathbf{Q}) = \Delta \times \Gamma, \tag{5.3.17}$$

with $\Delta \cong \mathrm{Gal}(F/\mathbf{Q})$ and $\Gamma = \mathrm{Gal}(F_\infty/F)$. We fix a topological generator γ_0 of Γ, and define $u \in U_1$ by $u := \langle\kappa(\gamma_0)\rangle$. This is meaningful because the character $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \ni \sigma \mapsto \langle\kappa(\sigma)\rangle$ factors through $\mathrm{Gal}(F_\infty/\mathbf{Q})$. We identify Γ with U_1 via the correspondence $\gamma_0 \leftrightarrow u$ and, hence, $\mathfrak{r}[[\Gamma]]$ with $\Lambda_\mathfrak{r}$. Also as usual, $\mathrm{Gal}(F_\infty/\mathbf{Q})$ acts on $\mathrm{Gal}(K_\infty/F_\infty)$ via the conjugation. The matrix computation

$$\begin{bmatrix} \det\rho(\sigma) & * \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & b(\sigma') \\ 0 & 1 \end{bmatrix}\begin{bmatrix} \det\rho(\sigma) & * \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & \det\rho(\sigma)b(\sigma') \\ 0 & 1 \end{bmatrix},$$

shows that Δ (resp. Γ) acts on $\mathrm{Gal}(K_\infty/F_\infty) \hookrightarrow B/I^*B$ via $(\chi\omega)^{-1}$ (resp. $\gamma \mapsto \langle\kappa(\gamma)\rangle^{-1}\iota(\langle\kappa(\gamma)\rangle^{-1})$).

LEMMA (5.3.18). *The mapping $\sigma \mapsto \bar{b}(\sigma)$ gives an isomorphism of* $\mathrm{Gal}(K/k)$ *onto B/I^*B.*

Proof. We only need to prove the surjectivity of this mapping. As we noted above, $\psi_1(I_p)$ contains $\left[\begin{smallmatrix} \xi & 0 \\ 0 & 1 \end{smallmatrix}\right]$ with a nontrivial $(p-1)$st root of unity ξ. Thus, for any $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, considering the commutator of $\psi_1(\sigma)$ with this element, we see that $\bar{b}(\sigma)$ is contained in the image.

On the other hand, we have seen above that the image is a $\Lambda_\mathfrak{r}$-submodule of B/I^*B. Since $\mathfrak{h}^*/I^*$ is isomorphic to a quotient ring of $\Lambda_\mathfrak{r}$, the image must coincide with B/I^*B. □

In general, for a finitely generated $\Lambda_\mathfrak{r}$-module M, we denote by $\mathrm{char}_{\Lambda_\mathfrak{r}}(M)$ its characteristic ideal.

THEOREM (5.3.19). *The notation and the assumption being as above, K_∞ is an unramified Abelian p-extension of F_∞ satisfying* $\mathrm{char}_{\Lambda_\mathfrak{r}}(\mathrm{Gal}(K_\infty/F_\infty)) \subseteq (F(T,\chi\omega^2))$. (See 2.3 for the right-hand side.)

Proof. We have already seen that K_∞/F_∞ is unramified outside N. That it is unramified at the primes dividing N is contained in the proof of [Wi] Lemma 6.1.

We now claim that $\mathrm{char}_{\Lambda_\mathfrak{r}}(B/I^*B) \subseteq (G(T,\chi\omega^2))$, where we view B/I^*B as a $\Lambda_\mathfrak{r}$-module through $\Lambda_\mathfrak{r} \to \mathfrak{h}^*$ as before. In fact, let $\mathfrak{a}$ be the ideal of $\Lambda_\mathfrak{r}$ such that $\mathfrak{h}^*/I^* \cong \Lambda_\mathfrak{r}/\mathfrak{a}$. Then, using (5.3.14) and (5.2.17), it is easy to see that the Fitting ideal of the $\Lambda_\mathfrak{r}$-module B/I^*B satisfies $\mathrm{Fitt}_{\Lambda_\mathfrak{r}}(B/I^*B) \subseteq \mathfrak{a} \subseteq (G(T,\chi\omega^2))$. This together with the Ferrero–Washington theorem implies our claim. (See Mazur and Wiles [MW1] Appendix for the general facts about Fitting ideals; cf. also [Wi] Section 6.)

