Hida families of p-adic modular forms

Luca Marannino

ALGANT master thesis

Supervisor: Prof. Dr. Massimo Bertolini

UNIVERSITÀ DEGLI STUDI DI MILANO
Facoltà di scienze e tecnologie

UNIVERSITÄT DUISBURG ESSEN
Offen im Denken
Fakultät für Mathematik

Acknowledgements

I would like to thank, first of all, Prof. Massimo Bertolini for accepting to supervise me for this Master thesis. He introduced me to Hida theory and helped me with his suggestions and explanations. It will be a pleasure for me to continue to work under his guide also for my PhD.

Secondly I would like to thank Algant consortium. These two (and a half) years turned out to be an opportunity to grow up as a mathematician and - what is more important - as a person. There was no lack of difficulties, but I always felt welcomed and encouraged during the whole period. In particular I would like to thank Prof. C. Mazza (Milano's coordinator) and Prof. V. Paškūnas (Essen's coordinator) for their help.

I also want to thank Prof. F. Andreatta for his lessons in the first year in Milano and for the time he dedicated to me in the last months.

During these years I had the chance of enjoying the help and the support of many friends. I thank them heartily. In particular I would like to mention Francesco, Margherita, Bianca, Fabio and Aryaman for their special role in this adventure.

A special thank goes to Costanza, for encouraging me and standing by my side when everything seemed to go in the wrong direction.

Infine vorrei ringraziare di cuore la mia famiglia, per essermi stata accanto durante gli alti e i bassi che non sono mancati in questi anni.

Dedico questa tesi al mio caro nonno Pino. Non hai fatto in tempo a vedere questo lavoro completato, ma sicuramente continui a tifare per me da lassù.

Contents

Notation **7**

Introduction **9**

1 Hida families as Lambda-adic forms **11**
1.1 Modular forms . . . 11
1.2 Hecke operators on modular forms . . . 13
1.3 Some results in p-adic analysis . . . 16
1.4 p-adic modular forms à la Serre . . . 19
1.5 Lambda-adic forms . . . 22
1.5.1 The structure of the Iwasawa algebra . . . 22
1.5.2 Specializations . . . 23
1.5.3 Lambda-adic forms . . . 24

2 The ordinary part **27**
2.1 The ordinary projector . . . 27
2.2 Vertical control theorem . . . 30
2.3 Duality . . . 32

3 Cohomological tools **37**
3.1 Eichler-Shimura isomorphism . . . 37
3.2 Hecke operators on cohomology groups . . . 40
3.3 The proof of theorem 2.2.1 . . . 42

4 Examples of Hida families **47**
4.1 Lambda-adic Eisenstein series . . . 47
4.2 Theta series . . . 49
4.2.1 CM modular forms . . . 49
4.2.2 CM Lambda-adic forms . . . 52

5 The homological counterpart **55**
5.1 The tower of modular curves . . . 55
5.2 Hecke operators . . . 57
5.3 Ordinary parts . . . 60
5.4 Iwasawa modules . . . 62
5.5 Modules over group rings . . . 64
5.6 The final result . . . 65

A Appendix to chapter 5 **69**
A.1 Some commutative algebra 69
A.2 The proof of lemma 5.6.1 70

Notation

In this thesis we will make use of the following standard notation

- $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ will denote respectevely natural, integer, rational, real, complex numbers.
- For a rational prime p, $\mathbb{Q}_p$ denotes the field of p-adic numbers and $\mathbb{Z}_p$ the ring of p-adic integers.
- $\mathrm{GL}_2(\mathbb{R})^+$ denotes the group of invertible 2×2 matrices with real entries and positive determinant.
- $\mathrm{SL}_2(\mathbb{Z})$ is the usual modular group (2×2 matrices with integral coefficients and determinant 1).
- For $N \in \mathbb{Z}$, $N > 0$ we define

$$\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid a \equiv d \equiv 1 \mod (N), \, c \equiv b \equiv 0 \mod (N) \right\}$$

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid a \equiv d \equiv 1 \mod (N), \, c \equiv 0 \mod (N) \right\}$$

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid c \equiv 0 \mod (N) \right\}$$

- $\mathcal{H} := \{ z \in \mathbb{C} \mid \mathrm{Im}(z) > 0 \}$.

Introduction

In this thesis we want to give a systematic introduction to the so-called Hida theory of p-adic modular forms.

It is worth mentioning that the first attempt to organize modular forms in *families* where the Fourier coefficients vary p-adically continuously in the weight is due to J.P. Serre, in his celebrated paper [17], where a first possible definition of p-adic modular form is given. Almost at the same time N. Katz was developing his theory of *geometric modular forms*.

It was H. Hida in the 80's who, after a careful analysis of the corresponding Hecke algebras, proved that modular forms lived in families for varying weight and level under the so-called *ordinarity* assumption. The pivotal papers for Hida theory are [10] and [11].

Following Hida's work, A. Wiles introduced the so-called Λ-adic forms in [23] in the more general framework of Hilbert modular forms. He was able to reprove the analogues of Hida's results using this tool.

In the last 30 years many further developments and generalizations took place in this theory. Let us just mention the construction of the so-called *Eigencurve* by R. Coleman and B. Mazur.

This thesis is essentially divided into two parts.

In the first part (consisting of the first four chapters) our main reference is [9], chapter 7. Here Hida gives a more *down-to-earth* description of his theory using Wiles' language of Λ-adic forms. We tried to expand Hida's proofs and examples. The main technical difference with our reference is the introduction of a tame level N throughout our exposition, which is thus slightly more general.

In chapter 4 we give explicit examples of Λ-adic forms. In particular CM Λ-adic forms are paid a particular attention.

In the second part (chapter 5 and the relative appendix) we follow mostly M. Emerton's article [7], where he reproves Hida's horizontal control theorem in the context of homology of modular curves. The aim was again to fully understand Emerton's techniques and to expand the proofs given in the paper.

We should finally make clear that nothing is this thesis is new. We decided to give an exposition based on our understanding of our references. Our hope is that this account on Hida theory might be useful for interested math students in the future.

Chapter 1

Hida families as Lambda-adic forms

In this chapter we develop the theory of classical and p-adic modular forms (for the latter ones we follow Serre's and Hida's approach) and, after a quick review of basic concepts in p-adic analysis, we give a definition of Hida family using the so called Λ-adic modular forms (introduced by Wiles in the more general framework of Hilbert modular forms, see for instance [23]).

1.1 Modular forms

If Γ denotes the group $\Gamma(N)$, $\Gamma_1(N)$ or $\Gamma_0(N)$, then Γ has finite index in $\mathrm{SL}_2(\mathbb{Z})$. For the moment let Γ denote in general a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, i.e. a subgroup containing $\Gamma(N)$ for some $N \geq 1$.

Let $k \geq 1$ be an integer. Recall that a modular form of weight k and level Γ is a holomorphic function $f\colon \mathcal{H} \to \mathbb{C}$ satisfying the following conditions

(a) $f(\gamma\tau) = (c\tau + d)^k f(\tau)$ for every $\tau \in \mathcal{H}$ and every $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$, where $\gamma\tau = \frac{a\tau+b}{c\tau+d}$

(b) f is holomorphic at the cusps (cf. [5] pagg 16-17 for the detailed explanation of this condition)

A modular form of weight k and level Γ is called a cusp form if it vanishes at the cusps (again cf. [5] pagg 16-17).

We denote by $M_k(\Gamma)$ (resp. $S_k(\Gamma)$) the $\mathbb{C}$-vector spaces of modular (resp. cusp) forms of weight k and level Γ. One can prove that these spaces are finite dimensional and even exhibit precise dimension formulas, which heavily depend on the study of the geometry of the so-called modular curve $\Gamma\backslash\mathcal{H}$ and of its canonical compactification (cf. chapter 3 of [5] for this).

We define the so called k-slash operators. For a matrix $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{R})^+$ and a function $f\colon \mathcal{H} \to \mathbb{C}$ we define

$$(f|_k\gamma)(\tau) := (\det(\gamma))^{k-1}(c\tau + d)^{-k} f(\gamma\tau). \tag{1.1}$$

This defines an action of $\mathrm{GL}_2(\mathbb{R})^+$ on the $\mathbb{C}$-vector space of functions $f\colon \mathcal{H} \to \mathbb{C}$. In particular condition (a) above is clearly equivalent to (a') $f|_k\gamma = f$ for every $\gamma \in \Gamma$

The assigment $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto d \mod (N)$ defines a (multiplicative) group isomorphism $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^\times$ for every $N \geq 1$. This means that the group $(\mathbb{Z}/N\mathbb{Z})^\times$ acts on $M_k(\Gamma_1(N))$ and $S_k(\Gamma_1(N))$ via the k-slash operator. By standard results in representation theory this yields a decomposition of $M_k(\Gamma_1(N))$ (and similarly for cusp forms) into

$$M_k(\Gamma_1(N)) = \bigoplus_\chi M_k(\Gamma_0(N), \chi)$$

where χ runs over Dirichlet characters defined modulo N and

$$M_k(\Gamma_0(N), \chi) \coloneqq \{f \in M_k(\Gamma_1(N)) \mid f|_k\gamma = \chi(d)f \text{ for every } \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)\}$$

Define $S_k(\Gamma_0(N), \chi)$ in the obvious way and notice that if $\chi(-1) \neq (-1)^k$, then $M_k(\Gamma_0(N), \chi) = 0 = S_k(\Gamma_0(N), \chi)$

Let $f\colon \mathcal{H} \to \mathbb{C}$ be a holomorphic function with $f(\tau+1) = f(\tau)$ for all $\tau \in \mathcal{H}$. Since $\mathcal{H}/\mathbb{Z} \cong D = \{z \in \mathbb{C}^\times \mid |z| < 1\}$ via $\tau \mapsto q = \exp(2\pi i\tau)$, we may regard f as a function of q undefined at $q = 0 \leftrightarrow \tau = i\infty$. Then the Laurent expansion of f gives

$$f(\tau) = \sum_n a(n, f)q^n = \sum_n a(n, f)\exp(2\pi i n\tau) \tag{1.2}$$

This is also called the Fourier expansion (or q-expansion) of f at ∞.

Now assume $f \in M_k(\Gamma)$ for $\Gamma = \Gamma_1(N)$ or $\Gamma = \Gamma_0(N)$. In this case the matrix $T \coloneqq \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ belongs to Γ and equation (a') above reads $f(\tau+1) = f(\tau)$, so that f has a Fourier expansion at the cusp ∞. In particular f holomorphic at ∞ means that $a(n, f) = 0$ for $n < 0$ and f vanishing at ∞ means that $a(n, f) = 0$ for $n \leq 0$.

For a subring $R \subseteq \mathbb{C}$ we define the R-module

$$M_k(\Gamma_1(N), R) \coloneqq \{f \in M_k(\Gamma_1(N)) \mid a(n, f) \in R \text{ for every } n \geq 0\}$$

Similarly we define the R-modules $S_k(\Gamma_1(N), R)$, $M_k(\Gamma_0(N), \chi, R)$, $S_k(\Gamma_0(N), \chi, R)$, viewed as submodules of $R[[q]]$.

The following is a standard result in the integrality theory of modular forms

Proposition 1.1.1. *For all positive integers N and k, the space $M_k(\Gamma_1(N))$ (resp. $S_k(\Gamma_1(N))$) has a basis in $M_k(\Gamma_1(N), \mathbb{Z})$ (resp. $S_k(\Gamma_1(N), \mathbb{Z})$). For every Dirichlet character χ defined modulo N, the space $M_k(\Gamma_0(N), \chi)$ (resp. $S_k(\Gamma_0(N), \chi)$) has a basis in $M_k(\Gamma_0(N), \chi, \mathbb{Z}[\chi])$ (resp. $S_k(\Gamma_0(N), \chi, \mathbb{Z}[\chi])$)*

Proof. See [4] corollary 12.3.12. We are sweeping under the rug the discussion concerning Katz's geometric approach to modular forms. Here $\mathbb{Z}[\chi]$ denotes the smallest subring of $\mathbb{C}$ containing the values of χ. □

Corollary 1.1.2. *(a) For every subring $A \subseteq \mathbb{C}$ the natural map*

$$M_k(\Gamma_1(N), A) \otimes_A \mathbb{C} \to M_k(\Gamma_1(N))$$

is an isomorphism of $\mathbb{C}$ vector spaces (and similarly for cusp forms) *(b) For every subring $A \subseteq \mathbb{C}$ containing $\mathbb{Z}[\chi]$ the natural map*

$$M_k(\Gamma_0(N), \chi, A) \otimes_A \mathbb{C} \to M_k(\Gamma_0(N), \chi)$$

is an isomorphism of $\mathbb{C}$ vector spaces (and similarly for cusp forms)

Let p be a rational prime. We fix once and for all in this thesis an algebraic closure $\bar{\mathbb{Q}}_p$ of $\mathbb{Q}_p$ and an embedding $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$ for an algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$. All algebraic extensions of $\mathbb{Q}_p$ will be considered as subfields of $\bar{\mathbb{Q}}_p$. On $\mathbb{Q}_p$ normalize the absolute value so that $|p| = \frac{1}{p}$ and extend it to $\bar{\mathbb{Q}}_p$ in the unique possible way.

The previous results lead us to the following definition (which somehow depends on the choice of the embedding of $\bar{\mathbb{Q}}$ inside $\bar{\mathbb{Q}}_p$).

Definition 1.1.3. Let $k \geq 1$ be an integer and consider a Dirichlet character χ defined modulo N. Let A be a subring of $\bar{\mathbb{Q}}_p$. Then we can define the space of classical p-adic modular forms with coefficients in A and level N as

$$M_k(\Gamma_1(N), A) := M_k(\Gamma_1(N), \mathbb{Z}) \otimes_{\mathbb{Z}} A$$

and similarly for cusp forms.

If A contains $\mathbb{Z}[\chi]$, then we can define the space of classical p-adic modular forms with coefficients in A of level N and character χ as

$$M_k(\Gamma_0(N), \chi, A) := M_k(\Gamma_0(N), \chi, \mathbb{Z}[\chi]) \otimes_{\mathbb{Z}[\chi]} A$$

Similarly we define the corresponding cuspidal subspace.

1.2 Hecke operators on modular forms

In this section we define Hecke operators on modular forms. Let $\Gamma = \Gamma_0(N)$ for some $N \geq 1$ and fix a Dirichlet character χ modulo N. One can prove that for $\alpha \in \mathrm{GL}_2(\mathbb{Q})^+$ the orbit space $\Gamma \backslash \Gamma\alpha\Gamma$ is a finite disjoint union of left cosets, say $\Gamma\alpha\Gamma = \bigsqcup_{j=1}^{\ell} \Gamma\alpha_j$ (cf. [5] lemma 5.1.2) and that setting, for $f \in M_k(\Gamma_0(N), \chi)$,

$$f|[\Gamma\alpha\Gamma] = \sum_{j=1}^{\ell} f|_k \alpha_j$$

defines a linear operator on $M_k(\Gamma_0(N), \chi)$, only depending on the double coset $\Gamma\alpha\Gamma$.

Among these operators there are some special ones.

Lemma 1.2.1. *If p is a rational prime we have*

$$\Gamma \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma = \begin{cases} \Gamma\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) \sqcup \left(\bigsqcup_{j=0}^{p-1} \Gamma\left(\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right)\right) & \text{if } p \nmid N \\ \bigsqcup_{j=0}^{p-1} \Gamma\left(\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right) & \text{if } p \mid N \end{cases}$$

Proof. See [5] proposition 5.2.1 □

We let $T(p)$ to be the operator corresponding to $\Gamma\left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right)\Gamma$. The following proposition describes the action of the $T(p)$ operator on Fourier coefficients

Proposition 1.2.2. *Let $f \in M_k(\Gamma_0(N),\chi)$ with a Fourier expansion*

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

Then $f|T(p) \in M_k(\Gamma_0(N),\chi)$ with a Fourier expansion given by

$$(f|T(p))(\tau) = \sum_{n=0}^{+\infty} a(n,f|T(p))q^n$$

where

$$a(n,f|T(p)) = \begin{cases} a(np,f) + \chi(p)p^{k-1}a(n/p,f) & \text{if } p \nmid N \\ a(np,f) & \text{if } p \mid N \end{cases}$$

Here $a(m,f) = 0$ if $m \notin \mathbb{Z}_{\geq 0}$. Moreover if p,q are distinct primes we have that $T(p)T(q) = T(q)T(p)$.

Proof. See [5] propositions 5.2.1 and 5.2.4 □

Now we want to define an operator $T(n)$ for every $n \in \mathbb{Z}_{\geq 1}$. We let $T(1)$ be the identity map. For prime powers, define for $r \geq 2$ inductively

$$T(p^r) = \begin{cases} T(p^{r-1})T(p) - p^{k-1}\chi(p)T(p^{r-2}) & \text{if } p \nmid N \\ T(p^{r-1})T(p) & \text{if } p \mid N \end{cases}$$

Then one inductively proves that for distinct primes p and q we have $T(p^r)T(q^s) = T(q^s)T(p^r)$. This allows us to extend the definition of $T(n)$ multiplicatively as

$$T(n) = \prod_j T(p_j^{r_j}) \quad \text{if} \quad n = \prod_j p_j^{r_j}$$

so that all the $T(n)$ commute and we have

$$T(mn) = T(n)T(m) = T(m)T(n) \quad \text{if} \quad \gcd(m,n) = 1$$

Since the action of Hecke operators $T(p)$ for p a prime differs depending of the fact that p divides N or not, we will often denote by $U(p)$ the Hecke operator $T(p)$ when $p \mid N$. It follows by our definitions that $U(p^r) = U(p)^r$ for $r \geq 0$.

Proposition 1.2.3. *Let $f \in M_k(\Gamma_0(N),\chi)$ with a Fourier expansion*

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

and let n be a positive integer. Then $f|T(n) \in M_k(\Gamma_0(N),\chi)$ with a Fourier expansion given by

$$a(m,f|T(n)) = \sum_{d|\gcd(m,n)} \chi(d)d^{k-1}a(mn/d^2,d) \tag{1.3}$$

where we set $\chi(d) = 0$ if $\gcd(d,N) \neq 1$.

Proof. This follows directly from the description of the action of the $T(p)$ operators on Fourier coefficients for p a prime. See [5] proposition 5.3.1. □

As an immediate consequence of the above proposition we get that the spaces $M_k(\Gamma_0(N), \chi, \mathbb{Z}[\chi])$ and $S_k(\Gamma_0(N), \chi, \mathbb{Z}[\chi])$ are preserved by the action of the Hecke operators $T(n)$ for all $n \geq 1$.

It is more generally possible to define Hecke operators $T(n)$ on $M_k(\Gamma_1(N))$ in an analogous way. In this case it is no longer obvious that $M_k(\Gamma_1(N), \mathbb{Z})$ is preserved by the action of these Hecke operators and one has to appeal again to Katz's theory of geometric modular forms (cf. [4] proposition 12.4.1).

Now we want to define Hecke algebras.

Definition 1.2.4. For a subring A of $\mathbb{C}$ or of $\bar{\mathbb{Q}}_p$ containing $\mathbb{Z}[\chi]$, we denote by $\mathcal{H}_k(\Gamma_0(N), \chi, A)$ (resp. $\mathfrak{h}(\Gamma_0(N), \chi, A)$) the A-subalgebra of $\mathrm{End}_A(M_k(\Gamma_0(N), \chi, A)$ (resp. of $\mathrm{End}_A(S_k(\Gamma_0(N), \chi, A))$ generated by the Hecke operators $\{T(n)\}_{n\geq 1}$. We will call this rings Hecke algebras.

Remark 1.2.1. Notice that since $T(1) = \mathrm{Id}$ and all the $T(n)$ commute, we have that $\mathcal{H}_k(\Gamma_0(N), \chi, A)$ and $\mathfrak{h}(\Gamma_0(N), \chi, A)$ are commutative A-algebras with unit.

It is clear that, essentially by definition, we have

$$\mathcal{H}_k(\Gamma_0(N), \chi, A) = \mathcal{H}_k(\Gamma_0(N), \chi, \mathbb{Z}[\chi]) \otimes_{\mathbb{Z}[\chi]} A$$

and

$$\mathfrak{h}_k(\Gamma_0(N), \chi, A) = \mathfrak{h}_k(\Gamma_0(N), \chi, \mathbb{Z}[\chi]) \otimes_{\mathbb{Z}[\chi]} A$$

We need now a definition

Definition 1.2.5. Let A be a subring of $\mathbb{C}$ or of $\bar{\mathbb{Q}}_p$ with $\mathbb{Z}[\chi] \subseteq A$ and let K be the quotient field of A. We define

$$m_k(\Gamma_0(N), \chi, A) := \{f \in M_k(\Gamma_0(N), \chi, K) \mid a(n, f) \in A \text{ for all } n \geq 1\}$$

Notice that for A as above we have a pairing

$$\mathcal{H}_k(\Gamma_0(N), \chi, A) \times m_k(\Gamma_0(N), \chi, A) \to A \tag{1.4}$$

given by $(H, f) = a(1, H(f))$ for all $H \in \mathcal{H}_k(\Gamma_0(N), \chi, A)$ and $f \in m_k(\Gamma_0(N), \chi, A)$.

Clearly there is also a cuspidal version of this pairing.

Proposition 1.2.6. *The above pairing* (1.4) *is perfect and induces isomorphisms of A-modules*

$$\begin{aligned}
\mathrm{Hom}_A(\mathcal{H}_k(\Gamma_0(N), \chi, A), A) &\cong m_k(\Gamma_0(N), \chi, A)\\
\mathrm{Hom}_A(\mathfrak{h}_k(\Gamma_0(N), \chi, A), A) &\cong S_k(\Gamma_0(N), \chi, A)\\
\mathrm{Hom}_A(m_k(\Gamma_0(N), \chi, A), A) &\cong \mathcal{H}_k(\Gamma_0(N), \chi, A)\\
\mathrm{Hom}_A(S_k(\Gamma_0(N), \chi, A), A) &\cong \mathfrak{h}_k(\Gamma_0(N), \chi, A)
\end{aligned}$$

Proof. See [9] corollary 5.4.1. □

1.3 Some results in p-adic analysis

This section develops the necessary tools in p-adic analysis without proofs. The contents are mainly based on chapter 5 of [19].

For a rational prime $p > 0$ we set

$$q = \begin{cases} 4 & \text{if } p = 2 \\ p & \text{if } p \text{ odd} \end{cases} \tag{1.5}$$

We have the following classical description for the units of $\mathbb{Z}_p$, namely

Lemma 1.3.1. *Let p be a prime $p > 0$, then there is a decomposition $\mathbb{Z}_p^\times = \mu \times \Gamma$ induced by the splitting exact sequence*

$$\begin{tikzcd} 1 \arrow[r] & \Gamma \arrow[r] & \mathbb{Z}_p^\times \arrow[r] & (\mathbb{Z}/q\mathbb{Z})^\times \arrow[r] \arrow[l, bend left, dashed, "\omega"] & 1 \end{tikzcd}$$

where $\Gamma = 1 + q\mathbb{Z}_p$, μ is the maximal torsion subgroup of $\mathbb{Z}_p^\times$ ($\mu = \{\pm 1\}$ if $p = 2$ and μ given by the $p-1$-th roots of unity if p is odd) and ω is the Teichmüller character

Proof. The fact that μ is the maximal torsion subgroup of $\mathbb{Z}_p^\times$ is an easy application of Hensel's lemma. For the Teichmüller lift (when p is odd) cf. [16] proposition II.4.8. ☐

In what follows we will often see ω as the composition

$$\mathbb{Z}_p^\times \twoheadrightarrow (\mathbb{Z}/q\mathbb{Z})^\times \xrightarrow{\omega} \mathbb{Z}_p^\times$$

Consider again the fixed algebraic closure $\bar{\mathbb{Q}}_p$ of $\mathbb{Q}_p$. It is well-known that $\bar{\mathbb{Q}}_p$ is not complete, so that sometimes it is useful to work with its p-adic completion, usually denoted by $\mathbb{C}_p$. We have the following crucial fact.

Proposition 1.3.2. *$\mathbb{C}_p$ is algebraically closed.*

Proof. See [19] prop 5.2. ☐

Now we introduce the p-adic exponential and the p-adic logarithm. Set formally

$$\exp(X) = \sum_{n=0}^{+\infty} \frac{X^n}{n!} \tag{1.6}$$

One can check that

Lemma 1.3.3. *The above series converges for $\{x \in \mathbb{C}_p \mid |x| < p^{-1/(p-1)}\}$*

Proof. See [19] pag. 49. ☐

The p-adic logarithm is defined again via a formal power series

$$\log_p(X+1) = \sum_{n=1}^{+\infty} \frac{(-1)^n X^n}{n} \tag{1.7}$$

It is easy to check that in this case one has convergence for $\{x \in \mathbb{C}_p \mid |x| < 1\}$.

The properties of exponential and logarithm comes formal properties of the corresponding power series, so that they still holds over $\mathbb{C}_p$ when exponential and logarithm make sense.

