Invent. math. 85, 545-613 (1986)

Inventiones mathematicae

Galois representations into $\mathrm{GL}_2(\mathbf{Z}_p[[X]])$ attached to ordinary cusp forms

Haruzo Hida

Department of Mathematics, Hokkaido University, Sapporo 060, Japan

§ 0. Introduction

Parabolic cohomology groups of congruence subgroups of $\mathrm{SL}_2(\mathbf{Z})$ have been utilized as an effective tool in the study of (i) the Hecke algebras on the space of cusp forms, (ii) the Galois representations of cusp forms, and (iii) the special values of their zeta functions. The utility of this type of cohomology groups was first found by Eichler, and their arithmetic applications have been chiefly studied by Shimura (e.g. [20, 23, 24 and 25, ch. 8]; see also Ohta [17]). In the present paper, we shall study these three subjects in the framework of p-adic modular forms and their Hecke algebras. We shall deduce all the main results of this paper from a key theorem (Theorem 3.1) on the structure of the parabolic cohomology groups of $\Gamma_1(Np^r)$ for a fixed prime p. Assume throughout the paper that $p \geqq 5$. We have defined in our previous paper [13] an universal Hecke algebra $\mathscr{h}(N;\mathbf{Z}_p)$, for each positive integer N prime to p, as a subalgebra of the endomorphism algebra of the space of p-adic cusp forms of level N, topologically generated by Hecke operators. Then, the ordinary part $\mathscr{h}^0(N;\mathbf{Z}_p)$ of $\mathscr{h}(N;\mathbf{Z}_p)$ is proven to be finite and flat over the Iwasawa algebra $\Lambda=\mathbf{Z}_p[[X]]$ of the topological group $\Gamma=1+p\mathbf{Z}_p$. Let Ω be a p-adic completion of an algebraic closure of $\mathbf{Q}_p$. Then the evaluation of power series in Λ at the point $\varepsilon(u)u^k-1$ $(u=1+p\in\Gamma)$ gives an algebra homomorphism of Λ into Ω for each finite order character ε of Γ into $\Omega^\times$ and for each integer k. Let $P_{k,\varepsilon}$ be the prime ideal of Λ which is the kernel of this morphism. We denote by $\bar{\mathbf{Q}}$ the algebraic closure of $\mathbf{Q}$ in $\mathbf{C}$ and we fix throughout this paper an embedding of $\bar{\mathbf{Q}}$ into Ω. We shall take an irreducible component of $\mathscr{h}^0(N;\mathbf{Z}_p)$. This is equivalent to fixing a (non-trivial) Λ-algebra homomorphism λ of $\mathscr{h}^0(N;\mathbf{Z}_p)$ into an integral domain finite over Λ. For simplicity, suppose that $N=1$ and that λ is a morphism of $\mathscr{h}^0(1;\mathbf{Z}_p)$ into Λ itself. We denote by $A(n;X)\in\Lambda$ the image of the Hecke operator $T(n)$ under λ. Define a formal q-expansion by

$$f_{k,\varepsilon}=\sum_{n=1}^{\infty} A(n;\varepsilon(u)u^k-1)q^n \qquad (u=1+p)$$

for each finite order character ε: $\Gamma\to\Omega$ and for each integer k. When ε is trivial, we write simply f_k for $f_{k,\varepsilon}$. Then, the first main result is

Theorem I. *For each integer $k\geqq 2$, $f_{k,\varepsilon}$ gives a complex q-expansion of a common eigenform of all Hecke operators $T(n)$ in $S_k(\Gamma_1(p^r))$ where r is defined by* $\mathrm{Ker}(\varepsilon)=1+p^r\mathbf{Z}_p$ (Corollary 1.3).

This means that the value $A(n;\varepsilon(u)u^k-1)$ is in fact an algebraic number in Ω, and if one considers it as a complex number, then it gives the n-th q-expansion coefficient of the modular form. This generalizes the result in [13, Cor. 3.7] and is deduced from structure theorems (Theorems 1.1 and 1.2 in the text) of the universal Hecke algebra. We note that $f_{k,\varepsilon}$ is minimal; namely, it is not a twist by any Dirichlet character of any modular form of smaller level than that of f (see the remark after Cor. 10.2 in the text). In particular, $f_{k,\varepsilon}$ is *not* a twist of f_k by ε.

As already shown by Deligne [4], one can attach to $f_{k,\varepsilon}$ an irreducible Galois representations $\pi(f_{k,\varepsilon})$ of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ into $\mathrm{GL}_2(\Omega)$. Then the main result as for the Galois representations is

Theorem II. *One can attach to λ a unique Galois representation $\pi(\lambda)$ of* $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ *into* $\mathrm{GL}_2(\Lambda)$ *such that the reduction of $\pi(\lambda)$ modulo $P_{k,\varepsilon}$ is equivalent to $\pi(f_{k,\varepsilon})$ for each integer $k\geqq 2$ and for each character ε of Γ* (Theorem 2.1).

Let $\tilde{\pi}(f_{k,\varepsilon})$ be the contragredient representation of $\pi(f_{k,\varepsilon})$. It is then well known that in the tensor product $\pi(f_{k,\varepsilon})\otimes\tilde{\pi}(f_{k,\varepsilon})$, there is a unique three dimensional subrepresentation $\hat{\pi}(f_{k,\varepsilon})$: $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})\to\mathrm{GL}_3(\Omega)$. Then, we can define the L-function $D(s,f_{k,\varepsilon})$ attached to this Galois representation $\hat{\pi}(f_{k,\varepsilon})$ in a standard manner. It is shown by Shimura [22] that $D(s,f_{k,\varepsilon})$ is holomorphic at $s=k$ and is proven by Gelbart and Jacquet [7] that this L-function is associated with an automorphic representation of GL(3), which is the base change lift of the representation of GL(2) corresponding to $f_{k,\varepsilon}$. On the other hand, in [13, (3.9b)], we have defined Iwasawa modules $\mathscr{C}$ and $\mathscr{N}_s$, associated with λ, with the properties that $\mathscr{C}$ is isomorphic to $\Lambda/H\Lambda$ with a non-trivial power series $H(X)\in\Lambda$ and $\mathscr{N}_s$ is pseudo-null. The module $\mathscr{N}_s$ is conjectured to be null and its vanishing can be shown under not so restrictive conditions (cf. [13, Prop. 3.9]). In §10, we shall define a canonical transcendental factor $U_\infty(k,\varepsilon)\in\mathbf{C}^\times$ of the special value $D(k,f_{k,\varepsilon})$. The main result as for the value $D(k,f_{k,\varepsilon})$ is

Theorem III. *If the character of f_2 is non-trivial and $\mathscr{N}_s=0$, then we can find a p-adic unit $U_p(2,\varepsilon)\in\Omega$ such that*

$$D(2,f_{2,\varepsilon})/U_\infty(2,\varepsilon)\,U_p(2,\varepsilon)=H(\varepsilon(u)u^2-1) \qquad (u=1+p\in\Gamma)$$

for each finite order character ε of Γ (Corollary 10.6).

In fact, we shall prove in §10 the equality of p-adic absolute values:

$$|H(\varepsilon(u)u^2-1)|_p=|D(2,f_{2,\varepsilon})/U_\infty(2,\varepsilon)|_p.$$

Thus our method gives only the existence of the p-adic unit $U_p(2,\varepsilon)$ dependent upon the choice of the power series H (up to unit factors in Λ), and the nature of $U_p(2,\varepsilon)$ remains unclear yet. The same type of assertion as Theorem III is expected to be true for all pairs (k,ε) with $k \geqq 2$, and we shall prove this for much more general k in the text when ε is trivial. As is clear from these results, the Hecke algebras, the Galois representations of modular forms and the zeta function of the Galois representation intertwine each other mysteriously. The clarification of the reason of this interaction may lead us to a non-abelian generalization of Iwasawa's theory (for cyclotomic fields).

Contents

Notations

We shall use the notation introduced in our previous papers [12] and [13]. Especially, for any congruence subgroup Δ of $\mathrm{SL}_2(\mathbf{Z})$, we denote by $\mathscr{M}_k(\Delta)$ (resp. $S_k(\Delta)$) the space of holomorphic modular forms (resp. holomorphic cusp forms) for Δ. If ψ is a character of Δ such that $\mathrm{Ker}(\psi)$ is again a congruence subgroup, we put

$$\mathscr{M}_k(\Delta,\psi)=\{f\in\mathscr{M}_k(\mathrm{Ker}(\psi))\,\big|\, f|_k\gamma=\psi(\gamma)f \text{ for } \gamma\in\Delta\},$$

and

$$S_k(\Delta,\psi)=S_k(\mathrm{Ker}(\psi))\cap\mathscr{M}_k(\Delta,\psi),$$

where $\left(f_k\middle|\begin{pmatrix} a & b \\ c & d\end{pmatrix}\right)(z)=f\left(\frac{az+b}{cz+d}\right)(cz+d)^{-k}$. Each element f of $\mathscr{M}_k(\Delta)$ has a Fourier expansion of the form:

$$f=\sum_{n=0}^{\infty} a\left(\frac{n}{M},f\right)\exp(2\pi i n z/M)$$

for a suitable integer $M>0$. When one can take 1 as M (for example, when $\Delta = \Gamma_1(N)$ or $\Gamma_0(N)$ for an integer $N>0$), we write $q=\exp(2\pi i z)$ and the Fourier expansion of f written as $\sum_{n=0}^{\infty} a(n,f)q^n$ will be called the q-expansion of f. For any subring A of $\mathbf{C}$, we put

$$\mathcal{M}_k(\Delta;A)=\left\{f\in\mathcal{M}_k(\Delta)\,\middle|\,a\left(\frac{n}{M},f\right)\in A \text{ for all } n\right\},$$

$$\mathcal{M}_k(\Delta,\psi;A)=\mathcal{M}_k(\mathrm{Ker}(\psi);A)\cap\mathcal{M}_k(\Delta,\psi)$$

$$S_k(\Delta;A)=\mathcal{M}_k(\Delta;A)\cap S_k(\Delta)$$

and

$$S_k(\Delta,\psi;A)=\mathcal{M}_k(\Delta,\psi;A)\cap S_k(\mathrm{Ker}(\psi)).$$

We write Ω for the p-adic completion of an algebraic closure of $\mathbf{Q}_p$ and throughout this paper, we fix an embedding: $\bar{\mathbf{Q}}\hookrightarrow\Omega$. Thus, the algebraic closure $\bar{\mathbf{Q}}$ of $\mathbf{Q}$ in $\mathbf{C}$ is also considered as a subfield of Ω. Any extension of $\mathbf{Q}_p$ will be considered in Ω.

The normalized p-adic absolute value of $x\in\Omega$ is denoted by $|x|_p$ $\left(\text{the normalization means that } |p|_p=\frac{1}{p}\right)$.

§ 1. Results on the Hecke algebras for ordinary forms

We begin by recalling the definitions of spaces of p-adic modular forms given in [12, §4] and [13, §1]. Let $p\geqq 5$ be a prime number and fix a positive integer N prime to p. For each power series $f=\sum_{n=0}^{\infty}a(n,f)q^n$ with coefficients in Ω, we define its p-adic norm by

$$|f|_p=\operatorname*{Sup}_n|a(n,f)|_p. \tag{1.1}$$

Especially we can speak of the norm of each modular form f in $\mathcal{M}_k(\Gamma_1(Np^r);\bar{\mathbf{Q}})$ through its q-expansion (see Notation for the symbols without any definition). Then the norm $|f|_p$ is known to be finite. Take a subfield K_0 of $\bar{\mathbf{Q}}$ and let K be the closure of K_0 in Ω. Let ψ: $\mathbf{Z}\to K_0$ be a Dirichlet character modulo Np^r $(0\leqq r\in\mathbf{Z})$ with values in K_0. Put, for each integer $r\geqq 0$,

$$\mathcal{M}_k(\Gamma_1(Np^r);K)=\mathcal{M}_k(\Gamma_1(Np^r);K_0)\otimes_{K_0}K,$$

$$S_k(\Gamma_1(Np^r);K)=S_k(\Gamma_1(Np^r);K_0)\otimes_{K_0}K,$$

$$\mathcal{M}_k(\Gamma_0(Np^r),\psi;K)=\mathcal{M}_k(\Gamma_0(Np^r),\psi;K_0)\otimes_{K_0}K,$$

$$S_k(\Gamma_0(Np^r),\psi;K)=S_k(\Gamma_0(Np^r),\psi;K_0)\otimes_{K_0}K.$$

Then these spaces are finite dimensional and are independent of the choice of the dense subfield K_0 of K. By definition, each element f of $\mathcal{M}_k(\Gamma_1(Np^r);K)$ has a unique q-expansion, which will be written as $\sum_{n=0}^{\infty}a(n,f)q^n\in K[[q]]$. Conversely, f is uniquely determined by its q-expansion. More generally, for each congruence subgroup Φ of $\mathrm{SL}_2(\mathbf{Z})$ and for each character ψ of Φ whose kernel is also a congruence subgroup, the spaces $\mathcal{M}_k(\Phi,\psi;K)$ and $S_k(\Phi,\psi;K)$ can be defined. For example, we will later deal with the group $\Phi_r^1 = \Gamma_1(Np) \cap \Gamma_0(p^r)$ and a character of Φ_r^1 given as follows: Let $\Gamma = 1 + p\mathbf{Z}_p$ be the subgroup of $\mathbf{Z}_p^\times$ consisting of p-adic units congruent to 1 modulo p. For each character ε of Γ modulo p^r, one can define a character of Φ_r^1 by putting $\varepsilon\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \varepsilon(d)$ for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Phi_r^1$. Of course, the space $\mathscr{M}_k(\Phi_r^1, \varepsilon; \Omega)$ can be further decomposed into the sum of the spaces of usual "Neben typus" $\mathscr{M}_k(\Gamma_0(Np^r), \psi; \Omega)$ over Dirichlet characters ψ modulo Np^r with $\psi|_\Gamma = \varepsilon$.

Let $Z = \mathbf{Z}_p^\times \times (\mathbf{Z}/N\mathbf{Z})^\times$ and write each element $z \in Z$ as $z = (z_p, z_0)$ for $z_p \in \mathbf{Z}_p^\times$ and $z_0 \in (\mathbf{Z}/N\mathbf{Z})^\times$. We let the topological group Z act on $\mathscr{M}_k(\Gamma_1(Np^r); \Omega)$ as follows: Choose an element $\sigma_z \in \mathrm{SL}_2(\mathbf{Z})$ so that $\sigma_z \equiv \begin{pmatrix} * & * \\ 0 & z \end{pmatrix} \bmod Np^r$, and define

$$f|z = z_p^k (f|_k \sigma_z) \qquad \text{for } f \in \mathscr{M}_k(\Gamma_1(Np^r); \Omega).$$

Any integer l prime to Np can be naturally considered as an element of Z. For each prime l, the Hecke operators $T(l)$ and $T(l,l)$ on $\mathscr{M}_k(\Gamma_1(Np^r); \Omega)$ are defined as follows:

$$a(n, f|T(l)) = \begin{cases} a(nl, f) + l^{-1} a\left(\frac{n}{l}, f|l\right) & \text{for } l \nmid Np, \\ a(nl, f) & \text{for } l | Np, \end{cases}$$

$$a(n, f|T(l,l)) = \begin{cases} l^{-2} a(n, f|l) & \text{for } l \nmid Np, \\ 0 & \text{for } l | Np. \end{cases}$$

Let $\mathcal{O}_K$ be the ring of p-adic integers of K and let A denote one of the rings K, $\mathcal{O}_K$ and K_0. Then it is known that the Hecke operators $T(l)$ and $T(l,l)$ preserve the space of A-rational modular forms (for details, see [13, §1]). For each subring A of K, let us define an A-algebra $h_k(\Gamma_1(Np^r); A)$ (resp. $h_k(\Phi, \psi; A)$) by the A-subalgebra of the algebra of K-endomorphisms of $S_k(\Gamma_1(Np^r); K)$ (resp. $S_k(\Phi, \psi; K)$) generated over A by the Hecke operators $T(l)$ and $T(l,l)$ for all primes l. We can similarly define the Hecke algebras $\mathscr{H}_k(\Gamma_1(Np^r); A)$ and $\mathscr{H}_k(\Phi, \psi; K)$ for the spaces $\mathscr{M}_k(\Gamma_1(Np^r); K)$ and $\mathscr{M}_k(\Phi, \psi; K)$. Put $\mathcal{O}_{K_0} = K_0 \cap \mathcal{O}_K$. Then, if A is one of the rings $\mathcal{O}_{K_0}$, $\mathcal{O}_K$, K_0 and K, the algebra $h_k(\Gamma_1(N); A)$ acts faithfully on the A-rational space $S_k(\Gamma_1(Np^r); A)$. For each couple of integers $r > s \geq 1$, we have a commutative diagram:

$$\begin{tikzcd} S_k(\Gamma_1(Np^s); K) \arrow[r, hook] \arrow[d, "T(l)(\text{resp.}\, T(l,l))"] & S_k(\Gamma_1(Np^r); K) \arrow[d, "T(l)(\text{resp.}\, T(l,l))"] \\ S_k(\Gamma_1(Np^s); K) \arrow[r, hook] & S_k(\Gamma_1(Np^r); K), \end{tikzcd}$$

where the horizontal arrows are the natural inclusion.

Thus, the restriction of operators in $h_k(\Gamma_1(Np^r); \mathcal{O}_K)$ to $S_k(\Gamma_1(Np^s); K)$ gives a surjective $\mathcal{O}_K$-algebra homomorphism of $h_k(\Gamma_1(Np^r); \mathcal{O}_K)$ onto $h_k(\Gamma_1(Np^s); \mathcal{O}_K)$. Thus we can form the limits:

$$(1.2)\qquad S_k(Np^\infty;A)=\bigcup_{r=1}^{\infty} S_k(\Gamma_1(Np^r);A)\quad \text{for } A=K \text{ and } \mathcal{O}_K;$$

$$\mathfrak{h}_k(Np^\infty;\mathcal{O}_K)=\varprojlim_r \mathfrak{h}_k(\Gamma_1(Np^r);\mathcal{O}_K).$$

The algebra $\mathfrak{h}_k(Np^\infty;\mathcal{O}_K)$ thus defined acts on $S_k(Np^\infty;A)$ for $A=\mathcal{O}_K$ and K, uniformly continuously under the norm (1.1). Let $\bar{S}_k(Np^\infty;A)$ be the completion of $S_k(Np^\infty;A)$ for the norm (1.1). Then the action of $\mathfrak{h}_k(Np^\infty;\mathcal{O}_K)$ can be extended to $\bar{S}_k(Np^\infty;A)$ by the uniform continuity.

So far, we have considered the Hecke algebra defined by growing the level for a fixed weight k. Now we shall define the Hecke algebra for a fixed level Np^r but varying weight. For each positive integer j, put

$$S^j(Np^r;K)=\bigoplus_{k=1}^{j} S_k(\Gamma_1(Np^r);K).$$

Naturally we can imbed $S^j(Np^r;K)$ into $K[[q]]$. Then we define

$$S^j(Np^r;\mathcal{O}_K)=S^j(Np^r;K)\cap\mathcal{O}_K[[q]]=\{f\in S^j(Np^r;K)\,\big|\,|f|_p\leqq 1\}.$$

Let A denote either of K or $\mathcal{O}_K$, and take the injective limit:

$$S^\infty(Np^r;A)=\varinjlim_j S^j(Np^r;A),$$

inside the formal power series ring $A[[q]]$. Let $\bar{S}(Np^r;A)$ be the completion of $S^\infty(Np^r;A)$ under the norm (1.1). Then, as seen in [13, (1.19a)], we have

$$(1.3)\qquad \bar{S}(Np^r;A)=\bar{S}(N;A)\quad \text{for every } r\geqq 0.$$

The space $S^j(Np^r;A)$ for each j is stable under the Hecke operators $T(l)$ and $T(l,l)$ for all primes l if $r\geqq 1$. We shall define an A-algebra $\mathfrak{h}^j(Np^r;A)$ by the A-subalgebra of $\mathrm{End}_A(S^j(Np^r;A))$ generated over A by $T(l)$ and $T(l,l)$ for all primes l. For each couple of integers $i>j>0$, we have a commutative diagram:

$$\begin{tikzcd}
S^j(Np^r;\mathcal{O}_K) \arrow[r, hook] \arrow[d, "T(l)(\text{resp.}\,T(l,l))"] & S^i(Np^r;\mathcal{O}_K) \arrow[d, "T(l)(\text{resp.}\,T(l,l))"] \\
S^j(Np^r;\mathcal{O}_K) \arrow[r, hook] & S^i(Np^r;\mathcal{O}_K);
\end{tikzcd}$$

where the horizontal maps are the natural inclusion.

Thus we have the restriction morphism of $\mathfrak{h}^i(Np^r;\mathcal{O}_K)$ onto $\mathfrak{h}^j(Np^r;\mathcal{O}_K)$. Put

$$\mathfrak{h}(Np^r;\mathcal{O}_K)=\varprojlim_j \mathfrak{h}^j(Np^r;\mathcal{O}_K),$$

which acts faithfully on $S^\infty(Np^r;\mathcal{O}_K)$ and also on $\bar{S}(Np^r;\mathcal{O}_K)$. Then we know from (1.3) that

$$(1.4)\qquad \mathfrak{h}(Np^r;\mathcal{O}_K)=\mathfrak{h}(Np;\mathcal{O}_K)\quad \text{in } \mathrm{End}(\bar{S}(N;\mathcal{O}_K))\quad \text{for every } r\geqq 1$$

(cf. [13, (1.19b)]). By (1.3), there is a natural inclusion of $S_k(\Gamma_1(Np^r);A)$ into $\bar{S}(N;A)$, and therefore,

(1.5) $\bar{S}_k(Np^\infty;A)$ *is contained in* $\bar{S}(N;A)$ *for* $A=\mathcal{O}_K$ *and* K

(In fact, the space $\bar{S}_k(Np^\infty;A)$ coincides with $\bar{S}(N;A)$ in $A[[q]]$ if $k\geqq 2$; so it is independent of the weight k, but we will not need this fact later). The restriction of operators in $h(Np;\mathcal{O}_K)$ to the subspace $S_k(\Gamma_1(Np^r);\mathcal{O}_K)$ of $\bar{S}(N;\mathcal{O}_K)$ induces a morphism of $\mathcal{O}_K$-algebras

$$\rho_{r,k}\colon h(Np;\mathcal{O}_K)\to h_k(\Gamma_1(Np^r);\mathcal{O}_K),$$

which is surjective, because both the algebras are topologically generated by $T(l)$ and $T(l,l)$. The projective limit of morphisms $\rho_{r,k}$ relative to r gives a surjective algebra homomorphism

$$\rho_{\infty,k}\colon h(Np;\mathcal{O}_K)\to h_k(Np^\infty;\mathcal{O}_K).$$

As seen in [12, (4.3)] and [13, (1.17a, b)], one can attach an idempotent e in $h(Np;\mathcal{O}_K)$ and $h_k(Np^\infty;\mathcal{O}_K)$ to the Hecke operator $T(p)$. When one restricts e to $h^j(Np^r;\mathcal{O}_K)$ or $h_k(\Gamma_1(Np^r);\mathcal{O}_K)$, one has the following explicit expression of e:

$$e=\lim_{t\to\infty} T(p)^{p^t(p^f-1)} \quad \text{in} \quad h^j(Np^r;\mathcal{O}_K) \quad \text{and} \quad h_k(\Gamma_1(Np^r);\mathcal{O}_K)$$

for a suitable positive integer f. Another characterization of e may be given as follows: Write R for $h^j(Np^r;\mathcal{O}_K)$ or $h_k(\Gamma_1(Np^r);\mathcal{O}_K)$. Then R is a semi-local complete ring. Thus, if we write $R_\mathfrak{m}$ for the localization of R for each maximal ideal $\mathfrak{m}$ of R, we have a decomposition of algebras:

$$R=\bigoplus_{\mathfrak{m}} R_\mathfrak{m}.$$

Then the image eR of e is given by $\bigoplus_{\mathfrak{m}\not\ni T(p)} R_\mathfrak{m}$. Thus eR is the maximal factor of R on which $T(p)$ acts as an automorphism. By this characterization, e does not depend on the choice of the positive integer f. The idempotent e in $h(Np^r;\mathcal{O}_K)$ (resp. $h_k(Np^\infty;\mathcal{O}_K)$) is defined to be the projective limit of the idempotent in each algebra $h^j(Np^r;\mathcal{O}_K)$ (resp. $h_k(\Gamma_1(Np^r);\mathcal{O}_K)$). We shall define the ordinary parts of the Hecke algebras by $h^0(N;\mathcal{O}_K)=eh(Np;\mathcal{O}_K)$ and $h_k^0(Np^\infty;\mathcal{O}_K)$ $=eh_k(Np^\infty;\mathcal{O}_K)$. For any module M over $h(Np;\mathcal{O}_K)$ or $h_k(Np^\infty;\mathcal{O}_K)$, we write M^0 for eM. We call M^0 the ordinary part of M. Then the morphism $\rho_{\infty,k}$ induces a surjection

$$\rho_{\infty,k}\colon h^0(N;\mathcal{O}_K)\to h_k^0(Np^\infty;\mathcal{O}_K). \tag{1.6}$$

Theorem 1.1. *The morphism* $\rho_{\infty,k}$ *induces an algebra isomorphism of* $h^0(N;\mathcal{O}_K)$ *onto* $h_k^0(Np^\infty;\mathcal{O}_K)$ *for each* $k\geqq 2$, *which takes the Hecke operators* $T(l)$ *and* $T(l,l)$ *of* $h^0(N;\mathcal{O}_K)$ *to the corresponding ones in* $h_k^0(Np^\infty;\mathcal{O}_K)$.

The proof of this theorem given in §7 is based on an isomorphism between the parabolic cohomology groups $H_P^1(\Gamma_1(Np);L_n(\mathbf{Z}/p^r\mathbf{Z}))$ and

$H_p^1(\Gamma_1(Np^r), \mathbf{Z}/p^r\mathbf{Z})$ due to an unpublished work [24] of Shimura. We shall give a construction of this morphism in §4 and prove this theorem in §7. One can even prove a much more general fact:

$$(1.7)\qquad \mathscr{h}(Np;\mathcal{O}_K)\simeq \mathscr{h}_k(Np^\infty;\mathcal{O}_K) \quad \text{for each } k\geqq 2,$$

by using a result in [24] which is already appeared in Ohta [17, Th. 3.1.3]. This guarantees the fact that $\bar{S}_k(Np^\infty;\mathcal{O}_K)=\bar{S}(N;\mathcal{O}_K)$ for $k\geqq 2$. However, we shall content ourselves with Theorem 1.1, because it is much easier to prove and we do not need the general fact (1.7) for our later application.

Hereafter we identify $\mathscr{h}_k^0(Np^\infty;\mathcal{O}_K)$ with $\mathscr{h}^0(N;\mathcal{O}_K)$ for all $k\geqq 2$, and we denote this universal Hecke algebra by $\mathscr{h}^0(N;\mathcal{O}_K)$. We shall say that a common eigenform $f=\sum_{n=0}^{\infty} a(n,f)q^n$ in $\mathscr{M}_k(\Gamma_1(Np^r))$ of all operators $T(l)$ is normalized if

$$f|T(l)=a(l,f)f \quad (\text{and } f\neq 0) \qquad \text{for all } l\geqq 1.$$

To each normalized eigenform f, one can associate a unique primitive form which has the same eigenvalues as f for $T(l)$ for almost all l. The smallest possible level of the associated primitive form is called the conductor of f. A normalized eigenform f is called *ordinary* if one of the following two equivalent conditions are satisfied:

(1.8a) $f|e=f$;

(1.8b) $|a(p,f)|_p=1$ *and the level of* f *is divisible by* p.

At first glance, the condition (1.8b) gives an impression that primitive forms in $\mathscr{M}_k(\Gamma_1(N))$ with $|a(p,f)|_p=1$ are not included in the ordinary forms, but in fact, if $k\geqq 2$, one can associate to each primitive form with this property a unique ordinary form f_0 in $\mathscr{M}_k(\Gamma_1(Np))$ by the following condition

(1.9) $f_0|T(n)=a(n,f)f_0$ *for all* n *prime to* p.

Indeed, f_0 coincides with $f|e$ up to the multiple of p-adic units (cf. [12, Lemma 3.3]).

As seen in [13, §3], one can regard naturally $\mathscr{h}^0(N;\mathcal{O}_K)$ as an algebra over the Iwasawa algebra $\Lambda_K=\mathcal{O}_K[[\Gamma]]$ of the p-profinite group $\Gamma=1+p\mathbf{Z}_p$, and therefore, $\mathscr{h}^0(N;\mathcal{O}_K)$ is equipped with a continuous Γ-action. One can specify a Λ_K-algebra structure on $\mathscr{h}^0(N;\mathcal{O}_K)$ so that the prime l with $l\equiv 1 \bmod Np$ as an element of Γ acts on $\mathscr{h}^0(N;\mathcal{O}_K)$ through the multiplication of the Hecke operator $l^2T(l,l)$. Indeed, in [13, §1], an action of a bigger group $Z=\mathbf{Z}_p^\times \times(\mathbf{Z}/N\mathbf{Z})^\times$ on $\mathscr{h}^0(N;\mathcal{O}_K)$ is discussed, and each prime l outside Np as an element of Z acts on $\mathscr{h}^0(N;\mathcal{O}_K)$ via the operator $l^2(T(l,l))$. Fix a topological generator u of Γ (for example, one can choose $1+p$ as u). By definition, there is a tautological character $\iota\colon \Gamma\to\mathcal{O}_K[[\Gamma]]$, which takes u to itself in Λ_K. For each character $\chi\colon \Gamma\to\mathcal{O}_K^\times$, the element $P_\chi=\iota(u)-\chi(u)$ of Λ_K is a prime element, and $\Lambda_K/P_\chi\Lambda_K$ is the maximal quotient of Λ_K on which Γ acts via χ. We have a canonical isomorphism: $\Lambda_K/P_\chi\Lambda_K\simeq\mathcal{O}_K$ so that $\iota(u)$ corresponds to $\chi(u)$. If $\chi(\gamma)$

$=\gamma^k\varepsilon(\gamma)$ for an integer k and a finite order character ε of Γ, we write $P_{k,\varepsilon}$ for P_χ, and when ε is trivial, we write simply P_k for $P_{k,\varepsilon}$. As seen in [13, Th. 3.1, Cor. 3.2],

(1.10a) *$h^0(N;\mathcal{O}_K)$ is free of finite rank over Λ_K,*

(1.10b) *The morphism $\rho_{1,k}$ induces an isomorphism of $\mathcal{O}_K$-algebras:*

$$h^0(N;\mathcal{O}_K)/P_k h^0(N;\mathcal{O}_K)\simeq h_k^0(\Gamma_1(Np);\mathcal{O}_K) \quad \textit{for each } k\geqq 2,$$

where we denote by $h_k^0(\Gamma_1(Np);\mathcal{O}_K)$ the ordinary part $e h_k(\Gamma_1(Np);\mathcal{O}_K)$ of $h_k(\Gamma_1(Np);\mathcal{O}_K)$. Put $\Gamma_r=1+p^r\mathbf{Z}_p$ and $\Phi_r^1=\Gamma_1(Np)\cap\Gamma_0(p^r)$ for each positive integer r. Then we have the following generalization of (1.10b).

Theorem 1.2. *Let ε be a character of finite order of Γ with values in $\mathcal{O}_K$, and define a positive integer r by $\Gamma_r=\mathrm{Ker}(\varepsilon)$. Then, for each weight $k\geqq 2$, the morphism $\rho_{r,k}$ induces an isomorphism:*

$$h^0(N;\mathcal{O}_K)/P_{k,\varepsilon}h^0(N;\mathcal{O}_K)\simeq h_k^0(\Phi_r^1,\varepsilon;\mathcal{O}_K),$$

where $h_k^0(\Phi_r^1,\varepsilon;\mathcal{O}_K)$ is the ordinary part $e h_k(\Phi_r^1,\varepsilon;\mathcal{O}_K)$. This isomorphism takes the Hecke operator $T(l)$ in $h^0(N;\mathcal{O}_K)$ to $T(l)$ in $h_k^0(\Phi_r^1,\varepsilon;\mathcal{O}_K)$ for each integer l.

Here are some remarks about this theorem. Without assuming that $k\geqq 2$, the restriction of operators of $h^0(N;\mathcal{O}_K)$ to the subspace $S_k(\Phi_r^1,\varepsilon;\mathcal{O}_K)$ of $\bar{S}(N;\mathcal{O}_K)$ yields a surjective $\mathcal{O}_K$-algebra homomorphism

$$\rho_{k,\varepsilon}\colon h^0(N;\mathcal{O}_K)/P_{k,\varepsilon}h^0(N;\mathcal{O}_K)\to h_k^0(\Phi_r^1,\varepsilon;\mathcal{O}_K).$$

Thus the theorem shows that $\rho_{k,\varepsilon}$ is in fact an isomorphism when $k\geqq 2$. Put $\omega_{k,r}=\prod_\varepsilon P_{k,\varepsilon}\in\Lambda_K$, where the product is taken over all characters ε of Γ/Γ_r. Note that $\omega_{k,r}$ is in fact contained in $\Lambda=\Lambda_{\mathbf{Q}_p}$. Then, by Theorem 1.2, one can easily conclude that for each $k\geqq 2$

$$h^0(N;\mathcal{O}_K)/\omega_{k,r}h^0(N;\mathcal{O}_K)\simeq h_k^0(\Gamma_1(Np^r);\mathcal{O}_K).$$

As for this assertion, $\mathcal{O}_K$ is arbitrary; i.e., we do not have to assume that a character of Γ with kernel Γ_r has values in $\mathcal{O}_K$.

Let $\mathcal{L}_K$ denote the quotient field of Λ_K and put $\mathcal{G}(N;K)=h^0(N;\mathcal{O}_K)\otimes_{\Lambda_K}\mathcal{L}_K$, which is an artinian algebra of finite dimension over $\mathcal{L}_K$. Let $\mathcal{K}$ be a local ring of $\mathcal{G}(N;K)$; thus, $\mathcal{K}$ is a direct summand of $\mathcal{G}(N;K)$. Let $h(\mathcal{K})$ be the projected image of $h^0(N;\mathcal{O}_K)$ in K. We shall use the terminology "*prime divisors* of Λ_K" exclusively for prime ideals of Λ_K of height 1. For each prime divisor P of Λ_K, we denote by $h(\mathcal{K})_P$ the localization of $h(\mathcal{K})$ at P. Define the *free closure* $\tilde{h}(\mathcal{K})$ of $h(\mathcal{K})$ by the intersection $\bigcap_P h(\mathcal{K})_P$ in $\mathcal{K}$, where P runs over all prime divisors of Λ_K. Then $\tilde{h}(\mathcal{K})$ is an algebra free of finite rank over Λ_K, and the quotient $\tilde{h}(\mathcal{K})/h(\mathcal{K})$ is a pseudo-null Λ_K-module; namely, it has only finitely many elements. Thus for each k and for each character $\varepsilon\colon\Gamma\to\mathcal{O}_K$ with $\mathrm{Ker}(\varepsilon)=\Gamma_r$, $\tilde{h}(\mathcal{K})/P_{k,\varepsilon}\tilde{h}(\mathcal{K})$ is a flat $\mathcal{O}_K$-algebra. The natural projection of

$\mathscr{h}^0(N;\mathcal{O}_K)$ into $\tilde{\mathscr{h}}(\mathscr{K})$ induces an $\mathcal{O}_K$-algebra homomorphism

$$\lambda_{k,\varepsilon}\colon \mathscr{h}^0(N;\mathcal{O}_K)/P_{k,\varepsilon}\mathscr{h}^0(N;\mathcal{O}_K)\to\tilde{\mathscr{h}}(\mathscr{K})/P_{k,\varepsilon}\tilde{\mathscr{h}}(\mathscr{K}).$$

On the other hand, there is a well known bijection between $\mathcal{O}_K$-algebra morphisms λ of $\mathscr{h}_k^0(\Phi_r^1,\varepsilon;\mathcal{O}_K)$ into Ω and ordinary forms f in $S_k^0(\Phi_r,\varepsilon;\Omega)$, which satisfy

$$f|h=\lambda(h)f \quad \text{for every } h\in\mathscr{h}_k^0(\Phi_r^1,\varepsilon;\mathcal{O}_K).$$

Terminology. We say that an ordinary form f (or the corresponding $\mathcal{O}_K$-algebra homomorphism λ) *belongs* to $\mathscr{K}$ if there is an $\mathcal{O}_K$-algebra homomorphism λ' of $\tilde{\mathscr{h}}(\mathscr{K})/P_{k,\varepsilon}\tilde{\mathscr{h}}(\mathscr{K})$ into Ω which makes the following diagram commutative:

(1.11)
$$\begin{tikzcd}
\mathscr{h}^0(N;\mathcal{O}_K)/P_{k,\varepsilon}\mathscr{h}^0(N;\mathcal{O}_K) \arrow[r, "\lambda_{k,\varepsilon}"] \arrow[d, "\rho_{k,\varepsilon}"] & \tilde{\mathscr{h}}(\mathscr{K})/P_{k,\varepsilon}\tilde{\mathscr{h}}(\mathscr{K}) \arrow[d, "\lambda'"] \\
\mathscr{h}_k^0(\Phi_r^1,\varepsilon;\mathcal{O}_K) \arrow[r, "\lambda"] & \Omega.
\end{tikzcd}$$

By definition, every ordinary form in $S_k(\Phi_r^1,\varepsilon;\mathcal{O}_K)$ belongs to some local ring of $\mathscr{g}(N;K)$.

