USC UNIVERSIDADE DE SANTIAGO DE COMPOSTELA
FACULTADE DE MATEMÁTICAS

Traballo Fin de Máster

Formas modulares e teoría de Hida

Lois Omil Pazos

Xullo, 2024

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

MÁSTER EN MATEMÁTICAS

Traballo Fin de Máster

Formas modulares e teoría de Hida

Lois Omil Pazos

Xullo, 2024

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Traballo proposto

Área de Coñecemento: Álxebra
Título: Formas Modulares e Teoría de Hida
Breve descrición do contido
O obxectivo deste traballo é estudar os resultados básicos de formas modulares, con especial énfase nas chamadas familias de Hida e nos fenómenos inherentes aos números p-ádicos. Traballaremos tanto os aspectos alxébricos da teoría como aqueles máis xeométricos, que están detrás dos últimos avances na área. Na primeira parte do traballo, o obxectivo é familiarizarse coas formas modulares, entender a estrutura alxébrica dos espazos correspondentes e motivar as súas aplicacións a problemas aritméticos. Na segunda parte, o prioritario é entender as bases da teoría de Hida desde o punto de vista alxébrico, seguindo os desenvolvementos de Hida e entendendo as demostracións dos resultados principais. Por último, segundo a evolución do traballo, poderiamos estudar tamén algúns aspectos xeométricos da teoría ou extensións da mesma a outros contextos menos coñecidos.
Recomendacións (non vinculantes)

Índice

Resumo

Este traballo ten como metas definir e estudar as formas modulares nos diferentes contextos existentes, así como introducir a teoría de Hida e expoñer as diferentes aplicacións da xeometría alxébrica no estudo das formas modulares. O traballo comeza introducindo as formas modulares clásicas no contexto do grupo linear xeral, que é a situación máis sinxela na que se poden estudar, e definindo sobre elas os operadores de Hecke. A continuación, xeneralízanse estes conceptos para poder entender as formas modulares nos chamados subgrupos de congruencia, e tras isto preséntanse varias ferramentas necesarias para avanzar ás etapas máis complexas do traballo, como poden ser os números p-ádicos ou a cohomoloxía de grupos. No seguinte paso realízase a construción de Serre das formas modulares p-ádicas e xeneralízanse os resultados presentados ata ese punto, ademais de discutir novos resultados intrínsecos desta construción. Nos últimos capítulos do documento introdúcese a teoría de Hida, que consiste en agrupar as formas modulares en familias que con boas propiedades desde o punto de vista p-ádico. Finalmente, exponse unha posible aproximación mediante conceptos da xeometría alxébrica para o estudo das formas modulares, levando á construción de Katz das formas modulares.

Abstract

This work aims to define and study modular forms in different contexts, as well as introducing Hida theory and presenting various applications of algebraic geometry in the study of modular forms. The work begins by defining classical modular forms in the context of the general linear group, which is the simplest setting in which they can be studied, and by defining Hecke operators on them. Then, these concepts are generalized to understand modular forms in the so-called congruence subgroups, and after this, various necessary tools for advancing to the more complex stages of the work are introduced, such as p-adic numbers or group cohomology. In the next stage, Serre's construction of p-adic modular

forms is carried out, and the results presented up to that point are generalized, in addition to discussing new intrinsic results of this construction. In the final chapters of the document, Hida theory is introduced. This consists of packaging modular forms into families which satisfy good algebraic properties. We further discuss a geometric approach, which leads to Katz's construction of modular forms.

Introdución

As formas modulares son un obxecto de gran relevancia en diversas áreas das matemáticas, pero resultaron ser especialmente importantes no desenvolvemento da teoría de números. Estas funcións do semiplano superior complexo deben o seu nome a matemáticos como Richard Dedekind (1831-1916) ou Felix Klein (1823-1891), que as bautizaron como "modulares" pola súa estreita relación co grupo modular $\mathrm{SL}_2(\mathbb{Z})$, que actúa no xa mencionado semiplano superior complexo pola esquerda. As formas modulares están estreitamente ligadas coa teoría das funcións elípticas, polo que o seu estudo no século XIX viña motivado polos traballos de grandes matemáticos do século XVIII, como Leonhard Euler (1707-1783), que foi un dos primeiros en estudar as funcións elípticas e as series theta. Máis adiante, xa a principios do século XIX, Carl Gustav Jacob Jacobi (1804-1851) desenvolveu en maior profundidade a teoría das series theta, que máis tarde se sabería que son exemplos de formas modulares. Simultaneamente, Leopold Kronecker (1823-1891) fixo contribucións á teoría de números e das funcións elípticas que serían de gran importancia para o futuro desenvolvemento da teoría das formas modulares. Xa no século XX Erich Hecke (1891-1947) desenvolveu a teoría dos operadores de Hecke, que actúan sobre os espazos de formas modulares e verifican moitas propiedades útiles (como a posibilidade de desenvolver unha teoría espectral sobre as formas modulares), e anos máis tarde André Weil (1906-1998) formulou unhas conxecturas que relacionaban as formas modulares coas curvas elípticas. Estas conxecturas volveríanse máis adiante unha parte fundamental do teorema de Shimura–Taniyama–Weil, o cal foi de vital importancia para a demostración de Andrew Wiles (1953) do último teorema de Fermat, no ano 1995.

Todos os estudos mencionados centrábanse nas formas modulares clásicas, pero no século XX comezouse a desenvolver simultaneamente o estudo das formas modulares p-ádicas de man de matemáticos como Jean-Pierre Serre (1926) ou Nicholas Katz (1943), este último cun enfoque máis xeral que o de Serre. Foi durante a década dos anos 80 cando o matemático xaponés Haruzo Hida (1952) levou a cabo grandes contribucións ao estudo das formas modulares p-ádicas, entre as que destacamos a hoxe en día denominada "teoría de Hida", que consiste de xeito resumido en estudar familias de funcións que interpolan

formas modulares p-ádicas. A teoría de Hida influenciou unha ampla gama de investigadores na teoría de números e na xeometría alxébrica, pois permitiu desenvolver estudos como as congruencias entre formas modulares, a teoría das formas automorfas p-ádicas ou a teoría de Hida superior, e hoxe en día segue a ser de gran relevancia no desenvolvemento da teoría de números. De feito, o emprego destas técnicas p-ádicas permitiu ao matemático Victor Kolyvagin (1955) obter o resultado máis importante ata o momento no estudo da conxectura de Birch (1931) e Swinnerton–Dyer (1927-2018).

Este traballo ten por obxectivos definir e estudar as formas modulares nos contextos clásicos, definir as súas versións p-ádicas e profundar nos principais resultados sobre as mesmas, así como introducir a teoría de Hida e expoñer as posibles aplicacións da xeometría alxébrica no estudo das formas modulares. Para levar todo isto a cabo, o traballo divídese en seis capítulos, cuxo contido vén detallado nos seguintes parágrafos.

No capítulo 1 introduciranse as formas modulares clásicas no caso máis sinxelo posible de estudar, o modular (ou grupo linear especial) das matrices cadradas de orde 2 con entradas nos números enteiros, $\mathrm{SL}_2(\mathbb{Z})$. Definiranse con detalle as formas modulares mediante a acción do grupo $\mathrm{SL}_2(\mathbb{Z})$ no semiplano superior complexo, exemplificaranse estas funcións mediante as series de Eisenstein, definiranse os operadores de Hecke nos espazos formados polas formas modulares e estudarase a dimensión destes últimos espazos (entre outras nocións e resultados que se introducirán). Este capítulo sentará pois as bases para o bo desenvolvemento de todos os demais.

O capítulo 2 xeneralizará os conceptos e resultados estudados no primeiro capítulo, levándonos así ao estudo das formas modulares no contexto dos denominados "subgrupos de congruencia", que son uns certos subgrupos do grupo linear verificando unhas certas condicións. Unha vez teñamos definidos estes grupos matriciais redefiniranse as formas modulares clásicas neste novo contexto, para o cal será necesario introducir a noción de "cúspide". Tras isto, volveremos estudar os operadores de Hecke para poder amplialos ás formas modulares definidas nos subgrupos de congruencia e introduciremos un novo tipo de operadores, os operadores "diamante". Finalmente, empregando ambos tipos de operadores definiremos as álxebras de Hecke, que nos permitirán desenvolver a xa mencionada teoría espectral das formas modulares.

O capítulo 3, cuxa temática cambiará drasticamente con respecto á dos anteriores, introducirá tres ferramentas que serán fundamentais para o estudo dos seguintes capítulos. A

primeira destas ferramentas será o corpo dos números p-ádicos xunto coas súas principais propiedades, elementais para definir as formas modulares p-ádicas. A segunda ferramenta será a cohomoloxía de grupos, que empregaremos nos capítulos vindeiros para demostrar diversos resultados. Finalmente, a última das ferramentas será a cohomoloxía parabólica, a cal nos permitirá enunciar o teorema do isomorfismo de Eichler–Shimura.

No capítulo 4 realizaremos a construción de Serre das formas modulares p-ádicas, cuxo concepto se basea en considerar os espazos de formas modulares como espazos vectoriais sobre o corpo dos números p-ádicos, a diferenza das formas clásicas que consideran estes espazos sobre $\mathbb{C}$. Unha vez definidas estas novas formas e unha vez ampliados os conceptos dos operadores de Hecke e das súas álxebras para consideralos neste novo contexto, definiremos o proxector ordinario, un operador das formas modulares p-ádicas que xogará un papel de gran importancia no traballo, pois nos permitirá definir tamén os espazos de formas ordinarias. Estes espazos terán a vantaxe de que a súa dimensión non aumentará co peso das formas modulares escollido a diferenza dos espazos de formas modulares p-ádicas habituais, cuxa dimensión medra linearmente co peso.

No capítulo 5 introduciremos a teoría de Hida, que nos permitirá agrupar as formas modulares p-ádicas de Serre en familias indexadas polos pesos das devanditas fórmulas. Aínda que estas familias son un obxecto un tanto estraño a primeira vista, veremos neste capítulo que en efecto existen, grazas a unha familia que construiremos de xeito explícito e que interpolará as series de Eisenstein p-ádicas. Unha vez feito isto, veremos como construír familias de Hida que interpolen a forma modular p-ádica desexada a partires da familia das series de Einsenstein mencionada. Tamén xeneralizaremos, unha vez máis, o concepto dos operadores de Hecke para facelos actuar sobre as familias de Hida, e introduciremos novamente o proxector ordinario paraa sí poder tamén considerar os espazos de familias de Hida ordinarias. Para finalizar, veremos varios teoremas de estrutura sobre estes últimos espazos, así como un teorema de control que nos proporcionará un isomorfismo entre un certo cociente dos espazos de familias de Hida e os espazos de formas modulares p-ádicas de Serre.

O capítulo 6 proporciona unha perspectiva sobre os posibles usos da xeometría alxébrica no estudo das formas modulares. En primeiro lugar introdúcense as curvas modulares e compróbase que son espazos de moduli, e a continuación realizaremos unha construción xeométrica que nos permitirá entender as formas modulares como funcións definidas sobre pares formados por unha curva elíptica e un punto ou un grupo cíclico dunha certa orde.

Tras todo isto, definiremos as formas modulares segundo a construción de Katz, para o cal será necesario introducir o obxecto xeométrico coñecido como a curva de Tate. Para finalizar, xeneralizaremos a definición de Katz ao caso p-ádico e exporemos brevemente como solucionar un problema que esta presenta con respecto ao operador U_p, dando así lugar á definición das formas modulares sobreconverxentes.

Capítulo 1

Caso introdutivo: $\mathrm{SL}_2(\mathbb{Z})$

Este capítulo servirá como motivación inicial para o estudo das formas modulares e da teoría de Hida nun contexto máis xeral. Con este obxectivo, daranse as definicións básicas referentes ás formas modulares e estudaranse as súas propiedades na situación máis sinxela posible: o caso do grupo linear especial sobre os números enteiros, $\mathrm{SL}_2(\mathbb{Z})$.

1.1. O semiplano superior complexo

Nesta sección daremos as definicións básicas que precisaremos para definir as formas modulares en $\mathrm{SL}_2(\mathbb{Z})$ e estudaremos algunhas das súas propiedades.

Recordemos a definición do *semiplano superior complexo*:

$$\mathbb{H} = \{z \in \mathbb{C} \mid \Im(z) > 0\},$$

onde $\Im(z)$ denota a parte imaxinaria de z. Recordemos tamén que o *grupo linear xeral* $\mathrm{GL}_2(\mathbb{R})$ está formado polas matrices cadradas de orde 2 con entradas reais e determinante non nulo (é dicir, invertibles). Este grupo matricial contén o subgrupo $\mathrm{GL}_2^+(\mathbb{R})$, constituído polas matrices de $\mathrm{GL}_2(\mathbb{R})$ con determinante positivo, e este último contén á súa vez o *grupo linear especial*, $\mathrm{SL}_2(\mathbb{R})$, definido como as matrices de $\mathrm{GL}_2(\mathbb{R})$ con determinante 1.

Imos comezar definindo a seguinte operación:

$$\begin{array}{rcl} \mathrm{GL}_2(\mathbb{R}) \times \mathbb{H} & \longrightarrow & \mathbb{C} \\ (\gamma, z) & \longmapsto & \gamma z = \begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \dfrac{az+b}{cz+d}. \end{array}$$

Lema 1.1. *Dados $z \in \mathbb{H}$ e $\gamma \in \mathrm{GL}_2(\mathbb{R})$, tense a igualdade seguinte:*

$$\Im(\gamma z) = \frac{\det \gamma}{|cz+d|^2}\Im(z), \qquad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Demostración. Próbase facendo directamente os cálculos:

$$\begin{aligned} \Im(\gamma z) &= \Im\left(\frac{az+b}{cz+d}\right) = \Im\left(\frac{(az+b)(c\bar{z}+d)}{|cz+d|^2}\right) \\ &= \frac{\Im(ac|z|^2 + adz + bc\bar{z} + bd)}{|cz+d|^2} \\ &= \frac{ad\Im(z) - bc\Im(z)}{|cz+d|^2} = \frac{\det\gamma}{|cz+d|^2}\Im(z). \end{aligned}$$

□

Corolario 1.2. $\mathrm{GL}_2^+(\mathbb{R})$ *actúa pola esquerda sobre* $\mathbb{H}$.

Demostración. En efecto, se restrinximos a operación ao caso das matrices $\gamma \in \mathrm{GL}_2^+(\mathbb{R})$, entón polo lema anterior sabemos que o signo de $\Im(\gamma z)$ coincidirá co de $\Im(z)$, logo $\gamma z \in \mathbb{H}$ para calquera $z \in \mathbb{H}$. As propiedades $Iz = z$ e $\gamma_1(\gamma_2 z) = (\gamma_1\gamma_2)z$ (con I a matriz identidade de orde 2 e $\gamma_1, \gamma_2 \in \mathrm{GL}_2^+(\mathbb{R})$) compróbanse facilmente. □

Nótese que o determinante nos proporciona a identificación $\mathrm{GL}_2^+(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R}) \times \mathbb{R}^+$, e posto que as matrices escalares $\left(\text{as da forma } \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda \end{smallmatrix}\right)\right)$ actúan trivialmente sobre $\mathbb{H}$ (é dicir, deixan fixos todos os elementos de $\mathbb{H}$), imos centrar a nosa atención nas matrices de $\mathrm{SL}_2(\mathbb{R})$, pois toda matriz de $\mathrm{GL}_2^+(\mathbb{R})$ pode escribirse como o produto dunha matriz escalar e unha matriz de $\mathrm{SL}_2(\mathbb{R})$.

O noso obxectivo agora é definir unha acción específica pola dereita de $\mathrm{GL}_2^+(\mathbb{R})$ nas funcións $f\colon \mathbb{H} \to \mathbb{C}$.

Definición 1.3. Defínese o *factor de automorfía* como a aplicación $j\colon \mathrm{GL}_2^+(\mathbb{R}) \times \mathbb{H} \to \mathbb{C}$ dada por:

$$j(\gamma, z) = cz + d, \qquad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Lema 1.4 (Relación cocíclica)**.** *Dados $\gamma_1, \gamma_2 \in \mathrm{GL}_2^+(\mathbb{R})$ e $z \in \mathbb{H}$, tense a igualdade:*

$$j(\gamma_1\gamma_2, z) = j(\gamma_1, \gamma_2 z) j(\gamma_2, z).$$

Demostración. Sexan $\gamma_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ e $\gamma_2 = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$. Resulta que

$$\gamma_1\gamma_2 = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix} \quad \text{e} \quad \gamma_2 z = \frac{a'z + b'}{c'z + d'},$$

logo podemos expresar as tres aplicacións do factor de automorfía que aparecen na igualdade do enunciado como segue:

$$j(\gamma_1\gamma_2, z) = (ca' + dc')z + (cb' + dd'), \qquad j(\gamma_1, \gamma_2 z) = c\frac{a'z + b'}{c'z + d'} + d \quad \text{e} \quad j(\gamma_2, z) = c'z + d'.$$

Conclúese a igualdade realizando os cálculos pertinentes:

$$\begin{aligned} j(\gamma_1, \gamma_2 z)j(\gamma_2, z) &= c(a'z + b') + d(c'z + d') \\ &= ca'z + cb' + dc'z + dd' = j(\gamma_1\gamma_2, z). \end{aligned}$$

□

Definición 1.5. Dada unha función $f\colon \mathbb{H} \to \mathbb{C}$, unha matriz $\gamma \in \mathrm{GL}_2^+(\mathbb{R})$ e un enteiro $k \in \mathbb{Z}$, definimos o *operador barra de peso k* como a aplicación $f|_k\gamma\colon \mathbb{H} \to \mathbb{C}$ dada por:

$$(f|_k\gamma)(z) = (\det\gamma)^{k-1} j(\gamma, z)^{-k} f(\gamma z).$$

É claro que, nas condicións da definición anterior, $f|_k I = f$ para calquera peso k. Ademais, utilizando a relación cocíclica do factor de automorfía, resulta que $f|_k(\gamma_1\gamma_2) = (f|_k\gamma_1)|_k\gamma_2$ para $\gamma_1, \gamma_2 \in \mathrm{GL}_2^+(\mathbb{R})$ arbitrarias. En efecto:

$$\begin{aligned} [(f|_k\gamma_1)|_k\gamma_2](z) &= (\det\gamma_2)^{k-1} j(\gamma_2, z)^{-k} (\det\gamma_1)^{k-1} j(\gamma_1, \gamma_2 z)^{-k} f(\gamma_1(\gamma_2 z)) \\ &= (\det(\gamma_1\gamma_2))^{k-1} j(\gamma_1\gamma_2, z)^{-k} f((\gamma_1\gamma_2)z) = (f|_k(\gamma_1\gamma_2))(z). \end{aligned}$$

Polo tanto, para cada $k \in \mathbb{Z}$ o operador barra de peso k define unha acción pola dereita de $\mathrm{GL}_2^+(\mathbb{R})$ nas aplicacións do semiplano superior complexo.

1.2. Definicións básicas sobre formas modulares

O obxectivo desta sección é definir axeitadamente as formas modulares e as formas cuspidais no grupo linear especial sobre $\mathbb{Z}$.

Sexa $\mathrm{SL}_2(\mathbb{Z})$ o subgrupo das matrices de $\mathrm{SL}_2(\mathbb{R})$ cuxas entradas son enteiras. É evidente que este subgrupo actúa nas funcións de $\mathbb{H}$ do mesmo xeito que na sección anterior.

Definición 1.6. Unha función holomorfa $f\colon \mathbb{H} \to \mathbb{C}$ dise *feblemente modular* de peso $k \in \mathbb{Z}$ en $\mathrm{SL}_2(\mathbb{Z})$ se $f|_k\gamma = f$ para calquera $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. De xeito explícito, isto equivale a

$$f(\gamma z) = j(\gamma, z)^k f(z).$$

Observación 1.7. Posto que $-I \in \mathrm{SL}_2(\mathbb{Z})$, dedúcese que non existen funcións feblemente modulares de peso impar, pois aplicando a definición previa a $-I$ teriamos

$$f(-Iz) = f(z) = (-1)^k f(z) = j(-I, z)^k f(z),$$

e se k é impar isto implica necesariamente $f = 0$.

Para poder definir axeitadamente as formas modulares en $\mathrm{SL}_2(\mathbb{Z})$ precisaremos facer algunhas consideracións analíticas. Con esta fin, obsérvese que

$$\begin{aligned}\frac{d(\gamma z)}{dz} &= \frac{a(cz+d) - c(az+b)}{(cz+d)^2} \\ &= \frac{ad-bc}{(cz+d)^2} = j(\gamma, z)^{-2},\end{aligned}$$

onde $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Podemos entón reescribir formalmente a definición das funcións feblemente modulares de peso k como "funcións $f\colon \mathbb{H} \to \mathbb{C}$ holomorfas tales que $f(z)(dz)^{\frac{k}{2}}$ sexa invariante en todo $\mathrm{SL}_2(\mathbb{Z})$". Isto proba á súa vez que se a condición orixinal das funcións feblemente modulares se verifica para dúas matrices $\gamma_1, \gamma_2 \in \mathrm{SL}_2(\mathbb{Z})$ entón tamén se verifica para $\gamma_1\gamma_2$.

Por outra banda, veremos máis adiante que o grupo $\mathrm{SL}_2(\mathbb{Z})$ está xerado polas matrices $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ e $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ (corolario 1.21). Utilizando este feito en conxunto coa observación anterior, dedúcese que para que unha función holomorfa f sexa feblemente modular basta que verifique a definición para as matrices T e S, isto é, basta que f verifique:

$$f(Tz) = f(z+1) = f(z) = j(T, z)^k f(z), \qquad f(Sz) = f\left(\frac{-1}{z}\right) = z^k f(z) = j(S, z)^k f(z).$$

Agora, se f é unha función feblemente modular, como $f(z+1) = f(z)$ entón f é claramente 1-periódica. Definindo a aplicación holomorfa

$$\begin{array}{rccc} \exp\colon & \mathbb{H} & \longrightarrow & \{q \in \mathbb{C} \mid 0 < |q| < 1\} \\ & z & \longmapsto & q = e^{2\pi i z}, \end{array}$$

como f é holomorfa e 1-periódica podemos definir $g(q) = f(z)$, é dicir,

$$g(q) = f\left(\frac{\log q}{2\pi i}\right),$$

expresión ben definida en toda rama do logaritmo grazas á periodicidade de f. A función g resulta ser holomorfa no disco unitario perforado por ser composición de funcións holomorfas, logo admite unha expansión en serie de Laurent:

$$g(q) = \sum_{n=-\infty}^{\infty} a_n q^n.$$

Polo tanto, f admite a seguinte expansión:

$$f(z) = \sum_{n=-\infty}^{\infty} a_n e^{2\pi i n z}.$$

Definición 1.8. Dise que unha función feblemente modular $f\colon \mathbb{H} \to \mathbb{C}$ de peso $k \in \mathbb{Z}$ é *meromorfa no infinito* (*holomorfa no infinito*) se $f(z) = \sum_{n \geq n_0} a_n q^n$ (e $n_0 = 0$). Nótese que f será holomorfa no infinito se, e só se, está limitada cando z se aproxima a infinito polo eixo imaxinario. Neste caso, o valor de f no infinito defínese como $f(\infty) = a_0$.
Diremos que f *se esvaece no infinito* se $n_0 = 1$ ou, equivalentemente, se $f(\infty) = 0$.

Agora si estamos en condicións de dar a definición das formas modulares:

Definición 1.9. Sexan $k \in \mathbb{Z}$ e $f\colon \mathbb{H} \to \mathbb{C}$. Dise que f é unha *forma modular* de peso k en $\mathrm{SL}_2(\mathbb{Z})$ se:

1. f é holomorfa.
2. f é feblemente modular de peso k en $\mathrm{SL}_2(\mathbb{Z})$.
3. f é holomorfa no infinito.

Unha forma modular que se esvaece no infinito dise unha *forma cuspidal*.
O espazo de formas modulares de peso k denótase $\mathrm{M}_k = \mathrm{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ e este contén o espazo de formas cuspidais de peso k, o cal escribimos como $\mathrm{S}_k = \mathrm{S}_k(\mathrm{SL}_2(\mathbb{Z}))$.

Observación 1.10. Tanto M_k como S_k son $\mathbb{C}$-espazos vectoriais. Ademais, a multiplicación de funcións dota ó espazo $\mathrm{M} = \bigoplus_{k \in \mathbb{Z}} \mathrm{M}_k$ dunha estrutura de *anel graduado* (é dicir, tal que $\mathrm{M}_r \mathrm{M}_s \subset \mathrm{M}_{r+s}$ para enteiros r e s). Finalmente, grazas á observación 1.7 se deduce trivialmente que $\mathrm{M}_k = \{0\} = \mathrm{S}_k$ para todo k impar.

1.3. Series de Eisenstein

Para cada enteiro $k \geq 3$, definimos a serie

$$G_k(z) = \sum_{(m,n) \in \mathbb{Z}^2}{}' (mz + n)^{-k}, \qquad z \in \mathbb{H},$$

onde o símbolo $'$ na parte superior do sumatorio indica que a suma se realiza sobre todos os pares $(m,n) \in \mathbb{Z}^2$ tales que $(m,n) \neq (0,0)$. O obxectivo desta sección é comprobar que estas series son formas modulares.

Comecemos co seguinte lema, que se demostra mediante un cálculo inmediato:

Lema 1.11. *G_k converxe absolutamente para todo z e uniformemente nos conxuntos da forma*

$$\Omega = \{z \in \mathbb{H} \mid |\Re(z)| \leq A, \Im(z) \geq B\},$$

sendo A e B constantes positivas e $\Re(z)$ a parte real de z.

Dedúcese inmediatamente que $G_k(z)$ é unha función holomorfa.

Proposición 1.12. *Para cada enteiro $k \geq 3$ a función holomorfa G_k é feblemente modular de peso k.*

Demostración. Sexa $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ e fagamos o seguinte cálculo:

$$\begin{aligned} G_k(\gamma z) &= \sum_{(m,n)\in\mathbb{Z}^2}{}' \left(m\frac{az+b}{cz+d} + n\right)^{-k} \\ &= \sum_{(m,n)\in\mathbb{Z}^2}{}' (cz+d)^k (m(az+b)+n(cz+d))^{-k} \\ &= (cz+d)^k \sum_{(m,n)\in\mathbb{Z}^2}{}' ((am+cn)z+(bm+dn))^{-k}. \end{aligned}$$

Nótese que o par $(am+cn, bm+dn)$ é o resultado de multiplicar o vector fila (m,n) pola matriz γ. Como esta última é invertible, resulta que o par $(am+cn, bm+dn)$ percorre todos os valores de $\mathbb{Z}^2$ agás $(0,0)$ cando (m,n) fai o propio. Polo tanto, reescribimos o último termo da igualdade como

$$G_k(\gamma z) = (cz+d)^k \sum_{(m',n')\in\mathbb{Z}^2}{}' (m'z+n')^{-k} = j(\gamma,z)^k G_k(z).$$

□

Só resta comprobar que G_k é holomorfa no infinito. Con esta fin, acharemos a súa expansión en serie de Fourier.

Comecemos dando a seguinte definición, que será relevante na serie de Fourier de G_k:

Definición 1.13. Os *números de Bernoulli* B_k defínense como segue:

$$\frac{x}{e^x-1}=\sum_{k=0}^{\infty}B_k\frac{x^k}{k!}=1-\frac{1}{2}x+\frac{1}{6}\frac{x^2}{2}-\frac{1}{30}\frac{x^4}{24}+...$$

Nótese que $B_k=0$ se k é impar e $k\geq 3$.

Precisaremos tamén a función "zeta de Riemann":

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s},\qquad s>1.$$

Esta función posúe un polo de orde 1 e pode ser estendida meromorfamente a todo $\mathbb{C}$ e holomorfamente a $\mathbb{C}\backslash\{1\}$. De feito, a función zeta de Riemann verifica as seguintes fórmulas, nas cales están presentes os números de Bernoulli:

$$\zeta(k)=\sum_{n=1}^{\infty}\left(\frac{1}{n^k}\right)=-\frac{(2\pi i)^k}{2}\frac{B_k}{k!},\qquad k\geq 2;\qquad \zeta(1-n)=-\frac{B_n}{n},\qquad n\geq 1. \tag{1.1}$$

Lema 1.14. *Tense a seguinte identidade de funcións holomorfas:*

$$\frac{1}{z}+\sum_{d=1}^{\infty}\left(\frac{1}{z-d}+\frac{1}{z+d}\right)=\pi\cot(\pi z)=\pi i-2\pi i\sum_{m=0}^{\infty}q^m,\qquad q=e^{2\pi iz}.$$

Demostración. Consideremos a fórmula do produto de Euler para a función seno:

$$\operatorname{sen}(\pi z)=\pi z\prod_{d=1}^{\infty}\left(1-\frac{z^2}{d^2}\right).$$

Se calculamos a súa derivada logarítmica obtemos a igualdade primeira:

$$\pi\cot(\pi z)=\frac{1}{z}+\sum_{d=1}^{\infty}\frac{2z}{z^2-d^2}=\frac{1}{z}+\sum_{d=1}^{\infty}\left(\frac{1}{z-d}+\frac{1}{z+d}\right).$$

Por outra banda, escribindo as funcións seno e coseno en termos da función exponencial obtemos:

$$\begin{aligned}\pi\cot(\pi z)&=\pi\frac{\cos(\pi z)}{\operatorname{sen}(\pi z)}=\pi\frac{\frac{e^{i\pi z}+e^{-i\pi z}}{2}}{\frac{e^{i\pi z}-e^{-i\pi z}}{2i}}=\pi i\frac{e^{i\pi z}+e^{-i\pi z}}{e^{i\pi z}-e^{-i\pi z}}\\&=\pi i\left(1-2\frac{e^{-i\pi z}}{e^{-i\pi z}-e^{i\pi z}}\right)=\pi i\left(1-2\frac{1}{1-e^{2\pi iz}}\right).\end{aligned}$$

Para rematar, escribimos $q=e^{2\pi iz}$ e obtemos a igualdade desexada mediante a fórmula da serie xeométrica con $|q|<1$. □

Lema 1.15. *Para cada enteiro $k \geq 2$ tense:*

$$\sum_{d\in\mathbb{Z}} \frac{1}{(z+d)^k} = \frac{(-2\pi i)^k}{(k-1)!} \sum_{d=1}^{\infty} d^{k-1} q^d.$$

Demostración. Grazas ao lema anterior sabemos que:

$$\frac{1}{z} + \sum_{d=1}^{\infty} \left(\frac{1}{z-d} + \frac{1}{z+d} \right) = \pi i - 2\pi i \sum_{d=0}^{\infty} q^d, \qquad q = e^{2\pi i z}.$$

Derivando a ambos lados da igualdade dedúcese:

$$\frac{-1}{z^2} + \sum_{d=1}^{\infty} \left(\frac{-1}{(z-d)^2} + \frac{-1}{(z+d)^2} \right) = -(2\pi i)^2 \sum_{d=1}^{\infty} d q^d.$$

Agora, como cada un dos termos da suma infinita da parte esquerda da igualdade converxe absolutamente, podemos reescribir a serie para obter a identidade

$$\sum_{d\in\mathbb{Z}} \frac{1}{(z+d)^2} = (2\pi i)^2 \sum_{d=1}^{\infty} d q^d,$$

o cal proba o enunciado para $k = 2$. O caso xeral obtense indutivamente, calculando a derivada da identidade en $k-1$. □

Como último engadido antes de estudar a xa mencionada expansión en serie de Fourier de G_k, para cada enteiro $m \geq 0$ definimos a *m-ésima función divisor* como:

$$\sigma_m(n) = \sum_{d|n} d^m.$$

Teorema 1.16. *Sexa $k \geq 4$ un enteiro par. Entón tense que $G_k(z) = 2\zeta(k)E_k(z)$, onde E_k denota a k-ésima serie de Eisenstein:*

$$E_k(z) = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n \in \mathbb{Q}[\![q]\!].$$

Demostración. Empregando o feito de que o enteiro $k \geq 4$ é par realizamos os seguintes cálculos:

$$\begin{aligned} G_k(z) &= \sum_{(m,n)\in\mathbb{Z}^2}{}' \frac{1}{(mz+n)^k} \\ &= \sum_{n\neq 0} \frac{1}{n^k} + \sum_{m\neq 0} \sum_{n\in\mathbb{Z}} \frac{1}{(mz+n)^k} \\ &= 2\zeta(k) + 2 \sum_{m=1}^{\infty} \sum_{n\in\mathbb{Z}} \frac{1}{(mz+n)^k}. \end{aligned}$$

Aplicando agora a fórmula do lema 1.15 con mz no canto de z, reescribimos o segundo termo para obter unha nova identidade:

$$G_k(z) = 2\zeta(k) + 2\sum_{m=1}^{\infty}\left(\frac{(-2\pi i)^k}{(k-1)!}\sum_{d=1}^{\infty} d^{k-1}q^{dm}\right) = 2\zeta(k) + 2\frac{(-2\pi i)^k}{(k-1)!}\sum_{m=1}^{\infty}\sum_{d=1}^{\infty} d^{k-1}q^{md}.$$

Para finalizar, agrupamos os sumatorios finais de maneira que $md = n$. Así, para que se manteña a igualdade, para cada n temos que incluír na suma todos os seus divisores d', o cal dá lugar á seguinte expresión:

$$\sum_{m=1}^{\infty}\sum_{d=1}^{\infty} d^{k-1}q^{md} = \sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n.$$

Agora aplicamos a primeira fórmula de (1.1) e volvemos utilizar a paridade de k, co cal finalizamos a proba:

$$\begin{aligned} G_k(z) &= 2\zeta(k) + 2\frac{(-2\pi i)^k}{(k-1)!}\sum_{m=1}^{\infty}\sum_{d=1}^{\infty} d^{k-1}q^{md} \\ &= 2\zeta(k) - 2\zeta(k)\frac{2k}{B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n = 2\zeta(k)E_k(z). \end{aligned}$$

□

Corolario 1.17. *Para cada enteiro par $k \geq 4$, G_k e E_k son formas modulares de peso k.*

Finalizamos esta sección realizando a construción explícita dunha forma cuspidal empregando as series de Eisenstein:

Exemplo 1.18. Sexan as series de Eisenstein

$$E_4(z) = 1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n \in \mathrm{M}_4 \quad \text{e} \quad E_6(z) = 1 - 504\sum_{n=1}^{\infty}\sigma_6(n)q^n \in \mathrm{M}_6.$$

Tanto E_4^3 como E_6^2 pertencen a M_{12}, logo a súa diferenza tamén será unha forma modular de peso 12. Explicitamente,

$$E_4^3(z) - E_6^2(z) = (1 + 720q + \dots) - (1 - 1008q + \dots) = 1728q + \dots \in \mathrm{M}_{12},$$

logo podemos definir a serie

$$\Delta(z) = \frac{E_4^3(z) - E_6^2(z)}{1728} = q - 24q^2 + 252q^3 + \dots \in \mathrm{S}_{12},$$

que é unha forma cuspidal de peso 12. De feito, esta é a forma cuspidal non nula de menor peso posible, como veremos máis adiante neste capítulo.

1.4. Dominios fundamentais

Nesta sección darase a definición xeral de dominio fundamental e estudarase o caso de $\mathrm{SL}_2(\mathbb{Z})$.

Definición 1.19. Sexa Γ un grupo actuando sobre $\mathbb{H}$. Un *dominio fundamental* de Γ é un subconxunto pechado $\mathcal{D} \subset \mathbb{H}$ tal que:

1. $\mathcal{D}$ é a clausura do seu interior.
2. Cada punto de $\mathbb{H}$ é Γ-equivalente a un punto en $\mathcal{D}$.
3. Se $z, z' \in \mathcal{D}$ son dous puntos distintos Γ-equivalentes entre si, entón ambos están na fronteira de $\mathcal{D}$.

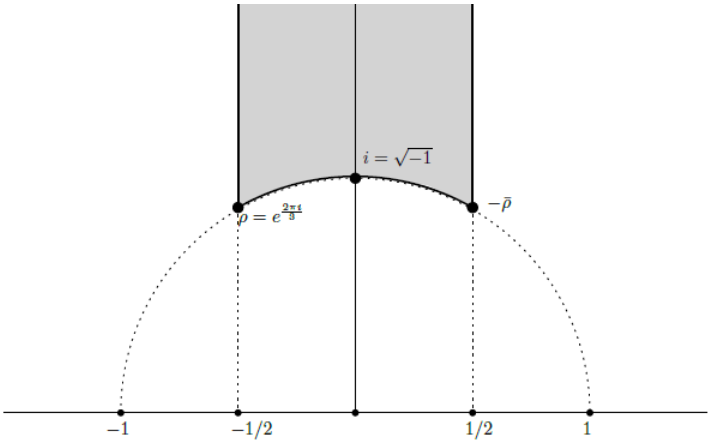


Figura 1.1: Dominio fundamental de $\mathrm{SL}_2(\mathbb{Z})$

Consideremos as matrices $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ e $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ e escribamos $\rho = e^{\frac{2\pi i}{3}}$. A demostración do resultado seguinte pódese consultar en [13, Teorema 1.5.1].

Teorema 1.20. *O subconxunto $\mathcal{D} \subset \mathbb{H}$ descrito pola figura 1.1 é un dominio fundamental (conexo) de $\mathrm{SL}_2(\mathbb{Z})$. Ademais, dado un punto $z \in \mathcal{D}$, o seu estabilizador en $\mathrm{SL}_2(\mathbb{Z})$ é:*

$$H_z = \begin{cases} C_6 = \langle ST \rangle = \left\langle \left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right) \right\rangle & \text{se } z = \rho, \\ C_6' = \langle TS \rangle = \left\langle \left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right) \right\rangle & \text{se } z = \rho + 1, \\ C_4 = \langle S \rangle = \left\langle \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \right\rangle & \text{se } z = i, \\ C_2 = \langle -I \rangle = \left\langle \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \right\rangle & \text{noutro caso.} \end{cases}$$

Corolario 1.21. *O grupo $\mathrm{SL}_2(\mathbb{Z})$ está xerado polas matrices T e S.*

Demostración. Sexa z_0 un punto interior de $\mathcal{D}$. Dada $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ o teorema previo proporciónanos unha matriz $\delta \in \langle T, S\rangle$ tal que $\delta\gamma^{-1}z_0 \in \mathcal{D}$. Polo tanto $\delta\gamma^{-1}z_0 = z_0$ e logo $\delta\gamma^{-1} = \pm I$. Se $\delta\gamma^{-1} = I$ entón non hai nada que probar, e en caso contrario, posto que $S^2 = I$, bastaría multiplicar δ por S^2. □

1.5. Operadores de Hecke

Nesta sección imos definir uns endomorfismos particulares en M_k e S_k que nos permitirán desenvolver unha teoría espectral máis adiante.