Actually for the logarithm one has

Proposition 1.3.4. *There exists a unique extension of* $\log_p$ *to all of* $\mathbb{C}_p^\times$ *such that* $\log_p(p) = 0$ *and* $log_p(xy) = \log_p(x) + \log_p(y)$ *for all* $x, y \in \mathbb{C}_p^\times$

Proof. See [19] prop. 5.4. We just remark here that the crucial point in the proof is the fact that one has a decomposition $\mathbb{C}_p^\times = p^{\mathbb{Q}} \times V \times U_1$ where V is the group of all roots of unity of order prime to p in $\mathbb{C}_p^\times$ and $U_1 = \{x \in \mathbb{C}_p \mid |x-1| < 1\}$. □

Remark 1.3.1. One can check that $\log(\exp(x)) = x$ and $\exp(\log_p(1+x)) = 1+x$ hold whenever we have $|x| < p^{-1/(p-1)}$.

Now let $a \in \mathbb{Z}_p^\times$ and set $\langle a \rangle := \omega(a)^{-1}a$, so that $\langle a \rangle \equiv 1$ modulo q. One can easily see that $\log_p(a) = \log_p(\langle a \rangle)$. Thus it makes sense to define for suitable $x \in \mathbb{C}_p$

$$\langle a \rangle^x := \exp(x \log_p(a)) = \exp(x \log_p(\langle a \rangle) \tag{1.8}$$

Remark 1.3.2. Since $|\log_p(a)| \le |q| = 1/q$, we see that the above assignment makes sense whenever $|x| < qp^{-1/(p-1)}$. By the above remark we have that $\langle a \rangle^1 = \langle a \rangle$. If for p odd $n \equiv 0 \mod p-1$ (for $p = 2$ the condition is $n \equiv 0 \mod 2$), then $\langle a \rangle^n = a^n$.

Remark 1.3.3. If $a \in \Gamma = 1 + q\mathbb{Z}_p$ and u is a topological generator of Γ, then $a = u^{s(a)}$ where $s(a) := \frac{\log_p(a)}{\log_p(u)}$, due to remark 1.3.1.

Now we need more general p-adic analytic functions. We introduce the generalized binomial coefficient

$$\binom{X}{n} := \frac{X(X-1)\cdots(X-n+1)}{n!}$$

If $p(X) \in \mathbb{Q}_p(X)$ is any polynomial, one can easily check that the function $x \mapsto p(x)$ is continuous on $\mathbb{Z}_p$. Since moreover $\mathbb{N}$ is dense in $\mathbb{Z}_p$ and the $\binom{m}{n} \in \mathbb{N}$ for all $m \in \mathbb{N}$, we conclude that $\binom{x}{n} \in \mathbb{Z}_p$ for every $x \in \mathbb{Z}_p$.

A classical result due to Mahler says that one can use binomial coefficients to interpolate continuous functions $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$. More precisely

Theorem 1.3.5. *Any continuous function* $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$ *can be written uniquely in the form*

$$f(X) = \sum_{n=0}^{+\infty} a_n \binom{X}{n} \qquad \text{with } a_n \to 0 \text{ for } n \to +\infty \tag{1.9}$$

Proof. See theorem 3.2.1 in [9]. □

Example 1.3.6. Not surprisingly one can write

$$\langle a\rangle^x = (1+\langle a\rangle - 1)^x = \sum_{n=0}^{+\infty} \binom{x}{n} (\langle a\rangle - 1)^n$$

and check that the right hand side converges for $|x| < qp^{-1/(p-1)}$. This agrees with remark 1.3.2. In particular we have convergence for $|x| < 1$.

Finally recall the definitions of Bernoulli numbers and Bernoulli polynomials.

Classical Bernoulli numbers are defined in terms of a generating function

$$\frac{t}{e^t - 1} = \sum_{n=0}^{+\infty} B_n \frac{t^n}{n!} \tag{1.10}$$

Given a primitive Dirichlet character modulo N we define generalized Bernoulli numbers via

$$\sum_{a=1}^{N} \frac{\chi(a) t e^{at}}{e^{Nt} - 1} = \sum_{n=0}^{+\infty} B_{n,\chi} \frac{t^n}{e^t - 1} \tag{1.11}$$

Now we are ready to construct the p-adic L-functions that we need.

Let χ be a primitive Dirichlet character modulo N. View χ as taking values in $\mathbb{C}_p$ via the embedding $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$. It is clear that $\omega \colon \mathbb{Z}_p^\times \to \mathbb{C}_p$ is a p-adic Dirichlet character of conductor q and order $\varphi(q)$. It makes sense to consider products of characters of the form $\chi\omega^r$ for some $r \in \mathbb{Z}$ in this setting.

We have the following

Theorem 1.3.7. *Let χ be a primitive Dirichlet character modulo N and let F be such that $N \mid F$ and $q \mid F$. Then there is a p-adic meromorphic (and analytic if $\chi \neq 1$) function $L_p(s,\chi)$ on $\{s \in \mathbb{C}_p \mid |s| < qp^{-1/(p-1)}\}$ such that*

$$L_p(1-k,\chi) = -(1-\chi\omega^{-k}(p)p^{k-1}) \frac{B_{k,\chi\omega^{-k}}}{k} = (1-\chi\omega^{-k}(p)p^{k-1}) L(1-k,\chi\omega^{-k}) \qquad k \geq 1 \tag{1.12}$$

If $\chi = 1$ then $L_p(s,1)$ is analytic expect for a pole at $s=1$ with residue $1-1/p$.

In fact one has the explicit description

$$L_p(s,\chi) = \frac{1}{F(s-1)} \sum_{\substack{a=1 \\ p\nmid a}}^{n} \chi(a) \langle a\rangle^{1-s} \sum_{j=0}^{+\infty} \binom{1-s}{j} B_j \left(\frac{F}{a}\right)^j \tag{1.13}$$

Proof. See [19] theorem 5.11. □

The above function is usually called Kubota-Leopoldt p-adic L-function. We are not interested in developing the theory leading to the proof of the results of the above theorem but we need to mention that there is another construction of this function due to Iwasawa.

Definition 1.3.8. Let χ be a Dirichlet character. We say that χ is of type Γ if it factors through $\Gamma = 1 + q\mathbb{Z}_p$. Let $u = 1 + q$ and set

$$H_\chi(X) := \begin{cases} \chi(u)(1+X) - 1 & \text{if } \chi \text{ is of type } \Gamma \\ 1 & \text{otherwise} \end{cases}$$

Theorem 1.3.9. *In the above setting, there is a unique power series $G_\chi(X) \in \mathbb{Z}_p[\chi][[X]]$ such that*

$$L_p(1-s,\chi) = \frac{G_\chi(u^s-1)}{H_\chi(u^s-1)} \tag{1.14}$$

More over if ρ is a character of type Γ, then it also holds

$$G_{\chi\rho}(X) = G_\chi(\rho(u)(1+X)-1) \tag{1.15}$$

1.4 p-adic modular forms à la Serre

In this section we briefly introduce Serre's point of view on p-adic modular forms, as it was first described in [17]. We fix an odd prime p and we let v_p denote the p-adic valuation on $\mathbb{Q}_p$, normalized in such a way that $v_p(p) = 1$. If we have a formal power series

$$f = \sum_{n=0}^{+\infty} a_n q^n \in \mathbb{Q}_p[[q]]$$

we set

$$v_p(f) := \inf_{n\geq 0} v_p(a_n)$$

If $v_p(f) \geq m > 0$ for some $m \in \mathbb{Z}$, we write $f \equiv 0 \mod p^m$.

Definition 1.4.1. If $(f_j)_{j\geq 1}$ is a sequence of elements in $\mathbb{Q}_p[q]]$ we say that

$$\lim_{j\to+\infty} f_j = f \in \mathbb{Q}_p[[q]]$$

if the coefficients of f_j tend uniformly to those of f, i.e. if

$$\lim_{j\to+\infty} v_p(f-f_j) = +\infty$$

Let $m \in \mathbb{Z}$, $m \geq 1$ and set

$$X_m = (\mathbb{Z}/p^m\mathbb{Z})^\times \cong \mathbb{Z}/p^{m-1}\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}$$

For $m \to +\infty$ the X_m form a projective system of abelian groups and we have that

$$X = \varprojlim_m X_m = \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$$

where obviously $\mathbb{Z}_p$ denotes the ring of p-adic integers.

There is a canonical injective homomorphism $\mathbb{Z} \hookrightarrow X$ and one can easily see that the image of $\mathbb{Z}$ inside X is dense for the p-adic topology on X.

One can also see the elements of X as p-adic characters of $\mathbb{Z}_p^\times$. More precisely, if $V_p = \mathrm{Hom}_{cont}(\mathbb{Z}_p^\times, \mathbb{Z}_p^\times)$, then $\mathbb{Z} \hookrightarrow V_p$ via the assignment $k \mapsto (x \mapsto x^k)$ and one can extend this inclusion to a continuous homomorphisms $\varepsilon\colon X \to V_p$ (if V_p is considered with the topology of uniform convergence). One can check that ε is actually an isomorphim.

We can make things more explicit as follows. One writes $k \in X$ as $k = (s, u)$ with $s \in \mathbb{Z}_p$ and $u \in \mathbb{Z}/(p-1)\mathbb{Z}$. If $v \in \mathbb{Z}_p^\times$ is written as $v = \omega(v)\langle v \rangle$ (as in the previous section), then we have that

$$v^k := \varepsilon(k)(v) = \omega(v)^u \langle v \rangle^s$$

We say that an element $k \in X$ is even if $(-1)^k = 1$.

Definition 1.4.2. A p-adic modular form (*à la Serre*) is a formal power series

$$f = \sum_{n=0}^{+\infty} a_n q^n \in \mathbb{Q}_p[[q]]$$

such that there is a sequence $(f_j)_{j \geq 1}$ of modular forms $f_j \in M_{k_j}(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Q})$ such that

$$\lim_{j \to +\infty} f_j = f$$

There is a well-defined notion of weight for such p-adic modular forms, given by the following

Proposition 1.4.3. *Let f be a p-adic modular form, $f \neq 0$ and let $(f_j)_{j \geq 1}$ be a sequence with $f_j \in M_{k_j}(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Q})$ such that $f_j \to f$ for $j \to +\infty$. Then $\exists k \in X$ such that $k_j \to k$ for $j \to +\infty$. Such k depends on f, but not on the choice of the sequence (f_j).*

Proof. This is théorème 2 in [17]. □

If we allow $f = 0$ to be a p-adic modular form of weight $k \in X$ for any $k \in X$, we then immediately see that p-adic modular forms of a fixed weight $k \in X$ form a $\mathbb{Q}_p$-vector space.

If f is a p-adic modular form, one can prove that $v_p(f) \neq -\infty$, i.e. $p^N f \in \mathbb{Z}_p[[q]]$ for some N.

We have the following interesting result

Theorem 1.4.4. *Let $(f^{(j)})_{j \geq 1}$ be a sequence of p-adic modular forms of weight $k^{(j)} \in X$. Write*

$$f^{(j)} = \sum_{n=0}^{+\infty} a_n^{(j)} q^n$$

and assume that

(i) $a_n^{(j)}$ for $n \geq 1$ converge uniformly to $a_n \in \mathbb{Q}_p$

(ii) the weights $k^{(j)}$ converge in X to a limit $k \neq 0$

Then the $a_0^{(j)}$ have a limit $a_0 \in \mathbb{Q}_p$ and the series

$$f = \sum_{n=0}^{+\infty} a_n q^n$$

is a p-adic modular form of weight k.

Proof. This is corollaire 2 in [17]. □

We are now going to apply the above discussion to the case of Eisenstein series. Basically the above result will give us the chance of reconstructing the p-adic zeta function of Kubota-Leopoldt.

Recall that the classical family of Eisenstein series of level $\mathrm{SL}_2(\mathbb{Z})$ and variable weight $k \geq 4$ even has q-expansion

$$E_k(z) = \frac{\zeta(1-k)}{2} + \sum_{n=1}^{+\infty} \sigma_{k-1}(n) q^n \tag{1.16}$$

where $\sigma_m(n) := \sum_{d|n} d^m$. It is well-known that $E_k(z) \in M_k(\mathrm{SL}_2(\mathbb{Z}))$.

Now for $k \in X$ define

$$\sigma_k^{(p)}(n) = \sum_{\substack{d|n \\ p \nmid d}} d^k$$

One can easily check that if $(k_j)_{j\geq 1}$ is a sequence of integers such that $k_j \to k \in X$ for the p-adic topology and $k_j \to +\infty$ in the Archimedean sense, then

$$\sigma_{k_j}(n) \to \sigma_k^{(p)}(n)$$

uniformly in $n \geq 1$. As a corollary of theorem 1.4.4 we immediately get:

Corollary 1.4.5. *For $k \neq 0, k \in X$ even, there is p-adic modular form*

$$E_k^{(p)} = \frac{\zeta^{(p)}(1-k)}{2} + \sum_{n=1}^{+\infty} \sigma_k^{(p)}(n) q^n$$

where $\zeta^{(p)}(1-k) = \lim_{j\to+\infty} \zeta(1-k_j)$.

We have thus defined a function $\zeta^{(p)}$ on the odd elements of $X \smallsetminus \{0\}$. Theorem 1.4.4 also shows that this function is continuous and we claim that it is indeed essentially the same as Kubota-Leopoldt p-adic zeta function.

For $(s,u) \in X = \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$ define

$$\zeta'(s,u) = L_p(s, \omega^{1-u})$$

where L_p is the Kubota-Leopoldt p-adic L-function defined in the previous section.

We know that ζ' is continuous and that

$$\zeta'(1-k) = (1-p^{k-1})\zeta(1-k) \quad \text{if } k \in 2\mathbb{Z}, k \geq 2$$

Now if $k \in 2X$, $k \neq 0$ and if $(k_j)_{j\geq 1}$ is a sequence of integers such that $k_j \to k$ p-adically and $k_j \to +\infty$ in the Archimedean sense, we get

$$\zeta'(1-k) = \lim_{j\to+\infty} \zeta'(1-k_j) = \lim_{j\to+\infty} (1-p^{k_j-1})\zeta(1-k_j) = \lim_{j\to+\infty} \zeta(1-k_j) = \zeta^{(p)}(1-k)$$

which shows that $\zeta^{(p)} = \zeta'$.

1.5 Λ-adic forms

Now fix a prime p and a positive integer N prime to p. As before set

$$q = \begin{cases} 4 & \text{if } p = 2 \\ p & \text{if } p \text{ odd} \end{cases}$$

This notation is quite standard. No confusion with the q used for the q-expansion should arise hopefully.

Let χ be a Dirichlet character modulo Nq (considered as taking values in $\bar{\mathbb{Q}}_p$). Let $u = 1 + q \in \Gamma = 1 + q\mathbb{Z}_p$ be a fixed topological generator of Γ.

As before assume that $F/\mathbb{Q}_p$ a finite extension with $\mathbb{Z}[\chi] \subseteq F$ and let $\mathcal{O}_F$ denote the corresponding integer ring. We set $\Lambda_F = \mathcal{O}_F[[X]]$ for the usual Iwasawa algebra. Let ω denote the p-adic Teichmüller character as in the above section.

In this section we will introduce Λ-adic forms of level N and character χ. For this we will need first some results about the structure of the ring $\Lambda_F = \mathcal{O}_F[[X]]$.

1.5.1 The structure of the Iwasawa algebra

Fix $\pi \in \mathcal{O}_F$ a uniformizer and let $\mathfrak{m}_F = (\pi)$ denote the maximal ideal of the discrete valuation ring $\mathcal{O}_F$. A polynomial $p(X) \in \mathcal{O}_F[X]$ is called distinguished if it takes the form

$$p(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \qquad \text{with } \pi \mid a_i \text{ for } i = 0, \ldots, n-1$$

A classical result concerning Λ_F is the so-called Weierstraß preparation theorem.

Proposition 1.5.1. *Let $f(X) = \sum_{i=0}^{+\infty} a_i X^i \in \Lambda_F$ and assume that for some n it holds that $a_i \in \mathfrak{m}_F$ for $i = 0, \ldots, n-1$ and $a_n \notin \mathfrak{m}_F$. Then $f(X)$ may be uniquely written as $f(X) = p(X)u(X)$ with $u(X) \in \Lambda_F$ is a unit and $p(X)$ is a distinguished polynomial of degree n. More generally any nonzero element $f(X) \in \Lambda_F$ can be written uniquely as $f(X) = \pi^r p(X)u(X)$ for some $r \geq 0$ and $u(X)$, $p(X)$ as before.*

Proof. See [19] theorem 7.3. □

An important consequence of this fact is that a non-zero power series $f(X) \in \Lambda_F$ has only finitely many zeroes in the disk $\{x \in \mathbb{C}_p \mid |x| < 1\}$.

The following lemma summarizes the algebraic properties of the ring $\Lambda_F = \mathcal{O}_F[[X]]$.

Lemma 1.5.2. *Λ_F is a Noetherian local ring of Krull dimension 2. It is a UFD. Its maximal ideal is $\mathfrak{m} = (\pi, T)$. All other prime ideals have height 1. They are (π) and $(p(X))$ where $p(X) \in \mathcal{O}_F[[X]]$ is an irreducible and distinguished polynomial.*

Proof. See [19] proposition 13.9. □

Finally it is important to recall that the ring Λ_F can be realized as the topological group ring $\mathcal{O}_F[[\Gamma]]$ as follows. Let $\Gamma_r = \Gamma^{p^r}$ for $r \geq 0$ denote the unique closed subgroup of Γ of index p^r. It is clear that Γ/Γ_r is cyclic of order p^r so that there is a natural isomorphism

$$\mathcal{O}_F[\Gamma/\Gamma_r] \cong \mathcal{O}_F[X]/((1+X)^{p^r}-1)$$

for all $r \geq 0$, given by sending the fixed topological generator $u = 1+q \mod (\Gamma_r)$ to $1+X \mod ((1+X)^{p^r}-1)$.

If $r \geq s$ one has a commutative diagram with obvious arrows

$$\begin{array}{ccc} \mathcal{O}_F[\Gamma/\Gamma_r] & \xrightarrow{\sim} & \mathcal{O}_F[X]/((1+X)^{p^r}-1) \\ \downarrow & & \downarrow \\ \mathcal{O}_F[\Gamma/\Gamma_s] & \xrightarrow{\sim} & \mathcal{O}_F[X]/((1+X)^{p^s}-1) \end{array}$$

One defines $\mathcal{O}_F[[\Gamma]] = \varprojlim \mathcal{O}_F[\Gamma/\Gamma_r]$, viewed as a topological ring with the profinite topology. Taking inverse limits on the above diagram one finds an isomorphism of topological rings

$$\mathcal{O}_F[[\Gamma]] \cong \mathcal{O}_F[[X]] = \Lambda_F$$

uniquely determined by the assignment $u \mapsto 1+X$. For the proof of this fact cf. [19], theorem 7.1.

1.5.2 Specializations

An element $\varphi \in \mathrm{Hom}_{\mathcal{O}_F-alg}(\Lambda_F, \bar{\mathbb{Q}}_p)$ is called a specialization. Notice that when $p > 2$, under the isomorphism given above, there is a natural bijection between continuous group homomorphisms $\alpha\colon \Gamma \to \bar{\mathbb{Q}}_p^\times$ and $\mathcal{O}_F$-algebra homomorphisms $\varphi\colon \mathcal{O}_F \to \bar{\mathbb{Q}}_p$. In particular such an α is uniquely determined by the image of a topological generator $u = 1+p$ of Γ, which must be a principal unit in a finite extension of $\mathbb{Q}_p$ inside $\bar{\mathbb{Q}}_p$. The corresponding φ is obtained setting $\varphi(f(X)) = f(\alpha(u)-1)$ for $f \in \Lambda_F$.

Note that the kernel of a specialization φ is necessarily a height one prime ideal P_φ of Λ_F generated by an irreducible distinguished polynomial. We will also refer to such prime ideals as specializations.

Definition 1.5.3. A specialization $\varphi\colon \Lambda_F \to \bar{\mathbb{Q}}_p$ is called arithmetic if it is uniquely determined by a continuous group homomorphism $\alpha\colon \Gamma \to \bar{\mathbb{Q}}_p^\times$ such that $\alpha(\gamma) = \varepsilon(\gamma)\gamma^k$ for a finite order character $\varepsilon\colon \Gamma \to \bar{\mathbb{Q}}_p^\times$ and some $k \geq 1$. We denote by $\varphi_{k,\varepsilon}$ such a specialization. If $k \geq 2$ we say that this specialization is classical. We denote by $P_{k,\varepsilon}$ the corresponding prime ideal of Λ_F.

We have that $\varphi_{k,\varepsilon}(X) = \varepsilon(u)u^k - 1$, so that we can see $\varphi_{k,\varepsilon}$ as the evaluation of power series at $X = \varepsilon(u)u^k - 1$.

If $p > 2$ we let $r = r_\varepsilon \in \mathbb{Z}_{\geq 0}$ be such that ε has exact order p^r, i.e. it factors optimally through Γ/Γ_r where $\Gamma_r := 1 + p^{r+1}\mathbb{Z}_p$. It is easy to see that to define such an ε it is enough to fix a primitive p^r-th root of unit in $\zeta_r \in \overline{Q_p}^\times$ and set $\varepsilon(u) = \zeta_r$.

Notice also that since $\Gamma/\Gamma_r \cong \mathbb{Z}/p^r\mathbb{Z}$ in the obvious way, it is possible to view ε as a Dirichlet character modulo p^{r+1} via the decomposition

$$(\mathbb{Z}/p^{r+1}\mathbb{Z})^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/p^r\mathbb{Z})$$

and defining a suitable Dirichlet character as trivial on the first component and given by ε on the second component.

If $p = 2$ one has to ask $r \geq 1$ and fix a 2^{r-1}-th root of unit in order to carry out the analogous construction for arithmetic and classical specializations.

Let now $\mathcal{L}$ be a finite field extension of $\mathrm{Frac}(\Lambda_F)$ and let $\mathcal{I}$ be the normalization of Λ_F inside $\mathcal{L}$. By Noetherianity, we know that $\mathcal{I}$ is a finite flat Λ_F-algebra.

Definition 1.5.4. We say that an $\mathcal{O}_F$-algebra homomorphism $\varphi: \mathcal{I} \to \bar{\mathbb{Q}}_p$ is an arithmetic (resp. classical) specialization if $\varphi|_{\Lambda_F}$ is an arithmetic (resp. classical) specialization.

Notice that in the above setting if $P \subseteq \Lambda_F$ is a prime ideal, there is always a prime ideal $\mathcal{P} \subseteq \mathcal{I}$ such that $\mathcal{P} \cap \Lambda_F = P$ (from the usual going-up theorem), so that we can extend specializations to $\mathcal{I}$.

If $\varphi: \mathcal{I} \to \bar{\mathbb{Q}}_p$ is a specialization and $\mathcal{F} = \sum_{n=0}^{+\infty} a(n,\mathcal{F})q^n \in \mathcal{I}[[q]]$ then we write $\varphi(\mathcal{F})$ for the series

$$\varphi(\mathcal{F}) = \sum_{n=0}^{+\infty} \varphi(a(n,\mathcal{F}))q^n \in \bar{\mathbb{Q}}_p[[q]]$$

1.5.3 Λ-adic forms

We are now ready to define Λ_F-adic forms.

Definition 1.5.5. A formal q-expansion $\mathcal{F} = \mathcal{F}(X;q) \in \Lambda_F[[q]]$ is called a Λ_F-adic form (of tame character χ and level N) if for almost all classical specializations $\varphi_{k,\varepsilon}$ it holds that

$$\varphi_{k,\varepsilon}(\mathcal{F}) \in M_k(\Gamma_0(Nqp^{r_\varepsilon}), \varepsilon\chi\omega^{-k}, \mathcal{O}_F[\varepsilon])$$

A Λ_F-adic form $\mathcal{F}(X;q)$ is called a cusp form if

$$\varphi_{k,\varepsilon}(\mathcal{F}) \in S_k(\Gamma_0(Nqp^{r_\varepsilon}), \varepsilon\chi\omega^{-k}, \mathcal{O}_F[\varepsilon])$$

for all but finitely many classical specializations $\varphi_{k,\varepsilon}$.

We write $\mathcal{M}(N,\chi,\Lambda_F)$ (resp. $\mathcal{S}(N,\chi,\Lambda_F)$) for the space of Λ_F-adic modular forms (resp. Λ_F-adic cusp forms). It is immediate to check that $\mathcal{M}(N,\chi,\Lambda_F)$ and $\mathcal{S}(N,\chi,\Lambda_F)$ have a natural structure of Λ_F-module.

These modules (or rather their corresponding Hecke algebras) will be the main object of study in this thesis.