By (5.3.18) and the remark preceding it, if we consider $\mathrm{Gal}(K_\infty/F_\infty)$ as a $\mathfrak{r}[[\Gamma]]$-module Iwasawa theoretically, then its characteristic ideal is obtained from the above by the change of variable: $T \mapsto u^{-1}(1+T)^{-1} - 1$. Our theorem follows from Definition (2.3.5) of $G(T, \chi\omega^2)$. □

Let L_∞ be the maximal unramified Abelian p-extension of F_∞, and L'_∞ its subextension whose Galois group over F_∞ is the '$(\chi\omega)^{-1}$-part' (cf. [MW1] page 192) of $\mathrm{Gal}(L_\infty/F_\infty)$.

COROLLARY (5.3.20). $K_\infty = L'_\infty$.

Proof. It is clear that $L'_\infty \supseteq K_\infty$. On the other hand, the Mazur–Wiles theorem (the Iwasawa main conjecture) says that $\mathrm{char}_{\Lambda_\mathfrak{r}}(\mathrm{Gal}(L'_\infty/F_\infty)) = (F(T, \chi\omega^2))$. The theorem above then implies that the natural homomorphism: $\mathrm{Gal}(L'_\infty/F_\infty) \twoheadrightarrow \mathrm{Gal}(K_\infty/F_\infty)$ is a pseudo-isomorphism. The conclusion follows from the well-known fact that $\mathrm{Gal}(L'_\infty/F_\infty)$ has no nontrivial finite $\Lambda_\mathfrak{r}$-submodules (cf. [Wa] Proposition 13.28). □

This in turn gives us the following

COROLLARY (5.3.21). *$\mathfrak{h}^*/I^*$ is isomorphic to $\Lambda_\mathfrak{r}/(G(T, \chi\omega^2))$.*

Proof. From the argument above, we know that B/I^*B has no nontrivial finite $\Lambda_\mathfrak{r}$-submodules; and hence its Fitting ideal coincides with the characteristic ideal ([MW1] Appendix, Corollary to Proposition 2). Thus the ideal $\mathfrak{a}$ in the proof of (5.3.19) is equal to $(G(T, \chi\omega^2))$. □

In the proof of the last two corollaries, we employed the Mazur–Wiles theorem. As a final remark, we note that our theorem (5.3.19) can be used to give a simple proof of this theorem for $\chi = \omega^i$ with i even. Indeed, it is enough to guarantee the existence of an extension K_∞ as in (5.3.19) for each $\chi = \omega^i \neq \omega^{-2}$ as above. In the case excluded from our argument, i.e. when $\chi = \mathbf{1}$, this is trivial because

$$F(0, \omega^2) = -B_{1,\omega} \equiv -\frac{B_2}{2} = -\frac{1}{12} \mod p$$

and, hence, $F(T, \omega^2)$ is a unit power series.

https://doi.org/10.1023/A:1000556212097 Published online by Cambridge University Press

References

[AS] Ash, A. and Stevens, G.: p-adic deformations of cohomology classes of subgroups of $\mathrm{GL}(n, \mathbb{Z})$, to appear in *Proc. Journées Arithmétiques 1995, Barcelone*.

[BLR] Bosch, S., Lütkebohmert, W. and Raynaud, M.: *Néron Models*, Ergebnisse der Math. 3, Folge 21, Springer-Verlag, 1990.

[D] Deligne, P.: Intégration sur un cycle évanescent, *Invent. Math.* 76 (1983), 129–143.

[HP] Harder, G. and Pink, R.: Modular konstruierte unverzweigte abelshe p-Erweiterungen von $\mathbb{Q}(\zeta_p)$ und die Struktur ihrer Galoisgruppen, *Math. Nachr.* 159 (1992), 83–99.