Comecemos fixando a seguinte notación para cada enteiro $m > 0$:

$$\mathcal{M}_m = \left\{A \in \mathrm{GL}_2^+(\mathbb{Z}) \mid \det A = m\right\}.$$

Definimos agora a seguinte acción de $\mathrm{SL}_2(\mathbb{Z})$ no anterior grupo matricial:

$$\begin{array}{ccc} \mathrm{SL}_2(\mathbb{Z}) \times \mathcal{M}_m & \longrightarrow & \mathcal{M}_m \\ (\gamma, A) & \longmapsto & \gamma A. \end{array}$$

A anterior aplicación está ben definida pola multiplicidade do determinante, e é evidente que é unha acción posto que a identidade actúa trivialmente sobre toda matriz de $\mathcal{M}_m$ e posto que o produto de matrices é asociativo.

Proposición 1.22. *Sexa $m > 0$ un enteiro. Tense o seguinte conxunto de representantes para a acción anterior (é dicir, facendo actuar $\mathrm{SL}_2(\mathbb{Z})$ sobre el obtense todo $\mathcal{M}_m$):*

$$\mathcal{M}'_m = \left\{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \mid ad = m,\ 0 \le b \le d-1,\ d > 0\right\}.$$

Ademais, dous elementos de $\mathcal{M}'_m$ nunca son equivalentes (é dicir, na órbita dunha matriz non hai ningunha matriz de $\mathcal{M}'_m$ agás ela mesma).

Demostración. Dada $A \in \mathcal{M}_m$ arbitraria vexamos que existen matrices $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ e $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in \mathcal{M}'_m$ tales que

$$\gamma^{-1}A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}.$$

Escribimos $A = \left(\begin{smallmatrix} x_1 & x_2 \\ x_3 & x_4 \end{smallmatrix}\right)$ e definimos $a = \mathrm{mcd}(x_1, x_3)$, $y_1 = \frac{x_1}{a}$ e $y_3 = \frac{x_3}{a}$. Grazas á identidade de Bézout sabemos que existen $y_2, y_4 \in \mathbb{Z}$ tales que $y_4y_1 - y_2y_3 = 1$, logo

$\left(\begin{smallmatrix} y_1 & y_2 \\ y_3 & y_4 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Así,

$$\begin{aligned}\begin{pmatrix} y_1 & y_2 \\ y_3 & y_4 \end{pmatrix}^{-1} A &= \begin{pmatrix} y_4 & -y_2 \\ -y_3 & y_1 \end{pmatrix} \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \\ &= \begin{pmatrix} y_4x_1 - y_2x_3 & y_4x_2 - y_2x_4 \\ y_1x_3 - y_3x_1 & y_1x_4 - y_3x_2 \end{pmatrix} = \begin{pmatrix} a & b' \\ 0 & d \end{pmatrix},\end{aligned}$$

onde b' e d son $y_4x_2 - y_2x_4$ e $y_1x_4 - y_3x_2$ respectivamente. Podemos supoñer $d > 0$, pois en caso contrario bastaría multiplicar por $-I$ pola esquerda.
Tomamos agora k o menor enteiro tal que $b' - kd \leq d - 1$ e definimos $b = b' - kd$. Tense entón que $0 \leq b \leq d - 1$, e así

$$\begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b' \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}.$$

Bastaría entón tomar

$$\gamma = \begin{pmatrix} y_1 & y_2 \\ y_3 & y_4 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix},$$

omitindo a segunda matriz se $d = y_1x_4 - y_3x_2 > 0$.
Para finalizar a demostración, supoñamos que existen $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right), \left(\begin{smallmatrix} a' & b' \\ 0 & d' \end{smallmatrix}\right) \in \mathcal{M}'_m$ tales que

$$\gamma \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix},$$

onde $\gamma = \left(\begin{smallmatrix} z_1 & z_2 \\ z_3 & z_4 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Calculando o produto do lado esquerdo da igualdade obtemos

$$\begin{pmatrix} z_1a & z_1b + z_2d \\ z_3a & z_3b + z_4d \end{pmatrix} = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix},$$

do cal se deduce que $z_3 = 0$. Como $\det \gamma = 1$ entón necesariamente $z_1z_4 = 1$, logo $z_1 = z_4 = \pm 1$, pero sabemos que $d, d' > 0$ e

$$\begin{pmatrix} z_1a & z_1b + z_2d \\ 0 & z_4d \end{pmatrix} = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix},$$

polo tanto $z_4 = 1 = z_1$ e $a = a', d = d'$. Finalmente, sabemos que $b + z_2d = b'$ pola igualdade matricial, ou equivalentemente $b - b' = -z_2d$, pero por outra banda $-d + 1 \leq b - b' \leq d - 1$, polo que deducimos que $z_2 = 0$ e entón $b = b'$. □

Denotemos por $\mathcal{M}_m/_\sim$ o espazo de órbitas da acción que estamos a tratar, o cal ten por conxunto de representantes $\mathcal{M}'_m$, como acabamos de ver na proposición anterior.

Definición 1.23. Sexan $m > 0$ e k enteiros. Defínese o m-ésimo *operador de Hecke* en $\mathrm{SL}_2(\mathbb{Z})$ como a aplicación $T_m \colon \mathrm{M}_k \to \mathrm{M}_k$ dada por:

$$T_m f = \sum_{\gamma \in \mathcal{M}_m/\sim} f|_k \gamma.$$

Obsérvese que a suma non depende da elección de representantes en $\mathcal{M}_m/\sim$, logo podemos reescribir a definición como

$$T_m f = \sum_{\substack{ad=m \\ d>0}} \sum_{b=0}^{d-1} f|_k \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right).$$

Aplicando isto a un elemento $z \in \mathbb{H}$ teriamos:

$$T_m f(z) = m^{k-1} \sum_{\substack{ad=m \\ d>0}} \sum_{b=0}^{d-1} d^{-k} f\left(\frac{az+b}{d}\right).$$

No caso particular no que $m = p$ é un número primo teríase a seguinte expresión:

$$T_p f(z) = p^{k-1} \sum_{b=0}^{p-1} p^{-k} f\left(\frac{z+b}{p}\right) + p^{k-1} f(pz) = \frac{1}{p} \sum_{b=0}^{p-1} f\left(\frac{z+b}{p}\right) + p^{k-1} f(pz).$$

Proposición 1.24. *Dados $m, k \in \mathbb{Z}$, $m > 0$, o operador de Hecke $T_m \colon \mathrm{M}_k \to \mathrm{M}_k$ está ben definido e é un endomorfismo. Ademais, a restrición de T_m a S_k é á súa vez un endomorfismo de S_k.*

Demostración. Sexa $f \in \mathrm{M}_k$. En vista de definición anterior, é evidente que $T_m f$ é holomorfa en todo $\mathbb{H}$ e no infinito e que é linear. Se, ademais, $f \in \mathrm{S}_k$ entón tamén se deduce trivialmente que $T_m f$ se esvaece no infinito. Vexamos pois que $T_m f$ é feblemente modular de peso k. Sexan $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ e $z \in \mathbb{H}$:

$$\begin{aligned}
T_m f(\gamma z) &= m^{k-1} \sum_{\substack{ad=m \\ d>0}} \sum_{b=0}^{d-1} d^{-k} f\left(\frac{a(\gamma z)+b}{d}\right) \\
&= m^{k-1} \sum_{\substack{ad=m \\ d>0}} \sum_{b=0}^{d-1} d^{-k} f\left(\left[\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)\gamma\right] z\right) \\
&= \sum_{\substack{ad=m \\ d>0}} \sum_{b=0}^{d-1} \left(\det \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)\gamma\right)^{k-1} j\left(\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right), \gamma z\right)^{-k} f\left(\left[\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)\gamma\right] z\right) \\
&= \sum_{\substack{ad=m \\ d>0}} \sum_{b=0}^{d-1} \left(\det \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)\gamma\right)^{k-1} j\left(\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)\gamma, z\right)^{-k} j(\gamma, z)^k f\left(\left[\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)\gamma\right] z\right) \\
&= j(\gamma, z)^k \sum_{\substack{ad=m \\ d>0}} \sum_{b=0}^{d-1} \left(f|_k \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)\gamma\right)(z) = j(\gamma, z)^k T_m f(z),
\end{aligned}$$

onde se empregou a relación cocíclica do factor de automorfía e a independencia do representante na definición de operador de Hecke. Dedúcese pois que $T_m f$ é feblemente modular de peso k, logo T_m está ben definida e é un endomorfismo de M_k. É obvio que a restrición de T_m a S_k segue sendo linear, logo é un endomorfismo de S_k. □

Veremos máis adiante que os operadores de Hecke verifican varias propiedades interesantes, como por exemplo:

- $T_m T_n = T_n T_m$ para enteiros $n, m > 0$ arbitrarios.
- Dada $f \in \mathrm{M}_k$ para certo $k \in \mathbb{Z}$, con $f(z) = \sum_{n=0}^{\infty} a_n(f) q^n$, resulta que para todo $m > 0$ enteiro:
$$T_m f(z) = \sum_{n=0}^{\infty} a_n(T_m f) q^n.$$

1.6. Dimensión dos espazos M_k e S_k

Para finalizar o capítulo faremos un breve estudo da forma e da dimensión dos distintos espazos de formas modulares e cuspidais sobre $\mathrm{SL}_2(\mathbb{Z})$.

Sexa f unha función feblemente modular meromorfa non nula nun subconxunto aberto de $\mathbb{H}$ e no infinito, e denotemos por $v_p(f)$ a valencia (ou orde) de f en $p \in \mathbb{H}$, é dicir, $v_p(f)$ é o único enteiro n tal que $(z-p)^{-n} f(z)$ é holomorfa e non nula en p. Así mesmo, defínese a orde de f no infinito como $v_\infty(f) = n_0$, onde $f(z) = \sum_{n \geq n_0} a_n q^n$.

Supoñamos agora que f é de peso k e sexan $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, $p \in \mathbb{H}$ con $v_p(f) = n$. Pódese comprobar facilmente que

$$\lim_{z \to \gamma p} (z - \gamma p)^{-n} f(z) = j(\gamma, p)^{k+2n} \lim_{z \to p} (z-p)^{-n} f(z),$$

e ademais $j(\gamma, p) \neq 0$, logo $v_p(f) = f_{\gamma p}(f)$. Así, a valencia de f nos puntos dunha mesma órbita da acción usual de $\mathrm{SL}_2(\mathbb{Z})$ en $\mathbb{H}$ é sempre a mesma.

Para o estudo que pretendemos realizar empregarase o seguinte resultado, cuxa proba se pode achar en [13, §1.6.2], subsección 1.6.2.

Teorema 1.25 (Fórmula de valencia)**.** *Sexa unha función feblemente modular de peso k en $\mathrm{SL}_2(\mathbb{Z})$, meromorfa en $\mathbb{H}$ e no infinito. Verifícase a igualdade seguinte:*

$$v_\infty(f) + \frac{1}{2} v_i(f) + \frac{1}{3} v_\rho(f) + \sum_{\substack{\tau \in \mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{H} \\ \tau \neq i, \rho}} v_\tau(f) = \frac{k}{12},$$

onde $\rho = e^{\frac{2\pi i}{3}}$ e $\mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ representa o conxunto de órbitas da acción usual.

Nótese que, en particular, a fórmula de valencia é valida para formas modulares e para formas cuspidais.

Nos seguintes resutados empregarase a notación xa introducida para as series de Eisenstein, así como a forma cuspidal Δ definida no exemplo 1.18.

Teorema 1.26. *Sexa $k \in \mathbb{Z}$ par. Téñense as seguintes afirmacións:*

1. $\mathrm{M}_k = \{0\}$ *se* $k < 0$ *ou* $k = 2$.
2. $\mathrm{S}_k = \{0\}$ *se* $k < 12$.
3. $\mathrm{M}_0 = \mathbb{C}$.
4. $\mathrm{S}_{12} = \mathbb{C}\Delta$.

Demostración.

1. Se aplicamos a fórmula de valencia a unha forma modular non nula de peso k entón o lado esquerdo da igualdade é non negativo (xa que f é holomorfa en $\mathbb{H}$ e no infinito), logo necesariamente $k \geq 0$ pois o lado dereito tamén debe ser non negativo. Ademais, se $k = 2$ entón o lado dereito da fórmula sería $\frac{1}{6}$, pero o lado esquerdo consiste unha suma de múltiplos non negativos de $1, \frac{1}{2}$ e $\frac{1}{3}$, polo que non existe ningunha posible configuración de valencias tal que esta suma sexa igual a $\frac{1}{6}$ $\left(\text{pode ser nula ou maior ou igual que } \frac{1}{3}\right)$.

2. Supoñamos que existe $0 \neq f \in \mathrm{S}_k$. Entón $v_\infty(f) \geq 1$, logo a fórmula de valencia garante $k \geq 12$ para que o lado dereito da igualdade sexa maior ou igual que 1.

3. Sexa $f \in \mathrm{M}_0$. Como a función constante $g = f(\infty)$ tamén pertence a M_0 entón a diferencia $f - g$ está en $\mathrm{S}_0 = \{0\}$. Así, $f = g$, logo f é unha función constante e así $\mathrm{M}_0 = \mathbb{C}$ é o espazo de funcións constantes en $\mathbb{H}$.

4. Sexa $f \in \mathrm{S}_{12}$. Sabemos que $v_\infty(f) \geq 1$, e como o lado dereito da fórmula de valencia con $k = 12$ é igual a 1 entón necesariamente $v_\infty(f) = 1$, polo que f non posúe ningún cero nin ningún polo en $\mathbb{H}$. Definamos agora a seguinte función para cada $z \in \mathbb{H}$:

$$g(z) = f(z) - \frac{f(i)}{\Delta(i)}\Delta(z) \in \mathrm{S}_{12}.$$

   Resulta evidente que $g(i) = 0$. Se g non fose a función nula entón aplicando a fórmula de valencia a g obteriamos unha contradición, pois $v_\infty(g) \geq 1$, $v_i(f) \geq 1$ e g é de peso 12. Conclúese entón que $g = 0$, logo f é un múltiplo de Δ para cada $z \in \mathbb{H}$:

$$f(z) = \frac{f(i)}{\Delta(i)}\Delta(z) \in \mathbb{C}\Delta.$$

□

Corolario 1.27. *Sexa k un enteiro.*

1. $\mathrm{S}_{k+12} = \Delta \mathrm{M}_k$.
2. *Para $k \geq 4$ tense a seguinte identificación:* $\mathrm{M}_k = \mathbb{C}E_k \oplus \mathrm{S}_k$.
3. *Se k é negativo ou impar entón* $\mathrm{M}_k = \{0\}$. *Ademais, para cada $k \geq 0$ par temos a seguinte afirmación:*

$$\dim(\mathrm{M}_k) = \begin{cases} \left\lfloor \frac{k}{12} \right\rfloor & \text{se } k \equiv 2 \,(\text{mód } 12), \\ 1 + \left\lfloor \frac{k}{12} \right\rfloor & \text{se } k \not\equiv 2 \,(\text{mód } 12). \end{cases}$$

Demostración.

1. Para $k < 0$ a igualdade é evidente grazas ao teorema anterior, e o caso $k = 0$ é precisamente o punto 4 do teorema 1.26. Supoñamos agora $k \geq 1$ e sexa $f \in \mathrm{S}_{k+12}$. A función $g = \frac{f}{\Delta}$ é holomorfa en $\mathbb{H}$ posto que Δ non se anula, e $g \in \mathrm{M}_k$ xa que $v_\infty(g) = v_\infty(f) - v_\infty(\Delta) = v_\infty(f) - 1 \geq 0$ por ser f unha forma cuspidal, do cal se deduce $\mathrm{S}_{k+12} \subset \Delta \mathrm{M}_k$. Conclúese así a igualdade buscada, pois a inclusión oposta vén dada pola observación 1.10.

2. Sexa a aplicación linear

$$\begin{array}{rccc} \varphi\colon & \mathrm{M}_k & \longrightarrow & \mathbb{C} \\ & f & \longmapsto & f(\infty). \end{array}$$

   Resulta que $\mathrm{S}_k = \ker \varphi$, e ademais φ é sobrexectiva debido a que a imaxe de E_k mediante dita aplicación é 1. Grazas ao primeiro teorema de isomorfía, séguese que $\mathrm{M}_k/\mathrm{S}_k \cong \mathbb{C}E_k$ e este isomorfismo proporciona a identificación buscada.

3. Obsérvese que as afirmación anteriores dan lugar a unha fórmula por recorrencia para obter M_k:

$$\mathrm{M}_k = \mathbb{C}E_k \oplus \mathrm{S}_k = \mathbb{C}E_k \oplus \Delta \mathrm{M}_{k-12}.$$

   Agora, $\mathrm{M}_k = \{0\}$ para k impar pola observación 1.10, e o mesmo acontece para $k < 0$ polo teorema previo.
   Finalmente, probemos a fórmula proporcionada mediante indución no peso $k \geq 2$. Grazas ao teorema anterior sabemos que $\dim(\mathrm{M}_2) = \dim(\{0\}) = 1$, xusto como a fórmula afirma. Ademais, se $k \in \{4, 6, 8, 10\}$ entón

$$\dim(\mathrm{M}_k) = \dim(\mathbb{C}E_k \oplus \mathrm{S}_{12}) = \dim(\mathbb{C}) + \dim(\Delta \mathrm{M}_{k-12}) = 1 + \dim(\mathrm{M}_{k-12}) = 1,$$

tamén como dita a fórmula. Para rematar, se k é par e $k \geq 12$ entón aplicamos $\dim(\mathrm{M}_k) = 1 + \dim(\mathrm{M}_{k-12})$, coincidindo unha vez máis coa fórmula do enunciado.

□

Observación 1.28. En particular, os espazos M_k e S_k teñen dimensión finita e esta medra a medida que crece o peso k.

Capítulo 2

Formas modulares clásicas

Este capítulo pretende xeneralizar e completar os contidos presentados no anterior. Polo tanto, nas próximas páxinas introduciranse os chamados "subgrupos de congruencia" e redefiniranse as formas modulares de xeito adaptado a estes novos contextos. Tamén se reescribirán as nocións de operadores de Hecke e se profundará no seu estudo.

2.1. Subgrupos de congruencia

Nesta sección definiremos os subgrupos de congruencia e introduciremos notacións relativas aos mesmos.

Definición 2.1. Sexa $N \geq 1$ un enteiro. Defínese o *subgrupo de congruencia principal* de nivel N como o seguinte subgrupo de $\mathrm{SL}_2(\mathbb{Z})$:

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

Dito doutro xeito: $\Gamma(N)$ é o subgrupo de $\mathrm{SL}_2(\mathbb{Z})$ formado polas matrices γ congruentes coa matriz identidade módulo N.

Nótese que, en particular, $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$. Por outra banda, se para cada nivel $N \geq 1$ consideramos a aplicación redución $\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$, que a cada enteiro lle asigna a súa clase de equivalencia módulo N, e definimos o homomorfismo (sobrexectivo)

$$\pi_N \colon \mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$$

que leva as entradas dunha matriz nas súas correspondentes reducións módulo N, entón resulta que $\Gamma(N)$ coincide co núcleo de π_N. Polo tanto, o subgrupo de congruencia principal é un subgrupo normal de índice finito de $\mathrm{SL}_2(\mathbb{Z})$ para calquera nivel.

Definición 2.2. Dise que un subgrupo Γ de $\mathrm{SL}_2(\mathbb{Z})$ é un *subgrupo de congruencia* se existe algún enteiro $N \geq 1$ tal que

$$\Gamma(N) \subset \Gamma \subset \mathrm{SL}_2(\mathbb{Z}).$$

De ser así, defínese o *nivel* de Γ como o menor N tal que $\Gamma(N) \subset \Gamma$.

Exemplo 2.3. Para cada enteiro $N \geq 1$ é inmediato comprobar que tanto

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

como

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

son subgrupos de congruencia de nivel N. De feito, tense a seguinte cadea de inclusións:

$$\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z}).$$

Proposición 2.4. *Tense un isomorfismo* $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^\times$ *para cada* $N \geq 1$ *dado por:*

$$\begin{array}{ccc} \Gamma_0(N)/\Gamma_1(N) & \longrightarrow & (\mathbb{Z}/N\mathbb{Z})^\times \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \longmapsto & d. \end{array}$$

Demostración. Consideremos a seguinte aplicación:

$$\begin{array}{rccc} f\colon & \Gamma_0(N) & \longrightarrow & (\mathbb{Z}/N\mathbb{Z})^\times \\ & \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \longmapsto & d. \end{array}$$

Dada $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ unha matriz de $\Gamma_0(N)$ sabemos que o seu determinante é igual a 1 e que $c \equiv 0 \,(\mathrm{mód}\, N)$, logo:

$$ad - bc \equiv ad \equiv 1 \,(\mathrm{mód}\, N).$$

Dedúcese entón que d é unha unidade en $\mathbb{Z}/N\mathbb{Z}$, logo a aplicación está ben definida. Ademais, f é un homomorfismo de grupos, como se proba a continuación:

$$\begin{aligned} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} &= \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix} \\ &\equiv \begin{pmatrix} aa' & ab' + bd' \\ 0 & dd' \end{pmatrix} \longmapsto dd'. \end{aligned}$$

É obvio que a aplicación é sobrexectiva, e ademais resulta que $\ker(f) = \Gamma_1(N)$, pois se $f(\gamma) = d \equiv 1 \,(\mathrm{mód}\, N)$ entón necesariamente $a \equiv 1 \,(\mathrm{mód}\, N)$ posto que $ad \equiv 1 \,(\mathrm{mód}\, N)$, como vimos previamente. Conclúese o resultado polo primeiro teorema de isomorfía para grupos: $\Gamma_0(N)/\ker(f) \cong \mathrm{Im}(f)$. □

2.2. Formas modulares

O obxectivo desta sección é redefinir as formas modulares e as formas cuspidais no contexto dos subgrupos de congruencia, así como estudar brevemente as propiedades que verifican e comparalas coas estudadas no caso de $\mathrm{SL}_2(\mathbb{Z})$.

Comecemos reconsiderando a noción de modularidade feble:

Definición 2.5. Sexa Γ un subgrupo de congruencia. Unha función holomorfa $f\colon \mathbb{H} \to \mathbb{C}$ dise *feblemente modular* de peso $k \in \mathbb{Z}$ en Γ se $f|_k\gamma = f$ para calquera $\gamma \in \Gamma$.

Nótese que a definición anterior é, en efecto, unha xeneralización estrita da súa análoga en $\mathrm{SL}_2(\mathbb{Z})$ para subgrupos de congruencia. Así, para poder definir as formas modulares en subgrupos de congruencia soamente resta xeneralizar a noción de holomorfidade no infinito, para o cal precisaremos introducir a noción de "cúspide".

Consideremos a *liña proxectiva racional* $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$ e definamos unha acción de $\mathrm{SL}_2(\mathbb{Z})$ (de feito, de $\mathrm{GL}_2(\mathbb{Q})$) en $\mathbb{P}^1(\mathbb{Q})$ como

$$\begin{array}{ccc} \mathrm{SL}_2(\mathbb{Z}) \times \mathbb{P}^1(\mathbb{Q}) & \longrightarrow & \mathbb{P}^1(\mathbb{Q}) \\ (\gamma, x) & \longmapsto & \gamma x = \begin{pmatrix} a & b \\ c & d \end{pmatrix} x = \dfrac{ax+b}{cx+d}, \end{array}$$

onde se entende que $\gamma\infty = \frac{a}{c}$ e que $\gamma x = \infty$ se $cx + d = 0$ (comprobar que esta aplicación é unha acción é inmediato). Así mesmo, imos considerar o seguinte conxunto:

$$\mathrm{SL}_2(\mathbb{Z})_\infty = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \infty = \infty \right\}.$$

Proposición 2.6. *A acción de* $\mathrm{SL}_2(\mathbb{Z})$ *en* $\mathbb{P}^1(\mathbb{Q})$ *é transitiva, logo induce un isomorfismo* $\mathrm{SL}_2(\mathbb{Z})/\mathrm{SL}_2(\mathbb{Z})_\infty \cong \mathbb{P}^1(\mathbb{Q})$, *onde resulta que* $\mathrm{SL}_2(\mathbb{Z})_\infty = \langle \pm T \rangle$, $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

Demostración. Vexamos que a órbita de ∞ coincide con $\mathbb{P}^1(\mathbb{Q})$. Sexa $\frac{a}{c} \in \mathbb{P}^1(\mathbb{Q})$ con $\mathrm{mcd}(a, c) = 1$. Grazas á identidade de Bézout podemos tomar $b, d \in \mathbb{Z}$ tales que $ad - bc = 1$, polo que a matriz $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ pertence a $\mathrm{SL}_2(\mathbb{Z})$ e ademais verifica $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\infty = \frac{a}{c}$, co cal se conclúe

a transitividade da acción e se deduce o isomorfismo buscado. Finalmente:

$$\begin{aligned}\mathrm{SL}_2(\mathbb{Z})_\infty &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \infty = \infty \right\} \\ &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \frac{a}{c} = \infty \right\} \\ &= \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \right\} = \langle \pm T \rangle.\end{aligned}$$

□

Definición 2.7. Defínese o conxunto de *cúspides* dun subgrupo de congruencia Γ como o espazo de Γ-órbitas de $\mathbb{P}^1(\mathbb{Q})$ ou, equivalentemente, como $\mathrm{Cusps}(\Gamma) = \Gamma \backslash \mathrm{SL}_2(\mathbb{Z}) / \mathrm{SL}_2(\mathbb{Z})_\infty$.

Obsérvese que, grazas á transitividade da acción de $\mathrm{SL}_2(\mathbb{Z})$ en $\mathbb{P}^1(\mathbb{Q})$, a única cúspide de $\mathrm{SL}_2(\mathbb{Z})$ é ∞.

Exemplo 2.8. Imos probar que, dado un primo p calquera, $\mathrm{Cusps}(\Gamma_0(p)) = \{\infty, 0\}$. Sexa un elemento $\gamma = \left(\begin{smallmatrix} a & b \\ pc & d \end{smallmatrix}\right) \in \Gamma_0(p)$ con $ad - pbc = 1$. Calculemos a órbita de ∞:

$$\begin{aligned}\Gamma_0(p) \cdot \infty &= \left\{ \begin{pmatrix} a & b \\ pc & d \end{pmatrix} \infty \mid \begin{pmatrix} a & b \\ pc & d \end{pmatrix} \in \Gamma_0(p) \right\} \\ &= \left\{ \frac{a}{pc} \mid a, c \in \mathbb{Z}, \mathrm{mcd}(a, pc) = 1 \right\} \\ &= \left\{ \frac{r}{s} \mid p | s, \mathrm{mcd}(r, s) = 1 \right\}.\end{aligned}$$

Esta órbita consiste pois no infinito xunto con aqueles números racionais tales que, ao expresalos como fraccións irreducibles, teñen denominador divisible por p. Agora, o elemento $0 = \frac{0}{1}$ non pertence a esta órbita, polo que ten a súa propia órbita. Calculémola:

$$\Gamma_0(p) \cdot 0 = \left\{ \begin{pmatrix} a & b \\ pc & d \end{pmatrix} 0 \mid \begin{pmatrix} a & b \\ pc & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \right\} = \left\{ \frac{b}{d} \mid b, d \in \mathbb{Z}, \mathrm{mcd}(b, d) = 1, p \nmid d \right\}.$$

A xeneralización das formas modulares a subgrupos de congruencia imporá como condición final a unha función $f \colon \mathbb{H} \to \mathbb{C}$ a necesidade de ser holomorfa non só no infinito, senón en todas as cúspides de Γ. Precisamos pois definir este concepto axeitadamente, para o cal teremos que estudar a expansión de Fourier de f en cada cúspide.

Sexa Γ un subgrupo de congruencia de nivel N. Nótese que a matriz $\left(\begin{smallmatrix} 1 & N \\ 0 & 1 \end{smallmatrix}\right)$ pertence a $\Gamma(N)$, logo ten sentido considerar o menor enteiro $h > 0$ tal que $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma$. Escribimos agora

$$q_h = q_h(z) = e^{\frac{2\pi i z}{h}}$$

e notemos que a aplicación que a cada $z \in \mathbb{H}$ lle asigna $q_h(z)$ é periódica con período h. Definimos agora $g(q_h) = f(z)$, é dicir, $g = f \circ q_h^{-1}$, polo que g admite unha expansión en serie de Laurent como segue:

$$f(z) = g(q_h) = \sum_{n=-\infty}^{\infty} a_n q_h^n.$$

Observación 2.9. No caso de $\mathrm{SL}_2(\mathbb{Z})$, $h = 1$, logo $q_h = q = e^{2\pi i z}$, polo que a expansión en q_h de f dada xeneraliza estritamente a expansión de f en q (en $\mathrm{SL}_2(\mathbb{Z})$) empregada na definición 1.8.

Xa podemos entón considerar funcións holomorfas $f\colon \mathbb{H} \to \mathbb{C}$ feblemente modulares nun subgrupo de congruencia Γ e holomorfas no infinito. Tomemos agora unha cúspide $s \in \mathrm{Cusps}(\Gamma)$, $s \neq \infty$ e consideremos $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ tal que $\alpha\infty = s$ (tal matriz existe pola transitividade da acción de $\mathrm{SL}_2(\mathbb{Z})$ en $\mathbb{P}^1(\mathbb{Q})$). Sexan $z \in \mathbb{H}$, $k \in \mathbb{Z}$ e consideremos a seguinte igualdade:

$$f(\alpha z) = j(\alpha, z)^k (f|_k\alpha)(z).$$

Como $j(\alpha, z) \neq 0$ e $j(\alpha, z) = \infty$ cando z se aproxima ao infinito, entón o comportamento de $f(z)$ preto de s relaciónase co de $(f|_k\alpha)(z)$ preto de ∞.
Supoñamos agora que f é feblemente modular de peso k en Γ. Tense a seguinte igualdade para $\gamma \in \Gamma$:

$$\begin{aligned}(f|_k\alpha)|_k\left(\alpha^{-1}\gamma\alpha\right) = f|_k\left(\alpha\alpha^{-1}\gamma\alpha\right) &= f|_k(\gamma\alpha) \\ &= (f|_k\gamma)|_k\alpha = f|_k\alpha.\end{aligned}$$

Dedúcese entón que a aplicación $f|_k\alpha$ é invariante polo grupo $\Gamma' = \alpha^{-1}\Gamma\alpha$, e como $\Gamma(N)$ (con N o nivel de Γ) é un subgrupo normal de $\mathrm{SL}_2(\mathbb{Z})$ entón Γ' é un novo subgrupo de congruencia de nivel N. Así, procedendo de xeito análogo a como o fixemos anteriormente, $f|_k\alpha$ ten unha expansión en serie de Laurent en q_N:

$$f|_k\alpha = \sum_{n=-\infty}^{\infty} b_n q_N^n.$$

Podemos entón dicir que f é holomorfa na cúspide s se $f|_k\alpha$ é holomorfa no infinito, co cal xa temos todo o necesario para definir as funcións modulares nos subgrupos de congruencia.

Definición 2.10. Sexan $k \in \mathbb{Z}$, $f\colon \mathbb{H} \to \mathbb{C}$ e Γ un subgrupo de congruencia de nivel $N \geq 1$. Dise que f é unha *forma modular* de peso k en Γ se:

1. f é holomorfa.

2. f é feblemente modular de peso k en Γ.

3. $f|_k\alpha$ é holomorfa no infinito para toda $\alpha \in \mathrm{SL}_2(\mathbb{Z})$.

Unha forma modular f en Γ tal que $f|_k\alpha$ se esvaece no infinito para toda $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ dise unha *forma cuspidal*.
Adóitase dicir que f é unha forma modular (cuspidal) de peso k e nivel Γ. O espazo de formas modulares de peso k en Γ denótase $\mathrm{M}_k(\Gamma)$ e este contén o espazo de formas cuspidais de peso k en Γ, o cal escribimos como $\mathrm{S}_k(\Gamma)$.

Nótese que no caso $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ a definición anterior coincide coa proporcionada para as formas modulares no capítulo primeiro. Por outra banda, dada a definición do conxunto $\mathrm{Cusps}(\Gamma)$, basta con que a función f verifique a condición 3 da definición para un número finito de matrices $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, pois só precisamos que sexa holomorfa nun representante de cada órbita.

Observación 2.11. Os espazos $\mathrm{M}_k(\Gamma)$ e $\mathrm{S}_k(\Gamma)$ para un certo grupo de congruencia Γ son $\mathbb{C}$-espazos vectoriais. Ademais, a multiplicación de funcións dota ó espazo $\mathrm{M}(\Gamma) = \bigoplus_{k\in\mathbb{Z}} \mathrm{M}_k(\Gamma)$ dunha estrutura de anel graduado. Finalmente, cabe mencionar que existen fórmulas para o cálculo das dimensións de $\mathrm{M}_k(\Gamma)$ e $\mathrm{S}_k(\Gamma)$ semellantes ás estudadas na sección 1.6, as cales se poden consultar en [5, Cap. 3].

2.3. Operadores de Hecke para subgrupos de congruencia

Nesta sección definiremos os operadores de Hecke T_p (con p un número primo) no contexto dos subgrupos de congruencia, para o cal será necesario considerar uns conxuntos definidos como un "dobre produto" e unha acción dos mesmos nas formas modulares.

Sexan Γ_1 e Γ_2 dous subgrupos de congruencia e sexa $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$. Consideremos o seguinte conxunto, definido como un produto por ambos lados da matriz α:

$$\Gamma_1\alpha\Gamma_2 = \{\gamma_1\alpha\gamma_2 \mid \gamma_1 \in \Gamma_1, \gamma_2 \in \Gamma_2\}\,.$$

Obsérvese que a multiplicación de matrices da lugar a unha acción pola esquerda de Γ_1 en $\Gamma_1\alpha\Gamma_2$, así como unha acción pola dereita de Γ_2 no mesmo conxunto.

Lema 2.12.

1. *Se Γ é un subgrupo de congruencia e $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$ entón $\alpha^{-1}\Gamma\alpha \cap \mathrm{SL}_2(\mathbb{Z})$ tamén é un subgrupo de congruencia.*

2. Dados dous subgrupos de congruencia Γ_1 *e* Γ_2*:* $[\Gamma_1 \colon \Gamma_1 \cap \Gamma_2] < \infty$, $[\Gamma_2 \colon \Gamma_1 \cap \Gamma_2] < \infty$.

Demostración.

1. Sexa N un enteiro positivo tal que $\Gamma(N) \subset \Gamma$ e tal que $N\alpha$ e $N\alpha^{-1}$ sexan matrices con entradas enteiras. Definamos tamén $M = N^3$. Un cálculo sinxelo amosa que $\alpha\Gamma(M)\alpha^{-1} \subset \Gamma(N) \subset \Gamma$, logo deducimos que $\Gamma(M) \subset \alpha^{-1}\Gamma\alpha$. Finalmente, posto que $\Gamma(M)$ é un subconxunto de $\mathrm{SL}_2(\mathbb{Z})$:

$$\Gamma(M) \cap \mathrm{SL}_2(\mathbb{Z}) = \Gamma(M) \subset \alpha^{-1}\Gamma\alpha \cap \mathrm{SL}_2(\mathbb{Z}) \subset \mathrm{SL}_2(\mathbb{Z}).$$

2. Nótese que existe un certo M tal que $\Gamma(M) \subset \Gamma_1 \cap \Gamma_2$, logo os índices do enunciado están limitados superiormente por $[\mathrm{SL}_2(\mathbb{Z}) \colon \Gamma(M)]$, o cal se pode ver que é finito.

□

Proposición 2.13. *Sexan* Γ_1 *e* Γ_2 *subgrupos de congruencia e sexa* $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$. *Definimos o subgrupo de congruencia*

$$\Gamma_3 = \left(\alpha^{-1}\Gamma_1\alpha\right) \cap \Gamma_2.$$

A aplicación $\gamma_2 \mapsto \Gamma_1\alpha\gamma_2$ *induce unha bixección entre espazos de órbitas:*

$$\Gamma_3\backslash\Gamma_2 \cong \Gamma_1\backslash\Gamma_1\alpha\Gamma_2.$$

Demostración. Sexa a aplicación

$$\begin{array}{ccc} \Gamma_2 & \longrightarrow & \Gamma_1\backslash(\Gamma_1\alpha\Gamma_2) \\ \gamma_2 & \longmapsto & \Gamma_1\alpha\gamma_2, \end{array}$$

a cal é claramente sobrexectiva. Dados dous elementos distintos γ_2 e γ_2', as imaxes $\Gamma_1\alpha\gamma_2$ e $\Gamma_1\alpha\gamma_2'$ coinciden se, e só se, $\gamma_2'\gamma_2^{-1} \in \alpha^{-1}\Gamma_1\alpha$, o cal acontece soamente se γ_2 e γ_2' pertencen á mesma órbita de $\left(\alpha^{-1}\Gamma_1\alpha\right) \cap \Gamma_2 = \Gamma_3$. □

Como consecuencia inmediata tense o seguinte corolario:

Corolario 2.14. *Nas mesmas hipóteses que na proposición anterior, sexa* J *un conxunto finito de índices tal que*

$$\Gamma_2 = \bigcup_{j \in J} \Gamma_3\gamma_j$$

é unha descomposición en órbitas de $\Gamma_3\backslash\Gamma_2$. *Tense que*

$$\Gamma_1\alpha\Gamma_2 = \bigcup_{j \in J} \Gamma_1\alpha\gamma_j$$

é unha descomposición en órbitas. En particular, o número de órbitas de $\Gamma_1\alpha\Gamma_2$ *mediante a acción pola esquerda de* Γ_1 *é finito.*

Sexa $f \in \mathrm{M}_k(\Gamma_1)$ unha forma modular de peso k e nivel un certo subgrupo de congruencia Γ_1. Sexan ademais $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$ e Γ_2 outro subgrupo de congruencia. Grazas ao resultado anterior podemos definir

$$f|_k(\Gamma_1\alpha\Gamma_2) = \sum_{j=1}^{m} f|_k\beta_j,$$

onde $\Gamma_1\alpha\Gamma_2 = \bigcup_{j=1}^{n} \Gamma_1\beta_j$ é unha descomposición en órbitas e m é o número (finito polo corolario previo) das mesmas. Esta asignación está ben definida independentemente da escolla dos β_j, pois f é feblemente modular de peso k en Γ_1.

O noso próximo obxectivo é comprobar que, en efecto, os conxuntos $\Gamma_1\alpha\Gamma_2$ definen unha aplicación de $\mathrm{M}_k(\Gamma_1)$ en $\mathrm{M}_k(\Gamma_2)$ (isto é, unha aplicación que muda o nivel dunha forma modular de peso k) que preserva as formas cuspidais. Para isto precisaremos un lema previo:

Lema 2.15. *Supoñamos que, para toda $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ e para unha certa función f, a aplicación $f|_k\gamma$ admite unha expansión da forma*

$$\sum_{n\geq n_0} a_n q_N^n,$$

con n_0 e a_n dependentes de γ. Sexa agora $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$. Resulta que, para toda $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, a función $f|_k(\alpha\gamma)$ admite unha expansión

$$\sum_{n\geq an_0} b_n q_{Nd}^n,$$

onde a e d son enteiros positivos que dependen unicamente de α.