We have the following useful fact

Proposition 1.5.6. *With the above notation and assuming that the character ε takes values in $\mathcal{O}_F^\times$, for any $f \in M_k(\Gamma_0(Nqp^{r(\varepsilon)}), \varepsilon\chi\omega^{-k}, \mathcal{O}_F)$, there exists a Λ_F-adic form $\mathcal{F} \in \mathcal{M}(N,\chi,\Lambda_F)$ such that $\varphi_{k,\varepsilon}(\mathcal{F}) = f$. A similar result holds for cusp forms.*

Proof. We will need to consider the Λ-adic Eisenstein series which will be constructed in theorem 4.1.2. Since in that theorem the construction is given for p an odd prime, we will prove the proposition under the same assumption. With the notation of that theorem we let $\mathcal{E} = \mathcal{E}_1/A_{0,1}(X)$ (so that $\mathcal{E}(0;q) = 1$) and then we set

$$\mathcal{E}_{k,\varepsilon}(X) = \mathcal{E}(\varepsilon(u)^{-1}u^{-k}(1+X)-1) \in \Lambda_F[[q]]$$

Then $\mathcal{F} := f \cdot \mathcal{E}_{k,\varepsilon} \in \Lambda_F[[q]]$ satisfies $\varphi_{k,\varepsilon}(\mathcal{F}) = f\mathcal{E}(0;q) = f$ and one checks that for all $l \geq k$ and all finite order characters $\lambda\colon \Gamma \to \bar{\mathbb{Q}}_p^\times$ it holds

$$\varphi_{l,\lambda}(\mathcal{F}) \in M_l(\Gamma_0(Np^{r(\lambda)+1}), \lambda\chi\omega^{-l}, \mathcal{O}_F[\lambda])$$

□

We now show how to extend to Λ-adic forms the definition of Hecke operators that we saw in section 1.2. Given $\mathcal{F} \in \mathcal{M}(N,\chi,\Lambda_F)$ with q-expansion

$$\mathcal{F}(X;q) = \sum_{n=0}^{+\infty} a(n,\mathcal{F})q^n$$

we let $\mathcal{F}|T(n)$ denote the q-expansion in $\Lambda_F[[q]]$ with coefficients given by

$$a(m,\mathcal{F}|T(n)) = \sum_{d|\gcd(m,n),\gcd(d,Np)=1} \chi(d)A_d \cdot a(mn/d^2,\mathcal{F}) \tag{1.17}$$

where for every $a \in \mathbb{Z}_p^\times$ we set

$$A_a = A_a(X) = \frac{1}{a}\sum_{n=0}^{+\infty}\binom{s(\langle a\rangle)}{n}X^n \in \Lambda = \mathbb{Z}_p[[X]]$$

with the notation of remark 1.3.3.

Lemma 1.5.7. *Hecke operators defined by equation* (1.17) *are well defined, i.e. for $\mathcal{F} \in \mathcal{M}(N,\chi,\Lambda_F)$, it holds that $\mathcal{F}|T(n) \in \mathcal{M}(N,\chi,\Lambda_F)$ (and similarly for cusp forms). More precisely, if $\varphi_{k,\varepsilon}$ is a classical specialization such that $\varphi_{k,\varepsilon}(\mathcal{F}) \in M_k(\Gamma_0(Nqp^{r_\varepsilon}),\varepsilon\chi\omega^{-k},\mathcal{O}_F[\varepsilon])$, then $\varphi_{k,\varepsilon}(\mathcal{F}|T(n)) = (\varphi_{k,\varepsilon}(\mathcal{F}))|T(n)$.*

Proof. By the proof of theorem 4.1.2 (with the same notation) we get for every $d \geq 1$ it holds $A_d(\varepsilon(u)u^k - 1) = \varepsilon(d)d^{k-1}\omega^{-k}(d)$. This means that evaluating at $X = \varepsilon(u)u^k - 1$ formula (1.17) reduces to formula (1.3) for the character $\varepsilon\chi\omega^{-k}$. The assertion now follows. □

Hence we have well defined Λ_F-linear operators defined on $\mathcal{M}(N,\chi,\Lambda_F)$ and $\mathcal{S}(N,\chi,\Lambda_F)$.

Now we are going to take coefficients in extensions of Λ_F. In particular let $\mathcal{I}$ be again the normalization of Λ_F in a finite extension of $\mathrm{Frac}(\Lambda_F)$. We will need to consider such extensions to construct Hida families of CM forms in the sequel.

Definition 1.5.8. We say that a formal q-expansion $\mathcal{F} \in \mathcal{I}[[q]]$ is called an $\mathcal{I}$-adic form (of tame character χ and level N) if for almost all classical specialization $\Phi: \mathcal{I} \to \bar{\mathbb{Q}}_p$ (extending $\varphi_{k,\varepsilon}$ for some $k \geq 2$ and finite order character $\varepsilon: \Gamma \to \bar{\mathbb{Q}}_p^\times$) it holds

$$\Phi(\mathcal{F}) \in M_k(\Gamma_0(Nqp^{r_\varepsilon}, \varepsilon\chi\omega^{-k}, \bar{\mathbb{Q}}_p)$$

Analogously one defines $\mathcal{I}$-adic cusp forms.

We denote by $\mathcal{M}(N, \chi, \mathcal{I})$ (resp. $\mathcal{S}(N, \chi, \mathcal{I})$) the $\mathcal{I}$-modules of $\mathcal{I}$-adic forms (resp. $\mathcal{I}$-adic cusp forms).

It is clear that the action of Hecke operators on this $\mathcal{I}$-modules is again given by equation (1.17).

Chapter 2

The ordinary part

This chapter is dedicated to the detailed exposition of the so-called control theorems for ordinary Λ-adic forms. To avoid technicalities and to simplify the notation, we assume that p is an odd prime number in this chapter (and if necessary we even ask $p \geq 5$).

2.1 The ordinary projector

As in the previous chapters F denotes a finite extension of $\mathbb{Q}_p$ with ring of integers $\mathcal{O}_F$. The maximal ideal in $\mathcal{O}_F$ will be denoted by $\mathfrak{m}_F$ and the residue field is $\mathbb{F} = \mathcal{O}_F/\mathfrak{m}_F$.

Let us start with a result from commutative algebra.

Lemma 2.1.1. *Let A be a commutative $\mathcal{O}_F$-algebra free of finite rank over $\mathcal{O}_F$. Then for any $x \in A$ the limit $\lim_{n\to+\infty} x^{n!}$ exists in A for the $\mathfrak{m}_F$-adic topology and gives an idempotent of A.*

Proof. By the Wedderburn Principal Theorem (cf. [3] theorem 72.19), any finite dimensional algebra over a perfect field decomposes as the direct sum (as a vector space) of its nilpotent radical and a semisimple subalgebra. Now $\overline{A} := A/\mathfrak{m}_F A$ is such an algebra over $\mathbb{F}$, so that given $x \in \mathcal{A}$, its class $\overline{x} \in \overline{A}$ can be written as $\overline{x} = s + n$ for some nilpotent element n and some semi-simple element s of $\overline{A}$. If $n^{p^k} = 0$, then

$$(s+n)^{p^k} = s^{p^k} + n^{p^k} = s^{p^k}$$

is semisimple in $\overline{A}$. Hence for a sufficiently large integer b we know that $(s+n)^b = s^b = \overline{e}$ is an idempotent in $\overline{A}$ ($A/\mathfrak{m}_F A$ is a finite ring). By Hensel's lemma we can lift such an idempotent to an idempotent e of A, which is easily seen to coincide with the limit

$$\lim_{n\to+\infty} x^{n!}$$

□

Let again $\chi\colon (\mathbb{Z}/Np^{r+1}\mathbb{Z})^\times \to \mathcal{O}_F^\times$ be a Dirichlet character (where N is prime to p). In the Hecke algebra $\mathcal{H}_k(\Gamma_0(Np^{r+1}), \chi, \mathcal{O}_F)$ (resp. $\mathfrak{h}_k(\Gamma_0(Np^{r+1}), \chi, \mathcal{O}_F)$) we have the operator $T(p) = U(p)$ and thanks to the above lemma we can define

$$e := \lim_{n\to+\infty} U(p)^{n!}$$

The operator e defined above is called Hida ordinary projector.

Remark 2.1.1. If f is an eigenform of U_p with eigenvalue $\lambda \in \bar{\mathbb{Q}}_p$, it is easy to check that

$$f|e = \begin{cases} f & \text{if } |\lambda| = 1 \\ 0 & \text{if } |\lambda| < 1 \end{cases}$$

Definition 2.1.2. We say that a modular form $f \in M_k(\Gamma_0(Np^{r+1}), \chi, \mathcal{O}_F)$ is p-ordinary if $f|e = f$. We define the ordinary part of the Hecke algebras and the spaces of modular forms by

$$\mathcal{H}_k^{ord}(\Gamma_0(Np^{r+1}), \chi, \mathcal{O}_F) = e\mathcal{H}_k(\Gamma_0(Np^{r+1}), \chi, \mathcal{O}_F)$$

$$\mathfrak{h}_k^{ord}(\Gamma_0(Np^{r+1}), \chi, \mathcal{O}_F) = e\mathfrak{h}_k(\Gamma_0(Np^{r+1}), \chi, \mathcal{O}_F)$$
$$M_k^{ord}(\Gamma_0(Np^{r+1}), \chi, \mathcal{O}_F) = M_k(\Gamma_0(Np^{r+1}), \chi, \mathcal{O}_F)|e$$
$$m_k^{ord}(\Gamma_0(Np^{r+1}), \chi, \mathcal{O}_F) = m_k(\Gamma_0(Np^{r+1}), \chi, \mathcal{O}_F)|e$$
$$S_k^{ord}(\Gamma_0(Np^{r+1}), \chi, \mathcal{O}_F) = S_k(\Gamma_0(Np^{r+1}), \chi, \mathcal{O}_F)|e$$

It is clear that we can define the ordinary projector and the ordinary parts of Hecke algebras and spaces of modular forms also for level $\Gamma_1(Np^{r+1})$ where N is prime to p.

Remark 2.1.2. Since e is an idempotent we get a decomposition

$$\mathcal{H}_k(\Gamma_0(Np^{r+1}, \chi, \mathcal{O}_F) = \mathcal{H}_k^{ord}(\Gamma_0(Np^{r+1}, \chi, \mathcal{O}_F) \times (1-e)\mathcal{H}_k(\Gamma_0(Np^{r+1}, \chi, \mathcal{O}_F)$$

and one can verify that $\mathcal{H}_k^{ord}(\Gamma_0(Np^{r+1}, \chi, \mathcal{O}_F)$ is the largest algebra direct summand on which the image of $U(p)$ is a unit, while $(1-e)\mathcal{H}_k(\Gamma_0(Np^{r+1}, \chi, \mathcal{O}_F)$ is the complementary direct summand such that $U(p)$ is topologically nilpotent.

Lemma 2.1.3. *The pairing* (1.4) *restricts to ordinary parts and induces, for all* $k \geq 1$, *isomorphisms*

$$\mathrm{Hom}_{\mathcal{O}_F}(\mathcal{H}_k^{ord}(\Gamma_0(Np^{r+1}), \chi, \mathcal{O}_F), \mathcal{O}_F) \cong m_k^{ord}(\Gamma_0(Np^{r+1}), \chi, \mathcal{O}_F)$$
$$\mathrm{Hom}_{\mathcal{O}_F}(\mathfrak{h}_k^{ord}(\Gamma_0(Np^{r+1}), \chi, \mathcal{O}_F), \mathcal{O}_F) \cong S_k^{ord}(\Gamma_0(Np^{r+1}), \chi, \mathcal{O}_F)$$
$$\mathrm{Hom}_{\mathcal{O}_F}(m_k^{ord}(\Gamma_0(Np^{r+1}), \chi, \mathcal{O}_F), \mathcal{O}_F) \cong \mathcal{H}_k^{ord}(\Gamma_0(Np^{r+1}), \chi, \mathcal{O}_F)$$
$$\mathrm{Hom}_{\mathcal{O}_F}(S_k^{ord}(\Gamma_0(Np^{r+1}), \chi, \mathcal{O}_F), \mathcal{O}_F) \cong \mathfrak{h}_k^{ord}(\Gamma_0(Np^{r+1}), \chi, \mathcal{O}_F)$$

Proof. For $H \in \mathcal{H}_k(\Gamma_0(Np^{r+1}), \chi, \mathcal{O}_F)$ and $f \in m_k(\Gamma_0(Np^{r+1}), \chi, \mathcal{O}_F)$ it holds

$$(H, f|e) = a(1, f|eH)) = (eH, f)$$

and similarly in the cuspidal case. This proves the assertion. □

We want to define an idempotent on the spaces of Λ_F-adic forms in a suitable way.

Assume now that χ is a Dirichlet character modulo Np (with N prime to p as usual) and with values in $\mathcal{O}_F^\times$.

For every $k \geq 2$ we let $\mathcal{M}^k(N,\chi,\Lambda_F)$ denote the submodule of Λ_F-adic forms given by the forms $\mathcal{F} \in \mathcal{M}(N,\chi,\Lambda_F)$ such that

$$\varphi_{j,\varepsilon}(\mathcal{F}) \in M_k(\Gamma_0(Np^{r(\varepsilon)+1}), \varepsilon\chi\omega^{-j}, \mathcal{O}_F[\varepsilon])$$

for all classical specializations with $j \geq k$.

It is clear that by definition we have

$$\mathcal{M}(N,\chi,\Lambda_F) = \bigcup_{k\geq 2} \mathcal{M}^k(N,\chi,\Lambda_F) \subseteq \Lambda_F[[q]]$$

We are ready to prove the following

Theorem 2.1.4. *There exists a unique idempotent $e \in \mathrm{End}_{\Lambda_F}(\mathcal{M}(N,\chi,\Lambda_F))$ commuting with $T(n)$ for all $n \geq 1$ and such that*

$$e(\varphi_{k,\varepsilon}(\mathcal{F})) = \varphi_{k,\varepsilon}(e(\mathcal{F}))$$

for all $\mathcal{F} \in \mathcal{M}(N,\chi,\Lambda_F)$ and meaningful specializations.

Proof. We claim that for every $k \geq 2$ the map

$$\mathcal{M}^k(N,\chi,\Lambda_F) \to \prod_{j\geq k,\varepsilon} M_j(\Gamma_0(Np^{r(\varepsilon)+1}, \varepsilon\chi\omega^{-j}, \mathcal{O}_F[\varepsilon])$$

induced by specializations is injective. Indeed assume $\varphi_{j,\varepsilon_0}(\mathcal{F}) = 0$ for all $j \geq k$ (where ε_0 is the trivial character of Γ). Writing

$$\mathcal{F} = \sum_{n=0}^{+\infty} a(n,\mathcal{F})q^n$$

it would follow that $X + 1 - u^j$ divides $a(n,\mathcal{F})$ for all $j \geq k$. But Λ_F is a unique factorization domain, so that necessarily $a(n,\mathcal{F}) = 0$ for all $n \geq 0$ and $\mathcal{F} = 0$.

Since the above map is injective, the $U(p)$ operator on $\mathcal{M}^k(N,\chi,\Lambda_F)$ is induced by the product operator of $U(p)$ on each $M_j(\Gamma_0(Np^{r(\varepsilon)+1}, \varepsilon\chi\omega^{-j}, \mathcal{O}_F[\varepsilon])$, since we verified that

$$U(p)(\varphi_{j,\varepsilon}(\mathcal{F})) = \varphi_{j,\varepsilon}(U(p)(\mathcal{F}))$$

Now the limit $\lim_{n\to+\infty} U(p)^{n!}$ exists in $M_j(\Gamma_0(Np^{r(\varepsilon)+1}, \varepsilon\chi\omega^{-j}, \mathcal{O}_F[\varepsilon])$. Such an operator gives an operator on the product $\prod_{j\geq k,\varepsilon} M_j(\Gamma_0(Np^{r(\varepsilon)+1}, \varepsilon\chi\omega^{-j}, \mathcal{O}_F[\varepsilon])$ which preserves the image of $\mathcal{M}^k(N,\chi,\Lambda_F)$. We thus have a well defined idempotent e_k on $\mathcal{M}^k(N,\chi,\Lambda_F)$ which satisfies the requirements.

It is now easy to see that such idempotents e_k define an idempotent e on $\mathcal{M}(N,\chi,\Lambda_F)$ given by $\mathcal{F}|e := \mathcal{F}|e_k$ if $\mathcal{F} \in \mathcal{M}^k(N,\chi,\Lambda_F)$ for some $k \geq 2$. □

Definition 2.1.5. (i) We define $\mathcal{M}^{ord}(N,\chi,\Lambda_F) = \mathcal{M}(N,\chi,\Lambda_F)|e$ (and analogously $\mathcal{S}^{ord}(N,\chi,\Lambda_F) = \mathcal{S}(N,\chi,\Lambda_F)|e$) and we call them the space of ordinary Λ_F-adic modular forms (resp. cusp forms).

(ii) We define $\mathbf{H}^{ord}(N, \chi, \Lambda_F)$ (respectively $\mathbf{h}^{ord}(N, \chi, \Lambda_F)$) by the subalgebra of $\mathrm{End}_{\Lambda_F}(\mathcal{M}^{ord}(N, \chi, \Lambda_F))$ (resp. $\mathrm{End}_{\Lambda_F}(\mathcal{S}^{ord}(N, \chi, \Lambda_F))$ generated by all Hecke operators $T(n)$ for $n \geq 1$ over Λ_F. We call it the universal ordinary Hecke algebra of level N and character χ (resp. the universal cuspidal ordinary Hecke algebra of level N and character χ).

Notice that by the above theorem we might also define $\mathcal{M}^{ord}(N, \chi, \Lambda_F)$ (resp. $\mathcal{S}^{ord}(N, \chi, \Lambda_F)$) as the subspace of $\mathcal{M}(N, \chi, \Lambda_F)$ (resp. $\mathcal{S}(N, \chi, \Lambda_F)$) given by those Λ_F-adic forms for which almost every classical specialization is ordinary.

2.2 Vertical control theorem

In this section we state and prove the most important results concerning Λ_F-adic forms.

Theorem 2.2.1. *With the usual notation (χ is again a Dirichlet character modulo Np here), we have that for all $k \geq 2$ it holds*

$$\mathrm{Rank}_{\mathcal{O}_F} M_k^{ord}(\Gamma_0(Np), \chi\omega^{-k}, \mathcal{O}_F) = \mathrm{Rank}_{\mathcal{O}_F} M_2^{ord}(\Gamma_0(Np), \chi\omega^{-2}, \mathcal{O}_F)$$

and

$$\mathrm{Rank}_{\mathcal{O}_F} S_k^{ord}(\Gamma_0(Np), \chi\omega^{-k}, \mathcal{O}_F) = \mathrm{Rank}_{\mathcal{O}_F} S_2^{ord}(\Gamma_0(Np), \chi\omega^{-2}, \mathcal{O}_F)$$

Proof. The proof of this result is postponed to chapter 3, theorem 3.3.3. □

The proof of the following result is due to Wiles.

Theorem 2.2.2. *The Λ_F-modules $\mathcal{M}^{ord}(N, \chi, \Lambda_F)$ and $\mathcal{S}^{ord}(N, \chi, \Lambda_F)$ are Λ_F-free of finite rank.*

Proof. We just prove the assertion for $\mathcal{M} := \mathcal{M}^{ord}(N, \chi, \Lambda_F)$ because the proof for cusp forms is identical. Ley M be a finitely generated free Λ_F-submodule of $\mathcal{M}$ with basis $\{\mathcal{F}_1, \ldots, \mathcal{F}_\ell\}$. Write

$$\mathcal{F}_j = \sum_{n=0}^{+\infty} a(n, \mathcal{F}_j) q^n$$

Then there is a sequence of integers $0 \leq n_1 < \cdots < n_\ell$ such that $D = \det(A) \neq 0$ for the $\ell \times \ell$ matrix $A = [a(n_i, \mathcal{F}_j)]_{i,j}$ with coefficients in Λ_F. By Weierstraß preparation theorem (cf. proposition 1.5.1) a non-zero power series in Λ_F has only finitely many zeroes in the unit disk $\{x \in \mathbb{C}_p \mid |x| < 1\}$. There exists an integer $k \gg 2$ such that $D(u^k - 1) \neq 0$ and

$$f_j := \varphi_{k,\varepsilon_0}(\mathcal{F}_j) \in M_k^{ord}(\Gamma_0(Np), \chi\omega^{-k}, \mathcal{O}_F)$$

for all $j = 1, \ldots, \ell$. In particular this implies that $\{f_1, \ldots, f_\ell\}$ are $\mathcal{O}_F$-linearly independent. We write $\varphi_k = \varphi_{k,\varepsilon_0}$ and $P_k = P_{k,\varepsilon_0}$ in the sequel.

By the previous theorem we know that the rank of $M_k^{ord}(\Gamma_0(Np), \chi\omega^{-k}, \mathcal{O}_F)$ is bounded independently of $k \geq 2$ (cf. also corollary 3.3.2). This means that ℓ is bounded independently of the choice of M, and we can thus assume that ℓ is the maximal possible rank of Λ_F-free submodules of $\mathcal{M}$. Hence it is clear that any $\mathcal{F} \in \mathcal{M}$ can be written as

$$\mathcal{F} = \sum_{j=1}^{\ell} \alpha_j \mathcal{F}_j$$

for suitable $\alpha_j \in \mathrm{Frac}(\Lambda_F)$. These elements α_j are the solution of the linear system $A\mathbf{x} = \mathbf{a}(\mathcal{F})$ where the matrix A was described before and

$$\mathbf{a}(\mathcal{F}) = (a(n_1, \mathcal{F}), \dots, a(n_\ell, \mathcal{F}))^t$$

Multiplying on the left by the cofactor matrix of A, one easily finds that $D\alpha_j \in \Lambda_F$ for all $j = 1, \dots, \ell$, where $D = \det(A)$ as above.

This shows that $D\mathcal{M} \subseteq M$. Since $\mathcal{M}$ (being a submodule of $\Lambda_F[[q]]$) torsion-free and Λ_F is Noetherian, we deduce immediately that $\mathcal{M}$ must be a finitely generated Λ_F-module.

Now we show that $\mathcal{M}$ is actually a free Λ_F-module. Since it is finitely generated, choose $\{\Phi_1, \dots, \Phi_m\}$ a set of generators of $\mathcal{M}$. For $k \gg 2$ we have that

$$\varphi_k(\Phi_j) \in M_k^{ord}(\Gamma_0(Np), \chi\omega^{-k}, \mathcal{O}_F)$$

for all $j = 1, \dots m$. Then given $\mathcal{F} \in \mathcal{M}$ we have that $\varphi_k(\mathcal{F})$ is a linear combination of $\varphi_k(\Phi_j)$, and hence

$$\varphi_k(\mathcal{F}) \in M_k^{ord}(\Gamma_0(Np), \chi\omega^{-k}, \mathcal{O}_F)$$

If $\varphi_k(\mathcal{F}) = 0$, then $a(n, \mathcal{F})/(X + 1 - u^k) \in \Lambda_F$ for all $n \geq 0$ and we have $\mathcal{F}' = \mathcal{F}/(X + 1 - u^k) \in \mathcal{M}$. In any case $\varphi_k(\mathcal{F}') \in M_k^{ord}(\Gamma_0(Np), \chi\omega^{-k}, \mathcal{O}_F)$ by what we saw above, so $\mathcal{F} = (X + 1 - u^k)\mathcal{F}'$. This means that we have an exact sequence

$$0 \to P_k\mathcal{M} \to \mathcal{M} \to M_k^{ord}(\Gamma_0(Np), \chi\omega^{-k}, \mathcal{O}_F) \to 0$$

Now pick $\{f_1, \dots, f_r\}$ an $\mathcal{O}_F$-basis of $M_k^{ord}(\Gamma_0(Np), \chi\omega^{-k}, \mathcal{O}_F)$. By the above exact sequence we can find $\{\mathcal{F}_1, \dots, \mathcal{F}_r\}$ in $\mathcal{M}$ such that $\varphi_k(\mathcal{F}_j) = f_j$ for all $j = 1, \dots, r$. We claim that $\{\mathcal{F}_1, \dots, \mathcal{F}_r\}$ is a Λ_F-basis of $\mathcal{M}$.

Assume $\sum_{j=1}^r b_j \mathcal{F}_j = 0$ for $b_j \in \Lambda_F$.

Then $\sum_{j=1}^r \varphi_k(b_j) f_j = 0$, so that $b_j = (X + 1 - u^k)b'_j$ with $b'_j \in \Lambda_F$ for all $j = 1, \dots, r$. We thus get an equation $\sum_{j=1}^r b'_j \mathcal{F}_j = 0$. Repeating the process, we find that any power of $X + 1 - u^k$ divides b_j, so $b_j = 0$ for all $j = 1, \dots, r$ and $\{\mathcal{F}_1, \dots, \mathcal{F}_r\}$ are Λ_F-linearly independent.