Corollary 1.3. *Assume $\mathscr{K}$ to be primitive in the sense of* [13, §3], *and write d for the dimension of $\mathscr{K}$ over $\mathscr{L}_K$. Then, for each $k\geqq 2$ and for each character ε: $\Gamma\to\mathcal{O}_K$ with $\Gamma_r=\mathrm{Ker}(\varepsilon)$, the $\mathcal{O}_K$-algebra $\tilde{\mathscr{h}}(\mathscr{K})/P_{k,\varepsilon}\tilde{\mathscr{h}}(\mathscr{K})$ can be canonically regarded as an $\mathcal{O}_K$-subalgebra of $\mathscr{h}_k^0(\Phi_r^1,\varepsilon;K)$, and there exist exactly d ordinary forms in $S_k(\Phi_r^1,\varepsilon;\Omega)$ belonging to $\mathscr{K}$. Moreover the primitive form associated with each ordinary form belonging to $\mathscr{K}$ has conductor divisible by N, and the original ordinary form is obtained by the process* (1.9). *Conversely, if f is an ordinary form in $S_k(\Phi_r^1,\varepsilon;\Omega)$ for $k\geqq 2$ and if f is associated with a primitive form with conductor divisible by N via* (1.9), *then the local ring to which f belongs is a field and is unique and primitive.*

One can deduce this from Theorem 1.2 by applying the same argument in [13, §6] which proves Corollary 3.7 there. We thus omit the proof of this corollary. The following *warning* may be necessary: Put $F=(\tilde{\mathscr{h}}(\mathscr{K})/P_{k,\varepsilon}\tilde{\mathscr{h}}(\mathscr{K}))\otimes_{\mathcal{O}_K}K$. What we know for F is only the semi-simplicity (when $k\geqq 2$), and thus F may not be a field. When $d=1$, F is obviously a field isomorphic to K. Actually, there is an example of a local ring $\mathscr{K}$ with $d=2$ (cf. [14]) which is defined over $\mathbf{Q}_p$. Thus, from this example, one can find a $P_{k,\varepsilon}$ so that F is no longer a field.

Let $\mathscr{K}$ be a primitive local ring of $\mathscr{g}(N;K)$ and let $\mathscr{I}(\mathscr{K})$ be the integral closure of Λ_K in $\mathscr{K}$. Then $\mathscr{I}(\mathscr{K})$ is an integrally closed noetherian domain of Krull dimension 2. We have the following inclusion relations:

$$\mathscr{h}(\mathscr{K})\subset\tilde{\mathscr{h}}(\mathscr{K})\subset\mathscr{I}(\mathscr{K}),$$

and $\tilde{\mathscr{h}}(\mathscr{K})/\mathscr{h}(\mathscr{K})$ is pseudo-null, and $\mathscr{I}(\mathscr{K})/\tilde{\mathscr{h}}(\mathscr{K})$ is a finite torsion Λ_K-module, but not necessarily pseudo-null. We now state Corollary 1.3 in a different formulation.

Corollary 1.4. *Let the notation be as in Corollary 1.3. For each $k \geqq 2$ and ε, the discrete valuation of $\mathscr{L}_K$ attached to the prime divisor $P_{k,\varepsilon}$ of Λ_K is unramified in $\mathscr{I}(\mathscr{K})$.*

Proof. By Corollary 1.3, $F = (\tilde{h}(\mathscr{K})/P_{k,\varepsilon}\tilde{h}(\mathscr{K})) \otimes_{\mathcal{O}_K} K$ is a direct summand of $h_k^0(\Phi_r^1, \varepsilon; K)$ which annihilates all the old forms in $S_k(\Phi_r^1, \varepsilon; K)$. Then, by [12, (4.4c)], F is semisimple. Thus the localizations of $\tilde{h}(\mathscr{K})$ and $\mathscr{I}(\mathscr{K})$ at $P_{k,\varepsilon}$ coincide, and therefore, $P_{k,\varepsilon}$ is unramified in $\mathscr{I}(\mathscr{K})$.

As a consequence of Corollary 1.4, one has

Corollary 1.5. *Assume that $k \geqq 2$. To each ordinary form $f \in S_k(\Phi_r^1, \varepsilon; \Omega)$ belonging to $\mathscr{K}$, one can attach a unique $\mathcal{O}_K$-algebra homomorphism*

$$\lambda_f \colon \mathscr{I}(\mathscr{K}) \to \Omega$$

such that $\lambda_f(T(n)) = a(n, f)$ for all $n > 0$.

Let $\mu = \{\zeta \in \mathbf{Z}_p^\times \mid \zeta^{p-1} = 1\}$. Then, the group Z is a product of Γ and the finite group $G = \mu \times (\mathbf{Z}/N\mathbf{Z})^\times$. Thus the Iwasawa algebra $\mathcal{O}_K[[Z]]$ of Z is isomorphic to $\Lambda_K \otimes_{\mathcal{O}_K} \mathcal{O}_K[G]$. Since the Hecke algebra is an algebra over $\mathcal{O}_K[[Z]]$, $\mathscr{G}(N; K)$ is decomposed accordingly to the decomposition of $K[G]$. Assume that all the characters of G have values in K. Then $K[G]$ is a product of copies of K on which G acts via each character of G. This induces a decomposition of $\mathscr{L}_K$-algebras

$$\mathscr{G}(N; K) = \bigoplus_{\psi} \mathscr{G}(N, \psi; K),$$

where ψ runs over all characters of G and

$$\mathscr{G}(N, \psi; K) = \{h \in \mathscr{G}(N; K) \,\big|\, h \mid g = \psi(g) h \text{ for each } g \in G\}.$$

Since G is naturally isomorphic to $(\mathbf{Z}/Np\mathbf{Z})^\times$, each character ψ of G may be regarded as a Dirichlet character modulo Np.

Terminology. Let $\mathscr{K}$ be a local ring of $\mathscr{G}(N; K)$ and ψ be a Dirichlet character modulo Np. We say that ψ is the *character* of $\mathscr{K}$ if $\mathscr{K}$ is a direct factor of $\mathscr{G}(N, \psi; K)$. By definition, each local ring $\mathscr{K}$ has a unique character ψ.

Corollary 1.6. *Let $\mathscr{K}$ be a local ring of $\mathscr{G}(N; K)$ and ψ be the character of $\mathscr{K}$. Let ε be a character of Γ of finite order with $\Gamma_r = \mathrm{Ker}(\varepsilon)$. Then, if an ordinary form f of $S_k(\Phi_r^1, \varepsilon; \Omega)$ belongs to $\mathscr{K}$, then f is an element of $S_k(\Gamma_0(Np^r), \varepsilon\psi\omega^{-k})$. Furthermore, if $\mathscr{K}$ is primitive and if the restriction of $\varepsilon\psi\omega^{-k}$ to $(\mathbf{Z}/p^r\mathbf{Z})^\times$ is non-trivial, then f itself is primitive.*

The first assertion is an easy consequence of Corollary 1.3 and the definition of the character of $\mathscr{K}$, and the second follows from [12, Lemma 3.3]. Even if the restriction of $\varepsilon\psi\omega^{-k}$ to $(\mathbf{Z}/p^r\mathbf{Z})^\times$ is trivial, it can happen that the ordinary form f belonging to $\mathscr{K}$ is primitive, but this is possible only when the weight k is equal to 2 by [12, Lemma 3.2]. By Corollary 1.6, it is evident that the character ψ of any local ring of $\mathscr{G}(N; K)$ is even; i.e., $\psi(-1) = 1$.

For each weight $k \geqq 2$ and for each character $\varepsilon \colon \Gamma \to K$ of finite order with $\mathrm{Ker}(\varepsilon) = \Gamma_r$, put

$$F=(\tilde{h}(\mathcal{K})/P_{k,\varepsilon}\tilde{h}(\mathcal{K}))\otimes_{\mathcal{O}_K}K$$

as a subalgebra of $h_k(\Phi_r^1,\varepsilon;K)$, and decompose

$$h_k^0(\Phi_r^1,\varepsilon;K)=F\oplus A \quad \text{as an algebra direct sum.}$$

Define $h(F)$ (resp. $h(A)$) by the projection of $h_k^0(\Phi_r^1,\varepsilon;\mathcal{O}_K)$ in F (resp. A), and put

$$(1.12) \qquad C_{k,\varepsilon}(\mathcal{K})=(h(F)\oplus h(A))/h_k^0(\Phi_r^1,\varepsilon;\mathcal{O}_K).$$

Then, in exactly the same manner as in the proof of [13, Cor. 3.8], we can verify

Corollary 1.7. *Let $\mathcal{K}$ be a primitive local ring of $\mathscr{G}(N;K)$, and let $\mathcal{C}(\mathcal{K};K)$* (resp. *$\mathcal{N}_s(\mathcal{K};K)$*) *be the torsion Iwasawa module* (resp. *the pseudo-null module*) *associated with $\mathcal{K}$ defined in* [13, (3.9b)]. *Then, for each finite order character ε: $\Gamma\to K^\times$ and for each weight $k\geqq 2$, we have a canonical exact sequence:*

$$0\to C_{k,\varepsilon}(\mathcal{K})\to\mathcal{C}(\mathcal{K};K)/P_{k,\varepsilon}\mathcal{C}(\mathcal{K};K)\to\mathcal{N}_s(\mathcal{K};K)/P_{k,\varepsilon}\mathcal{N}_s(\mathcal{K};K)\to 0.$$

Terminology. We say that a primitive local ring $\mathcal{K}$ of $\mathscr{G}(N;K)$ is *defined* over K if the algebraic closure of $\mathbf{Q}_p$ inside $\mathcal{K}$ coincides with K.

If $\mathcal{K}$ is defined over K, as seen in [13, Th. 3.6], $\mathcal{K}\otimes_K M$ remains a field and gives a primitive local ring of $\mathscr{G}(N;M)=\mathscr{G}(N;K)\otimes_K M$ for each finite extension M/K. Especially, we know that $\mathcal{C}(\mathcal{K}\otimes_K M;M)\simeq\mathcal{C}(\mathcal{K};K)\otimes_{\Lambda_K}\Lambda_M$ and the degree of the local ring over $\mathcal{L}_K$ does not change by scalar extension of ground fields over a field of definition.

§ 2. Galois representations

Let N be a positive integer prime to p. To each primitive form f of $S_k(\Gamma_0(Np^r),\psi)$, one can attach a simple representation $\pi=\pi(f)$ of the absolute Galois group $\mathfrak{G}=\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ into $\mathrm{GL}_2(\Omega)$, which is characterized by the following properties:

(2.1 a) *$\pi(f)$ is unramified outside Np;*

(2.1 b) *Let σ_l be the Frobenius element of $\mathfrak{G}$ for each prime l outside Np. Then we have that*

$$\det(1-\pi(\sigma_l)X)=1-a(l,f)X+\psi(l)l^{k-1}X^2.$$

When $k=2$, the existence of $\pi(f)$ follows from the Eichler-Shimura congruence relation [25, Th. 7.9]. More generally, this is shown by Deligne [4] for each weight $k\geqq 2$ and by Deligne and Serre [5] for $k=1$. A proof of the simplicity of $\pi(f)$ can be found in Ribet [18].

Let $\mathcal{K}$ be a primitive local ring of $\mathscr{G}(N;K)$ and let $\mathcal{I}(\mathcal{K})$ be the integral closure of Λ_K in $\mathcal{K}$.

Terminology. We say that a representation π of $\mathfrak{G}$ into $GL_2(\mathscr{K})$ is *continuous* if

(i) *π can be realized on a two dimensional $\mathscr{K}$-vector space V with a $\mathscr{I}(\mathscr{K})$-lattice L* (in the sense of [1, VII.4.1]) *stable under $\mathfrak{G}$,*

(ii) *π: $\mathfrak{G} \to \mathrm{Aut}_{\mathscr{I}(\mathscr{K})}(L)$ is continuous, where $\mathrm{Aut}_{\mathscr{I}(\mathscr{K})}(L)$ is equipped with the topology of the projective limit*

$$\mathrm{Aut}_{\mathscr{I}(\mathscr{K})}(L) = \varprojlim_j \mathrm{Aut}(L/\mathfrak{m}^j L)$$

for the maximal ideal $\mathfrak{m}$ of $\mathscr{I}(\mathscr{K})$.

We say a prime ideal P of $\mathscr{I}(\mathscr{K})$ a prime divisor if P is of height 1. For each prime divisor P of $\mathscr{I}(\mathscr{K})$, the localization $\mathscr{I}(\mathscr{K})_P$ of $\mathscr{I}(\mathscr{K})$ at P becomes a discrete valuation ring, and hence, the localization $L_P = L \otimes_{\mathscr{I}(\mathscr{K})} \mathscr{I}(\mathscr{K})_P$ is free of rank 2 over $\mathscr{I}(\mathscr{K})_P$. Let $K(P)$ be the residue field $\mathscr{I}(\mathscr{K})_P/P$. Thus π induces a representation

$$\pi \colon \mathfrak{G} \to GL_2(\mathscr{I}(\mathscr{K})_P).$$

The reduction $\pi \bmod P$ is defined to be the semi-simplification of the combination of π with the reduction map: $GL_2(\mathscr{I}(\mathscr{K})_P) \to GL_2(K(P))$. The reduction $\pi \bmod P$ does not depend on the choice of the lattice L. If $\pi \bmod P$ is simple, then $\pi \bmod P$ coincides with the combination of π and the reduction map.

Let ψ be the character of $\mathscr{K}$ and let ε: $\Gamma \to \Omega$ be a character of finite order with $\mathrm{Ker}(\varepsilon) = \Gamma_r$. Let $f \in S_k(\Gamma_0(Np^r), \varepsilon\psi\omega^{-k})$ be an ordinary form belonging to $\mathscr{K}$. We denote by $\pi(f)$, with an abuse of notation, the Galois representation as above associated with the primitive form corresponding to f via (1.9). By Corollary 1.5, one can attach to f a non-trivial $\mathcal{O}_K$-algebra homomorphism λ_f of $\mathscr{I}(\mathscr{K})$ into Ω. Put

$$P_f = \mathrm{Ker}(\lambda_f) \quad \text{and} \quad \mathscr{X}(\mathscr{K}) = \mathrm{Spec}(\mathscr{I}(\mathscr{K})).$$

Then P_f is a Ω-valued point of $\mathscr{X}(\mathscr{K})$; i.e., $P_f \in \mathscr{X}(\mathscr{K})(\Omega)$. The subset of $\mathscr{X}(\mathscr{K})(\Omega)$ of the points obtained from ordinary forms is dense under the Zariski topology on $\mathscr{X}(\mathscr{K})(\Omega)$.

Theorem 2.1. *Let $\mathscr{K}$ be a primitive local ring of $\mathscr{h}(N;K)$. Then there exists a continuous representation of $\mathfrak{G}$ into $GL_2(\mathscr{K})$ characterized by the following properties:*

(2.2a) *π is simple;*

(2.2b) *π is unramified outside Np;*

(2.2c) *For each ordinary form f of weight $k \geqq 2$ belonging to $\mathscr{K}$, the reduction $\pi \bmod P_f$ is equivalent to $\pi(f)$ as a Galois representation into $GL_2(\Omega)$.*

Here are some remarks about the theorem, whose proof will be given in §8: Firstly, the uniqueness of π is obvious since the point set $\{P_f\}$ for ordinary forms belonging to $\mathscr{K}$ is Zariski dense in $\mathscr{X}(\mathscr{K})(\Omega)$. Secondly, if we denote by $t(l)$ and $t(l,l)$ for the images of $T(l)$ and $T(l,l)$ in $\mathscr{K}$, then the assertion (2.2c) shows that for the Frobenius element σ_l at each prime l outside Np, we have

$$\det(1-\pi(\sigma_l)X)=1-t(l)X+lt(l,l)X^2.$$

Let F_∞ be the unique $\mathbf{Z}_p$-extension of $\mathbf{Q}$ unramified outside p. Then, by class field theory, Γ is canonically identified with $\mathrm{Gal}(F_\infty/\mathbf{Q})$ via the cyclotomic character. Thus, one may regard the tautological character ι: $\Gamma \to \Lambda_K$ as a character of $\mathfrak{G}$. By the definition of the character ψ of $\mathcal{K}$, one has that

$$lt(l,l)=\psi\chi^{-1}(\sigma_l)\iota(\sigma_l)\in\Lambda_K \quad \text{for each } l,$$

where χ: $\mathfrak{G}\to\mathbf{Z}_p^\times$ is the cyclotomic character of $\mathfrak{G}$ defined by $\chi(\sigma_l)=l$ and ψ: $\mathfrak{G}\to\mathcal{O}_K^\times$ is the finite order character whose value at σ_l is given by $\psi(l)$. Thus $\det(\pi)$ coincides with the character $\psi\chi^{-1}\cdot\iota$.

As a final remark, we add that the construction of π will be done without using any result of Deligne [4]. Thus our proof gives a different method for constructing $\pi(f)$ as in (2.1) for ordinary forms. This method of constructing Galois representations goes back to the paper of Shimura [24], where he showed the existence of $\pi(f)$ in a weaker form than (2.1 a, b) but even for modular forms for certain quaternion algebras over totally real fields. Recently, by combining Shimura's idea with the theory of etale cohomology, Ohta [17] has shown the conditions (2.1) for the Galois representations of Shimura.

When the local ring $\mathcal{K}$ comes from an imaginary quadratic field as described in [13, §7], there is another and a much simpler construction of the representation as in Theorem 2.1. We shall explain this here. We begin by recalling the construction of the local ring. Let M be an imaginary quadratic field and denote by R its ring of algebraic integers. Assume that

(2.3) *the fixed prime p is decomposed into the product of two distinct prime ideals in the ring R.*

We specify one of the factors of p in R by

$$\mathfrak{p}=\{x\in R\,|\,|x|_p<1\}.$$

Fix an ideal $\mathfrak{c}$ of R prime to p. For each prime ideal $\mathfrak{l}$ of R, put

$$R_\mathfrak{l}=\varprojlim_n R/\mathfrak{l}^n R, \qquad U_\mathfrak{l}=R_\mathfrak{l}^\times,$$

$$U_\mathfrak{l}(\mathfrak{c})=\{x\in U_\mathfrak{l}\,|\,x\equiv 1 \bmod \mathfrak{c}R_\mathfrak{l}\},$$

$$U(\mathfrak{c})=\prod_{\mathfrak{l}\neq\mathfrak{p}} U_\mathfrak{l}(\mathfrak{c}).$$

For the infinite place ∞ of M, let $M_\infty\simeq\mathbf{C}$ be the completion of M at ∞. We define a topological group $W(\mathfrak{c})$ by

$$W(\mathfrak{c})=M_A^\times/\overline{M^\times M_\infty^\times U(\mathfrak{c})},$$

where $M_A^\times$ is the idele group of M and the closure $\overline{M^\times M_\infty^\times U(\mathfrak{c})}$ is taken in the topological group $M_A^\times$. The natural inclusion of $\mathbf{Z}$ into R induces an isomorphism of Γ onto $U_{\mathfrak{p}}(\mathfrak{p})$, and thus, we have an embedding of Γ into $W(\mathfrak{c})$. Let us fix a maximal p-profinite torsion free subgroup $W_0(\mathfrak{c})$ of $W(\mathfrak{c})$ containing Γ, and let $W_t(\mathfrak{c})$ be the maximal finite subgroup of $W(\mathfrak{c})$.

Lemma 2.2. *$W_0(\mathfrak{c})$ is independent of $\mathfrak{c}$. More precisely, for any ideals $\mathfrak{c}$ and $\mathfrak{c}'$ prime to p, there is an isomorphism of p-profinite groups between $W_0(\mathfrak{c})$ and $W_0(\mathfrak{c}')$ which induces the identity on Γ. Especially, if the class number of M is prime to p, then $W_0(\mathfrak{c})$ coincides with Γ.*

Proof. By construction, we have a natural surjection: $W(\mathfrak{c})\to W(1)$. The kernel of this morphism is a finite group, and therefore, it induces an isomorphism of $W_0(\mathfrak{c})$ onto $W_0(1)$, which shows the first assertion. The index $[W_0(1):\Gamma]$ divides the class number of M; hence the second assertion follows.

Hereafter, we identify $W_0(\mathfrak{c})$ with $W_0(1)$ and write it as W_0. For each divisor $\mathfrak{c}'$ of $\mathfrak{c}$, there is a natural group homomorphism of $W_t(\mathfrak{c})$ onto $W_t(\mathfrak{c}')$. A character χ of $W_t(\mathfrak{c})$ is said to be primitive if χ is not a pull-back of any character of $W_t(\mathfrak{c}')$ for any proper divisor $\mathfrak{c}'$ of $\mathfrak{c}$.

Let K be a finite extension of $\mathbf{Q}_p$ and by $C(W(\mathfrak{c});K)$, we denote the Banach space of all continuous functions on $W(\mathfrak{c})$ with values in K. Let I be the set consisting of all ideals of R prime to $\mathfrak{p}\mathfrak{c}$. For each $\mathfrak{a}\in I$, take $x=(x_{\mathfrak{l}})\in M_A^\times$ such that $\mathfrak{a}=\bigcap_{\mathfrak{l}} x_{\mathfrak{l}}R_{\mathfrak{l}}$ in M and $x_{\mathfrak{l}}=1$ for $\mathfrak{l}|\mathfrak{p}\mathfrak{c}$. Then $x^{-1} \bmod \overline{U(\mathfrak{c})M^\times M_\infty^\times}$ is uniquely determined by $\mathfrak{a}\in I$. This correspondence gives an inclusion i: $I\to W(\mathfrak{c})$. Hereafter, by this isomorphism, we regard I as a subset of $W(\mathfrak{c})$. Then we define a linear form

$$\theta\colon\ C(W(\mathfrak{c});K)\to\tilde{S}(Nr(\mathfrak{c})d;K)$$

by

$$\theta(\phi)=\sum_{\mathfrak{a}\in I}\phi(\mathfrak{a})q^{Nr(\mathfrak{a})},$$

where $Nr(\mathfrak{a})$ denotes the norm of the ideal $\mathfrak{a}$ and $-d$ is the discriminant of the extension $M/\mathbf{Q}$. Let the Iwasawa algebra $\mathbf{Z}_p[[W(\mathfrak{c})]]$ act on $C(W(\mathfrak{c});K)$ via the translation of the elements of $W(\mathfrak{c})$; i.e., $(\phi|w)(w')=\phi(ww')$ for $\phi\in C(W(\mathfrak{c});K)$. For each prime ideal $\mathfrak{l}$ in I, let l denote the prime number in $\mathbf{Z}$ divisible by $\mathfrak{l}$. Then, we have that

$$(2.4\text{a})\qquad \theta(\phi)|T(l)=\begin{cases}\theta(\phi|\mathfrak{l})+\theta(\phi|\bar{\mathfrak{l}}) & \text{if } l=\mathfrak{l}\bar{\mathfrak{l}},\ \mathfrak{l}\neq\bar{\mathfrak{l}} \text{ and } \mathfrak{l},\bar{\mathfrak{l}}\in I,\\ 0 & \text{if } Nr(\mathfrak{l})=l^2\\ \theta(\phi|\mathfrak{l}) & \text{if } l=\mathfrak{l}^2, \text{ or } l=\mathfrak{l}\bar{\mathfrak{l}},\ \mathfrak{l}\neq\bar{\mathfrak{l}} \text{ and } \bar{\mathfrak{l}}\notin I\end{cases}$$

and

$$(2.4\text{b})\qquad \theta(\phi)|z=z\theta(\phi|z)\quad \text{for } z\in\Gamma.$$

This shows that θ induces an algebra homomorphism:

$$(2.5)\qquad \varphi\colon\ h^0(Nr(\mathfrak{c})d,\mathcal{O}_K)\to\mathcal{O}_K[[W(\mathfrak{c})]].$$

As seen in [13, Th. 7.1] and [28, Th. 4.3], φ is generically surjective (namely, it becomes surjective after tensoring $\mathcal{L}_K$). We know that

$$\mathcal{O}_K[[W(\mathfrak{c})]]\simeq\mathcal{O}_K[[W_0]]\otimes_{\mathcal{O}_K}\mathcal{O}_K[W_t(\mathfrak{c})],$$

and each primitive character of $W_t(\mathfrak{c})$ with valued in K determines a unique irreducible component of $\mathcal{O}_K[[W(\mathfrak{c})]]$ on which $W_t(\mathfrak{c})$ acts via χ. It is shown by Weil (e.g. [11, §1]) that there is a bijection between Hecke (ideal) characters λ with values in $\mathbf{C}$ satisfying

$$\lambda((a))=a^j \quad \text{if } a\in K \quad \text{and} \quad a\equiv 1 \bmod \mathfrak{c}\mathfrak{p} \text{ for an integer } j$$

and continuous characters $\hat{\lambda}$ of $W(\mathfrak{c})$ with values in Ω satisfying

$$\hat{\lambda}(a)=a^j \quad \text{for } a\in U_{\mathfrak{p}}(\mathfrak{p})(\simeq\Gamma).$$

If $\hat{\lambda}$ corresponds to λ, the values of λ and $\hat{\lambda}$ coincide on I.

Fix a Hecke character λ such that $\lambda((a))=a$ if $a\equiv 1 \bmod \mathfrak{p}$ (such λ exists because $p\geqq 5$), and denote by λ_1 the restriction to W_0 of the corresponding Ω-valued character. Via the natural surjection: $W(\mathfrak{c})\to W(1)$, we may regard λ_1 as a character of $W(\mathfrak{c})$. Define, for each $0\leqq j\in\mathbf{Z}$, a character λ_j: $W(\mathfrak{c})\to\Omega$ by $\lambda_j(w)=(\lambda_1(w))^j$. Then (2.5) shows the following refinement of [13, Th. 7.1]:

Proposition 2.3. *For each primitive character χ of $W_t(\mathfrak{c})$ with values in K, there is a unique primitive local ring $\mathcal{K}$ of $\mathcal{L}(Nr(\mathfrak{c})d;K)$ characterized by the following properties:*

(2.6a) *The morphism* (2.5) *induces an isomorphism:*

$$\mathcal{K}\simeq\mathcal{O}_K[[W_0]]\otimes_{\Lambda_K}\mathcal{L}_K;$$

(2.6b) *For each character of finite order ε: $W_0\to\Omega$ with $\Gamma_r=\Gamma\cap\operatorname{Ker}(\varepsilon)$ and for each non-negative integer j, the theta series $\theta(\varepsilon\chi\lambda_j)$ in $S_{j+1}(\Gamma_1(Nr(\mathfrak{c})dp^r))$ belongs to K.*

Now we shall construct the representation π as in Theorem 2.1 for the local ring $\mathcal{K}$ given in Proposition 2.3. By definition, there is a tautological character

$$\Phi\colon\ W_0\to\mathcal{O}_K[[W_0]]$$

given by $\Phi(w)=w\in\mathcal{O}_K[[W_0]]$ for $w\in W_0$. Since χ has values in $\mathcal{O}_K$, we can define another character $\chi\cdot\Phi$: $W(\mathfrak{c})\to\mathcal{O}_K[[W_0]]$ by $\chi\cdot\Phi(w)=\lambda_1(w_0)^{-1}\chi(w_t)\Phi(w_0)$ where we write $w=(w_0,w_t)\in W(\mathfrak{c})$ with $w_0\in W_0$ and $w_t\in W_t(\mathfrak{c})$. Let ε: $W_0\to K$ be a character of finite order. Then for each integer j, the ideal $\mathfrak{p}_{j,\varepsilon}$ of $\mathcal{O}_K[[W_0]]$ generated by $\Phi(w)-\varepsilon\lambda_j(w)$ for $w\in W_0$ is a prime divisor of $\mathcal{O}_K[[W_0]]$ over the prime element $P_{j,\varepsilon'}$ of Λ_K for $\varepsilon'=\varepsilon|_\Gamma$. By definition, $\chi\cdot\Phi \bmod \mathfrak{p}_{j+1,\varepsilon}$ coincides with $\varepsilon\chi\lambda_j$ as a character of $W(\mathfrak{c})$. By class field theory, the group $M_A^\times/\overline{M^\times M_\infty^\times}$ is isomorphic to the Galois group over M of the maximal abelian extension M_{ab} in $\bar{\mathbf{Q}}$ of M. Thus $\chi\cdot\Phi$ can be regarded as a character of the Galois group $\mathfrak{G}_M=\operatorname{Gal}(\bar{\mathbf{Q}}/M)$. Let π be the induced representation of $\chi\cdot\Phi$ to $\mathfrak{G}=\operatorname{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$; then, we have a two dimensional representation

$$\pi\colon\ \mathfrak{G}\to\operatorname{GL}_2(\mathcal{O}_K[[W_0]]).$$

By definition, $\pi \bmod \mathfrak{p}_{j+1,\varepsilon}$ gives the induced representation of $\varepsilon\chi\lambda_j$ from $\mathfrak{G}_M$ to $\mathfrak{G}$. Note that the representation $\pi(\theta(\varepsilon\chi\lambda_j))$ as in (2.1) is nothing but the induced representation of $\varepsilon\chi\lambda_j$ from $\mathfrak{G}_M$ to $\mathfrak{G}$. Thus we have

Theorem 2.4. *The induced representation of* $\chi\cdot\Phi$ *from* $\mathfrak{G}_M$ *to* $\mathfrak{G}$ *gives the representation* π *as in* (2.2) *attached to the local ring* $\mathscr{K}$ *of* $\not{h}(Nr(\mathfrak{c})d;K)$ *given in Proposition* 2.3.

Here are some remarks about this theorem: Firstly, the induced representation of $\chi\cdot\Phi$ to $\mathfrak{G}$ is simple, because the inner automorphism of $\mathfrak{G}$ induced by complex conjugation changes the character $\chi\cdot\Phi$. Secondly, the construction of the induced representation can be carried out even for primes $p=2$ or 3 with minor modification.

§3. A result on cohomology groups of modular curves

Fix a positive integer N prime to p. It is well known (e.g. [9, p. 240]) that the group $\Gamma_1(Np^r)$ has no torsion if $Np^r \geqq 3$. We always consider $\Gamma_1(Np^r)$ for positive r with $p\geqq 5$; so, this condition is automatically satisfied in our case. Put, for the upper half complex plane $\mathfrak{H}$

$$Y_r=\mathfrak{H}/\Gamma_1(Np^r)$$

as a complex manifold, and let X_r denote its smooth compactification. We consider usual sheaf cohomology groups

$$H^i(Y_r,M) \quad\text{and}\quad H^i(X_r,M)$$

of each constant sheaf M of $\mathbf{Z}$-modules. We can identify canonically $H^1(X_r,\mathbf{R})$ with the de Rham cohomology group on X_r with coefficients in $\mathbf{R}$. Then, the correspondence: $f\mapsto \mathrm{Re}(f\,dz)$ gives an $\mathbf{R}$-linear isomorphism

$$S_2(\Gamma_1(Np^r))\simeq H^1(X_r,\mathbf{R}). \tag{3.1}$$

As given in Shimura [25, Chap. 8], one can define a natural action of Hecke operators $T(l)$ and $T(l,l)$ on $H^1(X_r,M)$ and $H^1(Y_r,M)$ (for details, see the following section). Then, the morphism (3.1) is compatible with the action of Hecke operators on both sides. It is well known that

$$H^1(X_r,M)=H^1(X_r,\mathbf{Z})\otimes_{\mathbf{Z}}M \quad\text{and}\quad H^1(Y_r,M)=H^1(Y_r,\mathbf{Z})\otimes_{\mathbf{Z}}M.$$

Thus, the Hecke algebra $\not{h}_2(\Gamma_1(Np^r);\mathbf{Z})$ acts on $H^1(X_r,\mathbf{Z})$ because of (3.1), and therefore, $\not{h}_2(\Gamma_1(Np^r);\mathbf{Z}_p)$ acts on $H^1(X_r,\mathbf{Q}_p)$, $H^1(X_r,\mathbf{Z}_p)$ and $H^1(X_r,\mathbf{T}_p)$ for $\mathbf{T}_p=\mathbf{Q}_p/\mathbf{Z}_p$. If U denotes either of X_r or Y_r, we have

$$H^1(U,\mathbf{T}_p)\simeq H^1(U,\mathbf{Z}_p)\otimes_{\mathbf{Z}_p}\mathbf{T}_p\simeq H^1(U,\mathbf{Q}_p)/H^1(U,\mathbf{Z}_p). \tag{3.2}$$

We simply write

$$\mathscr{V}_r=H^1(X_r,\mathbf{T}_p) \quad\text{and}\quad \mathscr{W}_r=H^1(Y_r,\mathbf{T}_p).$$

By (3.2), $\mathscr{V}_r$ and $\mathscr{W}_r$ are p-divisible modules and their $\mathbf{Z}_p$-corank are finite. Thus $\mathrm{End}(\mathscr{V}_r)$ and $\mathrm{End}(\mathscr{W}_r)$ are free of finite rank over $\mathbf{Z}_p$, and therefore, we can define the idempotent attached to $T(p)$ in $\mathrm{End}(\mathscr{V}_r)$ and $\mathrm{End}(\mathscr{W}_r)$ by the p-adic limit

$$e_r=\lim_{n\to\infty} T(p)^{p^{tn}(p^t-1)}$$

for a suitable positive integer t. We shall define the ordinary parts of $\mathcal{V}_r$ and $\mathcal{W}_r$ by

$$\mathcal{V}_r^0 = e_r \mathcal{V}_r \quad \text{and} \quad \mathcal{W}_r^0 = e_r \mathcal{W}_r.$$

Naturally, $\mathcal{V}_r^0$ is a module over $\mathscr{h}_2^0(\Gamma_1(Np^r); \mathbf{Z}_p)$. Since $\Gamma_0(Np^r)$ normalizes $\Gamma_1(Np^r)$ and the quotient $\Gamma_0(Np^r)/\Gamma_1(Np^r)$ is isomorphic to $(\mathbf{Z}/Np^r\mathbf{Z})^\times$, this finite group acts on $\mathcal{V}_r^0$ and $\mathcal{W}_r^0$. We specify this isomorphism by

$$\Gamma_0(Np^r) \ni \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d \bmod Np^r \in (\mathbf{Z}/Np^r\mathbf{Z})^\times,$$

and we take the limit:

$$\mathcal{V} = \varinjlim_r \mathcal{V}_r, \qquad \mathcal{W} = \varinjlim_r \mathcal{W}_r, \qquad \mathcal{V}^0 = \varinjlim_r \mathcal{V}_r^0, \qquad \mathcal{W}^0 = \varinjlim_r \mathcal{W}_r^0$$

and

$$Z = \varprojlim_r (\mathbf{Z}/Np^r\mathbf{Z})^\times \simeq \mathbf{Z}_p^\times \times (\mathbf{Z}/N\mathbf{Z})^\times,$$

where the first four injective limits are taken with respect to the restriction morphisms of cohomology groups. Then, the topological group Z naturally acts on $\mathcal{V}$, $\mathcal{V}^0$, $\mathcal{W}$ and $\mathcal{W}^0$. We regard Γ as a subgroup of Z. Then these modules become continuous modules over the Iwasawa algebra $\Lambda = \mathbf{Z}_p[[\Gamma]]$ if we equip with them the discrete topology. Let V^0 and W^0 be the Pontryagin dual modules of $\mathcal{V}^0$ and $\mathcal{W}^0$; i.e.,

$$V^0 = \mathrm{Hom}(\mathcal{V}^0, \mathbf{T}_p) \quad \text{and} \quad W^0 = \mathrm{Hom}(\mathcal{W}^0, \mathbf{T}_p).$$

Then V^0 and W^0 are compact Λ-modules.

