A NEW PROOF OF A THEOREM OF HIDA

Matthew Emerton

University of Michigan

1. introduction

Let $p \geq 5$ be prime. Hida has developed an extensive theory of so-called ordinary p-adic modular forms. One of the basic results of his theory is that the projective limit of the ordinary parts of the homology modules of the Riemann surfaces $Y_1(p^r)$

$$\mathbf{W}^{\mathrm{ord}} := \varprojlim_r H_1(Y_1(p^r), \mathbf{Z}_p)^{\mathrm{ord}}$$

is a free Λ-module of finite rank with the property

$$\mathbf{W}^{\mathrm{ord}} \otimes_\Lambda \mathbf{Z}_p[\Gamma/\Gamma_r] = H_1(Y_1(p^r), \mathbf{Z}_p)^{\mathrm{ord}}$$

for all $r > 0$. (Here Γ denotes the group of units in $\mathbf{Z}_p$ congruent to one modulo p, Γ_r denotes the kernel of the reduction of Γ modulo p^r, and Λ denotes the completed group ring $Z_p[[\Gamma]] = \varprojlim_r \mathbf{Z}_p[\Gamma/\Gamma_r]$.)

Hida proves this through a series of group cohomological calculations combined with his theory of the ordinary part of the p-adic Hecke algebra. In this note we present a simple proof of the same result (Theorem 5.3 below) using only the elementary algebraic topology of the Riemann surfaces $Y_1(p^r)$. As with Hida, we also consider the case of auxiliary $\Gamma_1(N)$-level structure, for some N prime to p.

2. the tower of modular curves

Let p be an odd prime, and N a natural number coprime to p, such that $\Gamma_1(Np)$ is torsion free. The subject of Hida's theory is the tower of modular curves

$$\begin{array}{c} \vdots \\ \downarrow \\ Y_1(Np^r) \\ \downarrow \\ \vdots \\ \downarrow \\ Y_1(Np) \end{array}$$

corresponding to the chain of congruence subgroups

$$\cdots \subset \Gamma_1(Np^r) \subset \cdots \subset \Gamma_1(Np).$$

If we take the homology (with coefficients in $\mathbf{Z}$) of the tower of modular curves, we get a tower of finitely generated free abelian groups, which is the abelianization of the above chain of subgroups:

$$\cdots \to \Gamma_1(Np^r)^{\mathrm{ab}} \to \cdots \to \Gamma_1(Np)^{\mathrm{ab}}.$$

The inclusions become morphisms which need no longer be injective (abelianization is not an exact functor). To better understand this chain of morphisms, we follow Hida and introduce intermediate congruence subgroups

$$\Phi_r^1 = \Gamma_1(Np) \cap \Gamma_0(p^r).$$

The inclusion $\Gamma_1(Np^r) \subset \Gamma_1(Np)$ factors as

$$\Gamma_1(Np^r) \subset \Phi_r^1 \subset \Gamma_1(Np),$$

and $\Gamma_1(Np^r)$ is a normal subgroup of Φ_r^1 (in fact Φ_r^1 is the normalizer of $\Gamma_1(Np^r)$ in $\Gamma_1(Np)$).

Denote by Γ the principal units in $\mathbf{Z}_p$, defined by the short exact sequence

$$1 \to \Gamma \to \mathbf{Z}_p^\times \to (\mathbf{Z}_p/p)^\times \to 1.$$

We let Γ_r denote the (unique since p is odd) subgroup of index p^{r-1} contained in Γ defined by the short exact sequence

$$1 \to \Gamma_r \to \mathbf{Z}_p^\times \to (\mathbf{Z}_p/p^r)^\times \to 1.$$

We define a morphism of groups

$$\Phi_r^1 \to \Gamma/\Gamma_r$$

via the formula

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \to d \bmod p^r.$$

This is a surjective morphism with kernel equal to $\Gamma_1(Np^r)$which yields the short exact sequence

$$1 \to \Gamma_1(Np^r) \to \Phi_r^1 \to \Gamma/\Gamma_r \to 1.$$

The action of Φ_r^1 on $\Gamma_1(Np^r)$ by conjugation induces an action of the quotient $\Phi_r^1/\Gamma_1(Np^r) = \Gamma/\Gamma_r$ on the abelianization of $\Gamma_1(Np^r)$. Thus Γ acts naturally on $\Gamma_1(Np^r)^{\mathrm{ab}}$ through its quotient Γ/Γ_r. (The automorphisms induced by elements of Γ are sometimes referred to as the 'diamond operators'. Alternatively, one might call this action of Γ the 'nebentypus' action.) The morphisms in the chain

$$\cdots \to \Gamma_1(Np^r)^{\mathrm{ab}} \to \cdots \to \Gamma_1(Np)^{\mathrm{ab}}$$

are clearly Γ-equivariant.

If $r \geq s > 0$, we denote by Φ_r^s the subgroup of Φ_r^1 containing $\Gamma_1(Np^r)$ whose quotient by $\Gamma_1(Np^r)$ equals Γ_s/Γ_r. In other words,

$$\Phi_r^s = \Gamma_1(Np^s) \cap \Gamma_0(p^r).$$

If we abelianize the short exact sequence

$$1 \to \Gamma_1(Np^r) \to \Phi_r^s \to \Gamma_s/\Gamma_r \to 1$$

we obtain the (no longer short) exact sequence

$$\Gamma_1(Np^r)^{\mathrm{ab}} \to \Phi_r^{s\,\mathrm{ab}} \to \Gamma_s/\Gamma_r \to 1.$$

We let $\mathfrak{a}_s$ denote the augmentation ideal in the group ring $\mathbf{Z}[\Gamma_s]$. Then by definition

$$\mathfrak{a}_s\Gamma_1(Np^r)^{\mathrm{ab}} = [\Phi_r^s, \Gamma_1(Np^r)]/[\Gamma_1(Np^r), \Gamma_1(Np^r)] \subset \Gamma_1(Np^r)^{\mathrm{ab}}.$$

The extension

$$1 \to \Gamma_1(Np^r)/[\Phi_r^s, \Gamma_1(Np^r)] \to \Phi_r^s/[\Phi_r^s, \Gamma_1(Np^r)] \to \Gamma_s/\Gamma_r \to 1$$

is a central extension of a cyclic group, thus abelian, implying that

$$[\Phi_r^s, \Gamma_1(Np^r)] = [\Phi_r^s, \Phi_r^s].$$

Thus we we may rewrite this extension as the short exact sequence

$$1 \to \Gamma_1(Np^r)^{\mathrm{ab}}/\mathfrak{a}_s \to \Phi_r^{s\,\mathrm{ab}} \to \Gamma_s/\Gamma_r \to 1.$$

Summarizing this discussion, we see that a typical map

$$\Gamma_1(Np^r)^{\mathrm{ab}} \to \Gamma(Np^s)^{\mathrm{ab}}$$

in the chain of homology groups arising from the tower of modular curves may be factored as the composition of the surjection

$$\Gamma_1(Np^r)^{\mathrm{ab}} \to \Gamma_1(Np^r)^{\mathrm{ab}}/\mathfrak{a}_s,$$

the injection

$$\Gamma_1(Np^r)^{\mathrm{ab}}/\mathfrak{a}_s \to \Phi_r^{s\,\mathrm{ab}}$$

and the morphism

$$\Phi_r^{s\,\mathrm{ab}} \to \Gamma_1(Np^s)^{\mathrm{ab}}.$$

Hida observed that if one applies a certain projection operator arising from the Atkin U-operator to all these modules (tensored with $\mathbf{Z}_p$) then the second and third morphisms of this factorization become isomorphisms.