We claim that $\{\mathcal{F}_1, \dots, \mathcal{F}_r\}$ also generate $\mathcal{M}$. Indeed let M be the Λ_F submodule of $\mathcal{M}$ generated by $\{\mathcal{F}_1, \dots, \mathcal{F}_r\}$ and let $\mathcal{F} \in \mathcal{M}$. Then we can find a linear combination $\mathcal{G}_0$ of $\{\mathcal{F}_1, \dots, \mathcal{F}_r\}$ such that $\mathcal{F} - \mathcal{G}_0 \in P_k\mathcal{M}$. Then $(\mathcal{F} - \mathcal{G}_0)/(X + 1 - u^k) \in \mathcal{M}$. Repeating the argument we find $\mathcal{G}_1$ such that $(\mathcal{F} - \mathcal{G}_0)/(X + 1 - u^k) - \mathcal{G}_1 \in P_k\mathcal{M}$. Continuing in this way, we get a sequence $\mathcal{G}_0, \mathcal{G}_1, \dots,$ of elements of M such that

$$\mathcal{F} \equiv \sum_{i=0}^{j} (X + 1 - u^k)^i \mathcal{G}_i \mod P_k^j$$

for all $j \geq 0$. Now write

$$\mathcal{G}_i = \alpha_{1,i}\mathcal{F}_1 + \cdots + \alpha_{r,i}\mathcal{F}_r$$

for suitable $\alpha_{n,j} \in \Lambda_F$. Then by the completeness of Λ_F, we can take limits

$$\alpha_n := \lim_{j\to+\infty}\left(\sum_{i=0}^{j}\alpha_{n,j}(X+1-u^k)^j\right) \in \varprojlim \Lambda_F/P_k^j\Lambda_F = \Lambda_F$$

for $n = 1,\ldots,r$.

Let $\mathcal{G} := \alpha_1\mathcal{F}_1 + \cdots + \alpha_r\mathcal{F}_r \in M$, so that $\mathcal{F} - \mathcal{G} \in \mathcal{M}$ is divisible by $(X+1-u^k)^i$ for all $i \geq 1$, which implies $\mathcal{G} = \mathcal{F}$.

We conclude that $M = \mathcal{M}$ and that $\mathcal{M} = \mathcal{M}^{ord}(N,\chi,\Lambda_F)$ is Λ_F-free. □

Corollary 2.2.3 (Vertical control theorem)**.** *In the above setting, if $k \geq 2$ we have isomorphisms*

$$\mathcal{M}^{ord}(N,\chi,\Lambda_F)/P_k\mathcal{M}^{ord}(N,\chi,\Lambda_F) \cong M_k^{ord}(\Gamma_0(Np),\chi\omega^{-k},\mathcal{O}_F)$$
$$\mathcal{S}^{ord}(N,\chi,\Lambda_F)/P_k\mathcal{S}^{ord}(N,\chi,\Lambda_F) \cong S_k^{ord}(\Gamma_0(Np),\chi\omega^{-k},\mathcal{O}_F)$$

induced by the specializations φ_k.

Proof. This follows immediately from the proof of the above theorem. □

2.3 Duality

We now define a pairing

$$\langle -,-\rangle\colon \mathbf{H}^{ord}(N,\chi,\Lambda_F) \times \mathcal{M}^{ord}(N,\chi,\Lambda_F) \to \Lambda_F$$

given by $\langle H,\mathcal{F}\rangle := a(1,\mathcal{F}|H)$.

Define also

$$\mathbf{m}^{ord}(N,\chi,\Lambda_F) = \{\mathcal{F} \in \mathcal{M}^{ord}(N,\chi,\Lambda_F) \otimes_{\Lambda_F} \mathrm{Frac}(\Lambda_F) \mid a(n,\mathcal{F}) \in \Lambda_F \text{ for all } n \geq 1\}$$

The main result of this section is the following:

Theorem 2.3.1. *The above pairing induces isomorphisms of Λ_F-modules:*

(i)

$$\mathrm{Hom}_{\Lambda_F}(\mathbf{H}^{ord}(N,\chi,\Lambda_F),\Lambda_F) \cong \mathbf{m}^{ord}(N,\chi,\Lambda_F)$$
$$\mathrm{Hom}_{\Lambda_F}(\mathbf{m}^{ord}(N,\chi,\Lambda_F),\Lambda_F) \cong \mathbf{H}^{ord}(N,\chi,\Lambda_F)$$

(ii)

$$\mathrm{Hom}_{\Lambda_F}(\mathbf{h}^{ord}(N,\chi,\Lambda_F),\Lambda_F) \cong \mathcal{S}^{ord}(N,\chi,\Lambda_F)$$
$$\mathrm{Hom}_{\Lambda_F}(\mathcal{S}^{ord}(N,\chi,\Lambda_F),\Lambda_F) \cong \mathbf{h}^{ord}(N,\chi,\Lambda_F)$$

In particular $\mathbf{H}^{ord}(N,\chi,\Lambda_F)$ and $\mathbf{h}^{ord}(N,\chi,\Lambda_F)$ are free of finite rank over Λ_F.

Proof. Since (i) and (ii) are proven essentially in the same way, we just prove (ii).

Write $\mathbb{K} = \mathrm{Frac}(\Lambda_F)$. To ease the notation let also $\mathcal{S}(\Lambda_F) = \mathcal{S}^{ord}(N, \chi, \Lambda_F)$ and $\mathbf{h}(\Lambda_F) = \mathbf{h}^{ord}(N, \chi, \Lambda_F)$.

Set also $\mathcal{S}(\mathbb{K}) = \mathcal{S}(\Lambda_F) \otimes_{\Lambda_F} \mathbb{K}$ and $\mathbf{h}(\mathbb{K}) = \mathbf{h}(\Lambda_F) \otimes_{\Lambda_F} \mathbb{K}$.

By theorem 2.2.2 we know that $\mathcal{S}(\Lambda_F)$ is free of finite rank over Λ_F, so that

$$\dim_{\mathbb{K}}(\mathcal{S}(\mathbb{K})) = \mathrm{rank}_{\Lambda_F}(\mathcal{S}(\Lambda_F)) < +\infty$$

which implies

$$\dim_{\mathbb{K}}(\mathbf{h}(\mathbb{K})) < +\infty$$

Notice that if we prove that the induced pairing

$$\langle -, - \rangle \colon \mathbf{h}(\mathbb{K}) \times \mathcal{S}(\mathbb{K}) \to \mathbb{K}$$

is non-degenerate, then we get isomorphisms

$$\mathrm{Hom}_{\mathbb{K}}(\mathbf{h}(\mathbb{K}), \mathbb{K}) \cong \mathcal{S}(\mathbb{K})$$

and

$$\mathrm{Hom}_{\mathbb{K}}(\mathcal{S}(\mathbb{K}), \mathbb{K}) \cong \mathbf{h}(\mathbb{K})$$

induced by the pairing (because we are working over a field).

So let $H \in \mathbf{h}(\mathbb{K})$ and assume that $\langle H, \mathcal{F} \rangle = 0$ for all $\mathcal{F} \in \mathcal{S}(\mathbb{K})$. Then

$$a_n(\mathcal{F}|H) = a_1(F|HT(n)) = a_1(F|T(n)H) = \langle H, F|T(n) \rangle = 0$$

for all $n \geq 1$. This immediately implies that $\mathcal{F}|H = 0$ (since $\mathcal{F}$ is cuspidal by assumption). Since $\mathcal{F}$ is arbitrary we deduce that $H = 0$.

Fix now $\mathcal{F} \in \mathcal{S}(\mathbb{K})$ and assume that $\langle H, \mathcal{F} \rangle = 0$ for all $H \in \mathbf{h}(\mathbb{K})$. Then in particular for all $n \geq 1$ we have

$$a_n(\mathcal{F}) = a_1(\mathcal{F}|T(n)) = \langle T(n), \mathcal{F} \rangle = 0$$

so that $\mathcal{F} = 0$ again. This proves that the scalar extension to $\mathbb{K}$ of our pairing is non-degenerate.

Now we try to work over Λ_F. Arguing as above it is easy to see that the Λ_F-module homomorphism

$$\mathcal{S}(\Lambda_F) \to \mathrm{Hom}_{\Lambda_F}(\mathbf{h}(\Lambda_F), \Lambda_F), \qquad \mathcal{F} \mapsto (H \mapsto \langle H, \mathcal{F} \rangle)$$

is injective.

Now given $\varphi \in \mathrm{Hom}_{\Lambda_F}(\mathbf{h}(\Lambda_F), \Lambda_F)$ it is immediate to extend it to a

$$\tilde{\varphi} \in \mathrm{Hom}_{\mathbb{K}}(\mathbf{h}(\mathbb{K}), \mathbb{K})$$

(just set $\tilde{\varphi}(H) = \varphi(H)$ for every $H \in \mathbf{h}(\Lambda_F)$ and extend $\mathbb{K}$-linearly).

By what was proven above, there is $\mathcal{F} \in \mathcal{S}(\mathbb{K})$ such that

$$\tilde{\varphi}(H) = \langle H, \mathcal{F} \rangle$$

for every $H \in \mathbf{h}(\mathbb{K})$. In particular

$$a_n(\mathcal{F}) = a_1(\mathcal{F}|T(n)) = \langle T_n, \mathcal{F}\rangle = \tilde{\varphi}(T(n)) = \varphi(T(n)) \in \Lambda_F$$

for all $n \geq 1$, so that indeed $\mathcal{F} \in \mathcal{S}(\Lambda_F)$ as we wished to prove.

Finally we have to prove that the Λ_F-module homomorphism

$$\mathbf{h}(\Lambda_F) \xrightarrow{\alpha} \mathrm{Hom}_{\Lambda_F}(\mathcal{S}(\Lambda_F), \Lambda_F), \qquad H \mapsto (\mathcal{F} \mapsto \langle H, \mathcal{F}\rangle)$$

is an isomorphism. Again injectivity follows arguing as we did while working over $\mathbb{K}$. For surjectivity we have to work a bit more in this case.

Since from now on we will just work over Λ_F, we simplify the notation setting $\mathbf{h} = \mathbf{h}(\Lambda_F)$ and $\mathcal{S} = \mathcal{S}(\Lambda_F)$. For a Λ_F-module M we will write M^* to denote its Λ_F-dual, i.e.

$$M^* = \mathrm{Hom}_{\Lambda_F}(M, \Lambda_F)$$

In particular we have proven that $\mathcal{S} \cong \mathbf{h}^*$ via our pairing.

We can thus interpret α as the canonical morphism

$$\mathbf{h} \to \mathbf{h}^{**} = \mathrm{Hom}_{\Lambda_F}(\mathbf{h}^*, \Lambda_F), \qquad H \mapsto (\varphi \mapsto \varphi(H))$$

and we know that it is injective. Since $\mathbf{h}^{**}$ is free of finite rank over Λ_F, we deduce that $\mathbf{h}$ is torsion-free as Λ_F module. In particular for any height one prime ideal $\wp$ of Λ_F we get that the localization $\mathbf{h}_\wp$ is free of finite rank over $(\Lambda_F)_\wp$ (which is a discrete valuation ring).

Let $\mathbf{N} = \mathrm{Coker}(\alpha)$. Since localization is exact and free modules are reflexive (canonically isomorphic to their double dual), we immediately deduce that for any height one prime ideal $\wp$ of Λ_F it holds that $\mathbf{N}_\wp = 0$, i.e. $\mathbf{N}$ is a so-called pseudo-null Λ_F-module. It is well-known (cf. [14], remark 4 page 269) that pseudo-null Λ_F modules are finite, so that our $\mathbf{N}$ is finite.

Since $\mathbf{h}^{**}$ is Λ_F-free, then $\mathbf{h}^{***} \cong \mathcal{S}$. Thus we have the following chain of isomorphims for $k \geq 2$.

$$\begin{aligned}\mathrm{Hom}_{\mathcal{O}_F}(\mathbf{h}^{**}/P_k\mathbf{h}^{**}, \mathcal{O}_F) \cong \mathcal{S}/P_k\mathcal{S} \cong \mathcal{S}_k^{ord}(\Gamma_0(Np), \chi\omega^{-k}, \mathcal{O}_F) \cong \\ \cong \mathrm{Hom}_{\mathcal{O}_F}(\mathfrak{h}_k^{ord}(\Gamma_0(Np), \chi\omega^{-k}, \mathcal{O}_F), \mathcal{O}_F)\end{aligned}$$

where $P_k = (X + 1 - (1+p)^k)$ as usual.

The first isomorphisms follows from the fact that $\mathbf{h}^{**}$ is free over Λ_F. The second isomorphism is the control theorem 2.2.3. Finally the third isomorphism is the duality of lemma 2.1.3.

Tensoring the exact sequence

$$0 \to \mathbf{h} \to \mathbf{h}^{**} \to \mathbf{N} \to 0$$

with $\mathcal{O}_F = \Lambda_F/P_k\Lambda_F$ we obtain an exact sequence

$$\mathrm{Tor}^1_{\Lambda_F}(\mathbf{N}, \mathcal{O}_F) \to \mathbf{h}/P_k\mathbf{h} \to \mathbf{h}^{**}/P_k\mathbf{h}^{**} \to \mathbf{N}/P_k\mathbf{N}$$

Notice that tensoring with $\mathbf{N}$ the exact sequence

$$0 \to \Lambda_F \xrightarrow{\cdot(X+1-(1+p)^k)} \Lambda_F \to \mathcal{O}_F \to 0$$

we get that $\mathrm{Tor}^1_{\Lambda_F}(\mathbf{N}, \mathcal{O}_F) \hookrightarrow \mathbf{N}$, so that $\mathrm{Tor}^1_{\Lambda_F}(\mathbf{N}, \mathcal{O}_F)$ is itself a finite Λ_F-module.

Thus we have another exact sequence

$$0 \mapsto \mathfrak{h}^{ord}_k(\Gamma_0(Np), \chi\omega^{-k}, \mathcal{O}_F) \to \mathbf{h}^{**}/P_k\mathbf{h}^{**} \to \mathbf{N}/P_k\mathbf{N} \to 0$$

Indeed the image of $\mathbf{h}/P_k\mathbf{h}$ inside the $\mathcal{O}_F$-free algebra $\mathbf{h}^{**}/P_k\mathbf{h}^{**}$ is generated by the Hecke operators $T(n)$ for $n \geq 1$. Taking $\mathcal{O}_F$-duals (again we use lemma 2.1.3) in the above exact sequence we find

$$0 \to \mathrm{Hom}_{\mathcal{O}_F}(\mathbf{h}^{**}/P_k\mathbf{h}^{**}, \mathcal{O}_F) \to S^{ord}_k(\Gamma_0(Np), \chi\omega^{-k}, \mathcal{O}_F) \to \mathrm{Ext}^1_{\mathcal{O}_F}(\mathbf{N}/P_k\mathbf{N}, \mathcal{O}_F) \to 0$$

and since $\mathcal{O}_F$ is a discrete valuation ring and $\mathbf{N}/P_k\mathbf{N}$ is a torsion module, we have that

$$\mathrm{Ext}^1_{\mathcal{O}_F}(\mathbf{N}/P_k\mathbf{N}, \mathcal{O}_F) \cong \mathbf{N}/P_k\mathbf{N}$$

At the same time it is easy to see that the arrow

$$\mathrm{Hom}_{\mathcal{O}_F}(\mathbf{h}^{**}/P_k\mathbf{h}^{**}, \mathcal{O}_F) \to S^{ord}_k(\Gamma_0(Np), \chi\omega^{-k}, \mathcal{O}_F)$$

is the isomorphism that was proven above, so that

$$0 = \mathrm{Ext}^1_{\mathcal{O}_F}(\mathbf{N}/P_k\mathbf{N}, \mathcal{O}_F) \cong \mathbf{N}/P_k\mathbf{N}$$

Now we can apply Nakayama's lemma to conclude that $\mathbf{N} = 0$, showing that $\mathbf{h} \cong \mathrm{Hom}_{\Lambda_F}(\mathcal{S}, \Lambda_F)$ as we wished to prove. $\square$

The interpolation property for the Hecke algebras is now immediate.

Corollary 2.3.2. *In the above setting, for all $k \geq 2$ there are isomorphisms of $\mathcal{O}_F$-algebras, sending $T(n)$ to $T(n)$ for all $n \geq 1$:*

$$\mathbf{H}^{ord}(N, \chi, \Lambda_F)/P_k\mathbf{H}^{ord}(N, \chi, \Lambda_F) \cong \mathcal{H}^{ord}_k(\Gamma_0(Np), \chi\omega^{-k}, \mathcal{O}_F)$$

$$\mathbf{h}^{ord}(N, \chi, \Lambda_F)/P_k\mathbf{h}^{ord}(N, \chi, \Lambda_F) \cong \mathfrak{h}^{ord}_k(\Gamma_0(Np), \chi\omega^{-k}, \mathcal{O}_F)$$

Chapter 3

Cohomological tools

3.1 Eichler-Shimura isomorphism

In this section we introduce the cohomological tools which are needed for the proofs of the structure theorems in Hida theory and we state without proof the classical Eichler-Shimura isomorphism.

Let Γ be a group, let R be a commutative unitary ring and let M be any left $R[\Gamma]$-module. Then we define group cohomology of M with coefficients in R in the usual way as

$$H^i(\Gamma, M) = \mathrm{Ext}^i_{R[\Gamma]}(R, M) \tag{3.1}$$

The functors $(H^i(\Gamma, -))_n \geq 0$ form a universal cohomological δ-functor in the sense of [20], pages 30-32. We will use freely the properties of δ-functors in what follows to get long exact sequences in cohomology and induced morphisms in cohomology. A standard reference for this facts is again [20], chapters 1,2, 3 and 6.

Practically, we also adopt the explicit description of $H^i(\Gamma, M)$ in terms of the standard *Bar* resolution of inhomogeneous cochains (i.e. the usual description in terms of cocycles and coboundaries, cf. [20] section 6.5).

This means that we will consider for $i \geq 0$

$$\mathcal{C}^i(\Gamma, M) = \{f : \Gamma^i \to M \mid f \text{ function}\}$$

(where we set $\mathcal{C}^0(\Gamma, M) = M$) with differentials

$$\partial^i : \mathcal{C}^i(\Gamma, M) \to \mathcal{C}^{i+1}(\Gamma, M)$$

given by $\partial^0 m(\gamma) = (\gamma - 1)m$ for $m \in M$ and $\gamma \in \Gamma$ and by

$$\partial^i f(\gamma_1, \dots \gamma_{i+1}) =$$
$$= \gamma_1 f(\gamma_2, \dots, \gamma_{i+1}) + \left(\sum_{j=1}^{i} (-1)^j f(\gamma_1, \dots, \gamma_j\gamma_{j+1}, \dots, \gamma_{i+1})\right) + (-1)^{i+1} f(\gamma_1, \dots, \gamma_i)$$

for $i \geq 1$, $f \in \mathcal{C}^i(\Gamma, M)$ and $\gamma_1, \dots \gamma_{i+1} \in \Gamma$.

As usual one can identify $H^i(\Gamma, M) = Z^i(\Gamma, M)/B^i(\Gamma, M)$ where

$$Z^i(\Gamma, M) := \mathrm{Ker}(\partial_i) \qquad B^i(\Gamma, M) := \mathrm{Im}(\partial_{i-1})$$

are respectively the submodules of i-cocycles and i-coboundaries.

Lemma 3.1.1. *The following holds:*

(i)
$$H^0(\Gamma, M) = M^\Gamma = \{x \in M \mid \gamma x = x \text{ for all } \gamma \in \Gamma\} \cong \mathrm{Hom}_{R[\Gamma]}(R, M)$$

(ii) If Γ *acts trivially on* M *then* $H^1(\Gamma, M) = \mathrm{Hom}(\Gamma, M) = \mathrm{Hom}(\Gamma^{Ab}, M)$

Proof. This is an easy exercise. □

In particular this means that $H^i(\Gamma, -)$ compute also the right derived functors of the functor $M \mapsto M^\Gamma$ (which is easily seen to be left-exact).

Given a group homomorphism $\varphi: \Gamma_1 \to \Gamma_2$, there is an induced natural transformation $H^0(\Gamma_2, -) \to H^0(\Gamma_1, -)$. By universality, this implies that we have the so called restriction morphisms

$$\mathrm{Res}^n: H^n(\Gamma_2, M) \to H^n(\Gamma_1, M)$$

functorially in M for every $R[\Gamma_2]$-module M. One can easily see that at the level of inhomogeneous cochains these morphisms are essentially given by the precomposition with φ.

Assume now that $\Gamma_1 \leq \Gamma_2$ is a subgroup of finite index. Then the norm

$$N_{\Gamma_2/\Gamma_1}(-) = \sum_{j=1}^{n} \gamma_j \cdot (-)$$

where $\{\gamma_1, \dots, \gamma_h\}$ is a system of representatives of Γ_2/Γ_1 gives a natural transformation $H^0(\Gamma_1, -) \to H^0(\Gamma_2, -)$ where $(-)$ is an $R[\Gamma_2]$-module. By universality we obtain the so-called corestriction maps

$$\mathrm{Cores}^n: H^n(\Gamma_1, -) \to H^n(\Gamma_2, -)$$

Again one can find a suitable description of this morphisms in terms of inhomogeneous cochains.

Lemma 3.1.2. *In the above setting we have that* $\mathrm{Cores}^n \circ \mathrm{Res}^n$ *equals the multiplication by* $[\Gamma_2 : \Gamma_1]$ *for all* $n \geq 0$.

Proof. This is clear for $n = 0$ and it follows then for all $n \geq 1$ by universality. □

We want to apply the machinery of group cohomology in the following setting. Let X be a compact Riemann surface and let S a finite set of points in X. Let $Y = X \setminus S$ and we let Γ to be the fundamental group of Y with respect to a fixed base point $y \in Y$.

More specifically we will consider the case where Γ is a torsion-free congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, X is the compactification of the modular curve $Y(\Gamma) = \Gamma \backslash \mathcal{H}$ and S is the set of cusps for Γ.

For every $s \in S$ let $\Gamma_s = \{\gamma \in \Gamma \mid \gamma(s) = s\}$ be the stabilizer of s in Γ.

Definition 3.1.3. We define the parabolic cohomology group $H^1_P(\Gamma, M)$ as the kernel of the map

$$\phi_P \colon H^1(\Gamma, M) \to \bigoplus_{s \in S} H^1(\Gamma_s, M)$$

where ϕ_P is induced by the restrictions $\mathrm{Res}_s \colon H^1(\Gamma, M) \to H^1(\Gamma_s, M)$

One can verify that in terms of cocycles and coboundaries we have an identification

$$H^1_P(\Gamma, M) = Z^1_P(\Gamma, M)/B^1(\Gamma, M)$$

where

$$Z^1_P(\Gamma, M) = \{f \in Z^1(\Gamma, M) \mid f(\pi) \in (\pi - 1)M \text{ for all } \pi \in P\}$$

and P is the set of all Γ-conjugates of π_s for $s \in S$ where π_s is (the class of) a loop around s.

Again let R be a commutative ring with identity and let $V_n(R)$ be the space of homogeneous polynomials of degree n with two indeterminates X and Y. We let the semigroup $\mathrm{Mat}_2(\mathbb{Z})_{\neq 0} := \mathrm{Mat}_2(\mathbb{Z}) \cap \mathrm{GL}_2(\mathbb{Q})$ act on $V_n(R)$ by

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot P(X, Y) := P((X, Y)\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)) = P(aX + cY, bX + dY)$$

Let now $\chi \colon (\mathbb{Z}/N\mathbb{Z})^\times \to R^\times$ be a Dirichlet character. We denote by R^χ the $R[\Gamma_0(N)]$-module which is defined to be R with the action of $\Gamma_0(N)$ given by

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right).r = \chi(d)r$$

for $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$ and $r \in R$. One can readily check the setting

$$(f \otimes r).\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) := (f|_k\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)) \otimes \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right).r$$

makes $M_k(\Gamma_1(N)) \otimes_{\mathbb{C}} \mathbb{C}^\chi$ into a right $\Gamma_0(N)$-module and actually that

$$M_k(\Gamma_0(N), \chi) = (M_k(\Gamma_1(N)) \otimes_{\mathbb{C}} \mathbb{C}^\chi)^{(\mathbb{Z}/N\mathbb{Z})^\times}$$

and similarly for cusp forms.

Finally let $V_n^\chi(R) := V_n(R) \otimes_R R^\chi$ with the diagonal $\Gamma_0(N)$ action.