Demostración. Para comezar obsérvese que, para $a > 0$,

$$f|_k \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = a^{2(k-1)}a^{-k}f = a^{k-2}f.$$

Podemos entón asumir, sen perda de xeneralidade, que α é unha matriz con entradas enteiras. Sexa agora $\gamma_0 \in \mathrm{SL}_2(\mathbb{Z})$ tal que $\gamma_0^{-1}\alpha = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$, con $a, d \in \mathbb{Z}$ positivos. Así:

$$\begin{aligned} f|_k\alpha = (f|_k\gamma_0)|_k \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} &= \left(\sum_{n\geq n_0} a_n e^{\frac{2\pi inz}{N}}\right)|_k \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \\ &= (ad)^{k-1}d^{-k}\sum_{n\geq n_0} a_n e^{\frac{2\pi in(az+b)}{Nd}} = (ad)^{k-1}d^{-k}q_{Nd}^{an_0} + \ldots \end{aligned}$$

□

Proposición 2.16. *Sexan Γ_1 e Γ_2 subgrupos de congruencia e sexa $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$. Tense unha aplicación entre espazos de formas modulares de peso $k \in \mathbb{Z}$:*

$$\begin{array}{ccc} \mathrm{M}_k(\Gamma_1) & \longrightarrow & \mathrm{M}_k(\Gamma_2) \\ f & \longmapsto & f|_k\Gamma_1\alpha\Gamma_2. \end{array}$$

Demostración. Resulta evidente que se f é unha función holomorfa en $\mathbb{H}$ entón $f|_k\beta_j$ tamén o é para calquera $\beta_j \in \mathrm{GL}_2^+(\mathbb{Q})$. Sexa agora $\Gamma_3 = \left(\alpha^{-1}\Gamma_1\alpha\right) \cap \Gamma_2$ e consideremos unha descomposición en órbitas $\Gamma_2 = \bigcup_{j\in J} \Gamma_3\gamma_j$, con J un certo conxunto finito de índices. Polo corolario 2.14 podemos tomar $\beta_j = \alpha\gamma_j$ como representantes dunha descomposición en órbitas de $\Gamma_1\alpha\Gamma_2$. Tomemos $\gamma \in \Gamma_2$ e observemos que $\{\gamma_j\gamma\}_{j\in J}$ é un conxunto de representantes do espazo de órbitas $\Gamma_3\backslash\Gamma_2$, logo $\{\alpha\gamma_j\gamma\}_{j\in J}$ tamén é un conxunto de representantes de $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$. Dedúcese pois que f é feblemente modular de peso k en Γ_2. Só resta verificar que $f|_k\Gamma_1\alpha\Gamma_2$ é holomorfa en cada cúspide, pero precisamente isto nolo garante o lema 2.15, co cal a aplicación está ben definida. □

Exemplo 2.17. Sexan Γ, Γ_1 e Γ_2 subgrupos de congruencia, $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$ e $k \in \mathbb{Z}$.

- Supoñamos que $\Gamma_2 \subset \Gamma_1$ e $\alpha = I$. Entón $\Gamma_1\alpha\Gamma_2 = \Gamma_1$ e $\Gamma_1 = \Gamma_1 I$ é unha descomposición en órbitas, logo
$$f|_k\Gamma_1\alpha\Gamma_2 = f|_k I = f,$$
sendo $f \in \mathrm{M}_k(\Gamma_1)$. Dedúcese entón que $\mathrm{M}_k(\Gamma_1) \subset \mathrm{M}_k(\Gamma_2)$.

- Consideremos o subgrupo de congruencia dado pola conxugación $\Gamma' = \alpha^{-1}\Gamma\alpha$. Entón
$$\Gamma\alpha\Gamma' = \Gamma\alpha\alpha^{-1}\Gamma\alpha = \Gamma\alpha$$
é unha descomposición en órbitas, logo o produto das matrices de Γ por α induce unha aplicación $\mathrm{M}_k(\Gamma) \to \mathrm{M}_k\left(\alpha^{-1}\Gamma\alpha\right)$. Posto que esta aplicación ten como inversa aquela dada polo produto por α^{-1}, concluímos que os espazos de formas modulares $\mathrm{M}_k(\Gamma)$ e $\mathrm{M}_k\left(\alpha^{-1}\Gamma\alpha\right)$ son naturalmente isomorfos.

- Supoñamos que $\Gamma_1 \subset \Gamma_2$ e $\alpha = I$. Sexa $\Gamma_1\alpha\Gamma_2 = \bigcup_{j=1}^m \Gamma_1\beta_j$ unha descomposición en órbitas, $m \in \mathbb{Z}$. A aplicación
$$\begin{array}{ccc} \mathrm{M}_k(\Gamma_1) & \longrightarrow & \mathrm{M}_k(\Gamma_2) \\ f & \longmapsto & \displaystyle\sum_{j=1}^m f|_k\beta_j \end{array}$$
pódese ver como unha especie de "operador traza". De feito, este operador leva cada $f \in \mathrm{M}_k(\Gamma_2)$ en $[\Gamma_2 \colon \Gamma_1]f$, logo é sobrexectivo.

Xa estamos en condicións de definir os primeiros operadores no contexto dos subgrupos de congruencia.

Definición 2.18. Sexan p un número primo, $k \in \mathbb{Z}$ e Γ un subgrupo de congruencia. Defínese o p-ésimo *operador de Hecke* en Γ como a aplicación $T_p\colon \mathrm{M}_k(\Gamma) \to \mathrm{M}_k(\Gamma)$ dada por:

$$T_p f = f|_k \Gamma \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma.$$

Nótese que, grazas á proposición 2.16, os operadores de Hecke están ben definidos como funcións do espazo $\mathrm{M}_k(\Gamma)$ en si mesmo.

De agora en adiante centraremos a nosa atención no subgrupo de congruencia $\Gamma_1(N)$ para $N \geq 1$, pois veremos nas seccións próximas que este posúe unha especial relevancia.

O noso último obxectivo nesta sección será describir dun xeito máis preciso os operadores T_p en $\Gamma_1(N)$. Será necesario entón comprender o conxunto $\Gamma_1(N)\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)\Gamma_1(N)$. É inmediato que, dada $\gamma \in \Gamma_1(N)\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)\Gamma_1(N)$, $\det\gamma = p$ e $\gamma \equiv \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$ módulo N, onde a é un enteiro arbitrario. De feito, estas dúas propiedades caracterizan o conxunto (véxase unha posible proba en [13, pp. 45 e 46]):

Lema 2.19. *Dados enteiros $N \geq 1$ e p primo, tense que*

$$\Gamma_1(N) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_1(N) = \left\{ \gamma \in M_2(\mathbb{Z}) \mid \det\gamma = p \;\; e \;\; \gamma \equiv \begin{pmatrix} 1 & a \\ 0 & p \end{pmatrix} \,(\mathrm{mód}\, N),\, a \in \mathbb{Z} \right\},$$

sendo $M_2(\mathbb{Z})$ o conxunto de matrices cadradas de orde 2 con entradas enteiras.

Proposición 2.20. *Sexa $f \in \mathrm{M}_k(\Gamma_1(N))$, con $N \geq 1$ e $k \in \mathbb{Z}$. Dado un primo p, a imaxe de f polo operador T_p vén dada como segue:*

$$T_p f = \begin{cases} \displaystyle\sum_{j=0}^{p-1} f|_k \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix} & \text{se } p \mid N, \\ \displaystyle\sum_{j=0}^{p-1} f|_k \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix} + f|_k \begin{pmatrix} mp & n \\ Np & p \end{pmatrix} & \text{se } p \nmid N, \end{cases}$$

onde a matriz $\left(\begin{smallmatrix} mp & n \\ Np & p \end{smallmatrix}\right)$ é tal que $\gamma_\infty = \left(\begin{smallmatrix} mp & n \\ N & 1 \end{smallmatrix}\right) \in \Gamma_1(N)$.

Demostración. Necesitamos achar unha descomposición en órbitas explícita para o espazo $\Gamma_3\backslash\Gamma_1(N)$, onde

$$\Gamma_3 = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}^{-1} \Gamma_1(N) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \cap \Gamma_1(N).$$

Sexa $\Gamma^0(p)$ o grupo de matrices triangulares inferiores módulo p. Resulta inmediato comprobar que $\Gamma_3 = \Gamma_1(N) \cap \Gamma^0(p)$. Consideremos as matrices $\gamma_j = \left(\begin{smallmatrix} 1 & j \\ 0 & 1 \end{smallmatrix}\right)$, con $0 \leq j \leq p-1$, e notemos que todas elas son diferentes módulo $\Gamma_1(N) \cap \Gamma^0(p)$. Ademais, dada $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & -j \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & -aj+b \\ c & -cj+d \end{pmatrix}.$$

Así, se $p \nmid a$ entón podemos tomar un j tal que a matriz do lado dereito da igualdade pertenza a $\Gamma^0(p)$, o cal significa que se $p \mid N$ entón $p \nmid a$ pola condición do determinante 1. Neste caso, $\{\gamma_j\}_{j=0}^{p-1}$ é un conxunto de representantes do espazo de órbitas.
Se, pola contra, $p \nmid N$ entón precisamos considerar as matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ con $p \mid a$. Escollendo $\gamma_\infty = \left(\begin{smallmatrix} mp & n \\ N & 1 \end{smallmatrix}\right) \in \Gamma_1(N)$ tense

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \gamma_\infty^{-1} = \begin{pmatrix} * & -na+bmp \\ 0 & * \end{pmatrix},$$

onde os $*$ non son relevantes de xeito explícito. Posto que p divide a $-na+bmp$, a matriz $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ pertence a $\Gamma^0(p)\gamma_\infty$. Así, $\{\gamma_j\} \cup \{\gamma_\infty\}$ conforma un conxunto de representantes do espazo de órbitas $\Gamma_3 \backslash \Gamma_1(N)$. Finalmente, para descompoñer o conxunto $\Gamma_1(N)\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)\Gamma_1(N)$ en órbitas basta con aplicar o corolario 2.14, segundo o cal debemos multiplicar a matriz $\alpha = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$ pola esquerda con cada γ_j e γ_∞, obtendo así as matrices que aparecen no enunciado da proposición. □

Observación 2.21. Empregando estas expresións é inmediato comprobar que a definición dada neste capítulo dos operadores de Hecke coincide coa dada no capítulo (definición 1.23) para o caso dun primo p. Ademais, os operadores T_p son claramente endomorfismos de $\mathrm{M}_k(\Gamma_1(N))$ para cada peso $k \in \mathbb{Z}$ e cada $N \geq 1$, ou endomorfismos de $\mathrm{S}_k(\Gamma_1(N))$ se consideramos a restrición do operador ao devandito espazo.

2.4. Operadores diamante

Esta sección introduce un novo conxunto (finito) de operadores no espazo de formas modulares de $\Gamma_1(N)$. Tamén se definiran certos subespazos de formas modulares que empregaremos en futuras seccións e capítulos.

Precisaremos unha noción preliminar:

Definición 2.22. Un *carácter de Dirichlet* módulo $N \geq 1$ é un homomorfismo de grupos

$$\chi \colon (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times.$$

Nótese que todo carácter de Dirichlet pode estenderse a unha aplicación $\chi\colon \mathbb{Z} \to \mathbb{C}$ mediante

$$\chi(d) = \begin{cases} \chi(d \bmod N) & \text{se } (d,N)=1, \\ 0 & \text{se } (d,N)\neq 1. \end{cases}$$

Evidentemente, como o carácter de Dirichlet de partida é un homomorfismo de grupos entón a aplicación resultante da extensión anterior é multiplicativa, é dicir:

$$\chi(d_1d_2) = \chi(d_1)\chi(d_2) \text{ para calquera } d_1, d_2 \in \mathbb{Z}.$$

Definición 2.23. Sexa $N \geq 1$ e sexa $d \in \mathbb{Z}$ coprimo con N. Para cada $k \in \mathbb{Z}$, defínese o d-ésimo *operador diamante* como a aplicación $\langle d\rangle\colon \mathrm{M}_k(\Gamma_1(N)) \to \mathrm{M}_k(\Gamma_1(N))$ dada por

$$\langle d\rangle f = f|_k \begin{pmatrix} a & b \\ c & d' \end{pmatrix},$$

onde os enteiros a, b, c e d' son tales que $\left(\begin{smallmatrix} a & b \\ c & d' \end{smallmatrix}\right) \in \Gamma_0(N)$ e $d' \equiv d \,(\mathrm{mód}\, N)$.

Grazas ao isomorfismo $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^\times$ presentado na proposición 2.4, os operadores diamante están ben definidos. Ademais, estes operadores son obviamente lineares, invertibles e a súas restricións a $\mathrm{S}_k(\Gamma_1(N))$ son endomorfismos do mesmo. Polo tanto, ten sentido estudar os seus espazos propios.

Definición 2.24. Sexan $N \geq 1$ e k enteiros e sexa χ un carácter de Dirichlet. Defínese o *espazo de formas modulares con carácter* χ como

$$\mathrm{M}_k(\Gamma_0(N), \chi) = \left\{ f \in \mathrm{M}_k(\Gamma_1(N)) \mid \langle d\rangle f = \chi(d) f,\, d \in (\mathbb{Z}/N\mathbb{Z})^\times \right\}.$$

Analogamente, definimos o *espazo de formas cuspidais con carácter* χ como

$$\mathrm{S}_k(\Gamma_0(N), \chi) = \left\{ f \in \mathrm{S}_k(\Gamma_1(N)) \mid \langle d\rangle f = \chi(d) f,\, d \in (\mathbb{Z}/N\mathbb{Z})^\times \right\}.$$

Para finalizar a sección, vexamos unha propiedade interesante dos espazos anteriores, cuxa proba se basea na teoría de representacións (véxase [13, p. 47]):

Teorema 2.25. *Sexan $N \geq 1$ e k enteiros. Tense unha descomposición de $\mathbb{C}$-espazos vectoriais*

$$\mathrm{M}_k(\Gamma_1(N)) = \bigoplus_{\chi \bmod N} \mathrm{M}_k(\Gamma_0(N), \chi),$$

onde a suma se leva a cabo sobre $\phi(N) = |(\mathbb{Z}/N\mathbb{Z})^\times|$ caracteres de Dirichlet módulo N.

2.5. Descomposición dos operadores de Hecke

Esta sección pretende expresar os operadores T_p con p primo dun novo xeito, o cal consiste no emprego duns operadores máis sinxelos. Esta reescritura dos operadores de Hecke será empregada frecuentemente na sección vindeira.

Dada $f = \sum_{n=0}^{\infty} a_n q^n$, imos considerar dous novos operadores para cada número primo p. O primeiro é U_p:

$$U_p f = \sum_{n=0}^{\infty} a_{np} q^n = \sum_{n=0}^{\infty} a_n q^{n/p},$$

onde a segunda igualdade é un abuso da notación no que estamos definindo implicitamente $q^{n/p} = 0$ se $p \nmid n$. Este primeiro operador ten, como veremos proximamente, un comportamento moi semellante ao operador T_p, e será de moita utilidade máis adiante (en particular, no desenvolvemento da teoría de Hida). O segundo operador é $V_p f$:

$$V_p f = \sum_{n=0}^{\infty} a_n q^{np} = \sum_{n=0}^{\infty} a_{n/p} q^n,$$

cun abuso de notación análogo ao anterior. Nótese que, en termos da variable z complexa, $V_p f(z) = f(pz)$.

Lema 2.26. *Sexan $f = \sum_{n=0}^{\infty} a_n q^n$, con p un número primo e $k \in \mathbb{Z}$. Tense que:*

1. $U_p f = \frac{1}{p} \sum_{j=0}^{p-1} f\left(\frac{z+j}{p}\right) = \sum_{j=0}^{p-1} f|_k \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}$.
2. $V_p f = p^{1-k} f|_k \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$.

Demostración. Vexamos a primeira afirmación (a segunda é evidente). Definimos unha raíz p-ésima da unidade $\xi_p = e^{\frac{2\pi i}{p}}$ e observamos que

$$\sum_{j=0}^{p-1} \xi_p^{nj} = \begin{cases} p & \text{se } p \mid n, \\ 0 & \text{se } p \nmid n. \end{cases}$$

Por outra banda, facendo directamente os cálculos:

$$\sum_{j=0}^{p-1} f|_k \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix} = p^{k-1} p^{-k} \sum_{j=0}^{p-1} f\left(\frac{z+j}{p}\right) = \frac{1}{p} \sum_{j=0}^{p-1} f\left(\frac{z+j}{p}\right).$$

Finalmente:

$$\frac{1}{p} \sum_{j=0}^{p-1} \sum_{n=0}^{\infty} a_n e^{2\pi i n \frac{z+j}{p}} = \sum_{n=0}^{\infty} a_n e^{\frac{2\pi i n z}{p}} \frac{1}{p} \sum_{j=0}^{p-1} \xi_p^{nj} = U_p f.$$

□

Empregando todo o visto ata agora, podemos reescribir os operadores de Hecke T_p con p primo en termos dos operadores U_p e V_p e dos operadores diamante.

Teorema 2.27. *Dados un primo p, enteiros k e $N \geq 1$, consideremos unha forma modular $f \in \mathrm{M}_k(\Gamma_1(N))$:*

$$T_p f = \begin{cases} U_p f & \text{se } p \mid N, \\ U_p f + p^{k-1} V_p \langle p \rangle f & \text{se } p \nmid N. \end{cases}$$

Demostración. Bastará xuntar o enunciado do lema 2.26 e o da proposición 2.20. En efecto,

$$U_p f = \sum_{j=0}^{p-1} f|_k \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}.$$

Ademais, podemos escoller enteiros $m, n \in \mathbb{Z}$ tales que $mp - nN = 1$ pola identidade de Bézout, co cal $\left(\begin{smallmatrix} m & n \\ N & p \end{smallmatrix}\right) \in \Gamma_0(N)$. Así:

$$p^{k-1} V_p \langle p \rangle f = p^{k-1} V_p f|_k \begin{pmatrix} m & n \\ N & p \end{pmatrix} = f|_k \left[\begin{pmatrix} m & n \\ N & p \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \right] = f|_k \begin{pmatrix} mp & n \\ Np & p \end{pmatrix}.$$

□

Como consecuencia inmediata temos o seguinte corolario:

Corolario 2.28. *Sexan $N \geq 1$ e k enteiros, χ un carácter de Dirichlet e $f \in \mathrm{M}_k(\Gamma_0(N), \chi)$. Entón, para calquera primo p,*

$$T_p f = U_p f + \chi(p) p^{k-1} V_p f.$$

En particular, se $f \in \mathrm{M}_k(\Gamma_0(N))$ entón

$$T_p f = \begin{cases} U_p f & \text{se } p \mid N, \\ U_p f + p^{k-1} V_p f & \text{se } p \nmid N. \end{cases}$$

Para finalizar a sección, obsérvese que a estreira relación entre U_p e T_p para cada p primo nos induce a pensar en U_p como un operador de formas modulares en si mesmo, o cal aumenta (potencialmente) o nivel de ditas formas.

Corolario 2.29. *Sexan p un número primo, $N \geq 1$ e k enteiros. Téñense dous posibles casos para a boa definición do operador U_p:*

1. *Se $p \mid N$ entón $U_p \colon \mathrm{M}_k(\Gamma_1(N)) \to \mathrm{M}_k(\Gamma_1(N))$.*
2. *Se $p \nmid N$ entón $U_p \colon \mathrm{M}_k(\Gamma_1(N)) \to \mathrm{M}_k(\Gamma_1(Np))$.*

2.6. As álxebras de Hecke

Esta sección ten tres obxectivos: definir e estudar as álxebras de Hecke, estudar o comportamento dos operadores de Hecke ao facelos actuar en expansións en serie e introducir as formas propias de Hecke.

Definición 2.30. Sexan $N \geq 1$ e k enteiros. Defínese a *álxebra de Hecke* de $\mathrm{M}_k(\Gamma_1(N))$ como a $\mathbb{C}$-subálxebra de $\mathrm{End}_{\mathbb{C}}(\mathrm{M}_k(\Gamma_1(N)))$:

$$\mathcal{H}(\mathrm{M}_k(\Gamma_1(N))) = \left\langle T_p, \langle d\rangle \mid p \in \mathbb{Z} \text{ primo}, d \in (\mathbb{Z}/N\mathbb{Z})^\times \right\rangle.$$

Así mesmo, defínese a álxebra de Hecke de $\mathrm{S}_k(\Gamma_1(N))$, $\mathcal{H}(\mathrm{S}_k(\Gamma_1(N)))$, como a $\mathbb{C}$-subálxebra de $\mathrm{End}_{\mathbb{C}}(\mathrm{S}_k(\Gamma_1(N)))$ obtida restrinxindo os operadores da álxebra anterior ao espazo de formas cuspidais.
Para axilizar a escritura, é habitual empregar a seguinte notación:

$$\mathcal{H}_k(\Gamma_1(N)) = \mathcal{H}(\mathrm{M}_k(\Gamma_1(N))) \quad \text{e} \quad \mathfrak{h}_k(\Gamma_1(N)) = \mathcal{H}(\mathrm{S}_k(\Gamma_1(N))).$$

Teorema 2.31. *Para cada par de enteiros $N \geq 1$ e k, as álxebras de Hecke $\mathcal{H}_k(\Gamma_1(N))$ e $\mathfrak{h}_k(\Gamma_1(N))$ son conmutativas.*

Demostración. Imos probar o resultado soamente para $\mathcal{H}_k(\Gamma_1(N))$, pois a conmutatividade de $\mathfrak{h}_k(\Gamma_1(N))$ dedúcese inmediatamente unha vez demostrada a de $\mathcal{H}_k(\Gamma_1(N))$. Temos entón que comprobar que, para cada par de números primos p e r e para cada par de elementos $e, d \in (\mathbb{Z}/N\mathbb{Z})^\times$:

1. $\langle d\rangle T_p = T_p\langle d\rangle$.
2. $\langle d\rangle\langle e\rangle = \langle e\rangle\langle d\rangle$.
3. $T_pT_r = T_rT_p$.

Comecemos coa primeira afirmación. Sexa $f \in \mathrm{M}_k(\Gamma_1(N))$ e sexa unha matriz $\gamma \equiv \left(\begin{smallmatrix} * & * \\ 0 & d \end{smallmatrix}\right)$ (mód N), onde as entradas $*$ non son relevantes para o cálculo. Escribamos $\Gamma = \Gamma_1(N)$ durante o resto da proba para axilizar a notación. Posto que $\gamma \in \Gamma_0(N)$ e Γ é un subgrupo normal de $\Gamma_0(N)$ (é o núcleo do homomorfismo de grupos dado na demostración da proposición 2.4), tense que $\Gamma\gamma\Gamma = \Gamma\gamma$, polo que $\langle d\rangle f = f|_k\gamma$. Temos que demostrar que $\langle d\rangle^{-1}T_p\langle d\rangle = T_p$. Sexa un certo conxunto finito de índices J para o cal $\Gamma\alpha\Gamma = \bigcup_{j\in J}\Gamma\beta_j$ é a descomposición correspondente ao operador T_p, $\alpha = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$. Basta entón con demostrar que

$$\Gamma\alpha\Gamma = \bigcup_{j\in J}\Gamma\left(\gamma\beta_j\gamma^{-1}\right).$$

Nótese que

$$\bigcup_{j\in J}\Gamma\left(\gamma\beta_j\gamma^{-1}\right)=\gamma\left(\bigcup_{j\in J}\Gamma\beta_j\right)\gamma^{-1}=\gamma(\Gamma\alpha\Gamma)\gamma^{-1}=\Gamma\left(\gamma\alpha\gamma^{-1}\right)\Gamma,$$

co cal podemos concluír, pois cun simple cálculo compróbase que $\Gamma\alpha\Gamma=\Gamma\left(\gamma\alpha\gamma^{-1}\right)\Gamma$. Vexamos agora as afirmacións 2 e 3. Nótese que a propiedade 1 implica que o operador T_p preserva os espazos $\mathrm{M}_k(\Gamma_0(N),\chi)$ para cada carácter de Dirichlet χ, co cal basta comprobar 2 e 3 para formas modulares f con carácter χ (grazas ao teorema 2.25). Esta consideración fai que a afirmación 2 sexa obvia, pois

$$\langle d\rangle\langle e\rangle f=\chi(d)\chi(e)f=\chi(e)\chi(d)f=\langle e\rangle\langle d\rangle f.$$

Para comprobar 3 consideremos a expansión $f=\sum_{n=0}^{\infty}a_nq^n$. Polo corolario 2.28,

$$a_n(T_pf)=a_{pn}(f)+\chi(p)p^{k-1}a_{n/p}(f).$$

Así:

$$\begin{aligned}a_n(T_pT_rf)&=a_{pn}(T_rf)+\chi(p)p^{k-1}a_{n/p}(T_rf)\\&=a_{prn}(f)+\chi(r)r^{k-1}a_{pn/r}(f)+\chi(p)p^{k-1}\left(a_{rn/p}(f)+\chi(r)r^{k-1}a_{n/pr}(f)\right).\end{aligned}$$

Finalmente, obsérvese que a fórmula anterior non varía se intercambiamos p e r entre si, co cal se conclúe a última afirmación do teorema. □

Imos agora xeneralizar os operadores de Hecke e diamante aos casos T_n e $\langle n\rangle$, con $n\geq 1$ un enteiro calquera, e resultará que, coas definicións para os mesmos, estes serán operadores da álxebra de Hecke.

En primeiro lugar, estendemos os operadores diamante impoñendo que, para cada primo p, $\langle p\rangle=0$ se $p\mid N$. Nótese que os operadores diamante $\langle n\rangle$ así definidos conmutan entre si claramente.

Definición 2.32. Sexan enteiros $n,m,N\geq 1$ e k. Definimos os operadores de Hecke T_n mediante as seguintes condicións:

- $T_1=\mathrm{id}_{\mathrm{M}_k(\Gamma_1(N))}$.
- $T_{nm}=T_nT_m$ se $(n,m)=1$.
- Para cada primo p e cada $r\geq 2$: $T_{p^r}=T_pT_{p^{r-1}}-p^{k-1}\langle p\rangle T_{p^{r-2}}$.

Coa definición, anterior é evidente que todos os operadores de Hecke T_n teñen unha expresión explícita como polinomios en operadores T_p, logo conmutan entre si.

Vexamos agora como se comportan os operadores de Hecke ao actuar sobre expansións en serie:

Teorema 2.33. *Sexan enteiros k e $m, N \geq 1$ e sexa $f = \sum_{n=0}^{\infty} a_n(f)q^n \in \mathrm{M}_k(\Gamma_1(N))$. Entón $T_m f = \sum_{n=0}^{\infty} a_n(T_m f)q^n$, onde*

$$a_n(T_m f) = \sum_{d|(m,n)} d^{k-1} a_{\frac{mn}{d^2}}(\langle d \rangle f).$$

En particular, se existe un carácter de Dirichlet χ tal que $f \in \mathrm{M}_k(\Gamma_0(N), \chi)$ entón

$$a_n(T_m f) = \sum_{d|(m,n)} \chi(d) d^{k-1} a_{\frac{mn}{d^2}}(f).$$

Demostración. Véxase [5, pp. 179-180]. □

Estudemos agora as formas propias da álxebra de Hecke.

Definición 2.34. Unha *forma propia de Hecke* (ou simplemente unha *forma propia*) é unha forma modular f non nula de peso k e nivel $\Gamma_1(N)$ que é autovector de todos os operadores da álxebra de Hecke $\mathcal{H}_k(\Gamma_1(N))$. Unha *forma propia de Hecke normalizada* (ou simplemente unha *forma propia normalizada*) é unha forma propia de Hecke $f \in \mathcal{H}_k(\Gamma_1(N))$ tal que $a_1(f) = 1$.

Sexa $f \in \mathrm{M}_k(\Gamma_1(N))$ unha forma propia de Hecke para certos enteiros k e $N \geq 1$ e definamos λ_n para cada $n \geq 1$ como $T_n f = \lambda_n f$. Tense que

$$a_n(f) = a_1(T_n f) = \lambda_n a_1(f).$$

Así, se $a_1(f) = 0$ entón $a_n(f) = 0$ para todo n, logo $f = 0$. Polo tanto, toda forma propia de Hecke non constante verifica $a_1(f) \neq 0$, polo que se pode transformar nunha forma propia normalizada. En particular, tense o seguinte resultado:

Proposición 2.35. *Sexa f unha forma propia de Hecke normalizada de peso k e nivel $\Gamma_1(N)$. Os autovalores dos operadores de Hecke aplicados a f son os coeficientes da q-expansión de f no infinito:*

$$T_n f = a_n(f) f, \quad n \geq 1.$$

Demostración. Sexa λ_n o autovalor do operador de Hecke T_n en f. Sabemos que $a_n(f) = a_1(T_n f) = \lambda_n a_1(f)$ e, posto que f é normalizada, $a_1(f) = 1$, logo $a_n(f) = \lambda_n$. □

Aínda máis: os coeficientes de Fourier dunha forma modular indican se esta unha forma propia normalizada.

Proposición 2.36. *Sexa $f \in \mathrm{M}_k(\Gamma_0(N), \chi)$ para certos enteiros k e $N \geq 1$ e un certo carácter de Dirichlet χ. Se $f = \sum_{n=0}^{\infty} a_n(f) q^n$ entón f é unha forma propia de Hecke normalizada se, e só se, para enteiros arbitrarios m, n e un primo p:*

1. $a_1(f) = 1$.
2. $a_{mn}(f) = a_m(f) a_n(f)$ *se* $(m, n) = 1$.
3. $a_{p^r}(f) = a_p(f) a_{p^{r-1}}(f) - \chi(p) p^{k-1} a_{p^{r-2}}(f)$ *para todo* $r \geq 2$.

Demostración. Se f é unha forma propia normalizada entón as tres condicións se teñen pola definición dos operadores de Hecke T_n e polos resultados anteriores. Vexamos o recíproco: sexa $f \in \mathrm{M}_k(\Gamma_0(N), \chi)$ verificando as tres condicións do enunciado. Xa sabemos que f é normalizada grazas á condición 1. Vexamos pois que, para todo primo p e todo enteiro $n \geq 1$,

$$a_n(T_p f) = a_p(f) a_n(f).$$

Se $p \mid n$ entón séguese polo teorema 2.33 que $a_n(T_p f) = a_{pn}(f)$, que, pola condición 2, é igual a $a_p(f) a_n(f)$, o cal conclúe coa proba neste caso. Se $p \nmid n$, escribamos $n = p^r n'$, con $r \geq 1$ e n' un enteiro tal que $p \nmid n'$. Temos entón, novamente empregando 2.33,

$$a_n(T_p f) = a_{p^{r+1} n'}(f) + \chi(p) p^{k-1} a_{p^{r-1} n'}(f).$$

Empregando agora as condicións 2 e 3 de xeito reiterado chégase novamente a $a_p(f) a_m(f)$, xusto como queríamos. □

Para finalizar, introducimos o produto interior de Petersson:

Definición 2.37. Sexa Γ un subgrupo de congruencia, k un enteiro. Defínese o *produto interior de Petersson* de dúas formas cuspidais f e g de peso k e nivel Γ como

$$\langle f, g \rangle_\Gamma = \frac{1}{\mathrm{covol}(\Gamma)} \int_{\Gamma \backslash \mathbb{H}} f(z) \overline{g(z)} \Im(z)^k d\mu(z),$$

onde a integral se realiza sobre un dominio fundamental de Γ,

$$d\mu(z) = \frac{-1}{2i} \frac{dz \wedge d\bar{z}}{\Im(z)^2} \quad \text{e} \quad \mathrm{covol}(\Gamma) = \int_{\Gamma \backslash \mathbb{H}} d\mu(t).$$

Pódese consultar [13, §4.4] para estudar diversas propiedades e definicións relativas a este produto. En particular, destacamos que o $\mathbb{C}$-espazo vectorial das formas cuspidais de peso k e nivel Γ é un espazo hermítico co produto interior de Petersson, o cal permite chegar a demostrar o seguinte resultado:

Teorema 2.38. *O espazo* $\mathrm{S}_k(\Gamma_1(N))$ *para cada par de enteiros* k *e* $N \geq 1$ *ten unha base ortogonal formada por formas propias de Hecke dos operadores* T_n *e* $\langle n \rangle$*, con* $(n, N) = 1$*.*

Capítulo 3

Números p-ádicos e cohomoloxía de grupos

Este capítulo, cuxa temática difire en gran medida da dos capítulos anteriores, introduce dúas ferramentas clave para o desenvolvemento da teoría de Hida: os números p-ádicos e a cohomoloxía de grupos. Tamén se introducirán nocións cohomolóxicas adicionais relacionadas coas formas modulares na derradeira sección, reconducindo así o documento cara ás temáticas principais.

3.1. Números p-ádicos

Nesta sección construiremos de xeito alxébrico o corpo dos números p-ádicos para cada número primo p, pero tamén se mencionará unha construción alternativa dos mesmos como completación de $\mathbb{Q}$ (no canto da completación usual mediante a norma euclídea, é dicir, $\mathbb{R}$).

Sexa un número primo $p \in \mathbb{Z}$. Para cada $n \geq 1$ escribimos $A_n = \mathbb{Z}/p^n\mathbb{Z}$, o anel de clases de equivalencia dos enteiros módulo p^n. Ademais, definimos un homomorfismo de aneis $\varphi_n \colon A_n \to A_{n-1}$ para cada $n \geq 2$ que asigna a cada elemento de A_n a súa clase de equivalencia módulo p^{n-1}. É evidente que estas aplicacións son sobrexectivas e, ademais, $\ker(\varphi_n) = p^{n-1}A_n$.

Definición 3.1. Para cada número primo p, defínese o *anel de enteiros p-ádicos* $\mathbb{Z}_p$ como o límite proxectivo $\mathbb{Z}_p = \varprojlim (A_n, \varphi_n)$, onde (A_n, φ_n) é o sistema

$$\ldots \xrightarrow{\varphi_{n+1}} A_n \xrightarrow{\varphi_n} A_{n-1} \xrightarrow{\varphi_{n-1}} \ldots \xrightarrow{\varphi_3} A_2 \xrightarrow{\varphi_1} A_1.$$

Así, cada elemento $x \in \mathbb{Z}_p$ é unha sucesión $x = (x_n)_{n\geq 1} = (\ldots, x_n, \ldots, x_1)$ con $x_n \in A_n$ para cada $n \geq 1$ e $\varphi_n(x_n) = x_{n-1}$ se $n \geq 2$.

Definimos tamén unha suma e un produto en $\mathbb{Z}_p$ mediante a suma e o produto de A_n na n-ésima coordenada para cada n. Así, $\mathbb{Z}_p$ é un subanel de $\prod_{n\geq 1} A_n$.

Vexamos algunhas propiedades do anel de enteiros p-ádicos. Para cada $n \geq 1$, sexa $\pi_n \colon \mathbb{Z}_p \to A_n$ a proxección n-ésima, é dicir, a aplicación que leva cada $x \in \mathbb{Z}_p$ na súa n-ésima compoñente, $x_n \in A_n$.

Proposición 3.2. *Para cada primo p e cada enteiro $n \geq 1$, tense a sucesión exacta curta*

$$0 \longrightarrow \mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p \xrightarrow{\pi_n} A_n \longrightarrow 0,$$

onde a aplicación $p^n \colon \mathbb{Z}_p \to \mathbb{Z}_p$ denota a multiplicación por p^n. Polo tanto, podemos identificar $\mathbb{Z}_p/p^n\mathbb{Z}_p$ con $A_n = \mathbb{Z}/p^n\mathbb{Z}$.

Demostración. Vexamos primeiro que a multiplicación por p (e, polo tanto, por p^n) é inxectiva en $\mathbb{Z}_p$. Sexa un enteiro p-ádico $x = (x_n)_{n\geq 1}$ tal que $px = 0$. Tense que $px_{n+1} = 0$ para todo n, logo x_{n+1} é da forma $p^n y_{n+1}$ con $y_{n+1} \in A_{n+1}$. Como $x_n = \varphi_{n+1}(x_{n+1}) = \varphi_{n+1}(p^n y_{n+1})$ entón deducimos que $x_n = 0$, pois x_n é divisible por p^n. Concluímos procedendo indutivamente.
Por outra banda, é evidente que π_n é sobrexectiva e que o seu núcleo contén $p^n\mathbb{Z}_p$, a imaxe do produto por p^n. Para ver o recíproco, sexa $x = (x_m)_{m\geq 1} \in \ker(\pi_n)$. Sabemos que $x_m \equiv 0 \,(\mathrm{mód}\, p^n)$ para todo $m \geq n$, logo existe un elemento $y_{m-n} \in A_{m-n}$ ben definido para cada $m > n$ tal que a súa imaxe mediante o isomorfismo $A_{m-n} \cong p^n\mathbb{Z}/p^m\mathbb{Z} \subset A_m$ satisfai $x_m = p^n y_{m-n}$. Estes elementos y_i definen un enteiro p-ádico $y = (y_i)_{y\geq 1}$ tal que $p^n y = x$, o cal conclúe a demostración. □

Proposición 3.3. *Sexa un primo p.*

1. *Un elemento de $\mathbb{Z}_p$ (respectivamente de A_n para $n \geq 1$) ten inverso se, e só se, non é divisible por p.*

2. *Todo elemento non nulo de $\mathbb{Z}_p$ pode escribirse de xeito único na forma $p^n u$, con $n \geq 0$ e $u \in \mathbb{Z}_p^\times$ (u dise unha unidade p-ádica).*

Demostración.

1. Chega con probar 1 no caso de A_n para un $n \geq 1$ fixado. Sexa pois $x \in A_n$ tal que $x \notin pA_n$. Resulta entón que a súa imaxe en $A_1 = \mathbb{Z}/p\mathbb{Z}$ é non nula, logo é invertible (pois A_1 é un corpo). Así, existen $y, z \in A_n$ tales que $xy = 1 - pz$, logo

$$xy\left(1 + pz + \cdots + p^{n-1}z^{n-1}\right) = 1,$$

polo que x é invertible.

2. Sexa $x \in \mathbb{Z}_p$ non nulo. Sexa n o maior enteiro de xeito que $x_n = \pi_n(x) = 0$. Este verifica que $x = p^n u$, con $p \nmid u$. Pola afirmación 1, $u \in \mathbb{Z}_p^\times$ e a descomposición é claramente única.

□

Definición 3.4. Sexa un primo p e sexa $x \in \mathbb{Z}_p$ tal que $x = p^n u$, con $n \geq 0$ e $u \in \mathbb{Z}_p^\times$. O enteiro n denomínase a *valoración p-ádica* de x e denótase $v_p(x)$.

Observación 3.5. Definindo $v_p(0) = \infty$, pódese comprobar que, para $x, y \in \mathbb{Z}_p$,

$$v_p(xy) = v_p(x) + v_p(y) \quad \text{e} \quad v_p(x+y) \geq \text{ínf}(v_p(x), v_p(y)).$$

Finalmente, imos definir os números p-ádicos e a norma p-ádica.

Definición 3.6. Para cada primo p, defínese o corpo de *números p-ádicos* $\mathbb{Q}_p$ como o corpo de fraccións de $\mathbb{Z}_p$.