3. HECKE OPERATORS

In this section we give a group-theoretic discussion of Hecke operators, sufficient for the purposes of this paper. For a more thorough treatment one should consult [2, §4] or [4, Chapter 3].

Suppose that T is a group which contains subgroups G and H and that t is an element of T such that $t^{-1}Ht \cap G$ has finite index in G. Then one has a transfer morphism

$$V : G^{\mathrm{ab}} \to (t^{-1}Ht \cap G)^{\mathrm{ab}}.$$

Conjugation by t induces an isomorphism

$$(t^{-1}Ht \cap G)^{\mathrm{ab}} \cong (H \cap tGt^{-1})^{\mathrm{ab}}.$$

Inclusion of this last group in H induces a morphism

$$(H \cap tGt^{-1})^{\mathrm{ab}} \to H^{\mathrm{ab}}.$$

Taking the composition of all these we obtain a morphism

$$[t] : G^{\mathrm{ab}} \to H^{\mathrm{ab}},$$

the 'Hecke operator' corresponding to t.

In the case when $T = \mathbf{GL}_2(\mathbf{Q})$, $G = H =$ a congruence subgroup of $\mathbf{SL}(2, \mathbf{Z})$ of level divisible by p and $t := \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$, we denote the corresponding Hecke operator by U. It is called the 'Atkin U-operator' (for the prime p).

Suppose that G is one of the Φ_r^s of the previous Section. A calculation shows that

$$t^{-1}\Phi_r^s t \cap \Phi_r^s = \Phi_r^s \cap \Gamma^0(p), \;\; \Phi_r^s \cap t\Phi_r^s t^{-1} = \Phi_{r+1}^s.$$

(Here $\Gamma^0(p)$ denotes the subgroup of $\mathbf{SL}(2, \mathbf{Z})$ consisting of matrices which are congruent to $\begin{pmatrix} * & 0 \\ * & * \end{pmatrix}$ modulo p.) Thus the Atkin U-operator is by definition the composition

$$\Phi_r^{s\,\mathrm{ab}} \xrightarrow{V} (\Phi_r^s \cap \Gamma^0(p))^{\mathrm{ab}} \xrightarrow{t(-)t^{-1}} \Phi_{r+1}^{s\,\mathrm{ab}} \longrightarrow \Phi_r^{s\,\mathrm{ab}}.$$

(The final morphism is just that induced by the inclusion of groups $\Phi_{r+1}^s \subset \Phi_r^s$.) Define U' to be the composition of just the first two of these morphisms:

$$U' : \Phi_r^{s\,\mathrm{ab}} \xrightarrow{V} (\Phi_r^s \cap \Gamma^0(p))^{\mathrm{ab}} \xrightarrow{t(-)t^{-1}} \Phi_{r+1}^{s\,\mathrm{ab}}.$$

Lemma 3.1. *Suppose that $r \geq s > 0$, $r' \geq s' > 0$, $r \geq r'$, $s \geq s'$, so that $\Phi_r^s \subset \Phi_{r'}^{s'}$. Then the following diagram commutes:*

$$\begin{array}{ccc} \Phi_r^{s\,\mathrm{ab}} & \longrightarrow & \Phi_{r'}^{s'\,\mathrm{ab}} \\ \downarrow{\scriptstyle U'} & & \downarrow{\scriptstyle U'} \\ \Phi_{r+1}^{s\,\mathrm{ab}} & \longrightarrow & \Phi_{r'+1}^{s'\,\mathrm{ab}}. \end{array}$$

(The horizontal morphisms are those induced by inclusion.) Consequently the following diagram also commutes (by definition of U' and U):

$$\begin{array}{ccc} \Phi_r^{s\,\mathrm{ab}} & \longrightarrow & \Phi_{r'}^{s'\,\mathrm{ab}} \\ \downarrow{\scriptstyle U} & & \downarrow{\scriptstyle U} \\ \Phi_r^{s\,\mathrm{ab}} & \longrightarrow & \Phi_{r'}^{s'\,\mathrm{ab}}. \end{array}$$

Proof. The diagram whose commutativity is asserted by the Lemma factorizes into the composition of two diagrams:

$$\begin{array}{ccc}
{\Phi_r^s}^{\mathrm{ab}} & \longrightarrow & {\Phi_{r'}^{s'}}^{\mathrm{ab}} \\
\downarrow{\scriptstyle V} & & \downarrow{\scriptstyle V} \\
\left(\Phi_r^s \cap \Gamma^0(p)\right)^{\mathrm{ab}} & \longrightarrow & \left(\Phi_{r'}^{s'} \cap \Gamma^0(p)\right)^{\mathrm{ab}} \\
\downarrow{\scriptstyle t(-)t^{-1}} & & \downarrow{\scriptstyle t(-)t^{-1}} \\
{\Phi_{r+1}^{s+1}}^{\mathrm{ab}} & \longrightarrow & {\Phi_{r'+1}^{s'+1}}^{\mathrm{ab}}.
\end{array}$$

The lower portion of this diagram clearly commutes. To see that the upper half commutes is a calculation: $\Phi_r^s \cap \Gamma^0(p)$ has index p in Φ_r^s, and we can can take as the coset representatives the p matrices

$$\begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix},$$

$(0 \leq i \leq p-1)$. Since these coset representatives are independent of the particular values of r and s, the transfer

$${\Phi_r^s}^{\mathrm{ab}} \xrightarrow{V} \left(\Phi_r^s \cap \Gamma^0(p)\right)^{\mathrm{ab}}$$

is given by a formula independent of the values of r and s, so the upper portion of the diagram commutes. Thus the Lemma is proved. □

A particular case of the Lemma which is of interest is the case $r' = r-1$, $s' = s \leq r-1$. If we write π for the morphism

$$\pi : {\Phi_r^s}^{\mathrm{ab}} \to {\Phi_{r-1}^s}^{\mathrm{ab}}$$

and π' for the morphism

$$\pi' : {\Phi_{r+1}^s}^{\mathrm{ab}} \to {\Phi_r^s}^{\mathrm{ab}}$$

then the Lemma yields the following formula:

$$U' \circ \pi = \pi' \circ U' = U \in \mathrm{End}_{\mathbf{Z}}({\Phi_r^s}^{\mathrm{ab}}), \tag{3.2}$$

the second equality following from the definition of U and U'. The same definition yields the formula

$$\pi \circ U' = U \in \mathrm{End}_{\mathbf{Z}}({\Phi_{r-1}^s}^{\mathrm{ab}}). \tag{3.3}$$

More generally, Lemma 3.1 shows that each ${\Phi_r^s}^{\mathrm{ab}}$ is made a $\mathbf{Z}[U]$-module via the action of the Atkin U-operator and the morphisms between these modules arising from the inclusion relations between the Φ_r^s for varying r and s are morphisms of $\mathbf{Z}[U]$-modules.