Theorem 3.1. *Let Γ_r denote the subgroup $1 + p^r\mathbf{Z}_p$ of Γ. Then we have*

(i) *For each integer $r > 0$, the restriction morphism of cohomology groups induces an isomorphism of the module $\mathcal{V}_r^0$ (resp. $\mathcal{W}_r^0$) onto the module $(\mathcal{V}^0)^{\Gamma_r}$ (resp. $(\mathcal{W}^0)^{\Gamma_r}$) of all Γ_r-invariants of $\mathcal{V}^0$ (resp. $\mathcal{W}^0$).*

(ii) *The Λ-modules V^0 and W^0 are free of finite rank over Λ.*

(iii) $\mathrm{rank}_\Lambda(V^0) = 2 \cdot \mathrm{rank}_\Lambda(\mathscr{h}^0(N; \mathbf{Z}_p))$ *and*

$$\mathrm{rank}_\Lambda(W^0) = \mathrm{rank}_\Lambda(V^0) + \tfrac{1}{2}\varphi(p) \sum_{0 < t \mid N} \varphi(t)\varphi(N/t),$$

where φ denotes the Euler function and t runs over all divisor of N.

As will become clear in the proof of Theorem 3.1, which will be given in §6, the restriction morphism of $\mathcal{W}_r$ into $\mathcal{W}$ has fairly big kernel, and thus, the assertion similar to Theorem 3.1 for the whole $\mathcal{W}$ is false.

§4. Parabolic cohomology

In this and next section, we gather some results on the cohomology groups of $\Gamma_1(Np^r)$, which play a central role in the proof of Theorem 3.1. Let $\mathrm{GL}_2(\mathbf{R})$ act on the upper half complex plane $\mathfrak{H}$ in the following manner: For $\alpha \in \mathrm{GL}_2(\mathbf{R})$

with $\det(\alpha)>0$, we let α act on $\mathfrak{H}$ through the linear fractional transformation, and for $\varepsilon=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$ we let ε act on $\mathfrak{H}$ by $\varepsilon(z)=-\bar{z}$. Then this gives a well defined (real analytic) action of $\mathrm{GL}_2(\mathbf{R})$ on $\mathfrak{H}$. Let ι: $M_2(\mathbf{R})\to M_2(\mathbf{R})$ be the main involution defined by $\alpha+\alpha^\iota=Tr(\alpha)$, and let Δ be a semi-group in $\mathrm{GL}_2(\mathbf{Q})$. Define another semi-group Δ^ι by the image of Δ under ι. Let M be a $\mathbf{Z}$-module with left Δ^ι-action and Φ be a congruence subgroup of $\mathrm{SL}_2(\mathbf{Z})$ contained in Δ and Δ^ι. Thus M becomes a left Φ-module. We can define the abstract Hecke ring $R(\Phi,\Delta)$ by giving the multiplication law as in [25, 3.1] on the free $\mathbf{Z}$-module generated by double cosets $\Phi\alpha\Phi$ for all $\alpha\in\Delta$. We shall consider the usual cohomology group $H^1(\Phi,M)$ and the parabolic cohomology group $H^1_P(\Phi,M)$ defined as follows: Let U be any unipotent subgroup of $\mathrm{SL}_2(\mathbf{Q})$ and put $\Phi_U=\{\pm 1\}U\cap\Phi$. Then we have the restriction map

$$\mathrm{res}_U\colon H^1(\Phi,M)\to H^1(\Phi_U,M).$$

We shall define

(4.1 a) $H^1_P(\Phi,M)=\{c\in H^1(\Phi,M)\,|\,\mathrm{res}_U(c)=0 \text{ for all unipotent subgroups } U\}$.

Let U_∞ be the standard unipotent subgroup $\left\{\begin{pmatrix}1&u\\0&1\end{pmatrix}\middle|\, u\in\mathbf{Q}\right\}$. Then, every unipotent subgroup U of $\mathrm{SL}_2(\mathbf{Q})$ is written as $\alpha U_\infty\alpha^{-1}$ with $\alpha\in\mathrm{SL}_2(\mathbf{Z})$. The correspondence: $U\mapsto\alpha(\infty)\in\mathbf{P}^1(\mathbf{Q})=\mathbf{Q}\bigcup\{\infty\}$ gives a bijection between unipotent subgroups and cusps for $\mathrm{SL}_2(\mathbf{Z})$; so, for each cusp $s\in\mathbf{P}^1(\mathbf{Q})$, we may write U_s for the corresponding unipotent subgroup. We write Φ_s for Φ_{U_s}. Another description of Φ_s is given by

$$\Phi_s=\{\alpha\in\Phi\,|\,\alpha(s)=s\}.$$

Let $C(\Phi)$ be a representative set for the Φ-equivalence classes of cusps, which is a finite set. Then for each cusp $s\in\mathbf{P}^1(\mathbf{Q})$, we can find $\gamma\in\Phi$ and $s_0\in C(\Phi)$ so that $\gamma\Phi_s\gamma^{-1}=\Phi_{s_0}$. Thus it is sufficient to consider the restriction map res_{U_s} only for cusps in $C(\Phi)$ in order to define the parabolic cohomology group. This simplified definition gives an exact sequence:

(4.1 b) $$0\to H^1_P(\Phi,M)\to H^1(\Phi,M)\to\bigoplus_{s\in C(\Phi)}H^1(\Phi_s,M),$$

where the last arrow sends each cohomology class to the sum of its restriction to Φ_s. Put $G^i(\Phi,M)=\bigoplus_{s\in C(\Phi)}H^i(\Phi_s,M)$. We shall define the action of the abstract Hecke ring $R(\Phi,\Delta)$ on $H^1(\Phi,M)$, $H^1_P(\Phi,M)$ and $G^1(\Phi,M)$ by following [25, 8.3]. Let u: $\Phi\to M$ be a 1-cocycle; thus, u satisfies the relation: $u(\alpha\beta)=\alpha u(\beta)+u(\alpha)$ for all α, $\beta\in\Phi$. Let Φ' be another congruence subgroup of $\mathrm{SL}_2(\mathbf{Z})$ contained in Δ and Δ^ι. We shall define an operator $[\Phi\alpha\Phi']$: $H^1(\Phi,M)\to H^1(\Phi',M)$ for each double coset $\Phi\alpha\Phi'$ in Δ. Decompose the double coset $\Phi\alpha\Phi'$ into a disjoint union of left cosets $\bigcup_i\Phi\alpha_i$. Then the number of left cosets in $\Phi\alpha\Phi'$ is finite and for each $\gamma\in\Phi'$, by definition we can find $\gamma_i\in\Phi$ so that $\gamma_i\alpha_j=\alpha_i\gamma$ for some α_j. Then we can define a map v: $\Phi'\to M$ by $v(\gamma)=\sum_i\alpha_i^\iota\cdot u(\gamma_i)$. One can check that v is a 1-cocycle, and the cohomology class of

v depends only on the cohomology class of u. Thus this correspondence: $u \mapsto v$ gives a morphism

$$[\Phi\alpha\Phi']: H^1(\Phi, M) \to H^1(\Phi', M).$$

By definition, $[\Phi\alpha\Phi']$ takes parabolic cocycles into themselves and defines an action of $[\Phi\alpha\Phi']$ on $H_P^1(\Phi, M)$. By applying this argument to the special case: $\Phi = \Phi'$, the abstract Hecke ring $R(\Phi, \Delta)$ acts on $H^1(\Phi, M)$ and $H_P^1(\Phi, M)$. Similarly, we can define an operator

$$[\Phi\alpha\Phi']: H^0(\Phi, M) \to H^0(\Phi', M)$$

by putting $x | [\Phi\alpha\Phi'] = \sum_i \alpha_i^\iota \cdot x$ for each Φ-invariant $x \in M$. Via this action, $R(\Phi, \Delta)$ acts on $H^i(\Phi, M)$ for $i = 0$, 1 functorially. We shall now introduce an action of $R(\Phi, \Delta)$ on $G^i(\Phi, M)$. If the number of left Φ_t-cosets in $\Phi_t \alpha \Phi'_s$ for $t \in C(\Phi)$ and $s \in C(\Phi')$ is finite, we can define a morphism

$$[\Phi_t \alpha \Phi'_s]: H^i(\Phi_t, M) \to H^i(\Phi'_s, M) \qquad \text{for } i = 0, 1$$

in the same manner as above. Fix $s \in C(\Phi')$ and write, as disjoint unions,

(4.2a) $\Phi\alpha\Phi' = \bigcup_i \Phi \beta_i \Phi'_s$,

(4.2b) $\Phi \beta_i \Phi'_s = \bigcup_j \Phi \beta_i \pi_j$ with $\pi_j \in \Phi'_s$ for each β_i in (4.2a).

Lemma 4.1. *Let* $t = \beta_i(s)$ *in* $\mathbf{P}^1(\mathbf{Q})$. *Then the union* $\bigcup_j \Phi_t \beta_i \pi_j$ *coincides with* $\Phi_t \beta_i \Phi'_s$ *and is disjoint. Especially, the number of left cosets in* $\Phi_t \beta_i \Phi'_s$ *is finite.*

Proof. For each $\delta \in \Phi_t \beta_i \Phi'_s$, write $\delta = \delta_t \beta_i \delta_s$ with $\delta_t \in \Phi_t$ and $\delta_s \in \Phi'_s$. Since $\Phi \beta_i \Phi'_s = \bigcup_j \Phi \beta_i \pi_j$, we can find j and $\gamma \in \Phi$ so that $\delta = \gamma \beta_i \pi_j$. Then we know that

$$\gamma^{-1} \delta_t = \beta_i \pi_j \delta_s^{-1} \beta_i^{-1}$$

and thus $\gamma^{-1} \delta_t(t) = t$. This shows that $\gamma \in \Phi_t$, and we have

$$\Phi_t \beta_i \Phi'_s = \bigcup_j \Phi_t \beta_i \pi_j.$$

Since $\Phi_t \beta_i \pi_j \subset \Phi \beta_i \pi_j$, it is disjoint.

Now we are ready to introduce a morphism

$$[\Phi\alpha\Phi']: G^i(\Phi, M) \to G^i(\Phi', M) \qquad \text{for } i = 0, 1.$$

For a given $s \in C(\Phi')$, decompose $\Phi\alpha\Phi'$ as in (4.2a). By definition, we can find $\gamma \in \Phi$ so that $\gamma \beta_i(s) \in C(\Phi)$. Thus, we may assume that $\beta_i(s) \in C(\Phi)$ by substituting $\gamma \beta_i$ for β_i if necessary. Then, by Lemma 4.1, we can define a morphism

$$[\Phi_t \beta_i \Phi'_s]: H^i(\Phi_t, M) \to H^i(\Phi'_s, M) \qquad \text{for } t = \beta_i(s).$$

For $c \in G^i(\Phi, M)$ (resp. $G^i(\Phi', M)$), let us write c_t (resp. c_s) for the component of c in $H^i(\Phi_t, M)$ (resp. $H^i(\Phi'_s, M)$). Then, we shall define

$$(c | [\Phi\alpha\Phi'])_s = \sum_i c_{\beta_i(s)} | [\Phi_{\beta_i(s)} \beta_i \Phi'_s] \tag{4.3}$$

Proposition 4.2. *The operator defined by* (4.3) *depends only on the double coset* $\Phi\alpha\Phi'$, *and via this action, the module* $G^i(\Phi, M)$ *becomes a* $R(\Phi, \Delta)$*-module. Furthermore, the exact sequence* (4.1b) *gives that of* $R(\Phi, \Delta)$*-modules.*

Proof. We shall show only that the operator (4.3) is well defined, since the other assertions follow from the definition and the result in [25, 3.1]. If $\beta\in\Phi\beta_i\Phi'_s$, then we can write $\beta=\gamma\beta_i\gamma_s$ with $\gamma\in\Phi$ and $\gamma_s\in\Phi'_s$. Moreover, if $t=\beta(s)=\beta_i(s)$, then $t=\beta(s)=\gamma\beta_i\gamma_s(s)=\gamma\beta_i(s)=\gamma(t)$, which shows that $\gamma\in\Phi_t$ and $\Phi_t\beta\Phi'_s=\Phi_t\beta_i\Phi'_s$. This shows that the operator $[\Phi\alpha\Phi']$ does not depend on the choice of β_i and is determined only by the double coset $\Phi\alpha\Phi'$.

Now we shall relate the cohomology groups $H^1(\Phi, M)$ and $H^1_P(\Phi, M)$ with those of certain sheaves on $\Phi\backslash\mathfrak{H}$. Assume that

(4.4) *Φ has no non-trivial finite subgroup*

Later, we will be chiefly concerned with the groups $\Gamma_1(Np^r)$ with $p\geqq 5$ and $r\geqq 1$, and this condition is automatically satisfied in this case. Write Y for the complex (open) manifold $\Phi\backslash\mathfrak{H}$. We give the Δ^ι-module M the discrete topology and define $F(M)=\Phi\backslash(\mathfrak{H}\times M)$. Then $F(M)$ is an étale covering of Y, and we can consider the sheaf of continuous sections of $F(M)$ over Y, which we denote by the same symbol $F(M)$. When we have to indicate that $F(M)$ is a sheaf on Y, we write $F(M)|_Y$ instead of $F(M)$. Then, we consider the usual cohomology group $H^1(Y, F(M))$ and that of compact support $H^1_c(Y, F(M))$. We shall define the parabolic (sheaf) cohomology group $H^1_P(Y, F(M))$ by the natural image of $H^1_c(Y, F(M))$ in $H^1(Y, F(M))$. Then, there are well known isomorphisms (e.g. [9, Prop. 1.1]), which make the following diagram commutative:

(4.5)
$$\begin{tikzcd}
H^1(Y, F(M)) \arrow[r, phantom, "\simeq"] & H^1(\Phi, M) \\
H^1_P(Y, F(M)) \arrow[r, phantom, "\simeq"] \arrow[u] & H^1_P(\Phi, M). \arrow[u]
\end{tikzcd}$$

We now recall the action of double cosets on sheaf cohomology groups (e.g. [9, §3]). Let Φ' be another congruence subgroup of $\mathrm{SL}_2(\mathbf{Z})$ satisfying (4.4) and contained in Δ and Δ^ι. Put for each $\alpha\in\Delta$,

$$\Phi_\alpha=\Phi'\cap\alpha^{-1}\Phi\alpha, \qquad \Phi^\alpha=\alpha\Phi'\alpha^{-1}\cap\Phi=\alpha\Phi_\alpha\alpha^{-1}$$

and

$$Y'=\Phi'\backslash\mathfrak{H}, \qquad Y^\alpha=\Phi^\alpha\backslash\mathfrak{H}, \qquad Y_\alpha=\Phi_\alpha\backslash\mathfrak{H}.$$

Then the map α: $\mathfrak{H}\times M\to\mathfrak{H}\times M$ defined by $\alpha(z, v)=(\alpha^{-1}(z), \alpha^\iota v)$ induces a morphism $[\alpha]$: $F(M)|_{Y^\alpha}\to F(M)|_{Y^\alpha}$, which gives rise to a morphism $[\alpha]$: $H^i(Y^\alpha, F(M))\to H^i(Y_\alpha, F(M))$. Since Y_α/Y' is an etale covering, we have the trace map

$$\mathrm{Tr}_{Y_\alpha/Y'}\colon\ H^i(Y_\alpha, F(M))\to H^i(Y', F(M))$$

and the restriction map

$$\mathrm{res}_{Y^\alpha/Y}\colon\ H^i(Y, F(M))\to H^i(Y^\alpha, F(M)).$$

We shall define the action of double coset

$$[\Phi\alpha\Phi']\colon\ H^i(Y, F(M)) \to H^i(Y', F(M))$$

by $\mathrm{Tr}_{Y_\alpha/Y'} \circ [\alpha] \circ \mathrm{res}_{Y^\alpha/Y}$. In exactly the same manner, we define the action of $[\Phi\alpha\Phi']$ on $H^i_c(Y, F(M))$ and $H^1(Y, F(M))$. This action is compatible with the isomorphism (4.5).

Let us now give some examples of modules M, which will be dealt with later. Firstly, we consider the column vector space $L_n(\mathbf{Z}) = \mathbf{Z}^{n+1}$ for each non-negative integer n. Let ${}^t(x, y)$ be a variable vector in $L_1(\mathbf{Z})$ and define

$$\begin{pmatrix} x \\ y \end{pmatrix}^n = {}^t(x^n, x^{n-1}y, \ldots, y^n) \in L_n(\mathbf{Z}).$$

We let $M_2(\mathbf{Z})$ act on $L_n(\mathbf{Z})$ through the symmetric n-th tensor representation explicitly specified by

$$\begin{pmatrix} a & b \\ e & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}^n = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}^n.$$

For any $\mathbf{Z}$-module A, put $L_n(A) = L_n(\mathbf{Z}) \otimes_{\mathbf{Z}} A$, which is equipped with the natural left action of $M_2(\mathbf{Z})$. For $\Phi = \Gamma_1(Np^r)$, we take $M_2(\mathbf{Z}) \cap \mathrm{GL}_2(\mathbf{Q})$ as the semi-group Δ. Then the Hecke ring $R(\Phi, \Delta)$ acts on the cohomology groups for $L_n(A)$. For each prime l, the Hecke operators $T(l)$ and $T(l, l)$ on the cohomology groups are given by the action of double cosets:

(4.6a)
$$T(l) = \left[\Phi \begin{pmatrix} 1 & 0 \\ 0 & l \end{pmatrix} \Phi\right]$$

$$T(l, l) = \begin{cases} [\Phi l \sigma_l \Phi] & \text{if } l \nmid Np^r, \\ 0 & \text{if } l \mid Np^r, \end{cases}$$

where σ_l is an element of $\mathrm{SL}_2(\mathbf{Z})$ such that $\sigma_l \equiv \begin{pmatrix} * & * \\ 0 & l \end{pmatrix} \bmod Np^r$. We define the operator $T(1, n)$ for positive integer n by

(4.6b)
$$T(1, n) = \left[\Phi \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \Phi\right].$$

Next, we shall introduce another module. Let p be the fixed prime and N be a positive integer prime to p. For integers $r \geqq s \geqq 0$, put

$$\Phi_r^s = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) \,\middle|\, c \equiv 0 \bmod Np^r, a \equiv d \equiv 1 \bmod Np^s \right\}$$

$$\Delta_r^s = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbf{Z}) \,\middle|\, ad - bc > 0, c \equiv 0 \bmod Np^r, a \equiv 1 \bmod Np^s \right\}.$$

For each integer j, let $(\Delta_r^s)^t$ act on $\mathbf{Z}/p^r\mathbf{Z}$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^t \cdot x = a^j x \quad \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Delta_r^s \right).$$

Write this $(\Delta_r^s)^\iota$-module by $\mathbf{Z}/p^r\mathbf{Z}(j)$. Then the Hecke ring $R(\Phi_r^s, \Delta_r^s)$ acts on the cohomology groups for this module. Especially, we can define Hecke operators $T(l)$, $T(l,l)$ and $T(1,n)$ for the cohomology groups of $\mathbf{Z}/p^r\mathbf{Z}(j)$ by (4.6a, b). For our later use, we shall cite a result of [25, Chap. 3]:

Lemma 4.3.

(i) *We have an equality of double cosets:* $\Phi_r^s \begin{pmatrix} 1 & 0 \\ 0 & p^m \end{pmatrix} \Phi_r^s = \Phi_r^s \begin{pmatrix} 1 & 0 \\ 0 & p^m \end{pmatrix} \Phi_{r-m}^s$ *for each r, s and m satisfying* $r-s \geqq m > 0$ *and* $s \geqq 1$; *especially,*

$$\Phi_r^s \begin{pmatrix} 1 & 0 \\ 0 & p^{r-s} \end{pmatrix} \Phi_r^s = \Phi_r^s \begin{pmatrix} 1 & 0 \\ 0 & p^{r-s} \end{pmatrix} \Gamma_1(Np^s).$$

(ii) *Let r, s and m be as above. Take* $\alpha_u \in M_2(\mathbf{Z})$ *for each* $u \in \mathbf{Z}$ *so that*

$$\alpha_u \equiv \begin{pmatrix} 1 & u \\ 0 & p^m \end{pmatrix} \bmod N p^{\max(m,r)} \quad \textit{and} \quad \det(\alpha_u) = p^m.$$

Then we have a disjoint decomposition:

$$\Phi_r^s \begin{pmatrix} 1 & 0 \\ 0 & p^m \end{pmatrix} \Phi_r^s = \bigcup_{u \bmod p^m} \Phi_r^s \alpha_u.$$

(iii) *For each prime l, we have disjoint decompositions:*

$$\Phi_r^s \begin{pmatrix} 1 & 0 \\ 0 & l \end{pmatrix} \Phi_r^s = \begin{cases} \bigcup_{u \bmod l} \Phi_r^s \begin{pmatrix} 1 & u \\ 0 & l \end{pmatrix} \cup \Phi_r^s \sigma_l \begin{pmatrix} l & 0 \\ 0 & 1 \end{pmatrix}, & \text{if } l \nmid Np, \\ \bigcup_{u \bmod l} \Phi_r^s \begin{pmatrix} 1 & u \\ 0 & l \end{pmatrix}, & \text{if } l \mid Np, \end{cases}$$

and

$$\Phi_r^s l \sigma_l \Phi_r^s = \Phi_r^s l \sigma_l \quad \text{if } l \mid Np,$$

where σ_l *is an element of* $\mathrm{SL}_2(\mathbf{Z})$ *satisfying* $\sigma_l \equiv \begin{pmatrix} * & * \\ 0 & l \end{pmatrix} \bmod Np^r$.

(iv) *Take* $\delta \in \mathrm{SL}_2(\mathbf{Z})$ *such that* $\delta \equiv \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \bmod p^{2r}$ *and* $\delta \equiv 1 \bmod N^2$. *Then we have a disjoint decomposition:*

$$\Phi_r^0 \delta \Phi_r^0 = \bigcup_{u \bmod p^r} \Phi_r^0 \delta \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}.$$

The assertions (i), (ii) and (iii) follow from [25, 3.3] by a straight forward calculation, and (iv) is well known (e.g. [10, p. 235]); so, we omit the proof.

We now relate the cohomology groups for $L_n(\mathbf{Z}/p^r\mathbf{Z})$ and $\mathbf{Z}/p^r\mathbf{Z}(n)$. Define maps

$$i_r\colon L_n(\mathbf{Z}/p^r\mathbf{Z}) \to \mathbf{Z}/p^r\mathbf{Z}(n) \quad \text{and} \quad j_r\colon (\mathbf{Z}/p^r\mathbf{Z})(-n) \to L_n(\mathbf{Z}/p^r\mathbf{Z})$$

by $i_r({}^t(x_0, \ldots, x_n)) = x_n$ and $j_r(x) = {}^t(x, 0, \ldots, 0)$. We write simply Φ_r and Δ_r for Φ_r^0 and Δ_r^0. Then i_r and j_r are morphisms of Φ_r-modules, and thus, they covariantly induce morphism of cohomology groups

$$(i_r)_*\colon\ H^1(\Phi_r, L_n(\mathbf{Z}/p^r\mathbf{Z}))\to H^1(\Phi_r, \mathbf{Z}/p^r\mathbf{Z}(n)),$$

$$(j_r)_*\colon\ H^1(\Phi_r, \mathbf{Z}/p^r\mathbf{Z}(-n))\to H^1(\Phi_r, L_n(\mathbf{Z}/p^r\mathbf{Z})),$$

which also induce morphism of parabolic cohomology groups. Next, we choose $\tau\in M_2(\mathbf{Z})$ such that $\det(\tau)=p^r$, $\tau\equiv\begin{pmatrix}0 & -1\\ p^r & 0\end{pmatrix}\bmod p^{2r}$ and $\tau\equiv\begin{pmatrix}1 & 0\\ 0 & p^r\end{pmatrix}\bmod N^2$. Then, $\tau\Phi_r\tau^{-1}=\Phi_r$ and

$$\tau\begin{pmatrix}a & b\\ c & d\end{pmatrix}\tau^{-1}\equiv\begin{pmatrix}d & *\\ * & a\end{pmatrix}\bmod p^r \quad \text{for } \begin{pmatrix}a & b\\ c & d\end{pmatrix}\in\Phi_r.$$

Let φ denote the isomorphism of $\mathbf{Z}$-modules: $\mathbf{Z}/p^r\mathbf{Z}(n)\to\mathbf{Z}/p^r\mathbf{Z}(-n)$ which induces the identity to the underlying $\mathbf{Z}$-module $\mathbf{Z}/p^r\mathbf{Z}$. For each 1-cocycle u: $\Phi_r\to\mathbf{Z}/p^r\mathbf{Z}(n)$, define a map $u|[\tau]$: $\Phi_r\to\mathbf{Z}/p^r\mathbf{Z}(-n)$ by $u|[\tau](\alpha)=\varphi(u(\tau\alpha\tau^{-1}))$. Then $u|[\tau]$ is a 1-cocycle, and this correspondence induces an isomorphism:

$$[\tau]\colon\ H^1(\Phi_r, \mathbf{Z}/p^r\mathbf{Z}(n))\simeq H^1(\Phi_r, \mathbf{Z}/p^r\mathbf{Z}(-n)),$$

which induces an isomorphism on the parabolic cohomology subgroup.

Definition. Now we define important morphisms

$$\pi_r\colon\ H^1(\Phi_r, \mathbf{Z}/p^r\mathbf{Z}(n))\to H^1(\Phi_r, L_n(\mathbf{Z}/p^r\mathbf{Z})),$$

$$\iota_r\colon\ H^1(\Phi_r, L_n(\mathbf{Z}/p^r\mathbf{Z}))\to H^1(\Phi_r, \mathbf{Z}/p^r\mathbf{Z}(n))$$

by $\pi_r=[\Phi_r\delta\Phi_r]\circ(j_r)_*\circ[\tau]$ and $\iota_r=(i_r)_*$, where δ is an element of $\mathrm{SL}_2(\mathbf{Z})$ defined in Lemma 4.3, (iv).

Of course, the morphisms π_r and ι_r respect the parabolic cohomology subgroup. We now state the following generalization of [10, Th. 3.2]:

Theorem 4.4. *We have the following identity for each positive integer r:*

$$\pi_r\circ\iota_r=T(1,p^r) \quad \text{on } H^1(\Phi_r, L_n(\mathbf{Z}/p^r\mathbf{Z})),$$

$$\iota_r\circ\pi_r=T(1,p^r) \quad \text{on } H^1(\Phi_r, \mathbf{Z}/p^r\mathbf{Z}(n)).$$

Moreover, ι_r is equivariant under the action of $T(l)$ and $T(l,l)$ for all primes l.

Proof. Firstly, we shall show the equivariance of ι_r under the Hecke operators. Write T for either of $T(l)$ or $T(l,l)$. By Lemma 4.3, we can decompose T as a disjoint union of left cosets:

$$T=\bigcup_i \Phi_r\alpha_i \quad \text{with} \quad \alpha_i\equiv\begin{pmatrix}1 & *\\ 0 & *\end{pmatrix}\bmod p^r.$$

Thus, on $L_n(\mathbf{Z}/p^r\mathbf{Z})=(\mathbf{Z}/p^r\mathbf{Z})^{n+1}$, α_i^ι acts via a matrix of the form:

$$\begin{pmatrix}* & & *\\ & * & \\ & & * \\ 0 & & 1\end{pmatrix}\in M_{n+1}(\mathbf{Z}/p^r\mathbf{Z}).$$

Thus, for each 1-cocycle u: $\Phi_r \to L_n(\mathbf{Z}/p^r\mathbf{Z})$, we know that

$$i_r((u|T)(\gamma)) = i_r(\sum_i \alpha_i^\iota \cdot u(\gamma_i)) = \sum_i i_r(u(\gamma_i)) = (i_r \circ u|T)(\gamma) \quad (\gamma \in \Phi_r),$$

where $\gamma_i \in \Phi_r$ is defined by the relation $\alpha_i \gamma = \gamma_i \alpha_j$ for some j. Thus, we have the desired equivariance of ι_r.

Next, we shall prove the relation: $\pi_r \circ \iota_r = T(1, p^r)$. For each 1-cocycle u: $\Phi_r \to L_n(\mathbf{Z}/p^r\mathbf{Z})$, we have by definition

$$(\pi_r \circ \iota_r(u))(\gamma) = \sum_{a=0}^{p^r-1} \delta_a^\iota \cdot j_r(i_r(u(\tau\gamma_a\tau^{-1}))) \qquad \text{for } \gamma \in \Phi_r,$$

where $\delta_a = \delta \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ for δ as in Lemma 4.3, (iv), and $\gamma_a \in \Phi_r$ for each a is defined by $\delta_a \gamma = \gamma_a \delta_b$ for some b with $0 \leqq b < p^r$. Note that

$$\tau^\iota \cdot x = {}^t(x_n, 0, \ldots, 0) = j_r(i_r(x))$$

for $x = {}^t(x_0, \ldots, x_n) \in L_n(\mathbf{Z}/p^r\mathbf{Z})$. Then, we know from this formula that

$$((\pi_r \circ \iota_r)(u))(\gamma) = \sum_{a=0}^{p^r-1} (\tau\delta_a)^\iota u(\tau\gamma_a\tau^{-1}).$$

We write α_a for $\tau\delta_a$ and γ'_a for $\tau\gamma_a\tau^{-1}$. Then we see that

$$\alpha_a \equiv \begin{pmatrix} 1 & a \\ 0 & p^r \end{pmatrix} \bmod Np^r, \qquad \det(\alpha_a) = p^r \quad \text{and} \quad \alpha_a\gamma = \gamma'_a\alpha_b.$$

Then, Lemma 4.3(ii) shows that

$$T(1, p^r) = \bigcup_{a=0}^{p^r-1} \Phi_r \alpha_a \quad \text{(disjoint)},$$

and we have the identity: $\pi_r \circ \iota_r = T(1, p^r)$ on $H^1(\Phi_r, L_n(\mathbf{Z}/p^r\mathbf{Z}))$. Finally, we shall show that $\iota_r \circ \pi_r = T(1, p^r)$ on $H^1(\Phi_r, \mathbf{Z}/p^r\mathbf{Z}(n))$. For δ_a as above, we know that $\delta_a^\iota \equiv \begin{pmatrix} -a & -1 \\ 1 & 0 \end{pmatrix} \bmod p^r$; therefore, δ_a^ι acts on $L_n(\mathbf{Z}/p^r\mathbf{Z})$ via a matrix of the following form:

$$\begin{pmatrix} * & & & (-1)^n \\ & & (-1)^{n-1} & \\ & \cdot^{\cdot^{\cdot}} & & \\ 1 & & & 0 \end{pmatrix} \in M_{n+1}(\mathbf{Z}/p^r\mathbf{Z}).$$

Thus, for $x \in \mathbf{Z}/p^r\mathbf{Z}$, we know that $i_r(\delta_a^\iota j_r(x)) = x$.

For each 1-cocycle u: $\Phi_r \to \mathbf{Z}/p^r\mathbf{Z}(n)$, a simple calculation shows that for $\gamma \in \Phi_r$

$$((\iota_r \circ \pi_r)(u))(\gamma) = \sum_{a=0}^{p^r-1} i_r(\delta_a j_r(u(\gamma'_a))) = \sum_a u(\gamma'_a) = (u|T(1, p^r))(\gamma).$$

This finishes the proof.

Let A be either of $\mathbf{Z}/p^r\mathbf{Z}$ or $\mathbf{Z}_p$. Let e be the idempotent attached to $T(p)$ on $H^1(\Phi_r, L_n(A))$ and $H^1(\Phi_r, \mathbf{Z}/p^r\mathbf{Z}(n))$ (in the sense of [10, p. 236]).

Corollary 4.5. *We have isomorphisms for each* $r > s > 0$:

$$\mathrm{res}\colon\ eH^1(\Phi_r^s, L_n(A)) \simeq eH^1(\Gamma_1(Np^s), L_n(A)),$$

$$\mathrm{res}\colon\ eH^1(\Phi_1, L_n(A)) \simeq eH^1(\Phi_r, L_n(A)),$$

$$\iota_r \circ \mathrm{res}\colon\ eH^1(\Phi_1, L_n(\mathbf{Z}/p^r\mathbf{Z})) \simeq eH^1(\Phi_r, \mathbf{Z}/p^r\mathbf{Z}(n)),$$

where A denotes either of $\mathbf{Z}/p^r\mathbf{Z}$ or $\mathbf{Z}_p$. These assertions also hold for parabolic cohomology groups.

Proof. Note that $T(1,p^r) = T(p)^r$ on these cohomology groups. Thus, as seen in [10, p. 236], we can find a positive integer m so that $e = \lim_{n\to\infty} T(1,p^r)^{p^{mn}(p^m-1)}$ on these cohomology groups.

By Theorem 4.4, we have a commutative diagram:

$$\begin{tikzcd}
H^1(\Phi_r, L_n(\mathbf{Z}/p^r\mathbf{Z})) \arrow[r, "\iota_r"] \arrow[d, "T(1,p^r)"'] & H^1(\Phi_r, \mathbf{Z}/p^r\mathbf{Z}(n)) \arrow[d, "T(1,p^r)"] \arrow[dl, "\pi_r"'] \\
H^1(\Phi_r, L_n(\mathbf{Z}/p^r\mathbf{Z})) \arrow[r, "\iota_r"] & H^1(\Phi_r, \mathbf{Z}/p^r\mathbf{Z}(n)).
\end{tikzcd}$$

This yields another one:

$$\begin{tikzcd}
eH^1(\Phi_r, L_n(\mathbf{Z}/p^r\mathbf{Z})) \arrow[r, "\iota_r"] \arrow[d, "e"'] & eH^1(\Phi_r, \mathbf{Z}/p^r\mathbf{Z}(n)) \arrow[d, "e"] \arrow[dl, "\pi_r"'] \\
eH^1(\Phi_r, L_n(\mathbf{Z}/p^r\mathbf{Z})) \arrow[r, "\iota_r"] & eH^1(\Phi_r, \mathbf{Z}/p^r\mathbf{Z}(n)).
\end{tikzcd}$$

Since $T(1,p^r)$ gives automorphisms on $eH^1(\Phi_r, L_n(\mathbf{Z}/p^r\mathbf{Z}))$ and $eH^1(\Phi_r, \mathbf{Z}/p^r\mathbf{Z}(n))$, we obtain the desired isomorphism

$$\iota_r\colon\ eH^1(\Phi_r, L_n(\mathbf{Z}/p^r\mathbf{Z})) \simeq eH^1(\Phi_r, \mathbf{Z}/p^r\mathbf{Z}(n)).$$

By Lemma 4.3 (i) and (ii), we have a commutative diagram:

$$\begin{tikzcd}
H^1(\Gamma_1(Np^s), L_n(A)) \arrow[r, "\mathrm{res}"] \arrow[d, "T(1,p^{r-s})"'] & H^1(\Phi_r^s, L_n(A)) \arrow[d, "T(1,p^{r-s})"] \arrow[dl, "{\left[\Phi_r^s \begin{pmatrix}1 & 0\\ 0 & \mathrm{p}^{r-1}\end{pmatrix} \Gamma_1(Np^s)\right]}"] \\
H^1(\Gamma_1(Np^s), L_n(A)) \arrow[r, "\mathrm{res}"'] & H^1(\Phi_r^s, L_n(A)).
\end{tikzcd}$$

In the same manner as above, this yields an isomorphism

$$\mathrm{res}\colon\ eH^1(\Gamma_1(Np^s), L_n(A)) \simeq eH^1(\Phi_r^s; L_n(A)) \qquad \text{for } s > 0.$$

Similarly, one has

$$\mathrm{res}\colon\ eH^1(\Phi_1, L_n(A)) \simeq eH^1(\Phi_r, L_n(A)).$$

This proves the result for the usual cohomology groups. All the arguments as above still hold for parabolic cohomology groups and thus the lemma follows.

Let e_0 be the idempotent attached to $T(p)$ on $H^1(\Gamma_1(N), L_n(\mathbf{Z}_p))$. (Note that e and e_0 are different, since $T(p)$ of level N and that of level Np^r with $r \geqq 1$ are not equal).