Resulta inmediato que $\mathbb{Q}_p = \mathbb{Z}_p\left[p^{-1}\right]$. Ademais, é evidente que todo elemento $x \in \mathbb{Q}_p^\times$ pode ser reescrito de xeito único na forma $p^n u$, con $n \in \mathbb{Z}$ e $u \in \mathbb{Z}_p^\times$ (simplemente calculando o cociente dos enteiros p-ádicos que conforman a fracción x). Novamente, defínese n como a valoración p-ádica de x, e denótase $v_p(x)$. Tense ademais que $v_p(x) \geq 0$ se, e só se, $x \in \mathbb{Z}_p$, e que se $x = a/b \in \mathbb{Q}_p$ entón $v_p(x) = v_p(a) - v_p(b)$.

Definición 3.7. Para cada primo p, defínese a *norma p-ádica* $|\cdot|_p \colon \mathbb{Q}_p \to \mathbb{R}^+ \cup \{0\}$ mediante:

$$|x|_p = p^{-v_p(x)}.$$

Pódese comprobar de xeito sinxelo que, en efecto, a norma p-ádica verifica as propiedades necesarias para ser unha norma. Isto é, para $x, y \in \mathbb{Q}_p$ arbitrarios:

- $|x|_p \geq 0$ e $|x|_p = 0$ se, e só se, $x = 0$.
- $|xy|_p = |x|_p |y|_p$.
- $|x+y|_p \leq |x|_p + |y|_p$.

Observación 3.8. Poderiamos ter definido $\mathbb{Q}_p$ (respectivamente $\mathbb{Z}_p$) como a completación de $\mathbb{Q}$ (respectivamente $\mathbb{Z}$) coa norma p-ádica.

3.2. Cohomoloxía de grupos

O obxectivo desta sección é expoñer de xeito resumido as principais nocións sobre cohomoloxía de grupos, que serán necesarias para levar a cabo demostracións nos capítulos posteriores.

O noso primeiro obxectivo é definir os grupos de cohomoloxía, para o cal precisaremos dúas definicións previas.

Definición 3.9. Sexa G un grupo. Un *G-módulo* é un grupo abeliano M xunto cunha aplicación

$$\begin{array}{ccc} G \times M & \longrightarrow & M \\ (g, m) & \longmapsto & gm \end{array}$$

tal que, para $g, g' \in G$, $m, m' \in M$ e $1 \in G$ o neutro do grupo G:

1. $g(m + m') = gm + gm'$.
2. $(gg')m = g(g'm)$, $1m = m$.

Nótese que, alternativamente, poderíamos ter definido os G-módulos como grupos abelianos M xunto cun homomorfismo de grupos $G \to \mathrm{Aut}(M)$.

Definición 3.10. Sexa G un grupo. Un *homomorfismo de G-módulos* é unha apliación $\alpha\colon M \to N$, con M e N dous G-módulos, tal que:

1. $\alpha(m + m') = \alpha(m) + \alpha(m')$ para $m.m' \in M$ arbitrarios.
2. $\alpha(gm) = g\alpha(m)$ para todo $g \in G$ e todo $m \in M$.

Sexan agora un grupo G, un enteiro $r \geq 0$ e un G-módulo M e consideremos $\tilde{C}^r(G, M)$ o conxunto de funcións $\phi\colon G^{r+1} \to M$ que quedan fixas por G. Isto é, para elementos arbitrarios $g, g_0, \dots, g_r \in G$, son as funcións $\phi\colon G^{r+1} \to M$ tales que

$$\phi(gg_0, \dots, gg_r) = g\phi(g_0, \dots, g_r).$$

Introducimos unha *aplicación fronteira* $\tilde{d}^r\colon \tilde{C}^r(G, M) \to \tilde{C}^{r+1}(G, M)$ mediante

$$\left(\tilde{d}^r\phi\right)(g_0, \dots, g_{r+1}) = \sum_{k=0}^{r+1} (-1)^k \phi(g_0, \dots, \hat{g}_i, \dots, g_{r+1}),$$

onde a notación $\hat{g}_i$ significa que "omitimos" a variable g_i.

Definición 3.11. Sexan un grupo G, un enteiro $r \geq 0$ e un G-módulo M. Defínese o r-ésimo *grupo de cohomoloxía* $H^r(G, M)$ como

$$H^r(G, M) \cong \frac{\ker\left(\tilde{d}^r\right)}{\operatorname{Im}\left(\tilde{d}^{r-1}\right)}.$$

Como construción alternativa, podemos considerar o *grupo de r-cocadeas non homoxéneas de G* con valores en M (é dicir, as aplicacións $\phi\colon G^r \to M$), usualmente denotado por $C^r(G, M)$. Fixado $G^0 = \{1\}$, definimos os *homomorfismos de conexión* $d^r\colon C^r(G, M) \to C^{r+1}(G, M)$, onde o valor $\left(d^r\phi\right)(g_1, \dots, g_{r+1})$ vén dado por

$$g_1\phi(g_2 \dots, g_{r+1}) + \sum_{k=1}^{r}(-1)^k\phi(g_1, \dots, g_k g_{k+1}, \dots, g_{r+1}) + (-1)^{r+1}\phi(g_1, \dots, g_r).$$

Finalmente, considerando o conxunto de r-cociclos $Z^r(G, M) = \ker\left(d^r\right)$ e o conxunto de r-cobordes $B^r(G, M) = \operatorname{Im}\left(d^{r-1}\right)$, tense un isomorfismo canónico

$$H^r(G, M) \cong \frac{Z^r(G, M)}{B^r(G, M)}.$$

Observación 3.12. De xeito análogo podemos definir os *grupos de homoloxía* $\mathcal{H}_1(G, M)$.

Exemplo 3.13.

- Sexa G un grupo e sexa M un G-módulo. Denotemos por M^G o conxunto dos elementos $m \in M$ tales que $gm = m$ para cada $g \in G$. Entón $H^0(G, M) = M^G$.
- **Teorema 90 de Hilbert:** sexa L/K unha extensión de Galois finita con grupo de Galois G. Tense entón que $H^1\left(G, L^\times\right) = 0$.

Antes de continuar coas seguintes definicións relativas aos grupos de cohomoloxía, cabe destacar o bo comportamento dos mesmos respecto dos produtos:

Proposición 3.14. *Sexa un grupo G e tomemos un enteiro $r \geq 0$. Dados I un conxunto de índices e $\{M_i\}_{i\in I}$ unha familia de G-módulos,*

$$H^r\left(G, \prod_{i\in I} M_i\right) \cong \prod_{i\in I} H^r(G, M_i).$$

Demostración. Véxase [14, p. 68]. □

A seguinte etapa desta sección consistirá en estudar o comportamento dos grupos de cohomoloxía cando mudamos o grupo sobre o que estamos a traballar.

Definición 3.15. Sexan dous grupos G e G' e sexan M un G-módulo, M' un G'-módulo. Dous homomorfismos $\alpha\colon G' \to G$ e $\beta\colon M \to M'$ dinse *compatibles* se, para elementos calquera $g \in G'$ e $m \in M$:

$$\beta(\alpha(g)m) = g\beta(m).$$

Nótese que, nas condicións da definición anterior, a noción de compatibilidade induce un homomorfismo

$$\begin{array}{ccc} C^r(G,M) & \longrightarrow & C^r(G',M') \\ \phi & \longmapsto & \beta \circ \phi \circ \alpha^r. \end{array}$$

para cada enteiro $r \geq 0$, e isto define á súa vez un homomorfismo $H^r(G,M) \to H^r(G',M')$.

Definición 3.16. Sexan un grupo G, un enteiro $r \geq 0$ e un G-módulo M. Imos considerar o homomorfismo antes definido nuns casos particularmente importantes:

1. Sexa H un subgrupo de G e sexan α a inclusión de H en G e β a identidade de M. Obtense neste caso o *homomorfismo de restrición*

$$\mathrm{Res}\colon H^r(G,M) \longrightarrow H^r(H,M).$$

2. Sexa H un subgrupo normal de G e sexan $\alpha\colon G \to G/H$ a proxección natural e $\beta\colon M^H \hookrightarrow M$ a inclusión. Obtense neste caso o *homomorfismo de inflación*

$$\mathrm{Inf}\colon H^r\left(G/H, M^H\right) \longrightarrow H^r(G,M).$$

3. Sexa H un subgrupo de G de índice finito e sexa S un conxunto de representantes pola esquerda de G/H. Para cada $m \in M^H$, definimos unha norma

$$N_{G/H}(m) = \sum_{s \in S} sm,$$

que coincide coa noción de "norma" nunha extensión de Galois (isto é, o produto dun elemento polo seu conxugado). Nótese que $N_{G/H}$ é independente da escolla de S e queda fixo por G, o cal induce un homomorfismo $M^H \to M^G$. Podemos estender este homomorfismo para todo $r \geq 0$, dando lugar ao denominado *homomorfismo de correstrición*

$$\mathrm{Cor}\colon H^r(H,M) \longrightarrow H^r(G,M).$$

A continuación, presentamos algunhas das propiedades que verifican os anteriores homomorfismos:

Proposición 3.17. *Sexan un grupo G, un G-módulo M e un enteiro $r \geq 0$.*

- *Sexa H un subgrupo de G de índice finito. A composición*

$$\mathrm{Cor} \circ \mathrm{Res}\colon H^r(G,M) \longrightarrow H^r(G,M)$$

coincide coa multiplicación por $[G\colon H]$.

- *Sexa H un subgrupo normal de G. Supoñamos que $r > 0$ é que $H^i(H,M) = 0$ para todo $0 < i < r$. Entón*

$$0 \longrightarrow H^r\left(G/H, M^H\right) \xrightarrow{\mathrm{Inf}} H^r(G,M) \xrightarrow{\mathrm{Res}} H^r(H,M)$$

é unha sucesión exacta.

Demostración. Véxase [14, pp. 70 e 71]. □

3.3. Formas modulares e cohomoloxía

Nesta sección final do capítulo introduciremos unha nova ferramenta necesaria para o desenvolvemento da teoría de Hida: a cohomoloxía parabólica. Tamén enunciaremos o teorema do isomorfismo de Eichler–Shimura, relacionado coa cohomoloxía anterior.

Durante o desenvolvemento desta sección, o grupo G arbitrario que empregabamos para definir os grupos de cohomoloxía será trocado por un subgrupo de congruencia Γ, o cal é importante recordar que actúa en $\mathbb{P}^1(\mathbb{Q})$. Podemos entón considerar considerar a cohomoloxía correspondente a Γ.

Definición 3.18. Sexa Γ un subgrupo de congruencia. Un elemento $\gamma \in \Gamma$ dise *parabólico* se existe exactamente un elemento $a \in \mathbb{P}^1(\mathbb{Q})$ tal que $\gamma a = a$.

Nos termos da definición anterior, sexa P o conxunto de elementos parabólicos de Γ. Dado un Γ-módulo M, podemos considerar o Γ-submódulo $C_P^1(\Gamma,M)$ de $C^1(\Gamma,M)$ formado polos elementos $u \in C^1(\Gamma,M)$ tales que para todo $\gamma \in P$ existe $m \in M$ verificando $u(\gamma) = (\gamma - 1)m$. Podemos entón considerar os seguintes conxuntos:

$$Z_P^1(\Gamma,M) = Z^1(\Gamma,M) \cap C_P^1(\Gamma,M) \quad \text{e} \quad B_P^2(\Gamma,M) = d^1\left(C_P^1(\Gamma,M)\right).$$

Definición 3.19. Sexa Γ un subgrupo de congruencia e sexa M un Γ-módulo. Se P denota o conxunto de elementos parabólicos de Γ, definimos os *grupos de cohomoloxía parabólica* de Γ con coeficientes en M como:

$$H_P^0(\Gamma,M) = H^0(\Gamma,M), \qquad H_P^1(\Gamma,M) = \frac{Z_P^1(\Gamma,M)}{B^1(\Gamma,M)} \quad \text{e} \quad H_P^2(\Gamma,M) = \frac{Z^2(\Gamma,M)}{B_P^2(\Gamma,M)}.$$

Para finalizar esta sección, imos construír a base do teorema de Eichler–Shimura. Dado un enteiro $n \geq 0$, sexa $L_n(\mathbb{R})$ o submódulo de $\mathbb{R}[X,Y]$ formado polos polinomios homoxéneos de grao n e observemos que $M_2(\mathbb{R})$ actúa pola esquerda en $L_n(\mathbb{R})$ mediante

$$\gamma P(X,Y) = P\left(\left(\gamma^\iota \begin{pmatrix} X \\ Y \end{pmatrix}\right)^t\right),$$

onde γ^ι denota a matriz adxunta de γ, que sabemos que se pode calcular mediante

$$\gamma^\iota = \det(\gamma)\gamma^{-1}$$

se γ é invertible. Fixemos agora $z_0 \in \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ e un enteiro $k \geq 0$. Para cada $f \in \mathrm{S}_{k+2}(\Gamma)$ consideremos a *diferencial holomorfa*

$$D_k(f) = f(z)(X + zY)^k dz$$

e a aplicación $\varphi_{f,z_0} \colon \Gamma \to L_k(\mathbb{R})$ definida como

$$\varphi_{f,z_0}(\gamma) = \int_{z_0}^{\gamma z_0} \Re(D_k(f)) = \sum_{l=0}^{k} \binom{k}{\ell} X^{k-\ell} Y^\ell \int_{z_0}^{\gamma z_0} \Re\left(f(z) z^\ell dz\right).$$

A integral anterior está ben definida e converxe para todo $\gamma \in \Gamma$ (véxase [7, §6.2]). Polo teorema de Cauchy, dado outro punto $z_1 \in \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ temos

$$\begin{aligned} \varphi_{f,z_1}(\gamma) - \varphi_{f,z_0}(\gamma) &= \int_{z_1}^{\gamma z_1} \Re(D_k(f)) - \int_{z_0}^{\gamma z_0} \Re(D_k(f)) \\ &= \int_{z_0}^{z_1} \Re(D_k(f)) - \int_{z_0}^{z_1} \Re(\gamma^* D_k(f)) = (I - \gamma) \int_{z_0}^{z_1} \Re(D_k(f)). \end{aligned}$$

Aínda máis: dadas $\gamma_1, \gamma_2 \in \Gamma$:

$$\begin{aligned} \varphi_{f,z_0}(\gamma_1\gamma_2) &= \int_{z_0}^{\gamma_1(\gamma_2 z_0)} \Re(D_k(f)) \\ &= \int_{\gamma z_0}^{\gamma_1(\gamma_2 z_0)} \Re(D_k(f)) + \varphi_{f,z_0}(\gamma_1) \\ &= \gamma_1 \int_{z_0}^{\gamma_2 z_0} \Re(D_k(f)) + \varphi_{f,z_0}(\gamma_1) = \gamma_1 \varphi_{f,z_0}(\gamma_2) + \varphi_{f,z_0}(\gamma_1). \end{aligned}$$

Polo tanto, φ_{f,z_0} pertence a $Z^1(\Gamma, M)$ e a súa clase de cohomoloxía é independente do punto z_0 escollido. De feito, dado $s \in \mathbb{P}^1(\mathbb{Q})$ un punto parabólico e $\gamma \in \Gamma$ tal que $\gamma s = s$,

$$\varphi_f(\gamma) = \int_x^{\gamma s} \Re(D_k(f)) = 0.$$

Teorema 3.20 (Isomorfismo de Eichler-Shimura)**.** *Sexa un enteiro $k \geq 2$ e sexa Γ un subgrupo de congruencia con conxunto de puntos parabólicos P. A aplicación*

$$\begin{array}{rccc} \varphi\colon & \mathrm{S}_k(\Gamma) & \longrightarrow & H^1_P(\Gamma, L_{k-2}(\mathbb{R})) \\ & f & \longmapsto & \varphi_f \end{array}$$

é un isomorfismo $\mathbb{R}$-linear.

Demostración. Véxase [19, Teorema 18]. □

Observación 3.21. É importante destacar a gran relevancia deste teorema, pois este permite "entender" as formas cuspidais sobre un subgrupo de congruencia calquera como elementos dun grupo de cohomoloxía. Isto dá lugar á teoría dos *símbolos modulares*, que son de gran utilidade tanto dende o punto de vista computacional como na construción das chamadas *series L p-ádicas*.

Adicionalmente, dado N un enteiro positivo e χ un carácter de Dirichlet, se definimos o $\Gamma_0(N)$-módulo $L_n(\chi;\mathbb{C})$ como o submódulo de $\mathbb{C}[X,Y]$ formado polos polinomios homoxéneos de grao $n \geq 0$ coa $\Gamma_0(N)$-acción dada por

$$\gamma P(X,Y) = \chi(\gamma) P\left(\left(\gamma^{\iota}\begin{pmatrix} X \\ Y \end{pmatrix}\right)^t\right),$$

podemos enunciar o seguinte resultado:

Teorema 3.22. *Sexan enteiros positivos $k \geq 2$ e r, un primo impar p e un carácter de Dirichlet $\chi\colon (\mathbb{Z}/p^r\mathbb{Z})^\times \to \mathbb{C}^\times$. Téñense os seguintes isomorfismos de espazos vectoriais:*

$$\begin{aligned} \mathrm{M}_k(\Gamma_0(p^r),\chi) \oplus \overline{\mathrm{S}_k(\Gamma_0(p^r),\chi^{-1})} &\cong H^1(\Gamma_0(p^r), L_{k-2}(\chi;\mathbb{C})), \\ \mathrm{S}_k(\Gamma_0(p^r),\chi) \oplus \overline{\mathrm{S}_k(\Gamma_0(p^r),\chi^{-1})} &\cong H^1_P(\Gamma_0(p^r), L_{k-2}(\chi;\mathbb{C})), \end{aligned}$$

onde P é o conxunto de puntos parabólicos de $\Gamma_0(p^r)$ e

$$\overline{\mathrm{S}_k(\Gamma_0(p^r),\chi^{-1})} = \left\{\overline{f(z)} \mid f \in \mathrm{S}_k\left(\Gamma_0(p^r),\chi^{-1}\right)\right\}.$$

Demostración. Véxase [7, Teorema 6.3.4]. □

Capítulo 4

Formas modulares p-ádicas

Ata agora estivemos considerando as formas modulares como $\mathbb{C}$-espazos vectoriais. O obxectivo deste capítulo será definilas novamente e estudalas sobre o corpo dos números p-ádicos $\mathbb{Q}_p$, dando lugar ás "formas modulares p-ádicas". Tamén introduciremos os espazos de formas ordinarias, cuxas propiedades serán máis doadas de estudar e que terán unha gran importancia no desenvolvemento do capítulo seguinte.

4.1. Construción de Serre

Nesta sección faremos a construción de Serre das formas modulares p-ádicas para cada número primo p impar e veremos as súas boas propiedades. A teoría subseguinte podería ser tamén desenvolvida no caso de $p = 2$, pero omitiremos este caso polas complicacións técnicas que implica o seu estudo.

Comecemos introducindo novas notacións:

Notación 4.1. Sexan enteiros $N \geq 1$ e $k \geq 0$. Dado un corpo de números L (é dicir, unha extensión finita de $\mathbb{Q}$) e dado un carácter de Dirichlet χ, imos denotar o espazo de formas modulares (respectivamente, cuspidais) de peso k e nivel $\Gamma_0(N)$ con carácter χ cuxos coeficientes de Fourier $a_n(f)$ pertencen a L para todo $n \geq 0$ como $\mathrm{M}_k(\Gamma_0(N), \chi; L)$ (respectivamente, $\mathrm{S}_k(\Gamma_0(N), \chi; L)$). Ademais, en virtude do teorema 2.25, denotaremos por $\mathrm{M}_k(\Gamma_1(N); L)$ (respectivamente, $\mathrm{S}_k(\Gamma_1(N); L)$) o espazo de formas modulares (respectivamente, cuspidais) de peso k e nivel $\Gamma_1(N)$ con coeficientes en L.

Notación 4.2. Para cada primo impar p, sexa $\overline{\mathbb{Q}}_p$ a clausura alxébrica do corpo de números p-ádicos $\mathbb{Q}_p$. Denotaremos por $\mathbb{C}_p$ a completación de $\overline{\mathbb{Q}}_p$ coa norma p-ádica. Considerando o mergullo $i_p \colon \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_p$, poderemos considerar no futuro os elementos de $\overline{\mathbb{Q}}$ como números complexos e p-ádicos simultaneamente.

Precisaremos tamén unha ferramenta previa:

Definición 4.3. Sexa p un primo impar e sexa unha serie de potencias en q con coeficientes en $\mathbb{Q}$, $f = \sum_{n\geq 0} a_n q^n \in \mathbb{Q}[\![q]\!]$. Defínese a *valoración p-ádica* de f como

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

Vexamos agora a construción das formas modulares p-ádicas de Serre.

Definición 4.4. Sexan $N \geq 1$ e $k \geq 0$ enteiros e p un primo impar. Unha serie de potencias $f = \sum_{n=0}^{\infty} a_n q^n \in \mathbb{Q}_p[\![q]\!]$ dise unha *forma modular p-ádica de Serre* (ou simplemente unha *forma modular p-ádica*) se existe unha sucesión $\{f_i\}_{i=0}^{\infty}$ de formas modulares con $f_i \in \mathrm{M}_{k_i}(\Gamma_1(N); \mathbb{Q})$ e $k_i \geq 0$ enteiros tal que

$$v_p(f - f_i) \xrightarrow[i\to\infty]{} \infty.$$

Nótese que a definición das formas modulares p-ádicas non inclúe un peso asociado ás mesmas. Veremos a continuación por que non é necesario requirir esta noción na definición anterior.

Teorema 4.5. *Sexan f_1 e f_2 formas modulares non nulas de pesos k_1 e k_2 respectivamente, nivel $\Gamma_1(N)$ con $N \geq 1$ e coeficientes en $\mathbb{Q}$, con $v_p(f_1) = 0$ para un certo primo impar p. Se existe algún enteiro positivo m tal que $v_p(f_1 - f_2) \geq m$ entón*

$$k_1 \equiv k_2 \ \left(\mathrm{mód}\ (p-1)p^{m-1}\right).$$

Demostración. Véxase [18, pp. 197-200]. □

Consideremos agora para un primo impar p os espazos

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

para cada m e o espazo $X = \varprojlim X_m$. Nótese que, polo teorema chinés dos restos,

$$X \cong \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}.$$

Corolario 4.6. *Sexa p un primo impar. Consideremos unha forma modular p-ádica de Serre f con coeficientes en $\mathbb{Q}_p$ e unha sucesión de formas modulares $\{f_i\}_{i=0}^{\infty}$ con coeficientes en $\mathbb{Q}$ e pesos k_i respectivamente tales que*

$$v_p(f - f_i) \xrightarrow[i\to\infty]{} \infty.$$

Existe un único $k \in X$ tal que $\{k_i\}_{i=0}^{\infty}$ converxe a k, e este elemento é independente das f_i.

Demostración. Polo teorema 4.5 podemos considerar $k = \varprojlim k_i$, co cal $k \in X$ por definición e este elemento é único e independente das formas f_i por resultados estándares sobre os límites proxectivos. □

Nas hipóteses do corolario anterior, dise que k é o *peso* da forma modular p-ádica de Serre f.

Para finalizar a sección, imos facer mención a un resultado que asegura que para construír unha forma modular p-ádica de Serre basta con obter unha familia de formas modulares p-ádicas de pesos "compatibles" e cuxos coeficientes de Fourier a_n converxen uniformemente para $n \geq 1$. Unha vez feito isto, o termo constante da forma p-ádica obtense "automaticamente".

Teorema 4.7. *Sexa un primo impar p e sexa $\{f_i = \sum_{n=0}^{\infty} a_{i,n} q^n\}_{i=0}^{\infty}$ unha familia de formas modulares p-ádicas de pesos k_i respectivamente e coeficientes en $\mathbb{Q}_p$ tales que:*

- *Para $n \geq 1$ os coeficientes $a_{i,n}$ converxen uniformemente a un certo $a_n \in \mathbb{Q}_p$.*
- *$\{k_i\}_{i=0}^{\infty}$ converxe a un certo $k \in X$.*

Entón:

- *Os coeficientes $a_{i,0}$ converxen a un certo $a_0 \in \mathbb{Q}_p$.*
- *$f = \sum_{n=0}^{\infty} a_n q^n$ é unha forma modular p-ádica de Serre de peso k.*

Demostración. Véxase [18, pp. 204 e 205]. □

Os resultados anteriores permítennos entender as formas modulares p-ádicas de Serre como límites p-ádicos de formas modulares clásicas. Non obstante, máis adiante no traballo estudaremos tamén a definición de Katz das formas modulares p-ádicas, que será tratada nun contexto máis xeral e que terá unha maior complexidade.

4.2. Primeiros resultados

Nesta sección expandiremos nocións xa coñecidas para as formas modulares clásicas para así poder empregalas tamén no caso das formas modulares con coeficientes p-ádicos de pesos enteiros clásicos, pois polo de agora non será necesario considerar as formas modulares p-ádicas da sección anterior en toda a súa xeneralidade.

En primeiro lugar, novamente por mor do teorema 2.25, para cada enteiro $k > 0$, A unha subálxebra de $\mathbb{C}$ e V un A-submódulo de $\mathrm{M}_k(\Gamma_1(N); A)$ estable pola acción dos

operadores de Hecke e dos operadores diamante, definimos a *álxebra de Hecke* $\mathcal{H}(V;A)$ como a A-subálxebra de $\mathrm{End}_A(V)$ xerada por T_n e $\langle n\rangle$, con $n\in\mathbb{N}$. Así, para cada carácter de Dirichlet χ podemos considerar as seguintes álxebras de Hecke conmutativas:

$$\begin{aligned}\mathcal{H}_k(\Gamma_1(N);A) &= \mathcal{H}(\mathrm{M}_k(\Gamma_1(N);A);A),\\ \mathfrak{h}_k(\Gamma_1(N);A) &= \mathcal{H}(\mathrm{S}_k(\Gamma_1(N);A);A),\\ \mathcal{H}_k(\Gamma_0(N),\chi;A) &= \mathcal{H}(\mathrm{M}_k(\Gamma_0(N),\chi;A);A),\\ \mathfrak{h}_k(\Gamma_0(N),\chi;A) &= \mathcal{H}(\mathrm{S}_k(\Gamma_0(N),\chi;A);A).\end{aligned}$$

Se supoñemos ademais que $\mathbb{Z}[\chi]\subset A$, con $\mathbb{Z}[\chi]$ a extensión de $\mathbb{Z}$ xerada polos valores da imaxe de χ, e denotamos por K o corpo cociente de A, podemos definir o espazo

$$\mathrm{M}_{k,0}(\Gamma_0(N),\chi;A)=\{f\in\mathrm{M}_k(\Gamma_0(N),\chi;K)\mid a_n(f)\in A \text{ para todo } n\geq 1\}.$$

O seguinte resultado de dualidade pode ser demostrado adaptando a proba do teorema 4.14, que non é máis que unha versión máis xeral deste.

Teorema 4.8. *Sexan $N\geq 1$ e $k\geq 2$ enteiros, $\chi\colon(\mathbb{Z}/N\mathbb{Z})^\times\to\mathbb{C}^\times$ un carácter de Dirichlet. Para calquera subálxebra A de $\mathbb{C}$ contendo a $\mathbb{Z}[\chi]$, o emparellamento*

$$\begin{array}{ccc}\mathcal{H}_k(\Gamma_0(N),\chi;A)\times\mathrm{M}_{k,0}(\Gamma_0(N),\chi;A) & \longrightarrow & A\\ (T,f) & \longmapsto & a_1(Tf)\end{array}$$

induce os isomorfismos de A-módulos seguintes:

$$\begin{aligned}\mathrm{Hom}_A(\mathcal{H}_k(\Gamma_0(N),\chi;A),A)&\cong\mathrm{M}_{k,0}(\Gamma_0(N),\chi;A),\\ \mathrm{Hom}_A(\mathfrak{h}_k(\Gamma_0(N),\chi;A),A)&\cong\mathrm{S}_k(\Gamma_0(N),\chi;A),\\ \mathrm{Hom}_A(\mathrm{M}_{k,0}(\Gamma_0(N),\chi;A),A)&\cong\mathcal{H}_k(\Gamma_0(N),\chi;A),\\ \mathrm{Hom}_A(\mathrm{S}_k(\Gamma_0(N),\chi;A),A)&\cong\mathfrak{h}_k(\Gamma_0(N),\chi;A).\end{aligned}$$

Regresemos agora ao caso das formas modulares p-ádicas.

Notación 4.9. Sexa $\chi\colon(\mathbb{Z}/N\mathbb{Z})^\times\to\mathbb{C}^\times$ un carácter de Dirichlet para algún enteiro $N\geq 1$. Para calquera enteiro $k>0$ e calquera subanel A de $\mathbb{C}_p$ tal que $\mathbb{Z}[\chi]\subset A$, denotamos o *espazo de formas modulares p-ádicas de Serre* sobre A de peso k, nivel $\Gamma_0(N)$ e carácter χ por $\mathrm{M}_k(N,\chi;A)$, e o seu análogo de formas cuspidais por $\mathrm{S}_k(N,\chi;A)$.

Observación 4.10. Nas mesmas condicións, por extensión de escalares podemos considerar os espazos anteriores como

$$\begin{aligned}\mathrm{M}_k(N,\chi;A)&=\mathrm{M}_k(N,\chi;\mathbb{Z}[\chi])\otimes_{\mathbb{Z}[\chi]}A,\\ \mathrm{S}_k(N,\chi;A)&=\mathrm{S}_k(N,\chi;\mathbb{Z}[\chi])\otimes_{\mathbb{Z}[\chi]}A.\end{aligned}$$

O noso obxectivo agora é definir os operadores de Hecke actuando sobre os espazos anteriores, o cal faremos baseándonos nas fórmulas do teorema 2.33, así como as súas álxebras de Hecke.

Definición 4.11. Sexan enteiros $N \geq 1$ e $k > 0$, χ un carácter de Dirichlet e A un subanel da $\mathbb{C}_p$, con p un primo impar, tal que $\mathbb{Z}[\chi] \subset A$. Dada unha forma modular p-ádica de Serre $f \in \mathrm{M}_k(N, \chi; A)$ con expansión de Fourier $f = \sum_{n=0}^{\infty} a_n(f)q^n$, definimos o m-ésimo *operador de Hecke* de formas modulares p-ádicas $T_m \colon \mathrm{M}_k(N, \chi; A) \to \mathrm{M}_k(N, \chi; A)$ para cada $m > 0$ mediante

$$T_m f = \sum_{n=0}^{\infty} a_n(T_m f)q^n,$$

onde para cada $n \geq 0$

$$a_n(T_m f) = \sum_{d|(m,n)} \chi(d)d^{k-1}a_{\frac{mn}{d^2}}(f).$$

É claro que estes operadores son A-lineares e que a súa restrición a $\mathrm{S}_k(N, \chi; A)$ é unha aplicación A-linear do mesmo.

Definición 4.12. Sexan enteiros $N \geq 1$ e $k > 0$, χ un carácter de Dirichlet e A un subanel da $\mathbb{C}_p$, con p un primo impar, tal que $\mathbb{Z}[\chi] \subset A$. Definimos as *álxebras de Hecke* das formas modulares p-ádicas de Serre

$$\mathcal{H}_k(N, \chi; A) = \mathcal{H}(\mathrm{M}_k(N, \chi; A); A) \quad \text{e} \quad \mathfrak{h}_k(N, \chi; A) = \mathcal{H}(\mathrm{S}_k(N, \chi; A); A)$$

como as A-subálxebras de $\mathrm{End}_A(\mathrm{M}_k(N, \chi; A))$ e de $\mathrm{End}_A(\mathrm{S}_k(N, \chi; A))$, respectivamente, xeradas polos operadores de Hecke T_n para todos os enteiros $n \geq 1$.

Observación 4.13. Posto que

$$\mathrm{End}_A(\mathrm{M}_k(N, \chi; A)) \cong \mathrm{End}_{\mathbb{Z}[\chi]}(\mathrm{M}_k(N, \chi; \mathbb{Z}[\chi])) \otimes_{\mathbb{Z}[\chi]} A,$$
$$\mathrm{End}_A(\mathrm{S}_k(N, \chi; A)) \cong \mathrm{End}_{\mathbb{Z}[\chi]}(\mathrm{S}_k(N, \chi; \mathbb{Z}[\chi])) \otimes_{\mathbb{Z}[\chi]} A,$$

podemos considerar tamén as álxebras de Hecke das formas modulares p-ádicas mediante os isomorfismos seguintes:

$$\mathcal{H}_k(N, \chi; A) \cong \mathcal{H}_k(N, \chi; \mathbb{Z}[\chi]) \otimes_{\mathbb{Z}[\chi]} A,$$
$$\mathfrak{h}_k(N, \chi; A) \cong \mathfrak{h}_k(N, \chi; \mathbb{Z}[\chi]) \otimes_{\mathbb{Z}[\chi]} A.$$

Coas estruturas anteriores xa definidas, podemos enunciar un resultado de dualidade análogo ao teorema 4.8 para o caso das formas modulares p-ádicas de Serre, para o cal precisamos definir o espazo

$$\mathrm{M}_{k,0}(N, \chi; A) = \{f \in \mathrm{M}_k(N, \chi; K) \mid a_n(f) \in A \text{ para todo } n \geq 1\},$$

onde K denota o corpo de fraccións de A.

Teorema 4.14. *Sexan enteiros $N \geq 1$ e $k > 0$, p un primo impar, K unha extensión finita de $\mathbb{Q}_p$ con anel de valoración $\mathcal{O}$ (é dicir, un dominio $\mathcal{O} \subset K$ tal que $x \in \mathcal{O}$ ou $x^{-1} \in \mathcal{O}$ para todo $x \in K$, $x \neq 0$) e $\chi\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathcal{O}^\times$ un carácter de Dirichlet. Entón, para $A = K$ ou $A = \mathcal{O}$:*

$$\begin{aligned}
\mathrm{Hom}_A(\mathcal{H}_k(N,\chi;A),A) &\cong \mathrm{M}_{k,0}(N,\chi;A),\\
\mathrm{Hom}_A(\mathfrak{h}_k(N,\chi;A),A) &\cong \mathrm{S}_k(N,\chi;A),\\
\mathrm{Hom}_A(\mathrm{M}_{k,0}(N,\chi;A),A) &\cong \mathcal{H}_k(N,\chi;A),\\
\mathrm{Hom}_A(\mathrm{S}_k(N,\chi;A),A) &\cong \mathfrak{h}_k(N,\chi;A).
\end{aligned}$$

Demostración. Imos probar unicamente os casos referentes a $\mathrm{M}_{k,0}(N,\chi;A)$, pois o mesmo argumento é válido para os casos das formas cuspidais. Ademais, empregaremos a seguinte notación para axilizar o desenvolvemento da proba:

$$\mathrm{M}_{k,0}(N,\chi;A) =: \mathrm{M}(A) \quad \text{e} \quad \mathcal{H}_k(N,\chi;A) =: \mathcal{H}(A).$$

Probemos pois que, ao igual que no teorema 4.8, os isomorfismos veñen dados polo emparellamento

$$\begin{array}{ccc} \mathcal{H}(A)\times \mathrm{M}(A) & \longrightarrow & A \\ (T,f) & \longmapsto & a_1(Tf). \end{array}$$

Comecemos co caso $A = K$. Pódese comprobar en [7, §5.4] que $\mathrm{M}_k(N,\chi;\mathbb{Z}[\chi]))$ é libre e finitamente xerado sobre $\mathbb{Z}[\chi]$, do que se segue que $\mathrm{M}(K)$ ten dimensión finita sobre K. Así:

$$\dim_K(\mathcal{H}(K)) \leq \dim_K(\mathrm{End}_K(\mathrm{M}(K))) < \infty.$$

Posto que os espazos $\mathrm{M}(K)$ e $\mathcal{H}(K)$ son K-espazos vectoriais de dimensión finita, sabemos que

$$\begin{aligned}
\dim_K(\mathrm{M}(K)) &= \dim_K(\mathrm{Hom}_K(\mathrm{M}(K),K)),\\
\dim_K(\mathcal{H}(K)) &= \dim_K(\mathrm{Hom}_K(\mathcal{H}(K),K)).
\end{aligned}$$

Polo tanto, para demostrar que

$$\begin{aligned}
\mathrm{Hom}_K(\mathcal{H}(K),K) &\cong \mathrm{M}(K),\\
\mathrm{Hom}_K(\mathrm{M}(K),K) &\cong \mathcal{H}(K),
\end{aligned}$$

bastará con probar que a aplicación $\mathcal{H}(K) \to \mathrm{Hom}_K(\mathrm{M}(K),K)$ dada por $T \mapsto (T,\cdot)$ e que $\mathrm{M}(K) \to \mathrm{Hom}_K(\mathcal{H}(K),K)$ definida como $f \mapsto (\cdot,f)$ son homomorfismos inxectivos de K-espazos vectoriais. É dicir, bastará con probar que o emparellamento $(\cdot,\cdot)$ é non

dexenerado. Pola definición do emparellamento, as dúas aplicacións anteriores son claramente homomorfismos de K-espazos vectoriais. Supoñamos que existe $T \in \mathcal{H}(K)$ tal que $(T, f) = 0$ para toda $f \in \mathrm{M}(K)$. Pola definición 4.11 temos, para cada $n \geq 1$,

$$a_n(Tf) = a_1(T_n T f) = a_1(T T_n f) = (T, T_n f) = 0.$$

Isto implica que Tf é unha constante, e posto que o peso k é positivo entón necesariamente temos $Tf = 0$. Finalmente, como f foi seleccionada de xeito arbitrario entón T ten que ser o operador identicamente nulo, logo o homomorfismo de K-espazos vectoriais $T \mapsto (T, \cdot)$ é inxectivo. Por outra banda, supoñamos que existe $f \in \mathrm{M}(K)$ tal que $(T, f) = 0$ para todo $T \in \mathcal{H}(K)$. Para cada $n \geq 1$ temos, argumentando de xeito análogo ao caso anterior,

$$a_n(f) = a_1(T_n f) = (T_n, f) = 0,$$

polo que $f = 0$ posto que f ten que ser constante e o peso k é positivo. Así, o homomorfismo de K-espazos vectoriais $f \mapsto (\cdot, f)$ é inxectivo, o cal conclúe a proba do teorema no caso $A = K$.