We are interested in computing group cohomology for the modules $V_n(R)$. For higher degrees we have the following important general result:

Proposition 3.1.4. *Let Γ be a torsion-free congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and let M be any Γ-module. Then $H^2(\Gamma, M) = 0$*

Proof. See proposition 6.1.1 in [9]. □

Now let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. Fix $z_0, z_1 \in \mathcal{H}$ and for $f \in M_k(\Gamma)$ with $k \geq 2$ and $g, h \in \mathrm{SL}_2(\mathbb{Z})$ define

$$I_f(gz_0, hz_0) := \int_{gz_0}^{hz_0} f(z)(Xz + Y)^{k-2} dz \in V_{k-2}(\mathbb{C})$$

and

$$I_{\bar{f}}(gz_0, hz_0) := \int_{gz_0}^{hz_0} \overline{f(z)}(X\bar{z} + Y)^{k-2} d\bar{z} \in V_{k-2}(\mathbb{C})$$

We have the following crucial theorem

Theorem 3.1.5 (Eichler-Shimura isomorphism)**.** *Let $k \geq 2$ and Γ a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, and fix $z_0, z_1 \in \mathcal{H}$. Then the map*

$$\begin{aligned} M_k(\Gamma) \oplus \overline{S_k(\Gamma)} &\to H^1(\Gamma, V_{k-2}(\mathbb{C})) \\ (f, \bar{g}) &\mapsto (\gamma \mapsto I_f(z_0, \gamma z_0) + I_{\bar{g}}(z_1, \gamma z_1)) \end{aligned}$$

is a well-defined isomorphism of $\mathbb{C}$-vector spaces (called Eichler-Shimura map), not depending on the choice of z_0, z_1. Moreover the above map restricts to an isomorphism

$$S_k(\Gamma) \oplus \overline{S_k(\Gamma)} \to H^1_P(\Gamma, V_{k-2}(\mathbb{C}))$$

Proof. See [22] proposition 6.2.3 and theorem 6.4.1 □

One can then easily get some corollaries from the above result

Corollary 3.1.6. *Let $N \geq 1$, $k \geq 2$ and $\chi\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a Dirichlet character. Then the Eichler-Shimura map gives isomorphisms*

$$M_k(\Gamma_0(N), \chi) \oplus \overline{S_k(\Gamma_0(N), \chi)} \cong H^1(\Gamma_0(N), V^\chi_{k-2}(\mathbb{C}))$$

and

$$S_k(\Gamma_0(N), \chi) \oplus \overline{S_k(\Gamma_0(N), \chi)} \cong H^1_P(\Gamma_0(N), V^\chi_{k-2}(\mathbb{C}))$$

Proof. See [22] corollary 7.4.1. □

Corollary 3.1.7. *For $\Gamma = \Gamma_1(N)$ the map*

$$\begin{aligned} S_k(\Gamma, \mathbb{C}) &\to H^1_P(\Gamma, V_{k-2}(\mathbb{R})) \\ f &\mapsto (\gamma \mapsto \mathrm{Re}(I_f(z_0, \gamma z_0))) \end{aligned}$$

is an isomorphism and a similar result holds in presence of a Dirichlet character.

Proof. See [22] corollary 7.4.2. □

3.2 Hecke operators on cohomology groups

For a positive integer N define

$$\Delta^n_1(N) \coloneqq \{\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{Z}) \mid a \equiv 1 \mod (N), c \equiv 0 \mod (N), \det \alpha = n\}$$

and let

$$\Delta \coloneqq \Delta_1(N) \coloneqq \bigcup_{n \geq 1} \Delta^n_1(N)$$

From now on $\Gamma \coloneqq \Gamma_1(N)$.

For all $\alpha \in \Gamma$, set $\Gamma_\alpha \coloneqq \Gamma \cap \alpha^{-1}\Gamma\alpha$ and $\Gamma^\alpha \coloneqq \Gamma \cap \alpha\Gamma\alpha^{-1}$. It is easy to see that $[\Gamma : \Gamma_\alpha]$ and $[\Gamma : \Gamma^\alpha]$ are finite in this case.

For a matrix $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{Z}) \cap \mathrm{GL}_2(\mathbb{Q})$ set

$$\alpha^\iota = \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right) = \det(\alpha) \cdot \alpha^{-1}$$

Definition 3.2.1. Let $\alpha \in \Delta$ and let V be a left $R[\Gamma]$-module for some commutative ring R, such that the Γ-action extends to a semi-group action by the semi-group consisting of all α^ι for $\alpha \in \Delta$. The Hecke operator τ_α acting on group cohomology is the composition

$$\tau_\alpha : H^1(\Gamma, V) \xrightarrow{Res} H^1(\Gamma^\alpha, V) \xrightarrow{conj_\alpha} H^1(\Gamma_\alpha, V) \xrightarrow{Cores} H^1(\Gamma, V)$$

where for a cocycle $c \in H^1(\Gamma^\alpha, V)$ we set

$$conj_\alpha(c)(g_\alpha) := \alpha^\iota \cdot c(\alpha g_\alpha \alpha^{-1})$$

One can check via some computations that τ_α restricts to an operator on the parabolic subspace.

One has the following explicit description of τ_α.

Proposition 3.2.2. *Let $\alpha \in \Delta$ and suppose that $\Gamma\alpha\Gamma = \bigsqcup_{i=1}^n \Gamma\delta_i$. Then the Hecke operator τ_α acts on $H^1(\Gamma, V)$ and $H^1_P(\Gamma, V)$ sending $c \in H^1(\Gamma, V)$ to $\tau_\alpha(c)$, which is the class of the cocycle satisfying*

$$(\tau_\alpha(c))(g) = \sum_{i=1}^n \delta_i^\iota \cdot c(\delta_i g \delta_{\sigma_g(i)}^{-1})$$

for all $g \in \Gamma$, where $\sigma_g(i)$ is the index such that $\delta_i g \delta_{\sigma_g(i)}^{-1} \in \Gamma$.

Proof. See [22] proposition 7.3.2. □

More generally one can extend the definition of the Hecke operators τ_α on higher cohomology groups as follows (cf [12], pagg. 114-116). Assume again that $\Gamma\alpha\Gamma = \bigsqcup_{i=1}^n \Gamma\delta_i$. Given a q-cocycle c (viewed as a function $c : \Gamma^q \to M$) we set

$$(\tau_\alpha(c))(g_1, \dots, g_q) = \sum_{i=1}^n \delta_i^\iota \cdot c(\xi_i(g_1), \xi_{i(g_1)}(g_2), \dots, \xi_{i(g_1 g_2 \cdots g_{q-1})}(g_q))$$

where for all $i = 1, \dots n$ and for all $g \in \Gamma$ we set

$$\delta_i g = \xi_i(g)\alpha_{i(g)}$$

One can check that this induces a well-defined R-linear map on cohomology groups.

For a positive integer n, the Hecke operator T_n is defined as $\sum_\alpha \tau_\alpha$ where the sum runs through a set of representatives of the double coset in the quotient $\Gamma\backslash\Delta^n/\Gamma$. In particular if p is a prime number we have that $T_p = \tau_{\alpha_p}$ where $\alpha_p = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$.

In particular given a Γ-module V which is invariant under the action of α_p^ι, it is possible to define and apply the $T(p)$ operator on $H^i(\Gamma, M)$. This will happen in the sequel.

3.3 The proof of theorem 2.2.1

We start with the following crucial result.

Theorem 3.3.1 (Cf. theorem 7.2.2 in [9]). *Let $p \geq 3$ be a prime number and N be an integer prime to p. Then the integer* $\mathrm{rank}_{\mathbb{Z}_p}(S_k^{\mathrm{ord}}(\Gamma_1(Np^{r+1}), \mathbb{Z}_p))$ *is bounded independently of k if $k \geq 2$ and $r \geq 0$.*

Proof. Write $\Gamma = \Gamma_1(Np^{r+1})$. Let L be the intersection between the image of $H^1(\Gamma, V_{k-2}(\mathbb{Z}))$ in $H^1(\Gamma, V_{k-2}(\mathbb{R}))$ with $H^1_P(\Gamma, V_{k-2}(\mathbb{R}))$.

Then $L \otimes_{\mathbb{Z}} \mathbb{R} = H^1_P(\Gamma, V_{k-2}(\mathbb{R}))$ and $\mathfrak{h}_k(\Gamma, \mathbb{Z})$ is by definition a commutative subalgebra of $\mathrm{End}_{\mathbb{Z}}(L)$ which is free of finite rank over $\mathbb{Z}$. Let now $L_p = L \otimes_{\mathbb{Z}} \mathbb{Z}_p$, so that $\mathfrak{h}_k(\Gamma, \mathbb{Z}_p) = \mathfrak{h}_k(\Gamma, \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is a subalgebra of $\mathrm{End}_{\mathbb{Z}_p}(L_p)$. It is possible to attach to the operator $U(p) = T(p) \in \mathfrak{h}_k(\Gamma, \mathbb{Z}_p)$ an idempotent e, as described in lemma 2.1.1, so that it makes sense to consider $\mathfrak{h}_k^{ord}(\Gamma, \mathbb{Z}_p)$ as a subalgebra of $\mathrm{End}_{\mathbb{Z}_p}(L_p^{ord})$ where $L_p^{ord} = L_p|e$

Since

$$\mathrm{rank}_{\mathbb{Z}_p}(S_k^{ord}(\Gamma, \mathbb{Z}_p)) = \mathrm{rank}_{\mathbb{Z}_p}(\mathfrak{h}_k^{ord}(\Gamma, \mathbb{Z}_p))$$

by duality, in order to prove our thesis it is enough to prove that $\mathrm{rank}_{\mathbb{Z}_p}(L_p^{ord})$ is bounded independently on k.

Let L' denote the image of $H^1(\Gamma, V_{k-2}(\mathbb{Z}))$ in $H^1(\Gamma, V_{k-2}(\mathbb{R}))$. Note that $L/pL = L_p/pL_p$ and that L/pL injects into L'/pL', which is by definition a surjective image of $H^1(\Gamma, V_{k-2}(\mathbb{Z})) \otimes_{\mathbb{Z}} \mathbb{Z}/p\mathbb{Z}$.

Now set $n = k - 2$. We have an exact sequence of Γ-modules (where $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$)

$$0 \to V_n(\mathbb{Z}) \xrightarrow{p} V_n(\mathbb{Z}) \to V_n(\mathbb{F}_p) \to 0$$

yielding a long exact sequence in cohomology

$$\cdots \to H^1(\Gamma, V_n(\mathbb{Z})) \xrightarrow{p} H^1(\Gamma, V_n(\mathbb{Z})) \to H^1(\Gamma, V_n(\mathbb{F}_p)) \to \dots$$

This implies that $H^1(\Gamma, V_n(\mathbb{Z})) \otimes_{\mathbb{Z}} \mathbb{F}_p$ can be embedded in $H^1(\Gamma, V_n(\mathbb{F}_p))$.

By what we said above in order to prove our thesis is enough to prove that the $\mathbb{F}_p$-dimension of $H^1_{ord}(\Gamma, V_n(\mathbb{F}_p)) = H^1(\Gamma, V_n(\mathbb{F}_p))|e$ is bounded independently on n.

To prove this we will construct an isomorphism between $H^1_{ord}(\Gamma, V_n(\mathbb{F}_p))$ and $H^1_{ord}(\Gamma, \mathbb{F}_p)$.

Given $P(X,Y) = \sum_{i=0}^n a_i X^{n-i} Y^i \in V_n(R)$ for some ring R, one notices that

$$\left(\begin{smallmatrix} 1 & m \\ 0 & 1 \end{smallmatrix}\right) \cdot P(X,Y) = \sum_{i=0}^{n} a_i X^{n-i} (mX + Y)^i$$

so that

$$(\left(\begin{smallmatrix} 1 & m \\ 0 & 1 \end{smallmatrix}\right) \cdot P(X,Y))(0,1) = P(0,1)$$

Define a map $\varphi: V_n(\mathbb{F}_p) \to \mathbb{F}_p$ given by $\varphi(P(X,Y)) = P(0,1)$. Since for all $\gamma \in \Gamma$ it holds that $\gamma \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \mod p$, then φ is a homomorphism of Γ-modules, where clearly Γ acts trivially on $\mathbb{F}_p$.

Let
$$\Phi\colon H^1(\Gamma, V_n(\mathbb{F}_p)) \to H^1(\Gamma, \mathbb{F}_p)$$
be the induced morphism in cohomology. Using the explicit description of cohomology that we saw in the previous section, Φ is essentially given by postcomponing a 1-cocycle with φ. We want to prove that Φ induces an isomorphism $H^1_{ord}(\Gamma, V_n(\mathbb{F}_p)) \cong H^1_{ord}(\Gamma, \mathbb{F}_p)$.

We have an exact sequence of Γ-modules
$$0 \to \mathrm{Ker}(\varphi) \to V_n(\mathbb{F}_p) \xrightarrow{\varphi} \mathbb{F}_p \to 0$$
yielding a long exact sequence in cohomology
$$\cdots \to H^1(\Gamma, \mathrm{Ker}(\varphi)) \to H^1(\Gamma, V_n(\mathbb{F}_p)) \xrightarrow{\Phi} H^1(\Gamma, \mathbb{F}_p) \xrightarrow{\delta} H^2(\Gamma, \mathrm{Ker}(\varphi)) \to \dots$$

Let again $\alpha_p = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$. It is easy to check that the action of α_p^ι leaves $\mathrm{Ker}(\varphi)$ invariant, so that the operator $T(p)$ acts on $H^j(\Gamma, \mathrm{Ker}(\varphi))$ for all $j \geq 0$.

It is easy to check that
$$\mathrm{Ker}(\varphi) = \langle X^{n-i}Y^i \mid i = 0, \dots, n-1 \rangle_{\mathbb{F}_p}$$
and clearly
$$\alpha_p^\iota \cdot (X^{n-i}Y^i) = (pX)^{n-i}Y^i = 0$$
in $V_n(\mathbb{F}_p)$ for $i = 0, \dots, n-1$, so that the action of α_p^ι kills $\mathrm{Ker}(\varphi)$. Since
$$\Gamma\alpha_p\Gamma = \bigsqcup_{i=0}^{p-1} \Gamma\alpha_p \left(\begin{smallmatrix} 1 & i \\ 0 & 1 \end{smallmatrix}\right)$$
one verifies easily that the action of $T(p)$ is nilpotent on $H^j(\Gamma, \mathrm{Ker}(\varphi))$ for $j > 0$.

Since taking ordinary parts is exact (cf. section 5.3), we can conclude that indeed $H^1_{ord}(\Gamma, V_n(\mathbb{F}_p)) \cong H^1_{ord}(\Gamma, \mathbb{F}_p)$. □

Corollary 3.3.2. *Let $p \geq 3$ be a prime number and N be an integer prime to p. Let χ be a Dirichlet character modulo Np, taking values in $\mathcal{O}_F^\times$ where F is a finite extension of $\mathbb{Q}_p$. Then the integers*
$$\mathrm{Rank}_{\mathcal{O}_F}(M_k^{\mathrm{ord}}(\Gamma_1(Np), \chi\omega^{-k}, \mathcal{O}_F))$$
and
$$\mathrm{Rank}_{\mathcal{O}_F}(S_k^{\mathrm{ord}}(\Gamma_1(Np), \chi\omega^{-k}, \mathcal{O}_F))$$
are bounded independently of k if $k \geq 2$.

Proof. The assertion for cusp forms is immediate from the above theorem, since $S_k(\Gamma_1(Np), \mathcal{O}_F) = S_k(\Gamma_1(Np), \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathcal{O}_F$. For modular forms one has to know that the contribution of Eisenstein series basically depends only on the number of cusps of $\Gamma_1(Np)$, which is finite and, of course, independent of k. For more precise information about the space of Eisenstein series consider the dimension formulas on page 111 of [5]. □

Now we are ready to prove the following (this is theorem 2.2.1).

Theorem 3.3.3 (Cf. theorem 7.3.3 in [9]). *In the setting of the above corollary assume that $p \geq 5$. Then we actually have that*

$$\mathrm{Rank}_{\mathcal{O}_F}(S_k^{ord}(\Gamma_1(Np), \chi\omega^{-k}, \mathcal{O}_F) = \mathrm{Rank}_{\mathcal{O}_F}(S_2^{ord}(\Gamma_1(Np), \chi\omega^{-2}, \mathcal{O}_F)$$

and that

$$\mathrm{Rank}_{\mathcal{O}_F}(M_k^{ord}(\Gamma_1(Np), \chi\omega^{-k}, \mathcal{O}_F) = \mathrm{Rank}_{\mathcal{O}_F}(M_2^{ord}(\Gamma_1(Np), \chi\omega^{-2}, \mathcal{O}_F)$$

for all $k \geq 2$.

Proof. Assume first that M is any $\mathcal{O}_F$ module with an action of $\Gamma_0(Np)$. Let Γ be a normal subgroup of $\Gamma_0(Np)$ such that Γ is torsion free and $p \nmid [\Gamma_0(Np) : \Gamma]$. If $p \geq 5$ we know that $\Gamma = \Gamma_1(p) \cap \Gamma_0(Np)$ is torsion free and it is actually the kernel of the well-defined projection

$$\Gamma_0(Np) \to (\mathbb{Z}/p\mathbb{Z})^\times, \qquad \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto d \mod p$$

so that $[\Gamma_0(Np) : \Gamma] = p - 1$ is prime to p.

Via the restriction and corestriction maps on cohomology

$$H^j(\Gamma_0(Np), M) \xrightarrow{Res} H^i(\Gamma, M)^{\Gamma_0(Np)} \xrightarrow{Cor} H^i(\Gamma_0(Np), M)$$

we have that $Cor \circ Res$ is the multiplication by $[\Gamma_0(Np) : \Gamma] = p - 1$, which is prime to p. Hence if we take coefficients in $\mathcal{O}_F$ (i.e. we view M as $\mathcal{O}_F[\Gamma_0(Np)]$-module), we know that

$$H^j(\Gamma, M)^{\Gamma_0(Np)} \cong H^j(\Gamma_0(Np), M)$$

But by proposition 3.1.4 we know that $H^2(\Gamma, M) = 0$, so that also $H^2(\Gamma_0(Np), M) = 0$.

We know that if M is a $\mathcal{O}_F[\Gamma_0(Np)]$-module such that the action of $\Gamma_0(Np)$ extends to the semi-group ring generated over $\mathcal{O}_F$ by $\Gamma_0(Np)$ and α_p^ι (where $\alpha_p = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$), then we have a well-defined $T(p) = U(p)$ operator on $H^j(\Gamma_0(Np), M)$ and it makes sense to consider the ordinary part $H^j_{ord}(\Gamma_0(Np), M)$, defined (equivalently) as in sections 5.3 or 2.1.

Fix now a Dirichlet character ψ modulo Np taking values in $\mathcal{O}_F^\times$. Fix a uniformizer $\pi \in \mathcal{O}_F$ and let $\mathbb{F} := \mathcal{O}_F/(\pi)$ denote the residue field (a finite extension of $\mathbb{F}_p$).

For any integer $n \geq 0$ consider the short exact sequence of $\mathcal{O}_F[\mathrm{Mat}_2(\mathbb{Z})_{\neq 0}]$-modules

$$0 \to V_n^\psi(\mathcal{O}_F) \xrightarrow{\pi} V_n^\psi(\mathcal{O}_F) \to V_n^\psi(\mathbb{F}) \to 0 \tag{3.2}$$

As in the proof of theorem 3.3.1 we get an induced exact sequence in cohomology given by

$$0 \to H^1(\Gamma_0(Np), V_n^\psi(\mathcal{O}_F)) \otimes_{\mathcal{O}_F} \mathbb{F} \to H^1(\Gamma_0(Np), V_n^\psi(\mathbb{F})) \to H^2(\Gamma_0(Np), V_n^\psi(\mathcal{O}_F))$$

By what we said at the beginning of the proof it follows that

$$H^2(\Gamma_0(Np), V_n^{\psi}(\mathcal{O}_F)) = 0$$

so that

$$H^1(\Gamma_0(Np), V_n^{\psi}(\mathcal{O}_F)) \otimes_{\mathcal{O}_F} \mathbb{F} \cong H^1(\Gamma_0(Np), V_n^{\psi}(\mathbb{F}))$$

and in particular

$$H^1_{ord}(\Gamma_0(Np), V_n^{\psi}(\mathcal{O}_F)) \otimes_{\mathcal{O}_F} \mathbb{F} \cong H^1_{ord}(\Gamma_0(Np), V_n^{\psi}(\mathbb{F}))$$

so that

$$\mathrm{Rank}_{\mathcal{O}_F}(H^1_{ord}(\Gamma_0(Np), V_n^{\psi}(\mathcal{O}_F))) = \dim_{\mathbb{F}}(H^1_{ord}(\Gamma_0(Np), V_n^{\psi}(\mathbb{F})))$$

if we prove that $H^1_{ord}(\Gamma_0(Np), V_n^{\psi}(\mathcal{O}_F))$ is free (equivalently π-torsion-free) as $\mathcal{O}_F$-module.

To see this notice that the sequence (3.2) induces also the following exact sequence in cohomology

$$\begin{aligned} 0 \to H^0(\Gamma_0(Np), V_n^{\psi}(\mathcal{O}_F)) \otimes_{\mathcal{O}_F} \mathbb{F} \to & H^0(\Gamma_0(Np), V_n^{\psi}(\mathbb{F})) \to \\ & \xrightarrow{\delta} H^1(\Gamma_0(Np), V_n^{\psi}(\mathcal{O}_F))[\pi] \to 0 \end{aligned}$$

In particular taking ordinary parts it means that we have an exact sequence

$$H^0_{ord}(\Gamma_0(Np), V_n^{\psi}(\mathbb{F})) \to H^1_{ord}(\Gamma_0(Np), V_n^{\psi}(\mathcal{O}_F))[\pi] \to 0$$

so that if we prove that $H^0_{ord}(\Gamma_0(Np), V_n^{\psi}(\mathbb{F})) = 0$, then $H^1_{ord}(\Gamma_0(Np), V_n^{\psi}(\mathcal{O}_F))$ is free (equivalently π-torsion-free) as $\mathcal{O}_F$-module.

Now for $i = 0, \dots, n$ we have that

$$X^{n-i}Y^i | T(p) = \sum_{j=0}^{p-1} \left(\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right)^{\iota} \cdot X^{n-i}Y^i = \sum_{j=0}^{p-1} (pX)^n - i(Y - jX)^i$$

so that for $i = 0, \dots, n-1$ it holds $X^{n-i}Y^i | T(p) = 0 \mod p$.

If $i = n$ we have that

$$Y^n | T(p) = \sum_{j=0}^{p-1} (Y - jX)^n$$

does not have any term involving Y^n working $\mod p$, so that $Y^n | T(p)^2 = 0 \mod p$.

In particular this shows that

$$H^0_{ord}(\Gamma_0(Np), V_n^{\psi}(\mathbb{F})) = H^0(\Gamma_0(Np), V_n^{\psi}(\mathbb{F}))|e = 0$$

as we wanted to prove.

Again in the same way as in the proof of theorem 3.3.1 we define a surjective map

$$\varphi : V_n^{\psi}(\mathbb{F}) \to V_0^{\psi\omega^n}(\mathbb{F}), \qquad P(X, Y) \mapsto P(0, 1)$$

Given $P(X,Y) = \sum_{i=0}^{n} a_i X^{n-i} Y^i \in V_n^{\psi}(\mathbb{F})$, we have that

$$\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \cdot P(X,Y) = \sum_{i=0}^{n} \psi(d) a_i (aX)^{n-i} (bX + dY)^i$$

so that in $\mathbb{F}$ (i.e. modulo p) it holds that

$$(\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \cdot P(X,Y))(0,1) = a_n \psi(d) d^n = a_n \psi(d) \omega(d)^n$$

This shows that φ is a morphism of $\mathbb{F}[\Gamma_0(Np)]$-modules. Moreover one can check that

$$\varphi(\alpha_p^{\iota} \cdot P(X,Y)) = a_n = \alpha_p^{\iota} \cdot (\varphi(P(X,Y))$$

so that we have the following exact sequence in cohomology

$$H^1(\Gamma_0(Np), \mathrm{Ker}(\varphi) \to H^1(\Gamma_0(Np), V_n^{\psi}(\mathbb{F})) \to H^1(\Gamma_0(Np), V_0^{\psi\omega^n}(\mathbb{F})) \to 0$$

because $H^2(\Gamma_0(Np), \mathrm{Ker}(\varphi)) = 0$ by what we said before.