Lemma 4.6. *Let $\Phi_r^s = \Gamma_1(Np^s) \cap \Gamma_0(p^r)$ for $r > s \geqq 0$, and let Φ be either of Φ_r^s or $\Gamma_1(Np^r)$ with $r \geqq 1$. Then, the modules $e_0 H^1(\Gamma_1(N), L_n(\mathbf{Z}_p))$ and $eH^1(\Phi, L_n(\mathbf{Z}_p))$ are $\mathbf{Z}_p$-free for each $n \geqq 0$.*

Proof. Firstly, we prove the lemma for $eH^1(\Phi, L_n(\mathbf{Z}_p))$. The cohomology sequence coming from the exact sequence: $0 \to L_n(\mathbf{Z}_p) \to L_n(\mathbf{Q}_p) \to L_n(\mathbf{T}_p) \to 0$ yields another exact sequence:

$$0 = H^0(\Phi, L_n(\mathbf{Q}_p)) \to H^0(\Phi, L_n(\mathbf{T}_p)) \to H^1(\Phi, L_n(\mathbf{Z}_p)) \to H^1(\Phi, L_n(\mathbf{Q}_p)).$$

Thus, what we have to prove is the vanishing

$$eH^0(\Phi, L_n(\mathbf{T}_p)) = 0.$$

The operator $T(p)$ acts by definition on $L_n(\mathbf{T}_p)$ by

$$x | T(p) = \sum_{i=0}^{p-1} \begin{pmatrix} 1 & -i \\ 0 & p \end{pmatrix}^{t} \cdot x \quad \text{(cf. Lemma 4.3 (iv)).}$$

The action of $\begin{pmatrix} 1 & -i \\ 0 & p \end{pmatrix}^{t}$ on $L_n(\mathbf{Z}_p) = \mathbf{Z}_p^{n+1}$ can be expressed matricially as

$$\begin{pmatrix} p^n & p^{n-1}\binom{n}{1} i, \ldots, i^n & \\ & p^{n-1}, \qquad \ldots, i^{n-1} & \\ & \ddots & \\ 0 & & 1 \end{pmatrix}.$$

It is easy to verify that $\sum_{i=0}^{p-1} i^m \equiv 0 \bmod p$ when $m = 0$ or $m \not\equiv 0 \bmod p-1$. Thus as a matrix acting on $L_n(\mathbf{Z}/p\mathbf{Z})$, we have that

$$T(p) = \begin{array}{c} \begin{array}{cc} n & 1 \end{array} \\ \left(\begin{array}{c|c} 0 & * \\ \hline 0 & 0 \end{array}\right) \end{array} \begin{array}{c} \\ n \\ 1 \end{array},$$

and $T(p)^2$ annihilates $L_n(\mathbf{Z}/p\mathbf{Z})$. Thus e annihilates $L_n(\mathbf{T}_p)$. Next, we shall take care of the case of level N. In this case, $T(p)$ acts on $L_n(\mathbf{Z}_p)$ as follows:

$$x | T(p) = \sum_{i=0}^{p-1} \begin{pmatrix} 1 & -i \\ 0 & p \end{pmatrix}^{t} \cdot x + \left(\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \sigma \right)^{t} \cdot x$$

where σ can be any element of $\mathrm{SL}_2(\mathbf{Z})$ with $\sigma \equiv \begin{pmatrix} * & 0 \\ 0 & p \end{pmatrix} \bmod N$. Since N is prime to p, we may assume that $\sigma \equiv 1 \bmod p$. Then similarly to the above argument, if one expresses $T(p)^2$ on $L_n(\mathbf{Z}/p\mathbf{Z})$ as a matrix, one knows that only the first row of $T(p)^2$ is possibly non-zero, and thus $eL_n(\mathbf{Z}/p\mathbf{Z})$ is contained in

$$\{{}^t(x, 0, \dots, 0) \in L_n(\mathbf{Z}/p\mathbf{Z}) \mid x \in \mathbf{Z}/p\mathbf{Z}\}.$$

However, there is $\delta \in \Gamma_1(N)$ such that $\delta \equiv \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \bmod p$. Then, for $x \in eL_n(\mathbf{Z}/p\mathbf{Z})$, $\delta x = x$ is impossible except when $x = 0$. This shows that

$$eL_n(\mathbf{Z}/p\mathbf{Z})^{\Gamma_1(N)} \simeq \{x \in eL_n(\mathbf{T}_p)^{\Gamma_1(N)} \mid px = 0\} = 0,$$

and hence, $eH^0(\Gamma_1(N), L_n(\mathbf{T}_p)) = 0$. Q.E.D.

Proposition 4.7. *For each integer $r > 0$ and for each $n > 0$, the restriction map combined with e gives isomorphisms:*

$$e_0 H^1(\Gamma_1(N), L_n(\mathbf{Z}_p)) \simeq eH^1(\Phi_r, L_n(\mathbf{Z}_p)),$$

$$e_0 H^1_P(\Gamma_1(N), L_n(\mathbf{Z}_p)) \simeq eH^1_P(\Phi_r, L_n(\mathbf{Z}_p)).$$

Proof. By Corollary 4.5, we may assume that $r = 1$. Let A be either of $\mathbf{Z}/p\mathbf{Z}$ or $\mathbf{Z}_p$. Since the map $\mathrm{Tr}_{\Gamma_1(N)/\Phi_1} \circ \mathrm{res}_{\Gamma_1(N)/\Phi_1}$ coincides with the multiplication by $p+1$ on $H^1(\Gamma_1(N), L_n(A))$, the restriction morphism gives an isomorphism of $H^1(\Gamma_1(N), L_n(A))$ into $H^1(\Phi_1, L_n(A))$. It is well known that for any congruence subgroup Φ,

$$H^1(\Phi, L_n(\mathbf{Z}_p)) \otimes_{\mathbf{Z}_p} \mathbf{Z}/p\mathbf{Z} \simeq H^1(\Phi, L_n(\mathbf{Z}/p\mathbf{Z})) \quad \text{(e.g. [10, (1.10a)])}.$$

By [10, Cor. 3.3], we have that

$$e_0 H^1(\Gamma_1(N), L_n(\mathbf{Z}_p)) \otimes_{\mathbf{Z}_p} \mathbf{Z}/p\mathbf{Z} \simeq e_0 H^1(\Gamma_1(N), L_n(\mathbf{Z}/p\mathbf{Z})) \simeq eH^1(\Phi_1, \mathbf{Z}/p\mathbf{Z}(n)).$$

By Corollary 4.5, we have that

$$eH^1(\Phi_1, \mathbf{Z}/p\mathbf{Z}(n)) \simeq eH^1(\Phi_1, L_n(\mathbf{Z}/p\mathbf{Z})) \simeq eH^1(\Phi_1, L_n(\mathbf{Z}_p)) \otimes_{\mathbf{Z}_p} \mathbf{Z}/p\mathbf{Z}.$$

Thus, the morphisms $e \circ \mathrm{res}$ and $e_0 \circ \mathrm{Tr}$ give an isomorphism:

$$e_0 H^1(\Gamma_1(N), L_n(\mathbf{Z}_p)) \otimes_{\mathbf{Z}_p} \mathbf{Z}/p\mathbf{Z} \simeq eH^1(\Phi_1, L_n(\mathbf{Z}_p)) \otimes_{\mathbf{Z}_p} \mathbf{Z}/p\mathbf{Z}.$$

Thus, by Nakayama's lemma, $e \circ \mathrm{res}$ induces a surjection

$$e_0 H^1(\Gamma_1(N), L_n(\mathbf{Z}_p)) \to eH^1(\Phi_1, L_n(\mathbf{Z}_p)).$$

This morphism is injective since the both sides are $\mathbf{Z}_p$-free of the same rank (cf. Lemma 4.6). The isomorphism in each direction is explicitely given by $e \circ \mathrm{res}$ and $e_0 \circ Tr$, which preserve parabolic cohomology classes. Thus, the assertion for the parabolic cohomology groups is also shown.

Let Φ be either of $\Gamma_1(Np^r)$ or Φ_r^t for $r \geqq t \geqq 0$. Then the stabilizer Φ_s in Φ for each cusp $s \in C(\Phi)$ is either an infinite cyclic group or a product of an infinite cyclic group and $\{\pm 1\}$. We fix an element $\alpha = \alpha_s$ in $\mathrm{SL}_2(\mathbf{Z})$ for each $s \in C(\Phi)$

such that $\alpha(\infty)=s$. Then we can choose a generator $\pi=\pi_s$ of the torsion free part of Φ_s so that $\alpha^{-1}\pi\alpha=\pm\begin{pmatrix}1 & u\\ 0 & 1\end{pmatrix}$ with $u>0$.

Terminology. When $\alpha^{-1}\pi\alpha=-\begin{pmatrix}1 & u\\ 0 & 1\end{pmatrix}$, we say that the cusp s (or the parabolic element π) is *irregular*, and otherwise, we say that s (or π) is *regular* (cf. [25, 2.1]).

Lemma 4.8. *The ordinary part* $e_0G^1(\Gamma_1(N),L_n(\mathbf{Z}_p))$ *is* $\mathbf{Z}_p$*-free.*

Proof. We have the following exact sequence:

$$G^0(\Gamma_1(N),L_n(\mathbf{Q}_p))\xrightarrow{\delta}G^0(\Gamma_1(N),\ L_n(\mathbf{T}_p))\to G^1(\Gamma_1(N),L_n(\mathbf{Z}_p))\to G^1(\Gamma_1(N),L_n(\mathbf{Q}_p)).$$

Thus, what we have to show is the vanishing:

$$e_0(G^0(\Gamma_1(N);\ L_n(\mathbf{T}_p))/\delta(G^0(\Gamma_1(N);L_n(\mathbf{Q}_p)))=0.$$

We choose $\alpha_s\in\mathrm{SL}_2(\mathbf{Z})$ for each $s\in C(\Gamma_1(N))$ so that $\alpha_s(\infty)=s$ and fix a generator π_s of a torsion free part of $\Gamma_1(N)_s$ by $\alpha_s^{-1}\pi_s\alpha_s=\pm\begin{pmatrix}1 & u\\ 0 & 1\end{pmatrix}$. Since N is prime to p, we may assume $\alpha_s\equiv 1 \bmod p^3$ and $(u,p)=1$. Thus, $\pi_s\equiv\pm\begin{pmatrix}1 & u\\ 0 & 1\end{pmatrix}\bmod p^2$ and by Lemma 4.3 (iii), we can decompose

$$\Gamma_1(N)\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\Gamma_1(N)=\Gamma_1(N)\beta\Gamma_1(N)_s\cup\Gamma_1(N)\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\Gamma_1(N)_s,$$

where $\beta\in M_2(\mathbf{Z})$ satisfies $\det(\beta)=p$ and $\beta\equiv\begin{pmatrix}p & 0\\ 0 & 1\end{pmatrix}\bmod p^2$ and $\beta\equiv\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\bmod N$. We now choose γ_0 and γ_1 in $\Gamma_1(N)$ so that $t=\gamma_0\beta(s)\in C(\Gamma_1(N))$ and $v=\gamma_1\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}(s)\in C(\Gamma_1(N))$. As seen in the proof of Lemma 4.1, this is possible. Write π for π_s or π_s^2 according as s is regular or not. Then, by definition, $T(p)$ acts on $G^0(\Gamma_1(N),\ L_n(\mathbf{T}_p))$ by

$$(x|T(p))_s=(\gamma_0\beta)^\iota\cdot x_t+\sum_{i=0}^{p-1}\left(\gamma_1\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\pi^i\right)^\iota\cdot x_v,$$

where x_t indicates the component of x in $H^0(\Gamma_1(N)_t,\ L_n(\mathbf{T}_p))$.

Since $\alpha_s\equiv 1 \bmod p^3$, we see that $\gamma_0,\ \gamma_1\in\Gamma_0(p^2)$. As seen in the proof of Lemma 4.6, if $px=0$ and if x is of the form $x={}^t(x_0,x_1,\dots,x_{n-1},0)$ $(\gamma_1^\iota x_v$ is also of the same form), then

$$\sum_{i=0}^{p-1}\left(\gamma_1\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\pi^i\right)^\iota\cdot x_v=0.$$

If we write $(x|T(p))_s$ as ${}^t(x_0',\dots,x_n')$, then $x_n'=0$. Thus if $px=0$,

$$(x|T(p)^2)_s\in\left\{{}^t(a,0,\dots,0)\,\middle|\,a\in\left(\frac{1}{p}\mathbf{Z}/\mathbf{Z}\right)\right\}=X,$$

since $\beta \equiv \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \bmod p^2$. We now show that X is contained in the image of δ. If t is irregular and n is odd, then we know that

$$L_n(\mathbf{T}_p)^{\Gamma_1(N)_t} = H^0(\Gamma_1(N)_t, L_n(\mathbf{T}_p)) = 0.$$

In fact, if $x \in L_n(\mathbf{T}_p)$ is fixed by $\pi' = \alpha_t^{-1} \pi_t^2 \alpha_t = \begin{pmatrix} 1 & 2u' \\ 0 & 1 \end{pmatrix}$, then $x \in {}^t(1, 0, \ldots, 0)\mathbf{T}_p \subset L_n(\mathbf{T}_p)$ since $2u'$ is prime to p. On x as above, $\alpha_t^{-1} \pi_t \alpha_t$ acts as multiplication by -1. Since $p \geqq 5$, one sees that x must be 0 if $x = -x$. Thus in this case, $x_t = 0$; so we may assume that t is regular when n is odd. Let $U = \left\{ \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \middle| m \in \mathbf{Z}_p \right\}$. Then, we know that

$$\begin{array}{ccccc} L_n(\mathbf{Q}_p)^{\Gamma_1(N)_t} & \simeq & L_n(\mathbf{Q}_p)^U & \simeq & {}^t(1, 0, \ldots, 0)\,\mathbf{Q}_p. \\ \cup & & \cup & & \\ x & \mapsto & \alpha_t^{-1} x. & & \end{array}$$

Since $\alpha_t \equiv 1 \bmod p$, any element in X is contained in the image of δ. Since $G^0(\Gamma_1(N), L_n(\mathbf{Q}_p))$ is p-divisible, the image of δ is also p-divisible. Thus one can decompose

$$G^0(\Gamma_1(N); L_n(\mathbf{T}_p)) = \delta(G^0(\Gamma_1(N), L_n(\mathbf{Q}_p)) \oplus M$$

for a $\mathbf{Z}_p$-module M. Thus for any $x \in M$ with $px = 0$, we know that $x | T(p)^2 \bmod \delta(G^0(\Gamma_1(N),\ L_n(\mathbf{Q}_p))) = 0$ by the above argument. Then by Nakayama's lemma, the $T(p)$ is topologically nilpotent on the quotient $G^0(\Gamma_1(N);\ L_n(\mathbf{T}_p))/\delta(G^0(\Gamma_1(N), L_n(\mathbf{Q}_p)))$. Thus e_0 annihilates this space, Q.E.D.

We obtain the following generalization of [9, Th. 1.2]:

Theorem 4.9. *Let Φ be either of $\Gamma_1(N)$ or Φ_r for $r \geqq 0$. Then the quotient module*

$$eH^1(\Phi, L_n(\mathbf{Z}_p))/eH_P^1(\Phi, L_n(\mathbf{Z}_p)) = e(H^1(\Phi, L_n(\mathbf{Z}_p))/H_P^1(\Phi, L_n(\mathbf{Z}_p)))$$

is $\mathbf{Z}_p$-free.

Proof. The assertion for $n > 0$ follows from Lemma 4.8 and Cor. 4.5 combined with the exact sequence (4.1b). The assertion in the case where $n = 0$ is well known (cf. [10, §1] or else, see §5).

Corollary 4.10. *Let Φ be as in Theorem* 4.9. *Let A be either of $\mathbf{Z}/p^m\mathbf{Z}$ or $\mathbf{T}_p$. Then the natural map of $eH_P^1(\Phi, L_n(\mathbf{Z}_p)) \otimes_{f_p} A$ into $eH_P^1(\Phi, L_n(A))$ is injective* (we will see later that this morphism is in fact a surjective isomorphism).

Proof. We have an exact sequence:

$$0 \to eH_P^1(\Phi, L_n(\mathbf{Z}_p)) \to eH^1(\Phi, L_n(\mathbf{Z}_p)) \to e(H^1(\Phi, L_n(\mathbf{Z}_p))/H_P^1(\Phi, L_n(\mathbf{Z}_p))) \to 0.$$

Since the last module in the above sequence is $\mathbf{Z}_p$-free, the induced map:

$$eH_P^1(\Phi, L_n(\mathbf{Z}_p)) \otimes_{\mathbf{Z}_p} A \to eH^1(\Phi, L_n(\mathbf{Z}_p)) \otimes_{\mathbf{Z}_p} A$$

is injective. However, it is well known (e.g. [9, (1.10a)]) that

$$H^1(\Phi, L_n(\mathbf{Z}_p)) \otimes_{\mathbf{Z}_p} A \simeq H^1(\Phi, L_n(A)).$$

Thus the above injection factors through $H_P^1(\Phi, L_n(A))$ and proves the corollary.

§5. Eisenstein series and cohomology groups at cusps

Let Y_r denote the complex analytic space $\Gamma_1(Np^r)\backslash\mathfrak{H}$ for each non-negative integer r and X_r be the smooth compactification at cusps of Y_r. If $N \geqq 3$ or $r \geqq 1$, Y_r and X_r are smooth. The representative set $C(\Gamma_1(Np^r))$ of $\Gamma_1(Np^r)$-equivalence classes of cusps is naturally isomorphic to $X_r - Y_r$.

Terminology. Let Φ be a congruence subgroup of $\Gamma_1(N)$. Let $s \in C(\Phi)$ and $s_0 \in X_0$ be the image of s in $C(\Gamma_1(N))$. We say that s is *unramified* if s is unramified over s_0 as a point of the smooth compactification of $\Phi\backslash\mathfrak{H}$.

Lemma 5.1. *The number of unramified cusps of X_r is given by*

$$\tfrac{1}{2}\varphi(p^r) \cdot \sum_{0<t|N} \varphi(t)\varphi(N/t) \quad \textit{for each } r \geqq 1,$$

where φ denotes the Euler function. Furthermore, every unramified cusp of X_r can be represented by $\alpha(\infty)$ for $\alpha \in \Gamma_0(p^m)$ for each given $m \geqq r$.

Proof. Define a subset M of the additive group $(\mathbf{Z}/Np^r\mathbf{Z})^2$ by

$$M = \{v \in (\mathbf{Z}/Np^r\mathbf{Z})^2 \,|\, \textit{the order of } v \text{ is equal to } Np^r\}.$$

For each $v = {}^t(\bar{x}, \bar{y}) \in M$, we choose $x, y \in \mathbf{Z}$ so that

$$x \equiv \bar{x} \bmod Np^r \quad \text{and} \quad y \equiv \bar{y} \bmod Np^r.$$

Then the point $(x, y) \in \mathbf{P}^1(\mathbf{Q})$ can be regarded as a cusp of $\Gamma_1(Np^r)$. This correspondence induces a bijection (cf. [25, 1.6])

$$C(\Gamma_1(Np^r)) \simeq U\backslash M,$$

where U is a subgroup of $\mathrm{Aut}(M)$ defined matricially by

$$U = \left\{ \pm \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \middle| u \in \mathbf{Z}/Np^r\mathbf{Z} \right\}.$$

We can choose a coprime pair as (x, y) above. Then, we will find $a, b \in \mathbf{Z}$ so that $\alpha = \begin{pmatrix} x & a \\ y & b \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$ and we know that $\alpha(\infty) = \frac{x}{y}$. On the other hand, for the principal congruence subgroup $\Gamma(p^r)$, the compactified curve Z of $(\Gamma(p^r) \cap \Gamma_1(N))\backslash\mathfrak{H}$ is a Galois covering of X_0, and one has

$$\mathrm{Gal}(Z/X_0) \simeq \begin{cases} P\mathrm{SL}_2(\mathbf{Z}/p^r\mathbf{Z}) & \text{if } N = 1 \text{ or } 2 \\ \mathrm{SL}_2(\mathbf{Z}/p^r\mathbf{Z}) & \text{if } N > 2. \end{cases}$$

Let U_p be the image of $\left\{\begin{pmatrix}1 & u\\ 0 & 1\end{pmatrix}\middle| u\in\mathbf{Z}/p^r\mathbf{Z}\right\}$ in $\mathrm{Gal}(\mathbf{Z}/\mathbf{X}_0)$. Then, we can find a cusp on Z with inertia group U_p over each cusp of X_0. The inertia group of the cusp $s=\frac{x}{y}$ over X_0 is given by $\bar{\alpha}U_p\bar{\alpha}^{-1}$ for the image $\bar{\alpha}$ of α in $\mathrm{SL}_2(\mathbf{Z}/p^r\mathbf{Z})$. Note that $\mathrm{Gal}(Z/X_r)$ is given by U_p. Thus, for the unramifiedness of s over X_0, it is necessary and sufficient to have an inclusion: $\bar{\alpha}U_p\bar{\alpha}^{-1}\subset U_p$, i.e. $\alpha\in\Gamma_0(p_r)$. In other words, $s=\frac{x}{y}$ is unramified if and only if $y\equiv 0 \bmod p^r$. We may choose y so that $y\equiv 0 \bmod p^m$ for arbitrarily large $m\geqq r$. The cardinality of the set: $U\setminus\left\{\begin{pmatrix}x\\ y\end{pmatrix}\in M\middle| y\equiv 0 \bmod p^r\right\}$ can be easily calculated and is equal to the number as in the lemma.

Definition. For each subalgebra A of Ω or $\mathbf{C}$, we define

$$\mathscr{E}_k(\Gamma_1(Np^r);A)=\mathscr{M}_k(\Gamma_1(Np^r);A)/S_k(\Gamma_1(Np^r);A).$$

For a pair of positive divisors u and v of Np^r with $uv|Np^r$, let χ and ψ be Dirichlet characters modulo u and v, respectively. Put, formally for each $0<t\in\mathbf{Z}$,

$$E_k(\chi,\psi;t)=\delta(\psi)\,L(1-k,\chi)+\sum_{n=1}^{\infty}\Big(\sum_{0<d|n}\chi(d)\,\psi(n/d)\,d^{k-1}\Big)q^{tn}\in\bar{\mathbf{Q}}[[q]],$$

where

$$\delta(\psi)=\begin{cases}1/2 & \text{if } \psi \text{ is the identity}\\ 0 & \text{otherwise}\end{cases}$$

and $L(s,\chi)$ is the Dirichlet L-series with character χ. We write $E_k(\chi,\psi)$ for $E_k(\chi,\psi;1)$.

Lemma 5.2. (i) *$E_k(\chi,\psi;t)$ gives the q-expansion of an element of $\mathscr{M}_k(\Gamma_1(Np^r))$ if the following conditions are satisfied:*

(a) *$\chi\psi(-1)=(-1)^k$, and tuv is a divisor of Np^r;*

(b) *χ and ψ are primitive modulo u and v, respectively, if $k>2$;*

(c) *Suppose that $k=2$. Either χ and ψ are primitive or trivial. If χ and ψ are primitive modulo u and v, then at least one of them is non-trivial, and if both χ and ψ are trivial, then u is a prime and $v=1$.*

(ii) *$E_k(\chi,\psi;t)$ with χ, ψ and t satisfying* (a), (b) *and* (c) *spans the space $\mathscr{E}_k(\Gamma_1(Np^r);\bar{\mathbf{Q}})$ for each $k\geqq 2$ and $r\geqq 1$.*

Proof. This fact may be well known and a proof may be found in Doi-Miyake [6, §4.7], but we shall give a sketch of a proof because [6] is written in Japanese. For each integer M and for each pair $(a,b)\in(\mathbf{Z}/M\mathbf{Z})^2$, Hecke defined in [8, §§1 and 2] an Eisenstein series by

$$G_k(z;a,b;M)=\sum_{\substack{(c,d)\equiv(a,b)\bmod M\\ (c,d)\neq 0}}(cz+d)^{-k}\,|cz+d|^{-2s}\big|_{s=0}.$$

We write $z\in\mathfrak{H}$ as $x+\sqrt{-1}\,y$ with x, $y\in\mathbf{R}$. Then, the Fourier expansion of this series is given there as

$$G_k(z;a,b;M)$$
$$=-\delta_2\pi/M^2y+\delta(a)\zeta(k,b;M)+\frac{(-2\pi\sqrt{-1})^k}{M^k(k-1)\varepsilon}\sum_{\substack{mn>0\\ m\equiv a \bmod M}} n^{k-1}\,\mathrm{sgn}(n)\,e\left(\frac{bn+mnz}{M}\right),$$

where

$$e(z)=\exp(2\pi\sqrt{-1}\,z),\qquad \delta_2=\begin{cases}1 & \text{if } k=2\\ 0 & \text{otherwise,}\end{cases}\qquad \delta(a)=\begin{cases}1 & \text{if } a=0\\ 0 & \text{otherwise,}\end{cases}$$

and $\zeta(s,b;M)=\sum_{\substack{n\equiv b \bmod M\\ n>0}} n^{-s}$. Assume that χ is primitive modulo u. If $k>2$ or if one of χ and ψ is non-trivial, a simple calculation shows that $E_k(\chi,\psi)$ coincides, up to constant factor, with

$$E'_k(\chi,\psi)=\sum_{a=1}^{v}\sum_{b=1}^{uv}\psi(a)\,\bar{\chi}(b)\,G_k(z;au,b;uv)\in\mathcal{M}_k(\Gamma_1(uv)).$$

Thus, in this case, the first assertion has been proven. Let ι denote the trivial character (modulo 1). When $k=2$, what we know is that if we denote the linear combination as above for $\chi=\psi=\iota$ by $E'_2(\iota,\iota)$, then $E'_2(\iota,\iota)-cy^{-1}=dE_2(\iota,\iota)$ with non-zero constants c and d. Let ι_u be the trivial character modulo u for a prime u. Then, we see from this formula that

$$E'_k(\iota,\iota)-u\,E'_k(\iota,\iota)\,|\,[u]=d\,E_k(\iota_u,\iota),$$

where we write $f\,|\,[u](z)=f(uz)$ for each function f on $\mathfrak{H}$. This shows the assertion (i). To prove (ii), we shall calculate the cardinality of the set A consisting of triples (χ,ψ,t) satisfying the following condition: (i) χ and ψ are primitive Dirichlet characters modulo u and v, respectively, and (ii) t is a positive integer such that tuv divides a given positive integer M. Let B be the set consisting of pairs of characters (χ',ψ') such that χ': $(\mathbf{Z}/u'\mathbf{Z})^\times\to\mathbf{C}^\times$ and ψ': $(\mathbf{Z}/v'\mathbf{Z})^\times\to\mathbf{C}^\times$ for integers u' and v' with $u'v'=M$. For the element (χ',ψ') of B, we shall not impose primitiveness on the characters χ' and ψ'. The cardinality of B is obviously given by the number $d(M)=\sum_{0<u|M}\varphi(u)\,\varphi(M/u)$. We shall construct a bijection between A and B. For $(\chi,\psi,t)\in A$, we define an element $(\chi',\psi')\in B$ as follows: χ' is the restriction of χ modulo M/tv and ψ' is the restriction of ψ modulo tv. Conversely, if $(\chi',\psi')\in B$ is given, let u and v be the conductor of each χ' and ψ' and let χ and ψ be primitive characters which induce χ' and ψ'. Since $u'v'=M$, we define t by $tv=v'$. Then the triple (χ,ψ,t) belongs to A. This shows that the cardinality of A is equal to $d(M)$. The linear independence of $E_k(\chi,\psi;t)$ for χ, ψ, t with (a) and (b) is plain, and thus, for each $k>2$, the subspace $\mathscr{E}$ of $\mathscr{E}_k(\Gamma_1(Np^r);\mathbf{C})$ spanned by $E_k(\chi,\psi;t)$ has dimension $\frac{1}{2}d(Np^r)$, since an additional condition of parity: $\chi\psi(-1)=(-1)^k$ is imposed. As is clear from the proof of Lemma 5.1, the number of cusps on X_r is exactly given by $\frac{1}{2}d(Np^r)$; therefore, $\dim_{\mathbf{C}}\mathscr{E}_k(\Gamma_1(Np^r);\mathbf{C})=\frac{1}{2}d(Np^r)$ if $k>2$. This shows (ii) when $k>2$. When $k=2$, it is known by Hecke (e.g. [25, Th. 2.23, 2.24

and 2.25]) that $\dim_{\mathbf{C}}\mathscr{E}_k(\Gamma_1(Np^r);\mathbf{C})=\frac{1}{2}d(Np^r)-1$. There is only one linear relation between $E_k(\iota_u,\iota;t)$ and thus, (ii) can be shown similarly.

Lemma 5.3. *Let e be the idempotent attached to $T(p)$ on $\mathscr{E}_k(\Gamma_1(Np^r);\Omega)$. Suppose that $r>0$ and $k\geqq 2$. Then, the subspace $\mathscr{E}_k(\Gamma_1(Np^r);\mathbf{Q})$ of $\mathscr{E}_k(\Gamma_1(Np^r);\Omega)$ is stable under the action of e, and we have that*

$$\dim_{\mathbf{Q}} e\mathscr{E}_k(\Gamma_1(Np^r);\mathbf{Q})=\tfrac{1}{2}\varphi(p^r)\cdot\sum_{0<t\mid N}\varphi(t)\varphi(N/t).$$

Proof. We begin by showing the following dimension formula:

$$\dim_{\Omega}(e\mathscr{E}_k(\Gamma_1(Np^r);\Omega))=\tfrac{1}{2}\varphi(p^r)\cdot\sum_{0<t\mid N}\varphi(t)\varphi(N/t).$$

Let I be any positive integer and ξ be a Dirichlet character modulo I. We write ξ_1 for the restriction of ξ modulo Ip, if I is prime to p, and if p divides I, we simply put $\xi_1=\xi$. By definition, we have that

$$E_k(\chi,\psi)|T(p)=(\psi(p)+\chi(p)p^{k-1})E_k(\chi,\psi)$$

and $(\psi(p)-\chi(p)p^{k-1})E_k(\chi,\psi)=\psi(p)E_k(\chi_1,\psi)-\chi(p)p^{k-1}E_k(\chi,\psi_1)$. Thus, by [12, Lemma 4.2], we know that

$$E_k(\chi,\psi)|e=\begin{cases}(1-\psi^{-1}\chi(p)p^{k-1})^{-1}E_k(\chi_1,\psi) & \text{if } \psi(p)\neq 0\\ 0 & \text{if } \psi(p)=0.\end{cases}$$

Write $f|[t]$ for $f(q^t)$ for each power series $f(q)\in\Omega[[q]]$.

Since $(f|[p])|T(p)=f$ for $f\in\mathscr{M}_k(\Gamma_1(Np^r);\Omega)$, we have that if $t=t_0p^s$ with $(t_0,p)=1$, then

$$E_k(\chi,\psi;t)|e=(E_k(\chi,\psi)|[t])|e=\bar{\psi}(p)^s(E_k(\chi,\psi)|e)|[t_0].$$

Thus, in order to get a basis of $e\mathscr{E}_k(\Gamma_1(Np^r);\Omega)$ out of $E_k(\chi,\psi;t)$, we may only consider triples (χ,ψ,t) satisfying the following conditions: (i) χ is a primitive character modulo u, (ii) ψ is a primitive character modulo v, (iii) v and t are prime to p and tuv divides Np^r, and (iv) $\chi\psi(-1)=(-1)^k$. For these triples (χ,ψ,t), the Eisenstein series $E_k(\chi_1,\psi;t)$ are linearly independent and gives a basis of $e\mathscr{E}_k(\Gamma_1(Np^r);\Omega)$.

The number of triples (χ,ψ,t) satisfying (i)~(iv) can be calculated in a similar manner as in the proof of Lemma 5.2 and is equal to $\frac{1}{2}\varphi(p^r)\cdot\sum_{0<t\mid N}\varphi(t)\varphi(N/t)$. The above formulae of the action of e on $E_k(\chi,\psi;t)$ show that $\mathscr{E}_k(\Gamma_1(Np^r);\bar{\mathbf{Q}})$ is stable under e, by Lemma 5.2 (ii). Let $\sigma\in\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ act on $\mathscr{M}_k(\Gamma_1(Np^r);\bar{\mathbf{Q}})$ by $\left(\sum_{n=0}^{\infty}a(n)q^n\right)^{\sigma}=\sum_{n=0}^{\infty}a(n)^{\sigma}q^n$. Then we see that

$$(E_k(\chi,\psi;t)|e)=E_k(\chi^{\sigma},\psi^{\sigma};t)|e \quad \text{for each } \sigma\in\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}),$$

where $\chi^{\sigma}(m)=\chi(m)^{\sigma}$ and $\psi^{\sigma}(m)=\psi(m)^{\sigma}$ for all m. This shows that $\mathscr{E}_k(\Gamma_1(Np^r);\mathbf{Q})$ is stable under e. Then, the desired dimension formula follows since

$$\mathscr{E}_k(\Gamma_1(Np^r);\Omega)=\mathscr{E}_k(\Gamma_1(Np^r);\mathbf{Q})\otimes_{\mathbf{Q}}\Omega.$$

Lemma 5.4. *Let Φ be a congruence subgroup of* $\mathrm{SL}_2(\mathbf{Z})$ *and K be a field of characteristic* 0. *Consider the Φ-module $L_n(K)$ for each integer $n \geqq 0$. Put $\Phi_s = \{\gamma \in \Phi \mid \gamma(s) = s\}$ for each cusp $s \in \mathbf{P}^1(\mathbf{Q})$. Assume that n is even if $-1 \in \Phi$. Then we have*

$$H^1(\Phi_s, L_n(K)) \simeq \begin{cases} 0, & \text{if } n \text{ is odd and } s \text{ is an irregular cusp of } \Phi, \\ K, & \text{otherwise.} \end{cases}$$

Proof. Choosing $\alpha \in SL_2(\mathbf{Z})$ so that $s = \alpha(\infty)$, we know that $\alpha^{-1}\Phi_s\alpha \subset \{\pm 1\} U_\infty$ for $U_\infty = \left\{ \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \middle| u \in \mathbf{Q} \right\}$. If $-1 \in \Phi_s$, then the restriction and inflation sequence yields an exact sequence

$$0 \to H^1(\Phi_s/\{\pm 1\}, L_n(K)) \to H^1(\Phi_s, L_n(K)) \to H^1(\{\pm 1\}, L_n(K)) = 0.$$

Thus, we may assume that Φ_s is an infinite cyclic group by substituting $\Phi_s/\{\pm 1\}$ for Φ_s if necessary. Since α as above induces an isomorphism: $H^1(\Phi_s, L_l(K)) \simeq H^1(\alpha^{-1}\Phi_s\alpha, L_n(K))$, we may assume that $\Phi_s \subset \{\pm 1\} U_\infty$. Let π be a generator of Φ_s. Then it is well known that

$$H^1(\Phi_s, L_n(K)) \simeq L_n(K)/(\pi - 1) L_n(K).$$

If $\pi = \pm \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$, then π acts on $L_n(K)$ via a matrix of the form:

$$\begin{pmatrix} (\pm 1)^n & & * \\ & (\pm 1)^n & \\ & & \ddots & \\ 0 & & & (\pm 1)^n \end{pmatrix}.$$

Thus, if $\pi = -\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$ (i.e., s is irregular) and n is odd, $\pi - 1$ is an automorphism of $L_n(K)$, and thus, $H^1(\Phi_s, L_n(K)) = 0$.

Otherwise the K-linear map $\pi - 1$: $L_n(K) \to L_n(K)$ is of rank n, and hence $L_n(K)/(\pi - 1) L_n(K) \simeq K$.

Remark. If $r \geqq s > 0$ and $p \geqq 3$, every cusp of Φ_r^s and $\Gamma_1(Np^r)$ is regular. In fact, if $\pi \in \Gamma_1(Np^r)$ or Φ_r^s and if $\alpha^{-1}\pi\alpha = -\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$ with $\alpha \in \mathrm{SL}_2(\mathbf{Z})$, then $\alpha^{-1}\pi^p\alpha \equiv -1 \bmod p$ and thus $\pi^p \equiv -1 \bmod p$. This is a contradiction, since $\pi^p \in \Gamma_1(Np)$. On the other hand, $\Gamma_1(4)$ has one irregular cusp and two regular ones (for $\Gamma_1(N)$, if $N \neq 4$, all the cusps of $\Gamma_1(N)$ is regular (cf. [6, Th. 4.2.10])).