[H1] Hida, H.: A p-adic measure attached to the zeta functions associated with two elliptic modular forms. I, *Invent. Math.* 79 (1985), 159–195.

[H2] Hida, H.: Iwasawa modules attached to congruences of cusp forms, *Ann. Sci. École. Norm. Sup. (4)* 19 (1986), 231–273.

[H3] Hida, H.: Galois representations into $\mathrm{GL}_2(\mathbf{Z}_p[[X]])$ attached to ordinary cusp forms, *Invent. Math.* 85 (1986), 543–613.

[H4] Hida, H.: *Elementary Theory of L-functions and Eisenstein Series*, London Math. Soc. Stud. Texts 26, Cambridge Univ. Press, 1993.

[Ka1] Katz, N.: p-adic interpolation of real analytic Eisenstein series, *Ann. Math.* 104 (1976), 459–571.

[Ka2] Katz, N.: The Eisenstein measure and p-adic interpolation, *Amer. J. Math.* 99 (1977), 238–311.

[Ku] Kurihara, M.: Ideal class groups of cyclotomic fields and modular forms of level 1, *J. Number Theory* 45 (1993), 281–294.

[M] Mazur, B.: Rational isogenies of prime degree, *Invent. Math.* 44 (1978), 129–162.

[MW1] Mazur, B. and Wiles, A.: Class fields of abelian extensions of $\mathbb{Q}$, *Invent. Math.* 76 (1984), 179–330.

[MW2] Mazur, B. and Wiles, A.: On p-adic analytic families of Galois representations, *Compositio Math.* 59 (1986), 231–264.

[O1] Ohta, M.: On cohomology groups attached to towers of algebraic curves, *J. Math. Soc. Japan* 45 (1993), 131–183.

[O2] Ohta, M.: On the p-adic Eichler–Shimura isomorphism for Λ-adic cusp forms, *J. reine angew. Math.* 463 (1995), 49–98.

[Sa] Saby, N.: Théorie d'Iwasawa géométrique: un théorème de comparaison, *J. Number Theory* 59 (1996), 225–247.

[Se] Serre, J.-P.: *Groupes algébriques et corps de classes*, Hermann, Paris, 1959.

[Sh] Shimura, G.: *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten and Princeton Univ. Press, 1971.

[Ta] Tate, J.: p-divisible groups, in *Proc. Conf. on Local Fields*, Springer-Verlag, 1967, pp. 158–183.

[Ti] Tilouine, J.: Un sous groupe p-divisible de la jacobienne de $X_1(Np^r)$ comme module sur l'algèbre de Hecke, *Bull. Soc. Math. Fr.* 115 (1987), 329–360.

[Wa] Washington, L.: *Introduction to Cyclotomic Fields*, Graduate Texts in Math. 83, Springer-Verlag, 1982.

[Wi] Wiles, A.: The Iwasawa conjecture for totally real fields, *Ann. Math.* 131 (1990), 493–540.

[SGA4] *Théorie des Topos et Cohomologie Étale des Schémas, Tome 3*, dir. par M. Artin, A. Grothendieck et J. L. Verdier, Lecture Notes in Math. 305, Springer-Verlag, 1973.

[SGA$4^{1/2}$] *Séminaire de Géométrie Algébrique du Bois-Marie SGA* $4^{1/2}$, par P. Deligne *et al.*, Lecture Notes in Math. 569, Springer-Verlag, 1977.

Corrections to [O2]

Page 72, line 11: $e\,S_k(N;\mathfrak{o})$ should be $e\,S_k(N;\Lambda_{\mathfrak{o}})$.
Page 83, line 1: There, I quoted the formula of $T^*(p)$ in characteristic p from [MW1]. However, the models of our X_r are different from those in [MW1]; and it should be replaced by the formula given in [Sa] Théorème 2.2.3. The rest of the argument remains valid.