As in the proof of theorem 3.3.1 one checks easily that

$$T(p)(H^1(\Gamma_0(Np), \mathrm{Ker}(\varphi))) = 0$$

so that taking ordinary parts we find that

$$H^1_{ord}(\Gamma_0(Np), V_n^{\psi}(\mathbb{F})) \cong H^1_{ord}(\Gamma_0(Np), V_0^{\psi\omega^n}(\mathbb{F}))$$

Letting $n = k-2$ for $k \geq 2$ and $\psi = \chi\omega^{-k}$ we finally get that

$$H^1_{ord}(\Gamma_0(Np), V_n^{\chi\omega^{-k}}(\mathbb{F})) \cong H^1_{ord}(\Gamma_0(Np), V_0^{\chi\omega^{-2}}(\mathbb{F}))$$

Via the Eichler-Shimura isomorphism we can finally deduce that

$$\begin{aligned}
&\mathrm{Rank}_{\mathcal{O}_F}(M_k^{ord}(\Gamma_0(Np), \chi\omega^{-k}, \mathcal{O}_F)) + \mathrm{Rank}_{\mathcal{O}_F}(S_k^{ord}(\Gamma_0(Np), \chi\omega^{-k}, \mathcal{O}_F)) = \\
&= \mathrm{Rank}_{\mathcal{O}_F}(H^1_{ord}(\Gamma_0(Np), V_{k-2}^{\chi\omega^{-k}}(\mathcal{O}_F))) = \dim_{\mathbb{F}}(H^1_{ord}(\Gamma_0(Np), V_{k+2}(\chi\omega^{-k}(\mathbb{F}))) = \\
&= \dim_{\mathbb{F}}(H^1_{ord}(\Gamma_0(Np), V_0(\chi\omega^{-2}(\mathbb{F}))) = \mathrm{Rank}_{\mathcal{O}_F}(H^1_{ord}(\Gamma_0(Np), V_0^{\chi\omega^{-2}}(\mathcal{O}_F))) = \\
&= \mathrm{Rank}_{\mathcal{O}_F}(M_2^{ord}(\Gamma_0(Np), \chi\omega^{-2}, \mathcal{O}_F)) + \mathrm{Rank}_{\mathcal{O}_F}(S_2^{ord}(\Gamma_0(Np), \chi\omega^{-2}, \mathcal{O}_F))
\end{aligned}$$

It follows easily from lemma 5.3 in [11] that the rank of the space of ordinary Eisenstein series

$$\mathcal{E}_k^{ord}(\Gamma_0(Np), \chi\omega^{-k}, \mathcal{O}_F) = \frac{M_k^{ord}(\Gamma_0(Np), \chi\omega^{-k}, \mathcal{O}_F)}{S_k^{ord}(\Gamma_0(Np), \chi\omega^{-k}, \mathcal{O}_F)}$$

is independent of $k \geq 2$ (and actually one can find an explicit description of a basis for such a space).

In other words the difference

$$\mathrm{Rank}_{\mathcal{O}_F}(M_k^{ord}(\Gamma_0(Np), \chi\omega^{-k}, \mathcal{O}_F)) - \mathrm{Rank}_{\mathcal{O}_F}(S_k^{ord}(\Gamma_0(Np), \chi\omega^{-k}, \mathcal{O}_F))$$

is constant independent of $k \geq 2$.

We can thus deduce that for all $k \geq 2$ it holds

$$\mathrm{Rank}_{\mathcal{O}_F}(S_k^{ord}(\Gamma_0(Np), \chi\omega^{-k}, \mathcal{O}_F)) = \mathrm{Rank}_{\mathcal{O}_F}(S_2^{ord}(\Gamma_0(Np), \chi\omega^{-2}, \mathcal{O}_F))$$

and

$$\mathrm{Rank}_{\mathcal{O}_F}(M_k^{ord}(\Gamma_0(Np), \chi\omega^{-k}, \mathcal{O}_F)) = \mathrm{Rank}_{\mathcal{O}_F}(M_2^{ord}(\Gamma_0(Np), \chi\omega^{-2}, \mathcal{O}_F))$$

□

Chapter 4

Examples of Hida families

4.1 Lambda-adic Eisenstein series

Fix a prime p and a positive integer N prime to p. The aim of this section is to construct a Lambda-adic form out of Eisenstein series. For sake of simplicity let us assume that p is odd (but with slight modifications the same construction can be carried out even if $p = 2$). Here we follow mainly [1].

Recall that the classical family of Eisenstein series of level $\Gamma(1)$ and variable weight $k \geq 4$ even has q-expansion

$$E_k(z) = \frac{\zeta(1-k)}{2} + \sum_{n=1}^{+\infty} \sigma_{k-1}(n) q^n \tag{4.1}$$

where $\sigma_m(n) := \sum_{d|n} d^m$. It is well-known that $E_k(z) \in M_k(\Gamma(1))$.

Fix an integer N prime to p. If ψ is a Dirichlet character modulo Np^r such that $\psi(-1) = (-1)^k$ with $k \geq 1$ we also have modified Eisenstein series

$$E_{k,\psi}(z) = \frac{L(1-k,\psi)}{2} + \sum_{n=1}^{+\infty} \sigma_{k-1,\psi}(n) q^n \tag{4.2}$$

where $\sigma_{m,\psi} = \sum_{d|n} \psi(d) d^m$. It is well-known that $E_{k,\psi}(z) \in M_k(\Gamma_0(Np^r), \psi)$

If ψ has level N then $E_{k,\psi}$ has level N, not divisible by p. Define the p-stabilization of $E_{k,\psi}^{(p)}$ as

$$E_{k,\psi}^{(p)}(z) = E_{k,\psi}(z) - \psi(p) p^{k-1} E_{k,\psi}(pz) \tag{4.3}$$

Lemma 4.1.1. *It holds (for ψ of level N)*

$$E_{k,\psi}^{(p)}(z) = \frac{L^{(p)}(1-k,\psi)}{2} + \sum_{n=1}^{+\infty} \sigma_{k-1,\psi}^{(p)}(n) q^n \in M_k(\Gamma_0(Np), \psi)$$

where

$$L^{(p)}(s,\psi) = (1 - \psi(p) p^{-s}) L(s,\psi)$$

and

$$\sigma_{m,\psi}^{(p)}(n) = \sum_{\substack{d|n \\ p \nmid d}} \psi(d) d^m$$

Proof. This is an easy exercise. □

If ψ has conductor divisible by p, then $E^{(p)}_{k,\psi} = E_{k,\psi}$.

We now fix the following characters:

- χ is an even Dirichlet character modulo Np for some N prime to p.
- ε_ζ is a Dirichlet character of conductor p^r associated to a p-power root of unity ζ as follows: if ζ has order p^{r-1} with $r \geq 1$, send the image of $u = 1 + p$ in $(\mathbb{Z}/p^r\mathbb{Z})^\times$ to ζ (in $\bar{\mathbb{Q}}_p$).
- ω is the Teichmüller character already discussed.

Finally let $\psi = \chi\omega^{-k}\varepsilon_\zeta$, so that ψ is a character of level Np^r and, since χ is even, $\psi(-1) = (-1)^k$. We also consider $E^{(p)}_{k,\psi}$, which is a modular form in $M_k(\Gamma_1(Np^r), \psi)$.

Theorem 4.1.2. *Set $I = \mathcal{O}[[X]]$ with $\mathcal{O} = \mathbb{Z}_p[\chi]$. If $\chi \neq 1$, then there is a I-adic form*

$$\mathcal{E}_\chi = \sum_{n=0}^{+\infty} A_{n,\chi}(X)q^n \in I[[q]]$$

which specializes to $E^{(p)}_{k,\psi}$ with $\psi = \chi\omega^{-k}\varepsilon_\zeta$ under the homomorphism $I \to \bar{\mathbb{Q}}_p$ induced by $\varphi_{k,\varepsilon_\zeta}$ for $k > 1$, and ζ as above. If $\chi = 1$ then $\mathcal{E}_\chi$ exists, but it is not stricly speaking a I-adic form, since the constant term of $\mathcal{E}_\chi$ has denominator X.

Proof. Let $\Lambda = \mathbb{Z}_p[[X]]$. It should be clear from example 1.3.6 that if $s \in \mathbb{Z}_p$ then the power series

$$(1+X)^s = \sum_{n=0}^{+\infty} \binom{s}{n} X^n$$

is an element of Λ. Remark 1.3.3 shows that if d is an integer with $d \equiv 1 \mod p$, then $d = u^{s(d)}$ for $u = 1 + p$ (the fixed topological generator of $\Gamma = 1 + p\mathbb{Z}_p$). Hence setting

$$A_d(X) = \frac{1}{d}(1+X)^{s(d)}$$

one finds immediately

$$A_d(u^k - 1) = \frac{u^{s(d)k}}{d} = d^{k-1}$$

In general for d coprime to p we have $\langle d \rangle \in \Gamma$ so we can set

$$A_d(X) = \frac{(1+X)^{s(\langle d \rangle)}}{d}$$

obtaining

$$A_d(\zeta u^k - 1) = \frac{\zeta^{(s\langle d \rangle)} u^{ks(\langle d \rangle)}}{d} = \frac{\varepsilon_\zeta(\langle d \rangle)\langle d \rangle^k}{d} = \omega^{-k}(d)\varepsilon_\zeta(d)d^{k-1}$$

Finally for $n \geq 1$ set

$$A_{n,\chi}(X) = \sum_{\substack{d|n \\ (d,p)=1}} \chi(d)A_d(X)$$

so that

$$A_{n,\chi}(\zeta u^k - 1) = \sum_{\substack{d|n \\ (d,p)=1}} \psi(d)d^{k-1} = \sigma^{(p)}_{k-1,\psi}(n)$$

where $\psi = \chi\omega^{-k}\varepsilon_\zeta$. This interpolates the non-constant terms of $E^{(p)}_{k,\psi}$.

For the constant term we will use Iwasawa's construction of Kubota-Leopold p-adic L-functions. With the notation of theorem 1.3.9 we set

$$A_{0,\chi}(X) = \frac{G_\chi(X)}{2H_\chi(X)}$$

Notice that since χ has conductor Np, if χ is not trivial then it is not of type Γ and $H_\chi(X) = 1$ by definition. If χ is trivial then $H_\chi(X) = X$. So if $\chi \neq 1$ we have $A_{0,\chi}(X) \in \mathrm{Frac}(I)$, with $XA_{0,\chi}(X) \in I$ if $\chi = 1$. Finally

$$\begin{aligned} A_{0,\chi}(\zeta u^k - 1) &= \frac{G_\chi(\zeta u^k - 1)}{2H_\chi(\zeta u^k - 1)} = \frac{G_{\chi\varepsilon_\zeta}(u^k - 1)}{2H_{\chi\varepsilon_\zeta}(u^k - 1)} = \\ &= \frac{L_p(1-k, \chi\varepsilon_\zeta)}{2} = \frac{(1-\psi(p)p^{k-1}) \cdot L(1-k,\psi)}{2} = \\ &= \frac{L^{(p)}(1-k,\psi)}{2} \end{aligned}$$

where we used the properties of the p-adic Dirichlet L-functions that we already mentioned (cf. theorems 1.3.7 and 1.3.9).

Thus if we define

$$\mathcal{E}_\chi = \sum_{n=0}^{+\infty} A_{n,\chi}(X)q^n$$

then $\mathcal{E}_\chi \in I[[q]]$ if $\chi \neq 1$ (if $\chi = 1$ then $X\mathcal{E}_1 \in I[[q]]$) and satisfies the required interpolation properties. □

4.2 Theta series

4.2.1 CM modular forms

Let K be an imaginary quadratic field (of discriminant $-D$ for some $D > 0$), $\mathfrak{f}$ an integral ideal in K and $I_\mathfrak{f}$ be the group of fractional ideals prime to $\mathfrak{f}$. Let σ_1, σ_2 denote the two embeddings of K into $\mathbb{C}$ (say that σ_1 is 1_F) and let $(k_1, k_2) \in \mathbb{Z}^2$.

Definition 4.2.1. A Hecke Grössencharacter φ of infinity type (k_1, k_2) defined modulo $\mathfrak{f}$ is a group homomorphism $\varphi\colon I_\mathfrak{f} \to \mathbb{C}^\times$ such that $\varphi((\alpha)) = \sigma_1(\alpha)^{k_1}\sigma_2(\alpha)^{k_2}$ for all $\alpha \equiv 1 \mod {}^\times\mathfrak{f}$.

Remark 4.2.1. Here we say that $a \equiv b \mod {}^\times\mathfrak{f}$ if for every prime ideal $\mathfrak{q}$ appearing in $\mathfrak{f}$ it holds $v_\mathfrak{q}(a-b) > v_\mathfrak{q}(\mathfrak{f})$ (where $v_\mathfrak{q}$ denotes the $\mathfrak{q}$-adic valuation).

Remark 4.2.2. It is easily observed that a Hecke Grössencharacter φ takes values in $\bar{\mathbb{Q}}$ and that the field generated by the values of φ is a number field (cf. [21] page 4, here Hecke Grössencharacters correspond to the so-called Hecke characters of type A_0).

We can extend such a φ setting $\varphi(\mathfrak{a}) = 0$ if $\mathfrak{a}$ is an integral ideal not coprime to $\mathfrak{f}$. Given a Hecke Grössencharacter φ of infinity type $(k-1,0)$ for some $k \geq 2$ consider the series

$$f(z;\varphi) := \sum_{\mathfrak{a}} \varphi(\mathfrak{a}) q^{N(\mathfrak{a})}$$

where the sum is over all integral ideals $\mathfrak{a} \subseteq \mathcal{O}_K$ and $N(\mathfrak{a})$ denotes the usual norm of $\mathfrak{a}$ from K to $\mathbb{Q}$. This is called the theta series associated to φ.

It is proven in [18] (lemma 3) that if the character φ has exact conductor $\mathfrak{f}$ the above sum defines a cuspidal newform (eigenform for all Hecke operators) in $S_k(\Gamma_0(M), \chi)$ where $M = D \cdot N(\mathfrak{f})$ and χ is the Dirichlet character modulo M given by

$$\chi(n) = \left(\frac{-D}{n}\right) \frac{\varphi((n))}{n^{k-1}} \qquad \text{for } (n, M) = 1$$

(here $\left(\frac{-D}{\cdot}\right)$ denotes the Jacobi symbol).

This leads us to the notion of CM-modular form (modular form with complex multiplication).

Definition 4.2.2. We say that a classical modular normalized eigenform (for all Hecke operators) $g \in S_k(\Gamma_1(Np^m))$ (where N is prime to p and $m \geq 0$) has CM by an imaginary quadratic field K if its Hecke eigenvalues for the operators T_ℓ ($\ell \nmid Np$) coincide with those of $f(z;\varphi)$ for some Grössencharacter φ of K of infinity type $(k-1,0)$. Sometimes we say that g is CM without specifying the field.

Actually, at least for newforms, one can give a more down-to-earth definition of CM modular form, following [15].

Given a newform $f = \sum_{n=1}^{+\infty} a_n q^n$ of weight $k \geq 1$ and level $\Gamma_1(N)$ (with Nebentypus χ) and a Dirichlet character ε modulo D, we let $f \otimes \varepsilon$ to be the twist

$$f \otimes \varphi = \sum_{n=1}^{+\infty} \varepsilon(n) a_n q^n.$$

One can prove that $f \otimes \varepsilon \in S_k(\Gamma_0(ND^2), \chi\varepsilon^2)$. In particular for $p \nmid ND$ one can compute that

$$T(p)(f \otimes \varepsilon) = \varepsilon(p) a_p (f \otimes \varepsilon)$$

so that $f \otimes \varepsilon$ is again an eigenform.

Then one can give the following definition

Definition 4.2.3. In the above setting, suppose that ε is not the trivial character. The form f has CM (complex multiplication) by ε if

$$\varepsilon(p) a_p = a_p$$

for all primes p in a set of primes of density 1.

One can prove easily that if f has CM by ε in the above sense, then ε must be a quadratic character. Looking at ε as a Galois charcater $\varepsilon \colon \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \{\pm 1\}$, we know that its kernel determines a quadratic field K. In this case we say that f has CM by K.

It is easily verified (essentially by the definition of the Jacobi symbol) that the modular forms $f(z;\varphi)$ described above (when $\mathfrak{f}$ is the conductor of φ) have CM by the imaginary quadratic field K.

After a careful analysis of the ℓ-adic Galois representations associated to an eigenform, Ribet proved in [15] that also the converse is in some sense true, i.e. that essentially all CM newforms arise as theta series attached to a Grössencharacter of an imaginary quadratic field. This means that the two definitions that we gave of modular form with CM coincide for newforms (this is theorem 4.5 in [15]).

For the following proposition we need the notion of slope of a modular form.

Definition 4.2.4. Let f be a cuspidal eigenform (for all Hecke operators) of level Np^m for some N prime to p and $m \geq 1$ and Fourier coefficients in a finite extension of $\mathbb{Q}_p$. Write the q-expansion of f as

$$f = \sum_{n=1}^{+\infty} a_n q^n$$

Assume f is normalized, i.e. that $a_1 = 1$. Then the p-adic slope of f is the rational number

$$\alpha(f) := \mathrm{ord}_p(a_p)$$

where ord_p denotes the p-adic order, normalized in such a way that $\mathrm{ord}_p(p) = 1$.

Notice that f in the above definition is ordinary if and only if $\alpha(f) = 0$.

Proposition 4.2.5 (cf [2] prop. 3.5)**.** *Let $f = f(z;\varphi)$ be the newform associated to a Hecke Grössencharacter φ as above. Assume that the level of f is Np^m with N prime to p and $m \geq 1$. Then the p-slope of f is either $0, \frac{k-1}{2}$ or infinite, depending on the behaviour of the prime p in K.*

Proof. Let a_p be the U_p-eigenvalue of f (this is also the coefficient of q^p in the q-expansion). We have three possibilities

(i) If p is inert in K then $a_p = 0$ (there is not any ideal of norm p in K), so the p-slope is infinite.

(ii) If p splits in K as $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$, then $a_p = \varphi(\mathfrak{p}) + \varphi(\overline{\mathfrak{p}})$. We can find an integer n such that $\mathfrak{p}^n = (\alpha)$ with $\alpha \equiv 1 \mod {}^{\times}\mathfrak{f}$, so that $\varphi((\alpha)) = \alpha^{k-1}$. Notice that $\alpha \in \mathfrak{p}$, but $\alpha \notin \overline{\mathfrak{p}}$ (otherwise $\mathfrak{p} = \overline{\mathfrak{p}}$) and $\varphi(\mathfrak{p}^n) = (\psi(\mathfrak{p}))^n = \alpha^{k-1}$ so $\varphi(\mathfrak{p}) \in \mathfrak{p} \setminus \overline{\mathfrak{p}}$. Analogously $\varphi(\overline{\mathfrak{p}}) \in \overline{\mathfrak{p}} \setminus \mathfrak{p}$. This implies that $a_p \notin \mathfrak{p}$ necessarily, so that the p-slope is 0.

(iii) If p ramifies in K (so $p\mathcal{O}_K = \mathfrak{p}^2$), then $a_p = \varphi(\mathfrak{p})$ and as in the previous case we can write $\mathfrak{p}^n = (\alpha)$ for some n and some α with $\alpha \equiv 1 \mod {}^{\times}\mathfrak{f}$. Thus $\varphi(\mathfrak{p})^n = \alpha^{k-1}$ and looking at p-adic valuations one sees that the slope must be $(k-1)/2$.

□

Remark 4.2.3. Notice that the above proposition used the crucial (and easy to prove) fact that if $\mathfrak{f}$ is the conductor of φ and we set

$$P_1(\mathfrak{f}) = \{(\alpha) \in I_f \mid \alpha \equiv 1 \mod {}^\times \mathfrak{f}\}$$

then $I_f/P_1(\mathfrak{f})$ is a finite group. We will need again this fact later.

The above result shows that the natural situation to consider in order to obtain an ordinary Λ-adic form out of theta series associated to imaginary quadratic is the case when p splits.

4.2.2 CM Λ-adic forms

Now we explain the construction of a CM Λ-adic form $\mathcal{F}$ containing a fixed modular form of the kind $f = f(z;\varphi)$ described above. Here we follow [8], pages 234-236.

Assume that f has weight $k \geq 2$ and that the Nebentypus χ of f is described as follows

$$\chi = \psi\omega^{-k}\varepsilon_{\zeta_0}$$

where ψ is a Dirichlet character modulo Np where p is an odd prime number and N is prime to p, ε_{ζ_0} is obtained as in section 4.1 (from a p^{r_0-1} root of unity ζ_0) and ω is the usual Teichmüller character.

Observe that given χ, then ψ and ζ_0 are uniquely determined. It is clear that the level of f is given by Np^{r_0} under our assumptions.

Let again K be the quadratic imaginary field of discriminant $-D$ (with $D > 0$) by which f has complex multiplication. Let λ be any Hecke Grössencharacter of type $(1,0)$ and conductor $\mathfrak{p}$ and let $\mathbb{Q}(\lambda)$ be the number field (cf. remark 4.2.2) generated by the values of λ. Here $\mathfrak{p}$ is determined by the fixed embedding $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$.

Let E be the completion of $\mathbb{Q}(\lambda)$ at the prime over p determined by the fixed embedding as above. It is a finite extension of $\mathbb{Q}_p$.

Write $\mathcal{O}_E$ for the ring of integers of E and decompose $\mathcal{O}_E^\times = \mu_E \times W_E$ (cf. the analogous decomposition for $\mathbb{Z}_p$ for p odd) where μ_E is finite and W_E is $\mathbb{Z}_p$-free. Write $\langle x \rangle$ for the projection of an element $x \in \mathcal{O}_E^\times$ to W_E. Let W_K be the subgroup of W_E topologically generated by $\langle \lambda(\mathfrak{a}) \rangle$ for $\mathfrak{a}$ ranging over all integral ideals prime to $\mathfrak{p}$. Notice that $\lambda(\mathfrak{a}) \in \mathcal{O}_E^\times$ because for every $\mathfrak{a}$ coprime with $\mathfrak{p}$ there is n such that $\mathfrak{a}^n = (\alpha)$ for some $\alpha \in \mathcal{O}_K$ such that $\alpha \equiv 1 \mod {}^\times\mathfrak{p}$. Hence $(\lambda(\mathfrak{a}))^n = \lambda(\mathfrak{a}^n) = \lambda(\alpha) = \alpha \in \mathcal{O}_K$ and $\lambda(\mathfrak{a}) \in \mathcal{O}_E^\times$ follows immediately.

We claim that W_K is isomorphic to $\mathbb{Z}_p$. Indeed it contains naturally $\Gamma = 1 + p\mathbb{Z}_p$ because one can identify $\mathbb{Z}_p$ with the $\mathfrak{p}$-adic completion of $\mathcal{O}_K$ (thanks to the splitting of p in F) and because λ has type $(1,0)$. Hence W_K has at least rank 1 as $\mathbb{Z}_p$ module.

At the same time if $M := \#(I_{\mathfrak{p}}/P_1(\mathfrak{p}))$ we have that

$$W_K^{(M)} := \{x^M \mid x \in W_K\} \subseteq \Gamma$$

so that necessary W_K is free of rank 1 over $\mathbb{Z}_p$ as a multiplicative group.

Let $\gamma \geq 0$ be defined by $[W_K : \Gamma] = p^\gamma$ and fix a topological generator of W_K such that $w^{p^\gamma} = 1 + p$. For all integral ideals $\mathfrak{a}$ prime to $\mathfrak{p}$ define

$$t(\mathfrak{a}) = \frac{\log_p(\langle\lambda(\mathfrak{a})\rangle)}{\log_p(w)} \in \mathbb{Z}_p$$

Let $\mathcal{O}$ denote the ring of integers of $E(\varphi, \zeta_0)$ (still a finite extension of $\mathbb{Q}_p$) and consider the extension of $\Lambda = \mathbb{Z}_p[[X]]$ given by $\mathcal{I} = \mathcal{O}[[Y]]$ defined by the relation

$$\zeta_0(1+Y)^{p^\gamma} = 1 + X$$

Finally define the formal q-expansion $\mathcal{F} \in \mathcal{I}[[q]]$ given by

$$\mathcal{F} = \sum_{(\mathfrak{a},\mathfrak{p})=1} \varphi(\mathfrak{a})\langle\lambda(\mathfrak{a})\rangle^{-k}(1+Y)^{t(\mathfrak{a})}q^{N(\mathfrak{a})}. \tag{4.4}$$

This q-expansion actually does not depend on the particular choice of λ, since any two Hecke characters of infinity type $(1,0)$ and conductor $\mathfrak{p}$ differ by a finite order character. Indeed such a difference would be a character of type $(0,0)$, i.e. in fact a character on the finite quotient $I_\mathfrak{p}/P_1(\mathfrak{p})$.

By definition of $\mathcal{I}$, we see that every classical specialization of $\mathcal{I}$ takes the form $Y = \zeta w^l - 1$ where $l \geq 2$ and ζ is a p^{r-1}-th root of 1, for some $r \geq 1$. Such a specialization extends the evaluation $X = \zeta_0\zeta^{p^\gamma}(1+p)^l - 1$.

Set $\delta_\zeta(\mathfrak{a}) = \zeta^{t(\mathfrak{a})}$ and let

$$\varphi_{l,\zeta}(\mathfrak{a}) = \varphi(\mathfrak{a})\langle\lambda(\mathfrak{a})\rangle^{l-k}\delta_\zeta(\mathfrak{a}).$$

for $\mathfrak{a}$ integral ideal coprime with $\mathfrak{p}$.

Then δ_ζ is a finite order character and $\varphi_{l,\zeta}$ is a Hecke character of infinity type $(l-1,0)$. Specializing to $Y = \zeta w^l - 1$ we immediately get

$$(1+Y)^{t(\mathfrak{a})} = \delta_\zeta(\mathfrak{a})\langle\lambda(\mathfrak{a})\rangle^l$$

so that $\mathcal{F}$ specializes to the q-expansion

$$f_{l,\zeta} = \sum_{\mathfrak{a}} \varphi_{l,\zeta}(\mathfrak{a})q^{N(\mathfrak{a})}$$

which is (essentially by definition) a CM cusp form of weight l.