Let Φ be either of $\Gamma_1(Np^r)$ or Φ_r^s for $r \geqq s \geqq 0$. For each non-negative integer n, take $f \in \mathcal{M}_{n+2}(\Phi)$ and put

$$\omega(f) = f \cdot \begin{pmatrix} z \\ 1 \end{pmatrix}^n dz \qquad \left(\begin{pmatrix} z \\ 1 \end{pmatrix}^n = {}^t(z^n, z^{n-1}, \ldots, 1) \right)$$

as $L_n(\mathbf{C})$-valued differential form. For each $z \in \mathfrak{H}$ and $\gamma \in \Phi$, define a map

$$\delta(f)_z \colon \Phi \to L_n(\mathbf{C})$$

by

$$\delta(f)_z(\gamma) = \int_z^{\gamma(z)} \omega(f) \in L_n(\mathbf{C}).$$

As shown in [25, 8.2], $\delta(f)_z$ is a 1-cocycle of Φ with values in the Φ-module $L_n(\mathbf{C})$. The cohomology class $\delta(f)$ of $\delta(f)_z$ is independent of the choice of the point $z \in \mathfrak{H}$, and thus, one has a morphism of $\mathcal{M}_{n+2}(\Phi)$ into $H^1(\Phi, L_n(\mathbf{C}))$. It is proved by Shimura [25, Th. 8.4] that the real part of δ induces an isomorphism

$$\text{(5.1 a)} \qquad \varphi\colon\ S_{n+2}(\Phi) \simeq H_P^1(\Phi, L_n(\mathbf{R})),$$

or equivalently, if we write $\bar{S}_{n+2}(\Phi)$ for the complex conjugate of the image of $S_{n+2}(\Phi)$ under δ in $H_P^1(\Phi, L_n(\mathbf{C}))$, we have

$$\text{(5.1 b)} \qquad S_{n+2}(\Phi) \oplus \bar{S}_{n+2}(\Phi) \simeq H_P^1(\Phi, L_n(\mathbf{C})).$$

For each $s \in C(\Phi)$, choose a generator $\pi = \pi_s$ of Φ_s and $\alpha = \alpha_s \in \mathrm{SL}_2(\mathbf{Z})$ so that $\alpha^{-1}\pi\alpha = \pm\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$ with $u > 0$. By Lemma 5.4,

$$L_n(\mathbf{C})/(\alpha^{-1}\pi\alpha - 1)\, L_n(\mathbf{C}) \simeq \begin{cases} 0 & \text{if } n \text{ is odd and } s \text{ is irregular for } \Phi, \\ \mathbf{C} & \text{otherwise,} \end{cases}$$

and this isomorphism is induced by the projection of $L_n(\mathbf{C})$ onto $\mathbf{C}$ given by ${}^t(x_0, \ldots, x_n) \mapsto x_n$ if the quotient is non-trivial. Naturally, α induces an isomorphism

$$L_n(\mathbf{C})/(\alpha^{-1}\pi\alpha - 1)\, L_n(\mathbf{C}) \xrightarrow{\sim} L_n(\mathbf{C})/(\pi - 1)\, L_n(\mathbf{C}) \simeq H^1(\Phi_s, L_n(\mathbf{C})).$$

Write δ_s for the combined morphism:

$$\delta_s\colon\ \mathcal{M}_{n+2}(\Phi) \xrightarrow{\delta} H^1(\Phi, L_n(\mathbf{C})) \xrightarrow{\mathrm{res}} H^1(\Phi_s, L_n(\mathbf{C}))$$
$$\xrightarrow{\alpha^{-1}} L_n(\mathbf{C})/(\alpha^{-1}\pi\alpha - 1)\, L_n(\mathbf{C}) \simeq \begin{cases} \mathbf{C} \\ 0 \end{cases}.$$

A simple calculation yields that

$$\delta(f)_z(\pi) = \alpha \cdot \int_z^{z+u} \omega(f|_{n+2}\alpha) + (\pi - 1) \int_z^{\alpha(z)} \omega(f).$$

Thus, we know that

$$\text{(5.2)} \qquad \delta_s(f) = a(0, f|_{n+2}\alpha) \in \mathbf{C}.$$

If s is irregular and n is odd, it is well known that $a(0, f|_{n+2}\alpha) = 0$ (cf. [25, p. 29]) and thus, this is compatible with Lemma 5.4. Let us put, for any subalgebra A of $\mathbf{C}$ or Ω,

$$\mathscr{E}_k(\Phi; A) = \mathcal{M}_k(\Phi; A)/S_k(\Phi; A),$$

$$\mathscr{G}(\Phi; L_n(A)) = H^1(\Phi; L_n(A))/H_P^1(\Phi; L_n(A)).$$

Lemma 5.5. *The morphism δ induces an isomorphism of the modules over the Hecke ring $R(\Phi, \Delta)$:*

$$\mathscr{E}_{n+2}(\Phi;\mathbf{C}) \simeq \mathscr{G}(\Phi; L_n(\mathbf{C})) \quad \textit{for each } n \geqq 0.$$

Proof. Let r (resp. i) be the number of regular (resp. irregular) cusps of $C(\Phi)$. It is well known (e.g. [25, Th. 2.23, 2.24 and 2.25]) that

$$\dim_{\mathbf{C}} \mathscr{E}_{n+2}(\Phi;\mathbf{C}) = \begin{cases} i+r & \text{if } n>0 \text{ and } n \text{ is even,} \\ r & \text{if } n \text{ is odd,} \\ i+r-1 & \text{if } n=0. \end{cases}$$

By the exact sequence (4.2), $\mathscr{G}(\Phi; L_n(\mathbf{C})$ is a subspace of $G^1(\Phi, L_n(\mathbf{C}))$. By Lemma 5.4, we know that

$$\dim_{\mathbf{C}} G^1(\Phi, L_n(\mathbf{C})) = \begin{cases} i+r & \text{if } n \text{ is even,} \\ r & \text{if } n \text{ is odd.} \end{cases}$$

The fact (5.2) shows that δ induces an injection of $\mathscr{E}_{n+2}(\Phi;\mathbf{C})$ into $\mathscr{G}(\Phi; L_n(\mathbf{C}))$, which proves the assertion for $n>0$. It is known and will be shown later that $\dim_{\mathbf{C}} \mathscr{G}(\Phi;\mathbf{C}) = i+r-1$ (see 5.4). Thus, the lemma remains true even for $n=0$.

Corollary 5.6. *Let $\mathscr{H}$ be the* **Q**-*subalgebra of* $\mathrm{End}(\mathscr{E}_{n+2}(\Phi;\mathbf{Q}))$ *generated over* **Q** *by the Hecke operators $T(l)$ and $T(l,l)$ for all primes l. Then, there is an isomorphism of $\mathscr{H}$-modules:*

$$\mathscr{E}_{n+2}(\Phi;\mathbf{Q}) \simeq \mathscr{G}(\Phi; L_n(\mathbf{Q})) \quad \textit{for each } n \geqq 0,$$

and the idempotent attached to $T(p)$ is contained in $\mathscr{H}$.

Proof. Since Φ is either Φ_r^s or $\Gamma_1(Np^r)$, the space $\mathscr{E}_{n+2}(\Phi;\mathbf{C})$ is spanned by the image of $E_k(\chi,\psi;t)$ for suitable χ, ψ and t. Since $E_k(\chi,\psi;t)^\sigma = E_k(\chi^\sigma,\psi^\sigma;t)$ for any $\sigma \in \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, the space $\mathscr{E}_{n+2}(\Phi;\mathbf{Q})$ is also spanned by the image of Eisenstein series with **Q**-rational Fourier coefficients, which are linear combinations of the above type of series. Thus we may identify $\mathscr{E}_{n+2}(\Phi;\mathbf{Q})$ with the subspace of $\mathscr{M}_{n+2}(\Phi;\mathbf{Q})$ spanned by these **Q**-rational Eisenstein series, which is stable under Hecke operators $T(n)$. Write the q-expansion of each element $f \in \mathscr{E}_{n+2}(\Phi;\mathbf{C})$ as

$$\sum_{n=0}^{\infty} a(n,f) q^n.$$

Then the pairing

$$\langle\ ,\ \rangle : \mathscr{H} \times \mathscr{E}_{n+2}(\Phi;\mathbf{Q}) \to \mathbf{Q}$$

defined by $\langle h,f \rangle = a(1, f|h)$ induces a perfect duality over **Q** (cf. [13, Prop. 2.1]). Thus we know that

$$\mathscr{E}_{n+2}(\Phi;\mathbf{Q}) \simeq \mathrm{Hom}_{\mathbf{Q}}(\mathscr{H}, \mathbf{Q}) \quad \text{and} \quad \mathscr{E}_{n+2}(\Phi;\mathbf{C}) \simeq \mathrm{Hom}_{\mathbf{C}}(\mathscr{H} \otimes_{\mathbf{Q}} \mathbf{C}, \mathbf{C})$$

as $\mathscr{H}$-modules. Since $\mathscr{G}(\Phi; L_n(\mathbf{C})) = \mathscr{G}(\Phi; L_n(\mathbf{Q})) \otimes_{\mathbf{Q}} \mathbf{C}$ and the action of $\mathscr{H}$ leaves $\mathscr{G}(\Phi; L_n(\mathbf{Q}))$ stable, we know from Lemma 5.5 that

$$\mathscr{E}_{n+2}(\Phi;\mathbf{Q}) \simeq \mathscr{G}(\Phi; L_n(\mathbf{Q})) \quad \text{as } \mathscr{H}\text{-module (non canonically).}$$

By Lemma 5.3, e leaves $\mathscr{E}_{n+2}(\Phi;\mathbf{Q})$ stable. Thus e induces a homomorphism of $\mathscr{H}$-module $\mathrm{Hom}_{\mathbf{Q}}(\mathscr{H},\mathbf{Q})$ into itself. Thus e must be contained in $\mathscr{H}$.

Now we shall concentrate on the cohomology groups with constant coefficients.

Proposition 5.7. *Let Φ be either of $\Gamma_1(Np^r)$ or Φ_r^t for $r>t\geqq 0$, and let A be either of $\mathbf{Z}_p$, $\mathbf{Z}/p^i\mathbf{Z}$ or any field of characteristic 0. Let s be an unramified cusp of $C(\Phi)$ and ρ_s: $G^1(\Phi,A)\to H^1(\Phi_s,A)$ be the projection map. Then for any $c\in\mathscr{G}(\Phi,A)$, we have that $\rho_s(c|e)=\rho_s(c)$, where e denotes the idempotent attached to $T(p)$.*

Proof. By Corollary 5.6, e is contained in $\mathscr{H}$. Thus, e acts on $\mathscr{G}(\Phi;A)$ even for a field A of characteristic 0, since $\mathscr{G}(\Phi;A)=\mathscr{G}(\Phi;\mathbf{Q})\otimes_{\mathbf{Q}}A$. Let π be a generator of the free part of Φ_s. Then, the evaluation of 1-cocycle at π^{2N} yields an isomorphism (because of $(p,2N)=1$)

$$H^1(\Phi_s,A)\simeq A.$$

Thus we know

$$H^1(\Phi_s,A)=H^1(\Phi_s,\mathbf{Z})\otimes_{\mathbf{Z}}A.$$

Thus we may assume that $A=\mathbf{Z}_p$ to prove the result. Take an integer $m\geqq r$ so that $p^m\equiv 1 \bmod N$. By replacing s by another cusp in the Φ-equivalence class of s if necessary, we may suppose that $\alpha(\infty)=s$ with $\alpha\in\Gamma_0(p^m)$ since s is unramified (cf. the proof of Lemma 5.1). Then $\alpha^{-1}\pi\alpha=\pm\begin{pmatrix}1&u\\0&1\end{pmatrix}$ with u prime to p. Since p is odd, one has $\alpha^{-1}\pi^2\alpha=\begin{pmatrix}1&2u\\0&1\end{pmatrix}$, and $2u$ is prime to p. We shall choose a disjoint decompositions:

$$(*)\qquad \Phi\begin{pmatrix}1&0\\0&p^m\end{pmatrix}=\bigcup_{j=0}^{p^m-1}\Phi\beta_j \quad\text{and}\quad \Phi_s\beta_0\Phi_s=\bigcup_{j=0}^{p^m-1}\Phi_s\beta_j$$

such that (i) $\beta_j(s)=s$ for all j and (ii) $\beta_j\pi^{2N}=\begin{cases}\beta_{j+1} & \text{if } 0\leqq j<p^m-1,\\ \pi^{2N}\beta_0 & \text{if } j=p^m-1.\end{cases}$

Let us admit this decomposition for a while. Then, the definition (4.3) of the action of $T(p^m)$ on $\mathscr{G}(\Phi,A)$ shows that

$$\rho_s(c|T(p^m))=\rho_s(c)|[\Phi_s\beta_0\Phi_s]$$

and for each 1-cocycle φ: $\Phi_s\to A$, we have by the condition (ii)

$$(**)\qquad \varphi|[\Phi_s\beta_0\Phi_s](\pi^{2N})=\varphi(\pi^{2N}).$$

Thus, we know from (**) that

$$\rho_s(c|T(p^m))=\rho_s(c)\quad\text{and hence}\quad \rho_s(c|e)=\rho_s(c).$$

Thus what we have to show is the decomposition as in (*). Put

$$\beta'_j=\begin{pmatrix}1&2uNj\\0&p^m\end{pmatrix}\quad\text{for } 0\leqq j<p^m.$$

Then obviously, $\beta'_j \equiv 1 \bmod N$ and thus, if we put $\beta_j = \alpha\beta_j\alpha^{-1}$, then $\beta_j \equiv 1 \bmod N$.

Since $\alpha \in \Gamma_0(p^m)$, we know that

$$\beta_j \equiv \begin{pmatrix} 1 & j' \\ 0 & p^m \end{pmatrix} \bmod p^r \quad \text{and} \quad \det(\beta_j) = p^m$$

and j' runs over all residues modulo p^m. Then, by Lemma 4.3 (ii), $\Phi \begin{pmatrix} 1 & 0 \\ 0 & p^m \end{pmatrix} \Phi = \bigcup_{j=0}^{p^m-1} \Phi\beta_j$ and this gives obviously a decomposition satisfying (*).

Remark. Proposition 5.7 does not necessarily mean that the subgroup $H^1(\Phi_s, A)$ of $G^1(\Phi, A)$ is stable under $T(p^m)$ or e even if s is unramified. In fact, it can happen that for some $\beta \in \Phi \begin{pmatrix} 1 & 0 \\ 0 & p^m \end{pmatrix} \Phi$ and some ramified cusp t, $\beta(t)$ gives the unramified cusp s. Then, by (4.3), the component of $c|T(p^m)$ in $H^1(\Phi_t, A)$ for $c \in H^1(\Phi_s, A)$ may not be trivial. As a concrete example, we take $\Gamma_0(p)$ as Φ. Then for $\beta = \begin{pmatrix} 1 & 1 \\ 0 & p \end{pmatrix}$, we see that $\beta(0) = \frac{1}{p} = \begin{pmatrix} 1 & 0 \\ p & 1 \end{pmatrix}(\infty)$. Thus, the cusp $\frac{1}{p}$ is unramified, but the cusp 0 is certainly ramified over $\infty \in \mathbf{P}^1(j)$.

Let Φ be an arbitrary congruence subgroup of $SL_2(\mathbf{Z})$, but assume that Φ is torsion free. Put $Y = \Phi\backslash\mathfrak{H}$ as an open Riemann surface, and take one point $y \in Y$. Then Φ can be naturally identified with the topological fundamental group $\pi_1(Y)$ of Y with the base point y. Let X be the smooth compactification of Y at cusps. Let g denote the genus of X. We choose $2g$-curves $\{\alpha_1, \beta_1, \ldots, \alpha_g, \beta_g\}$ passing through y but not crossing any cusps of X, which form a system of canonical generators of the fundamental group $\pi_1(X)$ of X; namely, $\pi_1(X)$ is isomorphic to the quotient of the free group generated by $\{\alpha_1, \beta_1, \ldots, \alpha_g, \beta_g\}$ by the unique relation

$$[\alpha_g, \beta_g] \cdot \ldots \cdot [\alpha_1, \beta_1] = 1,$$

where $[\alpha, \beta] = \alpha\beta\alpha^{-1}\beta^{-1}$. By cutting X along these $2g$-curves, we have a simply connected polygone of $4g$-sides, and inside the polygone, there are cusps of X. Write $X - Y = \{x_1, \ldots, x_d\}$, and draw curves π_i on the polygone from y encircling each cusp x_i and assume that they intersect only at y. Then, $\Phi = \pi_1(Y)$ is generated by $\pi_1, \ldots, \pi_d$ and $\alpha_1, \beta_1, \ldots, \alpha_g, \beta_g$ with the only relation:

$$\pi_d \pi_{d-1} \cdots \pi_1 [\alpha_g, \beta_g] \cdot \ldots \cdot [\alpha_1, \beta_1] = 1.$$

Let Φ_{ab} be the free $\mathbf{Z}$-module generated by $\{\alpha_1, \beta_1, \ldots, \alpha_g, \beta_g, \pi_1, \ldots, \pi_d\}$ and Φ_{ab}^{∞} be the free submodule of Φ_{ab} generated by $\{\pi_1, \ldots, \pi_d\}$. For each $\mathbf{Z}$-module A, let Φ act on A trivially. Then we have a natural diagram

(5.3)
$$\begin{tikzcd}
H^1(Y, A) \simeq & H^1(\Phi, A) \simeq & \{\varphi \in \operatorname{Hom}(\Phi_{ab}, A) \mid \varphi(\pi_1) + \ldots + \varphi(\pi_d) = 0\} \\
H^1(X, A) \simeq \arrow[u, hook] & H^1_P(\Phi, A) \simeq \arrow[u, hook] & \{\varphi \in \operatorname{Hom}(\Phi_{ab}, A) \mid \varphi(\pi_i) = 0 \text{ for } i = 1, \ldots, d\}, \arrow[u, hook]
\end{tikzcd}$$

which is commutative. Put $P(\Phi)=\{\pi_1,\dots,\pi_d\}$. By definition, we can identify $P(\Phi)$ with the set of generators of (the free part of) Φ_s for $s\in C(\Phi)$. Then, we have

$$(5.4)\qquad H^1(\Phi,A)\simeq H^1(\Phi,\mathbf{Z})\otimes_{\mathbf{Z}}A,\qquad H^1_P(\Phi,A)\simeq H^1_P(\Phi,\mathbf{Z})\otimes_{\mathbf{Z}}A,$$

and

$$\mathscr{G}(\Phi;A)=H^1(\Phi,A)/H^1_P(\Phi,A)\simeq\mathscr{G}(\Phi;\mathbf{Z})\otimes_{\mathbf{Z}}A\simeq\{\varphi\in\mathrm{Hom}(\Phi^\infty_{ab},A)\mid\sum_{n\in P(\Phi)}\varphi(\pi)=0\}.$$

Especially, this shows that $\dim_h\mathscr{G}(\Phi;\mathbf{C})=d-1$ and finishes the proof of Lemma 5.5 in the remaining case: $n=0$.

Theorem 5.8. *Let e be the idempotent attached to $T(p)$ and let A be either of $\mathbf{Z}_p$, $\mathbf{Z}/p^i\mathbf{Z}$, $\mathbf{T}_p$ or any field of characteristic 0. Then, we have for each $r>0$,*

$$(5.5)\quad (1-e)\mathscr{G}(\Gamma_1(Np^r);A)=\{\varphi\in\mathrm{Hom}(\Gamma_1(Np^r)^\infty_{ab},A)\mid\varphi(\pi)=0$$
$$\textit{for all } \pi\in P(\Gamma_1(Np^r)) \textit{ corresponding to unramified cusps}\}$$

and $\mathrm{corank}_{\mathbf{Z}_p}e\mathscr{G}(\Gamma_1(Np^r);\ \mathbf{T}_p)=\frac{1}{2}\varphi(p^r)\sum_{0<t\mid N}\varphi(t)\varphi(n/t)$.

Proof. Write Φ for $\Gamma_1(Np^r)$. Let $\mathscr{H}$ be a $\mathbf{Q}$-subalgebra of $\mathrm{End}(\mathscr{E}_2(\Phi;\mathbf{Q}))$ generated over $\mathbf{Q}$ by $T(l)$ and $T(l,l)$ for all primes l. Then, by Corollary 5.6, the idempotent e defined in $\mathscr{H}\otimes_{\mathbf{Q}}\mathbf{Q}_p$ is in fact contained in $\mathscr{H}$. Thus e naturally acts on $\mathscr{G}(\Phi;A)$ for A as in the theorem. Write the right-hand side of (5.5) as $V(A)$. Firstly, we suppose that A is an algebra. Let d_u be the number of unramified cusps in $C(\Phi)$ and put $d=\dim_{\mathbf{C}}\mathscr{G}(\Phi;\mathbf{C})$. By (5.4), $\mathscr{G}(\Phi;A)$ is A-free of rank d and thus, $V(A)$ is A-free and its rank is given by $d-d_u$, because A-linear forms: $\varphi\mapsto\varphi(\pi)$ for unramified π are linearly independent and vanish on $V(A)$. By Proposition 5.7, $V(A)$ contains $(1-e)\mathscr{G}(\Phi;A)$. Again by (5.4), we know that $(1-e)\mathscr{G}(\Phi;A)$ is A-free and

$$\mathrm{rank}_A(1-e)\mathscr{G}(\Phi;A)=\dim_{\mathbf{C}}(1-e)\mathscr{G}(\Phi;\mathbf{C})=d-\dim_{\mathbf{C}}e\mathscr{G}(\Phi;\mathbf{C}).$$

By Lemma 5.1, Lemma 5.3 and Corollary 5.6, we know that

$$d_u=\dim_{\mathbf{C}}e\mathscr{G}(\Phi;\mathbf{C}).$$

Summing up these arguments, we know that

$$\mathrm{rank}_A(1-e)\mathscr{G}(\Phi;A)=\mathrm{rank}_A V(A)\quad\text{and}\quad(1-e)\mathscr{G}(\Phi;A)\subset V(A),$$

which proves the assertion for an algebra A. For $A=\mathbf{T}_p$, we know that

$$V(\mathbf{T}_p)=\varprojlim_i V(\mathbf{Z}/p^i\mathbf{Z})\quad\text{and}\quad(1-e)\mathscr{G}(\Phi;\ \mathbf{T}_p)=\varprojlim_i(1-e)\mathscr{G}(\Phi;\mathbf{Z}/p^i\mathbf{Z}).$$

Thus the desired result follows from that of $\mathbf{Z}/p^i\mathbf{Z}$ and Lemma 5.1.

§6. Proof of Theorem 3.1

We divide our argument into several steps.

Step I. *The proof of*

$$(6.1) \qquad (\mathcal{W}^0)^{\Gamma_r} \simeq \mathcal{W}_r^0 \quad \textit{and} \quad (\mathcal{V}^0)^{\Gamma_r} \simeq \mathcal{V}_r^0 \quad \textit{for each } r \geqq 1.$$

We begin with a general lemma.

Lemma 6.1. *The image of* $H^1(\Phi_r^s/\Gamma_1(Np^r), \mathbf{Z}/p^m\mathbf{Z}(n))$ *in* $H^1(\Phi_r^s, \mathbf{Z}/p^m\mathbf{Z}(n))$ *under the inflation map is annihilated by the idempotent* e *attached to* $T(p)$ *for each* n, m *and* $r > s \geqq 0$ (of course, we have to assume that $m \leqq r$ if Φ_r^s acts on $\mathbf{Z}/p^m\mathbf{Z}(n)$ non-trivially, i.e., $n \not\equiv 0 \bmod p^{m-1}(p-1)$).

Proof. We write i for the inflation map. We identify $\Phi_r^s/\Gamma_1(Np^r)$ with Γ_s/Γ_r by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d \bmod p^r$ (we understand that Γ_0 denotes $\mathbf{Z}_p^\times$). For any 1-cocycle φ: $\Gamma_s/\Gamma_r \to \mathbf{Z}/p^m\mathbf{Z}(n)$, one knows that

$$i(\varphi)\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \varphi(d \bmod p^r) = \varphi(a^{-1} \bmod p^r) \quad \text{for } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Phi_r^s.$$

By Lemma 4.3 (ii), we have an explicit decomposition:

$$\Phi_r^s \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Phi_r^s = \bigcup_{u=1}^{p} \Phi_r^s \alpha_u$$

with $\alpha_u = \begin{pmatrix} 1 & u \\ 0 & p \end{pmatrix}$. For each $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Phi_r^s$, write

$$\alpha_u \gamma = \gamma_u \alpha_v \quad \text{for some } 1 \leqq v \leqq p \quad \text{and} \quad \gamma_u = \begin{pmatrix} a_u & b_u \\ c_u & d_u \end{pmatrix} \in \Phi_r^s.$$

Then, a simple computation shows that $a \equiv a_u \bmod p^r$ and hence, $d \equiv d_u \bmod p^r$. This shows that

$$(i(\varphi) | T(p))(\gamma) = \sum_{u=1}^{p} \varphi(d_u \bmod p^r) = p\, i(\varphi)(\gamma),$$

and thus, e annihilates the image $i(H^1(\Phi_r^s/\Gamma_1(Np^r), \mathbf{Z}/p^m\mathbf{Z}(n))$.

Lemma 6.2. *Let* $\Phi_r^s/\Gamma_1(Np^r)$ *act on* $\mathbf{T}_p = \mathbf{Q}_p/\mathbf{Z}_p$ *trivially. Then, we have the vanishing*

$$H^2(\Phi_r^s/\Gamma_1(Np^r), \mathbf{T}_p) = 0 \qquad \textit{for each } r \geqq s \geqq 0.$$

Proof. Let $\mathcal{N}$: $\mathbf{T}_p \to \mathbf{T}_p$ be the norm map defined by

$$\mathcal{N}(x) = \sum_\sigma \sigma \cdot x,$$

where σ runs over all elements of $\Phi_r^s/\Gamma_1(Np^r)$. Since $\Phi_r^s/\Gamma_1(Np^r)$ acts trivially on $\mathbf{T}_p$, $\mathcal{N}$ is the multiplication of the index $[\Phi_r^s : \Gamma_1(Np^r)]$. Thus $\mathcal{N}$ is surjective. It is well known that

$$H^2(\Phi_r^s/\Gamma_1(Np^r), \mathbf{T}_p) = \mathbf{T}_p/\mathcal{N}(\mathbf{T}_p),$$

since $\Phi_r^s/\Gamma_1(Np^r)$ is a finite cyclic group. Thus the lemma follows.

Now we shall prove (6.1) for $\mathscr{W}^0$. For each $r \geqq s \geqq 1$, we have the inflation and the restriction sequence:

$$0 \longrightarrow H^1(\Phi_r^s/\Gamma_1(Np^r), \mathbf{T}_p) \xrightarrow{\ i\ } H^1(\Phi_r^s, \mathbf{T}_p) \xrightarrow{\text{res}} H^1(\Gamma_1(Np^r), \mathbf{T}_p)^{\Gamma_s}$$
$$\longrightarrow H^2(\Phi_r^s/\Gamma_1(Np^r), \mathbf{T}_p).$$

The last term $H^2(\Phi_r^s/\Gamma_1(Np^r), \mathbf{\Pi}_p)$ is null by Lemma 6.2. After applying the idempotent e to the above sequence, we obtain another exact sequence:

$$0 \to e(i(H^1(\Phi_r^s/\Gamma_1(Np^r), \mathbf{T}_p))) \to eH^1(\Phi_r^s, \mathbf{T}_p) \to eH^1(\Gamma_1(Np^r), \mathbf{T}_p)^{\Gamma_s} \to 0.$$

We know that

$$e(i(H^1(\Phi_r^s/\Gamma_1(Np^r),\ \mathbf{T}_p))) = \varinjlim_m e(i(H^1(\Phi_r^s/\Gamma_1(Np^r), \mathbf{Z}/p^m\mathbf{Z}))) = 0$$

by Lemma 6.1. This shows that

$$eH^1(\Phi_r^s, \mathbf{T}_p) \simeq eH^1(\Gamma_1(Np), \mathbf{T}_p)^{\Gamma_s} \simeq (\mathscr{W}_r^0)^{\Gamma_s} \quad \text{(cf. (5.3))}.$$

By Lemma 4.5, we have

$$\text{res}:\ \mathscr{W}_s^0 \simeq eH^1(\Gamma_1(Np^s), \mathbf{T}_p) \simeq eH^1(\Phi_r^s, \mathbf{T}_p).$$

Thus, by combining these isomorphisms, we obtain

$$(6.2) \qquad (\mathscr{W}_r^0)^{\Gamma_s} \simeq \mathscr{W}_s^0 \quad \text{for each } r \geqq s > 0.$$

By taking the injective limit of this isomorphism with respect to r, we obtain the desired identity (6.1) for $\mathscr{W}^0$.

Next, we shall prove (6.1) for $\mathscr{V}^0$. Since $\mathscr{V}_r$ is a submodule of $\mathscr{W}_r$ defined by

$$\mathscr{V}_r = \{\varphi \in \operatorname{Hom}(\Gamma_1(Np^r), \mathbf{T}_p) \mid \varphi(\pi) = 0 \text{ for } \pi \in P(\Gamma_1(Np^r))\} \quad \text{(cf. (5.3))},$$

for each homomorphism φ: $\Gamma_1(Np^r) \to \mathbf{T}_p$ invariant under Γ_s and satisfying $\varphi|e = \varphi$, there is a homomorphism ψ: $\Gamma_1(Np^s) \to \mathbf{T}_p$ such that

$$\psi = \varphi \text{ on } \Gamma_1(Np^r) \quad \text{and} \quad \psi|e = \psi.$$

If we know that $\psi(\pi) = 0$ for all $\pi \in P(\Gamma_1(Np^s))$, then we will have an isomorphism

$$(\mathscr{V}_r^0)^{\Gamma_s} \simeq \mathscr{V}_s^0 \quad \text{for each } r > s,$$

and hence, $(\mathscr{V}^0)^{\Gamma_s} \simeq \mathscr{V}_s^0$ for each $r > s$. Thus, what we have to show is that $\psi \in H_P^1(\Gamma_1(Np^s), \mathbf{T}_p)$. Let $[\psi]$ be the class of ψ in

$$\mathscr{G}(\Gamma_1(Np^s), \mathbf{T}_p) = H^1(\Gamma_1(Np^s), \mathbf{T}_p)/H_P^1(\Gamma_1(Np^s), \mathbf{T}_p).$$

Since $\pi \in P(\Gamma_1(Np^r))$ generates the inertia group in $\Gamma_1(Np^r) = \pi_1(Y_r)$ for the corresponding cusp t of X_r, if t is unramified over a cusp t_0 of X_s, we may suppose that π generates the inertia group for t_0 in $\Gamma_1(Np^s) = \pi_1(Y_s)$. Thus we may suppose that each element of $P(\Gamma_1(Np^s))$ corresponding to unramified cusps over X_s is contained in $P(\Gamma_1(Np^r))$. Thus, especially, $\psi(\pi) = \varphi(\pi) = 0$ for all $\pi \in P(\Gamma_1(Np^s))$ corresponding unramified cusps of X_s over X_0, since every unramified cusp of X_s over X_0 is under an unramified cusp of X_r over X_0. Then, from Theorem 5.8, we know that

$$[\psi]|(1-e)=[\psi].$$

However, we have already known that $[\psi]|e=[\psi]$ because of $\psi|e=\psi$. This shows $[\psi]=0$ and we have the desired conclusion:

$$\psi \in H^1_P(\Gamma_1(Np^s), \mathbf{T}_p).$$

Step II. *V^0 and W^0 are Λ-free.*

We begin with a lemma:

Lemma 6.3. *Let M be a continuous compact Λ-module, and let $\mathcal{M}$ be its Pontryagin dual module. Put $\mathcal{M}[P_n]=\{m \in \mathcal{M} \mid P_n \cdot m=0\}$. Then M is Λ-free of finite* rank *r if and only if there is a subset I of integers with infinitely many elements such that $\mathcal{M}[P_n] \simeq \mathbf{T}_p^r$ for all $n \in I$.*

Proof. "Only if" part is clear; so, we shall prove the other direction. If $\mathcal{M}[P_n] \simeq \mathbf{T}_p^r$ for one $n \in \mathbf{Z}$, we have by duality that $M/P_nM \simeq \mathbf{Z}_p^r$. By Nakayama's lemma, M is generated by r-elements over Λ. Thus we can construct a surjective morphism of Λ-modules φ: $\Lambda^r \to M$. For each $n \in I$, this induces a surjection φ_n: $(\Lambda/P_n\Lambda)^r \to M/P_nM$. By duality, M/P_nM is $\mathbf{Z}_p$-free of rank r, and it is obvious that $\Lambda/P_n\Lambda \simeq \mathbf{Z}_p$; thus, φ_n is an isomorphism. Thus we know that $\mathrm{Ker}(\varphi)$ is contained in $P_n(\Lambda^r)$ and hence in the intersection of $P_n(\Lambda^r)$ for all $n \in I$, which is reduced to $\{0\}$, because Λ is a unique factorization domain and $\{P_n \mid n \in I\}$ is a set of infinitely many distinct prime elements of Λ.

Next we shall quote a result of Shimura [25, Th. 3.51 and Th. 8.4]:

Lemma 6.4. *For any subfield K of $\mathbf{C}$ or Ω, $H^1_P(\Gamma_1(M), L_n(K))$ is free of rank 2 over the Hecke algebra $\mathscr{h}_{n+2}(\Gamma_1(M); K)$ for each positive integer M.*

Proof. For the readers convenience, we give a proof of this fact, which is essential in the sequel. The proof given here looks a bit different from that given in [25, Th. 3.51] but in fact, they are essentially the same. Let $\varepsilon = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and $\tau = \begin{pmatrix} 0 & -1 \\ M & 0 \end{pmatrix}$. Since τ and ε normalize $\Gamma_1(M)$, we may let τ and ε act on $H^1_P(\Gamma_1(M), L_n(K))$ as described in §4. Write $[\tau]$ and $[\varepsilon]$ for the corresponding automorphism of $H^1_P(\Gamma_1(M), L_n(K))$. Let

$$\langle\ ,\ \rangle\colon\ H^1_P(\Gamma_1(M), L_n(K))^2 \to K$$

be the perfect pairing defined in [9, §3]. For any K-linear operator T on $H^1_P(\Gamma_1(M), L_n(K))$, let T^* be the adjoint operator of T under this pairing. Then we have the following interrelations of operators (e.g. [9, §3]):

$$T(m)^* = [\tau] \circ T(m) \circ [\tau]^{-1}, \qquad [\varepsilon] \circ T(m) = T(m) \circ [\varepsilon], \qquad [\varepsilon]^2 = 1$$

$$[\varepsilon]^* = (-1)^{n+1}[\varepsilon], \qquad [\tau]^* = (-1)^n[\tau], \qquad [\tau]^2 = (-1)^n N^n$$

and

$$[\tau]\circ[\varepsilon]=(-1)^n[\varepsilon]\circ[\tau].$$

Define another perfect pairing

$$(\ ,\ ):\ H_P^1(\Gamma_1(M),L_n(K))^2\to K \quad \text{by} \quad (x,y)=\langle x,y|[\tau]\rangle.$$

Then, we see that

$$(x|T(m),y)=(x,y|T(m)), \qquad (x,y)=-(y,x), \qquad (x|[\varepsilon],y)=-(x,y|[\varepsilon]).$$

Put $V^{\pm}(K)=\{v\in H_P^1(\Gamma_1(M),L_n(K)|\,v|[\varepsilon]=\pm v\}$. Then, by these formulae, $V^{\pm}(K)$ are modules over $\mathscr{h}_{n+2}(\Gamma_1(M);K)$ and under the pairing $(\ ,\ )$,

$$(*) \qquad V^{\pm}(K)\simeq \mathrm{Hom}_K(V^{\mp}(K),K) \quad \text{as} \quad \mathscr{h}_{n+2}(\Gamma_1(M);K)\text{-modules.}$$

Let ρ denote complex conjugation, and let ρ act on $S_{n+2}(\Gamma_1(M))$ by

$$\left(\sum_{n=1}^{\infty} a(n)q^n\right)^{\rho}=\sum_{n=1}^{\infty} a(n)^{\rho}q^n.$$

Then, if we write the isomorphism of (5.1a) as $\varphi\colon S_{n+2}(\Gamma_1(M))\simeq H_P^1(\Gamma_1(M),L_n(\mathbf{R}))$, one can easily check that $\varphi(f^{\rho})=-\varphi(f)|[\varepsilon]$. This shows that φ induces isomorphisms

$$V^-(\mathbf{R})\simeq S_{n+2}(\Gamma_1(M);\mathbf{R}) \quad \text{and} \quad V^+(\mathbf{R})\simeq\sqrt{-1}\,S_{n+2}(\Gamma_1(M);\mathbf{R}).$$

By the multiplication of $\sqrt{-1}$, we know that $V^+(\mathbf{R})\simeq V^-(\mathbf{R})$ as $\mathscr{h}_{n+2}(\Gamma_1(M);\mathbf{R})$-modules. From [13, Prop. 2.1], we know that

$$V^-(\mathbf{R})\simeq \mathrm{Hom}_{\mathbf{R}}(h_{n+2}(\Gamma_1(M);\mathbf{R}),\mathbf{R}) \quad \text{as} \quad \mathscr{h}_{n+2}(\Gamma_1(M),\mathbf{R})\text{-modules.}$$

Thus, by (*), we have that

$$V^-(\mathbf{R})\simeq V^+(\mathbf{R})\simeq \mathscr{h}_{n+2}(\Gamma_1(M);\mathbf{R}).$$

This shows that $V^{\pm}(\mathbf{Q})\simeq \mathscr{h}_{n+2}(\Gamma_1(M);\mathbf{Q})$, which yields the general identity: $V^{\pm}(K)\simeq \mathscr{h}_{n+2}(\Gamma_1(M);K)$ since $V^{\pm}(K)=V^{\pm}(\mathbf{Q})\otimes_{\mathbf{Q}}K$.