Consider in particular the morphism $\Gamma_1(Np^r)^{\mathrm{ab}} \to {\Phi_r^s}^{\mathrm{ab}}$. Since this is a morphism of $\mathbf{Z}[U]$-modules its cokernel is naturally a $\mathbf{Z}[U]$-module. We saw in the preceding section that this cokernel is the abelian group Γ_s/Γ_r.

Lemma 3.4. *The operator U acts on Γ_s/Γ_r as multiplication by p.*

Proof. This is easily proved by direct calculation, using the coset representatives for $\Phi_r^s \cap \Gamma^0(p)$ in Φ_r^s listed above. □

Lemma 3.5. *If $r \geq s > 0$, the action of U on ${\Phi_r^s}^{\mathrm{ab}}$ commutes with the nebentypus action of Γ on ${\Phi_r^s}^{\mathrm{ab}}$.*

Proof. Let $\alpha \in \Phi_{r+1}^1 \cap \Gamma^0(p)$. Then the following diagram certainly commutes:

$$\begin{array}{ccc}
{\Phi_r^s}^{\mathrm{ab}} & \xrightarrow{\alpha(-)\alpha^{-1}} & {\Phi_r^s}^{\mathrm{ab}} \\
\downarrow V & & \downarrow V \\
(\Phi_r^s \cap \Gamma^0(p))^{\mathrm{ab}} & \xrightarrow{\alpha(-)\alpha^{-1}} & (\alpha(\Phi_r^s \cap \Gamma^0(p))\alpha^{-1})^{\mathrm{ab}} = (\Phi_r^s \cap \Gamma^0(p))^{\mathrm{ab}} \\
\downarrow t(-)t^{-1} & & \downarrow \alpha t\alpha^{-1}(-)\alpha t^{-1}\alpha^{-1} \\
{\Phi_{r+1}^s}^{\mathrm{ab}} & \xrightarrow{\alpha(-)\alpha^{-1}} & (\alpha\Phi_{r+1}^s\alpha^{-1})^{\mathrm{ab}} = {\Phi_{r+1}^s}^{\mathrm{ab}} \\
\downarrow & & \downarrow \\
{\Phi_r^s}^{\mathrm{ab}} & \xrightarrow{\alpha(-)\alpha^{-1}} & \alpha{\Phi_r^s}^{\mathrm{ab}}\alpha^{-1} = {\Phi_r^s}^{\mathrm{ab}}.
\end{array}$$

Also, if $g \in \Phi_r^s \cap \Gamma^0(p)$, then

$$\alpha t\alpha^{-1} g \alpha t^{-1}\alpha^{-1} = (\alpha t\alpha^{-1}t^{-1})tgt^{-1}(\alpha t\alpha^{-1}t^{-1})^{-1}.$$

Now a calculation shows that $\alpha t\alpha^{-1}t^{-1} \in \Gamma_1(Np^{r+1})$, and thus conjugation by this element induces the identity on ${\Phi_{r+1}^s}^{\mathrm{ab}}$. Hence the following diagram also commutes:

$$\begin{array}{ccc}
{\Phi_r^s}^{\mathrm{ab}} & \xrightarrow{\alpha(-)\alpha^{-1}} & {\Phi_r^s}^{\mathrm{ab}} \\
\downarrow V & & \downarrow V \\
(\Phi_r^s \cap \Gamma^0(p))^{\mathrm{ab}} & & (\Phi_r^s \cap \Gamma^0(p))^{\mathrm{ab}} \\
\downarrow t(-)t^{-1} & & \downarrow t(-)t^{-1} \\
{\Phi_{r+1}^s}^{\mathrm{ab}} & & {\Phi_{r+1}^s}^{\mathrm{ab}} \\
\downarrow & & \downarrow \\
{\Phi_r^s}^{\mathrm{ab}} & \xrightarrow{\alpha(-)\alpha^{-1}} & {\Phi_r^s}^{\mathrm{ab}}.
\end{array}$$

Recall that the composition of the vertical morphisms on either side of this diagram is, by definition, the operator U. Thus U commutes with the automorphism of ${\Phi_r^s}^{\mathrm{ab}}$ induced by conjugation by α. Since the nebentypus action may be realized by conjugation by such elements α, the proposition is proved. (If $d \in \Gamma/\Gamma_s$, we may certainly find an element $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ of $\mathbf{SL}(2, \mathbf{Z})$ such that $p^{r+1}|c$ and $p|b$. Then the nebentypus action of d on ${\Phi_r^s}^{\mathrm{ab}}$ is given by conjugation by α, and $\alpha \in \Phi_{r+1}^1 \cap \Gamma^0(p)$, as is required in the preceding discussion.) □

4. ordinary parts

Let U be an indeterminate, and consider the full subcategory of the category of $\mathbf{Z}_p[U]$-modules consisting of those modules which are finitely generated as $\mathbf{Z}_p$-modules. This is an abelian category.

Let M be any module in this category. Then we have a morphism of $\mathbf{Z}_p$-modules

$$\mathbf{Z}_p[U] \to \mathrm{End}_{\mathbf{Z}_p}(M).$$

The endomorphism ring $\mathrm{End}_{\mathbf{Z}_p}(M)$ of M is a finite $\mathbf{Z}_p$-algebra, since M is finitely generated as a $\mathbf{Z}_p$-module. Thus the image of $\mathbf{Z}_p[U]$ in $\mathrm{End}_{\mathbf{Z}_p}(M)$ is also a finite $\mathbf{Z}_p$-algebra; call it A. Any finite $\mathbf{Z}_p$-algebra factors as a product of local rings; in particular A so factors. The projection of U onto some of the local factors of A will be contained in the corresponding maximal ideal, while its projection onto the others will be a unit. We let A^{ord} denote the product of all those local factors of A in which the image of U is a unit, and A^{nil} its complementary factor, so that $A = A^{\mathrm{ord}} \times A^{\mathrm{nil}}$. Each of these is a flat A-algebra, and a subalgebra of $\mathrm{End}_{\mathbf{Z}_p}(M)$. We define

$$M^{\mathrm{ord}} := M \otimes_A A^{\mathrm{ord}}$$

and call this the ordinary part of M. It is now easily seen that taking ordinary parts is an exact functor on our abelian category.

If we now consider U to be Atkin's U-operator corresponding to the prime p, we may consider the ordinary part of the $\mathbf{Z}_p$ homology of the curve $Y_1(Np^r)$, i.e. the module $\left(\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p\right)^{\mathrm{ord}}$. This is a Γ-module, since Lemma 3.4 shows that the Γ action commutes with U. We have the following fundamental Theorem, proved in [2]:

Theorem 4.1 [Hida]**.** *If $r \geq s > 0$ then the morphism of abelian groups*

$$\left(\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p\right)^{\mathrm{ord}} / \mathfrak{a}_s \to \left(\Gamma_1(Np^s)^{\mathrm{ab}} \otimes \mathbf{Z}_p\right)^{\mathrm{ord}}$$

is an isomorphism.