Demostremos agora o resultado no caso $A = \mathcal{O}$. Podemos repetir novamente o argumento anterior para demostrar que o emparellamento é non dexenerado. En particular, o homomorfismo de $\mathcal{O}$-módulos $\mathrm{M}(\mathcal{O}) \to \mathrm{Hom}_{\mathcal{O}}(\mathcal{H}(\mathcal{O}), \mathcal{O})$ definido como $f \colon (\cdot, f)$ é inxectivo. Para probar a sobrexectividade, nótese que todo $\varphi \in \mathrm{Hom}_{\mathcal{O}}(\mathcal{H}(\mathcal{O}), \mathcal{O})$ pode ser estendido a un homomorfismo $\varphi' \in \mathrm{Hom}_K(\mathcal{H}(K), K)$ definindo $\varphi'(T) = \varphi(T)$ para todo $T \in \mathcal{H}(\mathcal{O})$ e estendéndoo por K-linearidade ao resto do espazo. Polo xa visto ata agora, sabemos que existe $f \in \mathrm{M}(K)$ tal que

$$\varphi'(T) = (T, f)$$

para todo operador $T \in \mathcal{H}(K)$, pero isto implica que, para todo $n \geq 1$,

$$a_n(f) = a_1(T_n f) = (T_n, f) = \varphi'(T_n) = \varphi(T_n) \in \mathcal{O}.$$

Polo tanto, $f \in \mathrm{M}(\mathcal{O})$, logo

$$\mathrm{M}(\mathcal{O}) \cong \mathrm{Hom}_{\mathcal{O}}(\mathcal{H}(\mathcal{O}), \mathcal{O}).$$

Como comentario adicional, é precisamente a sobrexectividade deste isomorfismo a única razón pola que no enunciado do teorema aparece $\mathrm{M}_{k,0}(N, \chi; A)$ no canto de $\mathrm{M}_k(N, \chi; A)$. Finalmente, para probar a última afirmación do teorema, nótese que $\mathcal{H}(\mathcal{O})$ é un $\mathcal{O}$-módulo libre finitamente xerado pola observación 4.13 e polo teorema 4.8, logo é isomorfo ao seu bidual con respecto a $\mathcal{O}$. Así,

$$\mathcal{H}(\mathcal{O}) \cong \mathrm{Hom}_{\mathcal{O}}(\mathrm{M}(\mathcal{O}), \mathcal{O}).$$

□

Para finalizar a sección, imos probar unha consecuencia do teorema anterior relativa ás formas propias de Hecke das álxebras de Hecke de formas modulares p-ádicas, cuxa definición é análoga á dada en 2.34. Consideremos pois, nas mesmas hipóteses que no teorema anterior, unha forma propia de Hecke normalizada $f \in \mathrm{M}_k(N, \chi; A)$. Se $\lambda \in \mathrm{Hom}_A(\mathcal{H}(N, \chi; A), A)$ é o homomorfismo correspondente a f mediante o isomorfismo do teorema, entón para cada par de enteiros positivos m e n temos

$$\lambda(T_n T_m) = a_1(T_n T_m f) = a_n(f) a_1(T_m f) = a_1(T_n f) a_1(T_m f) = \lambda(T_n)\lambda(T_m),$$

co cal λ é un homomorfismo de A-álxebras. Reciprocamente, se λ é o homomorfismo de A-álxebras correspondente a $f \in \mathrm{M}_k(N, \chi; A)$ mediante o isomorfismo do teorema anterior, para cada par de enteiros positivos m e n temos

$$\begin{aligned} a_m(T_n f) &= a_1(T_m T_n f) = \lambda(T_m T_n) = \lambda(T_m)\lambda(T_n) \\ &= a_1(T_m f) a_1(T_n f) = a_m(f) a_n(f). \end{aligned}$$

Polo tanto, o isomorfismo do teorema 4.14 induce unha bixección entre homomorfismos de A-álxebras de $\mathcal{H}(N, \chi; A)$ a A e formas propias de Hecke normalizadas. De feito, isto permite formular o seguinte resultado:

Proposición 4.15. *Sexan enteiros $N \geq 1$ e $k > 0$, p un primo impar, K unha extensión finita de $\mathbb{Q}_p$ con anel de valoración $\mathcal{O}$ e $\chi\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathcal{O}^\times$ un carácter de Dirichlet. Se $f \in \mathrm{M}_k(N, \chi; K)$ é unha forma propia de Hecke normalizada entón f é unha forma propia de Hecke normalizada en $\mathrm{M}_k(N, \chi; \overline{\mathbb{Q}})$.*

Demostración. Consideremos o homomorfismo

$$\lambda\colon \mathcal{H}_k(N, \chi; K) \longrightarrow K$$

inducido por f baixo o emparellamento do teorema 4.14. Posto que

$$\mathcal{H}_k(N, \chi; K) \cong \mathcal{H}_k(N, \chi; \mathbb{Q}(\chi)) \otimes_{\mathbb{Q}(\chi)} K,$$

podemos restrinxir λ ao espazo $\mathcal{H}_k(N, \chi; \mathbb{Q}(\chi))$. De feito, posto que $\mathcal{H}_k(N, \chi; \mathbb{Q}(\chi))$ ten dimensión finita sobre $\mathbb{Q}$, sabemos que $\lambda(\mathcal{H}_k(N, \chi; \mathbb{Q}(\chi))) \subset \overline{\mathbb{Q}}$. Podemos entón definir o homomorfismo de $\overline{\mathbb{Q}}$-álxebras

$$\lambda'\colon \mathcal{H}_k(N, \chi; \overline{\mathbb{Q}}) \longrightarrow \overline{\mathbb{Q}}$$

impoñendo $\lambda'(T_n) = \lambda(T_n)$ para todo $n \geq 1$ e estendéndoo por $\overline{\mathbb{Q}}$-linearidade. Agora, pola dualidade do teorema 4.8 sabemos que existe $f' \in \mathrm{M}_k(N, \chi; \overline{\mathbb{Q}})$ tal que $\lambda'(T) = a_1(Tf')$ para todo $T \in \mathcal{H}_k(N, \chi; \overline{\mathbb{Q}})$. De feito,

$$a_n(f') = a_1(T_n f') = \lambda'(T_n) = \lambda(T_n) = a_1(T_n f) = a_n(f)$$

para todo enteiro positivo n, logo $f - f'$ é necesariamente unha constante, pero como $f - f'$ tamén é unha forma modular p-ádica de peso $k > 0$ entón necesariamente $f - f' = 0$, logo $f = f'$. □

4.3. Formas ordinarias

Os espazos das formas modulares p-ádicas de Serre presentan un problema: son demasiados "grandes" como para estudalos en profundidade, pois a súa dimensión aumenta linearmente co peso k. É por isto que definiremos nesta sección uns subespazos cuxa dimensión non "medre", coñecidos como os espazos de formas ordinarias.

Definición 4.16. Sexan p un primo impar, $r \geq 1$ un enteiro, K unha extensión finita de $\mathbb{Q}_p$ con anel de valoración $\mathcal{O}$ e $\chi\colon (\mathbb{Z}/p^r\mathbb{Z})^\times \to \mathcal{O}^\times$ un carácter de Dirichlet. Defínese o *proxector ordinario* e asociado ao operador T_p como o límite

$$e = \lim_{n\to\infty} T_p^{n!}.$$

Este obxecto será fundamental no desenvolvemento da teoría de Hida. En primeiro lugar, vexamos que está ben definido, para o cal recordamos tres nocións alxébricas:

- Un elemento $a \in A$, con A un anel conmutativo, dise *idempotente* se $a^2 = a$.
- Defínese o *nilradical* dun anel A como o ideal η_A formado polos elementos nilpotentes de A (pódese comprobar facilmente que $\eta_A = \mathrm{rad}(0)$).
- Dise que unha álxebra é *simple* se o seu único ideal propio é 0. Dise que unha álxebra é *semisimple* se a podemos expresar como produto cartesiano de álxebras simples.

Lema 4.17. *Sexan p un primo impar, K unha extensión finita de $\mathbb{Q}_p$ con anel de valoración $\mathcal{O}$ e A unha $\mathcal{O}$-álxebra de rango finito. O límite*

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

está definido para todo $x \in A$. De feito, este límite é un idempotente de A.

Demostración. Nótese que $\mathcal{O}$ é un anel local por ser un anel de valoración. Sexa pois $\mathfrak{p}$ o seu ideal maximal e sexa F o corpo residual $\mathcal{O}/\mathfrak{p}$. Polo Teorema Principal de Wedderburn, toda álxebra de dimensión finita sobre un corpo perfecto é igual á suma directa (como espazo vectorial) do seu nilradical e dunha álxebra semisimple. Posto que $A/\mathfrak{p}A$ sobre F é unha tal álxebra, sabemos que a imaxe de x en $A/\mathfrak{p}A$ pode escribirse como $s + n$, con n un elemento nilpotente e s semisimple. Se $n^a = 0$ entón

$$(s+n)^{ap} = s^{ap} + n^{ap} = s^{ap}$$

tamén é semisimple. Así, para un enteiro suficientemente grande b sabemos que $(s+n)^b$ é un elemento idempotente de $A/\mathfrak{p}A$. Sabendo que $(s+n)^{bp^m}$ é un idempotente de $A/\mathfrak{p}^m A$ para todo enteiro positivo m, deducimos que o límite do enunciado si existe e que, en efecto, é un idempotente. □

Posto que para todo enteiro $k>0$ $\mathcal{H}_k(p^r,\chi;\mathcal{O})$ e $\mathfrak{h}_k(p^r,\chi;\mathcal{O})$ son $\mathcal{O}$-álxebras de rango finito, a proposición anterior se pode aplicar ao caso do proxector ordinario, polo que este é un idempotente ben definido de ambas álxebras.

Definición 4.18. Sexan enteiros positivos k e r, un primo impar p, K unha extensión finita de $\mathbb{Q}_p$ con anel de valoración $\mathcal{O}$ e $\chi\colon (\mathbb{Z}/p^r\mathbb{Z})^\times \to \mathcal{O}^\times$ un carácter de Dirichlet. Dada $f\in \mathrm{M}_k(p^r,\chi;\mathcal{O})$, escribimos $ef=f|e$. Dirase que f é *ordinaria* se $f|e=f$. Nótese que, posto que e é idempotente, $f|e$ é unha forma ordinaria para toda $f\in \mathrm{M}_k(p^r,\chi;\mathcal{O})$.

Exemplo 4.19. Sexan enteiros positivos $k>2$ e r, un primo impar p, K unha extensión finita de $\mathbb{Q}_p$ con anel de valoración $\mathcal{O}$ e $\chi\colon (\mathbb{Z}/p^r\mathbb{Z})^\times \to \mathcal{O}^\times$ un carácter de Dirichlet. Imos considerar unha versión xeneralizada das series de Eisenstein dadas na sección 1.3 ás formas modulares p-ádicas. Definimos

$$E_{k,\chi}(z)=\frac{L(1-k,\chi)}{2}+\sum_{n=1}^{\infty}\sigma_{k-1,\chi}(n)q^n\in \mathrm{M}_k(p^r,\chi;\mathbb{Q}(\chi)),$$

$$G_{k,\chi}(z)=\sum_{n=1}^{\infty}\sigma'_{k-1,\chi}(n)q^n\in \mathrm{M}_k(p^r,\chi;\mathbb{Z}[\chi]),$$

onde

$$\sigma_{k-1,\chi}(n)=\sum_{d|n}\chi(d)d^{k-1},\qquad \sigma'_{k-1,\chi}(n)=\sum_{d|n}\chi(n/d)d^{k-1}$$

e $L(1-k,\chi)\in\mathbb{Q}(\chi)$ é o valor en $1-k$ da serie L de Dirichlet asociada ao carácter χ (para a definición desta serie e a comprobación de que $E_{k,\chi}$ e $G_{k,\chi}$ pertencen aos espazos de formas modulares indicados, véxase [7, §5.1]). Estas series coinciden coas xa coñecidas series de Eisenstein estudadas na sección 1.3 cando χ é un carácter trivial. Pódese consultar en [16, Teoremas 4.7.2 e 7.2.18] a proba de que, para todo enteiro $n>0$,

$$T_nE_{k,\chi}=a_n(E_{k,\chi})E_{k,\chi}\quad\text{e}\quad T_nG_{k,\chi}=a_n(G_{k,\chi})G_{k,\chi}.$$

En particular, as series de Eisenstein $E_{k,\chi}$ e $G_{k,\chi}$ son formas propias de Hecke.
Estudemos como actúa o proxector ordinario ao aplicarllo ás series de Eisenstein p-ádicas con carácter χ. En primeiro lugar, posto que $E_{k,\chi}$ é unha forma propia de T_p con autovalor $a_p(E_{k,\chi})=1$ (nótese que isto non sería certo se o módulo de χ non dividise a p),

$$E_{k,\chi}|e=\lim_{n\to\infty}T_p^{n!}E_{k,\chi}=\lim_{n\to\infty}a_p(E_{k,\chi})^{n!}E_{k,\chi}=E_{k,\chi},$$

co cal $E_{k,\chi}$ é unha forma ordinaria. Por outra banda, $T_p G_{k,\chi} = \sigma'_{k-1,\chi}(p) G_{k,\chi} = p^{k-1} G_{k,\chi}$, logo

$$G_{k,\chi}|e = \lim_{n\to\infty} \left(p^{k-1}\right)^{n!} G_{k,\chi} = 0,$$

e así $G_{k,\chi}$ non é unha forma ordinaria.

Deducimos deste estudo que se $f \in \mathrm{M}_k(p^r, \chi; \mathcal{O})$ é unha forma propia de T_p con autovalor α entón

$$f|e = \begin{cases} f & \text{se } |\alpha|_p = 1, \\ 0 & \text{se } |\alpha|_p < 1. \end{cases}$$

Así, ao estudar soamente as formas propias ordinarias estámonos restrinxindo a aquelas cuxo autovalor é unha unidade p-ádica.

Definición 4.20. Sexan enteiros positivos k e r, un primo impar p, K unha extensión finita de $\mathbb{Q}_p$ con anel de valoración $\mathcal{O}$ e $\chi\colon (\mathbb{Z}/p^r\mathbb{Z})^\times \to \mathcal{O}^\times$ un carácter de Dirichlet. Definimos o *espazo de formas modulares ordinarias*, o *espazo de formas cuspidais ordinarias* e as *álxebras de Hecke ordinarias* mediante, respectivamente,

$$\begin{aligned} \mathrm{M}_k^{\mathrm{ord}}(p^r, \chi; \mathcal{O}) &= \{f|e \mid f \in \mathrm{M}_k(p^r, \chi; \mathcal{O})\}, \\ \mathrm{S}_k^{\mathrm{ord}}(p^r, \chi; \mathcal{O}) &= \{f|e \mid f \in \mathrm{S}_k(p^r, \chi; \mathcal{O})\}, \\ \mathcal{H}_k^{\mathrm{ord}}(p^r, \chi; \mathcal{O}) &= \{Te \mid T \in \mathcal{H}_k(p^r, \chi; \mathcal{O})\}, \\ \mathfrak{h}_k^{\mathrm{ord}}(p^r, \chi; \mathcal{O}) &= \{Te \mid T \in \mathfrak{h}_k(p^r, \chi; \mathcal{O})\}. \end{aligned}$$

Vexamos para rematar a sección que o teorema de dualidade 4.14 se mantén cando nos restrinximos aos espazos ordinarios correspondentes.

Proposición 4.21. *Sexan enteiros positivos k e r, un primo impar p, K unha extensión finita de $\mathbb{Q}_p$ con anel de valoración $\mathcal{O}$ e $\chi\colon (\mathbb{Z}/p^r\mathbb{Z})^\times \to \mathcal{O}^\times$ un carácter de Dirichlet. Definindo*

$$M_{k,0}^{\mathrm{ord}}(p^r, \chi; \mathcal{O}) = \left\{ f \in \mathrm{M}_k^{\mathrm{ord}}(p^r, \chi; K) \mid a_n(f) \in \mathcal{O} \text{ para todo } n \geq 1 \right\},$$

temos os seguintes isomorfismos:

$$\begin{aligned} \mathrm{Hom}_{\mathcal{O}}\left(\mathcal{H}_k^{\mathrm{ord}}(p^r, \chi; \mathcal{O}), \mathcal{O}\right) &\cong \mathrm{M}_{k,0}^{\mathrm{ord}}(p^r, \chi; \mathcal{O}), \\ \mathrm{Hom}_{\mathcal{O}}\left(\mathfrak{h}_k^{\mathrm{ord}}(p^r, \chi; \mathcal{O}), \mathcal{O}\right) &\cong \mathrm{S}_k^{\mathrm{ord}}(p^r, \chi; \mathcal{O}), \\ \mathrm{Hom}_{\mathcal{O}}\left(\mathrm{M}_{k,0}^{\mathrm{ord}}(p^r, \chi; \mathcal{O}), \mathcal{O}\right) &\cong \mathcal{H}_k^{\mathrm{ord}}(p^r, \chi; \mathcal{O}), \\ \mathrm{Hom}_{\mathcal{O}}\left(\mathrm{S}_k^{\mathrm{ord}}(p^r, \chi; \mathcal{O}), \mathcal{O}\right) &\cong \mathfrak{h}_k^{\mathrm{ord}}(p^r, \chi; \mathcal{O}). \end{aligned}$$

Demostración. Imos probar unicamente os casos que involucran $\mathrm{M}_{k,0}^{\mathrm{ord}}(p^r, \chi; \mathcal{O})$, pois o mesmo argumento serve para demostrar os casos cuspidais. Recordemos que os isomorfismos do teorema 4.14 viñan inducidos polo emparellamento

$$\begin{array}{ccc} \mathcal{H}_k(p^r, \chi; \mathcal{O}) \times \mathrm{M}_{k,0}(p^r, \chi; \mathcal{O}) & \longrightarrow & \mathcal{O} \\ (T, f) & \longmapsto & a_1(Tf). \end{array}$$

Posto que

$$(T, f|e) = a_1(T(f|e)) = a_1(Tef) = (Te, f),$$

deducimos que os isomorfismos inducidos polo emparellamento se restrinxen aos espazos ordinarios. □

4.4. Rango dos espazos ordinarios

Nesta sección presentaremos un único resultado (para ver a demostración completa, véxase [10, Teorema 3.2.1]), que proporciona unha forte afirmación sobre o rango dos espazos de formas modulares ordinarias e das súas correspondentes álxebras de Hecke ordinarias. Este teorema será unha peza fundamental para poder interpolar os espazos das formas ordinarias en familias, como veremos no capítulo seguinte.

Definición 4.22. Sexa p un primo impar. Defínese o *carácter de Teichmüller* como o homomorfismo de grupos

$$\omega\colon (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \mathbb{Z}_p^\times$$

tal que, para cada $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, $\omega(a)$ é a única raíz da unidade en $\mathbb{Z}_p^\times$ congruente con a módulo p. Nótese que este carácter está ben definido, pois a ecuación

$$x^{p-1} \equiv 1 \,(\mathrm{mód}\, p)$$

ten como solucións $1, 2, \ldots, p-1$ polo pequeno teorema de Fermat, e polo lema de Hensel cada unha destas $p-1$ solucións pode levantarse a unha solución en $\mathbb{Z}_p$ congruente módulo p co número tomado inicialmente.

Nótese que o carácter de Teichmüller módulo p se pode estender a un endomorfismo de $\mathbb{Z}_p^\times$ mediante $\omega(a) = \omega(a \bmod p)$.

Teorema 4.23. *Sexan enteiros positivos $k \geq 2$ e r, un primo impar p, K unha extensión finita de $\mathbb{Q}_p$ con anel de valoración $\mathcal{O}$, $\chi\colon (\mathbb{Z}/p^r\mathbb{Z})^\times \to \mathcal{O}^\times$ un carácter de Dirichlet e*

$\omega\colon (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{Z}_p^\times$ *o carácter de Teichmüller. Tense que:*

$$\begin{aligned}\mathrm{Rang}_{\mathcal{O}}\left(\mathcal{H}_k^{\mathrm{ord}}\left(p^r,\chi\omega^{-k};\mathcal{O}\right)\right) &= \mathrm{Rang}_{\mathcal{O}}\left(\mathrm{M}_k^{\mathrm{ord}}\left(p^r,\chi\omega^{-k};\mathcal{O}\right)\right)\\ &= \mathrm{Rang}_{\mathcal{O}}\left(\mathrm{M}_2^{\mathrm{ord}}\left(p^r,\chi\omega^{-2};\mathcal{O}\right)\right),\\ \mathrm{Rang}_{\mathcal{O}}\left(\mathfrak{h}_k^{\mathrm{ord}}\left(p^r,\chi\omega^{-k};\mathcal{O}\right)\right) &= \mathrm{Rang}_{\mathcal{O}}\left(\mathrm{S}_k^{\mathrm{ord}}\left(p^r,\chi\omega^{-k};\mathcal{O}\right)\right)\\ &= \mathrm{Rang}_{\mathcal{O}}\left(\mathrm{S}_2^{\mathrm{ord}}\left(p^r,\chi\omega^{-2};\mathcal{O}\right)\right).\end{aligned}$$

Idea de demostración. Imos probar unicamente o primeiro caso, pois o caso das formas cuspidais pode demostrarse adaptando o argumento para as formas modulares. Antes de comezar, imos considerar $\psi\colon (\mathbb{Z}/p^r\mathbb{Z})^\times \to \mathcal{O}^\times$ un carácter adicional e $F = \mathcal{O}/(\pi)$ con $\pi \in \mathcal{O}$ algún elemento primo. Ademais, para axilizar a proba, imos escribir $\Gamma = \Gamma_0(p^r)$.

En primeiro lugar imos probar que

$$\mathrm{Rang}_{\mathcal{O}}\left(\mathcal{H}_k^{\mathrm{ord}}\left(\Gamma,\chi\omega^{-k};\mathcal{O}\right)\right) = \mathrm{Rang}_{\mathcal{O}}\left(\mathrm{M}_k^{\mathrm{ord}}\left(\Gamma,\chi\omega^{-k};\mathcal{O}\right)\right).$$

Posto que $\mathrm{M}_k\left(\Gamma,\chi\omega^{-k};\mathcal{O}\right)$ é un $\mathcal{O}$-módulo libre finitamente xerado, $\mathrm{M}_k^{\mathrm{ord}}\left(\Gamma,\chi\omega^{-k};\mathcal{O}\right)$ tamén o é, logo

$$\mathrm{Rang}_{\mathcal{O}}\left(\mathrm{M}_k^{\mathrm{ord}}\left(p^r,\chi\omega^{-k};\mathcal{O}\right)\right) \leq \mathrm{Rang}_{\mathcal{O}}\left(\mathrm{M}_{k,0}^{\mathrm{ord}}\left(p^r,\chi\omega^{-k};\mathcal{O}\right)\right).$$

Supoñamos agora que $\mathrm{Rang}_{\mathcal{O}}\left(\mathrm{M}_k^{\mathrm{ord}}\left(p^r,\chi\omega^{-k};\mathcal{O}\right)\right) = N$. Entón, para calquera conxunto $\{F_1,\dots,F_{N+1}\}$ contido en $\mathrm{M}_{k,0}^{\mathrm{ord}}\left(\Gamma,\chi\omega^{-k};\mathcal{O}\right)$, existe un elemento non nulo $\alpha \in \mathcal{O}$ tal que $\alpha F_i \in \mathrm{M}_k^{\mathrm{ord}}\left(p^r,\chi\omega^{-k};\mathcal{O}\right)$ para todo $1 \leq i \leq N+1$. Dedúcese entón que $\{\alpha F_1,\dots,\alpha F_{N+1}\}$ é un conxunto linearmente dependente sobre $\mathcal{O}$, do que se deduce que $\{F_1,\dots,F_{N+1}\}$ tamén o é. Así,

$$\mathrm{Rang}_{\mathcal{O}}\left(\mathrm{M}_k^{\mathrm{ord}}\left(p^r,\chi\omega^{-k};\mathcal{O}\right)\right) \geq \mathrm{Rang}_{\mathcal{O}}\left(\mathrm{M}_{k,0}^{\mathrm{ord}}\left(p^r,\chi\omega^{-k};\mathcal{O}\right)\right),$$

polo que

$$\mathrm{Rang}_{\mathcal{O}}\left(\mathrm{M}_k^{\mathrm{ord}}\left(p^r,\chi\omega^{-k};\mathcal{O}\right)\right) = \mathrm{Rang}_{\mathcal{O}}\left(\mathrm{M}_{k,0}^{\mathrm{ord}}\left(p^r,\chi\omega^{-k};\mathcal{O}\right)\right).$$

Posto que $\mathrm{M}_{k,0}^{\mathrm{ord}}\left(p^r,\chi\omega^{-k};\mathcal{O}\right)$ é un módulo libre de torsión e finitamente xerado sobre un dominio de ideais principais, entón deducimos que é libre, logo

$$\mathrm{Rang}_{\mathcal{O}}\left(\mathrm{M}_{k,0}^{\mathrm{ord}}\left(p^r,\chi\omega^{-k};\mathcal{O}\right)\right) = \mathrm{Rang}_{\mathcal{O}}\left(\mathrm{End}_{\mathcal{O}}\left(\mathrm{M}_{k,0}^{\mathrm{ord}}\left(p^r,\chi\omega^{-k};\mathcal{O}\right)\right)\right),$$

do que se conclúe que

$$\mathrm{Rang}_{\mathcal{O}}\left(\mathcal{H}_k^{\mathrm{ord}}\left(\Gamma,\chi\omega^{-k};\mathcal{O}\right)\right) = \mathrm{Rang}_{\mathcal{O}}\left(\mathrm{M}_k^{\mathrm{ord}}\left(\Gamma,\chi\omega^{-k};\mathcal{O}\right)\right).$$

A continuación, dado M un $\mathcal{O}[\Gamma_0(p)]$-módulo, imos considerar algúns feitos relativos aos grupos de cohomoloxía con coeficientes en M. Sexa Δ un subgrupo normal de $\Gamma_0(p)$

tal que Δ é libre de torsión e $[\Gamma_0(p)\colon \Delta]$ é coprimo con p. Para ver que tal grupo existe, nótese que por [7, §6.1] para todo enteiro $N \geq 4$ o subgrupo $\Gamma_1(N)$ é libre de torsión. Polo tanto, $\Delta = \Gamma_1(p)$ verifica as condicións antes impostas para todo primo $p > 3$. Para o caso $p = 3$ podemos tomar $\Delta = \Gamma_0(2) \cap \Gamma_0(3)$, que tamén satisfai as condicións posto que

$$\Gamma_0(3)/(\Gamma_0(2) \cap \Gamma_0(3)) \cong \mathbb{Z}/2\mathbb{Z}.$$

Nótese que $\Delta \cap \Gamma$ é un subgrupo normal de Γ con índice coprimo con p. Polo tanto, temos a composición de homomorfismos

$$H^i(\Gamma, M) \xrightarrow{\text{Res}} H^i(\Gamma \cap \Delta, M)^{\Gamma} \xrightarrow{\text{Cor}} H^i(\Gamma, M),$$

do que se deduce que $\text{Cor} \circ \text{Res} = [\Gamma\colon \Gamma \cap \Delta]$. Posto que $[\Gamma\colon \Gamma \cap \Delta]$ é coprimo con p,

$$H^i(\Gamma, M) \cong H^i(\Gamma \cap \Delta, M)^{\Gamma}.$$

Agora ben, por [7, Prop. 6.1.1], sabemos que $H^2(\Gamma \cap \Delta, M) = 0$, do que se deduce que $H^2(\Gamma, M) = 0$. Este feito será empregado máis adiante na demostración.

Sexa agora $\mathcal{O}\langle \Gamma, \lambda_p^{\iota} \rangle$ o anel semigrupo xerado por Γ e λ_p^{ι} sobre $\mathcal{O}$, onde

$$\lambda_p = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$$

e λ_p^{ι} denota a súa matriz adxunta. É dicir, $\mathcal{O}\langle \Gamma, \lambda_p^{\iota} \rangle$ é o conxunto de combinacións lineares finitas de elementos de Γ e de λ_p^{ι} sobre $\mathcal{O}$. Polo lema 4.17, pódese comprobar que e é un operador idempotente ben definido sobre a $\mathcal{O}$-subálxebra de $\text{End}_{\mathcal{O}}(H^i(\Gamma, M))$ xerada por T_p sobre $\mathcal{O}$. Denotamos $H^i(\Gamma, M)|e$ por $H^i_{\text{ord}}(\Gamma, M)$.

Consideremos agora para $n \geq 2$ a sucesión exacta curta de $\mathcal{O}\langle \Gamma, \lambda_p^{\iota} \rangle$-módulos

$$0 \longrightarrow L_n(\psi; \mathcal{O}) \xrightarrow{\pi} L_n(\psi; \mathcal{O}) \xrightarrow{\text{mód } \pi} L_n(\psi; F) \longrightarrow \mathcal{O}$$

onde, recordemos, $L_n(\psi; \mathcal{O})$ é o $\Gamma_0(N)$-submódulo de $\mathcal{O}[X, Y]$ formado polos polinomios homoxéneos de grao $n \geq 0$. Pódese ver que o proxector ordinario conmuta coas aplicacións π^*, $(\text{ mód } \pi)^*$ e o homomorfismo de conexión $d^1 = d$ introducido na sección 3.2. Xunto a algunhas consideracións cohomolóxicas sobre os grupos implicados a continuación, obtéñense as seguintes sucesións exactas:

$$H^0_{\text{ord}}(\Gamma, L_n(\psi; F)) \xrightarrow{d} H^1_{\text{ord}}(\Gamma, L_n(\psi; \mathcal{O}))[\pi^*] \longrightarrow 0,$$

$$0 \longrightarrow H^1_{\text{ord}}(\Gamma, L_n(\psi; \mathcal{O})) \otimes_{\mathcal{O}} F \xrightarrow{(\text{ mód } \pi)^*} H^1_{\text{ord}}(\Gamma, L_n(\psi; F)) \xrightarrow{d} d\left(H^1_{\text{ord}}(\Gamma, L_n(\psi; F))\right).$$

O seguinte paso é estudar cada unha delas de xeito individual. Da primeira dedúcese que $H^1_{\mathrm{ord}}(\Gamma, L_n(\psi;\mathcal{O}))$ é $\mathcal{O}$-libre. Por outra banda, posto que $H^2(\Gamma, L_n(\psi;\mathcal{O})) = 0$, da segunda sucesión exacta deducimos que

$$H^1(\Gamma, L_n(\psi;\mathcal{O})) \otimes_{\mathcal{O}} F \cong H^1(\Gamma, L_n(\psi;F)).$$

Isto implica que

$$H^1_{\mathrm{ord}}(\Gamma, L_n(\psi;\mathcal{O})) \otimes_{\mathcal{O}} F \cong H^1_{\mathrm{ord}}(\Gamma, L_n(\psi;F)),$$

co cal chegamos a

$$\mathrm{Rang}_{\mathcal{O}}\left(H^1_{\mathrm{ord}}(\Gamma, L_n(\psi;\mathcal{O}))\right) = \dim_F\left(H^1_{\mathrm{ord}}(\Gamma, L_n(\psi;F))\right).$$

Sexa agora a aplicación sobrexectiva $E\colon L_n(\psi;F) \to L_0\left(\psi\omega^n;F\right)$ dada por

$$E(P(X,Y)) = P(1,0).$$

Queremos ver que esta aplicación é un homomorfismo de $\mathcal{O}\langle\Gamma, \lambda_p^{\iota}\rangle$-módulos. Para isto, sexa $P(X,Y) \in L_n(\psi;F)$, con

$$P(X,Y) = \sum_{i=0}^{n} c_i XY^{n-i},$$

e sexa $\gamma \in \Gamma$ con

$$\gamma \equiv \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \ (\mathrm{m\acute{o}d}\, p^r).$$

Tense que

$$\begin{aligned} E(\gamma P(X,Y)) &= E\left(\chi(\gamma)P\left(\begin{pmatrix} X & Y \end{pmatrix}\left(\gamma^{-1}\right)^t\right)\right) \\ &= E(\chi(d)P(dX - bY, aY)) \\ &= c_n\chi(d)d^n = c_n\chi(d)\omega(d)^n = \chi(\gamma)\omega(\gamma)^n E(P(X,Y)). \end{aligned}$$

Argumentando de xeito semellante pódese probar que $E(\lambda_p^{\iota}P(X,Y)) = \lambda_p^{\iota}E(P(X,Y))$. Chegamos así á seguinte sucesión exacta de cohomoloxía:

$$H^1(\Gamma, \ker(E)) \longrightarrow H^1(\Gamma, L_n(\psi;F)) \xrightarrow{E^*} H^1(\Gamma, L_0(\psi\omega^n;F)) \xrightarrow{d} H^2(\Gamma, \ker(E)).$$

Posto que $\ker(E)$ é un $\mathcal{O}[\Gamma_0(p)]$-módulo, sabemos que $H^2(\Gamma, \ker(E)) = 0$. Polo visto anteriormente, se $u\colon \Gamma \to \ker(E)$ é un 1-cociclo (é dicir, un elemento do núcleo de d) entón para toda $\gamma \in \Gamma$ sabemos que cada termo de $u(\gamma) = P_\gamma(X,Y)$ é divisible por Y. Isto implica que

$$T_p u(\gamma) = \sum_{i=0}^{p-1} \begin{pmatrix} 1 & i \\ 0 & p \end{pmatrix}^{\iota} u(\gamma_i) = \sum_{i=0}^{p-1} P(X + iY, pY) \equiv 0 \ (\mathrm{m\acute{o}d}\, p).$$

Así, $T_pH^1(\Gamma, \ker(E)) = 0$, logo

$$H^1_{\mathrm{ord}}(\Gamma, L_n(\psi; F)) \cong H^1_{\mathrm{ord}}(\Gamma, L_0(\psi\omega^n; F)).$$

Impoñendo agora $n = k-2$ para $k \geq 2$ e $\psi = \chi\omega^{-k}$,

$$H^1_{\mathrm{ord}}\left(\Gamma, L_n\left(\chi\omega^{-k}; F\right)\right) \cong H^1_{\mathrm{ord}}\left(\Gamma, L_0\left(\chi\omega^{-2}; F\right)\right).$$

Finalmente, xuntando todo o visto ata agora e empregando o teorema 3.22:

$$\begin{aligned}
2\mathrm{Rang}_{\mathcal{O}}\left(\mathrm{M}_k^{\mathrm{ord}}\left(\Gamma, \chi\omega^{-k}; \mathcal{O}\right)\right) - 1 &= \mathrm{Rang}_{\mathcal{O}}\left(\mathrm{M}_k^{\mathrm{ord}}\left(\Gamma, \chi\omega^{-k}; \mathcal{O}\right)\right) \\
&+ \mathrm{Rang}_{\mathcal{O}}\left(\mathrm{S}_k^{\mathrm{ord}}\left(\Gamma, \chi\omega^{-k}; \mathcal{O}\right)\right) \\
&= \mathrm{Rang}_{\mathcal{O}}\left(H^1_{\mathrm{ord}}\left(\Gamma, L_k\left(\chi\omega^{-k}; \mathcal{O}\right)\right)\right) \\
&= \dim_F\left(H^1_{\mathrm{ord}}\left(\Gamma, L_k\left(\chi\omega^{-k}; F\right)\right)\right) \\
&= \dim_F\left(H^1_{\mathrm{ord}}\left(\Gamma, L_0\left(\chi\omega^{-2}; \mathcal{O}\right)\right)\right) \\
&= \mathrm{Rang}_{\mathcal{O}}\left(H^1_{\mathrm{ord}}\left(\Gamma, L_0\left(\chi\omega^{-2}; \mathcal{O}\right)\right)\right) \\
&= \mathrm{Rang}_{\mathcal{O}}\left(\mathrm{M}_2^{\mathrm{ord}}\left(\Gamma, \chi\omega^{-2}; \mathcal{O}\right)\right) \\
&+ \mathrm{Rang}_{\mathcal{O}}\left(\mathrm{S}_2^{\mathrm{ord}}\left(\Gamma, \chi\omega^{-2}; \mathcal{O}\right)\right) \\
&= 2\mathrm{Rang}_{\mathcal{O}}\left(\mathrm{M}_2^{\mathrm{ord}}\left(\Gamma, \chi\omega^{-2}; \mathcal{O}\right)\right) - 1.
\end{aligned}$$

Concluímos entón que o rango de $\mathrm{M}_k\left(p^r, \chi\omega^{-k}; \mathcal{O}\right)$ sobre $\mathcal{O}$ non depende do peso k. □

Capítulo 5

Familias de Hida

Neste capítulo desenvolveremos a denominada teoría de Hida, a cal consiste en agrupar as formas modulares p-ádicas estudadas nos capítulos anteriores en series de potencias con polinomios nunha variable como coeficientes. Estas series serán as denominadas familias de Hida, e poderemos entendelas como coleccións de formas modulares indexadas polos seus pesos. Ademais, estudaremos as propiedades dos espazos formados por estas familias e xeneralizaremos os operadores de Hecke e as súas álxebras para empregalos tamén no estudo da teoría de Hida.

5.1. Definicións iniciais

Nesta primeira sección construiremos as familias de Hida e os espazos que conforman. Tamén veremos algunha propiedade sinxela destas novas construcións que será relevante nas seccións seguintes.

Para comezar, será necesario estudar algunhas propiedades dos caracteres de Dirichlet.

Definición 5.1. Sexa p un primo impar. Dado un carácter de Dirichlet módulo $N \geq 1$, defínese o seu *condutor* como o menor enteiro positivo f_χ tal que $\chi(m) = \chi(n)$ para todo par de enteiros m e n coprimos con N e tales que $m \equiv n \,(\text{mód } f_\chi)$. Ademais, dicimos que:

- χ é un *carácter da primeira especie con respecto a* p se $f_\chi = Mp$ ou $f_\chi = M$ para algún enteiro positivo M coprimo con p.
- χ é un *carácter da segunda especie con respecto a* p se $f_\chi = p^{n+1}$ para algún enteiro $n \geq 1$.

Vexamos algún carácter de Dirichlet que ilustre as definicións anteriores:

Exemplo 5.2.

- O carácter de Dirichlet $\chi\colon (\mathbb{Z}/3\mathbb{Z})^\times \to \mathbb{C}^\times$ definido mediante

$$\chi(1) = 1 \quad \text{e} \quad \chi(2) = -1,$$

é da primeira especie con respecto a 5, pois $f_\chi = 3$ (de feito, o condutor do carácter coincide co seu módulo, situación na que se di que o carácter é *primitivo*).

- O carácter de Dirichlet $\chi\colon (\mathbb{Z}/5\mathbb{Z})^\times \to \mathbb{C}^\times$ definido mediante

$$\chi(1) = 1, \quad \chi(2) = -1, \quad \chi(3) = -1, \quad \chi(4) = 1,$$

é da primeira especie con respecto a 3, pois $f_\chi = 3$. Se en cambio agora consideramos $\psi\colon (\mathbb{Z}/10\mathbb{Z})^\times \to \mathbb{C}^\times$ o carácter tal que

$$\psi(1) = 1, \quad \psi(3) = -1, \quad \psi(7) = -1, \quad \psi(9) = 1,$$

temos un carácter non primitivo, pois este provén do carácter χ anterior.

- O carácter de Dirichlet $\chi\colon (\mathbb{Z}/9\mathbb{Z})^\times \to \mathbb{C}^\times$ definido mediante

$$\chi(1) = 1, \quad \chi(2) = \xi, \quad \chi(4) = \xi^2, \quad \chi(5) = -\xi^2, \quad \chi(7) = -\xi, \quad \chi(8) = -1,$$

onde ξ é unha raíz terceira da unidade, é da segunda especie con respecto a 3, pois $f_\chi = 9$.