Corollary 6.5. *$\mathscr{h}_k(\Gamma_1(M);K)$ is a Frobenius algebra over K for $k\geqq 2$.*

Proof. By the above proof of Lemma 6.4, we have that

$$\mathscr{h}_k(\Gamma_1(M)\mathbf{R})\simeq \mathrm{Hom}_{\mathbf{R}}(\mathscr{h}_k(\Gamma_1(M);\mathbf{R}),\mathbf{R}) \quad \text{as} \quad \mathscr{h}_k(\Gamma_1(M);\mathbf{R})\text{-modules.}$$

Thus $\mathscr{h}_k(\Gamma_1(M);\mathbf{R})=\mathscr{h}_k(\Gamma_1(M);\mathbf{Q})\otimes_{\mathbf{Q}}\mathbf{R}$ is a Frobenius $\mathbf{R}$-algebra.

The property of being Frobenius algebra can be descended (cf. [3, Chap. IX]), and thus, $\mathscr{h}_k(\Gamma_1(M);\mathbf{Q})$ is a Frobenius algebra over $\mathbf{Q}$. Since $\mathscr{h}_k(\Gamma_1(M);K)=\mathscr{h}_k(\Gamma_1(M);\mathbf{Q})\otimes_{\mathbf{Q}}K$, the general assertion follows.

We shall start proving the assertion of this step. We shall only take care of the module $\mathscr{V}^0$, since the proof for $\mathscr{W}^0$ is quite the same. Put $\mu=\{\zeta\in\mathbf{Z}_p^{\times}|\,\zeta^{p-1}=1\}$. Then, as a subgroup of $Z(=\mathbf{Z}_p^{\times}\times(\mathbf{Z}/N\mathbf{Z})^{\times})$, the finite group μ acts on

$\mathcal{V}^0$. Thus we can decompose

$$\mathcal{V}^0=\bigoplus_{a=0}^{p-2}\mathcal{V}^0(a),$$

where $\mathcal{V}^0(a)=\{v\in\mathcal{V}^0\,|\,v|\zeta=\zeta^a v \text{ for } \zeta\in\mu\}$. Let $r(a)$ be the rank of the Hecke algebra $\mathscr{h}_2^0(\Phi_1,\omega^a;\mathbf{Z}_p)$, where ω is the character of $\mathbf{Z}_p^\times$ such that $\omega(x)=\lim\limits_{n\to\infty} x^{p^n}$ and $\Phi_1=\Gamma_0(p)\cap\Gamma_1(N)$. Then, we will show

$$\text{(6.3)}\qquad \mathcal{V}^0(a)[P_n]\simeq\mathbf{T}_p^{2r(a)}\quad\text{for each } n>0 \text{ with } n\equiv a \bmod p-1.$$

If we admit (6.3), then we conclude the Pontryagin dual module $V^0(a)$ of $\mathcal{V}^0(a)$ is Λ-free of rank $2r(a)$ by Lemma 6.3. Then, we obtain the desired result, since $V^0=\bigoplus\limits_{a=0}^{p-2}V^0(a)$. Now we shall prove (6.3). By [13, Cor. 3.2], we know that for each positive integer $n\equiv a \bmod (p-1)$,

$$\text{(6.4)}\qquad \operatorname{rank}_{\mathbf{Z}_p} e\mathscr{h}_{n+2}(\Phi_1,\mathbf{Z}_p)=r(a).$$

As seen in Lemma 4.6, we know that

$$eH_P^1(\Phi_1,L_n(\mathbf{Z}_p))\otimes_{\mathbf{Z}_p}\mathbf{T}_p \quad \text{is } p\text{-divisible},$$

and by Lemma 6.4, we know from (6.4) that

$$\text{(6.5)}\qquad eH_P^1(\Phi_1,L_n(\mathbf{Z}_p))\otimes_{\mathbf{Z}_p}\mathbf{T}_p\simeq\mathbf{T}_p^{2r(a)}.$$

By Corollary 4.10, the natural map

$$\text{(6.6)}\qquad eH_P^1(\Phi_1,L_n(\mathbf{Z}_p))\otimes_{\mathbf{Z}_p}\mathbf{Z}/p^r\mathbf{Z}\to eH_P^1(\Phi_1,L_n(\mathbf{Z}/p^r\mathbf{Z}))\quad\text{is injective.}$$

Let us put

$$H^1(\Gamma_1(Np^r),n;\mathbf{Z}/p^r\mathbf{Z})=\{v\in H^1(\Gamma_1(Np^r),\mathbf{Z}/p^r\mathbf{Z})\,\big|\,v|z=z^n v \text{ for } z\in\mathbf{Z}_p^\times\}.$$

Then, the inflation and the restriction sequence gives an exact sequence

$$0\to H^1(\Phi_r/\Gamma_1(Np^r),\mathbf{Z}/p^r\mathbf{Z}(n))\to H^1(\Phi_r,\mathbf{Z}/p^r\mathbf{Z}(n))\to H^1(\Gamma_1(Np^r),n;\mathbf{Z}/p^r\mathbf{Z}).$$

By Lemma 6.1, we know that the restriction map

$$\text{(6.7)}\qquad eH_P^1(\Phi_r,\mathbf{Z}/p^r\mathbf{Z}(n))\to eH_P^1(\Gamma_1(Np^r),n;\mathbf{Z}/p^r\mathbf{Z}) \text{ is injective.}$$

On the other hand, we have by Lemma 4.5 an isomorphism

$$\text{(6.8)}\qquad eH_P^1(\Phi_r,L_n(\mathbf{Z}/p^r\mathbf{Z}))\simeq eH_P^1(\Phi_r,\mathbf{Z}/p^r\mathbf{Z}(n)).$$

By (6.1), $eH_P^1(\Gamma_1(Np^r),n;\mathbf{Z}/p^r\mathbf{Z})$ $(=e(H^1(\Gamma_1(Np^r),n;\mathbf{Z}/p^r\mathbf{Z})\cap H_P^1(\Gamma_1(Np^r),\mathbf{Z}/p^r\mathbf{Z})))$ can be identified with a subspace of $\mathcal{V}^0(a)[P_n]$ for $n\equiv a \bmod p-1$. By combining these morphisms (6.6), (6.8) and (6.7) in order, we have an injection

$$I_r^n\colon\; eH_P^1(\Phi_1,L_n(\mathbf{Z}_p))\otimes_{\mathbf{Z}_p}\mathbf{Z}/p^r\mathbf{Z}\to\mathcal{V}^0(a)[P_n]$$

for each n with $n \equiv a \bmod p-1$. By taking the injective limit of I_r^n with respect to r, we have an embedding

$$I^n\colon\ eH_P^1(\Phi_1, L_n(\mathbf{Z}_p)) \otimes_{\mathbf{Z}_p} \mathbf{T}_p \to \mathscr{V}^0(a)[P_n].$$

By (6.1), we have a surjective Λ-morphism: $\Lambda^{2r(a)} \to V^0(a)$. This induces a surjection: $\mathbf{Z}_p^{2r(a)} \simeq (\Lambda/P_n\Lambda)^{2r(a)} \to V^0(a)/P_n V^0(a)$. By duality, we know that

$$\mathscr{V}^0(a)[P_n] \text{ is embedded into } \mathbf{T}_p^{2r(a)}.$$

Thus we have the following inclusions:

$$\begin{aligned} \mathbf{T}_p^{2r(a)} &\simeq eH_P^1(\Phi_1, L_n(\mathbf{Z}_p)) \otimes_{\mathbf{Z}_p} \mathbf{T}_p \\ &\subset eH_P^1(\Phi_1, L_n(\mathbf{T}_p)) \\ &\subset \mathscr{V}^0(a)[P_n] \hookrightarrow \mathbf{T}_p^{2r(a)}. \end{aligned}$$

This shows that every inclusion as above is in fact a surjective isomorphism, and we now know that

$$\mathscr{V}^0(a)[P_n] \simeq \mathbf{T}_p^{2r(a)} \qquad \text{for each } n>0 \quad \text{with} \quad n \equiv a \bmod p-1.$$

This finishes Step II.

Before going into the final step, we record a byproduct of Step II:

Theorem 6.6. *For each $m>0$, there is a canonical isomorphism:*

$$eH_P^1(\Phi_1, L_n(\mathbf{Z}_p)) \otimes_{\mathbf{Z}_p} \mathbf{Z}/p^m\mathbf{Z} \simeq eH_P^1(\Phi_1, L_n(\mathbf{Z}/p^m\mathbf{Z})).$$

Moreover, if $n \equiv a \bmod p-1$, we have an isomorphism of $\mathscr{h}_2^0(Np^\infty; \mathbf{Z}_p)$-modules:

$$eH_P^1(\Phi_1, L_n(\mathbf{Z}_p)) \otimes_{\mathbf{Z}_p} \mathbf{T}_p \simeq eH_P^1(\Phi_1, L_n(\mathbf{T}_p)) \simeq \mathscr{V}^0(a)[P_n].$$

Step III $\operatorname{rank}_\Lambda W^0 = \operatorname{rank}_\Lambda V^0 + \frac{1}{2}\varphi(p) \cdot \sum_{0<t|N} \varphi(t)\varphi(N/t)$.

The fact that $\operatorname{rank}_\Lambda(V^0) = 2\operatorname{rank}_\Lambda(\mathscr{h}^0(N; \mathbf{Z}_p))$ is clear from Step II. Thus what we have to prove is

Proposition 6.7. *Let us put $\mathscr{G}^0 = \mathscr{W}^0/\mathscr{V}^0$ and $G^0 = \operatorname{Hom}(\mathscr{G}^0, \mathbf{T}_p)$. Then G^0 is Λ-free of finite rank and*

$$\operatorname{rank}_\Lambda(G^0) = \tfrac{1}{2}\varphi(p) \cdot \sum_{0<t|N} \varphi(t)\varphi(N/t).$$

Moreover, for each $r>0$, we have that

$$(\mathscr{G}^0)^{\Gamma_r} \simeq e\mathscr{G}(\Gamma_1(Np^r); \mathbf{T}_p).$$

Proof. We have an exact sequence:

$$0 \to G^0 \to W^0 \to V^0 \to 0.$$

Since V^0 is Λ-free, this exact sequence splits, and thus G^0 is Λ-free. This shows that

$$(\mathscr{G}^0)^{\Gamma_r} \simeq (\mathscr{W}^0)^{\Gamma_r}/(\mathscr{V}^0)^{\Gamma_r} \simeq e\mathscr{G}(\Gamma_1(Np^r); \mathbf{T}_p).$$

By Theorem 5.8, we have that

$$\operatorname{corank}_{\Lambda}\mathscr{G}^0=\operatorname{corank}_{\mathbf{Z}_p} e\mathscr{G}(\Gamma_1(Np);\ \mathbf{T}_p)=\tfrac{1}{2}\varphi(p)\cdot\sum_{0<t\mid N}\varphi(t)\,\varphi(N/t).$$

This finishes the proof.

§7. Proof of Theorems 1.1 and 1.2

We begin by defining a pairing between the Hecke algebras and the spaces of modular forms. Let K be a finite extension of $\mathbf{Q}_p$, and let $\mathcal{O}_K$ be its p-adic integer ring. We write $\mathbf{T}_p$ for $\mathbf{Q}_p/\mathbf{Z}_p$, and put

$$S_k(Np^r;K/\mathcal{O}_K)=S_k(\Gamma_1(Np^r);K)/S_k(\Gamma_1(Np^r);\mathcal{O}_K).$$

By definition, one can embed via q-expansion this space into the module of formal series $(K/\mathcal{O}_K)[[q]]$. We take the injective limit:

$$S_k(Np^\infty;K/\mathcal{O}_K)=\varinjlim_r S_k(Np^r;K/\mathcal{O}_K)\to(K/\mathcal{O}_K)[[q]].$$

Naturally $S_k(Np^\infty;K/\mathcal{O}_K)$ is isomorphic to $S_k(Np^\infty;K)/S_k(Np^\infty;\mathcal{O}_K)$. For each element $f\in S_k(Np^\infty;K/\mathcal{O}_K)$, we write its q-expansion as $\sum_{n=0}^{\infty}a(n,f)q^n$. Naturally, the Hecke algebra $\mathscr{h}_k(Np^\infty;\mathcal{O}_K)$ acts on $S_k(Np^\infty;K/\mathcal{O}_K)$. We define a pairing

(7.1a) $(\ ,\ )$: $\mathscr{h}_k(Np^\infty;\mathcal{O}_K)\times S_k(Np^\infty;K/\mathcal{O}_K)\to K/\mathcal{O}_K$ by $(h,f)=a(1,f\mid h)$.

This pairing satisfies

(7.1b) $$(h,f\mid h')=(hh',f)\quad\text{for } h,h'\in\mathscr{h}_k(Np^\infty;\mathcal{O}_K).$$

We shall equip $S_k(Np^\infty;K/\mathcal{O}_K)$ with the discrete topology.

Lemma 7.1. *Put* $S_k^0(Np^r;K/\mathcal{O}_K)=eS_k(Np^r;K/\mathcal{O}_K)$ *for the idempotent* e *in* $\mathscr{h}_k(Np^\infty;\mathcal{O}_K)$ *attached to* $T(p)$. *Then the pairing* (7.1a) *induces the Pontryagin duality between* $\mathscr{h}_k(Np^r;\mathbf{Z}_p)$ *and* $S_k(Np^r;\mathbf{T}_p)$ (*resp.* $\mathscr{h}_k^0(Np^r;\mathbf{Z}_p)$ *and* $S_k^0(Np^r;\mathbf{T}_p)$) *for* $r=1,2,\ldots,\infty$.

This follows from the argument in [13, §2].

Lemma 7.2. *For each pair of weights* $k>l\,(\geqq 1)$, *there is a continuous surjective algebra homomorphism of* $\mathscr{h}_k(Np^\infty;\mathcal{O}_K)$ *onto* $\mathscr{h}_l(Np^\infty;\mathcal{O}_K)$, *which sends the Hecke operator* $T(n)$ *of weight* k *to that of weight* l *for each positive integer* n. *It induces a surjective algebra homomorphism of the ordinary part of the Hecke algebras.*

Proof. Since $\mathscr{h}_k(Np^\infty;\mathcal{O}_K)=\mathscr{h}_k(Np^\infty;\mathbf{Z}_p)\hat{\otimes}_{\mathbf{Z}_p}\mathcal{O}_K$, we may assume that $\mathcal{O}_K=\mathbf{Z}_p$. It suffices to construct the homomorphism for $l=k-1$. Define a formal q-expansion for each $t\in(\mathbf{Z}/p^r\mathbf{Z})^\times$ by

$$G(r,t)=-t_0p^{-r}+\tfrac{1}{2}+\sum_{n=1}^{\infty}\Big(\sum_{\substack{d\mid n\\ d\equiv t \bmod p^r}}\operatorname{sgn}(d)\Big)q^n,$$

where t_0 is an integer satisfying $0 \leqq t_0 < p^r$ and $t_0 \equiv t \bmod p^r$. Then, as shown by Hecke [8, §2], $G(r,t)$ gives in fact the q-expansion of an element of $\mathcal{M}_1(\Gamma_1(Np^r); \mathbf{Q})$ and satisfies

$$G(r,t)|_1 \begin{pmatrix} a & b \\ c & d \end{pmatrix} = G(r, at) \quad \text{for} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(Np^r)$$

(e.g. [12, Lemma 6.1]). Put $E(r,t) = -p^r G(r,t)$. Then, we have a congruence: $E(r,t) \equiv t \bmod p^r$ (because of our assumption $p \geqq 5$). For any $\mathbf{Z}_p$-module M, we write $M[p^r]$ for the kernel in M of the multiplication by p^r. Then, the multiplication of $E(r,1)$ induces an injective morphism

$$i_r\colon\ S_{k-1}(Np^\infty; \mathbf{T}_p)[p^r] \to S_k(Np^\infty; \mathbf{T}_p)[p^r],$$

since i_r preserves the q-expansion. This injection is compatible with Hecke operators. Let us verify this fact: If we take $f \in S_{k-1}(\Gamma_1(Np^s); \mathbf{Q})$ such that $p^r f \in S_{k-1}(\Gamma_1(Np^s); \mathbf{Z}_p)$ and if write f' for $f E(r,1)$, then f and f' has the same q-expansion modulo $\mathbf{Z}_p[[q]]$. For each prime l outside Np, we take $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(Np^m)$ (for m larger than r and s) such that $d \equiv l \bmod Np^m$. Then we have that

$$f'|_k \gamma = (f|_{k-1}\gamma)(E(r,1)|_1 \gamma) \equiv l^{-1}(f|_{k-1}\gamma) \bmod \mathbf{Z}_p[[q]],$$

since $E(r,1)|_1 \gamma = E(r,a) \equiv a \equiv l^{-1} \bmod p^r \mathbf{Z}_p[[q]]$.

This show that

$$\begin{aligned} a(n, f'|T(l)) &= a(nl, f') + l^{k-1} a\left(\frac{n}{l}, f'|_k \gamma\right) \\ &\equiv a(nl, f) + l^{k-2} a\left(\frac{n}{l}, f|_{k-1}\gamma\right) \bmod \mathbf{Z}_p. \\ &\equiv a(n, f|T(l)) \bmod \mathbf{Z}_p. \end{aligned}$$

Thus we know that $i_r \circ T(l) = T(l) \circ i_r$. The equivariance of i_r with $T(l)$ for prime divisors l of Np and with $T(l,l)$ for arbitrary primes l is obvious. Since i_r preserves q-expansion, we have a commutative diagram for $r > s$:

$$\begin{tikzcd} i_s\colon\ S_{k-1}(Np^\infty; \mathbf{T}_p)[p^s] \arrow[r] \arrow[d] & S_k(Np^\infty; \mathbf{T}_p)[p^s] \arrow[d] \\ i_r\colon\ S_{k-1}(Np^\infty; \mathbf{T}_p)[p^r] \arrow[r] & S_k(Np^\infty; \mathbf{T}_p)[p^r]. \end{tikzcd}$$

After taking the injective limit relative to r of these morphisms i_r, we obtain an embedding

$$i\colon\ S_{k-1}(Np^\infty; \mathbf{T}_p) \to S_k(Np^\infty; \mathbf{T}_p),$$

which is equivariant under Hecke operators. By duality, we obtain a continuous surjective algebra homomorphism: $h_k(Np^\infty; \mathbf{Z}_p) \to h_{k-1}(Np^\infty; \mathbf{Z}_p)$, which was to be shown.

Proof of Theorem 1.1. As seen in §1 and Lemma 7.2, we have surjective continuous morphisms which make the following diagram commutative:

$$\begin{tikzcd} \mathscr{h}^0(Np;\mathcal{O}_K) \arrow[r, "\rho_{\infty,k}"] \arrow[dr, "\rho_{\infty,2}"'] & \mathscr{h}_k^0(Np^\infty;\mathcal{O}_K) \arrow[d] \\ & \mathscr{h}_2^0(Np^\infty;\mathcal{O}_K) \quad \text{(for each } k \geqq 2). \end{tikzcd}$$

Thus, what we have to prove is that $\rho_{\infty,2}$ is an injection.

Since $\mathscr{h}^0(Np;\mathcal{O}_K)$ is finite over Λ_K (cf. [13, Cor. 4.2]), $\mathscr{h}_2^0(Np^\infty;\mathcal{O}_K)$ is also finite over Λ_K,

$$\mathscr{h}_2^0(Np^\infty;\mathcal{O}_K)=\mathscr{h}_2^0(Np^\infty;\mathbf{Z}_p)\otimes_{\mathbf{Z}_p}\mathcal{O}_K \quad \text{and} \quad \mathscr{h}^0(Np;\mathcal{O}_K)=\mathscr{h}^0(Np;\mathbf{Z}_p)\otimes_{\mathbf{Z}_p}\mathcal{O}_K.$$

Thus we may assume that $\mathcal{O}_K=\mathbf{Z}_p$. Since the subgroup $\mu=\{\zeta\in\mathbf{Z}_p^W|\zeta^{p-1}=1\}$ of Z acts on $\mathscr{h}^0(Np;\mathbf{Z}_p)$, $\mathscr{h}_2^0(Np^\infty;\mathbf{Z}_p)$ and $\mathscr{V}^0$, we can decompose

$$\mathscr{h}^0(Np;\mathbf{Z}_p)=\bigoplus_{a \bmod p-1}\mathscr{h}^0(a),$$

$$\mathscr{h}_2^0(Np^\infty;\mathbf{Z}_p)=\bigoplus_{a \bmod p-1}\mathscr{h}_2^0(a)$$

and

$$\mathscr{V}^0=\bigoplus_{a \bmod p-1}\mathscr{V}^0(a),$$

where $\zeta\in\mu$ acts on $\mathscr{h}^0(a)$, $\mathscr{h}_2^0(a)$ and $\mathscr{V}^0(a)$ by he character: $\zeta\mapsto\zeta^a$. Then, $\rho_{\infty,2}$ induces a surjective homomorphism of Λ-algebras: $\mathscr{h}^0(a)\to\mathscr{h}_2^0(a)$ for each a. Here we regard $\mathscr{h}_2^0(Np^\infty;\mathbf{Z}_p)$ as Λ-algebra through the action of $z=(z_p,z_0)\in Z$ on $S_2(\Gamma_1(Np^r);\mathbf{Z}_p)$ given by $f|z=z_p^2f|\sigma$ for $\sigma\in\Gamma_0(Np^r)$ with $\sigma\equiv\begin{pmatrix}* & *\\ 0 & z\end{pmatrix} \bmod Np^r$. On the other hand, we have let $z\in Z$ act on $H_P^1(\Gamma_1(Np^r), \mathbf{T}_p)$ by the action of $\sigma\in\Gamma_0(Np^r)$ as above. Thus the action of Z on $\mathscr{h}_2^0(Np^\infty;\mathbf{Z}_p)$ induced by the former is the twist of that induced by the latter by the character: $z\mapsto z_p^2$ of Z. Thus $\mathscr{h}_2^0(a)$ acts on $\mathscr{V}^0(a-2)$. Write n for $k-2$ for each integer $k\geqq 2$ and suppose that $k\equiv a \bmod (p-1)$. Then the restriction of operators in $\mathscr{h}_2^0(a)$ to $\mathscr{V}^0(a-2)[P_n]$ gives an $\mathbf{Z}_p$-algebra homomorphism β of $\mathscr{h}_2^0(a)/P_k\mathscr{h}_2^0(a)$ onto the subalgebra of $\mathrm{End}(\mathscr{V}^0(a-2)[P_n])$ generated by all Hecke operators $T(l)$ and $T(l,l)$, which is isomorphic to $\mathscr{h}_k^0(\Phi_1;\mathbf{Z}_p)$ by Theorem 6.6 and Lemma 6.4. On the other hand, we have already seen in [13, Cor. 3.2] that $\mathscr{h}^0(a)/P_k\mathscr{h}^0(a)\simeq\mathscr{h}_k^0(\Phi_1;\mathbf{Z}_p)$ for each $k\geqq 2$ with $k\equiv a \bmod (p-1)$. Thus, we have the following commutative diagram:

$$\begin{tikzcd} \mathscr{h}^0(a)/P_k\mathscr{h}^0(a) \arrow[r, "\alpha"] \arrow[d, phantom, "\wr\|"] & \mathscr{h}_2^0(a)/P_k\mathscr{h}_2^0(a), \arrow[dl, "\beta"] \\ \mathscr{h}_k^0(\Phi_1;\mathbf{Z}_p) & \end{tikzcd}$$

where α is induced by $\rho_{\infty,2}$. Since α and β are surjective, they are isomorphisms. Then, by Lemma 6.3, $\mathscr{h}_2^0(a)$ is free of the same rank as $\mathscr{h}^0(a)$ over Λ. This shows the desired isomorphism: $\mathscr{h}^0(a)\simeq\mathscr{h}_2^0(a)$ for each a.

Proof of Theorem 1.2. As seen in §1, one has a surjective homomorphism of $\mathcal{O}_K$-algebras:

$$\rho_{k,\varepsilon}\colon h^0(N;\mathcal{O}_K)/P_{k,\varepsilon}h^0(N;\mathcal{O}_K)\to h_k^0(\Phi_r^1,\varepsilon;\mathcal{O}_K).$$

What we have to show is the injectivity of $\rho_{k,\varepsilon}$. Write R for the rank of $h^0(N;\mathcal{O}_K)$ over Λ_K and $R(k,\varepsilon)$ for the rank of $h_k^0(\Phi_r^1,\varepsilon;\mathcal{O}_K)$ over $\mathcal{O}_K$. If $R=R(k,\varepsilon)$, we have the desired injectivity from the surjectivity of $\rho_{k,\varepsilon}$. What we know is the inequality $R(k,\varepsilon)\leqq R$. By Theorem 3.1, the rank of $eH_P^1(\Gamma_1(Np^r);\mathbf{Z}_p)$ is equal to $2[\Gamma:\Gamma_r]R$. Thus, by Lemma 6.4, we know that

$$\operatorname{rank}_{\mathcal{O}_K}(h_2^0(\Gamma_1(Np^r);\mathcal{O}_K))=[\Gamma:\Gamma_r]R.$$

Since $h_k^0(\Gamma_1(Np^r);\mathcal{O}_K)=h_k^0(\Gamma_1(Np^r);\mathbf{Z}_p)\otimes_{\mathbf{Z}_p}\mathcal{O}_K$ and since

$$h_k^0(\Gamma_1(Np^r);K)=h_k^0(\Gamma_1(Np^r);\mathcal{O}_K)\otimes_{\mathcal{O}_K}K=\bigoplus_{\varepsilon}h_k^0(\Phi_r^1,\varepsilon;K),$$

we know that $[\Gamma:\Gamma_r]R=\sum_{\varepsilon}R(2,\varepsilon)$, where ε runs over all the characters of Γ/Γ_r. Since $R(2,\varepsilon)\leqq R$, the only possibility is the equality $R=R(2,\varepsilon)$. This finishes the proof for $k=2$. In order to prove the result for general $k>2$, we take the Eisenstein series $E(1,1)\equiv 1 \bmod p$ defined in the proof of Lemma 7.2. Then, the multiplication of $E(1,1)^{k-2}$ induces an injection:

$$S_2^0(Np;\mathbf{T}_p)[p]\to S_k^0(Np^r;\mathbf{T}_p)[p].$$

By duality, we have a surjection:

$$h_k^0(\Gamma_1(Np^r);\mathbf{Z}_p)\otimes_{\mathbf{Z}_p}\mathbf{Z}/p\mathbf{Z}\to h_2^0(\Gamma_1(Np^r);\mathbf{Z}_p)\otimes_{\mathbf{Z}_p}\mathbf{Z}/p\mathbf{Z}.$$

Thus, we have the following inequality:

$$\sum_{\varepsilon}R(k,\varepsilon)=\operatorname{rank}_{\mathcal{O}}(h_k^0(\Gamma_1(Np^r);\mathcal{O}_K))\geqq R[\Gamma:\Gamma_r],$$

and we conclude that $R=R(k,\varepsilon)$ for each k and ε because of $R(k,\varepsilon)\leqq R$. This finishes the proof.

§8. Proof of Theorem 2.1

Before proving Theorem 2.1, we shall construct several Galois modules out of modular curves. We shall take the compactified canonical model $X_r=X_1(Np^r)$ over $\mathbf{Q}$ of $\Gamma_1(Np^r)\backslash\mathfrak{H}$ (cf. [25, 6.7]) corresponding to the idele group:

$$\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in\prod_l \mathrm{GL}_2(\mathbf{Z}_l)\,\middle|\, c\equiv 0 \bmod Np^r \text{ and } a\equiv 1 \bmod Np^r\right\}.$$

Then, we consider the jacobien variety $J_{r/\mathbf{Q}}$ of $X_1(Np^r)_{/\mathbf{Q}}$. Let $J_r[p^n]_{/\mathbf{Q}}$ denote the finite group scheme over $\mathbf{Q}$ which is the kernel of the multiplication of p^n on J_r. Put $J_r[p^\infty]=\bigcup_n J_r[p^n]$. We identify $J_r[p^n]$ for each $n=1,2,\ldots,\infty$ with the group of its $\bar{\mathbf{Q}}$-points. Then $J_r[p^n]$ for $0<n\leqq\infty$ is equipped with natural left action of the absolute Galois group $\mathfrak{G}=\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. Let

$$\mathscr{T}_r=\varprojlim_n J_r[p^n] \quad \text{(the Tate module of } J_r\text{)},$$

which is a left Galois module free of finite rank over $\mathbf{Z}_p$ and unramified outside Np. Let $\mu_{p^n/\mathbf{Z}}$ be the finite flat group scheme over $\mathbf{Z}$ which is obtained as the kernel of the multiplication of p^n on the multiplicative group $\mathbf{G}_{m/\mathbf{Z}}$, and put $\mu_{p^\infty/\mathbf{Z}}=\bigcup_n \mu_{p^n}$ as a p-divisible group over $\mathbf{Z}$. The Galois action on $\mu_{p^\infty}(\bar{\mathbf{Q}})$ defines the cyclotomic character $\chi\colon \mathfrak{G}\to\mathbf{Z}_p^\times$. Under the identification of J_r with $\mathrm{Pic}^0(X_r)$, the ring of algebraic correspondences on $X_r\times X_r$ acts on J_r contravariantly. Since $\mathscr{h}_2(\Gamma_1(Np^r);\mathbf{Z})$ can be considered as a subring of this ring of correspondences, $J_r[p^n]$ becomes a right $\mathscr{h}_2(\Gamma_1(Np^r);\mathbf{Z}_p)$-module. There is a well known isomorphism

$$\varphi\colon\ J_r[p^\infty]\simeq \mathrm{Pic}^0(X_r)[p^\infty]\simeq H^1(X_{r/\mathbf{Q}},\mu_{p^\infty})$$

as $\mathscr{h}_2(\Gamma_1(Np^r);\mathbf{Z}_p)$-modules, where we have taken the cohomology group over the étale site on $X_{r/\bar{\mathbf{Q}}}$. Since the functor of the cohomology groups is contravariant, the Galois action on $H^1(X_{r/\bar{\mathbf{Q}}},\mu_{p^\infty})$ is a right action and is different from that on $J_r[p^\infty]$. For $x\in J_r[p^\infty](\bar{\mathbf{Q}})$ and $\sigma\in\mathfrak{G}$, the relation between the two action is given by

$$\varphi(\sigma\cdot x)=\varphi(x)\cdot\sigma^{-1}. \tag{8.1}$$

The projection: $X_r\to X_s$ for $r>s$ induces contravariantly a morphism: $J_s\to J_r$. This morphism is compatible with the Galois action. Thus we can define the injective limit

$$J_\infty[p^n]=\varinjlim_r J_r[p^n] \qquad \text{for } 0<n\leqq\infty,$$

which is an $\mathscr{h}_2(Np^\infty;\mathbf{Z}_p)$-module as well as a Galois module.

The two module structures on $J_\infty[p^n]$ are compatible. If we identify $\mu_{p^n/\bar{\mathbf{Q}}}$ with $(\mathbf{Z}/p^n\mathbf{Z})_{/\bar{\mathbf{Q}}}$ by $e\left(\dfrac{2\pi i}{p^n}\right)\mapsto 1$, we have an isomorphism of $\mathscr{h}_2(\Gamma_1(Np^r);\mathbf{Z}_p)$-modules: $\mathscr{V}_r\simeq J_r[p^\infty]$. Next, we identify J_r with the Albanese variety of X_r. Then, $\mathscr{h}_2(\Gamma_1(Np^r);\mathbf{Z}_p)$ acts on $\mathscr{T}_r$ covariantly, and hence, $\mathscr{T}_r$ is a left $\mathscr{h}_2(\Gamma_1(Np^r);\mathbf{Z}_p)$-module as well as a left Galois module. For each pair $r>s$, the projection: $X_r\to X_s$ induces covariantly a $\mathbf{Q}$-rational morphism: $J_r\to J_s$. Put

$$\mathscr{T}_\infty=\varprojlim_r \mathscr{T}_r,$$

which is a left module of $\mathscr{h}_2(Np^\infty;\mathbf{Z}_p)$ as well as a left $\mathfrak{G}$-module unramified outside Np. Since $\mathrm{Alb}(X_r)$ and $\mathrm{Pic}^0(X_r)$ are mutually dual, there is a natural pairing

$$\langle\ ,\ \rangle\colon\ \mathscr{T}_r\times J_r[p^\infty]\to\mu_{p^\infty}(\bar{\mathbf{Q}})$$

satisfying the conditions:

(i) $\langle \sigma\cdot x, \sigma\cdot y\rangle = \langle x,y\rangle^{\sigma} = \chi(\sigma)\langle x,y\rangle$ for each $\sigma\in\mathfrak{G}$;

(ii) $\langle h\cdot x, y\rangle = \langle x, y\cdot h\rangle$ for each $h\in \mathfrak{h}_2(\Gamma_1(Np^r);\mathbf{Z}_p)$.

Moreover, if we identify μ_{p^∞} with $\mathbf{T}_p$ as above, this pairing gives the Pontryagin duality between $\mathscr{T}_r$ and $J_r[p^\infty]$. The natural morphisms: $\mathscr{T}_r\to\mathscr{T}_s$ and $J_s[p^\infty]\to J_r[p^\infty]$ for $r>s$ are mutually adjoint, and thus, this pairing induces a pairing

$$\langle\ ,\ \rangle\colon \mathscr{T}_\infty\times J_\infty[p^\infty]\to\mu_{p^\infty}(\bar{\mathbf{Q}}),$$

which gives the Pontryagin duality between them. Let e be the idempotent attached to $T(p)$ in $\mathfrak{h}_2(Np^\infty;\mathbf{Z}_p)$, and put

$$\mathscr{T}_\infty^0 = e\cdot\mathscr{T}_\infty \quad\text{and}\quad J_\infty^0[p^\infty] = J_\infty[p^\infty]\,|\,e.$$

Then, we have isomorphisms of $\mathfrak{h}^0(N;\mathbf{Z}_p)$-modules

$$\mathscr{T}_\infty^0 \simeq V^0 \quad\text{and}\quad J_\infty^0[p^\infty]\simeq\mathscr{V}^0.$$

A warning may be necessary: The two action of the Hecke operators on J_r (i.e. the right action through viewing J_r as $\mathrm{Pic}^0(X_r)$ and the left action via the identification: $J_r=\mathrm{Alb}(X_r)$) are different, and they are transformed each other by the involution associated with the canonical divisor on J_r.

Now let us begin the proof of Theorem 2.1. Let K be a finite extension of $\mathbf{Q}_p$, and let $\mathscr{L}_K$ be the quotient field of Λ_K. Put $\mathfrak{g}(N;K)=\mathfrak{h}^0(N;\mathcal{O}_K)\otimes_{\Lambda_K}\mathscr{L}_K$, and $V_K=\mathscr{T}_\infty^0\otimes_\Lambda\mathscr{L}_K$. Then $\mathfrak{g}(N;K)$ naturally acts on V_K.

Lemma 8.1. *The module V_K is free of* rank 2 *over* $\mathfrak{g}(N;K)$.