Proof. The proof of this Theorem rests on the two facts referred to at the end of Section 2: that

$$\left(\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p\right)^{\mathrm{ord}} / \mathfrak{a}_s \to \left(\Phi_r^{s\,\mathrm{ab}} \otimes \mathbf{Z}_p\right)^{\mathrm{ord}}$$

is an isomorphism and that

$$\left(\Phi_r^{s\,\mathrm{ab}} \otimes \mathbf{Z}_p\right)^{\mathrm{ord}} \to \left(\Gamma_1(Np^s)^{\mathrm{ab}}\right)^{\mathrm{ord}}$$

is an isomorphism.

The second of these isomorphisms is well known, and goes back (in a slightly different guise) to the paper [1] of Atkin and Lehner which introduced the operator U. The general principle is that when we apply U to any 'modular object' with a greater power of p in the level then in the conductor of the nebentypus character, we remove a power of p from the level.

To be more precise: in the previous Section we constructed a Hecke operator

$$U' : {\Phi_{r-1}^s}^{\mathrm{ab}} \to \Phi_r^{s\,\mathrm{ab}}$$

which satisfies equations (3.3) and (3.4): if

$$\pi : {\Phi_r^s}^{\mathrm{ab}} \to {\Phi_{r-1}^s}^{\mathrm{ab}}$$

is the morphism induced by the inclusion of groups $\Phi_r^s \subset \Phi_{r-1}^s$ then

$$U' \circ \pi = U \in \mathrm{End}({\Phi_r^s}^{\mathrm{ab}}),\ \pi \circ U' = U \in \mathrm{End}({\Phi_{r-1}^s}^{\mathrm{ab}}).$$

The existence of U' implies that upon tensoring over $\mathbf{Z}_p$ and taking the ordinary parts π induces an isomorphism

$$({\Phi_r^s}^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}} = ({\Phi_{r-1}^s}^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}};$$

$U^{-1} \circ U'$ provides an inverse to π. By descending induction on r we obtain the required isomorphism:

$$({\Phi_r^s}^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}} = ({\Phi_s^s}^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}} = (\Gamma_1(Np^s)^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}.$$

To prove the first isomorphism consider the short exact sequence

$$1 \to \Gamma_1(Np^r)^{\mathrm{ab}}/\mathfrak{a}_s \to {\Phi_r^s}^{\mathrm{ab}} \to \Gamma_s/\Gamma_r \to 1.$$

Tensor this with $\mathbf{Z}_p$ and take ordinary parts to obtain the short exact sequence

$$1 \to (\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}/\mathfrak{a}_s \to ({\Phi_r^s}^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}} \to (\Gamma_s/\Gamma_r)^{\mathrm{ord}} \to 1.$$

(The group Γ_s/Γ_r is p-torsion, and so is unaffected by tensoring with $\mathbf{Z}_p$. Recall also that U is Γ-equivariant, so that the taking of Γ_s-coinvariants and the taking of ordinary parts are commuting functors.) The isomorphism will follow if we can show that $(\Gamma_s/\Gamma_r)^{\mathrm{ord}}$ is trivial.

By Lemma 3.4 The operator U acts on the group Γ_s/Γ_r as multiplication by p and so is a nilpotent operator (since Γ_s/Γ_r is p-torsion). Thus Γ_s/Γ_r has trivial ordinary part and the Theorem follows. □

5. IWASAWA MODULES

We may take the projective limit of the chain of $\mathbf{Z}_p$-modules

$$\cdots \to \Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p \to \cdots \to \Gamma_1(Np)^{\mathrm{ab}} \otimes \mathbf{Z}_p$$

to obtain a limiting module which we denote by

$$\mathbf{W} := \varprojlim_r \Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p.$$

The profinite group Γ acts on the $\mathbf{Z}_p$-module $\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p$ through its finite quotient Γ/Γ_r. Thus the limiting module $\mathbf{W}$ not only has a Γ-action, but is a module over the completed group algebra

$$\Lambda := \varprojlim_r \mathbf{Z}_p[\Gamma/\Gamma_r].$$

The $\mathbf{Z}_p$- algebra Λ is called the 'Iwasawa algebra' and $\mathbf{W}$ is said to be an 'Iwasawa module'.

The Iwasawa module $\mathbf{W}$ is difficult to understand in its entirety, because we do not have a good characterization of the image of the morphism

$$\Gamma_1(Np^r)^{\mathrm{ab}} \to \Gamma_1(Np^s)^{\mathrm{ab}}$$

($r \geq s > 0$) in general, and so we cannot get a good description of the projective limit. However, Theorem 1 allows us to understand the ordinary part of $\mathbf{W}$ very well.

It will be convenient to abstract the situation slightly. Thus suppose that M_r is a projective system of Λ-modules indexed by positive integers r with the property that each M_r invariant under Γ_r. Then for any $r \geq s$ the given morphism

$$M_r \to M_s$$

factors as

$$M_r \to M_r/\mathfrak{a}_s \to M_s.$$

Define $\mathbf{M} = \varprojlim_r M_r$. Then for any s the natural morphism

$$\mathbf{M} \to M_s$$

factors as

$$\mathbf{M} \to \mathbf{M}/\mathfrak{a}_s \to M_s.$$

Proposition 5.1. *Suppose in the situation of the preceding paragraph that each M_r is p-adically complete and that the morphisms $M_r/\mathfrak{a}_s \to M_s$ are isomorphisms for any $r \geq s$. Then for any s the morphism $\mathbf{M}/\mathfrak{a}_s \to M_s$ is an isomorphism.*

Proof. First note that the hypotheses imply in particular that all the morphisms $M_r \to M_s$ for $r \geq s$ are surjective. Thus if m_s is any element of M_s we may construct an element (m_r) of $\mathbf{M}$ whose projection to M_s is the given element m_s.

For any s the group Γ_s is procyclic. If γ_s denotes a topological generator then the augmentation ideal $\mathfrak{a}_s$ is a principal ideal of Λ generated by the element $\gamma_s - 1$. If $i > 0$ then Γ_{s+i} is generated by $\gamma_s^{p^i}$ and so $\mathfrak{a}_{s+i}$ is principal with generator $\gamma_s^{p^i} - 1$. One easily computes that $\dfrac{\gamma_s^{p^i} - 1}{\gamma_s - 1}$ is an element of the ideal $(\gamma_s - 1, p)^i$.

Let $\mathfrak{m} = (\mathfrak{a}_1, p)$ denote the maximal ideal of Λ. Then $(\gamma_s - 1, p)^i \subset \mathfrak{m}^i$. Note that each M_r is $\mathfrak{m}$-adically complete, being both fixed by Γ_r and p-adically complete.

Now let us fix some s and suppose that (m_r) is an element of the projective limit $\mathbf{M}$ whose projection m_s to M_s vanishes; we must construct an element (m'_r) of $\mathbf{M}$ such that $(m_r) = (\gamma_s - 1)(m'_r)$. By assumption we may construct an element $m_{1,s+1}$ of M_{s+1} such that $m_{s+1} = (\gamma_s - 1)m_{1,s+1}$. Let $(m_{1,r})$ denote an element of $\mathbf{M}$ projecting to $m_{1,s+1}$. Then the element $(m_r) - (\gamma_s - 1)(m_{1,r})$ has vanishing projection to M_{s+1}. Proceeding inductively, we construct for any $i > 0$ an element $(m_{i,r})$ of $\mathbf{M}$ such that

$$(m_r) - \sum_{j=1}^{i} (\gamma_s^{p^{j-1}} - 1)(m_{j,r}) = (m_r) - (\gamma_s - 1) \sum_{j=1}^{i} \left(\frac{\gamma_s^{p^{j-1}} - 1}{\gamma_s - 1} \right) (m_{j,r})$$

has vanishing projection to M_{s+i}.