Consideremos un primo impar p e un carácter de Dirichlet $\chi\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ para un certo $N \geq 1$. Posto que $(\mathbb{Z}/2\mathbb{Z})^\times = 1$, sabemos que ou ben $(f_\chi, p) = 1$ ou ben $p \mid f_\chi$, e polo tanto

$$f_\chi = M \quad \text{e} \quad f_\chi = Mp^r,$$

onde M é un enteiro positivo coprimo con p e $r \geq 1$. Agora, grazas ao isomorfismo dado polo teorema chinés dos restos,

$$\begin{array}{ccc} (\mathbb{Z}/Mp^r\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/Mp\mathbb{Z})^\times \times (1+p\mathbb{Z}_p)/(1+p^r\mathbb{Z}) \\ \alpha \bmod Mp^r & \longmapsto & (\alpha \bmod Mp,\, \alpha \bmod (1+p^r\mathbb{Z}_p)), \end{array}$$

deducimos que $\chi = \chi_F\chi_S$, onde

$$\chi_F\colon (\mathbb{Z}/Mp\mathbb{Z})^\times \longrightarrow \overline{\mathbb{Q}}^\times \quad \text{e} \quad \chi_S\colon (1+p\mathbb{Z}_p)/(1+p^r\mathbb{Z}) \longrightarrow \overline{\mathbb{Q}}^\times$$

son caracteres de Dirichlet da primeira e da segunda especie con respecto a p, respectivamente. Polo tanto, podemos expresar todo carácter de Dirichlet como o produto dun

carácter da primeira especie e dun carácter da segunda. A utilidade desta descomposición, que veremos conforme avancemos no capítulo, reside no feito de que, dado un carácter $\chi\colon (\mathbb{Z}/p^r\mathbb{Z})^\times \to \mathbb{C}^\times$, a imaxe de χ_F reside en $\mathbb{Z}_p$, mentres que a de χ_S ten a orde dunha potencia de p.

Notación 5.3. De agora en adiante, fixado un primo impar p denotaremos a *álxebra de Iwasawa* $\mathbb{Z}_p[\![X]\!]$ por Λ e escribiremos $u = 1 + p$.

Definición 5.4. Sexan p un primo impar e enteiros $N \geq 1$, $k \geq 2$ e $r \geq 1$. Para cada carácter de Dirichlet $\chi\colon (\mathbb{Z}/Np^r\mathbb{Z})^\times \to \mathbb{C}^\times$, definimos a *aplicación de especialización en k e χ* como $\nu_{k,\chi}\colon \Lambda \to \overline{\mathbb{Q}}_p$ inducida por $X \mapsto \zeta_\chi u^k - 1$, onde $\zeta_\chi = \chi_S(u)$.

Proposición 5.5. *Sexan p un primo impar, enteiros $N \geq 1$, $k \geq 2$ e $r \geq 1$ e un carácter de Dirichlet $\chi\colon (\mathbb{Z}/Np^r\mathbb{Z})^\times \to \mathbb{C}^\times$. A aplicación de especialización $\nu_{k,\chi}$ está ben definida.*

Demostración. Temos que comprobar que cando avaliamos un elemento de Λ en $\zeta_\chi u^k - 1$ obtemos un elemento de $\overline{\mathbb{Q}}_p$. Sexa $(\pi) = \mathfrak{p}$ o ideal primo de $\mathcal{O}$, con $\mathcal{O}$ o anel de valoración dunha extensión finita K de $\mathbb{Q}_p$. Posto que $\zeta_\chi \in \mathcal{O}$,

$$\zeta_\chi = \sum_{n=0}^{\infty} c_n \pi^n,$$

onde os c_n son elementos dun sistema de representantes do corpo residual $\mathcal{O}/\mathfrak{p}$. Agora, como $\mathcal{O}/\mathfrak{p}$ é isomorfo a unha extensión finita do corpo finito $\mathbb{F}_p$, sabemos que todo elemento de $\mathcal{O}/\mathfrak{p}$ ten orde coprima con p. Así, o feito de que ζ_χ sexa unha potencia de p raíz da unidade implica que $c_0 = 1$. Como $u^k \equiv 1 \,(\mathrm{mód}\, p)$, sabemos que $\left|\zeta_\chi u^k - 1\right|_p < 1$ para todo enteiro $k \geq 2$. Concluímos entón que a avaliación dun elemento de Λ en $\zeta_\chi u^k - 1$ dá lugar a unha serie de potencias en $\mathcal{O}$ que converxe de xeito p-ádico. □

Precisamos entender un último obxecto antes de definir as familias de Hida. Nas mesmas hipóteses que antes, nótese que Λ non contén ningún divisor de cero, logo o núcleo da aplicación de especialización $\nu_{k,\chi}$ é un ideal primo de Λ. Podemos entón pensar nesta aplicación como un mergullo de $\Lambda/\ker(\nu_{k,\chi})$ en $\overline{\mathbb{Q}}_p$. Sexa I unha Λ-álxebra finitamente xerada e enteira sobre Λ (isto é, unha Λ-álxebra cuxos elementos son raíces de algún polinomio mónico con coeficientes en Λ). Grazas a [23, Teorema VIII.6.15 e p. 264], sabemos que I é un anel local, completo e noetheriano con dimensión de Krull 2. O noso obxectivo agora é estender $\nu_{k,\chi}$ a I. Posto que I é enteiro sobre Λ, existe un ideal primo P de I tal que $P \cap \Lambda = \ker(\nu_{k,\chi})$, e isto á súa vez implica que I/P é unha extensión de $\Lambda/\ker(\nu_{k,\chi})$. De feito, como I é un Λ-módulo finitamente xerado sabemos que I/P é unha extensión finita de $\Lambda/\ker(\nu_{k,\chi})$. Podemos entón, grazas á aplicación de especialización, identificar

$\Lambda/\ker(\nu_{k,\chi})$ con $\mathcal{O}$ e I/P cunha extensión finita de $\mathcal{O}$. Deste xeito obtemos unha aplicación de especialización $\nu\colon I/P \to \overline{\mathbb{Q}}_p$ que estende $\nu_{k,\chi}$, pero esta depende da escolla de P.

Definición 5.6. Sexan p un primo impar, enteiros $N \geq 1$, $k \geq 2$ e $r \geq 1$, K unha extensión finita de $\mathbb{Q}_p$ con anel de valoración $\mathcal{O}$, $\chi\colon (\mathbb{Z}/Np^r\mathbb{Z})^\times \to \mathbb{C}^\times$ un carácter de Dirichlet e I unha Λ-álxebra finitamente xerada enteira sobre Λ. Imos denotar por $\mathcal{A}_k(\chi, I)$ o conxunto de homomorfismos de $\mathcal{O}$-álxebras de I a $\overline{\mathbb{Q}}_p$ que inducen a aplicación de especialización $\nu_{k,\chi}$ en Λ. Definimos tamén o conxunto

$$\mathcal{A}(\chi, I) = \bigcup_{k=1}^{\infty} \mathcal{A}_k(\chi, I),$$

cuxos elementos denominamos *puntos aritméticos* de $\mathrm{Hom}_{\mathcal{O}}(I, \overline{\mathbb{Q}}_p)$.

Finalmente, estamos en condicións de definir o obxecto de estudo principal do capítulo.

Definición 5.7. Sexa p un primo impar, enteiros $r \geq 1$ e $N \geq 1$ coprimo con p, $\mathcal{K}$ unha extensión finita do corpo cociente de Λ, I a clausura íntegra de Λ en $\mathcal{K}$, $\chi\colon (\mathbb{Z}/Np^r\mathbb{Z})^\times \to \overline{\mathbb{Q}}^\times$ un carácter de Dirichlet e $\omega\colon (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{Z}_p^\times$ o carácter de Teichmüller. Unha *forma modular Λ-ádica* de carácter χ e nivel Np^r (ou simplemente unha *familia de Hida* de carácter χ e nivel Np^r) é unha expansión en serie

$$\boldsymbol{f}(X) = \sum_{n=0}^{\infty} a_n(\boldsymbol{f})(X) q^n \in I[\![q]\!]$$

tal que, para todo enteiro $k \geq 2$ salvo para unha cantidade finita dos mesmos e para toda $\nu \in \mathcal{A}_k(\chi, I)$,

$$\nu(\boldsymbol{f}) = \sum_{n=0}^{\infty} \nu(a_n(\boldsymbol{f})(X)) q^n \in \mathrm{M}_k\left(Np^r, \chi\omega^{-k}; \overline{\mathbb{Q}}_p\right).$$

Nas mesmas condicións, se $\nu(\boldsymbol{f}) \in \mathrm{S}_k\left(Np^r, \chi\omega^{-k}; \overline{\mathbb{Q}}_p\right)$ dise que $\boldsymbol{f}$ é unha *forma cuspidal Λ-ádica* de carácter χ e nivel Np^r.
De xeito semellante, se $\nu(\boldsymbol{f}) \in \mathrm{M}_k^{\mathrm{ord}}\left(Np^r, \chi\omega^{-k}; \overline{\mathbb{Q}}_p\right)$ ou $\nu(\boldsymbol{f}) \in \mathrm{S}_k^{\mathrm{ord}}\left(Np^r, \chi\omega^{-k}; \overline{\mathbb{Q}}_p\right)$ dise que $\boldsymbol{f}$ é unha *forma Λ-ádica ordinaria* ou unha *forma Λ-ádica cuspidal ordinaria*, respectivamente.

En realidade sería máis preciso referirnos ás formas modulares Λ-ádicas como I-ádicas, onde I é a Λ-álxebra finitamente xerada na que residen os seus coeficientes, polo que adoptaremos esta terminoloxía durante o resto do capítulo.

Definición 5.8. Sexa p un primo impar, χ un carácter de Dirichlet como na definición anterior e I unha Λ-álxebra finitamente xerada. Denotamos os *I-módulos de formas modulares, cuspidais, ordinarias e cuspidais ordinarias I-ádicas* de carácter χ por $\mathrm{M}(\chi; I)$,

$\mathrm{S}(\chi;I)$, $\mathrm{M}^{\mathrm{ord}}(\chi;I)$ e $\mathrm{S}^{\mathrm{ord}}(\chi;I)$, respectivamente. Ademais, para cada I-álxebra A contendo a $\mathbb{Z}[\chi][\![X]\!]$, definimos os *espazos de formas modulares, cuspidais, ordinarias ou cuspidais ordinarias I-ádicas* con coeficientes en A mediante:

$$\begin{aligned}\mathrm{M}(\chi;A) &= \mathrm{M}(\chi;I)\otimes_I A,\\ \mathrm{S}(\chi;A) &= \mathrm{S}(\chi;I)\otimes_I A,\\ \mathrm{M}^{\mathrm{ord}}(\chi;A) &= \mathrm{M}^{\mathrm{ord}}(\chi;I)\otimes_I A,\\ \mathrm{S}^{\mathrm{ord}}(\chi;A) &= \mathrm{S}^{\mathrm{ord}}(\chi;I)\otimes_I A.\end{aligned}$$

Observación 5.9. Nótese que a definición anterior coincide coa definición 5.7 se tomamos $I=\Lambda$ e a I-álxebra A como a clausura íntegra dunha extensión finita do corpo cociente de Λ.

Para finalizar esta sección, nótese que aplicación de especialización $\nu_{k,\chi}\colon \Lambda \to \overline{\mathbb{Q}}_p$ foi escollida porque fai referencia ao peso da forma modular p-ádica na que especializa as familias de Hida. Porén, $\nu_{k,\chi}$ non é a única aplicación de especialización que se pode escoller, de feito existen traballos nos que se emprega como aplicación de especialización $X \mapsto \zeta_\chi u^{k-2}-1$. O seguinte lema, cuxa proba se pode consultar en [10, Prop. 4.1.1], permite deducir que todas estas especializacións son equivalentes.

Lema 5.10. *Sexa $\mathcal{O}$ o anel de valoración dunha extensión finita de $\mathbb{Q}_p$, con p un primo impar. Dados $\alpha,\beta\in\mathcal{O}$ tales que $|\alpha|_p=1$ e $|\beta|_p<1$, a aplicación inducida por $X\mapsto \alpha X+\beta$ é un automorfismo do anel $\mathcal{O}[\![X]\!]$.*

Empregando o lema, podemos trocar a aplicación de especialización $\nu_{k,\chi}$ por $\nu_{l,\chi}$ para calquera enteiro $l\neq 0$ mediante o automorfismo de Λ inducido por

$$X \mapsto u^{k-l}X - \left(u^{k-l}-1\right).$$

5.2. A familia de Hida das series de Eisenstein

Esta sección amosará a existencia e o sentido de considerar un obxecto tan peculiar como son as familias de Hida mediante a construción dunha forma modular Λ-ádica que parametrice a familia das series de Eisenstein. Ademais, centraremos a nosa atención en formas de nivel p^r, pois todo o descrito a continuación pode ser adaptado de xeito sinxelo ao caso de nivel Np^r.

Antes de comezar será conveniente introducir a exponenciación e o logaritmo p-ádicos, o cal facemos a continuación seguindo [9]:

Definición 5.11. Sexa p un primo impar. Definimos a *exponencial p-ádica* de $x \in p\mathbb{Z}_p$ e o seu *logaritmo p-ádico* mediante, respectivamente,

$$e^x = \exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!} \quad \text{e} \quad \log(1+x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n}.$$

Tense que $\exp(\log(1+x)) = 1+x$ para $x \in p\mathbb{Z}_p$. Dado b un enteiro positivo, definimos tamén

$$b^x = \exp(x \log b).$$

Proposición 5.12. *Sexa p un primo impar, un enteiro $r \geq 1$, $\omega\colon (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{Z}_p^\times$ o carácter de Teichmüller e $\chi\colon (\mathbb{Z}/p^r\mathbb{Z})^\times \to \overline{\mathbb{Q}}^\times$ un carácter de Dirichlet. Consideremos a serie de Eisenstein normalizada $E_{k,\chi\omega^{-k}} \in \mathrm{M}_k\left(p^r, \chi\omega^{-k}; \mathbb{Q}\left(\chi\omega^{-k}\right)\right)$ para cada $k > 2$ introducida no exemplo 4.19:*

$$E_{k,\chi\omega^{-k}} = \frac{L\left(1-k, \chi\omega^{-k}\right)}{2} + \sum_{n=1}^{\infty} \sigma_{k-1,\chi\omega^{-k}}(n) q^n.$$

Existe unha forma modular Λ-ádica $\mathcal{E}_\chi(X)$ tal que, para cada enteiro $k > 2$,

$$\mathcal{E}_\chi\left(\zeta_\chi u^k - 1\right) = E_{k,\chi\omega^{-k}}.$$

Demostración. Para simplificar a notación durante a proba, escribiremos $\psi_k := \chi\omega^{-k}$. Agora, para cada enteiro $n > 0$ temos que construír unha serie de potencias $a_n(\mathcal{E}_\chi)(X) \in \Lambda$ tal que

$$a_n(\mathcal{E}_\chi)\left(\zeta_\chi u^k - 1\right) = \sum_{\substack{d|n \\ (d,p)=1}} \psi_k(d) d^{k-1}$$

para todo enteiro $k > 2$. Pódese consultar en [6, pp. 123 e 124] que, para todo $s \in \mathbb{Z}_p$,

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

onde

$$\binom{s}{n} = \frac{s(s-1)\ldots(s-n+1)}{n!}.$$

Por outra banda, podemos considerar a aplicación

$$\begin{array}{rccc} \varphi\colon & \mathbb{Z}_p & \longrightarrow & 1+p\mathbb{Z}_p \\ & s & \longmapsto & u^s, \end{array}$$

que é claramente un homomorfismo de grupos posto que $u^{s+t} = u^s u^t$. De feito, pódese probar que esta aplicación é un isomorfismo comprobando que o seu homomorfismo inverso é

$$s \mapsto \frac{\log(s)}{\log(u)}.$$

Polo tanto, para todo $s \in 1 + p\mathbb{Z}_p$,

$$s = u^{\varphi^{-1}(s)}.$$

Tendo isto en mente, dado calquera enteiro $n > 0$ e un divisor d de n tal que $d \equiv 1 \pmod{p}$, definimos

$$A_d(X) = \frac{1}{d}(1+X)^{\varphi^{-1}(d)}.$$

Agora, como $(d,p) = 1$ e $\varphi^{-1}(d) \in \mathbb{Z}_p$, deducimos que $A_d(X) \in \Lambda$. Ademais, tendo en conta que $\omega(d) = 1$ (pois tomamos d congruente con 1 módulo p),

$$\begin{aligned} A_d\left(\zeta_\chi u^k - 1\right) &= \frac{1}{d}\left(1 + \left(\zeta_\chi u^k - 1\right)\right)^{\varphi^{-1}(d)} \\ &= \frac{1}{d}\left(\zeta_\chi u^k\right)^{\varphi^{-1}(d)} \\ &= \chi_S(u)^{\varphi^{-1}(d)}\left(u^{\varphi^{-1}(d)}\right)^k d^{-1} \\ &= \chi_S(d)d^{k-1} = \omega(d)^{-k}\chi_S(d)d^{k-1}. \end{aligned}$$

Así, dado un enteiro positivo n, se todos os seus divisores d tales que $(d,p) = 1$ satisfán $d \equiv 1 \,(\mathrm{mód}\, p)$ entón

$$\sum_{\substack{d|n \\ (d,p)=1}} \chi_F(d) A_d\left(\zeta_\chi u^k - 1\right) = \sum_{\substack{d|n \\ (d,p)=1}} \chi_F(d)\chi_S(d)\omega(d)^{-k}d^{k-1} = \sum_{\substack{d|n \\ (d,p)=1}} \psi_k(d)d^{k-1},$$

que é precisamente o resultado que buscamos. De feito, posto que

$$\sum_{\substack{d|n \\ (d,p)=1}} \chi_F(d) A_d(X) \in \Lambda,$$

o único que resta por resolver é o problema dos enteiros n que posúen divisores d coprimos con p tales que $d \not\equiv 1 \pmod{p}$. Para tratar isto, notemos que o carácter ω se pode estender a todo elemento de $\mathbb{Z}_p^\times$ mediante $\omega(\alpha) = \omega(\alpha \bmod p)$. Agora, sabendo que a aplicación

$$\begin{array}{rcl} \mathbb{Z}_p^\times & \longrightarrow & (1+p\mathbb{Z}_p) \times (\mathbb{Z}/p\mathbb{Z})^\times \\ \alpha & \longmapsto & \left(\omega(\alpha)^{-1}\alpha, \alpha \bmod p\right) \end{array}$$

é un isomorfismo multiplicativo de grupos (véxase [22, p. 118]), podemos considerar a primeira proxección que induce,

$$\begin{array}{rccl} \pi\colon & \mathbb{Z}_p^\times & \longmapsto & 1 + p\mathbb{Z}_p \\ & \alpha & \longmapsto & \pi(\alpha) = \omega(\alpha)^{-1}\alpha, \end{array}$$

para así deducir que, para todo enteiro d coprimo con p, $\pi(d) \equiv 1 \,(\mathrm{mód}\, p)$. Polo tanto, definimos

$$a_n(\mathcal{E}_\chi)(X) = \sum_{\substack{d|n \\ (d,p)=1}} \frac{\chi_F(d)}{d}(1+X)^{\varphi^{-1}(\pi(d))} \in \Lambda$$

e concluímos, empregando o feito de que χ_S leva $\omega(d)^{-1}$ en 1 (pois χ_S é un carácter de orde unha potencia de p),

$$\begin{aligned} a_n(\mathcal{E}_\chi)\left(\zeta_\chi u^k - 1\right) &= \sum_{\substack{d|n \\ (d,p)=1}} \frac{\chi_F(d)}{d}\left(\zeta_\chi u^k\right)^{\varphi^{-1}(\pi(d))} \\ &= \sum_{\substack{d|n \\ (d,p)=1}} \frac{\chi_F(d)}{d}\chi_S\left(\omega(d)^{-1}d\right)\left(\omega(d)^{-1}d\right)^k \\ &= \sum_{\substack{d|n \\ (d,p)=1}} \frac{\chi_F(d)}{d}\chi_S(d)\omega(d)^{-k}d^k = \sum_{\substack{d|n \\ (d,p)=1}} \psi_k(d)d^{k-1}. \end{aligned}$$

Para finalizar, debemos achar unha serie de potencias $a_0(\mathcal{E}_\chi)(X) \in \Lambda$ tal que

$$a_0(\mathcal{E}_\chi)\left(\zeta_\chi u^k - 1\right) = \frac{L(1-k,\psi_k)}{2}$$

para todo enteiro $k > 2$. Empregando [22, Teorema 5.11] deducimos que, para todo $k \geq 1$,

$$L(1-k,\psi_k) = \left(1 - \chi\omega^{-k}(p)p^{k-1}\right)L(1-k,\psi_k) = L_p(1-k,\chi),$$

onde $L_p(s,\chi)$ é unha función L p-ádica meromorfa (analítica se $\chi \neq 1$) en

$$\left\{s \in \mathbb{C}_p \mid |s| < p^{(p-2)/(p-1)}\right\}.$$

Aínda máis, empregando [22, Teorema 7.10] sabemos que existe $F_\chi(X) \in \Lambda$ tal que

$$L_p(s,\chi) = F_\chi\left(\zeta_\chi u^s - 1\right).$$

Polo lema 5.10, a aplicación $X \mapsto u^{1-2k}X + \left(u^{1-2k} - 1\right)$ induce un automorfismo do anel Λ. Se H denota a imaxe de F_χ por dito isomorfismo, entón

$$H\left(\zeta_\chi u^k - 1\right) = F_\chi\left(u^{1-2k}\left(\zeta_\chi u^k - 1\right) + \left(u^{1-2k} - 1\right)\right) = F_\chi\left(\zeta_\chi u^{1-k} - 1\right) = L_p(1-k,\chi),$$

co cal basta tomar $a_0(\mathcal{E}_\chi)(X) = H(X)/2 \in \Lambda$. □

Observación 5.13. A serie de potencias $F_\chi(X)$ da demostración anterior é en realidade o cociente de dúas series, $G_\chi(X), H_\chi(X) \in \Lambda$, con $H_1(X) = X$, $H_\chi(X) = 1$ para $\chi \neq 1$ e

$X \nmid G_1(X)$. Polo tanto, se $\chi = 1$ na proposición anterior entón $\mathcal{E}_1(X)$ segue interpolando a serie de Eisenstein como desexamos, mais $\mathcal{E}_1(X) \notin \Lambda[\![q]\!]$ posto que

$$a_0(\mathcal{E}_1)(X) = F_1\left(u^{1-2k}X + \left(u^{1-2k} - 1\right)\right) = \frac{G_1\left(u^{1-2k}X + \left(u^{1-2k} - 1\right)\right)}{u^{1-2k}X + (u^{1-2k} - 1)} \notin \Lambda.$$

A pesares disto, a familia de Hida $\mathcal{E}_1(X)$ será de gran utilidade na sección 5.4, na que a empregaremos para construír formas modulares Λ-ádicas que se especialicen en formas modulares p-ádicas fixadas.

Observación 5.14. A función L p-ádica $L_p(1-k, \chi)$ empregada durante a proba da proposición 5.12 é a denominada *función L p-ádica de Kubota–Leopoldt.*

Agora que conseguimos construír unha familia de Hida que parametriza as series de Eisenstein $E_{k,\chi\omega^{-k}}$, gustaríanos facer o mesmo coas series $G_{k,\chi\omega^{-k}}$. A construción desta nova familia será semellante á xa feita, pero a incluiremos a continuación por completitude. Recordemos que

$$G_{k,\chi\omega^{-k}}(z) = \sum_{n=1}^{\infty} \sigma'_{k-1,\chi\omega^{-k}}(n)q^n$$

para todo enteiro $k > 2$. Recuperando toda a notación incluída na proba da proposición 5.12, para cada $n > 1$ podemos considerar a serie de potencias

$$B_n(X) = \sum_{d|n} \frac{d^{2k-1}\chi_F(n/d)}{n^k}(X+1)^{\varphi^{-1}(\pi(n/d))} \in \Lambda,$$

posto que todo factor de n divisible por p resulta cancelado ou ben polo d^{2k-1} do numerador ou ben por $\chi_F(n/d) = 0$. Se agora calculamos a especialización correspondente:

$$\begin{aligned} B_n\left(\zeta_\chi u^k - 1\right) &= \sum_{d|n} \frac{d^{2k-1}\chi_F(n/d)}{n^k}\left(\zeta_\chi u^k\right)^{\varphi^{-1}(\pi(n/d))} \\ &= \sum_{d|n} \frac{d^{2k-1}\chi_F(n/d)}{n^k}\chi_S\left(\omega(n/d)^{-1}(n/d)\right)\left(\omega(n/d)^{-1}(n/d)\right)^k \\ &= \sum_{d|n} d^{k-1}\chi\omega^{-k}(n/d) = a_n\left(G_{k,\chi\omega^{-k}}\right). \end{aligned}$$

Así pois, definimos a familia de Hida

$$\mathcal{G}_\chi(X) = \sum_{n=1}^{\infty} B_n(X)q^n$$

e observamos que, en efecto, $\mathcal{G}_\chi\left(\zeta_\chi u^k - 1\right) = G_{k,\chi}$ para todo $k > 2$.

5.3. Operadores de Hecke e o proxector ordinario para familias de Hida

O obxectivo desta sección é, unha vez máis, xeneralizar o concepto dos operadores de Hecke, neste caso aos espazos das formas Λ-ádicas. Tamén xeneralizaremos o xa estudado proxector ordinario ao contexto destas novas formas.

Sexan p un primo impar, un enteiro $r \geq 1$ e $\chi\colon (\mathbb{Z}/p^r\mathbb{Z})^\times \to \mathbb{C}^\times$ un carácter de Dirichlet e ω o carácter de Teichmüller módulo p. O noso primeiro obxectivo será construír os operadores de Hecke T_n para cada $n > 0$ de xeito que conmuten coa aplicación de especialización $\nu_{k,\chi}$. Isto é, queremos definilos de xeito que

$$T_n \boldsymbol{f}\left(\zeta_\chi u^k - 1\right) = T_n\left(\boldsymbol{f}\left(\zeta_\chi u^k - 1\right)\right)$$

para toda $\boldsymbol{f} \in \mathrm{M}(\chi;\Lambda)$ e para todo enteiro $k > 1$ tal que $\boldsymbol{f}\left(\zeta_\chi u^k - 1\right) \in \mathrm{M}_k\left(p^r, \chi\omega^{-k}; \overline{\mathbb{Q}}_p\right)$. Para isto será importante recordar que, dados enteiros $m > 0$ e $n \geq 0$ e $\mathrm{M}_k\left(p^r, \chi\omega^{-k}; \overline{\mathbb{Q}}_p\right)$:

$$a_n(T_m f) = \sum_{d|(m,n)} \chi\omega^{-k}(d) d^{k-1} a_{\frac{mn}{d^2}}(f) = \sum_{\substack{d|(m,n)\\(d,p)=1}} \chi\omega^{-k}(d) d^{k-1} a_{\frac{mn}{d^2}}(f).$$

Definición 5.15. Sexan p un primo impar, enteiros $r \geq 1$ e $m > 0$, $\chi\colon (\mathbb{Z}/p^r\mathbb{Z})^\times \to \mathbb{C}^\times$ un carácter de Dirichlet e ω o carácter de Teichmüller módulo p. Defínese o m-ésimo *operador de Hecke* T_m para formas modulares Λ-ádicas como a aplicación que a cada $\boldsymbol{f} \in \mathrm{M}(\chi;\Lambda)$ lle asigna a serie de potencias en q cuxos coeficientes de Fourier veñen dados, para cada $n \geq 0$, pola expresión

$$a_n(T_m \boldsymbol{f}) = \sum_{\substack{d|(m,n)\\(d,p)=1}} (X+1)^{\varphi^{-1}(\pi(d))} \chi_F(d) d^{-1} a_{\frac{mn}{d^2}}(\boldsymbol{f})(X)\Lambda,$$

onde as aplicacións ϕ e π son as que se definiron durante a proba da proposición 5.12:

$$\begin{array}{rccc} \varphi\colon & \mathbb{Z}_p & \longrightarrow & 1+p\mathbb{Z}_p \\ & s & \longmapsto & u^s \end{array} \quad \text{e} \quad \begin{array}{rccc} \pi\colon & \mathbb{Z}_p^\times & \longmapsto & 1+p\mathbb{Z}_p \\ & \alpha & \longmapsto & \omega(\alpha)^{-1}\alpha. \end{array}$$

Dedúcese trivialmente da definición anterior que T_n é Λ-linear. Vexamos agora que é un endomorfismo de $\mathrm{M}(\chi;\Lambda)$ e que, en efecto, conmuta coa aplicación de especialización $\nu_{k,\chi}$. Sexa $\boldsymbol{f} \in \mathrm{M}(\chi;\Lambda)$ tal que

$$\boldsymbol{f}\left(\zeta_\chi u^k - 1\right) = f_k \in \mathrm{M}_k\left(p^r, \chi\omega^{-k}; \overline{\mathbb{Q}}_p\right)$$

para todo $k \geq M$, con M un certo enteiro positivo. Entón, para todo $n \geq 0$ e todo $m > 0$:

$$\begin{aligned} a_n(T_m \boldsymbol{f}) \left(\zeta_\chi u^k - 1\right) &= \sum_{\substack{d|(m,n) \\ (d,p)=1}} \left(\zeta_\chi u^k\right)^{\varphi^{-1}(\pi(d))} \chi_F(d) d^{-1} a_{\frac{mn}{d^2}}(\boldsymbol{f}) \left(\zeta_\chi u^k - 1\right) \\ &= \sum_{\substack{d|(m,n) \\ (d,p)=1}} \chi(d)\omega(d)^{-k} d^{k-1} a_{\frac{mn}{d^2}}(f_k) = a_n(T_m f_k) \end{aligned}$$

para cada $k \geq M$, o cal proba ambas afirmacións.

Unha vez estendido o concepto de operador de Hecke ao contexto das familias de Hida, podemos definir tamén as formas propias de Hecke:

Definición 5.16. Sexan p un primo impar, $r \geq 1$ un enteiro, $\mathcal{K}$ unha extensión finita do corpo cociente de Λ, I a clausura íntegra de Λ en $\mathcal{K}$ e $\chi\colon (\mathbb{Z}/p^r)^\times \to \mathbb{C}^\times$ un carácter de Dirichlet. Dicimos que $\boldsymbol{f} \in \mathrm{M}(\chi; I)$ é unha *forma propia de Hecke* se, para todo enteiro $n \geq 1$, $T_n \boldsymbol{f} = c_n(X)\boldsymbol{f}$ con $c_n(X) \in I$ (isto é, se $\boldsymbol{f}$ é autovector de todos os operadores T_n).

Sexa $\mathcal{O}$ o anel de valoración dunha extensión finita de $\mathbb{Q}_p$. Nótese que, se $\boldsymbol{f} \in \mathrm{M}(\chi; I)$ é unha forma propia de Hecke e $\nu(\boldsymbol{f}) \in \mathrm{M}_k(p^r, \chi; \mathcal{O})$ para algunha $\nu \in \mathcal{A}_k(\chi; I)$ e algún $k \geq 2$, entón $\nu(\boldsymbol{f})$ tamén é unha forma propia de Hecke.

Para finalizar a sección, xeneralizaremos o proxector ordinario e das formas modulares p-ádicas ao caso das familias de Hida, para o cal precisaremos uns resultado previos.

Teorema 5.17 (Teorema de preparación de Weierstrass)**.** *Sexan p un primo impar, $\mathcal{O}$ o anel de valoración dunha extensión finita de $\mathbb{Q}_p$ e $\mathfrak{m} = (\pi)$ o anel maximal de $\mathcal{O}$. Consideremos unha serie de potencias*

$$f(X) = \sum_{i=0}^{\infty} a_i X^i \in \mathcal{O}[\![X]\!]$$

para a que exista un certo enteiro positivo n verificando $a_i \in \mathfrak{m}$, con $0 \leq i \leq n-1$, e $a_n \notin \mathfrak{m}$ (logo $a_n \in \mathcal{O}^\times$). Entón f pode ser reescrita de xeito único como $f(X) = P(X)U(X)$, onde $U(T) \in \mathcal{O}[\![X]\!]^\times$ e $P(X)$ é un polinomio mónico de grao n cuxos coeficientes, agás o principal, pertencen a $\mathfrak{m}$. Aínda máis: se $f(X) \in \mathcal{O}[\![X]\!]$ é non nula entón podémolo escribir de xeito único como

$$f(X) = \pi^\mu P(X)U(X),$$

con P e U coma antes e μ un enteiro non negativo.

Demostración. Véxase [22, Teorema 7.3]. □

Corolario 5.18. *Sexa p un primo impar e sexa $\mathcal{O}$ o anel de valoración dunha extensión finita de $\mathbb{Q}_p$. Unha serie de potencias $f \in \mathcal{O}[\![X]\!]$ non nula ten soamente unha cantidade finita de ceros no disco unitario p-ádico: $\{x \in \mathbb{C}_p \mid |x|_p < 1\}$.*

Demostración. Véxase [22, Corolario 7.4]. □

Proposición 5.19. *Sexan p un primo impar, un enteiro $r \geq 1$, $\chi\colon (\mathbb{Z}/p^r\mathbb{Z})^\times \to \mathbb{C}^\times$ un carácter de Dirichlet e ω o carácter de Teichmüller módulo p. Existe un único idempotente $e\colon \mathrm{M}(\chi;\Lambda) \to \mathrm{M}^{\mathrm{ord}}(\chi;\Lambda)$ satisfacendo*

$$\boldsymbol{f}|e\left(\zeta_\chi u^k - 1\right) = \boldsymbol{f}\left(\zeta_\chi u^k - 1\right)|e$$

para toda $\boldsymbol{f} \in \mathrm{M}(\chi;\Lambda)$ e para todo $k > 1$ tal que $\boldsymbol{f}\left(\zeta_\chi u^k - 1\right) \in \mathrm{M}_k\left(p^r, \chi\omega^{-k}; \overline{\mathbb{Q}}_p\right)$.

Demostración. Sexa $\boldsymbol{f} \in \mathrm{M}(\chi;\Lambda)$ e sexa un enteiro positivo a tal que

$$\boldsymbol{f}\left(\zeta_\chi u^k - 1\right) \in \mathrm{M}_k\left(p^r, \chi\omega^{-k}; \overline{\mathbb{Q}}_p\right)$$

para todo $k \geq a$. Definimos os conxuntos

$$\mathrm{M}_{a,k} = \left\{\boldsymbol{g} \in \mathrm{M}(\chi;\Lambda) \mid \boldsymbol{g}\left(\zeta_\chi u^j - 1\right) \in \mathrm{M}_j\left(p^r, \chi\omega^{-k}; \overline{\mathbb{Q}}_p\right) \text{ para } a \leq j \leq k\right\},$$
$$\mathrm{M}^0_{a,k} = \left\{\boldsymbol{g} \in \mathrm{M}_{a,k} \mid \boldsymbol{g}\left(\zeta_\chi u^j - 1\right) = 0 \text{ para } a \leq j \leq k\right\},$$

e observemos que

$$\boldsymbol{f} \in \mathrm{M}_{a,\infty} \coloneqq \bigcap_{j=a}^{\infty} \mathrm{M}_{a,k}.$$

Ademais, para cada $\boldsymbol{g} \in \mathrm{M}_{a,k}$ denotaremos a súa clase en $\mathrm{M}_{a,k}/\mathrm{M}^0_{a,k}$ por $\boldsymbol{g}_k$. Consideremos agora, para $k \geq a$, o mergullo

$$\begin{array}{ccc} \mathrm{M}_{a,k}/\mathrm{M}^0_{a,k} & \longrightarrow & \displaystyle\bigoplus_{j=a}^{k} \mathrm{M}_j\left(p^r, \chi\omega^{-k}; \overline{\mathbb{Q}}_p\right) \\ \boldsymbol{g}_k & \longmapsto & \displaystyle\bigoplus_{j=a}^{k} \boldsymbol{g}\left(\zeta_\chi u^j - 1\right), \end{array}$$

do cal deducimos que $\mathrm{M}_{a,k}/\mathrm{M}^0_{a,k}$ é un $\mathcal{O}$-módulo finitamente xerado, con $\mathcal{O}$ o anel de valoración dunha extensión finita de $\mathbb{Q}_p$. De feito, como $\mathrm{M}_{a,k}$ e $\mathrm{M}^0_{a,k}$ son estables pola acción de T_p, polo lema 4.17 sabemos que

$$e_k = \lim_{n\to\infty} T_p^{n!}$$

é un idempotente ben definido en $\mathrm{M}_{a,k}/\mathrm{M}^0_{a,k}$. Este operador só esta ben definido módulo $\mathrm{M}^0_{a,k}$ pero a especialización $\nu_{j,\chi}(\boldsymbol{g}|e_k)$ está ben definida para toda $\boldsymbol{g} \in \mathrm{M}_{a,k}$, con $j \in$

$\{a, \dots, k\}$. Ademais, como o operador de Hecke T_p conmuta coa especialización $\nu_{k,\chi}$, para toda $\boldsymbol{g} \in \mathrm{M}_{a,k}$ e para todo $j \in \{a, \dots, k\}$, temos:

$$\begin{aligned}(\boldsymbol{g}|e_k)\left(\zeta_\chi u^j - 1\right) &= \lim_{n\to\infty} T_p^{n!}\boldsymbol{g}\left(\zeta_\chi u^j - 1\right) \\ &= \lim_{n\to\infty} T_p^{n!}\left(\boldsymbol{g}\left(\zeta_\chi u^j - 1\right)\right) = \boldsymbol{g}\left(\zeta_\chi u^j - 1\right)|e.\end{aligned}$$

Definamos agora

$$\Omega_k = \prod_{j=a}^{k} \ker(\nu_{k,\chi})$$

e consideremos a seguinte aplicación:

$$\begin{aligned}\mathrm{M}_{a,k}/\mathrm{M}_{a,k}^0 &\longrightarrow \Lambda/\Omega_k[\![q]\!] \\ \boldsymbol{g}_k &\longmapsto \sum_{n=0}^{\infty}(a_n(\boldsymbol{g})(X) \bmod \Omega_k)q^n.\end{aligned}$$

Nótese que se $a_n(\boldsymbol{g})(X) \in \Omega_k$ para todo n entón $\boldsymbol{g} \in \mathrm{M}_{a,k}^0$, logo $\boldsymbol{g}_k = 0$. Así, a aplicación anterior é inxectiva e a imaxe pola mesma de $\boldsymbol{f}_k|e_k$ vén dada por

$$\sum_{n=0}^{\infty}(a_n(\boldsymbol{f}|e_k)(X) \bmod \Omega_k)q^n.$$

Agora, polo corolario 5.18 toda serie de potencias de Λ ten unha cantidade finita de ceros en $\{x \in \mathbb{C}_p \mid |x|_p < 1\}$, logo $\{\Omega_k\}_{k=a}^{\infty}$ é unha sucesión decrecente de ideais tal que

$$\bigcap_{j=a}^{\infty} \Omega_j = \{0\},$$

polo que $\Lambda = \varprojlim \Lambda/\Omega_k$. Por outra banda, para cada $a \le j \le k$ consideremos a aplicación

$$\pi_{k,j} \colon \mathrm{M}_{a,k}/\mathrm{M}_{a,k}^0 \longrightarrow \mathrm{M}_{a,j}/\mathrm{M}_{a,j}^0$$

e observemos que $e_j \circ \pi_{k,j} = \pi_{k,j} \circ e_k$. Isto implica que

$$\boldsymbol{f}|e_j = (\pi_{k,j}(\boldsymbol{f}_k))|e_j = \pi_{k,j}(\boldsymbol{f}_k|e_k),$$

logo

$$\boldsymbol{f}_j|e_j \equiv \boldsymbol{f}_k|e_k \left(\bmod \mathrm{M}_{a,j}^0\right).$$

Así, para todo enteiro $n \ge 0$,

$$a_n(\boldsymbol{f}|e_k) \equiv a_n(\boldsymbol{f}|e_j) \,(\bmod \Omega_j),$$

polo que definimos

$$a_n(\boldsymbol{f}|e)(X) = \varprojlim (a_n(\boldsymbol{f}|e_k) \bmod \Omega_k) \in \Lambda.$$

O seguinte paso, agora que temos definido un elemento $\boldsymbol{f}|e \in \Lambda[\![q]\!]$, será probar que $\boldsymbol{f}|e \in \mathrm{M}^{\mathrm{ord}}(\chi;\Lambda)$. Para isto, notemos que

$$a_n(\boldsymbol{f}|e) \equiv a_n(\boldsymbol{f}|e_k)\,(\mathrm{mód}\Omega_k)$$

para todo $n \geq 0$ e todo $k \geq a$. Polo tanto, como xa probamos antes que e_k conmuta coa especialización $\nu_{k,\chi}$, para cada $j \geq a$:

$$a_f(\boldsymbol{f}|e)\left(\zeta_\chi u^j - 1\right) = a_n(\boldsymbol{f}|e_{j+1})\left(\zeta_\chi u^j - 1\right) = a_n\left(\boldsymbol{f}\left(\zeta_\chi u^j - 1\right)|e\right).$$

Así, $\boldsymbol{f}|e\left(\zeta_\chi u^j - 1\right) = \boldsymbol{f}\left(\zeta_\chi u^j - 1\right)|e$, polo que $\boldsymbol{f}|e \in \mathrm{M}^{\mathrm{ord}}(\chi;\Lambda)$.
Para finalizar, nótese que, para todo $k \geq a$,

$$\begin{aligned}\boldsymbol{f}|e^2\left(\zeta_\chi u^k - 1\right) - \boldsymbol{f}|e\left(\zeta_\chi u^k - 1\right) &= \boldsymbol{f}|e\left(\zeta_\chi u^k - 1\right)|e - \boldsymbol{f}\left(\zeta_\chi u^k - 1\right)|e \\ &= \boldsymbol{f}\left(\zeta_\chi u^k - 1\right)|e^2 - \boldsymbol{f}\left(\zeta_\chi u^k - 1\right)|e = 0,\end{aligned}$$

polo que $\boldsymbol{f}|e^2 - \boldsymbol{f}|e \in \ker(\nu_{k,\chi})$ para todo $k \geq a$. Non obstante, como a intersección de todos os Ω_k é nula, sabemos que

$$\bigcap_{j=a}^{\infty} \ker(\nu_{j,\chi}) = \{0\},$$

polo que $\boldsymbol{f}|e^2 = \boldsymbol{f}|e$, concluíndo así que e é idempotente. □

5.4. Construción de familias de Hida

Nesta seccion amosaremos o proceso a seguir para construír unha familia de Hida cuxa especialización nun certo k sexa a forma modular p-ádica de peso k que escollamos. Neste proceso serán fundamentais as familias das series de Eisenstein introducidas na sección 5.2.