Proof. Let P denote the height one prime P_0 in Λ, and let Λ_P be the localization of Λ at P. By Theorem 3.1, one knows that $\mathscr{T}_\infty^0/P\mathscr{T}_\infty^0\simeq e\mathscr{T}_1$ as $\mathfrak{h}^0(N;\mathbf{Z}_p)$-modules. Put $\mathscr{T}_{\infty,P}^0=\mathscr{T}_\infty^0\otimes_\Lambda\Lambda_P$. Then, we know that

$$\mathscr{T}_{\infty,P}^0/P\mathscr{T}_{\infty,P}^0\simeq e\mathscr{T}_1^0\otimes_{\mathbf{Z}_p}\mathbf{Q}_p.$$

By Lemma 6.4, $\mathscr{T}_1\otimes_{\mathbf{Z}_p}\mathbf{Q}_p$ is free of rank 2 over $\mathfrak{h}_2(\Gamma_1(Np);\mathbf{Q}_p)$. Let x_1 and x_2 be elements of $\mathscr{T}_{\infty,P}^0$ which generate $\mathscr{T}_{\infty,P}^0/P\mathscr{T}_{\infty,P}^0$. Put $\mathfrak{h}_P=\mathfrak{h}^0(N;\mathbf{Z}_p)\otimes_\Lambda\Lambda_P$ and define a morphism

$$\varphi\colon\ \mathfrak{h}_P^2\to\mathscr{T}_{\infty,P}^0$$

by $\mathfrak{h}_P^2\ni(h_1,h_2)\mapsto h_1x_1+h_2x_2\in\mathscr{T}_{\infty,P}^0$, which is surjective by Nakayama's lemma, since $\mathfrak{h}_P$ is a semi-local ring. Note that $\mathfrak{h}_P^2$ and $\mathscr{T}_{\infty,P}^0$ are free of the same rank over Λ_P by Theorem 3.1. Thus, φ is an isomorphism and V_K is free of rank 2 over $\mathfrak{g}(N;K)$.

Let $\mathscr{K}$ be a primitive local ring of $\mathfrak{g}(N;K)$ and put $L=\mathscr{T}_\infty^0\otimes_\Lambda\Lambda_K$ as a submodule of V_K. Then L is a Λ_K-lattice in V_K stable under $\mathfrak{h}^0(N;\mathcal{O}_K)$ and $\mathfrak{G}$. By Lemma 8.1, we can identify V_K with $\mathfrak{g}(N;K)^2$, and we put

$$L'(\mathscr{K})=L\cap\mathscr{K}^2\subset V_K.$$

Then $L'(\mathscr{K})$ is a Λ_K-lattice in $\mathscr{K}^2$ stable under the Galois action. Let $L(\mathscr{K})$ be the natural image of $L'(\mathscr{K})\otimes_{\mathfrak{h}(\mathscr{K})}\mathscr{I}(\mathscr{K})$ in $\mathscr{K}^2$. Then $L(\mathscr{K})$ may be regarded as an $\mathcal{I}(\mathcal{K})$-lattice in $\mathcal{K}^2$ stable under the Galois action. Let π be the representation of $\mathfrak{G}$ on $L(\mathcal{K})$. By construction, π is continuous in the sense of §2. To see that π satisfies the required properties of Theorem 2.1, we fix a topological generator u of Γ and put $\omega_r = \iota(u^{p^r}) - 1 \in \Lambda$ for the tautological character ι: $\Gamma \to \Lambda$. Then $\Lambda/\omega_r\Lambda$ is naturally isomorphic to the group algebra $\mathbf{Z}_p[\Gamma/\Gamma_r]$. From Theorem 3.1, we know that

$$\mathcal{T}_\infty^0/\omega_r\mathcal{T}_\infty^0 \simeq e\mathcal{T}_r = e(\varprojlim_m J_r[p^m]).$$

Let λ: $\mathscr{h}^0(N;\mathbf{Z}_p) \to \Omega$ be a homomorphism of $\mathcal{O}_K$-algebras associated with an ordinary form $f \in S_2(\Gamma_0(Np^r), \varepsilon\psi\omega^{-2})$ of weight 2 belonging to $\mathcal{K}$. Thus, if $f = \sum_{n=1}^{\infty} a(n,f)q^n$, then $\lambda(T(n)) = a(n,f)$. Write $P_f = \mathrm{Ker}(\lambda)$, and put $F = (\mathscr{h}^0(N;\mathbf{Z}_p)/P_f) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. Then by Corollaries 1.3 and 1.4, F is naturally an algebra direct summand of $\mathscr{h}_2^0(\Gamma_1(Np^r);\mathbf{Q}_p)$. Let A_f be the quotient abelian variety of J_r attached to f, which is constructed in [21, Th. 1]. Let $V(A_f) = (\varprojlim_m A_f[p^m]) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. Write $\mathscr{h}$ for $\mathscr{h}_2^0(\Gamma_1(Np^r);\mathbf{Z}_p)$. Then, F, $e\mathcal{T}_r$ and $V(A_f)$ are naturally $\mathscr{h}$-modules, and by construction, $V_f = e\mathcal{T}_r \otimes_{\mathscr{h}} F$ is a direct summand of $V(A_f)$ as Galois modules. The space V_f is a vector space of dimension 2 over F. The Galois representation on V_f is unramified outside Np, and the characteristic polynomial for the Frobenius element σ_l for each prime l outside Np is given by

$$1 - a(l,f)X + \varepsilon\psi\omega^{-2}(l)lX^2.$$

This follows from [21, Th. 1]. Especially $\pi \bmod P_f$ coincides with $\pi(f)$ as in (2.1), since $\pi(f)$ is simple [18, Th. 2.3]. By Corollary 1.5, we can consider λ as a morphism of $\mathcal{I}(\mathcal{K})$ into Ω. Then, by definition, we have an isomorphism of Galois modules:

$$L(\mathcal{K}) \otimes_{\mathcal{I}(\mathcal{K})} \Omega \simeq V_f \otimes_F \Omega,$$

where we have regarded Ω as an $\mathcal{I}(\mathcal{K})$-module through λ. Write $P_f = \mathrm{Ker}(\lambda) \subset \mathcal{I}(\mathcal{K})$ and $\det(1 - \pi(\sigma_l)X) = 1 - A(l)X + B(l)X^2$ for $A(l)$ and $B(l)$ in $\mathcal{I}(\mathcal{K})$. Since $\pi \bmod P_f$ is isomorphic to $\pi(f)$,

$$A(l) \equiv a(l,f) \bmod P_f \quad \text{and} \quad B(l) \equiv \varepsilon\psi\omega^{-2}(l) \bmod P_f.$$

The set of points of the form P_f for ordinary forms of weight 2 in $\mathrm{Spec}(\mathcal{I}(\mathcal{K}))(\Omega) \simeq \mathrm{Hom}_{\mathrm{alg}}(\mathcal{I}(\mathcal{K}), \Omega)$ is Zariski dense (i.e. infinitely many), and thus, $A(l)$ (resp. $B(l)$) must be the projection of $T(l)$ (resp. $lT(l,l)$) in $\mathcal{K}$. Thus, for each ordinary form $f \in S_k(\Gamma_0(Np^r), \varepsilon\psi\omega^{-k})$ belonging to $\mathcal{K}$, the characteristic polynomial of $\pi \bmod P_f$ for σ_l is given by

$$1 - a(l,f)X + \varepsilon\psi\omega^{-k}(l)l^{k-1}X^2.$$

Thus $\pi \bmod P_f$ is isomorphic to $\pi(f)$. Since $\pi(f)$ is simple, π is also simple. This finishes the proof of Theorem 2.1.

§9. Structure of $J_\infty^0[p^\infty]$ as $\mathscr{h}^0(N;\mathbf{Z}_p)$-module

Let R be a local ring of $\mathscr{h}^0(N;\mathbf{Z}_p)$ with the idempotent $1_R\in\mathscr{h}^0(N;\mathbf{Z}_p)$. Put $J_r(R)=1_R(J_r^0[p^\infty])$ for each $r=1,2,\dots,\infty$. Define an integer a with $0\leqq a<p-1$ so that $\zeta\in\mu$ acts on R via the character: $\zeta\mapsto\zeta^a$. We shall give exact structure theorems of $J_r(R)$ as R-module by assuming one of the following conditions on R:

(9.1 a) a and $p-1$ have a non-trivial common divisor, and $a\neq 2$;

(9.1 b) $R\simeq\mathrm{Hom}_\Lambda(R,\Lambda)$ as R-modules.

Condition (9.1 b) is equivalent to

(9.1 c) There is a prime divisor P of Λ such that

$$R/PR\simeq\mathrm{Hom}_{\Lambda/P\Lambda}(R/PR,\Lambda/P\Lambda).$$

As a byproduct, we can prove the flatness of R over Λ without using the result of [13]. As already mentioned, the natural action of $\mathbf{Z}_p^\times$ on $J_r[p^\infty]$ is different from the action induced by the $\mathbf{Z}_p[[\mathbf{Z}_p^\times]]$-algebra structure of $\mathscr{h}^0(N;\mathbf{Z}_p)$ and is obtained by twisting the latter by the character: $z\mapsto z^2$. Thus, μ acts on $J_r(R)$ through the character: $\zeta\mapsto\zeta^{a-2}$, which is non-trivial if $a\neq 2$. By Theorem 3.1, $J_\infty(R)$ is Λ-cofree and $J_r(R)\simeq J_\infty(R)[\omega_r]$ for $\omega_r=\iota(u^{p^{r-1}})-1\in\Lambda$. Especially, $J_r(R)$ is always p-divisible. Let δ be the greatest common divisor of a and $p-1$, and let ζ_r be a primitive p^r-th root of unity in Ω, and let K_r be the unique subfield of $\mathbf{Q}_p(\zeta_r)$ with $[K_r:\mathbf{Q}_p]=p^{r-1}(p-1)/\delta$. We denote by $\mathcal{O}_r$ for the ring of p-adic integers in K_r and by $\mathfrak{p}_r$ its maximal ideal.

We say that a p-divisible group G over $\mathcal{O}_r$ is of *multiplicative* type if its Cartier dual is etale over $\mathcal{O}_r$ and is *ordinary* if for every geometric point s of $\mathrm{Spec}(\mathcal{O}_r)$, its fibre at s is a product of multiplicative ones and etale ones.

Lemma 9. (Langlands). *Suppose that $a\neq 2$. Then the p-divisible subgroup $J_r(R)/\mathbf{Q}$ of $J_r/\mathbf{Q}$ is contained in an abelian subvariety A_r defined over $\mathbf{Q}$ of J_r such that*

(i) A_r has good reduction over $\mathcal{O}_r$;

(ii) A_r is stable under the Hecke operator $T(p)$

(iii) Let $\mathcal{A}_r/\mathcal{O}_r$ be the Neron model of A_r over $\mathcal{O}_r$ and $\mathcal{A}_r[p^\infty]$ be the p-divisible group associated with $\mathcal{A}_r/\mathcal{O}_r$. Then $e(\mathcal{A}_r[p^\infty])$ is ordinary.

Proof. Let f be a primitive form in $S_2(\Gamma_1(Np^r))$ (but it does not necessarily mean that f is a new form of level Np^r). Let $C(f)$ be the smallest possible level of f (thus, f is a new form of level $C(f)$). Let A_f be the abelian subvariety of $J_1(C(f))$ attached to f ([25, Th. 7.14]). For divisors t of $Np^r/C(f)$, the morphism: $z\mapsto tz$ on $\mathfrak{H}$ induces a morphism of abelian varieties $[t]$: $J_1(C(f))\to J_r$. Let $A_f|[t]$ denote the image of A_f in J_r under $[t]$. By definition, $J_r(R)$ is covered by $\sum_f\sum_t A_f|[t]$ for some primitive forms f and integers t. Let Φ be the minimal set of primitive forms such that

$$J_r(R)\subset\sum_{f\in\Phi}\sum_t A_f|[t] \text{ in } J_r.$$

Since $J_r(R)$ belongs to the ordinary part of $J_r[p^\infty]$, we may assume that $|a(p,f)|_p=1$ if $f\in\Phi$, by replacing f by its conjugate under Galois action if necessary. Let π be the cuspidal automorphic representation of $\mathrm{GL}_2(\mathbf{A})$ associated with $f\in\Phi$, and decompose $\pi=\bigotimes_l \pi_l$ as a restricted tensor product of local representations. Since $a(p,f)\neq 0$, π_p must be principal or special. If π_p is special and f is ordinary, then μ acts trivially on f (e.g. [12, Lemma 3.2]). This case is eliminated by the assumption: $a\neq 2$. Thus π_p is principal and corresponds to two quasi characters λ and μ of $\mathbf{Q}_p^\times$, one of which is unramified. By local class field theory, we can consider λ and μ as characters of $\mathrm{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)$. Then the restriction of λ and μ to $\mathrm{Gal}(\bar{\mathbf{Q}}_p/K_r)$ becomes unramified over K_r, since the restriction of $\lambda\cdot\mu$ to $\mathbf{Z}_p^\times$ coincides with the p-part of the character of f which is unramified over K_r. Then, by virtue of a result of Langlands [15, Th. 7.1 and 7.5].

(9.2) *The l-adic representation on $A_f[l^\infty]$ $(f\in\Phi)$ for each prime l outside p is unramified at $\mathfrak{p}_r$ over K_r.*

Let $T^*(p)$ be the adjoint operator of $T(p)$ in $S_k(\Gamma_1(C(f)))$ under the Petersson inner product. Since f is primitive, A_f is stable under $T(p)$ and $T^*(p)$. Then, again by the result of Langlands, the characteristic polynomial of the Frobenius element in $\mathrm{Gal}(\bar{\mathbf{Q}}_p/K_r)$ is given by

$$X^2-(T(p)+T^*(p)\circ[\sigma])X+p\cdot[\sigma]$$

over the Hecke algebra in $\mathrm{End}(A_f)$. On the other hand, by [12, Prop. 4.4], we know that

$$J_r(R)\subset\sum_{f\in\Phi}\sum_{\substack{0<t\mid Np^r/C(f)\\(t,p)=1}} A_f|[t]=A.$$

By the criterion of Néron-Ogg-Schafarevich ([19, Th. 2.1]), (9.2) shows that A_f has good reduction over $\mathcal{O}_r$ and by the above characteristic polynomial, $e(A_f[p^\infty])$ is ordinary (cf. [10, Prop. 4.4]). Note that $T(p)$, e and $[t]$ for t prime to p are commutative and induce $\mathbf{Q}$-rational maps on A_f. Moreover A is isogeneous to a product of A_f over $\mathbf{Q}$. Thus A has good reduction over $\mathcal{O}_r$ and $eA[p^\infty]$ is ordinary.

By Lemma 9.1, $A_r[p^\infty]$ has a structure of p-divisible group over $\mathcal{O}_r$ (in the sense of Tate [27]) if $a\neq 2$, and $J_r(R)$ becomes also *a* p-divisible group over $\mathcal{O}_r$ as a director factor of $A_r[p^\infty]$.

Corollary 9.2. *Assume that $a\neq 2$. Then $J_r(R)/\mathcal{O}_r$ is ordinary.*

This is clear from the assertion (iii) of Lemma 9.1 and the definition of the ordinary part of $J_r[p^\infty]$.

Let $C_r(R)/\mathcal{O}_r$ (resp. $E_r(R)/\mathcal{O}_r$) be the connected component (resp. the maximal étale quotient) of the p-divisible group $J_r(R)/\mathcal{O}_r$. The modules $C_r(R)$ and $E_r(R)$ are naturally R-modules. The inclusion map: $J_s(R)\to J_r(R)$ for $r>s>0$ induces natural morphisms:

$$C_s(R)\to C_r(R)\quad\text{and}\quad E_s(R)\to E_r(R).$$

Put

$$C_\infty(R) = \varinjlim_r C_r(R) \quad \text{and} \quad E_\infty(R) = \varinjlim_r E_r(R).$$

Then, we have an exact sequence of R-modules:

$$0 \to C_r(R) \to J_r(R) \to E_r(R) \to 0 \qquad \text{for each } r = 1, 2, \ldots, \infty.$$

Theorem 9.3. *Assume* (9.1 a). *Then we have natural isomorphisms:*

$$C_\infty(R)^{\Gamma_r} \simeq C_r(R) \quad \text{and} \quad E_\infty(R)^{\Gamma_r} \simeq E_r(R) \qquad \text{for each } r > 1$$

and as R-modules.

$$C_r(R) \simeq (R/\omega_{2,r}R) \otimes_{\mathbf{Z}_p} \mathbf{T}_p, \qquad E_r(R) \simeq \mathrm{Hom}_{\mathbf{Z}_p}(R/\omega_{2,r}R, \mathbf{T}_p)$$

$$C_\infty(R) \simeq R \otimes_\Lambda \mathrm{Hom}_{\mathbf{Z}_p}(\Lambda, \mathbf{T}_p), \qquad E_\infty(R) \simeq \mathrm{Hom}_{\mathbf{Z}_p}(R, \mathbf{T}_p),$$

where $\omega_{2,r} = \iota(u^{p^{r-1}}) - u^{2p^{r-1}} = \prod_\varepsilon P_{2,\varepsilon}$ *over all character* ε: $\Gamma/\Gamma_r \to \Omega$. *Furthermore, we have that as R-modules*

$$J_r(R) \simeq C_r(R) \oplus E_r(R) \qquad \textit{for each } r = 1, 2, \ldots, \infty\,^{*}.$$

Proof. For each pair of integers (r, s) with $s > r > 0$, we have a commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & C_r(R) \arrow[r] \arrow[d, "\alpha"] & J_r(R) \arrow[r] \arrow[d, "\beta", "\wr"'] & E_r(R) \arrow[r] \arrow[d, "\gamma"] & 0 & \text{(exact)} \\
0 \arrow[r] & C_s(R)^{\Gamma_r} \arrow[r] & J_s(R)^{\Gamma_r} \arrow[r] & E_s(R)^{\Gamma_r} & & \text{(exact)}
\end{tikzcd}$$

By definition, α is injective, and by virtue of a result in Mazur and Wiles [16, Chap. 0], γ is injective, since $J_r(R)$ is ordinary and the ramification index of K_r over $\mathbf{Q}_p$ is not divisible by $p-1$. Then, by the snake lemma, we know that

$$C_s(R)^{\Gamma_r} \simeq C_r(R).$$

Thus, we also have that $C_\infty(R)^{\Gamma_r} \simeq C_r(R)$, and thus $C_\infty(R)^{\Gamma_r}$ is p-divisible. Let $\tau = \begin{pmatrix} 0 & -1 \\ Np^r & 0 \end{pmatrix}$, and we denote by the same symbol τ the automorphism of J_r induced by this matrix. Note that τ, as an automorphism of J_r, is defined over maximal real subfield of the cyclotomic field of Np^r-th roots of unity, and also we have the relations:

$$T^*(p) = \tau \circ T(p) \circ \tau^{-1} \quad \text{and} \quad \tau^2 = 1.$$

Let e^* be the idempotent in $\mathrm{End}(J_r) \otimes_{\mathbf{Z}} \mathbf{Z}_p$ attached to $T^*(p)$. Then, we know that $e^* = \tau \circ e \circ \tau^{-1}$. Thus, $J_r(R)[p^m]$ and $\tau(J_r(R))[p^m]$ are mutually dual under

---

[*] This fact has been also proven by Mazur and Wiles in their preprint: On p-adic analytic families of Galois representations (§8, Prop. 2)

the Weil pairing for the canonical divisor of the jacobian $J_r/\mathbf{Q}$, and therefore, $C_r(R)[p^m]$ is dual to $\tau(E_r(R))[p^m]$ for each $m>0$ (see the proof of [11, Prop. 3.1]). This shows that $\mathrm{corank}_{\mathbf{Z}_p}(C_r(R))=\mathrm{corank}_{\mathbf{Z}_p}(E_r(R))$. Let $2t$ denote the corank of $J_\infty(R)$ over Λ. Then we know that

$$J_r(R)=J_\infty(R)^{\Gamma_r}\simeq \mathrm{Hom}(\mathbf{Z}_p[\Gamma/\Gamma_r],\mathbf{T}_p)^{2t} \text{ as } \Lambda\text{-module}$$

and $\mathrm{corank}_{\mathbf{Z}_p} C_r(R)=t[\Gamma:\Gamma_r]$. Let $C_r^*(R)=\mathrm{Hom}(C_r(R),\mathbf{T}_p)$ for each $r=1,2,\dots,\infty$. Then, we have already shown that

$$C_\infty^*(R)/\omega_1 C_\infty^*(R)\simeq C_1^*(R)\simeq \mathbf{Z}_p^t.$$

Thus, there is a surjective morphism: $\Lambda^t\to C_\infty^*(R)$ of Λ-modules. For each $r\geqq 1$, this morphism induces a surjection: $(\Lambda/\omega_r\Lambda)^t\to C_r^*(R)$, but the both sides are $\mathbf{Z}_p$-free of the same rank; thus, $(\Lambda/\omega_r\Lambda)^t\simeq C_r^*(R)$ for all $r\geqq 1$. This shows that $C_\infty^*(R)$ is Λ-free of rank t, $C_\infty(R)$ is Λ-injective and the exact sequence:

$$0\to C_\infty(R)\to J_\infty(R)\to E_\infty(R)\to 0$$

splits as Λ-modules. Hence $E_\infty(R)$ is also Λ-injective, and especially, $E_\infty(R)^{\Gamma_r}$ is p-divisible. The corank of $E_\infty(R)^{\Gamma_r}$ and $E_r(R)$ over $\mathbf{Z}_p$ are equal to $t[\Gamma:\Gamma_r]$ and $E_r(R)$ is injected into $E_\infty(R)^{\Gamma_r}$. This shows that $E_\infty(R)^{\Gamma_r}\simeq E_r(R)$.

Let $E_r^*(R)$ denote the Pontryagin dual module of $E_r(R)$ for each $r=1,2,\dots,\infty$. Then we know that $E_r^*(R)\simeq E_\infty^*(R)/\omega_r E_\infty^*(R)$ for each finite $r\geqq 1$. It is known by [11, Prop. 3.1] that

$$E_1^*(R)\simeq R/\omega_{2,1}R \text{ as } R\text{-modules.}$$

Let $\bar{x}\in E_1^*(R)$ be the element corresponding to the identity of R, and take $x\in E_\infty^*(R)$ so that $x \bmod \omega_1 E_\infty^*(R)=\bar{x}$. Then, we can define a morphism φ of R-modules: $R\to E_\infty^*(R)$ by $r\to r\cdot x$ for $r\in R$. By construction, φ is surjective (to define φ and show the surjectivity of φ, we have used [13, Cor. 3.2] implicitly, but we can do this without [13, Cor. 3.2] as follows: Anyway, $h_2^0(\Gamma_1(Np);\mathbf{Z}_p)$ is a residue ring of $h^0(N;\mathbf{Z}_p)$. Since $E_1^*(R)$ is non-trivial, the image R_0 of R in $h_2^0(\Gamma_1(Np);\mathbf{Z}_p)$ is a non-trivial local factor. By [11, Prop. 3.1], $E_1^*(R)\simeq R_0$, and by taking $x\in E_\infty^*(R)$ so that the image of x in $E_1^*(R)$ gives the identity of R_0, we can define surjective φ as above). Since R acts on $E_\infty^*(R)$ faithfully by Lemma 6.4, φ must be injective (if one admits the flatness of R over Λ, the injectivity of φ is obvious, since R and $E_\infty^*(R)$ are Λ-free of the same rank). Thus we have that as R-modules

$$E_\infty^*(R)\simeq R \quad\text{and}\quad E_\infty(R)\simeq \mathrm{Hom}(R,\mathbf{T}_p),$$

and we get a new proof of the fact that R is flat over Λ. By [11, Prop. 3.1], we have that $C_1(R)\simeq(R/\omega_{2,1}R)\otimes_{\mathbf{Z}_p}\mathbf{T}_p$ as R-modules, and thus

$$C_1^*(R)\simeq \mathrm{Hom}_{\mathbf{Z}_p}(R/\omega_{2,1}R,\mathbf{Z}_p).$$

Put $M=\mathrm{Hom}_\Lambda(C_\infty^*(R),\Lambda)$. Then, M is Λ-free, since $C_\infty^*(R)$ is Λ-free. Furthermore, we have that

$$M/\omega_1 M\simeq \mathrm{Hom}_{\mathbf{Z}_p}(C_1^*(R),\mathbf{Z}_p)\simeq R/\omega_{2,1}R.$$

The same argument as above shows that $M \simeq R$ as R-modules. This shows that

$$C^*_\infty(R) \simeq \mathrm{Hom}_\Lambda(R, \Lambda), \qquad C_\infty(R) \simeq \mathrm{Hom}(\mathrm{Hom}_\Lambda(R, \Lambda), \mathbf{T}_p) \simeq R \otimes_\Lambda \mathrm{Hom}(\Lambda, \mathbf{T}_p)$$

and

$$C_r(R) \simeq R/\omega_{2,r} R \otimes_{\mathbf{Z}_p} \mathbf{T}_p.$$

Finally, we shall prove the splitting of exact sequence of R-modules:

$$0 \to C_r(R)/\mathcal{O}_r \to J_r(R)/\mathcal{O}_r \to E_r(R)/\mathcal{O}_r \to 0.$$

The inertia group I over K_r acts trivially on $E_r(R)$ and on $C_r(R)$ via a character λ: $I \to R$ since $C^*_\infty(R) \simeq \mathrm{Hom}_\Lambda(R, \Lambda)$. By the remark about $\det \pi$ after Theorem 2.1, we know that λ coincides with the restriction of $\omega^a \chi^{-1} \cdot \iota$ to I, where ω is the Teichmuller character regarded as a character of I, χ is the cyclotomic character and ι is the tautological character of Γ into Λ. If $\sigma \in I$ coincides on $\mathbf{Q}_p(\zeta_r)$ with the generator of $\mathrm{Gal}(\mathbf{Q}_p(\zeta_r)/K_r)$, we thus know from (9.1a) that $\lambda(\sigma)$ is congruent to a non-trivial $(p-1)$-th root of unity modulo the maximal ideal of R. Then, for each $m > 0$, we can find sufficiently large integer t so that the kernel of the operator $\sigma^{p^t} - 1$ on $J_r(R)[p^m]$ gives the splitting image of $E_r(R)[p^m]$, since $\sigma - 1$ annihilates $E_r(R)$ and coincides on $C_r(R)$ with an action of a unit of R. This finishes the proof.

Now we shall give a similar structure theorem of the R-module $J_r(R)$ by assuming (9.1b) instead of (9.1a). We consider the action of $\varepsilon = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ on $H^1_P(\Gamma_1(Np^r); \mathbf{T}_p) \simeq J_r[p^\infty]$ as defined in §4. As already mentioned in the proof of Lemma 6.4, ε commutes with the Hecke operators $T(n)$. Therefore, ε acts on the p-divisible group $J_r(R)$. Put

$$J_r^\pm(R) = \{v \in J_r(R) \,|\, v|\varepsilon = \pm v\}.$$

Since $p \geqq 5$, $J_r(R) = J_r^+(R) \oplus J_r^-(R)$. As is clear from the proof of Lemma 6.4, we know that

$$\mathrm{corank}_{\mathbf{Z}_p} J_r^+(R) = \mathrm{corank}_{\mathbf{Z}_p} J_r^-(R) = t[\Gamma : \Gamma_r].$$

Since the action of ε is compatible with the inclusion map: $J_s(R) \to J_r(R)$ for $r > s > 0$, we may take the injective limit: $J^\pm_\infty(R) = \varinjlim_r J_r^\pm(R)$. Evidently, we know that

$$\text{(9.3)} \qquad J_\infty(R) = J^+_\infty(R) \oplus J^-_\infty(R) \text{ as } R\text{-module, and } (J^\pm_\infty(R))^{\Gamma_r} \simeq J_r^\pm(R).$$

Especially, $J^\pm_\infty(R)$ is Λ-injective (of Λ-corank t). If μ acts on $J_\infty(R)$ non-trivially, then by [11, Prop. 3.1], there exist an exact sequence of R-modules:

$$0 \to R/\omega_{2,1} R \to \mathrm{Hom}_{\mathbf{Z}_p}(J_1(R), \mathbf{T}_p) \to \mathrm{Hom}(R/\omega_{2,1} R, \mathbf{Z}_p) \to 0.$$

By Assumption (9.1b), which is equivalent to (9.1c), $\mathrm{Hom}(R/\omega_{2,1} R, \mathbf{Z}_p)$ is $R/\omega_{2,1} R$-free, and hence this exact sequence splits. Namely, we have

$$\mathrm{Hom}_{\mathbf{Z}_p}(J_1(R), \mathbf{T}_p) \simeq (R/\omega_{2,1} R)^2 \quad \text{and} \quad J_1(R) \simeq \mathrm{Hom}(R/\omega_{2,1} R, \mathbf{T}_p)^2.$$

Since $R/\omega_{2,1}R$ is an indecomposable R-module, we know from the theorem of Krull-Schmidt ([3, 14.5])

$$\mathrm{Hom}_{\mathbf{Z}_p}(J_1^{\pm}(R), \mathbf{T}_p) \simeq R/\omega_{2,1}R \text{ as } R\text{-modules.}$$

This combined with (9.3) show that

$$J_\infty^{\pm}(R) \simeq \mathrm{Hom}(R, \mathbf{T}_p).$$

Thus we obtain

Theorem 9.4. *Assume one of the equivalent conditions* (9.1 b, c) *and that* μ *acts on* $J_\infty(R)$ *non-trivially* (i.e. $a \neq 2$). *Then, the Pontryagin dual module of* $J_\infty(R)$ *is free of rank* 2 *over* R.

§ 10. Special values of *L*-functions of GL(3)

Let f be a normalized eigenform in $S_k(\Gamma_0(Np^m), \psi)$ and f_0 be the primitive form associated with f. Let π be the automorphic representation of $\mathrm{GL}_2(\mathbf{A})$ associated with f_0, for the adeles $\mathbf{A}$ of $\mathbf{Q}$. Let $C(f)$ be the conductor of π (i.e. $C(f)$ is the smallest possible level of f_0). Decompose $\pi = \bigotimes_l \pi_l$ as a restricted tensor product of local representations over all places of $\mathbf{Q}$. The L-function of GL(2) associated with f_0 (or π) is defined by

$$L(s,f) = \sum_{n=1}^{\infty} a(n, f_0) n^{-s},$$

which has an Euler product expansion of the form:

$$L(s,f) = \prod_l [(1-\alpha_l l^{-s})(1-\beta_l l^{-s})]^{-1}$$

for suitable algebraic numbers α_l and β_l for each prime l. In the flame work of representation theory, one usually takes the "unitarization" $L(s,\pi) = L\left(s+\frac{k-1}{2}, f_0\right)$ instead of $L(s, f_0)$, but we prefer the classical form, because it is suited for p-adic theory. As defined in Gelbart and Jacquet [7, § 3], there is a canonical base change lifting of automorphic representations of GL(2) into those of GL(3). Let $\hat{\pi}$ be the lifted automorphic representation of GL(3) of π and put $D(s,f) = L(s-k+1, \hat{\pi})$. We recall here the explicit Euler factor of $D(s,f)$ according to [7, (1.3), (1.4), (3.1.1)]. Let η_l denote the unique unramified quadratic character of $\mathbf{Q}_l^\times$ for each prime l. Put

$$D(s,f) = \prod_l D_l(s,f) \tag{10.1}$$

with

$$D_l(s,f)=\begin{cases} 1 & \text{if } \pi_l \text{ is super cuspidal and } \pi_l\otimes\eta_l\not\simeq\pi_l, \\ (1+l^{k-1-s})^{-1} & \text{if } \pi_l \text{ is super cuspidal and } \pi_l\otimes\eta_l\simeq\pi_l, \\ [(1-l^{k-1-s})(1-\lambda\bar{\mu}(l)l^{k-1-s})(1-\bar{\lambda}\mu(l)l^{k-1-s})]^{-1} & \text{if } \pi_l \text{ is principal and} \\ \pi_l\simeq\pi(\lambda,\mu) \text{ for two quasi characters } \lambda \text{ and } \mu \text{ of } \mathbf{Q}_l^\times, & \\ (1-l^{k-2-s})^{-1} & \text{if } \pi_l \text{ is special,} \end{cases}$$

where we understand that $\bar{\lambda}\mu(l)=\lambda\bar{\mu}(l)=0$ if $\lambda\bar{\mu}$ is ramified.

Let ψ_0 be the primitive character modulo $C(\psi)$ which induces ψ modulo Np^m. If l is prime to $C(f)$, we have that

$$D_l(s,f)=[(1-\bar{\psi}_0(l)\alpha_l^2 l^{-s})(1-\bar{\psi}_0(l)\alpha_l\beta_l l^{-s})(1-\bar{\psi}_0(l)\beta_l^2 l^{-s})]^{-1}.$$

Now we define another (auxiliary) Dirichlet series by

$$(10.2)\quad \mathscr{D}(s,f)=\prod_l[(1-\bar{\psi}_0(l)\alpha_l^2 l^{-s})(1-\bar{\psi}_0(l)\alpha_l\beta_l l^{-s})(1-\bar{\psi}_0(l)\beta_l^2 l^{-s})]^{-1}.$$

For each Dirichlet character χ, the twist of f by χ is defined by

$$f|\chi=\sum_{n=1}^{\infty}\chi(n)a(n,f)q^n.$$

Evidently, $f|\chi$ is a normalized eigenform. The L-function $L(s,f)$ depends only on the primitive form f_0, and $D(s,f)$ depends only on the class of all twists of f_0, but $\mathscr{D}(s,f)$ depends on the choice of the normalized eigenform f.

Terminology. Assume that f is primitive. The form f is said to be *minimal* if $C(f|\chi)\geqq C(f)$ for all primitive Dirichlet character χ. Always in the class of twists of f, the minimal forms exist but they may be several.

Lemma 10.1. *Suppose that f is primitive and minimal. Then we have for each prime l:*

(i) *If π_l is special, then l divides $C(f)$ exactly once, the restriction of ψ to $(\mathbf{Z}/l\mathbf{Z})^\times$ is trivial, and $a(l,f)^2=\psi_0(l)l^{k-2}$.*

(ii) *π_l is principal if and only if l is prime to $C(f)/C(\psi)$.*

(iii) *If π_l is special or principal, then we have that*

$$D_l(s,f)=[(1-\bar{\psi}_0(l)\alpha_l^2 l^{-s})(1-\bar{\psi}_0(l)\alpha_l\beta_l l^{-s})(1-\bar{\psi}_0(l)\beta_l^2 l^{-s})]^{-1}.$$

(iv) *$D(s,f)=D(s,f|\chi)$ for any Dirichlet character χ.*

Proof. Assertions (iii) and (iv) are obvious from the definition and (i) and (ii). Firstly, we shall prove (i). If π_l is special, then $\pi_l\simeq\sigma(\lambda,\mu)$ with quasi characters λ and μ of $\mathbf{Q}_l^\times$ with $\lambda\mu^{-1}(x)=|x|_l$. Let $C(\pi_l)$ (resp. $C(\lambda)$) be the local conductor of π_l (resp. λ). Then it is known that $C(\pi)=C(\lambda)^2$ or l according as λ is ramified or not. Let χ be a Dirichlet character of l-power conductor whose restriction χ_l to $\mathbf{Z}_l^\times$ coincides with λ. Then, we know that

$$\pi_l\otimes\chi_l^{-1}\simeq\sigma(\lambda\chi_l^{-1},\mu\chi_l^{-1})\quad\text{and}\quad C(\pi_l\otimes\chi_l^{-1})=l.$$

Since f is minimal, this shows that λ must be unramified, and thus the assertion (i) follows. Then, we assume that π_l is principal, and $\pi_l \simeq \pi(\lambda, \mu)$. Then it is known that $C(\pi_l) = C(\lambda)\,C(\mu)$. Let χ be a Dirichlet character whose restriction χ_l to $\mathbf{Z}_p^\times$ coincides with λ. Then obviously, we have that

$$C(\pi_l \otimes \chi_l^{-1}) = C(\lambda \chi_l^{-1}) \leqq C(\chi_l)\,C(\mu) = C(\lambda)\,C(\mu) = C(\pi_l).$$

Thus the minimality of f at l is equivalent to the condition: $C(\pi_l) = C(\psi_l)$, where ψ_l is the l-part of ψ.

Corollary 10.2. *Let Σ be the set of primes l such that $\pi_l \otimes \eta_l \simeq \pi_l$ and π_l is supercuspidal* (then, if $l \in \Sigma$, l^2 divides Np^m). *If f is primitive and minimal, then we have*

$$D(s,f) = \prod_{l \in \Sigma} (1 + l^{k-1-s})^{-1}\, \mathcal{D}(s,f).$$

By a result of Shimura [22, Th. 2], $\mathcal{D}(s,f)$ is holomorphic at $s = k$ (in fact, by Gelbart and Jacquet [7, Th. 9.3, 3.7], $D(s,f)$ is holomorphic on the whole s-plane and satisfies a functional equation of the form: $2k-1-s \mapsto s$).