Since each M_r is $\mathfrak{m}$-adically complete, we see that the infinite series

$$(m'_r) := \sum_{j=1}^{\infty} \left(\frac{\gamma_s^{p^{j-1}} - 1}{\gamma_s - 1} \right) (m_{j,r})$$

yields a well-defined element of $\mathbf{M}$ with the property that

$$(m_r) = (\gamma_s - 1)(m'_r).$$

This proves the Proposition. □

Corollary 5.2. *For any $r > 0$ we have*

$$\left(\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p\right)^{\mathrm{ord}} = (\mathbf{W}^{\mathrm{ord}})/\mathfrak{a}_r$$

is the Γ_r-coinvariants of $\mathbf{W}^{\mathrm{ord}}$.

Proof. This follows from Proposition 5.1 (by taking r to be s in the statement of that Proposition) together with Theorem 4.1. □

Let us remark that the analogous statement to Corollary 5.2 is not true for $\mathbf{W}$.

Each module $\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p$ is free of finite rank over $\mathbf{Z}_p$, and so is compact in its p-adic topology. Thus if we give the limiting module $\mathbf{W}$ the topology which is the projective limit of the p-adic topology on each module $\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p$ it becomes a compact Λ-module. Furthermore, Λ acts continuously on $\mathbf{W}$, since Γ acts on each of the modules $\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p$ through a finite quotient. Since $\mathbf{W}^{\mathrm{ord}}$ is a direct factor of $\mathbf{W}$ the same remarks hold true for $\mathbf{W}^{\mathrm{ord}}$. Furthermore, Corollary 5.2 implies that the projective limit topology on $\mathbf{W}^{\mathrm{ord}}$ coincides with its $\mathfrak{m}$-adic topology (where $\mathfrak{m} = (\mathfrak{a}_1, p) \subset \Lambda$ denotes the maximal ideal of Λ), because the kernels of the projection

$$\Lambda \to \mathbf{Z}_p/p^r[\Gamma/\Gamma_r]$$

are cofinal with the sequence of ideals $\mathfrak{m}^r$ in Λ.

Thus $\mathbf{W}^{\mathrm{ord}}$ is a Λ-module, compact in its $\mathfrak{m}$-adic topology, such that

$$\mathbf{W}^{\mathrm{ord}}/\mathfrak{m} = \mathbf{W}^{\mathrm{ord}}/(\mathfrak{a}_1, p) = \left(\Gamma_1(Np)^{\mathrm{ab}} \otimes \mathbf{Z}_p/p\right)^{\mathrm{ord}}$$

is a finite dimensional $\mathbf{Z}_p/p$-module, of dimension d (say). This implies that $\mathbf{W}^{\mathrm{ord}}$ is a finitely generated Λ-module, with a minimal generating set of order equal to d. Of course d is equal to the $\mathbf{Z}_p$-rank of the free $\mathbf{Z}_p$-module $\left(\Gamma_1(Np)^{\mathrm{ab}} \otimes \mathbf{Z}_p\right)^{\mathrm{ord}}$.

The following Theorem is one of the key results of [2], and its proof is the object of this note:

Theorem 5.3 [Hida]**.** *The Λ-module $\mathbf{W}^{\mathrm{ord}}$ is free of finite rank equal to d.*

Before we explain the proof of this Theorem (which is the subject of the next three Sections) let us elucidate its meaning. Suppose that $x_1, \ldots, x_d$ is a basis for the free Λ-module $\mathbf{W}^{\mathrm{ord}}$. The projections of $x_1, \ldots, x_d$ in

$$\left(\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p\right)^{\mathrm{ord}} = \mathbf{W}^{\mathrm{ord}}/\mathfrak{a}_r$$

will generate this module, and in fact will realize it as a free module over the group algebra $\mathbf{Z}_p[\Gamma/\Gamma_r]$.

We may think of the projections of the x_i as being certain (homology classes of) cycles on $Y_1(Np^r)$ with $\mathbf{Z}_p$ coefficients. The diamond operators Γ/Γ_r are a certain group of automorphisms of the curve $Y_1(Np^r)$ (the covering transformations of $Y_1(Np^r)$ over $Y(\Phi_r^1)$) which induce the nebentypus action on $\Gamma_1(Np^r)^{\mathrm{ab}}$ via functoriality of homology. Since the x_i are a free basis for the $\mathbf{Z}_p[\Gamma/\Gamma_r]$-module $(\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}$, the collection of all translates by the diamond operators of the cycles $x_1, \ldots, x_d$ is a linearly independent set of cycles on $Y_1(Np^r)$ which generates the ordinary part of its homology. The fact that we may choose such cycles on $Y_1(Np^r)$, coherently as r approaches infinity (in particular keeping d constant), is one way of interpreting Theorem 5.3.

In fact, it is easy to see that Theorem 5.3 would follow if we knew that each ordinary homology module $(\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}$ was free as a $\mathbf{Z}_p[\Gamma/\Gamma_r]$-module. For suppose this was known. Then Theorem 1 would show that the rank of the free $\mathbf{Z}_p[\Gamma/\Gamma_r]$-module $(\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}$ would be a constant independent of r, and it is not hard to see that we could make coherent choices of $\mathbf{Z}_p[\Gamma/\Gamma_r]$-bases for these modules which would in the limit realize $\mathbf{W}^{\mathrm{ord}}$ as a free Λ-module.

It is difficult to characterize free modules over the group rings $\mathbf{Z}_p[\Gamma/\Gamma_r]$. However, the completed group ring Λ is a regular local ring of dimension two, and so any reflexive Λ-module is free [3]. We will prove Theorem 5.3 by considering the duality theory of the modules $(\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}$, showing that they are reflexive as $\mathbf{Z}_p[\Gamma/\Gamma_r]$-modules, and taking the limit to infer that $\mathbf{W}^{\mathrm{ord}}$ is a reflexive Λ-module. The following Section proves the necessary results on dual modules over group rings of finite groups and Section 7 contains the details involved in taking the limit. In order to complete the argument of Section 7 we must show that a certain pushforward morphism of cohomology modules is an isomorphism. This is the subject of Section 8.

6. Modules over group rings

Suppose that R is a commutative ring, G a finite group and M a left $R[G]$-module. Let N be any R-module. Then $\mathrm{Hom}_R(M, N)$ becomes a right $R[G]$-module, via composition with the action of G on M. The ring $R[G]$ is naturally a bimodule over itself, via ring multiplication on the left and right. Thus $R[G] \otimes_R N$ is an $R[G]$-bimodule, making $\mathrm{Hom}_{R[G]}(M, R[G] \otimes_R N)$ a right $R[G]$-module (the Hom being taken in the category of left $R[G]$-modules).