For a Hecke character ϑ of K of infinity type $(t,0)$, write $\vartheta|_\mathbb{Q}$ for the induced Dirichlet character defined by $m \mapsto \vartheta((m))/m^t$. Then one checks that $\langle\lambda\rangle|_\mathbb{Q} = \omega^{-1}$ and that $\delta_\zeta|_\mathbb{Q} = \varepsilon_{\zeta^{p^\gamma}}$.

By the result recalled in the previous subsection we know that the Nebentypus χ of f is given by $\chi = \varphi|_\mathbb{Q} \cdot \chi_{K/\mathbb{Q}}$ where $\chi_{K/\mathbb{Q}}$ is the quadratic character corresponding to K (described in terms of the Jacobi symbol).

Hence the character of $\varphi_{l,\zeta}$ is given by

$$\varphi_{l,\zeta}|_\mathbb{Q} \cdot \chi_{K/\mathbb{Q}} = \varphi|_\mathbb{Q} \cdot \chi_{K/\mathbb{Q}} \cdot \langle\lambda\rangle^{l-k}|_\mathbb{Q} \cdot \delta_\zeta|_\mathbb{Q} = \psi\omega^{-l}\varepsilon_{\zeta_0\zeta^{p^\gamma}}$$

and one can check that $f_{l,\zeta}$ has level $Np^{r'}$ where $p^{r'-1}$ is the exact order of $\zeta_0\zeta^{p^\gamma}$.

We deduce that $\mathcal{F}$ is indeed a $\mathcal{I}$-adic form. Moreover $\mathcal{F}$ is p-ordinary, since $a(p, f_{l,\zeta}) = \varphi_{l,\zeta}(\bar{\mathfrak{p}})$ has the same p-adic valuation as $\varphi(\bar{\mathfrak{p}})$. Finally when $l = k$, then $\varphi_{l,1} = \varphi$ and $f_{k,1} = f$, thus $\mathcal{F}$ contains f as a specialization.

Chapter 5

The homological counterpart

This chapter is almost completely based on [7]. We describe Hida theory by studying the ordinary part of the homology modules of the Riemann surfaces $Y_1(Np^r) = \Gamma_1(Np^r)\backslash\mathcal{H}$ for some odd prime p and N an auxiliary level prime to p. The results obtained by M. Emerton in [7] are essentially the homological couterpart of theorem 3.1 in [11]. The latter theorem is the keystone of that article and allows Hida to prove the finiteness and freeness of the *universal ordinary Hecke algebra*, as well as the horizontal control theorem for it.

This quick discussion should in some sense justify our decision to include Emerton's contribution in our thesis. We tried to expand some of the proofs given in [7].

5.1 The tower of modular curves

As above, let $p \geq 3$ be an odd prime number and let N be a positive integer prime to p such that $\Gamma_1(Np)$ is torsion-free. This is not a strong requirement since it holds that $\Gamma_1(M)$ is torsion-free for all $M \geq 4$ (cf. [9] pag. 160 for this). In particular we are asking that the Riemann surface $Y_1(Np)$ does not contain elliptic points. Associated to the tower of modular curves

$$\cdots \to Y_1(Np^r) \to \cdots \to Y_1(Np)$$

we have a corresponding chain of congruence subgroups (obtained taking the topological fundamental group of our Riemann surfaces)

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

It is well-known that the first homology group with coefficients in $\mathbb{Z}$ corresponds to the abelianization of the topological fundamental group, so that if we apply the functor $H_1(-,\mathbb{Z})$ to the above tower of modular forms we get a tower of finitely generated free abelian groups

$$\cdots \to \Gamma_1(Np^r)^{ab} \to \cdots \to \Gamma_1(Np)^{ab} \tag{5.1}$$

Recall that abelianization is not an exact functor (it is only right exact), so that we do not necessarily have inclusions in the above chain of morphisms.

We now follow Hida and Emerton, so we introduce intermediate congruence subgroups

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

We have inclusions $\Gamma_1(Np^r) \subset \Phi_r^1 \subset \Gamma_1(Np)$ and it is immediate to check that $\Gamma_1(Np^r)$ is a normal subgroup of Φ_r^1.

Let $\Gamma = 1 + p\mathbb{Z}_p$ denote as usual the principal units in $\mathbb{Z}_p$ and let Γ_r for $r \geq 1$ denote the unique subgroup of index p^{r-1} contained in Γ. It is the kernel of the canonical projection $\mathbb{Z}_p^\times \to (\mathbb{Z}/p^r)^\times$. Notice this notation differs from the one used in section 1.5.1.

There is a surjective morphism of groups $\Phi_r^1 \to \Gamma/\Gamma_r$ induced by the assignment $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto d \mod (p^r)$. It is immediately verified that the kernel of this morphism is $\Gamma_1(Np^r)$, so that there is an exact sequence of groups

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

Lemma 5.1.1. *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* $\Gamma_1(Np^r)^{ab}$*. Thus* Γ *acts naturally on* $\Gamma_1(Np^r)^{ab}$ *for all* r *and the morphisms in the chain* (5.1) *are morphisms of* Γ*-modules.*

Proof. In general if G is a group and $H \triangleleft G$ is a normal subgroup, then the group G/H acts on H^{ab} by conjugation. Indeed if $h = [h_1, h_2] = h_1^{-1}h_2^{-1}h_1h_2 \in H$ is the commutator of $h_1, h_2 \in H$, then for every $g \in G$ we have that

$$g^{-1}hg = [g^{-1}h_1g, g^{-1}h_2g]$$

is again a commutator. In particular if $g \in H$, we have that $g^{-1}hg \in [H,H] \triangleleft H$. This proves that Γ acts on $\Gamma_1(Np^r)^{ab}$ for all $r \geq 1$ via its quotients $\Gamma/\Gamma_r = \Phi_r^1/\Gamma_1(Np^r)$.

Next we verify that the morphism $\Gamma_1(Np^{r+1})^{ab} \to \Gamma_1(Np^r)^{ab}$ is Γ-equivariant for all $r \geq 1$. This gives us the opportunity to describe explicitly the action of Γ. Let $\alpha \in \Gamma$, then there exists a matrix $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Phi_r^1$ such that $\alpha \equiv d \mod (p^{r+1})$. Then the automorphism induced by α on $\Gamma_1(Np^{r+1})^{ab}$ is essentially conjugation by g. Since by our choice we also have $\alpha \equiv d \mod (p^r)$, then also the action of α on $\Gamma_1(Np^{r+1})^{ab}$ is essentially given by the conjugation by g. This clearly shows the Γ-equivariants of the morphism $\Gamma_1(Np^{r+1})^{ab} \to \Gamma_1(Np^r)^{ab}$. □

The automorphisms induced by elements of Γ as above will be referred to as *diamond operators* and the action of Γ will be referred to as the *Nebentypus* action.

If $r \geq s > 0$ we let Φ_r^s to be the subgroup of Φ_r^1 containing $\Gamma_1(Np^r)$ and such $\Phi_r^s/\Gamma_1(Np^r)$ identifies with Γ_s/Γ_r. More explicitly

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

Hence there is an exact sequence

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

which yields, taking the abelianizations, the exact sequence

$$\Gamma_1(Np^r)^{ab} \to \Phi_r^{s\,ab} \to \Gamma_s/\Gamma_r \to 1 \tag{5.2}$$

Let $\mathfrak{a}_s$ denote the augmentation ideal in the group $\mathbb{Z}[\Gamma_s]$, so that $\mathfrak{a}_s$ is the kernel of the projection $\mathbb{Z}[\Gamma_s] \to \mathbb{Z}$. Then we claim that under the Nebentypus action we have

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

Indeed $\mathfrak{a}_s$ is generated by elements $\alpha - 1$ for $\alpha \in \Gamma_s$ and the action of such elements on $[x] \in \Gamma_1(Np^r)^{ab}$ is given exactly by

$$(\alpha - 1) \cdot [x] = [gxg^{-1}x^{-1}]$$

for a matrix $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Phi_r^s$ (we can choose g in Φ_r^s because $\alpha \in \Gamma_s$) such that $d \equiv \alpha \mod (p^r)$.

The group 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 it is abelian and we obtain immediately that

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

Thus the above extension can be rewritten as

$$1 \to \Gamma_1(Np^r)^{ab}/\mathfrak{a}_s\Gamma_1(Np^r)^{ab} \to \Phi_r^{s\,ab} \to \Gamma_s/\Gamma_r \to 1 \tag{5.3}$$

This discussion allows us to give a more detailed description of a the morphisms

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

which appear in the chain (5.1). Indeed such morphism factors as the composition of the projection

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

the injection (in the above exact sequence)

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

and the morphism

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

5.2 Hecke operators

Suppose T is a group which contains subgroups G and H and that $t \in T$ satisfies the property that $K = t^{-1}Ht \cap G$ has finite index in G. Then one has the transfer morphism

$$V\colon G^{ab} \to K^{ab}$$

which is defined as follows. Write $G = \bigsqcup_{i=1}^{r} x_i K$ for a choice $x_1, \dots, x_r$ of coset representatives. Given $g \in G$ write $gx_i = x_j k_j$ for a suitable $j = j(i)$ and $k_j \in K$. Finally send the class of g in G^{ab} to the class of $\prod_{i=1}^{r} k_i$ in K^{ab}. One can then check that this is well defined and gives a group homomorphism V as above.

Conjugation by t induces an isomorphism

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

Finally the inclusion of $H \cap tGt^{-1}$ in H induces a morphism

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

Taking the composition of these arrows we finally get a group homomorphism

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

which we will call the *Hecke operator* attached to t.

In our case we will set $T = \mathrm{GL}_2(\mathbb{Q})$, $G = H$ to be a suitable congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ of level divisible by p and $t := \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$. The corresponding Hecke operator will be denoted by $U = U(p)$.

Suppose that $G = \Phi_r^s$ as in the previous section. One can check that $t^{-1}\Phi_r^s t \cap \Phi_r^s = \Phi_r^s \cap \Gamma^0(p)$ where

$$\Gamma^0(p) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \mid b \equiv 0 \mod (p)\}$$

and that $\Phi_r^s \cap t\Phi_r^s t^{-1} = \Phi_{r+1}^s$. Hence the U operator is by definition the composition

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

Following Emerton we denote by U' the composition of the first two of these morphisms, i.e.

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

Lemma 5.2.1. *Suppose that $r \geq s > 0$ and $r' \geq s' > 0$ with $r \geq r'$ and $s \geq s'$ (so that $\Phi_r^s \subset \Phi_{r'}^{s'}$). Then the following diagram commutes*

$$\begin{tikzcd}
\Phi_r^{s\ ab} \arrow[r] \arrow[d, "U'"] & \Phi_{r'}^{s'\ ab} \arrow[d, "U'"] \\
\Phi_{r+1}^{s\ \ ab} \arrow[r] & \Phi_{r'+1}^{s'\ \ ab}
\end{tikzcd}$$

Proof. We can factor the above diagram into the composition of two diagrams as

$$\begin{tikzcd}
\Phi_r^{s\ ab} \arrow[r] \arrow[d, "V"] & \Phi_{r'}^{s'\ ab} \arrow[d, "V"] \\
(\Phi_r^s \cap \Gamma^0(p))^{ab} \arrow[r] \arrow[d, "t(-)t^{-1}"] & (\Phi_{r'}^{s'} \cap \Gamma^0(p))^{ab} \arrow[d, "t(-)t^{-1}"] \\
\Phi_{r+1}^{s\ \ ab} \arrow[r] & \Phi_{r'+1}^{s'\ \ ab}
\end{tikzcd}$$

The lower square of the diagram clearly commutes. Now we prove that the upper square is commutative. We claim that $\Phi_r^s \cap \Gamma^0(p)$ has index p in Φ_s^r with coset representatives given by the p matrices $\left(\begin{smallmatrix} 1 & i \\ 0 & 1 \end{smallmatrix}\right)$ for $i = 0, \dots, p-1$. It is immediate to check that these matrices lie in different cosets of $\Phi_r^s/(\Phi_r^s \cap \Gamma^0(p))$. Moreover if $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Phi_r^s$ it is enough to choose the unique $i \in \{0, 1, \dots, p-1\}$ such that $i \equiv b \mod (p)$ to get that

$$\begin{pmatrix} 1 & -i \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a - ic & b - id \\ c & d \end{pmatrix} \in \Phi_r^s \cap \Gamma^0(p)$$

Notice that what we proved does not depend on the particular value of r, s, so that the transfer

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

applied to elements of $\Phi_r^{s\ ab}$ is given by the same formula as the transfer applied to elements of $\Phi_r^{s\ ab}$ when we view them inside $\Phi_{r'}^{s'\ ab}$. This is equivalent to say that the upper portion of the above diagram commutes. $\square$

In particular we deduce immediately that the following diagram commutes

$$\begin{tikzcd} \Phi_r^{s\ ab} \arrow[r] \arrow[d, "U"] & \Phi_{r'}^{s'\ ab} \arrow[d, "U"] \\ \Phi_r^{s\ ab} \arrow[r] & \Phi_{r'}^{s'\ ab} \end{tikzcd}$$

saying that the natural morphism $\Phi_r^{s\ ab} \to \Phi_{r'}^{s'\ ab}$ is a morphism of $\mathbb{Z}[U]$-modules.

Now assume that $r' = r - 1$ and $s' = s \geq r - 1$.

If $\pi\colon \Phi_r^{s\ ab} \to \Phi_{r-1}^{s}{}^{ab}$ and $\pi'\colon \Phi_{r+1}^{s}{}^{ab} \to \Phi_r^{s\ ab}$ are the obvious maps, then the above lemma gives the following equalities

$$U' \circ \pi = \pi' \circ U' = U \in \mathrm{End}_{\mathbb{Z}}(\Phi_r^{s\ ab}) \tag{5.4}$$

$$\pi \circ U' = U \in \mathrm{End}_{\mathbb{Z}}(\Phi_{r-1}^{s}{}^{ab}) \tag{5.5}$$

In particular the morphism $\Gamma_1(Np^r)^{ab} \to \Phi_r^{s\ ab}$ is a morphism of $\mathbb{Z}[U]$-modules, so that its cokernel is naturally a $\mathbb{Z}[U]$-module. By the sequence (5.2) we know that this cokernel is given by Γ_s/Γ_r.

Lemma 5.2.2. *The operator U acts on Γ_s/Γ_r as multiplication by p.*

Proof. This is proven by direct calculation. Let $\alpha \in \Gamma_s$ and choose $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Phi_r^s$ such that $d \equiv \alpha \mod (p^r)$. We now need to analyse the action of the transfer. For $i \in \{0, \dots, p-1\}$ we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & ai + b \\ c & ci + d \end{pmatrix}$$

We know that there is $j = j(i)$ and a matrix $g_j = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)$ such that

$$\begin{pmatrix} a & ai+b \\ c & ci+d \end{pmatrix} = \begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix}$$

In particular one sees immediately that it must be

$$w = ci + d \equiv d \mod (p^r)$$

as $p^r \mid c$ by definition. We know that the transfer is the class of the product $\prod_{j=0}^{p-1} g_j$ and that then one as to consider conjugation by $t = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$.

Since conjugation by t does not alter the lower right entry of a 2×2 matrix, we conclude that, as classes in $\Phi_s^{r\ ab}$, it must be

$$U \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} * & * \\ * & \tilde{d} \end{pmatrix}$$

for some $\tilde{d} \equiv d^p \mod (p^r)$. Hence the morphism $U \colon \Gamma_s / \Gamma_r \to \Gamma_s \Gamma_r$ is given by raising to the p-th power (or multiplication by p if we use an additive notation). ☐

We conclude this section with the following result

Lemma 5.2.3. *If $r \geq s > 0$, the action of U on $\Phi_r^{s\ ab}$ commutes with the Nebentypus action of Γ on $\Phi_r^{s\ ab}$.*

Proof. See lemma 3.5 in [7]. ☐

5.3 Ordinary parts

Let U be an indeterminate and consider the full subcategory (denoted by $\mathcal{A}$) of the category of $\mathbb{Z}_p[U]$-modules given by those modules which are finitely generated as $\mathbb{Z}_p$-modules. One checks quite easily that this is an abelian category (essentially because $\mathbb{Z}_p$ is a Noetherian ring). Let M be any module in this category, so that there is a morphism of $\mathbb{Z}_p$-modules

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

Since M is a finitely generated $\mathbb{Z}_p$-module, we have that $\mathrm{End}_{\mathbb{Z}_p}(M)$ is a finitely generated $\mathbb{Z}_p$-algebra, so that the image of $\mathbb{Z}_p[U]$ in $\mathrm{End}_{\mathbb{Z}_p}(M)$ is also a finite commutative $\mathbb{Z}_p$-algebra, which will be denoted by A. By lemma 10.158.2 in [24] the ring A factors as a product of finitely many complete local rings. We can thus write $A = A^{ord} \times A^{nil}$, where A^{ord} is the product of the local factors of A where the image of U is a unit and A^{nil} is the product of the local factors of A where the image of U is contained in the maximal ideal. In particular A^{ord} (and also A^{nil}) is a flat A-algebra and a subalgebra of $\mathrm{End}_{\mathbb{Z}_p}(M)$. We define the ordinary part of M as

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

As A^{ord} is flat over A, it is obvious that taking ordinary part is an exact functor on our abelian category $\mathcal{A}$.

Now let U denote again the Hecke operator defined in the previous section. By what we just said, it makes sense to consider the ordinary part of

$$H_1(Y_1(Np^r), \mathbb{Z}_p) = \Gamma_1(Np^r)^{ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p$$

By lemma 5.2.3 we have that $(\Gamma_1(Np^r)^{ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^{ord}$ is also a Γ-module for the Nebentypus action.

We are now ready to state one of the most important results of this chapter

Theorem 5.3.1. *If $r \geq s > 0$ then the natural morphism of abelian groups*

$$(\Gamma_1(Np^r)^{ab} \otimes_Z \mathbb{Z}_p)^{ord}/\mathfrak{a}_s \to (\Gamma_1(Np^s)^{ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^{ord}$$

is an isomorphism.

Proof. We saw at the end of section 5.1 that this morphism can be viewed as the compostion of

$$(\Gamma_1(Np^r)^{ab} \otimes_Z \mathbb{Z}_p)^{ord}/\mathfrak{a}_s \to (\Phi_r^{s\,ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^{ord}$$

and

$$(\Phi_r^{s\,ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^{ord} \to (\Gamma_1(Np^s)^{ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^{ord}.$$

We will prove that these arrows are both isomorphisms.

For the second one recall that we saw that if $r > s$, then there is an operator

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

such that (5.4) and (5.5) hold. These equations can be interpreted saying that, upon tensoring with $\mathbb{Z}_p$ and taking ordinary parts, the natural map

$$\pi \colon \Phi_r^{s\,ab} \to \Phi_{r-1}^{s}{}^{ab}$$

induces an isomorphism

$$(\Phi_r^{s\,ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^{ord} \cong (\Phi_{r-1}^{s}{}^{ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^{ord}$$

whose inverse is given, so to say, by "$U^{-1} \circ U'$". Applying descending induction it is clear that we get the required isomorphism

$$(\Phi_r^{s\,ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^{ord} \cong (\Phi_s^{s\,ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^{ord} = (\Gamma_1(Np^s)^{ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^{ord}$$

Now we have to prove that

$$(\Gamma_1(Np^r)^{ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^{ord}/\mathfrak{a}_s \to (\Phi_r^{s\,ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^{ord}$$

is an isomorphism. For this consider the short exact sequence (5.3). Tensoring with $\mathbb{Z}_p$ and taking ordinary parts yields the short exact sequence

$$1 \to (\Gamma_1(Np^r)^{ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^{ord}/\mathfrak{a}_s \to (\Phi_r^{s\,ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^{ord} \to (\Gamma_s/\Gamma_r)^{ord} \to 1$$

Notice that since Γ_s/Γ_r is p-torsion, it does not change when tensoring with $\mathbb{Z}_p$. By lemma 5.2.2 the operator U acts on Γ_s/Γ_r as multiplication by p, so it is a nilpotent operator. This shows that $(\Gamma_s/\Gamma_r)^{ord}$ is trivial and proves our isomorphism. □

5.4 Iwasawa modules

Write

$$\mathbf{W} := \varprojlim_r \Gamma_1(Np^r)^{ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p$$

where the projective limit is taken over the chain of $\mathbb{Z}_p$-modules

$$\cdots \to \Gamma_1(Np^r)^{ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p \to \cdots \to \Gamma_1(Np)^{ab} \otimes \mathbb{Z}_p.$$

We know that Γ acts on $\Gamma_1(Np^r)^{ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ through its finite quotient Γ/Γ_r. This immediately implies that $\mathbf{W}$ is a module over the completed group algebra (the Iwasawa algebra that we studied in subsection 1.5.1)

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

Our main focus will be to study the ordinary part of $\mathbf{W}$ from now on.

Following Emerton, we now prove a general result on Λ-modules which tell us something on the quotients $\mathbf{W}^{ord}/\mathfrak{a}_r$ for $r > 0$.

Suppose that $\{M_r\}_{r\geq 1}$ is a projective system of Λ-modules, with M_r invariant under Γ_r for all r. Then for any $r \geq s$ the given morphism

$$M_r \to M_s$$

factors as

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

Let

$$\mathbf{M} := \varprojlim_r M_r$$

so that for every s the natural morphism $\mathbf{M} \to M_s$ factors as

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

Proposition 5.4.1. *In the above setting, assume that M_r is p-adically complete for all r and that the morphisms $M_r/\mathfrak{a}_s \to M_s$ are isomorphisms for all $r \geq s$. Then for any s the morphism $\mathbf{M} \to \mathbf{M}/\mathfrak{a}_s \to M_s$ is an isomorphism.*

Proof. Essentially by assumption we have that all the morphisms $M_r \to M_s$ are surjective, so that given $m_s \in M_s$ we can construct an element $\mu \in \mathbf{M}$ whose projection to M_s is m_s. Let $\gamma_s \in \Gamma_s$ be a topological generator of Γ_s, so that $\mathfrak{a}_s$ is principal and generated by $\gamma_s - 1$. It is easy to verify that

$$\frac{\gamma_s^{p^i} - 1}{\gamma_s - 1} \in (\gamma_s - 1, p)^i$$

The maximal ideal of Λ is $\mathfrak{m} = (\mathfrak{a}_1, p)$ and obviously we have $(\gamma_s - 1, p)^i \subset \mathfrak{m}^i$. Since M_r is p-adically complete and fixed by Γ_r, we have that M_r is $\mathfrak{m}$-adically complete for all r.

Now for a fixed s, let (m_r) be an element of $\mathbf{M}$ whose projection m_s to M_s vanishes. We want to prove that there exists $(m'_r) \in \mathbf{M}$ such that $(m_r) = (\gamma_s - 1)(m'_r)$. By assumption there is an element $m_{1,s+1} \in M_{s+1}$ such that $m_{s+1} = (\gamma_s - 1)m_{1,s+1}$. Let $(m_{1,r}) \in \mathbf{M}$ be an element projecting to $m_{1,s+1}$. Then $(m_r) - (\gamma_s - 1)(m_{1,r})$ has vanishing projection to M_{s+1}.

Applying the same procedure we can find for all $i \geq 0$ an element $(m_i, r) \in \mathbf{M}$ such that

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

has vanishing projection to M_{s+i}.

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

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

yields a well-defined element of $\mathbf{M}$, which satisfies clearly that $(m_r) = (\gamma_s - 1)(m'_r)$. $\square$

The following result is now immediate.

Corollary 5.4.2. *For any $r > 0$ we have that*

$$(\Gamma_1(Np^r)^{ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^{ord} = \mathbf{W}^{ord}/\mathfrak{a}_r$$

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

From now on the aim will be to study the structure of the Λ-module $\mathbf{W}^{ord}$. In particular the final result will be the $\mathbf{W}^{ord}$ is finite and free over Λ. This should sound familiar to us and should remind of theorem 2.2.2.

Each module $\Gamma_1(Np^r)^{ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is $\mathbb{Z}_p$-free of finite rank, so it is compact in its p-adic topology. So if we give $\mathbf{W}$ the topology which is the projective limit of the p-adic topology on each module $\Gamma_1(Np^r)^{ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p$, it becomes a compact Λ-module. The action of Λ is clearly continuous. The same remarks hold true for $\mathbf{W}^{ord}$, which is a direct summand of $\mathbf{W}$.