Here are some remarks about the criteria of the minimality: Let f be a primitive form, and let $\pi = \bigotimes_l \pi_l$ be the corresponding automorphic representation.

(i) For a prime factor l of $C(f)$, if the l-part of the character of f is primitive modulo the l-primary part of $C(f)$, the assertion (ii) of Lemma 10.1 (or its proof) implies that π_l is principal and f is minimal at l; namely, f has a minimal conductor in the class of twists of f by characters modulo *l-power*. In particular, each primitive form associated with a primitive local ring of $\mathfrak{h}(N; \mathcal{O}_K)$ is minimal at p. Thus $f_{k,\varepsilon}$ is *not* the twist of f_k by ε.

(ii) If the character of f is primitive modulo $C(f)$, f is then minimal by the first remark and the exceptional set Σ is empty. Thus the primitive function $D(s,f)$ coincides with $\mathcal{D}(s,f)$.

(iii) If $a(C(f),f) \neq 0$, then f is minimal and Σ is empty, and therefore $D(s,f) = \mathcal{D}(s,f)$.

This follows from Lemma 10.1 and the following facts for each prime factor l of $C(f)$ (cf. [2] and [12, Lemma 3.2]): (a) if π_l is special and minimal, then the l-part of the character ψ of f is trivial, $l \mid C(f)$ but $l^2 \nmid C(f)$, and $a(l,f)^2 = \psi_0(l)\, l^{k-2}$, where ψ_0 is the primitive character associated with ψ; (b) if π_l is principal and minimal, $|a(l,f)|^2 = l^{k-1}$; (c) if π_l is super-cuspidal or non-minimal, then $a(l,f) = 0$ and $l^2 \mid C(f)$. As a special case of this criterion, if the N-part (i.e. the prime to p part) of the character of a primitive local ring $\mathcal{K}$ of $\mathfrak{h}(N; K)$ is primitive modulo N (cf. Cor. 1.6), then every primitive form f associated with $\mathcal{K}$ is minimal, $\Sigma = \phi$ and $D(s,f) = \mathcal{D}(s,f)$.

Fix a primitive local ring $\mathcal{K}$ of $\mathfrak{h}(N; K)$ defined over K, and let ψ be the character of $\mathcal{K}$. Let $\varepsilon\colon \Gamma \to \bar{\mathbf{Q}}^\times$ be a finite order character of Γ with $\mathrm{Ker}(\varepsilon) = \Gamma_r$. For each integer $k \geqq 2$, let $\Psi(k, \varepsilon)$ be the set of the primitive forms associated with all ordinary forms in $S_k(\Gamma_0(Np^r), \varepsilon\psi\omega^{-k})$ belonging to $\mathcal{K}$. We write $\Psi = \Psi(k, \varepsilon)$ if no confusion is likely. We shall now define a canonical transcendental factor of the value of

$$Z(s,\Psi(k,\varepsilon))=\prod_{f\in\Psi(k,\varepsilon)}\mathscr{D}(s,f)\quad\text{at}\quad s=k.$$

Let K_0 be a finite extension of $\mathbf{Q}$ which contains every Fourier coefficient of all forms in Ψ. We may assume that K is the topological closure of K_0 in Ω (see the remark after Cor. 1.7). We suppose that

(10.3) *The conductors of all the elements in* $\Psi(k,\varepsilon)$ *are equal to an integer* C.

This condition is imposed because the semi-simple algebra: $F=(\mathscr{h}(K)/P_{k,\varepsilon}\mathscr{h}(K))\otimes_{\mathcal{O}_K}K$ may not be a field, and thus we do not know in general whether all the forms belonging to F have the same conductor or not (see the remark after Cor. 1.3).

This condition is verified (by Corollary 1.6 and the remark after that), when $k>2$ or the restriction of $\varepsilon\psi\omega^{-k}$ to $(\mathbf{Z}/p^r\mathbf{Z})^\times$ is non-trivial. We thus know that $C=Np^r$ if p divides C, and $C=N$ if C is prime to p. We now consider the parabolic cohomology group $H_P^1(\Gamma_1(C),L_n(\mathbf{C}))$ for $n=k-2$. Complex conjugation: $L_n(\mathbf{C})\to L_n(\mathbf{C})$ induces an automorphism of $H_P^1(\Gamma_1(C),L_n(\mathbf{C}))$, which we also call complex conjugation, and to denote it, we use the symbol "$-$". As seen in (5.1b), $S_k(\Gamma_1(C))$ can be considered as a subspace of $H_P^1(\Gamma_1(C),L_n(\mathbf{C}))$. Then we can identify

$$S_k(\Gamma_1(C))\oplus\bar{S}_k(\Gamma_1(C))\simeq H_P^1(\Gamma_1(C),L_n(\mathbf{C}))\qquad\text{for } n=k-2.$$

We write simply S for this space. If p divides C, let

$$S(\varepsilon)=S_k(\Phi_r^1,\varepsilon)\oplus\overline{S_k(\Phi_r^1,\bar{\varepsilon})}\subset S.$$

Then we have

$$S=\bigoplus_{\varepsilon}S(\varepsilon),\tag{10.4}$$

and $\Phi_r^1/\Gamma_1(Np^r)(\simeq\Gamma/\Gamma_r)$ acts on $S(\varepsilon)$ through the character ε. When C is prime to p, then ε is trivial and we understand that $S(\varepsilon)$ and S are the same. Naturally, $\mathscr{h}_k(\Phi_r^1,\varepsilon;\mathbf{C})$ (or $\mathscr{h}_k(\Gamma_1(N);\mathbf{C})$ if C is prime to p) acts on $S(\varepsilon)$. On the other hand, we can decompose $\mathscr{h}_k(\Phi_r^1,\varepsilon;K)=F\oplus A$ according to the decomposition of $\mathscr{q}(N;K)=\mathscr{K}\oplus\mathscr{A}$ (i.e. $F=(\mathscr{h}(\mathscr{K})/P_{k,\varepsilon}\mathscr{h}(\mathscr{K}))\otimes_{\mathcal{O}_K}K$). If C is prime to p, the idempotent e induces an isomorphism: $\mathscr{h}_k^0(\Phi_1^0;\mathcal{O}_K)\simeq e_0\mathscr{h}_k(\Gamma_1(N);\mathcal{O}_K)$, where e_0 is the idempotent attached to $T(p)$ on $S_k(\Gamma_1(N))$. Thus we can also decompose $\mathscr{h}_k(\Gamma_1(N);K)=F\oplus A$ as above. Put

$$S(F)=\sum_{\varphi\in F}\varphi(S(\varepsilon))\quad\text{and}\quad S(A)=\sum_{\alpha\in A}\alpha(S(\varepsilon)).$$

Then we have

$$S(\varepsilon)=S(F)\oplus S(A),\quad\text{and}\quad S(F)=\sum_{f\in\Psi}(\mathbf{C}f+\mathbf{C}\bar{f}_\rho),\tag{10.5}$$

where $f_\rho(z)=\overline{f(-\bar{z})}=\sum_{n=0}^{\infty}\overline{a(n)}\,q^n$ for $f=\sum_{n=0}^{\infty}a(n)q^n$. Let π_F: $S(\varepsilon)\to S(F)$ (resp. π_ε: $S\to S(\varepsilon)$) be the projection according to the decomposition (10.5) (resp. (10.4)).

Let $\mathcal{O}_{K_0}=\mathcal{O}_K\cap K_0$, and define L by the natural image of $H^1_P(\Gamma_1(C), L_n(\mathcal{O}_{K_0}))$ in S. Then, we know from [25, Prop. 8.6] that $S=L\otimes_{\mathcal{O}_{K_0}}\mathbf{C}$, and thus L is a $\mathcal{O}_{K_0}$-lattice in S. Put

(10.6) $L_{\varepsilon,F}=L\cap S(F)$, $\quad L^F_\varepsilon=\pi_F(L\cap S(\varepsilon))$, $\quad L^\varepsilon_F=\pi_\varepsilon(L)\cap S(F)$, $\quad L^{\varepsilon,F}=\pi_F(\pi_\varepsilon(L))$.

Then, we have that $L^F_\varepsilon\supset L_{\varepsilon,F}$ and $L^{\varepsilon,F}\supset L^\varepsilon_F$, and they are all $\mathcal{O}_{K_0}$-lattice in $S(F)$. Now we shall define a pairing on S by (10.7a)

$$(10.7\text{a})\qquad \langle f,g\rangle=2^{n+1}(-\sqrt{-1})^{n-1}\int_{\Gamma_1(C)\backslash\mathfrak{H}}\overline{f(z)}\,g(z)\,y^n\,dx\,dy\qquad(n=k-2).$$

Then, it was shown in [20, §4] and [23, Prop. 4.2] (see also [9, §2] for integrality) that

$$(10.7\text{b})\qquad \langle L,L\rangle\subset\mathcal{O}_{K_0},\quad \langle L^F_\varepsilon,\overline{L^\varepsilon_F}\rangle\subset\mathcal{O}_{K_0},\quad \langle L_{\varepsilon,F},\overline{L^{\varepsilon,F}}\rangle\subset\mathcal{O}_{K_0}.$$

By construction, $S(\varepsilon)$ and $S(\bar\varepsilon)(=\overline{S(\varepsilon)})$ (resp. $S(F)$ and $\bar S(F)$) are mutually dual (over $\mathbf{C}$) under this pairing, and $S(F)$ and $\bar S(A)$ (resp. $S(F)$ and $S(A)$) are orthogonal. Let d be the degree of K over $\mathcal{L}_K$; so, Ψ has d-elements. Consider $\omega=(f,f_\rho)_{f\in\Psi}$ as a row vector of the elements of $S(F)$. Take $\mathcal{O}_{K_0}$-basis $\delta_1,\dots,\delta_{2d}$ of $L_{\varepsilon,F}$ and $\delta'_1,\dots,\delta'_{2d}$ of L^ε_F, and put

$$\delta=(\delta_1,\dots,\delta_{2d})\quad\text{and}\quad\delta'=(\delta'_1,\dots,\delta'_{2d})$$

as row-vectors. Define matrices X^F and X_F in $\mathrm{GL}_{2d}(\mathbf{C})$ by $\delta\cdot X_F=\omega$ and $\delta'\cdot X^F=\omega$, and put

$$(10.8\text{a})\qquad U_F=\det(X_F)\quad\text{and}\quad U^F=\det(X^F),$$

$$(10.8\text{b})\qquad U_\infty(k,\varepsilon)=\pi^{d(k+1)}(U_F\overline{U^F})^{\frac{1}{2}}\cdot\{(k-1)!\,C\cdot C(\varepsilon\psi\omega^{-k})\,\varphi(C/C(\varepsilon\psi\omega^{-k}))\}^{-d},$$

where $C(\varepsilon\psi\omega^{-k})$ denotes the conductor of $\varepsilon\psi\omega^{-k}$ and φ is the Euler function. An algebraicity theorem for the value $\mathcal{D}(m,f)$ was proved by Sturm [26]. Here, we give a version of it for the values $\mathcal{D}(k,f)$:

Proposition 10.3. *The number $U_\infty(k,\varepsilon)$ is determined up to the multiple of p-adic units in $\bar{\mathbf{Q}}$, and we have that*

$$0\neq(Z(k,\Psi(k,\varepsilon))/U_\infty(k,\varepsilon))^2\in\mathcal{O}_{K_0}.$$

Moreover, if the pairing $\langle\ ,\ \rangle$ induces an isomorphism:

$$L^\varepsilon_F\simeq\mathrm{Hom}_{\mathcal{O}_{K_0}}(\overline{L^F_\varepsilon},\mathcal{O}_{K_0}),$$

Then we have the formula:

$$|Z(k,\Psi(k,\varepsilon))/U_\infty(k,\varepsilon)|_p^{-2[K:\mathbf{Q}_p]}=[L^F_\varepsilon:L_{\varepsilon,F}].$$

Proof. Write $\Psi=\{f_1,f_2,\dots,f_d\}$ and put

$$\omega_i(\text{resp. }\omega'_i)=\begin{cases}f_i(\text{resp. }f_i^\rho) & \text{if } 1\leqq i\leqq d,\\ \overline{f^\rho_{i-d}}(\text{resp. }\overline{f_{i-d}}) & \text{if } d<i\leqq 2d.\end{cases}$$

Then we have that

$$(\delta_1,\dots,\delta_{2d})\cdot X_F=(\omega_1,\dots,\omega_{2d}) \quad \text{and} \quad (\overline{\delta'_1},\dots,\overline{\delta'_{2d}})\cdot X^F=(\omega'_1,\dots,\omega'_{2d}).$$

Thus, we see that

$$\begin{aligned}\mathcal{O}_{K_0}\ni\det(\langle\delta_i,\delta'_j\rangle)_{1\leqq i,j\leqq 2d}&=(U_F\overline{U^F})^{-1}\det(\langle\omega_i,\omega'_j\rangle)\\&=-(U_F\overline{U^F})^{-1}2^{2(n+1)d}\prod_{f\in\Psi}(f,f)^2,\end{aligned}$$

where $(f,f)=\int_{\Gamma_1(C)\backslash\mathfrak{H}}|f|^2y^{k-2}\,dx\,dy$. Then, [9, Th. 5.1] shows the first assertion. Now we shall prove the second. By the assumption, we can choose a basis $\{\delta_i^*\}$ of L_ε^F so that

$$\langle\delta_i^*,\overline{\delta'_j}\rangle=\delta_{ij} \quad \text{for the Kronecker symbol } \delta_{ij}.$$

Then, there exists an invertible matrix $\alpha\in M_{2d}(\mathcal{O}_{K_0})$ such that

$$(\delta_1^*,\dots,\delta_{2d}^*)\cdot\alpha=(\delta_1,\dots,\delta_{2d}).$$

Then we have that

$$\det(\langle\delta_i,\overline{\delta'_j}\rangle)=\det(\alpha) \quad \text{and} \quad |\det(\alpha)|_p^{-[K:\mathbf{Q}_p]}=[L_\varepsilon^F:L_{\varepsilon,F}].$$

Proposition 10.4. *If the restriction of* $\varepsilon\psi\omega^{-k}$ *to* $(\mathbf{Z}/p^r\mathbf{Z})^\times$ *is trivial or if* $k=2$, *then* $\langle\ ,\ \rangle$ *induces isomorphisms:*

$$L_{\varepsilon,F}\simeq\operatorname{Hom}_{\mathcal{O}_{K_0}}(\overline{L^{\varepsilon,F}},\mathcal{O}_{K_0}) \quad \text{and} \quad L_\varepsilon^F\simeq\operatorname{Hom}_{\mathcal{O}_{K_0}}(\overline{L_F^\varepsilon},\mathcal{O}_{K_0}).$$

Especially, we have that

$$L_\varepsilon^F/L_{\varepsilon,F}\simeq L^{\varepsilon,F}/L_F^\varepsilon \quad \textit{as } \mathbf{Z}\textit{-modules}.$$

Proof. When $k=2$, it is well known that L is a self dual $\mathcal{O}_{K_0}$-lattice under $\langle\ ,\ \rangle$. Then the assertions are obvious from the definition (10.6); so, we assume that $\varepsilon\psi\omega^{-k}|_{(\mathbf{Z}/p^r\mathbf{Z})^\times}$ is trivial and $k>2$. This implies that $C=N$. Since

$$\mathscr{h}_k(\Gamma_1(N);\Omega)=\mathscr{h}_k(\Gamma_1(N);K)\otimes_K\Omega=\mathscr{h}_k(\Gamma_1(N);\bar{\mathbf{Q}})\otimes_{\bar{\mathbf{Q}}}\Omega,$$

every idempotent in $\mathscr{h}_k(\Gamma_1(N);K)$ is actually contained in $\mathscr{h}_k(\Gamma_1(N);\bar{\mathbf{Q}})$. By replacing K_0 by its finite extension if necessary, we may thus assume that the idempotent e_0 attached to $T(p)$ of level N is contained in $\mathscr{h}_k(\Gamma_1(N);\mathcal{O}_{K_0})$. Put $L^0=e_0L$. On $S_k(\Gamma_1(N))$, the adjoint operator of $T(p)$ under $\langle\ ,\ \rangle$ is given by $T(p)\circ[\sigma]$ for $\sigma\in\Gamma_0(N)$ such that $\sigma\equiv\begin{pmatrix}* & *\\0 & p\end{pmatrix}\bmod N$. Thus e_0 is self adjoint. Especially, $\langle\ ,\ \rangle$ induces a perfect pairing on $L^0\otimes_{\mathcal{O}_{K_0}}K_0$. If $\langle\,,\rangle$ is perfect on L^0 over $\mathcal{O}_{K_0}$, the assertions are obvious from the definition (10.6). Note that

$$L^0\otimes_{\mathcal{O}_{K_0}}\mathcal{O}_K\simeq e_0H_P^1(\Gamma_1(N),L_n(\mathcal{O}_K))\simeq(e_0H_P^1(\Gamma_1(N),L_n(\mathbf{Z}_p)))\otimes_{\mathbf{Z}_p}\mathcal{O}_K.$$

Thus, what we have to show is the "perfectness" of the pairing $\langle\,,\rangle$ on $e_0H_P^1(\Gamma_1(N),L_n(\mathbf{Z}_p))$. By Corollary 4.10, $e_0H_P^1(\Gamma_1(N),L_n(\mathbf{Z}_p))\otimes_{\mathbf{Z}_p}\mathbf{Z}/p\mathbf{Z}$ is naturally injected into $e_0 H^1_P(\Gamma_1(N), L_n(\mathbf{Z}/p\mathbf{Z}))$, which is isomorphic to $e H^1_P(\Phi_1, L_n(\mathbf{Z}_p)) \otimes_{\mathbf{Z}_p} \mathbf{Z}/p\mathbf{Z}$ (Theorem 6.6 and [10, Cor. 3.3]). Thus we know that

$$e_0 H^1_P(\Gamma_1(N), L_n(\mathbf{Z}/p\mathbf{Z})) \simeq e_0 H^1_P(\Gamma_1(N), L_n(\mathbf{Z}_p)) \otimes_{\mathbf{Z}_p} \mathbf{Z}/p\mathbf{Z}.$$

By [10, Cor. 3.5], the pairing $\langle\ ,\ \rangle$ induces a perfect duality on $e_0 H^1_P(\Gamma_1(N), L_n(\mathbf{Z}/p\mathbf{Z}))$; thus it induces a perfect duality on L^0 over $\mathcal{O}_{K_0}$.

Let R be a local ring of $\mathscr{h}^0(N;\mathcal{O}_K)$ such that $R \otimes_{\Lambda_K} \mathscr{L}_K$ contains $\mathscr{K}$. Take an integer a with $0 \leqq a < p-1$ so that μ acts on R via the character: $\zeta \mapsto \zeta^a$. We suppose one of the following two conditions:

(10.9a) $a \neq 2$, *and* a *and* $p-1$ *have non-trivial common divisor;*

(10.9b) $a \neq 2$, *and* $R \simeq \mathrm{Hom}_{\Lambda_K}(R, \Lambda_K)$ (i.e. R is a Gorenstein algebra).

The condition (10.3) is automatically satisfied under the condition: $a \neq 2$, because $\varepsilon\psi\omega^{-2}$ is non-trivial.

Then we have

Theorem 10.5. *If* $k=2$ *or* $C=N$, *then we have*

$$|Z(k, \Psi(k,\varepsilon))/U_\infty(k,\varepsilon)|_p^{-[k:\mathbf{Q}_p]} = |C_{k,\varepsilon}(\mathscr{K})|,$$

where $C_{k,\varepsilon}(\mathscr{K})$ *is the module of congruence defined in* (1.12) *and the right-hand side of the above formula is the cardinality of the module* $C_{k,\varepsilon}(\mathscr{K})$.

Here are some remarks about the theorem:

(i) Under the assumption of the theorem, Conjecture 3.10 in [13] is proven to be true.

(ii) We have adopted in the formulation of the theorem the special value $\mathscr{D}(k,f)$ for $f \in \Psi(k,\varepsilon)$ instead of the value of the primitive L-function $D(s,f)$. The reason of the adoption of $\mathscr{D}(k,f)$ is as follows: By twisting a minimal form f by a character χ, $f|\chi$ may have more congruence than f has, and at least conjecturally, the amount of extra congruences of $f|\chi$ should be governed by the excluded Euler factor of $\mathscr{D}(k,f|\chi)$ from $D(k,f)$. Thus, to give a precise statement for non-minimal forms has some meaning to examine this phenomenon. However, as already seen, the value $D(k,f)$ depends only on the class of twists of f; so, for the definition of the standard p-adic interpolation of the values $D(k,f)$, it is certainly better to take the local ring to which minimal forms belong (see Corollary 10.6 below). In fact, we shall prove in our subsequent paper that if $f \in \Psi(k,\varepsilon)$ is minimal for at least one couple (k,ε), then it is true for all couple (k,ε) with $k \geqq 2$. And, if one supposes that all the non-archimedean local factors of the automorphic representation of $f \in \Psi(k,\varepsilon)$ are principal and f is minimal, (this is equivalent to saying that $\varepsilon\psi\omega^{-k}$ is primitive modulo C)), then $D(s,f) = \mathscr{D}(s,f)$ by Corollary 10.2, and the transcendental factor $U_\infty(k,\varepsilon)$ is substantially simplified and is given by the formula:

$$U_\infty(k,\varepsilon) = \pi^{d(k+1)}(U_F \overline{U^F})^{\frac{1}{2}}\{(k-1)!\,C^2\}^{-d}.$$

Proof of Theorem 10.5. We shall prove the theorem only in the case where R satisfies (10.9a), because the other case can be shown by an argument similar to that given below, by Theorem 9.4 instead of Theorem 9.3. We know from Propositions 10.3–4 that

$$|Z(k, \Psi(k,\varepsilon))/U_\infty(k,\varepsilon)|_p^{-2[K:\mathbf{Q}_p]}=[L_\varepsilon^F : L_{\varepsilon,F}]=[L^{\varepsilon,F} : L_F^\varepsilon].$$

Thus, what we have to prove is the formula:

$$[L_\varepsilon^F : L_{\varepsilon,F}]=[L^{\varepsilon,F} : L_F^\varepsilon]=|C_{k,\varepsilon}(\mathcal{K})|^2.$$

Firstly we suppose that $C=N$. Let e_0 be the idempotent attached to $T(p)$ in $h_k(\Gamma_1(N);\mathcal{O}_K)$. Then e induces an isomorphism:

$$e_0 S_k(\Gamma_1(N);\mathbf{Z}_p)\otimes_{\mathbf{Z}_p}\mathbf{Z}/p\mathbf{Z}\simeq eS_k(\Phi_1;\mathbf{Z}_p)\otimes_{\mathbf{Z}_p}\mathbf{Z}/p\mathbf{Z}.$$

By duality (e.g. Lemma 7.1), we know that

$$h_k^0(\Phi_1;\mathbf{Z}_p)\otimes_{\mathbf{Z}_p}\mathbf{Z}/p\mathbf{Z}\simeq e_0 h_k(\Gamma_1(N);\mathbf{Z}_p)\otimes_{\mathbf{Z}_p}\mathbf{Z}/p\mathbf{Z}.$$

Thus, as $\mathcal{O}_K$-algebra, we have that

$$h_k^0(\Phi_1;\mathcal{O}_K)\simeq e_0 h_k(\Gamma_1(N);\mathcal{O}_K).$$

Let R_k be the local ring of $e_0 h_k(\Gamma_1(N);\mathcal{O}_K)$ corresponding to R (i.e. $R_k\simeq R/P_k R$), and decompose

$$R_k\otimes_{\mathcal{O}_K}K=F\oplus A \text{ as an algebra direct sum,}$$

where e induces an isomorphism: $F\simeq(h(\mathcal{K})/P_k h(\mathcal{K}))\otimes_{\mathcal{O}_K}K$. Let $h(F)$ (resp. $R(A)$) be the image of R_k in F (resp. A). Then, we see that

$$C_{k,\varepsilon}(\mathcal{K})\simeq(h(F)\oplus R(A))/R_k.$$

Let $L(R)=\sum_{r\in R_k} r(L\otimes_{\mathcal{O}_{K_0}}\mathcal{O}_K)$. Then, by Theorem 9.3 and the proof of Proposition 10.4, we know that

$$L(R)\simeq R_k\oplus\mathrm{Hom}_{\mathcal{O}_K}(R_k,\mathcal{O}_K)\quad\text{as } R\text{-modules.}$$

Thus, by definition, we know that (e.g. [11, §3])

$$L_\varepsilon^F/L_{\varepsilon,F}\simeq C_{k,\varepsilon}(\mathcal{K})\oplus\mathrm{Hom}_{\mathbf{Z}_p}(C_{k,\varepsilon}(\mathcal{K}),\mathbf{T}_p),$$

and this shows the theorem when $C=N$. Now we treat the case: $k=2$ and $p|C$. Put $R_{k,\varepsilon}=R/P_{k,\varepsilon}R$. Then, $R_{k,\varepsilon}$ is a local factor of $h_k^0(\Phi_r^1,\varepsilon;\mathcal{O}_K)$ for r given by $\Gamma_r=\mathrm{Ker}(\varepsilon)$ (Theorem 1.2). Let $L^\varepsilon(R)=\sum_{r\in R_{k,\varepsilon}} r(\pi_\varepsilon(L)\otimes_{\mathcal{O}_{K_0}}\mathcal{O}_K)\subset S(\varepsilon)$. Then, similarly as above we have

$$L^\varepsilon(R)\simeq R_{k,\varepsilon}\oplus\mathrm{Hom}_{\mathcal{O}_K}(R_{k,\varepsilon},\mathcal{O}_K)\quad\text{as } R\text{-modules}$$

and

$$L^{\varepsilon,F}/L_F^\varepsilon\simeq C_{k,\varepsilon}(\mathcal{K})\oplus\mathrm{Hom}_{\mathbf{Z}_p}(C_{k,\varepsilon}(\mathcal{K}),\mathbf{T}_p),$$

which finishes the proof.

Finally, we shall discuss the p-adic interpolation of the values $Z(k, \Psi(k,\varepsilon))/U_\infty(k,\varepsilon)$. Let M be a finite torsion Λ_K-module. For each prime divisor P of Λ_K, let $l_P(M)$ be the length of $M \otimes_{\Lambda_K} \Lambda_P$ over the localization Λ_P of Λ_K at P, and put

$$\chi(M) = \prod_P P^{l_P(M)}.$$

Then, $\chi(M)$ is a principal ideal of Λ_K. We now identify Λ_K with $\mathcal{O}_K[[X]]$ via $\imath(u) \mapsto 1+X$.

Since the following corollary gives the main result corresponding to Theorem III in the introduction, we shall repeat here all the assumptions we have already made, in order to make clear in what extent we have achieved this final result and what remains as a conjecture: Firstly, we have to assume one of the following conditions to assure the decomposition as in Theorems 9.3 and 9.4:

(ia) $(p-1, a) > 1$;

(ib) $R \simeq \mathrm{Hom}_\Lambda(R, \Lambda)$ as R-module,

where R is the local ring of $\mathscr{h}^0(N; \mathbf{Z}_p)$ such that $R \otimes_\Lambda \mathscr{L}_K \supset \mathscr{K}$ and a is the integer such that $0 \leqq a < p-1$ and μ acts on R via the character: $\zeta \mapsto \zeta^a$. In addition to one of (ia, b), we shall suppose the following three conditions:

(ii) $a \neq 2$ (to guarantee the good reduction for the minimal abelian subvariety of $J_1(Np^r)$ containing $J_r(R)$; cf. §9);

(iii) *The module of defect $\mathscr{N}_s(\mathscr{K}; \mathscr{K})$ is trivial* (this is known if (ib) is true and $[\mathscr{K}; \mathscr{L}_K] = 1$; cf. [13, Prop. 3.9]; especially when $\mathscr{K}$ is with complex multiplication as in Prop. 2.3 and $a \neq 1, 2$ ([28, §6]));

(iv) Either $k=2$ or the p-part of $\varepsilon\psi\omega^{-k}$ is trivial (to assure the self duality; cf. Prop. 10.4).

Corollary 10.6. *Let $H(X)$ be a generator of $\chi(\mathscr{C}(\mathscr{K}; K))$ in Λ_K. Then, under the above assumptions, there exists a p-adic unit $U_p(k,\varepsilon) \in \Omega$ for each couple (k,ε) with $k \geqq 2$ such that*

$$Z(k, \Psi(k,\varepsilon))/U_\infty(k,\varepsilon)\, U_p(k,\varepsilon) = H(\varepsilon(u)u^k - 1).$$

Thus the Iwasawa function: $s \mapsto H(\varepsilon(u)u^s - 1)\,(s \in \mathbf{Z}_p)$ gives a p-adic interpolation of the values $Z(k, \Psi(k,\varepsilon))/U_\infty(k,\varepsilon)$.

Note that when $N=1$ and $[\mathscr{K} : \mathscr{L}_K] = 1$, the condition (ia) is automatically satisfied, and hence Theorem III in §0 follows from this corollary.

Proof. Decompose $\mathscr{q}(N; K) = \mathscr{K} \oplus \mathscr{A}$ as an algebra direct sum, and let $\mathscr{h}(\mathscr{K})$ (resp. $\mathscr{h}(\mathscr{A})$) be the image of $\mathscr{h}^0(N; \mathcal{O}_K)$ in $\mathscr{K}$ (resp. $\mathscr{A}$). The vanishing of $\mathscr{N}_s(\mathscr{K}; K)$ means that (i) $\mathscr{h}(\mathscr{K}) \oplus \mathscr{h}(\mathscr{A})$ is Λ_K-free, and (ii) $\mathscr{C}(\mathscr{K}; K) \otimes_{\Lambda_K} \Lambda_K/P_{k,\varepsilon}\Lambda_K \simeq C_{k,\varepsilon}(\mathscr{K})$. The assertion (i) follows from the definition of $\mathscr{N}_s(\mathscr{K}; K)$ in [13, (3.9b)], and (ii) is a consequence of Corollary 1.7. By (i), we can take a Λ_K-free basis of $\mathscr{h}(\mathscr{K}) \oplus \mathscr{h}(\mathscr{A})$ and $\mathscr{h}^0(N; \mathcal{O}_K)$. Then, we find a matrix $\alpha \in M_d(\Lambda_K) \cap GL_d(\mathscr{L}_K)$ for $d = \mathrm{rank}_{\Lambda_K}(\mathscr{h}^0(N; \mathcal{O}_K))$ so that

$$\alpha(\mathscr{h}(\mathscr{K}) \oplus \mathscr{h}(\mathscr{A})) = \mathscr{h}^0(N; \mathcal{O}_K).$$

It is well known (e.g. [1, VII.4.6]) that $\det(\alpha)\in\Lambda_K$ generates $\chi(\mathscr{C}(\mathscr{X};K))$. We may thus assume that $H=\det(\alpha)$. If we put $\mathscr{h}(F)=\mathscr{h}(\mathscr{X})/P_{k,\varepsilon}\mathscr{h}(\mathscr{X})$ and $\mathscr{h}(A)=\mathscr{h}(\mathscr{A})/P_{k,\varepsilon}\mathscr{h}(\mathscr{A})$, then

$$C_{k,\varepsilon}(\mathscr{X})\simeq(\mathscr{h}(F)\oplus\mathscr{h}(A))/\mathscr{h}_k^0(\Phi_r^1,\varepsilon;\mathcal{O}_K),$$

where r is given by $\Gamma_r=\mathrm{Ker}(\varepsilon)$. Furthermore, if we write $\bar{\alpha}\in M_d(\mathcal{O}_K)$ for $\alpha \bmod P_{k,\varepsilon}$, we know that

$$\bar{\alpha}(\mathscr{h}(F)\oplus\mathscr{h}(A))=\mathscr{h}_k^0(\Phi_r^1,\varepsilon;\mathcal{O}_K).$$

Thus we obtain the formula:

$$|C_{k,\varepsilon}(\mathscr{X})|=|\det(\bar{\alpha})|_p^{-[K:\mathbf{Q}_p]}=|H(\varepsilon(u)u^k-1)|_p^{-[K:\mathbf{Q}_p]},$$

and we see from Theorem 10.5 that

$$|Z(k,\Psi(k,\varepsilon))/U_\infty(k,\varepsilon)|_p=|H(\varepsilon(u)u^k-1)|_p,$$

which finishes the proof.

References

1. Bourbaki, N.: Commutative algebra. Paris: Hermann 1972
2. Casselman, W.: On some results of Atkin and Lehner. Math. Ann. **201**, 301–304 (1973)
3. Curtis, C.W., Reiner, I.: Representation theory of finite groups and associative algebras. Pure and Applied Math. **11**, New York: Interscience 1962
4. Deligne, P.: Formes modulaires et représentations *l*-adiques. Sém. Bourbaki. Exp. 355 (1969)
5. Deligne, P., Serre, J.-P.: Formes modulaires de poids 1. Ann. Sci. Ec. Norm. Super. 4ème série, **7**, 507–530 (1974)
6. Doi, K., Miyake, T.: Automorphic forms and number theory. (in Japanese), Tokyo: Kinokuniya Shoten 1976
7. Gelbart, S., Jacquet, H.: A relation between automorphic representations of GL(2) and GL(3). Ann. Sci. Ec. Norm. Super, 4ème série **11**, 471–542 (1978)
8. Hecke, E.: Theorie der Eisensteinschen Reihen höherer Stufe und ihre Anwendung auf Funktionentheorie und Arithmetik. Abh. Math. Semin. Hamb. **5**, 199–224 (1927)
9. Hida, H.: Congruences of cusp forms and special values of their zeta functions. Invent. Math. **63**, 225–261 (1981)
10. Hida, H.: On congruence divisors of cusp forms as factors of the special values of their zeta functions. Invent. Math. **64**, 221–262 (1981)
11. Hida, H.: Kummer's criterion for the special values of Hecke *L*-functions of imaginary quadratic fields and congruences among cusp forms. Invent. Math. **66**, 415–459 (1982)
12. Hida, H.: A *p*-adic measure attached to the zeta functions associated with two elliptic modular forms, I. Invent. Math. **79**, 159–195 (1985)
13. Hida, H.: Iwasawa modules attached to congruences of cusp forms. (To appear in Ann. Sci. Ec. Norm. Super.)
14. Hida, H.: Congruences of cusp forms and Hecke algebras. Sém. Théorie des Nombres, Paris, 1983–84
15. Langlands, R.P.: Modular forms and *l*-adic representations. In: Modular functions of one variable, II, Lect. Notes Math. **349**, pp. 361–500. Berlin-Heidelberg-New York: Springer 1973
16. Mazur, B., Wiles, A.: Class fields of abelian extensions of **Q**. Invent. Math. **76**, 179–330 (1984)
17. Ohta, M.: On *l*-adic representations attached to automorphic forms. Jap. J. Math. **8** (new series), 1–47 (1982)

18. Ribet, K.A.: Galois representations attached to eigenforms with Nehentypus. In: Modular functions of one variable, V, Lect. Notes Math. **601**, pp. 17–52. Berlin-Heidelberg-New York: Springer 1977
19. Serre, J.-P., Tate, J.: Good reduction of abelian varieties. Ann. Math. **88**, 492–517 (1968)
20. Shimura, G.: Sur les intégrales attachées aux formes automorphes. J. Math. Soc. Japan **11**, 291–311 (1959)
21. Shimura, G.: On the factors of the jacobian variety of a modular function field, J. Math. Soc. Japan **25**, 523–544 (1973)
22. Shimura, G.: On the holomorphy of certain Dirichlet series. Proc. Lond. Math. Soc. **31**, 79–98 (1975)
23. Shimura, G.: The periods of certain automorphic forms of arithmetic type. J. Fac. Sci. Univ. Tokyo, Sec. I A, **28**, 605–632 (1982)
24. Shimura, G.: An *l*-adic method in the theory of automorphic forms. (Unpublished (1968))
25. Shimura, G.: Introduction to the arithmetic theory of automorphic functions. Tokyo: Iwanami Shoten and Princeton Univ. Press 1971
26. Sturm, J.: Special values of zeta functions, and Eisenstein series of half integral weight. Amer. J. Math. **102**, 219–240 (1980)
27. Tate, J.: *p*-divisible groups. In: Proceeding of a Conference on local fields, pp. 158–183. Berlin-Heidelberg-New York: Springer 1967
28. Hida, H.: Hecke algebras for GL(1) and GL(2). Séminaire de Théorie des Nombres, Paris, 1984–85

Oblatum 15-IX-1985