Lemma 6.1. *There is a canonical isomorphism of right $R[G]$-modules*

$$\mathrm{Hom}_R(M, N) = \mathrm{Hom}_{R[G]}(M, R[G] \otimes_R N).$$

Proof. If X is any set, and $R[X]$ denotes the free R-module based on X, we may think of $R[X]$ as the R-module of finitely supported R-valued measures on X. If we think of $R[G]$ in this way then its ring structure arises from convolution of measures. Since G is finite the multiplication map

$$G \times G \to G$$

has finite fibers, so pushforward of functions ('integration along the fibers') yields a pullback of measures

$$R[G] \to R[G \times G] = R[G] \otimes_R R[G].$$

This is a morphism of $R[G]$-modules which gives rise to a morphism of $R[G]$-modules for any left $R[G]$-module M:

$$\begin{aligned} M = R[G] \otimes_{R[G]} M \longrightarrow (R[G] \otimes_R R[G]) \otimes_{R[G]} M \\ = R[G] \otimes_R (R[G] \otimes_{R[G]} M) = R[G] \otimes_R M. \end{aligned}$$

This in turn gives rise to a morphism

$$\mathrm{Hom}_{R[G]}(R[G] \otimes_R M, R[G] \otimes_R N) \to \mathrm{Hom}_{R[G]}(M, R[G] \otimes_R N)$$

which when composed with the natural morphism

$$\mathrm{Hom}_R(M, N) \to \mathrm{Hom}_{R[G]}(R[G] \otimes_R M, R[G] \otimes_R N)$$

yields the isomorphism of the Lemma. □

Here is an explicit description of the isomorphism of Lemma 6.1: for any element ϕ of $\mathrm{Hom}_R(M, N)$ the image of ϕ in $\mathrm{Hom}_{R[G]}(M, R[G] \otimes_R N)$ acts via the following formula:

$$m \mapsto \sum_{g \in G} g \otimes \phi(g^{-1} m).$$

Now consider the case in which $N = R$. Write $M^* = \mathrm{Hom}_R(M, R)$; this is the R-dual of M. Applying Lemma 6.1, we see that M^* and $\mathrm{Hom}_{R[G]}(M, R[G])$ are canonically isomorphic as right $R[G]$-modules. The analogue of Lemma 6.1 for right $R[G]$-modules is obviously also true, and applying it to M^* we see that $\mathrm{Hom}_R(M^*, R)$ and $\mathrm{Hom}_{R[G]}(M^*, R[G])$ are canonically isomorphic as left $R[G]$-modules. By definition of M^* there is a natural morphism of R-modules

$$M \to \mathrm{Hom}_R(M^*, R)$$

which one checks is a morphism of left $R[G]$-modules. Suppose that this morphism is in fact an isomorphism, i.e. that M is a reflexive R-module. Then we have the isomorphisms of left $R[G]$-modules:

$$M = \mathrm{Hom}_R(M^*, N) = \mathrm{Hom}_{R[G]}(M^*, R[G]).$$

Thus we have proved the following Lemma:

Lemma 6.2. *If M is a left $R[G]$-module which is reflexive as an R-module then M is reflexive as an $R[G]$-module.*

7. limits of cohomology modules

Cohomology is the dual of homology:

$$H^1(Y_1(Np^r), \mathbf{Z}_p) := \mathrm{Hom}_{\mathbf{Z}}(\Gamma_1(Np^r)^{\mathrm{ab}}, \mathbf{Z}_p) = \mathrm{Hom}_{\mathbf{Z}_p}(\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p, \mathbf{Z}_p).$$

The ring Λ acts on $\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p$ through its quotient

$$\Lambda_r := \Lambda/\mathfrak{a}_r = \mathbf{Z}_p[\Gamma/\Gamma_r].$$

Lemma 6.1 yields an isomorphism of Λ_r-modules

$$\mathrm{Hom}_{\mathbf{Z}_p}(\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p, \mathbf{Z}_p) = \mathrm{Hom}_{\Lambda_r}(\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p, \Lambda_r).$$

If $r \geq s > 0$ then the ring Λ_s is the quotient of the ring Λ_r by the augmentation ideal $\mathfrak{a}_s$:

$$\Lambda_r \to \Lambda_r/\mathfrak{a}_s = \Lambda_s.$$

Thus we get the following sequence of morphisms of Λ_r-modules

$$\begin{aligned}\mathrm{Hom}_{\Lambda_r}(\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p, \Lambda_r) &\longrightarrow \mathrm{Hom}_{\Lambda_r}(\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p, \Lambda_r)/\mathfrak{a}_s \\ &\longrightarrow \mathrm{Hom}_{\Lambda_r}(\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p, \Lambda_s) = \mathrm{Hom}_{\Lambda_s}(\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p/\mathfrak{a}_s, \Lambda_s).\end{aligned}$$

Before we continue let us interpose a remark relating ordinary parts and duality: If M is any $\mathbf{Z}_p[U]$-module which is finitely generated as a $\mathbf{Z}_p$-module then the $\mathbf{Z}_p$-dual $M^* := \mathrm{Hom}_{\mathbf{Z}_p}(M, \mathbf{Z}_p)$ of M is also finitely generated as a $\mathbf{Z}_p$-module, and becomes a $\mathbf{Z}_p[U]$-module via the dual action of U. Clearly

$$(M^*)^{\mathrm{ord}} = (M^{\mathrm{ord}})^*,$$

that is, taking ordinary parts commutes with taking duals.

Thus we may take ordinary parts of the above diagram of homomorphisms to obtain a diagram

$$\begin{aligned}\mathrm{Hom}_{\Lambda_r}((\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}, \Lambda_r) &\longrightarrow \mathrm{Hom}_{\Lambda_r}((\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}, \Lambda_r)/\mathfrak{a}_s \\ &\longrightarrow \mathrm{Hom}_{\Lambda_s}((\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}/\mathfrak{a}_s, \Lambda_s).\end{aligned}$$

Combining this with the isomorphism

$$(\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}/\mathfrak{a}_s = (\Gamma_1(Np^s)^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}$$

of Theorem 4.1 yields the diagram

$$\begin{aligned}\mathrm{Hom}_{\Lambda_r}((\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}, \Lambda_r) &\longrightarrow \mathrm{Hom}_{\Lambda_r}((\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}, \Lambda_r)/\mathfrak{a}_s \\ &\to \mathrm{Hom}_{\Lambda_s}((\Gamma_1(Np^s)^{\mathrm{ab}} \otimes \mathbf{Z}_p{}^{\mathrm{ord}}, \Lambda_s).\end{aligned}$$

Lemma 7.1. *The morphism*

$$\mathrm{Hom}_{\Lambda_r}((\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}, \Lambda_r)/\mathfrak{a}_s \to \mathrm{Hom}_{\Lambda_s}((\Gamma_1(Np^s)^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}, \Lambda_s)$$

is an isomorphism.