Notación 5.20. Sexa p un primo impar e sexa $\mathcal{O}$ o anel de valoración dunha extensión finita de $\mathbb{Q}_p$. Denotaremos o espazo de series de potencias $\mathcal{O}[\![X]\!]$ por $\Lambda_{\mathcal{O}}$. Nótese que, para todo enteiro $k > 2$ e para todo carácter de Dirichlet $\chi\colon (\mathbb{Z}/p^r\mathbb{Z})^\times \to \mathcal{O}^\times$, $\nu_{k,\chi}$ se estende trivialmente a $\Lambda_{\mathcal{O}}$.

Definición 5.21. Sexan p un primo impar, $k > 2$ e ℓ enteiros positivos, $\mathcal{O}$ o anel de valoración dunha extensión finita de $\mathbb{Q}_p$, $\chi\colon (\mathbb{Z}/p^r\mathbb{Z})^\times \to \mathcal{O}^\times$ un carácter de Dirichlet, ω o carácter de Teichmüller módulo p e $f \in \mathrm{M}_\ell(p^r,\psi;\mathcal{O})$ unha forma modular p-ádica de peso ℓ con $\psi\colon (\mathbb{Z}/p^r\mathbb{Z})^\times \to \mathcal{O}^\times$ outro carácter de Dirichlet. Xa sabemos que

$$fE_{k,\chi\omega^{-k}} \in \mathrm{M}_{k+\ell}\left(p^r,\psi\chi\omega^{-k};\mathcal{O}\right).$$

Definimos series de potencias $c_n(X) \in \Lambda_{\mathcal{O}}$ para cada enteiro positivo n mediante

$$f\mathcal{E}_\chi(X) = \sum_{n=0}^{\infty} c_n(X) q^n.$$

Definimos o *produto de convolución* de f e $\mathcal{E}_\chi$, que denotaremos por $f * \mathcal{E}_\chi$, como a expansión

$$(f * \mathcal{E}_\chi)(X) = \sum_{n=0}^{\infty} c_n\left(u^{-\ell}X + \left(u^{-\ell} - 1\right)\right) q^n.$$

Nótese que, nos termos da definición anterior, $\left|u^{-\ell}\right|_p = 1$ e $\left|u^{-\ell} - 1\right|_p < 1$, logo $c_n\left(u^{-\ell}X + \left(u^{-\ell} - 1\right)\right) \in \Lambda_{\mathcal{O}}$. Séguese entón que $(f * \mathcal{E}_\chi)(X) \in \Lambda_{\mathcal{O}}[\![q]\!]$. De feito, para cada $k > 2$ temos

$$\begin{aligned}
(f * \mathcal{E}_\chi)\left(\zeta_\chi u^{k+\ell} - 1\right) &= \sum_{n=0}^{\infty} c_n\left(u^{-\ell}\left(\zeta_\chi u^{k+\ell} - 1\right) + u^{-\ell} - 1\right) q^n \\
&= \sum_{n=0}^{\infty} c_n\left(\zeta_\chi u^{k} - 1\right) q^n \\
&= f\mathcal{E}_\chi\left(\zeta_\chi u^{k} - 1\right) = fE_{k,\chi\omega^{-k}},
\end{aligned}$$

polo que $f * \mathcal{E}_\chi$ é unha forma modular $\Lambda_{\mathcal{O}}$-ádica. En realidade, polo argumento anterior podemos ver que f é unha forma cuspidal p-ádica, logo $f * \mathcal{E}_\chi$ é unha forma cuspidal $\Lambda_{\mathcal{O}}$-ádica.

Na proba do seguinte teorema faremos un argumento semellante para amosar que podemos levantar toda forma modular p-ádica con coeficientes de Fourier en $\mathcal{O}$ a unha forma $\Lambda_{\mathcal{O}}$-ádica.

Teorema 5.22. *Sexan p un primo impar, $r \geq 0$ e $k \geq 1$ enteiros, $\mathcal{O}$ o anel de valoración dunha extensión finita de $\mathbb{Q}_p$, $\chi\colon (\mathbb{Z}/p^r\mathbb{Z})^\times \to \mathcal{O}^\times$ un carácter de Dirichlet e ω o carácter de Teichmüller módulo p. Para toda $f \in \mathrm{M}_k\left(p^r, \chi\omega^{-k}; \mathcal{O}\right)$ existe $\boldsymbol{f} \in \mathrm{M}(\chi; \Lambda_{\mathcal{O}})$ tal que $\boldsymbol{f}\left(\zeta_\chi u^k - 1\right) = f$.*

Demostración. Xa vimos na observación 5.13 que $\mathcal{E}_1 \notin \Lambda[\![q]\!]$ posto que o seu coeficiente constante é da forma F/X para certa $F \in \Lambda$. Non obstante, $\mathcal{E}'(X) \coloneqq X\mathcal{E}_1(X) \in \Lambda[\![q]\!]$ e

$$\mathcal{E}'\left(u^k - 1\right) = \frac{\left(u^k - 1\right)\zeta_p(1-k)}{2},$$

onde ζ_p é a función zeta p-ádica, a cal sabemos que ten un polo simple en 0 con residuo $(1 - 1/p)$ (véxase [7, Teorema 3.5.2]). Así, grazas a [7, Teorema 7.3.3],

$$\mathcal{E}'(0) = \lim_{k\to 0} \frac{\left(u^k - 1\right)\zeta_p(1-k)}{2} = \lim_{k\to 0} \frac{k\left(u^k - 1\right)\zeta_p(1-k)}{2k} = \frac{\log(u)\left(p^{-1} - 1\right)}{2} \in \mathcal{O}^\times.$$

Agora, definindo

$$\mathcal{E}(X) \coloneqq \frac{2}{\log(u)\,(p^{-1}-1)}\mathcal{E}'(X),$$

temos $\mathcal{E} \in \Lambda_{\mathcal{O}}[\![q]\!]$ e $a_0(\mathcal{E}) = 1$. Así, para toda $f \in \mathrm{M}_k\left(p^r, \chi\omega^{-k}; \mathcal{O}\right)$ tense que $f\mathcal{E} \in \Lambda_{\mathcal{O}}[\![q]\!]$ e

$$f\mathcal{E}(0) = fa_0(\mathcal{E}) = f.$$

Finalmente, escribindo

$$(f * \mathcal{E}) = \sum_{n=0}^{\infty} a_n(f\mathcal{E})\left(\zeta_\chi^{-1}u^{-k}X + \left(\zeta_\chi^{-1}u^{-k} - 1\right)\right)q^n \in \Lambda_{\mathcal{O}}[\![q]\!],$$

temos

$$(f * \mathcal{E})\left(\zeta_\chi u^k - 1\right) = f,$$

polo que $f * \mathcal{E}$ é a forma $\boldsymbol{f}$ buscada. □

Nos termos da proba anterior, nótese que se $f \in \mathrm{M}_k^{\mathrm{ord}}\left(p^r, \chi\omega^{-k}; \mathcal{O}\right)$ entón

$$(f * \mathcal{E})|e\left(\zeta_\chi u^k - 1\right) = (f * \mathcal{E})\left(\zeta_\chi u^k - 1\right)|e = f|e = f,$$

logo $f * \mathcal{E} \in \mathrm{M}^{\mathrm{ord}}(\chi; \Lambda_{\mathcal{O}})$. Nótese tamén que o teorema anterior garante a existencia dunha familia de Hida que interpola a forma modular p-ádica desexada, pero non asegura que esta familia sexa única.

5.5. A estrutura do espazo das formas modulares $\Lambda_{\mathcal{O}}$-ádicas ordinarias

Nesta última sección estudaremos dous teoremas sobre a estrutura do $\Lambda_{\mathcal{O}}$-módulo de formas modulares $\Lambda_{\mathcal{O}}$-ádicas ordinarias xunto cun teorema de control respecto ao mesmo. Para isto, serán importantes os seguintes feitos sobre $\Lambda_{\mathcal{O}}$, cuxas probas se poden achar en [7, Teorema 7.3.1] e [11, Teorema 9.4]:

- $\Lambda_{\mathcal{O}}$ é un dominio de factorización única.
- $\Lambda_{\mathcal{O}}$ é un anel compacto coa topoloxía definida mediante o sistema de veciñanzas dado polas potencias do ideal maximal $\mathfrak{m} = (p, X)$ (en particular, $\Lambda_{\mathcal{O}}$ é simultaneamente anel alxébrico e topolóxico).
- $\Lambda_{\mathcal{O}}$ é noetheriano.

Tamén será necesario empregar novamente o corolario 5.18 do teorema de preparación de Weierstrass.

Teorema 5.23. *Sexan p un primo impar, $r \geq 1$ un enteiro, $\mathcal{O}$ o anel de valoración dunha extensión finita de $\mathbb{Q}_p$ e $\chi\colon (\mathbb{Z}/p^r\mathbb{Z})^\times \to \mathcal{O}^\times$ un carácter de Dirichlet. Os $\Lambda_{\mathcal{O}}$-módulos $\mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})$ e $\mathrm{S}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})$ son finitamente xerados.*

Demostración. Imos probar o teorema unicamente para $\mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})$, pois a demostración é idéntica no caso de $\mathrm{S}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})$. En primeiro lugar, nótese que $\mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})$ é libre de torsión sobre $\Lambda_{\mathcal{O}}$, pois é, por definición, un submódulo de $\Lambda_{\mathcal{O}}[\![q]\!]$, que é libre de torsión. Vexamos agora que o rango de todo $\Lambda_{\mathcal{O}}$-submódulo finitamente xerado e libre de $\mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})$ ten un límite superior independente do submódulo en cuestión.
Sexa pois M un $\Lambda_{\mathcal{O}}$-submódulo de $\mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})$ finitamente xerado e libre cunha base $\{\boldsymbol{f}_1,\dots,\boldsymbol{f}_l\}$, $l \geq 1$ un certo enteiro. Posto que os elementos $\boldsymbol{f}_i$ son linearmente independentes sobre $\Lambda_{\mathcal{O}}$, sabemos que existen enteiros $n_1,\dots,n_l$ tales que

$$D(X) \coloneqq \det \begin{pmatrix} a_{n_1}(\boldsymbol{f}_1)(X) & a_{n_1}(\boldsymbol{f}_2)(X) & \dots & a_{n_1}(\boldsymbol{f}_l)(X) \\ a_{n_2}(\boldsymbol{f}_1)(X) & a_{n_2}(\boldsymbol{f}_2)(X) & \dots & a_{n_2}(\boldsymbol{f}_l)(X) \\ \vdots & \vdots & \ddots & \vdots \\ a_{n_l}(\boldsymbol{f}_1)(X) & a_{n_l}(\boldsymbol{f}_2)(X) & \dots & a_{n_l}(\boldsymbol{f}_l)(X) \end{pmatrix} \neq 0.$$

Agora, polo corolario 5.18 sabemos que só existe unha cantidade finita de elementos $\alpha \in \mathbb{C}_p$ tales que $|\alpha|_p < 1$ e $D(\alpha) = 0$, logo existe un enteiro positivo a tal que, para todo $k \geq a$, $D\left(\zeta_\chi u^k - 1\right) \neq 0$ e $\boldsymbol{f}_i\left(\zeta_\chi u^k - 1\right) \in \mathrm{M}_k^{\mathrm{ord}}\left(p^r, \chi\omega^{-k};\mathcal{O}\right)$ para todo i, onde ω é o carácter de Teichmüller módulo p. Tomemos pois $k \geq a$ e denotemos, para cada $1 \leq i \leq l$, $\boldsymbol{f}_i\left(\zeta_\chi u^k - 1\right) = f_i$. Así,

$$\det \begin{pmatrix} a_{n_1}(f_1) & a_{n_1}(f_2) & \dots & a_{n_1}(f_l) \\ a_{n_2}(f_1) & a_{n_2}(f_2) & \dots & a_{n_2}(f_l) \\ \vdots & \vdots & \ddots & \vdots \\ a_{n_l}(f_1) & a_{n_l}(f_2) & \dots & a_{n_l}(f_l) \end{pmatrix} = D\left(\zeta_\chi u^k - 1\right) \neq 0,$$

logo $\{f_1,\dots,f_l\}$ é unha base dun $\mathcal{O}$-submódulo libre de $\mathrm{M}_k^{\mathrm{ord}}\left(p^r, \chi\omega^{-k};\mathcal{O}\right)$. Polo teorema 4.23 sabemos que o rango de $\mathrm{M}_k^{\mathrm{ord}}\left(p^r, \chi\omega^{-k};\mathcal{O}\right)$ sobre $\mathcal{O}$ ten un valor independente do peso k, logo l está limitado independentemente do submódulo M. É dicir, o rango de calquera $\Lambda_{\mathcal{O}}$-submódulo finitamente xerado e libre de $\mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})$ está limitado por $\mathrm{Rang}_{\mathcal{O}}\left(\mathrm{M}_2^{\mathrm{ord}}\left(p^r, \chi\omega^{-2};\mathcal{O}\right)\right)$.
Empregaremos agora este feito para probar que $\mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})$ é finitamente xerado. Deducimos pola devandita afirmación que existe un enteiro positivo t tal que todo conxunto de $t+1$ elementos de $\mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})$ é linearmente dependente sobre $\Lambda_{\mathcal{O}}$. Sexa entón $\{\boldsymbol{f}_1,\dots,\boldsymbol{f}_t\} \subset \mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})$ un conxunto linearmente independente sobre $\Lambda_{\mathcal{O}}$. Para toda

$\boldsymbol{f} \in \mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})$ existen $\lambda_1,\dots,\lambda_{t+1} \in \Lambda_{\mathcal{O}}$ con $\lambda_t \neq 0$ tales que

$$\lambda_1 \boldsymbol{f}_1 + \cdots + \lambda_t \boldsymbol{f}_t + \lambda_{t+1}\boldsymbol{f} = 0,$$

o cal implica que

$$\boldsymbol{f} = -\frac{\lambda_1}{\lambda_{t+1}}\boldsymbol{f}_1 - \cdots - \frac{\lambda_t}{\lambda_{t+1}}\boldsymbol{f}_t.$$

Dedúcese entón que toda forma modular $\Lambda_{\mathcal{O}}$-ádica ordinaria se pode expresar como combinación linear das $\boldsymbol{f}_i$ sobre o corpo cociente $\mathcal{K}$ de Λ. Escribamos entón

$$\boldsymbol{f} = \sum_{i=0}^{t} \alpha_i \boldsymbol{f}_i,$$

con $\alpha_i \in \mathcal{K}$. Posto que as formas $\boldsymbol{f}_i$ son linearmente independentes sobre $\Lambda_{\mathcal{O}}$, existen enteiros positivos $n_1,\dots,n_t$ tales que

$$D(X) = \det \begin{pmatrix} a_{n_1}(\boldsymbol{f}_1)(X) & a_{n_1}(\boldsymbol{f}_2)(X) & \dots & a_{n_1}(\boldsymbol{f}_t)(X) \\ a_{n_2}(\boldsymbol{f}_1)(X) & a_{n_2}(\boldsymbol{f}_2)(X) & \dots & a_{n_2}(\boldsymbol{f}_t)(X) \\ \vdots & \vdots & \ddots & \vdots \\ a_{n_t}(\boldsymbol{f}_1)(X) & a_{n_t}(\boldsymbol{f}_2)(X) & \dots & a_{n_t}(\boldsymbol{f}_t)(X) \end{pmatrix} \neq 0.$$

Así, como

$$\begin{pmatrix} a_{n_1}(\boldsymbol{f}_1)(X) & a_{n_1}(\boldsymbol{f}_2)(X) & \dots & a_{n_1}(\boldsymbol{f}_t)(X) \\ a_{n_2}(\boldsymbol{f}_1)(X) & a_{n_2}(\boldsymbol{f}_2)(X) & \dots & a_{n_2}(\boldsymbol{f}_t)(X) \\ \vdots & \vdots & \ddots & \vdots \\ a_{n_t}(\boldsymbol{f}_1)(X) & a_{n_t}(\boldsymbol{f}_2)(X) & \dots & a_{n_t}(\boldsymbol{f}_t)(X) \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_t \end{pmatrix} = \begin{pmatrix} a_{n_1}(\boldsymbol{f})(X) \\ a_{n_2}(\boldsymbol{f})(X) \\ \vdots \\ a_{n_t}(\boldsymbol{f})(X) \end{pmatrix},$$

deducimos que

$$D(X)\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_t \end{pmatrix} = \mathrm{Adx}\begin{pmatrix} a_{n_1}(\boldsymbol{f}_1)(X) & a_{n_1}(\boldsymbol{f}_2)(X) & \dots & a_{n_1}(\boldsymbol{f}_t)(X) \\ a_{n_2}(\boldsymbol{f}_1)(X) & a_{n_2}(\boldsymbol{f}_2)(X) & \dots & a_{n_2}(\boldsymbol{f}_t)(X) \\ \vdots & \vdots & \ddots & \vdots \\ a_{n_t}(\boldsymbol{f}_1)(X) & a_{n_t}(\boldsymbol{f}_2)(X) & \dots & a_{n_t}(\boldsymbol{f}_t)(X) \end{pmatrix} \begin{pmatrix} a_{n_1}(\boldsymbol{f})(X) \\ a_{n_2}(\boldsymbol{f})(X) \\ \vdots \\ a_{n_t}(\boldsymbol{f})(X) \end{pmatrix},$$

onde $\mathrm{Adx}(A)$ denota a matrix adxunta de A. Posto que o lado dereito da igualdade é un elemento de $\Lambda_{\mathcal{O}}^t$, séguese que $D(X)\alpha_i \in \Lambda_{\mathcal{O}}$ para todo $1 \leq i \leq t$. Así,

$$D(X)\boldsymbol{f} = D(X)\alpha_1\boldsymbol{f}_1 + \cdots + D(X)\alpha_t\boldsymbol{f}_t \in \Lambda_{\mathcal{O}}\boldsymbol{f}_1 + \cdots + \Lambda_{\mathcal{O}}\boldsymbol{f}_t,$$

e como a forma $\boldsymbol{f}$ foi escollida de xeito arbitrario isto implica que

$$D(X)\mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}}) \subset \Lambda_{\mathcal{O}}\boldsymbol{f}_1 + \cdots + \Lambda_{\mathcal{O}}\boldsymbol{f}_t.$$

Como $\Lambda_{\mathcal{O}}$ é noetheriano e $D(X)\mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})$ é un submódulo dun $\Lambda_{\mathcal{O}}$-módulo finitamente xerado deducimos que $D(X)\mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})$ é finitamente xerado. Finalmente, como $\mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})$ é libre de torsión sobre $\Lambda_{\mathcal{O}}$, a aplicación $\mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}}) \to D(X)\mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})$ é un isomorfismo, co que concluímos que $\mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})$ é finitamente xerado. □

Teorema 5.24. *Sexan p un primo impar, $r \geq 1$ un enteiro, $\mathcal{O}$ o anel de valoración dunha extensión finita de $\mathbb{Q}_p$ e $\chi\colon (\mathbb{Z}/p^r\mathbb{Z})^\times \to \mathcal{O}^\times$ un carácter de Dirichlet. Os $\Lambda_{\mathcal{O}}$-módulos $\mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})$ e $\mathrm{S}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})$ son libres.*

Demostración. Para probar este resultado imos achar unha base de $\mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})$ sobre $\Lambda_{\mathcal{O}}$. Polo teorema 5.23 sabemos $\mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})$ é finitamente xerado, logo existe un enteiro positivo a tal que para todo $k \geq a$ temos $\nu_{k,\chi}(\boldsymbol{f}) = \boldsymbol{f}\left(\zeta_\chi u^k - 1\right) \in \mathrm{M}_k^{\mathrm{ord}}\left(p^r, \chi\omega^{-k}; \mathcal{O}\right)$ para toda $\boldsymbol{f} \in \mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})$, onde ω é o carácter de Teichmüller módulo p. Sexa entón $k \geq a$ e observemos que se $\nu_{k,\chi}(\boldsymbol{f}) = 0$ entón $P_{k,\chi} = X - \left(\zeta_\chi u^k - 1\right)$ é un factor de $a_n(\boldsymbol{f})(X)$ para todo $n \geq 0$. Neste caso, como

$$(\boldsymbol{f}/P_{k,\chi})\left(\zeta_\chi u^j - 1\right) = \frac{\boldsymbol{f}\left(\zeta_\chi u^j - 1\right)}{\zeta_\chi u^j - \zeta_\chi u^k} \in \mathrm{M}_k^{\mathrm{ord}}\left(p^r, \chi\omega^{-k}; \overline{\mathbb{Q}}_p\right)$$

para todo $j > k$, deducimos que $\boldsymbol{f}/P_{k,\chi} \in \mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})$, logo

$$\ker(\nu_{k,\chi}) = P_{k,\chi}\mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}}).$$

Así, $\nu_{k,\chi}$ proporciona un mergullo de $\mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})/P_{k,\chi}\mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})$ en $\mathrm{M}_k^{\mathrm{ord}}\left(p^r, \chi\omega^{-k}; \mathcal{O}\right)$. Ademais, como $\mathcal{O}$ é un dominio de ideais principais e $\mathrm{M}_k^{\mathrm{ord}}\left(p^r, \chi\omega^{-k}; \mathcal{O}\right)$ é un $\mathcal{O}$-módulo libre, séguese que todo $\mathcal{O}$-submódulo de $\mathrm{M}_k^{\mathrm{ord}}\left(p^r, \chi\omega^{-k}; \mathcal{O}\right)$ é tamén libre. En particular, $\mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})/P_{k,\chi}\mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})$ é un $\mathcal{O}$-módulo libre. Sexa agora $\{\boldsymbol{f}_1, \dots, \boldsymbol{f}_N\} \subset \mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})$, con $N \geq 1$ un enteiro, tal que $\{\boldsymbol{f}_1 \bmod P_{k,\chi}, \dots, \boldsymbol{f}_N \bmod P_{k,\chi}\}$ é unha base do espazo $\mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})/P_{k,\chi}\mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})$ e vexamos que $\{\boldsymbol{f}_1, \dots, \boldsymbol{f}_N\}$ é linearmente independente. Supoñamos que existen $\alpha_i \in \Lambda_{\mathcal{O}}$, con $i \in \{1, \dots, N\}$ e polo menos un α_i non nulo, tales que

$$\alpha_1\boldsymbol{f}_1 + \cdots + \alpha_N\boldsymbol{f}_N = 0.$$

En caso de ser necesario, dividimos ambos lados da igualdade por unha potencia suficientemente grande de $P_{k,\chi}$ para poder asumir que polo menos un dos α_i non é divisible por $P_{k,\chi}$. Reducindo a igualdade módulo $P_{k,\chi}$ obtemos unha combinación linear non trivial dos elementos da base de $\mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})/P_{k,\chi}\mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})$, o cal é unha contradición e, por tanto, demostra que o conxunto $\{\boldsymbol{f}_1, \dots, \boldsymbol{f}_N\}$ é linearmente independente sobre $\Lambda_{\mathcal{O}}$.
Para finalizar a proba, consideremos o $\Lambda_{\mathcal{O}}$-módulo

$$M = \langle \boldsymbol{f}_1, \dots, \boldsymbol{f}_N \rangle$$

e vexamos que $M = \mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})$. É evidente que $M \subset \mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})$, logo só resta probar a outra inclusión. Sexa $\boldsymbol{f} \in \mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})$. Sabemos que existe unha combinación linear sobre $\Lambda_{\mathcal{O}}$ dos $\boldsymbol{f}_i$, que denotamos por $\boldsymbol{g}_0$, tal que $\boldsymbol{f} - \boldsymbol{g}_0 \in P_{k,\chi}\mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})$, logo

$$(\boldsymbol{f} - \boldsymbol{g}_0)/P_{k,\chi} \in \mathrm{M}^{\mathrm{ord}}(\chi;\Omega_{\mathcal{O}}).$$

Analogamente, existe unha combinación linear sobre $\Lambda_{\mathcal{O}}$ dos $\boldsymbol{f}_i$, que denotamos por $\boldsymbol{g}_1$, tal que $(\boldsymbol{f} - \boldsymbol{g}_0)/P_{k,\chi} - \boldsymbol{g}_1 \in P_{k,\chi}\mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})$. Procedendo indutivamente deste xeito obtemos unha sucesión $\{\boldsymbol{g}_i\}_{i=0}^{\infty}$ de elementos de M tal que

$$\boldsymbol{f} \equiv \sum_{i=0}^{j} P_{k,\chi}^{i}\boldsymbol{g}_i \left(\mathrm{mód}\, P_{k,\chi}^{j+1}\right)$$

para todo enteiro $j \geq 0$. Sexa, para cada $i \geq 0$,

$$\boldsymbol{g}_i = \alpha_{1,i}\boldsymbol{f}_1 + \cdots + \alpha_{N,i}\boldsymbol{f}_N$$

para certos $\alpha_{n,j} \in \Lambda_{\mathcal{O}}$. Posto que $\Lambda_{\mathcal{O}}$ é un anel compacto deducimos que, para todo $1 \leq n \leq N$,

$$\alpha_n = \lim_{j\to\infty} \sum_{i=0}^{j} \alpha_{n,j}P_{k,\chi}^{j} \in \varprojlim \Lambda_{\mathcal{O}}/P_{k,\chi}^{i}\Lambda_{\mathcal{O}} = \Lambda_{\mathcal{O}}.$$

Así,

$$\boldsymbol{g} = \alpha_1\boldsymbol{f}_1 + \cdots + \alpha_N\boldsymbol{f}_N \in M.$$

De feito, sabemos que $\boldsymbol{f} - \boldsymbol{g} \in \mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}}) \subset \Lambda_{\mathcal{O}}[\![q]\!]$ é divisible por $P_{k,\chi}^{i}$ para todo enteiro positivo i, logo $\boldsymbol{g} = \boldsymbol{f}$, o cal conclúe a proba. □

Agora que xa temos establecidos os dous teoremas desexados sobre a estrutura dos $\Lambda_{\mathcal{O}}$-módulos $\mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})$ e $\mathrm{S}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})$, imos finalizar o capítulo probando a seguinte relación entre os espazos das familias de Hida ordinarias e os espazos das formas modulares p-ádicas ordinarias dun peso fixado:

Teorema 5.25. *Sexan p un primo impar, $r \geq 1$ e $k \geq 2$ enteiros, $\mathcal{O}$ o anel de valoración dunha extensión finita K de $\mathbb{Q}_p$, $\chi\colon (\mathbb{Z}/p^r\mathbb{Z})^{\times} \to \mathcal{O}^{\times}$ un carácter de Dirichlet e ω o carácter de Teichmüller módulo p. A aplicación $\boldsymbol{f} \mapsto \boldsymbol{f}\left(\zeta_\chi u^k - 1\right)$ induce os isomorfismos*

$$\mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})/P_{k,\chi}\mathrm{M}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}}) \cong \mathrm{M}_k^{\mathrm{ord}}\left(p^r, \chi\omega^{-k};\mathcal{O}\right),$$
$$\mathrm{S}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}})/P_{k,\chi}\mathrm{S}^{\mathrm{ord}}(\chi;\Lambda_{\mathcal{O}}) \cong \mathrm{S}_k^{\mathrm{ord}}\left(p^r, \chi\omega^{-k};\mathcal{O}\right),$$

onde $P_{k,\chi}$ é o ideal primo xerado por $X - \left(\zeta_\chi u^k - 1\right)$.

Demostración. Polo teorema 5.22, sabemos que para toda $f \in \mathrm{M}_k^{\mathrm{ord}}\left(p^r, \chi\omega^{-k}; \mathcal{O}\right)$ existe $\boldsymbol{f} \in \mathrm{M}^{\mathrm{ord}}(\chi; \Lambda_{\mathcal{O}})$ tal que $\boldsymbol{f}\left(\zeta_\chi u^k - 1\right) = f$. De feito, a proba dese teorema adaptada ás formas cuspidais dá lugar a unha afirmación semellante nese caso. Isto implica que a aplicación $\boldsymbol{f} \mapsto \boldsymbol{f}\left(\zeta_\chi u^k - 1\right)$ é sobrexectiva. Agora, posto que todos os espazos implicados nos isomorfismos do enunciado son $\mathcal{O}$-módulos libres, para probar o teorema chega con demostrar que,

$$\begin{aligned}
\mathrm{Rang}_{\mathcal{O}}\left(\mathrm{M}^{\mathrm{ord}}(\chi; \Lambda_{\mathcal{O}})/P_{k,\chi}\mathrm{M}^{\mathrm{ord}}(\chi; \Lambda_{\mathcal{O}})\right) &= \mathrm{Rang}_{\mathcal{O}}\left(\mathrm{M}_k^{\mathrm{ord}}\left(p^r, \chi\omega^{-k}; \mathcal{O}\right)\right), \\
\mathrm{Rang}_{\mathcal{O}}\left(\mathrm{S}^{\mathrm{ord}}(\chi; \Lambda_{\mathcal{O}})/P_{k,\chi}\mathrm{S}^{\mathrm{ord}}(\chi; \Lambda_{\mathcal{O}})\right) &= \mathrm{Rang}_{\mathcal{O}}\left(\mathrm{S}_k^{\mathrm{ord}}\left(p^r, \chi\omega^{-k}; \mathcal{O}\right)\right),
\end{aligned}$$

para cada $k \geq 2$. Ademais, o teorema 4.23 asegura que

$$\begin{aligned}
\mathrm{Rang}_{\mathcal{O}}\left(\mathrm{M}_k^{\mathrm{ord}}\left(p^r, \chi\omega^{-k}; \mathcal{O}\right)\right) &= \mathrm{Rang}_{\mathcal{O}}\left(\mathrm{M}_2^{\mathrm{ord}}\left(p^r, \chi\omega^{-2}; \mathcal{O}\right)\right), \\
\mathrm{Rang}_{\mathcal{O}}\left(\mathrm{S}_k^{\mathrm{ord}}\left(p^r, \chi\omega^{-k}; \mathcal{O}\right)\right) &= \mathrm{Rang}_{\mathcal{O}}\left(\mathrm{S}_2^{\mathrm{ord}}\left(p^r, \chi\omega^{-2}; \mathcal{O}\right)\right),
\end{aligned}$$

logo basta con demostrar as igualdades para un k fixo. Nótese tamén que probar as igualdades equivale a probar que

$$\begin{aligned}
\dim_K\left(\mathrm{M}^{\mathrm{ord}}(\chi; \Lambda_{\mathcal{O}})/P_{k,\chi}\mathrm{M}^{\mathrm{ord}}(\chi; \Lambda_{\mathcal{O}}) \otimes_{\mathcal{O}} K\right) &= \dim_K\left(\mathrm{M}_k^{\mathrm{ord}}\left(p^r, \chi\omega^{-k}; K\right)\right), \\
\dim_K\left(\mathrm{S}^{\mathrm{ord}}(\chi; \Lambda_{\mathcal{O}})/P_{k,\chi}\mathrm{S}^{\mathrm{ord}}(\chi; \Lambda_{\mathcal{O}}) \otimes_{\mathcal{O}} K\right) &= \dim_K\left(\mathrm{S}_k^{\mathrm{ord}}\left(p^r, \chi\omega^{-k}; K\right)\right).
\end{aligned}$$

Agora, por [7, Prop. 4.5.3], existe un k tal que

$$\left(\mathrm{M}^{\mathrm{ord}}(\chi; \Lambda_{\mathcal{O}})/P_{k,\chi}\mathrm{M}^{\mathrm{ord}}(\chi; \Lambda_{\mathcal{O}})\right) \otimes_{\mathcal{O}} K \cong \mathrm{M}_k^{\mathrm{ord}}\left(p^r, \chi\omega^{-k}; K\right).$$

Ademais, como se amosa na demostración dese mesmo resultado,

$$\mathrm{M}_k^{\mathrm{ord}}\left(p^r, \chi\omega^{-k}; K\right) \cong \mathrm{S}_k^{\mathrm{ord}}\left(p^r, \chi\omega^{-k}; K\right) \oplus KE_{k,\chi\omega^{-k}}.$$

Finalmente, como $E_{k,\chi\omega^{-k}} = \mathcal{E}_{k,\chi}\left(\zeta_\chi u^k - 1\right)$ entón

$$\mathrm{S}^{\mathrm{ord}}(\chi; \Lambda_{\mathcal{O}})/P_{k,\chi}\mathrm{S}^{\mathrm{ord}}(\chi; \Lambda_{\mathcal{O}}) \otimes_{\mathcal{O}} K \cong \mathrm{S}_k^{\mathrm{ord}}\left(p^r, \chi\omega^{-k}; K\right),$$

probando así as igualdades buscadas para todo k. □

Capítulo 6

Formas modulares xeométricas

Neste último capítulo veremos como podemos empregar ferramentas da xeometría alxébrica no estudo das formas modulares e da teoría de Hida. Introduciranse pois conceptos como as curvas modulares, a curva de Tate ou as formas modulares p-ádicas de Katz e exporanse resultados de utilidade sobre eles.

6.1. As curvas modulares como espazos de moduli

O obxectivo desta sección é introducir as denominadas curvas modulares e estudar os seus espazos de moduli, para o cal será necesario falar primeiro das curvas elípticas.

Definición 6.1. Un *retículo* en $\mathbb{C}$ é un conxunto $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, onde $\{\omega_1, \omega_2\}$ é unha base de $\mathbb{C}$ como $\mathbb{R}$-espazo vectorial tal que $\omega_1/\omega_2 \in \mathbb{H}$. Por outra banda, unha *curva elíptica* (complexa) E é o lugar xeométrico dado por unha expresión do tipo

$$y^2 = x^3 + Ax + B, \quad \text{con } 4A^3 + 27B^2 \neq 0.$$

Pódese consultar [20] para ver un tratamento exhaustivo das curvas elípticas.

Observación 6.2. Existen resultados (véxase [5, §1.4]) que permiten identificar toda curva elíptica E con algún cociente $\mathbb{C}/\Lambda$, onde Λ é un certo retículo; estes resultados coñécense como teoremas de uniformización. Así, durante este capítulo falaremos de curvas elípticas complexas $E = \mathbb{C}/\Lambda$ como cocientes do plano complexo por certos retículos. Aínda máis: por [5, Corolario 1.3.3], dúas curvas elípticas $\mathbb{C}/\Lambda_1$ e $\mathbb{C}/\Lambda_2$ son isomorfas como grupos se, e só se, existe $m \in \mathbb{C}$ tal que $m\Lambda_1 = \Lambda_2$. Tomando $\Lambda_1 = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$,

$$(1/\omega_2)\Lambda_1 = \mathbb{Z}(\omega_1/\omega_2) \oplus \mathbb{Z} = \mathbb{Z}\tau \oplus \mathbb{Z} =: \Lambda_\tau$$

se consideramos $\tau = \omega_1/\omega_2$, co cal toda curva elíptica é isomorfa a $\mathbb{C}/\Lambda_\tau$ para algún $\tau \in \mathbb{H}$. Escribiremos entón $E_\tau = \mathbb{C}/\Lambda_\tau$.

Definamos agora os espazos que, como despois veremos, serán os espazos de moduli das curvas modulares, así como estas últimas.

Definición 6.3. Sexa $N \geq 1$ un enteiro. Unha *curva elíptica mellorada* é un par (E, Q), onde E é unha curva elíptica complexa e Q é un punto de E de orde N (isto é, un punto tal que $NQ = 0$ e $nQ \neq 0$ para $0 < n < N$). Definimos ademais unha relación de equivalencia $\sim$ de curvas elípticas melloradas:

$$(E, Q) \sim (E', Q') \text{ se existe un isomorfismo } \varphi\colon E \to E' \text{ tal que } \varphi(E) = E'.$$

Esta relación é evidentemente unha relación de equivalencia, pois a composición de isomorfismos é un isomorfismo. Denotamos o seu conxunto cociente como

$$\mathrm{S}_1(N) = \{\text{curvas elípticas melloradas}\}/_{\sim},$$

e denotamos as clases de equivalencia de $\mathrm{S}_1(N)$ como $[E, Q]$.