Moreover, the above corollary implies that the projective limit topology on $\mathbf{W}^{ord}$ coincides with the $\mathfrak{m}$-adic topology, because the kernels of the projection

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

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

In conclusion $\mathbf{W}^{ord}$ is a Λ-module, compact in its $\mathfrak{m}$-adic topology, with the property that

$$\mathbf{W}^{ord}/\mathfrak{m} = \mathbf{W}^{ord}/(\mathfrak{a}_1, p) \equiv (\Gamma_1(Np)^{ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p/p)^{ord}$$

is a finite dimensional $\mathbb{F}_p = \mathbb{Z}_p/p\mathbb{Z}_p$-module. By Nakayama's lemma this implies that $\mathbf{W}^{ord}$ is finitely generated as Λ-module. We will prove in the end that $\mathbf{W}^{ord}$ is free of rank $d = \dim_{\mathbb{F}_p} \mathbf{W}^{ord}/\mathfrak{m}$.

5.5 Modules over group rings

In this section we prove a general result about reflexivity of modules over group rings.

We let R be a commutative ring , G be a finite group and M be a left $R[G]$-module. In N is an R-module, then $\mathrm{Hom}_R(M,N)$ is naturally a right $R[G]$-module with G-action given by $(\varphi.g)(m) = \varphi(g.m)$ for all $\varphi \in \mathrm{Hom}_R(M,N)$, $g \in G$, $m \in M$.

The ring $R[G]$ is clearly a bimodule over itself, so that $R[G] \otimes_R N$ is naturally a bimodule over $R[G]$. This implies that $\mathrm{Hom}_{R[G]}(M, R[G] \otimes_R N)$ is a right $R[G]$-module setting $\psi.g(m) = \psi(m).g$ for all $\psi \in \mathrm{Hom}_{R[G]}(M, R[G] \otimes_R N)$, $g \in G$, $m \in M$.

Lemma 5.5.1. *With the above notation, there is a canonical isomorphism of right $R[G]$-modules*

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

Proof. We associate to $\varphi \in \mathrm{Hom}_R(M,N)$ the map $\tilde{\varphi}: M \to R[G] \otimes_R N$ given by

$$\tilde{\varphi}(m) := \sum_{g \in G} g \otimes \varphi(g^{-1}m)$$

We have that for all $a \in G$

$$\tilde{\varphi}(a.m) = \sum_{g \in G} g \otimes \varphi(g^{-1}a.m) = a \sum_{g \in G} a^{-1}g \otimes \varphi(g^{-1}a.m) = a.\tilde{\varphi}(m)$$

so that $\tilde{\varphi} \in \mathrm{Hom}_{R[G]}(M, R[G] \otimes_R N)$. This means that the association $\varphi \mapsto \tilde{\varphi}$ is well-defined as a map $\eta: \mathrm{Hom}_R(M,N) \to \mathrm{Hom}_{R[G]}(M, R[G] \otimes_R N)$. This is also a morphism of right $R[G]$-modules because

$$(\tilde{\varphi}.a)(m) = \tilde{\varphi}(m).a = \sum_{g \in G} ga \otimes \varphi(g^{-1}m) = \sum_{g \in G} g \otimes ((\varphi.a)(g^{-1}m) = \widetilde{\varphi.a}(m)$$

Finally we claim that in this way we have defined an isomorphism of right $R[G]$-modules. To prove this we define an inverse to our association $\varphi \mapsto \tilde{\varphi}$.

Given $\psi \in \mathrm{Hom}_{R[G]}(M, R[G] \otimes_R N)$ we set

$$\hat{\psi}(m) = n_{1_G} \Leftrightarrow \psi(m) = \sum_{g \in G} g \otimes n_g$$

Using that ψ is a morphism of $R[G]$-modules one checks easily that for all $a \in G$ it holds $\hat{\psi}(a^{-1}m) = n_a$ if $\psi(m) = \sum_{g \in G} g \otimes n_g$.

This proves that $\psi \mapsto \hat{\psi}$ defines an inverse to η, since clearly $\hat{\tilde{\varphi}}(m) = \varphi(m)$ for all $\varphi \in \mathrm{Hom}_R(M,N)$ and

$$\tilde{\hat{\psi}}(m) = \sum_{g \in G} g \otimes \hat{\psi}(g^{-1}m) = \sum_{g \in G} g \otimes n_g = \psi(m).$$

□

Now we consider the case when $N = R$ and we write $M^* = \mathrm{Hom}_R(M, R)$ for the R-dual of M. By the above lemma we see that M^* and $\mathrm{Hom}_{R[G]}(M, R[G])$ are canonically isomorphic as right $R[G]$-modules. The analogue of the above lemma for right $R[G]$-modules is obviously true so we also get the there is a canonical isomorphism of left $R[G]$-modules between $\mathrm{Hom}_R(M^*, R)$ and $\mathrm{Hom}_{R[G]}(M^*, R[G])$.

We know that there is a canonical morphism of R-modules

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

which turns out to be a morphism of left $R[G]$-modules (easy to check). By our discussion we immediately get the following corollary.

Corollary 5.5.2. *Assume that the above canonical morphism is an isomorphism for M, i.e. that M is a reflexive R-module. Then M is reflexive as $R[G]$-module.*

Proof. We get a chain of isomorphisms $M \cong \mathrm{Hom}_R(M^*, R) \cong \mathrm{Hom}_{R[G]}(M^*, R[G])$. □

5.6 The final result

By the universal coefficient theorem we know that cohomology in degree 1 is the dual to homology, i.e. that

$$H^1(Y_1(Np^r), \mathbb{Z}_p) = \mathrm{Hom}_{\mathbb{Z}}(\Gamma_1(Np^r)^{ab}, \mathbb{Z}_p) = \mathrm{Hom}_{\mathbb{Z}_p}(\Gamma_1(Np^r)^{ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p, \mathbb{Z}_p)$$

As we already remarked, Λ acts on $\Gamma_1(Np^r)^{ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ through its quotient

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

By lemma 5.5.1 we immediately get an isomorphism of Λ_r-modules

$$\mathrm{Hom}_{\mathbb{Z}_p}(\Gamma_1(Np^r)^{ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p, \mathbb{Z}_p) \cong \mathrm{Hom}_{\Lambda_r}(\Gamma_1(Np^r)^{ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p, \Lambda_r).$$

If $r \geq s > 0$ we have a projection

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

This yields the following chain of canonical morphisms

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

Now we would like to take ordinary parts in this chain of morphism. This is justified by the fact that if M is a $\mathbb{Z}_p[U]$-module which is finitely generated as $\mathbb{Z}_p$-module, then $M^* = \mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Z}_p)$ is also a finitely generated $\mathbb{Z}_p$-module and becomes a $\mathbb{Z}_p[U]$-module via the dual action of U. In this case it is easy to verify that

$$(M^*)^{ord} = (M^{ord})^*$$

Thus we can take ordinary parts to get a chain of morphisms

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

By theorem 5.3.1 we know that there is an isomorphism

$$(\Gamma_1(Np^r)^{ab}\otimes_{Z}\mathbb{Z}_p)^{ord}/\mathfrak{a}_s\cong(\Gamma_1(Np^s)^{ab}\otimes_{\mathbb{Z}}\mathbb{Z}_p)^{ord}$$

so that we indeed get a chain of morphisms

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

Now we are ready to state the key lemma of this section.

Lemma 5.6.1. *The morphism*

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

is an isomorphism.

Proof. See in the appendix. ☐

Lemma 5.6.2. *Consider the chain of* Λ*-modules*

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

Then there is a canonical isomorphism

$$\mathrm{Hom}_\Lambda(\mathbf{W}^{ord},\Lambda)\cong\varprojlim_r\mathrm{Hom}_{\Lambda_r}((\Gamma_1(Np^r)^{ab}\otimes_{\mathbb{Z}}\mathbb{Z}_p)^{ord},\Lambda_r)$$

Proof. We have the following series of canonical isomorphisms

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

where the first two isomorphisms are the obvious ones and the third one follows from corollary 5.4.2. ☐

We immediately get the following

Corollary 5.6.3. *For any* $r>0$ *there is a canonical isomorphism*

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

Proof. This follows from proposition 5.4.1 and from the previous two lemmas. ☐

Finally we can prove the main result of this chapter.

Theorem 5.6.4. *The Λ-module $\mathbf{W}^{ord}$ is free of finite rank.*

Proof. Since we already know that $\mathbf{W}^{ord}$ is a finitely generated Λ-module, it is enough (by proposition A.1.2 in the appendix) to prove that it is reflexive to see that it must be free. But now we a chain of canonical isomorphisms

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

where the first two isomorphisms are the obvious ones, the third follows form the above corollary, the fourth is a consequence of lemma 5.5.1 (because $(\Gamma_1(Np^r)^{ab}\otimes_{\mathbb{Z}}\mathbb{Z}_p)^{ord}$ is a finite free $\mathbb{Z}_p$-modules, so it is cleary reflexive as $\mathbb{Z}_p$-module, hence as Λ_r-module). $\square$

Appendix A

Appendix to chapter 5

A.1 Some commutative algebra

In this section we want to develop the theory which is necessary to prove that a finitely generated and reflexive module over the Iwasawa algebra $\Lambda := \mathbb{Z}_p[[X]]$ is actually free. This is the crucial result which is used in chapter 5 to prove that the Λ-module $\mathbf{W}^{ord}$ is free. We will actually work in some more generality.

Let A be an integral domain. For an A-module M we let

$$M^* := \mathrm{Hom}_A(M, A)$$

to be its A-dual. As usual we have a pairing

$$M^* \times M \to A, \qquad (\alpha, m) \mapsto \alpha(m)$$

inducing a canonical homomorphism of A-modules

$$\varphi_M : M \to M^{**}, \qquad m \mapsto (\alpha \mapsto \alpha(m))$$

Definition A.1.1. An A-module M is called reflexive if the canonical map φ_M defined above is an isomorphism.

Remark A.1.1. It is easy to see that if M is finitely generated and free over A, then M is reflexive.

Remark A.1.2. Since A is an integral domain it is immediate to check that M^* is always torsion-free. Hence M reflexive always implies that M is torsion free.

Proposition A.1.2 (cf. [14] prop. 5.1.9)**.** *Assume A is an n-dimensional Noetherian regular local ring, with $2 \leq n < +\infty$. Let $\{p_1, \dots, p_n\}$ be a regular system of parameters generating the maximal ideal of A. Let $p_0 = 0$. Then for a finitely generated A-module M, the following are equivalent:*

(1) For every $i = 0, \dots, n-2$ the $A/(p_0, \dots, p_i)$-module $M/(p_0, \dots, p_i)M$ is reflexive.

(2) M is a free A-module.

In particular, a reflexive A-module over a 2-dimensional regular local ring A is free.

Proof. We only need to prove that (1) implies (2). From (1) we get immediately that M is reflexive, hence torsion-free. Let $\varphi\colon A^r \twoheadrightarrow M$ be a minimal free presentation of M (i.e. M can be generated by r elements). Consider the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A^r & \xrightarrow{p_1} & A^r & \longrightarrow & (A/(p_1))^r & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\varphi} & & \downarrow{\scriptstyle\varphi} & & \downarrow{\scriptstyle\tilde{\varphi}} & & \\ 0 & \longrightarrow & M & \xrightarrow{p_1} & M & \longrightarrow & M/(p_1)M & \longrightarrow & 0 \end{array}$$

Assume for a while that $M/(p_1)M$ is a free $A/(p_1)$-module. Then by the minimality of r and Nakayama's lemma $M/(p_1)M$ is free of rank r over $A/(p_1)$. We clearly have that $\tilde{\varphi}$ is surjective and thus an isomorphism again by Nakayama's lemma. By the snake lemma we see that multiplication by p_1 is a surjection $\ker(\varphi) \xrightarrow{p_1} \ker(\varphi)$, so that by Nakayama's lemma again we deduce that $\ker(\varphi) = 0$ and that φ is an isomorphism. Hence M is free of rank r over A.

We are left to prove that $M/(p_1)M$ is a free $A/(p_1)$-module. For this note that $A/(p_1)$ is a regular local ring of dimension $n-1$ and that if $\overline{p_i} = p_i + p_1 A$ for $i = 2, \dots n$, then $\{\overline{p_2}, \dots, \overline{p_n}\}$ is a regular system of parameters of $A/(p_1)$. Thus the hypothesis (1) holds for the couple $A/(p_1)$ and $M/(p_1)M$. By descending induction we are left to check that (1) $\Rightarrow$ (2) only in the case $n = 2$ (which is the one we are actually interested in). In this case $A/(p_1)$ is a discrete valuation ring (regular local ring of dimension 1) and an integral domain. Hence the $A/(p_1)$-module $\mathrm{Hom}_A(M^*, A/(p_1))$ is torsion-free and (using that M is reflexive) we have that

$$M/(p_1)M \cong M^{**}/(p_1)M^{**} = \mathrm{Hom}_A(M^*, A) \otimes_A A/(p_1) \hookrightarrow \mathrm{Hom}_A(M^*, A/(p_1))$$

Hence $M/(p_1)M$ is torsion-free over the discrete valuation ring $A/(p_1)$, hence it is free. This concludes the proof. □

A.2 The proof of lemma 5.6.1

In this section we focus on the proof of lemma 5.6.1, i.e. we want to show that the canonical map

$$\mathrm{Hom}_{\Lambda_r}((\Gamma_1(Np^r)^{ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^{ord}, \Lambda_r)/\mathfrak{a}_s \to \mathrm{Hom}_{\Lambda_s}((\Gamma_1(Np^s)^{ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^{ord}, \Lambda_s) \quad \text{(A.1)}$$

is an isomorphism for all $r \geq s > 0$ integers.

Recall that the inclusion $\Gamma_1(Np^r) \subset \Phi_r^s$ gives rise to a transfer morphism

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

Lemma A.2.1. *The transfer morphism $\Phi_r^{s\,ab} \xrightarrow{V} \Gamma_1(Np^r)^{ab}$ commutes with the action of the Hecke operator U on its source and target.*

Proof. By the functoriality of the transfer one reduces to prove that the following diagram is commutative

$$\begin{tikzcd}
(\Phi_r^s \cap \Gamma^0(p))^{ab} \arrow[r, "V"] \arrow[d, "t(-)t^{-1}"] & (\Gamma_1(Np^r) \cap \Gamma^0(p))^{ab} \arrow[d, "t(-)t^{-1}"] \\
\Phi_r^{s\;ab} \arrow[r, "V"] & \Gamma_1(Np^r)^{ab}
\end{tikzcd}$$

where $t = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$ as usual.

One finds coset representatives for $\Gamma_1(Np^r) \cap \Gamma^0(p)$ in $\Phi_r^s \cap \Gamma^0(p)$ of the form $\sigma_d = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with d ranging through coset representatives of Γ_r in Γ_s. Then one computes that $t\sigma_d t^{-1}$ form a set of coset representatives of $\Gamma_1(Np^r)$ in Φ_r^s, so that the action of the transfer is indeed compatible with conjugation by t in this case and the above square is commutative. $\square$

Thanks to the above lemma we can restrict V to the ordinary parts of its source and target to get a morphism

$$(\Phi_r^{s\;ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^{ord} \xrightarrow{V} (\Gamma_1(Np^r)^{ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^{ord}.$$

There is clearly a dual morphism

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

fitting in the following commutative diagram

$$\begin{tikzcd}
\mathrm{Hom}_{\mathbb{Z}_p}((\Gamma_1(Np^r)^{ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^{ord}), \mathbb{Z}_p) \arrow[r, "\sim"] \arrow[d, "V^*"] & \mathrm{Hom}_{\Lambda_r}((\Gamma_1(Np^r)^{ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^{ord}, \Lambda_r) \arrow[d] \\
\mathrm{Hom}_{\mathbb{Z}_p}((\Phi_r^{s\;ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^{ord}, \mathbb{Z}_p) \arrow[dd, equal] & \mathrm{Hom}_{\Lambda_r}((\Gamma_1(Np^r)^{ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^{ord}, \Lambda_r)/\mathfrak{a}_s \arrow[d] \\
 & \mathrm{Hom}_{\Lambda_s}((\Gamma_1(Np^r)^{ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^{ord}/\mathfrak{a}_s, \Lambda_s) \arrow[d, equal] \\
\mathrm{Hom}_{\mathbb{Z}_p}((\Gamma_1(Np^r)^{ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^{ord}, \mathbb{Z}_p) \arrow[r, "\sim"] & \mathrm{Hom}_{\Lambda_s}((\Gamma_1(Np^s)^{ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^{ord}, \Lambda_s)
\end{tikzcd}$$

Let us describe this diagram:

(i) the horizontal isomorphisms are given by lemma 5.5.1;

(ii) the vertical equalities follow from theorem 5.3.1 and its proof;

(iii) the vertical arrows on the right column are the obvious ones.

The proof of the commutativity of the above diagram is essentially a computation again. Thus to prove lemma 7.1 it is enough to prove that

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

is surjective with kernel equal to $\mathfrak{a}_s \mathrm{Hom}_{\mathbb{Z}_p}((\Gamma_1(Np^r)^{ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^o rd, \mathbb{Z}_p)$.

Since by lemma A.2.1 we have that U commutes with V and since taking ordinary parts commutes with taking $\mathbb{Z}_p$-duals, we get that the above morphism is the ordinary part of the morphism

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

Taking ordinary parts is exact and commutes with the Nebentypus action of Γ (lemma 5.2.3), so that to prove our result it is enough to show that

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

is surjective with kernel $\mathfrak{a}_s \mathrm{Hom}_{\mathbb{Z}_p}(\Gamma_1(Np^r)^{ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p, \mathbb{Z}_p)$.

To see this we work in some more generality. Let G be a torsion-free congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. Then we have already used that

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

where $Y(G) \coloneqq G\backslash\mathcal{H}$ is the corresponding open Riemann surface. We know that $Y(G)$ can be completed to a compact Riemann surface $X(G)$ adding finitely many points, called cusps, which correspond to the orbit space $G\backslash\mathbb{P}^1(\mathbb{Q})$. For a precise description of the structure of $Y(G)$ as a Riemann surface and the compactification we refer to [5], chapter 2.

The Lefschetz duality theorem (cf. [6] proposition VIII.7.2) gives a canonical isomorphism

$$H^1(Y(G), \mathbb{Z}_p) \cong H_1(X(G), \mathrm{cusps}, \mathbb{Z}_p)$$

where the right-hand module is the homology taken relative to the set of cusps of $X(G)$.

Consider the group $\mathcal{M} \coloneqq \mathrm{Div}_0(\mathbb{P}^1(\mathbb{Q})$ of degree zero divisors on the set of cusps of the complex upper half plane. The group G acts on $\mathcal{M}$ via its action on $\mathbb{P}^1(\mathbb{Q})$ by Möbius transformations. We can take G-coinvariants and consider

$$(\mathcal{M} \otimes_{\mathbb{Z}} \mathbb{Z}_p)/\mathfrak{a}_G = H^0(G, \mathcal{M} \otimes_{\mathbb{Z}} \mathbb{Z}_p)$$

where $\mathfrak{a}_G$ is the augmentation ideal in the group ring $\mathbb{Z}_p[G]$.

Given a divisor $[x] - [y] \in \mathcal{M}$ one can associate to it any path from x to y in $\mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$. Such a path gives a well-defined element $[\gamma_{x,y}]$ in $H_1(X(G), \mathrm{cusps}, \mathbb{Z})$. Since we are assuming that G is torsion-free, one can apply the results of [13] to see that the association $[x] - [y] \mapsto [\gamma_{x,y}]$ gives an isomorphism

$$H^0(G, \mathcal{M} \otimes_{\mathbb{Z}} \mathbb{Z}_p) \cong H_1(X(G), \mathrm{cusps}, \mathbb{Z}_p)$$

Now assume that H is contained in G, so that $Y(G)$ and $X(G)$ are respectively quotients of $Y(H)$ and $X(H)$. As described above we have the transfer $V : G^{ab} \to H^{ab}$ and the dual morphism

$$V^* : \mathrm{Hom}_{\mathbb{Z}_p}(H^{ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p, \mathbb{Z}_p) \to \mathrm{Hom}_{\mathbb{Z}_p}(G^{ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p, \mathbb{Z}_p).$$

We get a commutative diagram:

$$\begin{tikzcd}
\operatorname{Hom}_{\mathbb{Z}_p}(H^{ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p, \mathbb{Z}_p) \arrow[r, "V^*"] \arrow[d, equal] & \operatorname{Hom}_{\mathbb{Z}_p}(G^{ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p, \mathbb{Z}_p) \arrow[d, equal] \\
H^1(Y(H), \mathbb{Z}_p) \arrow[r] \arrow[d, equal] & H^1(Y(G), \mathbb{Z}_p) \arrow[d, equal] \\
H_1(X(H), \text{cusps}, \mathbb{Z}_p) \arrow[r] \arrow[d, equal] & H_1(X(G), \text{cusps}, \mathbb{Z}_p) \arrow[d, equal] \\
(\mathcal{M} \otimes_{\mathbb{Z}} \mathbb{Z}_p)/\mathfrak{a}_H \arrow[r] & (\mathcal{M} \otimes_{\mathbb{Z}} \mathbb{Z}_p)/\mathfrak{a}_G
\end{tikzcd}$$

where the vertical arrows are the canonical isomorphisms that we have described and the horizontal arrows are (from the top to the bottom) 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

$$\mathfrak{a}_G \operatorname{Hom}_{\mathbb{Z}_p}(H^{ab} \otimes_{\mathbb{Z}} \mathbb{Z}_p, \mathbb{Z}_p).$$

In particular this finishes the proof of lemma 5.6.1 if we take $H = \Gamma_1(Np^r)$ and $G = \Phi_r^s$.

Bibliography

[1] D. Banerjee, V.G. Narasimha Kumar & E. Ghate, *Lambda-adic Forms and the Iwasawa Main Conjecture*, in *Guwahati Workshop on Iwasawa Theory of Totally Real Fields*, pages 15-47, Ramanujan Mathematical Society, 2008.

[2] A. Conti, A. Iovita & J. Tilouine, *Big Image of Galois Representations Associated with Finite Slope p-adic Families of Modular Forms*, in *Elliptic Curves, Modular Forms and Iwasawa Theory*, pages 87-123, Springer, 2016.

[3] C.W. Curtis & I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, Interscience Publishers, 1962

[4] F. Diamond & J. Im, *Modular Forms and Modular Curves*, in *Seminar on Fermat's Last Theorem* (Toronto, ON, 1993–1994), pages 39–133, Amer. Math. Soc., Providence, RI, 1995.

[5] F. Diamond & J.Shurman, *A First Course in Modular Forms*, Springer, 2005.

[6] A. Dold. *Lectures on Algebraic Topology*, Springer, New York, 1972

[7] M. Emerton, *A New Proof of a Theorem of Hida*, International Mathematics Research Notices, Volume 1999, Issue 9, 1999, pages 453–472.

[8] E. Ghate, *Ordinary Forms and their Local Galois Representations*, in *Algebra and number theory* pages 226–242. Hindustan Book Agency, 2005.

[9] H. Hida, *Elementary Theory of L-functions and Eisenstein Series*, Cambridge University Press, 1993.

[10] H. Hida, *Iwasawa Modules of Congruences of Cusp Forms*, Ann. Sci. École Norm. Sup. (4) **19** (1986), no. 2, pages 231–273.

[11] H. Hida, *Galois Representations into* $\mathrm{GL}_2(\mathbb{Z}_p[[X]])$ *attached to Ordinary Cusp Forms*, Inv. Math. **85**, pages 545-613.

[12] Min Ho Lee, *Hecke Operators on Cohomology*, Revista de la Union Matematica Argentina, Vol. 50 N.1, pages 99-144, 2009.

[13] J.I. Manin, *Parabolic Points and Zeta Functions of Modular Curves* Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), pages 19–66.

[14] J. Neukirch, A. Schmidt & K. Wingberg, *Cohomology of number fields*, Springer-Verlag, 2000.

[15] K.A. Ribet *Galois Representations Attached to Eigenforms with Nebentypus*, in *Modular functions of one variable, V*, pages 17–51, Lecture Notes in Math., Vol. 601. Springer, 1977.

[16] J.P. Serre, *Local Fields*, Springer, 1979.

[17] J.P. Serre, *Formes Modulaires et Fonctions Zêta p-adiques*, in *Modular Functions of One Variable III*, volume 350, pages 191–268. Springer-Verlag, 1972.

[18] G. Shimura,*On Elliptic Curves with Complex Multiplication as Factors of the Jactobian of Modular Function Fields*, Nagoya Math. J. **43** (1971), pages 199-208.

[19] L. Washington, *Introduction to Cyclotomic Fields*, Springer, 1980.

[20] C.A. Weibel, *An Introduction to Homological Algebra*, Cambridge Univ. Press, 1994.

[21] A. Weil, *On a Certain Type of Characters of the Idèle-Class Group of an Algebraic Number-Field*, in *Proc. Int. Symp. on Alg. Number Th. Tokyo* (1955) pages 1-7.

[22] G. Wiese, *Computational Arithmetic of Modular Forms*, lecture notes available at math.uni.lu/ wiese/notes/MFII.pdf.

[23] A. Wiles, *On Ordinary λ-adic Representations Associated to Modular Forms*, Inventiones Math. **94** (1988), pages 529-573.

[24] *The Stacks project*, stacks.math.columbia.edu/.