Proof. The proof of this Lemma is postponed to the next section. □

Consider the chain of Λ-modules

$$\cdots \to \mathrm{Hom}_{\Lambda_r}((\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}, \Lambda_r) \to \cdots \to \mathrm{Hom}_{\mathbf{Z}_p}((\Gamma_1(Np)^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}, \mathbf{Z}_p).$$

Lemma 7.2. *There is a canonical isomorphism*

$$\mathrm{Hom}_{\Lambda}(\mathbf{W}^{\mathrm{ord}}, \Lambda) = \varprojlim_r \mathrm{Hom}_{\Lambda_r}((\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}, \Lambda_r).$$

Proof. We have the following series of canonical isomorphisms:

$$\begin{aligned}\mathrm{Hom}_{\Lambda}(\mathbf{W}^{\mathrm{ord}}, \Lambda) = \varprojlim_r \mathrm{Hom}_{\Lambda}(\mathbf{W}^{\mathrm{ord}}, \Lambda_r) &= \varprojlim_r \mathrm{Hom}_{\Lambda_r}(\mathbf{W}^{\mathrm{ord}}/\mathfrak{a}_r, \Lambda_r) \\ &= \varprojlim_r \mathrm{Hom}_{\Lambda_r}((\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}, \Lambda_r),\end{aligned}$$

where the last isomorphism follows from Corollary 5.2. This proves the Lemma. □

Lemma 7.3. *For any $r > 0$ there is a canonical isomorphism*

$$\mathrm{Hom}_{\Lambda}(W^{\mathrm{ord}}, \Lambda)/\mathfrak{a}_r = \mathrm{Hom}_{\Lambda_r}((\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}, \Lambda_r).$$

Proof. This follows from the previous two Lemmas, together with Proposition 5.1. □

Lemmas 5 and 8 imply Theorem 5.3: since any finitely generated reflexive Λ-module is free [3], it suffices to show that $\mathbf{W}^{\mathrm{ord}}$ is a reflexive Λ-module. This follows from the following series of canonical isomorphisms:

$$\begin{aligned}\mathrm{Hom}_{\Lambda}(\mathrm{Hom}_{\Lambda}(\mathbf{W}^{\mathrm{ord}}, \Lambda), \Lambda) &= \varprojlim_r \mathrm{Hom}_{\Lambda}(\mathrm{Hom}_{\Lambda}(\mathbf{W}^{\mathrm{ord}}, \Lambda), \Lambda_r) \\ &= \varprojlim_r \mathrm{Hom}_{\Lambda_r}(\mathrm{Hom}_{\Lambda}(\mathbf{W}^{\mathrm{ord}}, \Lambda)/\mathfrak{a}_r, \Lambda_r) \\ &\overset{(1)}{=} \varprojlim_r \mathrm{Hom}_{\Lambda_r}(\mathrm{Hom}_{\Lambda_r}((\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}, \Lambda_r), \Lambda_r) \\ &\overset{(2)}{=} \varprojlim_r (\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}} \overset{(3)}{=} \mathbf{W}^{\mathrm{ord}}.\end{aligned}$$

(Equality (1) follows from Lemma 7.3. Equality (2) follows from Lemma 6.2, since $(\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}$ is a free $\mathbf{Z}_p$-module and so is certainly a reflexive $\mathbf{Z}_p$-module. Equality (3) is the definition of $\mathbf{W}^{\mathrm{ord}}$.)

8. proof of Lemma 7.1

The aim of this Section is to prove Lemma 7.1, that is, to show that

$$\mathrm{Hom}_{\Lambda_r}((\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}, \Lambda_r)/\mathfrak{a}_s \to \mathrm{Hom}_{\Lambda_s}((\Gamma_1(Np^s)^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}, \Lambda_s)$$

is an isomorphism.

We begin by observing that the inclusion of groups

$$\Gamma_1(Np^r) \to \Phi_r^s$$

gives rise to the transfer

$$\Phi_r^{s\,\mathrm{ab}} \xrightarrow{V} \Gamma_1(Np^r)^{\mathrm{ab}}$$

(corresponding to pullback of cycles if one thinks of these abelianizations as homology modules).

Lemma 8.1. *The transfer morphism $V : \Phi_r^{s\,\mathrm{ab}} \to \Gamma_1(Np^r)^{\mathrm{ab}}$ commutes with the action of U on its source and target.*

Proof. It suffices to show that the following diagram (in which V is used ubiquitously to denote transfer between various abelianizations, and t denotes the matrix $\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$) commutes:

$$\begin{array}{ccc}
\Phi_r^{s\,\mathrm{ab}} & \xrightarrow{V} & \Gamma_1(Np^r)^{\mathrm{ab}} \\
\downarrow{\scriptstyle V} & & \downarrow{\scriptstyle V} \\
(\Phi_r^s \cap \Gamma^0(p))^{\mathrm{ab}} & \xrightarrow{V} & (\Gamma_1(Np^r) \cap \Gamma^0(p))^{\mathrm{ab}} \\
\downarrow{\scriptstyle t(-)t^{-1}} & & \downarrow{\scriptstyle t(-)t^{-1}} \\
\Phi_r^{s\,\mathrm{ab}} & \xrightarrow{V} & \Gamma_1(Np^r)^{\mathrm{ab}}.
\end{array}$$

The commutativity of the top square follows from the functoriality of transfer. The commutativity of the second diagram is an easy calculation: one can find coset representatives for $\Gamma_1(Np^r) \cap \Gamma^0(p)$ in $\Phi_r^s \cap \Gamma^0(p)$ of the form $\sigma_d = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, with d ranging through coset representatives of Γ_r in Γ_s. Then one computes that the conjugates $t\sigma_d t^{-1} = \begin{pmatrix} a & b/p \\ pc & d \end{pmatrix}$ form a set of coset representatives of $\Gamma_1(Np^r)$ in Φ_r^s. $\square$

By virtue of Lemma 8.1 we may restrict V to the ordinary parts of its source and target to obtain a morphism which we continue to denote by V

$$(\Phi_r^{s\,\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}} \xrightarrow{V} (\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}.$$

There is a dual morphism

$$\mathrm{Hom}_{\mathbf{Z}_p}((\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}, \mathbf{Z}_p) \xrightarrow{V^*} \mathrm{Hom}_{\mathbf{Z}_p}((\Phi_r^{s\,\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}, \mathbf{Z}_p)$$

which sits in the first column of the following commutative diagram:

$$\begin{array}{ccc}
\mathrm{Hom}_{\mathbf{Z}_p}((\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}), \mathbf{Z}_p) & \xrightarrow{\sim} & \mathrm{Hom}_{\Lambda_r}((\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}, \Lambda_r) \\
\downarrow{\scriptstyle V^*} & & \downarrow \\
\mathrm{Hom}_{\mathbf{Z}_p}((\Phi_r^{s\,\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}, \mathbf{Z}_p) & & \mathrm{Hom}_{\Lambda_r}((\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}, \Lambda_r)/\mathfrak{a}_s \\
\| & & \downarrow \\
 & & \mathrm{Hom}_{\Lambda_s}((\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}/\mathfrak{a}_s, \Lambda_s) \\
 & & \| \\
\mathrm{Hom}_{\mathbf{Z}_p}((\Gamma_1(Np^s)^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}, \mathbf{Z}_p) & \xrightarrow{\sim} & \mathrm{Hom}_{\Lambda_s}((\Gamma_1(Np^s)^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}, \Lambda_s)
\end{array}$$

in which the two horizontal isomorphisms are those provided by Lemma 6.1, and the two vertical equalities follow from Theorem 4.1 and its proof. (The commutativity of the diagram follows from a direct calculation, using the explicit formula for the isomorphism of Lemma 6.1 together with the formula for the transfer in terms of coset representatives.) Thus to prove Lemma 7.1 it suffices to prove that

$$\mathrm{Hom}_{\mathbf{Z}_p}((\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}), \mathbf{Z}_p) \xrightarrow{V^*} \mathrm{Hom}_{\mathbf{Z}_p}((\Phi_r^{s\,\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}, \mathbf{Z}_p)$$

is surjective with kernel equal to $\mathfrak{a}_s \mathrm{Hom}_{\mathbf{Z}_p}((\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}), \mathbf{Z}_p)$.