Definición 6.4. Sexa $N \geq 1$ un enteiro. Defínese a *curva modular* $Y_1(N)$ como o espazo de órbitas da acción de $\Gamma_1(N)$ en $\mathbb{H}$ pola esquerda:

$$\mathrm{Y}_1(N) = \Gamma_1(N)\backslash\mathbb{H} = \{\Gamma_1(N)\tau \mid \tau \in \mathbb{H}\}.$$

Vexamos agora un teorema que relaciona os espazos anteriores:

Teorema 6.5. *Sexa $N \geq 1$ un enteiro. O espazo de moduli de $\Gamma_1(N)$ é*

$$\mathrm{S}_1(N) = \{[E_\tau, 1/N + \Lambda_\tau] \mid \tau \in \mathbb{H}\}.$$

Ademais, dous puntos $[E_\tau, 1/N + \Lambda_\tau]$ e $[E_{\tau'}, 1/N + \Lambda_{\tau'}]$ son iguais se, e só se, $\Gamma_1(N)\tau = \Gamma_1(N)\tau'$, logo temos unha bixección

$$\begin{array}{rccc} \psi\colon & \mathrm{S}_1(N) & \xrightarrow{\sim} & \mathrm{Y}_1(N) \\ & [E_\tau, 1/N + \Lambda_\tau] & \longmapsto & \Gamma_1(N)\tau. \end{array}$$

Demostración. Sexa $[E, Q] \in \mathrm{S}_1(N)$. Posto que E é isomorfa a $\mathbb{C}/\Lambda_{\tau'}$ para algún $\tau' \in \mathbb{H}$, podemos tomar $E = \mathbb{C}/\Lambda_{\tau'}$, logo

$$Q = \frac{c\tau' + d}{N} + \Lambda_{\tau'}$$

para certos enteiros c e d. Ademais, como Q é un punto de orde N entón $\mathrm{mcd}(c, d, N) = 1$, polo que, pola identidade de Bézout, existen enteiros a, b e k tales que $ad - bc - kN = 1$ e a matriz $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ é invertible módulo N. Agora, modificar as entradas de γ módulo

N non repercute en Q, logo podemos asumir que $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Tomemos agora $\tau = \gamma\tau'$ e $m = c\tau' + d$ e notemos que $m\tau = a\tau' + b$, logo

$$m\Lambda_\tau = m(\mathbb{Z}\tau \oplus \mathbb{Z}) = \mathbb{Z}(a\tau' + b) \oplus \mathbb{Z}(c\tau' + d) = \mathbb{Z}\tau' \oplus \mathbb{Z} = \Lambda_{\tau'},$$

onde a terceira igualdade se deduce de [5, Lema 1.3.1]. Polo tanto,

$$m\left(\frac{1}{N} + \Lambda_\tau\right) = \frac{c\tau' + d}{N} + \Lambda_{\tau'} = Q,$$

co cal chegamos a que $[E, Q] = [E_\tau, 1/N + \Lambda_\tau]$, onde $\tau \in \mathbb{H}$.
Consideremos agora dous puntos $\tau, \tau' \in \mathbb{H}$ tales que $\Gamma_1(N)\tau = \Gamma_1(N)\tau'$. Existe entón $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ tal que $\tau = \gamma\tau'$. Sexa novamente $m = c\tau' + d$, co cal

$$m\Lambda_\tau = \Lambda_{\tau'} \quad \text{e} \quad m\left(\frac{1}{N} + \Lambda_\tau\right) = \frac{c\tau' + d}{N} + \Lambda_{\tau'}.$$

Posto que $(c, d) \equiv (0, 1) \,(\mathrm{mód}\, N)$, a segunda igualdade convértese módulo N en

$$m\left(\frac{1}{N} + \Lambda_\tau\right) = \frac{1}{N} + \Lambda_{\tau'},$$

co cal $[E_\tau, 1/N + \Lambda_\tau] = [E_{\tau'}, 1/N + \Lambda_{\tau'}]$.
Reciprocamente, sexan $\tau, \tau' \in \mathbb{H}$ tales que $[E_\tau, 1/N + \Lambda_\tau] = [E_{\tau'}, 1/N + \Lambda_{\tau'}]$. Por [5, Corolario 1.3.3], existe $m \in \mathbb{C}$ tal que $m\Lambda_\tau = \Lambda_{\tau'}$ e $m(1/N + \Lambda_\tau) = 1/N + \Lambda_{\tau'}$. Empregando novamente [5, Lema 1.3.1], a primeira destas condicións tradúcese en

$$\begin{pmatrix} m\tau \\ m \end{pmatrix} = \gamma \begin{pmatrix} \tau' \\ 1 \end{pmatrix} \text{ para certo } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),$$

logo $m = c\tau' + d$, co cal a segunda condición transfórmase en

$$\frac{c\tau' + d}{N} + \Lambda_\tau = \frac{1}{N} + \Lambda_{\tau'},$$

probando así que $(c, d) \equiv (0, 1) \,(\mathrm{mód}\, N)$ e $\gamma \in \Gamma_1(N)$. Conclúese así, posto que $\tau = \gamma\tau'$, que $\Gamma_1(N)\tau = \Gamma_1(N)\tau'$. □

Séguese entónque as curvas modulares $\mathrm{Y}_1(N)$ son espazos de moduli. Alternativamente, pódese ver que o functor

$$\begin{array}{rccc} \mathrm{Ell}\colon & \mathrm{Var}_{\text{álx}} & \longrightarrow & \mathrm{Sets} \\ & X & \longmapsto & \{\text{curvas elípticas}/X\}\,/_\sim, \end{array}$$

onde $\mathrm{Var}_{\text{álx}}$ é a categoría das variedades alxébricas definidas sobre o anel $\mathbb{Z}[1/N]$ e Sets a dos conxuntos, é representable, isto é, $\mathrm{Ell}(X) = \mathrm{Hom}(X, X_0)$ para algunha variedade alxébrica X_0. Polo tanto, toda curva elíptica mellorada (E, Q) pode verse como un morfismo

$X \to X_0$, sendo neste caso $X_0 = Y_1(N)$.

Para finalizar o capítulo, obsérvese que podemos facer unha construción análoga á de $S_1(N)$ e $Y_1(N)$ considerando pares (E, C), onde E é unha curva elíptica e C un subgrupo cíclico de orde N. Defínese unha relación de equivalencia entre estes pares como:

$$(E, C) \sim (E', C') \text{ se existe un isomorfismo } \varphi\colon E \to E' \text{ tal que } \varphi(C) = C'$$

Denótase por $S_0(N)$ o seu conxunto cociente e por $[E, C]$ a clase de equivalencia de (E, C). Finalmente, definindo a curva modular $Y_0(N) = \Gamma_0(N)\backslash\mathbb{H}$, pódese ver de xeito análogo a como o fixemos con $Y_1(N)$ que $Y_0(N)$ é isomorfo a $S_0(N)$ e, por tanto, que é un espazo de moduli.

Observación 6.6. Todo isto proporciona un novo xeito de identificar $\Gamma_0(N)/\Gamma_1(N)$ con $(\mathbb{Z}/N\mathbb{Z})^\times$, pois podemos definir un morfismo

$$\begin{array}{ccc} Y_1(N) & \longrightarrow & Y_0(N) \\ [E, P] & \longmapsto & [E, \langle P\rangle], \end{array}$$

sendo $\langle P\rangle$ o grupo cíclico xerado por P, e cada punto de $Y_0(N)$ ten $\varphi(N)$ preimaxes posto que un grupo cíclico de orde N ten $\varphi(N)$ xeradores, sendo $\varphi(N)$ a función de Euler de N.

6.2. Diferenciais en curvas elípticas

Nesta sección sentaremos as bases para reinterpretar as formas modulares clásicas en $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$ a través de diferenciais nas curvas elípticas e da curva modular $Y(1) \coloneqq Y_1(1) = Y_0(1) = \mathrm{SL}_2(\mathbb{Z})/\mathbb{H}$, o cal dará lugar á construción de Katz.

Para comezar, denotemos a compactificación de $Y(1)$ como $X(1)$ e notemos que ambos espazos son superficies de Riemann (en particular, curvas alxébricas suaves). Ademais $X(1)$ é compacto, polo que é unha curva proxectiva, mentres que $Y(1)$ é unha curva afín.

Notación 6.7. Sexa $k > 0$ un enteiro e sexa $f \in \mathrm{M}_k$ unha forma modular de nivel 1. Empregaremos a seguinte 1-forma durante o resto da sección:

$$\omega_f = f(z)dz^{\otimes \frac{k}{2}} \in \left(\Omega^1_{\mathbb{H}}\right)^{\otimes \frac{k}{2}},$$

onde $\Omega^1_{\mathbb{H}}$ denota o espazo das formas diferenciais en $\mathbb{H}$ e o expoñente $\otimes\frac{k}{2}$ denota o produto tensorial da base consigo mesma $\frac{k}{2}$ veces.

Nótese que, dada $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ e sendo $\gamma^*\omega_f$ o pullback de ω_f mediante γ,

$$\gamma^*\omega_f = f(\gamma z)d(\gamma z)^{\otimes \frac{k}{2}} = (cz+d)^k f(z)\left(\frac{d}{dz}\frac{az+b}{cz+d}\right)^{\frac{k}{2}} dz^{\otimes \frac{k}{2}} = \omega_f,$$

logo ω_f é $\mathrm{SL}_2(\mathbb{Z})$-invariante e, polo tanto, pode entenderse como unha diferencial na curva modular $Y(1)$:

$$\omega_f \in \left(\Omega^1_{Y(1)}\right)^{\otimes \frac{k}{2}}.$$

Denotemos por $\mathcal{R}$ o conxunto de retículos $\mathbb{Z}\alpha_1 \oplus \mathbb{Z}\alpha_2$ en $\mathbb{C}$, con α_1/α_2 non real e $\alpha_i \neq 0$, e escribamos

$$\mathcal{M} = \left\{(\alpha_1, \alpha_2) \in (\mathbb{C}^\times)^2 \mid \Im\left(\frac{\alpha_1}{\alpha_2} > 0\right)\right\}.$$

Consideremos a seguinte aplicación:

$$\begin{array}{rccc} \varphi\colon & \mathcal{M} & \longrightarrow & \mathcal{R} \\ & (\alpha_1, \alpha_2) & \longmapsto & \mathbb{Z}\alpha_1 \oplus \mathbb{Z}\alpha_2. \end{array}$$

Obsérvese que φ é sobrexectiva e que podemos considerar as seguintes accións:

- $\mathrm{SL}_2(\mathbb{Z})$ actúa en $\mathcal{M}$ pola esquerda mediante

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(\alpha_1, \alpha_2) \coloneqq (a\alpha_1 + b\alpha_2, c\alpha_1 + d\alpha_2).$$

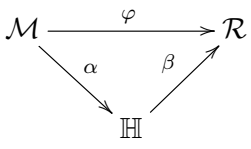
- $\mathbb{C}^\times$ actúa en $\mathcal{R}$ mediante o produto por un escalar. Esta acción permítenos trasladarnos dun retículo a outro que sexa homotético do primeiro (isto é, a imaxe do primeiro a través dunha homotecia).

- $\mathbb{C}^\times$ actúa en $\mathcal{M}$ mediante o produto por un escalar.

Por outra banda, definamos as aplicacións

$$\begin{array}{rccc} \alpha\colon & \mathcal{M} & \longrightarrow & \mathbb{H} \\ & (\alpha_1, \alpha_2) & \longmapsto & \frac{\alpha_1}{\alpha_2} \end{array} \quad \text{e} \quad \begin{array}{rccc} \beta\colon & \mathbb{H} & \longrightarrow & \mathcal{R} \\ & \tau & \longmapsto & \Lambda_\tau, \end{array}$$

onde $\Lambda_\tau = \mathbb{Z}\tau \oplus \mathbb{Z}$ como na sección anterior. Xuntando todo isto, temos o seguinte diagrama non conmutativo



Pódese ver así que α é $\mathrm{SL}_2(\mathbb{Z})$-invariante e que β induce un isomorfismo $\mathbb{H} \cong \mathcal{R}/\mathbb{C}^\times$. Isto é, todo punto do semiplano superior complexo $\mathbb{H}$ correspóndese cun retículo (módulo homotecia).

Definimos agora o conxunto $\mathcal{E}$ como o conxunto de clases de isomorfía de curvas elípticas complexas, do cal obtemos as aplicacións

$$\begin{array}{ccc} \mathbb{H} & \longrightarrow & \mathcal{E} \\ \tau & \longmapsto & E_\tau \end{array} \quad \text{e} \quad \begin{array}{ccc} u\colon \mathcal{R} & \longrightarrow & \mathcal{E} \\ \Lambda & \longmapsto & \mathbb{C}/\Lambda. \end{array}$$

Proposición 6.8. *A aplicación $u\colon \mathcal{R} \to \mathcal{E}$ factorízase a través de $\mathbb{C}^\times$ e induce un isomorfismo $\mathcal{R}/\mathbb{C}^\times \cong \mathcal{E}$.*

Demostración. A sobrexectividade séguese do feito de que se E é unha curva elíptica entón $E \cong \mathbb{C}/\Lambda$ para algún retículo Λ, o cal podemos calcular fixando unha diferencial invariante en E e definindo o seguinte retículo:

$$\Lambda = \left\{ \int_\gamma \omega \mid \gamma \in H_1(E, \mathbb{Z}) \right\},$$

sendo $H_1(E, \mathbb{Z})$ o primeiro grupo de homoloxía da curva elíptica, como é habitual escribilo. Para ver a inxectividade consideremos $\Lambda_1, \Lambda_2 \in \mathcal{R}$ dous retículos tales que existe un isomorfismo

$$\psi\colon \mathbb{C}/\Lambda_1 \cong \mathbb{C}/\Lambda_2.$$

Neste caso, como $\mathbb{C}$ é o espazo recubrimento universal de $\mathbb{C}/\Lambda_i$ para cada i, podemos levantar ψ a unha aplicación holomorfa $\overline{\psi}\colon \mathbb{C} \to \mathbb{C}$ tal que $\overline{\psi}(0) = 0$. Así, para cada $z \in \mathbb{C}$ e cada $l_1 \in \Lambda_1$,

$$\overline{\psi}(z + l_1) - \overline{\psi}(z) \in \Lambda_2,$$

e como Λ_2 é discreto entón polo teorema da aplicación aberta

$$\overline{\psi}(z + l_1) - \overline{\psi}(z) = a,$$

con a unha constante. Calculando a derivada do anterior deducimos que $\overline{\psi}'$ é invariante por Λ_1 e que é holomorfa, logo $\overline{\psi}' = b \in \mathbb{C}$ é unha aplicación constante. Isto implica que $\psi(z) = bz + c$ para unha certa constante $c \in \mathbb{C}$ e, como $\psi(0) = 0$, necesariamente tense $c = 0$. Concluímos entón que $\psi(z) = bz$ e que $\Lambda_2 = b\Lambda_1$, como queríamos demostrar. □

Por outra banda, a aplicación β induce un isomorfismo de $\mathcal{R}/\mathbb{C}^\times \cong \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ pois dous retículos Λ_τ e $\Lambda_{\tau'}$ son homotéticos se, e só se,

$$\tau' = \frac{a\tau + b}{c\tau + d} \text{ para certa } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Consideremos agora o conxunto $\mathbb{H}\times\mathbb{C}$ xunto coa súa proxección canónica p_1 sobre $\mathbb{H}$. Resulta que $\mathbb{Z}^2$ e $\mathrm{SL}_2(\mathbb{Z})$ actúan en $\mathbb{H}\times\mathbb{C}$ mediante as seguintes accións para un certo $(\tau,z)\in\mathbb{H}\times\mathbb{C}$

$$\begin{aligned}(\tau,z)\cdot(a,b) &= (\tau, z+a\tau+b),\\ \begin{pmatrix}a & b\\ c & d\end{pmatrix}(\tau,z) &= \left(\begin{pmatrix}a & b\\ c & d\end{pmatrix}\tau, (c\tau+d)^{-1}z\right).\end{aligned}$$

Grazas a estas accións deducimos que a proxección p_1 é $\mathrm{SL}_2(\mathbb{Z})$-equivariante. Consideremos agora o cociente $\mathbb{E}=(\mathbb{H}\times\mathbb{C})/\mathbb{Z}^2$ e tomemos a aplicación $p\colon \mathbb{E}\to\mathbb{H}$ inducida por p_1. Dado $\tau\in\mathbb{H}$ sabemos por todo o anterior que a fibra $p^{-1}(\tau)$ é isomorfa a E_τ. Se ademais facemos o cociente de $\mathbb{E}$ por $\mathrm{SL}_2(\mathbb{Z})$ obtemos o conxunto $\mathbb{E}(1)$ xunto coa aplicación

$$\begin{array}{ccc}\mathbb{E}(1) & \longrightarrow & \mathrm{Y}(1)\\ [E_\tau] & \longmapsto & [\tau].\end{array}$$

Sexa agora unha función homoxénea $F\colon\mathcal{R}\to\mathbb{C}$. É dicir, tal que, para un certo enteiro $k>0$,

$$F(\lambda\Lambda)=\lambda^{-k}F(L)\text{ para todo }\lambda\in\mathbb{C}^\times\text{ e todo }\Lambda\in\mathcal{R}.$$

Definimos a partir desta F outra función $f\colon\mathbb{H}\to\mathbb{C}$ mediante

$$f(\tau)=F(\Lambda_\tau)=F(\mathbb{Z}\tau\oplus\mathbb{Z})$$

e notemos que, dada $\gamma=\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)\in\mathrm{SL}_2(\mathbb{Z})$:

$$\begin{aligned}f(\gamma\tau)=F(\Lambda_{\gamma\tau}) &= \left(\mathbb{Z}\frac{a\tau+b}{c\tau+d}\oplus\mathbb{Z}\right)\\ &= F\left(\frac{1}{c\tau+d}(\mathbb{Z}(a\tau+b)\oplus\mathbb{Z}(c\tau+d))\right)\\ &= F\left((c\tau+d)^{-1}{}_\tau\right)\\ &= (c\tau+d)^kF(\Lambda_\tau)=(c\tau+d)^kf(\tau).\end{aligned}$$

Polo tanto, se a función f é holomorfa en $\mathbb{H}$ e en ∞ entón $f\in\mathrm{M}_k$.

Para continuar observemos que $\mathcal{R}$ é un fibrado sobre $\mathcal{R}/\mathbb{C}^\times$ e busquemos un fibrado $\mathcal{E}'$ de $\mathcal{E}$ tal que

$$\begin{array}{ccc}\mathcal{R} & \longrightarrow & \mathcal{E}'\\ \downarrow & & \downarrow\\ \mathcal{R}/\mathbb{C}^\times & \longrightarrow & \mathcal{E}\end{array}$$

Definamos pois $\mathcal{E}'$ como o conxunto de clases de isomorfía de pares (E,ω) formados por unha curva elíptica E e unha base ω de $H^0\left(E,\Omega^1_E\right)$. Nótese que este último espazo ten

dimensión 1 posto que as curvas elípticas teñen xénero 1 e o xénero é precisamente a dimensión do espazo cotanxente, logo ω é simplemente un elemento non nulo. O isomorfismo defínese como segue:

$$(E,\omega) \cong (E',\omega') \text{ se existe un isomorfismo } \varphi\colon E \to E' \text{ tal que } \varphi^*\omega' = \omega.$$

Obtemos así unha aplicación trivial $\mathcal{E}' \to \mathcal{E}$ que simplemente esquece o elemento ω de cada par (E,ω), logo existe unha aplicación $\mathcal{R} \to \mathcal{E}'$ que a cada $\Lambda \in \mathcal{R}$ lle asocia o par $(\mathbb{C}/\Lambda, dz)$, sendo z a función coordenada en $\mathbb{C}$. Ademais, dado $\lambda \in \mathbb{C}^\times$, esta aplicación leva $\lambda\Lambda$ en

$$[\mathbb{C}/(\lambda\Lambda), dz] = [\mathbb{C}/\Lambda, \lambda dz].$$

Podemos entón facer actuar $\mathbb{C}^\times$ en $\mathcal{E}'$ de xeito compatible co anterior mediante

$$\lambda[E,\omega] \coloneqq [E,\lambda\omega].$$

Novamente, para cada k enteiro consideremos unha aplicación $G\colon \mathcal{E}' \to \mathbb{C}$ tal que

$$G(E,\lambda\omega) = \lambda^{-k}G(E,\omega) \text{ para todo } \lambda \in \mathbb{C}^\times.$$

Repetindo os cálculos xa feitos para F e f obtemos unha función $g\colon \mathbb{H} \to \mathbb{C}$ definida mediante

$$g(\tau) = G([\mathbb{C}/\Lambda_\tau, dz])$$

que é feblemente modular, logo en caso de que sexa holomorfa en $\mathbb{H}$ e en ∞ deducimos que $g \in \mathrm{M}_k$.

Observación 6.9. É posible engadir a toda a construción anterior unha estrutura de nivel, permitindo así traballar en subgrupos de congruencia. Para estudar isto véxase [12, §5].

Recapitulando, nesta sección vimos como considerar as formas modulares como aplicacións definidas sobre os pares (E,ω), con E unha curva elíptica e ω unha forma diferencial. O seguinte paso deste capítulo será discutir este novo punto de vista das formas modulares desde un marco axiomático.

6.3. Formas modulares de Katz e a curva de Tate

Comezaremos esta sección xeneralizando a noción de forma modular a un anel R calquera (sempre conmutativo e unitario) a partir da construción feita na sección anterior. A continuación introduciremos a chamada curva de Tate e as formas modulares de Katz e falaremos brevemente sobre o principio da q-expansión.

Definición 6.10. Sexan $k > 0$ un enteiro e R un anel. Unha *forma modular meromorfa* f de peso k sobre R é unha función definida sobre os pares $(E/A, \omega)$, con E unha curva elíptica, A unha R-álxebra e ω unha sección de $\Omega^1_{E/A}$ que non se anula en ningún punto, tal que:

1. $f(E/A, \omega)$ depende unicamente da clase de A-isomorfía de $(E/A, \omega)$.
2. $f(E, \mu\omega) = \mu^{-k} f(E, \omega)$ para todo $\mu \in A^\times$.
3. Dado $\phi\colon A \to B$ un homomorfismo de aneis calquera, $f(E/B, \omega_B) = \phi(f(E/A, \omega))$.

Nótese que a anterior definición non inclúe ningunha condición sobre o comportamento de f nas cúspides. Completaremos pois a definición introducindo a curva de Tate, chegando así á construción de Katz das formas modulares.

A aplicación exponencial complexa que a cada z lle asigna $q = e^{2\pi i z}$ induce un isomorfismo

$$\mathbb{C}/\Lambda_\tau \xrightarrow{\sim} \mathbb{C}^\times/q^{\mathbb{Z}}.$$

Grazas a [20] sabemos que $\mathbb{C}^\times/q^{\mathbb{Z}}$ vén dado polo modelo

$$y^2 + xy = x^3 + a_4(q)x + a_6(q),$$

onde

$$a_4 = -\sum_{n=1}^{\infty} \frac{n^r q^n}{1-q^n} \quad \text{e} \quad a_6 = -\sum_{n=1}^{\infty} \frac{\left(5n^3 + 7n^5\right) q^n}{12\left(1-q^n\right)}$$

pertencen ambos a $\mathbb{Z}[\![q]\!]$. Ademais, o discriminante desta curva é

$$\Delta = q \prod_{n=1}^{\infty} (1-q^n)^{24},$$

polo que a ecuación define de xeito formal unha curva elíptica sobre o anel de series de Laurent $\mathbb{Z}[\![q]\!]\left[\Delta^{-1}\right] = \mathbb{Z}((q))$.

Observación 6.11. É necesario considerar o anel $\mathbb{Z}[\![q]\!]\left[\Delta^{-1}\right]$ para que o discriminante Δ sexa unha unidade neste espazo de series de Laurent, pois se o discriminante fose cero entón a curva non sería elíptica.

Definición 6.12. Para cada $z \in \mathbb{C}$ defínese a *curva de Tate* $T(q)$ como a serie de $\mathbb{Z}((q))$ definida por

$$y^2 + xy = x^3 + a_4(q)x + a_6(q).$$

Agora, á curva de Tate $T(q)$ podémoslle asociar unha diferencial canónica

$$\omega_{\text{can}} = \frac{dt}{t} \in H^0\left(T(q), \Omega^1\right),$$

sendo $T(q) = \mathbb{G}_m/q^{\mathbb{Z}}$ e $\mathbb{G}_m = \text{Spec}\left(\mathbb{Z}\left[t, t^{-1}\right]\right)$ o grupo multiplicativo. En particular, dada unha forma modular meromorfa f de peso k definimos a súa q-expansión como

$$f(T(q), \omega_{\text{can}}) \in \mathbb{Z}((q)).$$

Isto permítenos tratar o problema das cúspides xa mencionado, co cal podemos enunciar finalmente a definición de Katz das formas modulares:

Definición 6.13. Sexan $k > 0$ un enteiro e R un anel. Unha *forma modular de Katz* (ou simplemente unha *forma modular*) f de peso k sobre R é unha función definida sobre os pares $(E/A, \omega)$, con E unha curva elíptica, A unha R-álxebra e ω unha sección de $\Omega^1_{E/A}$ que non se anula en ningún punto, tal que:

1. $f(E/A, \omega)$ depende unicamente da clase de A-isomorfía de $(E/A, \omega)$.
2. $f(E, \mu\omega) = \mu^{-k} f(E, \omega)$ para todo $\mu \in A^\times$.
3. Dado $\phi\colon A \to B$ un homomorfismo de aneis calquera, $f(E/B, \omega_B) = \phi(f(E/A, \omega))$.
4. $f(T(q), \omega_{\text{can}}) \in A[\![q]\!]$.

Observación 6.14. A definición de Katz pode estenderse para que inclúa unha estrutura de nivel, ampliando así este obxecto a subgrupos de congruencia arbitrarios.

Dada f unha forma modular de Katz sobre un anel R tal que existe unha aplicación inxectiva $\phi\colon R \to \mathbb{C}$, a imaxe da q-expansión de f por ϕ coincide coa definición habitual da q-expansión de Fourier dunha forma modular clásica.

Para finalizar esta sección, mencionamos o seguinte resultado:

Teorema 6.15 (O principio da q-expansión)**.** *Unha forma modular f está totalmente determinada pola súa q-expansión.*

Demostración. Véxase [8, Prop. 1.6]. □

Observación 6.16. Nótese que se a curva modular $X(\Gamma)$ sobre a que se considera f non é conexa entón é necesario considerar as expansións de f nunha cúspide de cada compoñente conexa.

6.4. Formas modulares sobreconverxentes

Nesta última sección retomaremos a anterior definición de Katz particularizándoa ao caso p-ádico e comentaremos un problema que presenta esta definición, o cal nos levará a falar das curvas elípticas ordinarias e a introducir a noción de sobreconverxencia.

Definición 6.17. Sexan p un primo impar e $k > 0$ un enteiro. Dada unha álxebra A completa para a norma p-ádica, unha *forma modular p-ádica de Katz* f de peso k sobre A é unha función definida sobre os pares $(E/R, \omega)$, con E unha curva elíptica, ω unha sección de $\Omega^1_{E/A}$ que non se anula en ningún punto e R unha A-álxebra completa para a norma p-ádica verificando que $A(E/B, \omega_B)$ é invertible, sendo $B = A/p$, tal que:

1. $f(E/A, \omega)$ depende unicamente da clase de A-isomorfía de $(E/A, \omega)$.
2. $f(E, \mu\omega) = \mu^{-k} f(E, \omega)$ para todo $\mu \in A^\times$.
3. Dado $\phi\colon A \to B$ un homomorfismo de aneis calquera, $f(E/B, \omega_B) = \phi(f(E/A, \omega))$.
4. $f(T(q), \omega_{\text{can}}) \in A[\![q]\!]$.

Observación 6.18. Como vén sendo habitual, a definición anterior pódese dotar dunha estrutura da nivel que permita considerar formas modulares p-ádicas de Katz en subgrupos de congruencia arbitrarios.

A definición de Katz das formas modulares p-ádicas presenta un problema: o espectro do operador U_p non é discreto, polo que non podemos considerar descomposicións dunha forma modular dada en suma de formas propias. Para evitar esta situación precisaremos considerar as formas modulares sobreconverxentes, pero para definilas teremos que considerar varias nocións previas (para estudar todo isto con maior detalle véxase [3]).

Consideremos un anel S tal que $pS = 0$; é habitual considerar $S = \mathbb{Z}/p\mathbb{Z}$. Sexa A o invariante de Hasse, seguindo a definición de [3]. Entón, A é unha forma modular meromorfa (no estilo de Katz) de nivel 1 e peso $p-1$ sobre S. É dicir, dada E/S unha curva elíptica e ω unha diferencial xeradora de $\Omega^1_{E/S}$, temos $A(E, \omega) \in S$. O seguinte resultado de Deligne permite calcular a q-expansión de A:

Teorema 6.19 (Deligne)**.** $A(T(q), \omega_{\text{can}}) = 1$.

Agora, se $p \geq 5$ podemos ver o invariante de Hasse como a redución módulo p dunha forma modular en $\mathbb{Z}_p$ grazas ao seguinte teorema:

Teorema 6.20 (Buzzard)**.** *Sexa $p \geq 5$ un primo. $E_{p-1} \equiv A \,(\text{mód}\, p)$; é dicir, a serie de Eisenstein de peso $p-1$ é un levantamento de A.*

Demostración. Véxase [2]. □

Observación 6.21. Existe resultados análogos ao anterior nos casos $p = 2$ e $p = 3$, para os cales é necesario realizar varias modificacións.

Definición 6.22. Dado un primo impar p e S un anel tal que $pS = 0$, unha curva elíptica E/S dise *supersingular* se o seu anel de endomorfismos ten rango 4 sobre $\mathbb{Z}$. Noutro caso, dise que a curva elíptica E/S é *ordinaria*.

Existen diversas caracterizacións das curvas elípticas supersingulares, as cales se poden consultar en [20, Cap. 5]. Agora, empregando o teorema de Buzzard pódese ver que $A(E, \omega) = 0$ se, e só se, E é supersingular.

Definición 6.23. Consideremos un primo impar p. Definimos o *lugar ordinario* dunha curva modular X sobre $\mathbb{F}_p$ como o conxunto de puntos de X que se corresponden cunha curva elíptica sobre $\mathbb{F}_p$ coa súa estrutura de punto ou de subgrupo, segundo o caso. Séguese que o lugar ordinario consiste entón na parte de X correspondente ás curvas elípticas ordinarias.

O noso seguinte obxectivo é definir o lugar ordinario sobre $\mathbb{Z}_p$, para o que precisaremos empregar a noción xeométrica de *espazo ríxido analítico*, que no caso dunha curva modular X suave sobre $\mathbb{Z}[1/p]$ e sen singularidades consiste en considerar X como unha variedade complexa X^{rig} sobre $\mathbb{C}_p$ (para estudar a área da xeometría ríxida en maior profundidade véxase [3]).

Definición 6.24. Sexan p un primo impar e $k > 0$ un enteiro. As formas modulares p-ádicas son as seccións globais de $H^0\left(X^{\text{rig}}[0], \omega^k\right)$, onde $X^{\text{rig}}[0]$ denota o *lugar ordinario* do espazo ríxido analítico X^{rig}.

Antes de continuar con este tema, é importante notar que, dada unha unha curva elíptica E calquera, $E\left(\overline{K}\right)[p] = (\mathbb{Z}/p\mathbb{Z})^2$, onde K é unha extensión finita de $\mathbb{Q}_p$. Por outra banda, $E\left(\overline{k}\right)[p] = \mathbb{Z}/p\mathbb{Z}$ se E é ordinaria, sendo k o corpo residual de K. Así, a aplicación de redución módulo p mediante

$$E\left(\overline{K}\right) \longrightarrow E\left(\overline{k}\right)$$

ten como núcleo un subgrupo isomorfo a $\mathbb{Z}/p\mathbb{Z}$. Pola contra, se E é unha curva elíptica supersingular nada disto se cumple, pois $E\left(\overline{k}\right) = \{0\}$, logo en $E\left(\overline{K}\right)[p]$ temos $p + 1$ subgrupos de orde p e ningún deles é canónico. Porén, existe o seguinte resultado sobre este posible grupo canónico cando E "non é demasiado supersingular":

Teorema 6.25 (Lubin–Katz). *Sexan p un primo impar, R unha $\mathbb{Z}_p$-álxebra e v a valoración de R como anel de valoración discreta. Unha curva elíptica E/R posúe un subgrupo canónico de orde p se, e só se,*

$$v(A) < \frac{p}{p+1},$$

onde $A(E_S, \omega_S)$ é o invariante de Hasse de E/S, con $S = R/p$.

Fixemos unha curva modular X de nivel coprimo con p e sexa k unha extensión finita de $\mathbb{F}_p$. O espazo ríxido analítico X^{rig} admite unha aplicación de redución

$$X^{\mathrm{rig}}(\mathbb{C}_p) \longrightarrow X\left(\overline{k}\right),$$

que consiste simplemente en considerar os puntos de X módulo p. A preimaxe pola anterior aplicación dun punto $x \in X\left(\overline{k}\right)$ é un disco aberto e o lugar ordinario $X^{\mathrm{rig}}[0]$ é o complementario das preimaxes dos puntos supersingulares. Definimos o espazo $X^{\mathrm{rig}}[r]$ para un certo racional r como o espazo obtido eliminando os discos de raio p^{-r} de X^{rig} (pódese ver en [3, §3.2] que estes espazos están ben definidos).

Teorema 6.26. *Sexan p un primo impar, $k > 0$ un enteiro, $0 < r < 1/(p+1)$ un racional e X unha curva modular de nivel coprimo con p. Dada f unha sección de $H^0\left(X^{\mathrm{rig}}[r], \omega^k\right)$, $U_p f \in H^0\left(X^{\mathrm{rig}}[pr], \omega^k\right)$. En particular:*

$$U_p \colon H^0\left(X^{\mathrm{rig}}[r], \omega^k\right) \longrightarrow H^0\left(X^{\mathrm{rig}}[pr], \omega^k\right).$$

Demostración. Véxase [3, Teorema 3.3.2]. □

Este resultado significa que o operador U_p mellora as propiedades de converxencia: se consideramos seccións excluíndo un disco de raio p^{-r}, o operador U_p esta definido salvo nun disco de raio p^{-pr}, polo que converxe máis alá do que as seccións o facían no punto de partida. É por isto que consideramos a seguinte definición:

Definición 6.27. Sexan p un primo impar, $k > 0$ un enteiro, $0 < r < 1/(p+1)$ un racional e X unha curva modular de nivel Γ coprimo con p. O espazo de *formas modulares sobreconverxentes* de peso k, nivel Γ e raio r defínese como

$$M_k^\dagger(\Gamma, r) = H^0\left(X^{\mathrm{rig}}[r], \omega^k\right).$$

Para finalizar a sección, enunciamos un último teorema, cuxa demostración se pode ver en [3, §3.5].

Teorema 6.28. *Sexan p un primo impar, $k > 0$ un enteiro, $0 < r < 1/(p+1)$ un racional e X unha curva modular de nivel coprimo con p. A aplicación*

$$U_p \colon H^0\left(X^{\mathrm{rig}}[r], \omega^k\right) \longrightarrow H^0\left(X^{\mathrm{rig}}[r], \omega^k\right)$$

é compacta.

A modo de conclusión do capítulo, é importante entender a utilidade desta definición xeométrica das formas modulares sobreconverxentes, pois permite interpretar mellor os resultados que traballamos, especialmente aqueles relativos á variación p-ádica en familias. Para entender todo isto na súa totalidade sería necesario introducir un obxecto xeométrico denominado *eigencurve*, pero non incluiremos isto neste documento. Para estudar esta noción, pódense consultar tanto [4] como [1].

Bibliografía

[1] Bellaïche, J. (2021). *The Eigenbook. Eigenvarieties, families of Galois representations, p-adic L-functions*, Birkhäuser.

[2] Buzzard, K. (2003). *Analytic continuation of overconvergent eigenforms*, Lecture Notes.

[3] Calegari, F. (2013). *Congruences between modular forms*, Lecture Notes.

[4] Coleman, R. & Mazur, B. (1998). *The eigencurve*, de "Galois representations in arithmetic algebraic geometry", London Math. Soc. Lecture Note Ser., vol 254, Cambridge University Press.

[5] Diamond, D. & Shurman, J. (2005). *A First Course in Modular Forms*, Springer: Graduate texts in mathematics 228.

[6] Gouvêa, F. Q. (1997). *p-adic numbers: An introduction*, Springer - Universitext.

[7] Hida, H. (1993). *Elementary theory of L-functions and Eisenstein series*, London Math. Soc. Student Texts 85, Cambridge University Press.

[8] Katz, N. M. (1973). *p-adic properties of modular schemes and modular forms* en "Modular functions of one variable, III", Lecture Notes in Mathematics 350, Springer-Verlag.

[9] Koblitz, N. (1984). *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Springer: Graduate texts in mathematics 58.

[10] Lafferty, M. J. (s. d). *Hida Theory*, Lecture Notes.

[11] Lange, S. (2002). *Algebra*, Springer: Graduate texts in mathematics 211.

[12] Masdeu, M. (2009). *Geometric Modular Forms*, Lecture Notes.

[13] Masdeu, M. (2015). *Modular Forms*, Lecture Notes.
Dispoñible en `https://mat.uab.cat/~masdeu/`.

[14] Milne, J. S. (2020). *Class Field Theory (v4.03)*, Lecture Notes.
Dispoñible en `www.jmilne.org/math/`.

[15] Milne, J. S. (2017). *Modular Functions and Modular Forms (v1.31)*, Lecture Notes.
Dispoñible en `www.jmilne.org/math/`.

[16] Miyake, T. (1989). *Modular Forms*, Springer-Verlag.

[17] Serre, J. P. (1973). *A Course in Arithmetic*, Springer: Graduate texts in mathematics 7.

[18] Serre, J. P. (1973). *Formes modulaires et fonctions zêta p-adiques* en "Modular functions of one variable, III", Lecture Notes in Mathematics 350, Springer-Verlag.

[19] Shimura, G. (1971). *Introduction to the arithmetic theory of automorphic functions*, Iwanami Shoten & Princeton University Press.

[20] Silverman, J. H. (2009). *The Arithmetic of Elliptic Curves*, Springer: Graduate Texts in Mathematics 106.

[21] Spicer, S. (2011). *p-adic Modular Forms: An Introduction*, Lecture Notes.

[22] Washington, L. (1997). *Introduction to Cyclotomic Fields*, Springer: Graduate texts in mathematics 83.

[23] Zariski, L. & Samuel, P. (1960). *Commutative Algebra II*, D. Van Nostrand Company, Inc.