Since V commutes with U and taking ordinary parts commutes with taking $\mathbf{Z}_p$-duals,

$$\mathrm{Hom}_{\Lambda_r}((\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}, \Lambda_r) \xrightarrow{V^*} \mathrm{Hom}_{\mathbf{Z}_p}((\Phi_r^{s\,\mathrm{ab}} \otimes \mathbf{Z}_p)^{\mathrm{ord}}, \mathbf{Z}_p)$$

is the ordinary part of the morphism

$$\mathrm{Hom}_{\mathbf{Z}_p}(\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p, \mathbf{Z}_p) \xrightarrow{V^*} \mathrm{Hom}_{\mathbf{Z}_p}(\Phi_r^{s\,\mathrm{ab}} \otimes \mathbf{Z}_p, \mathbf{Z}_p).$$

Taking ordinary parts is also exact and commutes with the action of Γ; thus to prove Lemma 7.1 it suffices to show that

$$\mathrm{Hom}_{\mathbf{Z}_p}(\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p, \mathbf{Z}_p) \xrightarrow{V^*} \mathrm{Hom}_{\mathbf{Z}_p}(\Phi_r^{s\,\mathrm{ab}} \otimes \mathbf{Z}_p, \mathbf{Z}_p)$$

is surjective with kernel equal to $\mathfrak{a}_s \mathrm{Hom}_{\mathbf{Z}_p}(\Gamma_1(Np^r)^{\mathrm{ab}} \otimes \mathbf{Z}_p, \mathbf{Z}_p)$. This we now prove.

If G is any torsion-free congruence subgroup of $\mathbf{SL}(2, \mathbf{Z})$ then (letting $\mathcal{H}$ denote the Poincaré upper half-plane)

$$\mathrm{Hom}_{\mathbf{Z}_p}(G^{\mathrm{ab}} \otimes \mathbf{Z}_p, \mathbf{Z}_p) = \mathrm{Hom}_{\mathbf{Z}}(G^{\mathrm{ab}}, \mathbf{Z}_p) = H^1(Y(G), \mathbf{Z}_p)$$

is the one-dimensional cohomology module of the open Riemann surface

$$Y(G) := G \setminus \mathcal{H}$$

with coefficients in $\mathbf{Z}_p$. This curve can be completed to a compact Riemann surface $X(G)$ by the addition of finitely many points (known as the 'cusps'). Intersection of cycles yields a canonical isomorphism

$$H^1(Y(G), \mathbf{Z}_p) = H_1(X(G), \text{cusps}, \mathbf{Z}_p).$$

(The right-hand module is homology of the compact Riemann surface $X(G)$ with coefficients in $\mathbf{Z}_p$, taken relative to the set of cusps of $X(G)$.) It is well-known that the cusps correspond to the points of the orbit space $G \setminus \mathbf{P}^1(\mathbf{Q})$ and that there is a canonical isomorphism

$$H_1(X(G), \text{cusps}, \mathbf{Z}_p) = (\text{Div}^{\text{o}}(\mathbf{P}^1(\mathbf{Q})) \otimes \mathbf{Z}_p)/\mathfrak{a}_G,$$

where $\mathfrak{a}_G$ is the augmentation ideal of the group ring $\mathbf{Z}[G]$ and $\text{Div}^{\text{o}}(\mathbf{P}^1(\mathbf{Q}))$ is made a $\mathbf{Z}[G]$-module via the action of G on $\mathbf{P}^1(\mathbf{Q})$. If H is contained in G then the Riemann surfaces $Y(G)$ and $X(G)$ are respectively quotients of $Y(H)$ and $X(H)$. As above we have the transfer

$$V : G^{\text{ab}} \to H^{\text{ab}}$$

and the dual morphism

$$V^* : \text{Hom}_{\mathbf{Z}_p}(H^{\text{ab}} \otimes \mathbf{Z}_p, \mathbf{Z}_p) \to \text{Hom}_{\mathbf{Z}_p}(G^{\text{ab}} \otimes \mathbf{Z}_p, \mathbf{Z}_p).$$

This situation gives rise to the following commutative diagram:

$$\begin{array}{ccc}
\text{Hom}_{\mathbf{Z}_p}(H^{\text{ab}} \otimes \mathbf{Z}_p, \mathbf{Z}_p) & \xrightarrow{V^*} & \text{Hom}_{\mathbf{Z}_p}(G^{\text{ab}} \otimes \mathbf{Z}_p, \mathbf{Z}_p) \\
\| & & \| \\
H^1(Y(H), \mathbf{Z}_p) & \longrightarrow & H^1(Y(G), \mathbf{Z}_p) \\
\| & & \| \\
H_1(X(H), \text{cusps}, \mathbf{Z}_p) & \longrightarrow & H_1(X(G), \text{cusps}, \mathbf{Z}_p) \\
\| & & \| \\
(\text{Div}^{\text{o}}(\mathbf{P}^1(\mathbf{Q})) \otimes \mathbf{Z}_p)/\mathfrak{a}_H & \longrightarrow & (\text{Div}^{\text{o}}(\mathbf{P}^1(\mathbf{Q})) \otimes \mathbf{Z}_p)/\mathfrak{a}_G
\end{array}$$

in which the vertical arrows are (in order) the dual of the transfer, pushforward on cohomology, pushforward on homology, and the natural quotient morphism. Thus we see that V^* is surjective, with kernel equal to $\mathfrak{a}_G \,\text{Hom}_{\mathbf{Z}_p}(H^{\text{ab}} \otimes \mathbf{Z}_p, \mathbf{Z}_p)$. In particular, if we take $H = \Gamma_1(Np^r)$ and $G = \Phi_r^s$, we find that Lemma 7.1 is proved.

References

1. A. O. L. Atkin and J. Lehner, *Hecke operators on* $\Gamma_0(m)$, Math. Ann. **185** (1970), 134-160.
2. H. Hida, *Galois representations into* $\mathbf{GL}_2(\mathbf{Z}_p[[X]])$ *attached to ordinary cusp forms*, Inv. Math. **85**, 545-613.
3. J.-P. Serre, *Classes des corps cyclotomiques (d'après Iwasawa)*, Seminaire Bourbaki 174, Décembre 1958.
4. G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Iwanami Shoten, Publishers and Princeton University Press, 1971.

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109
E-mail address: emerton@math.lsa.umich.edu