MODULAR FORMS AND THEIR GALOIS REPRESENTATIONS

HARUZO HIDA

In this course, assuming basic knowledge of algebraic number theory, commutative algebra and topology, we study non-archimedean deformation theory of modular forms on $GL(2)$ and modular Galois representations into $GL(2)$. We plan to discuss the following four topics:

(1) analytic/algebraic theory of elliptic modular forms (at the level of my book [LFE]),
(2) p-adic deformation theory of modular forms via the theory of p-adic analytic family of classical/p-adic modular forms,
(3) a description of Galois representation attached to modular forms (not the construction which requires good knowledge, out of the scope of this course, of functorial algebraic/arithmetic geometry of Grothendieck),
(4) description of the "big" Galois representation attached to a p-adic families of modular forms (including its construction assuming the item (3)).

If we do not reach the last two items within this quarter, we continue to go in this line in the Winter quarter 2013. If we finish the objectives listed here within this quarter, Winter 2013 course will cover slightly more advanced topics.

Here are basic notations and terminology used in this note. Commutative rings R are all supposed to have a multiplicative identity denoted by $1 = 1_R$. We write $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ for the filed of rational numbers, real numbers and complex numbers. We write $\overline{\mathbb{Q}} \subset \mathbb{C}$ be the collection of all numbers satisfying a polynomial equations in $\mathbb{Q}[X]$. The subset $\overline{\mathbb{Q}}$ is actually an algebraically closed field. A number field F is a subfield of $\overline{\mathbb{Q}}$ (possibly an infinite extension, but often we assume it is a finite extension). By definition, $\overline{\mathbb{Q}}/F$ is a Galois extension for all number field F (why?). If $[F : \mathbb{Q}] := \dim_{\mathbb{Q}} F$ is finite, $\overline{\mathbb{Q}}/F$ has infinite dimension over F (so, an infinite Galois extension of F; why infinite?). The Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ made out of all field automorphisms inducing the identity map on F is a compact group. Indeed, by the fundamental theorem of Galois theory, the restriction map $\mathrm{Gal}(\overline{\mathbb{Q}}/F)/\mathrm{Gal}(\overline{\mathbb{Q}}/E) \cong \mathrm{Gal}(E/F)$ for any finite Galois extensions E/F inside $\overline{\mathbb{Q}}$; so, we have a canonical isomorphism $\mathrm{Gal}(\overline{\mathbb{Q}}/F) = \varprojlim_{E/F} \mathrm{Gal}(E/F)$ making $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ a profinite group which is compact. In particular, open subgroups of $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ is $\mathrm{Gal}(\overline{\mathbb{Q}}/E)$ for any finite extension E/F inside $\overline{\mathbb{Q}}$. The subset $\overline{\mathbb{Z}}$ of $\overline{\mathbb{Q}}$ made up of numbers satisfying a monic integral polynomial in $\mathbb{Z}[X]$ is actually a subring stable under $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ whose field of fractions is equal to $\overline{\mathbb{Q}}$. The ring $\overline{\mathbb{Z}}$ is called the integer ring of $\overline{\mathbb{Q}}$ (which is non-noetherian). The ring $O_F := \overline{\mathbb{Z}} \cap F$ for a number field F

Date: November 16, 2012.
The author is partially supported by the NSF grant: DMS 0753991 and DMS 0854949.

is called integer ring of F, and plainly $O_{\mathbb{Q}} = \mathbb{Z}$. For a prime ideal $\mathfrak{P}$ of $\overline{\mathbb{Z}}$ containing a prime number p, $\mathfrak{P} \cap O_F$ is a maximal ideal of O_F, and we put

$$D_{\mathfrak{P}/\mathfrak{p}} = \{\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/F) | \sigma(\mathfrak{P}) = \mathfrak{P}\}, I_{\mathfrak{P}/\mathfrak{p}} = \{\sigma \in D_{\mathfrak{P}/\mathfrak{p}} | x^\sigma \equiv x \bmod \mathfrak{P} \text{ for all } x \in \overline{\mathbb{Z}}\}.$$

These closed subgroups of $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ are called the decomposition group and inertia group for $\mathfrak{P}/\mathfrak{p}$, respectively (why closed?). As you can find in any book of algebraic number theory, $D_{\mathfrak{P}/(p)}$ is isomorphic to $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ for the p-adic field $\mathbb{Q}_p$ and its algebraic closure $\overline{\mathbb{Q}}_p$. Since $\sigma \in D_{\mathfrak{P}}$ induces an automorphism of $\overline{\mathbb{Z}}/\mathfrak{P}$ which is an algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$, we have an exat sequence of compact groups

$$1 \to I_{\mathfrak{P}/\mathfrak{p}} \to D_{\mathfrak{P}/\mathfrak{p}} \to \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_{\mathfrak{p}}) \to 1.$$

for $\mathbb{F}_{\mathfrak{p}} = O_F/\mathfrak{p}$. Thus there is a unique generator $Frob_{\mathfrak{p}}$ of $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_{\mathfrak{p}})$ such that $Frob_{\mathfrak{p}}(x) = x^q$ for $q = |\mathbb{F}_{\mathfrak{p}}|$. Write again $Frob_{\mathfrak{p}}$ for any lift of $Frob_{\mathfrak{p}} \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_{\mathfrak{p}})$ to $D_{\mathfrak{P}/\mathfrak{p}}$ (which is unique modulo $I_{\mathfrak{P}/\mathfrak{p}}$). Also the conjugacy class of $D_{\mathfrak{P}/\mathfrak{p}}$ (and $I_{\mathfrak{P}/\mathfrak{p}}$, $Frob_{\mathfrak{p}} I_{\mathfrak{P}/\mathfrak{p}}$) in $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ only depends on $\mathfrak{p}$. A continuous homomorphism $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to G$ for a topological group G is unramified at $\mathfrak{p}$ if $I_{\mathfrak{P}} \subset \mathrm{Ker}(\rho)$ (for all $\mathfrak{P}$ inducing $\mathfrak{p}$). If $G = GL_n(K)$ for a finite extension K of a p-adic field $\mathbb{Q}_p$, ρ is called a p-adic Galois representation over F. If $[F : \mathbb{Q}] < \infty$, ρ is always assumed to have finite set of ramification primes (any geometrically made ρ satisfies this condition). Thus if $\mathfrak{p}$ is unramified for ρ, the conjugacy class of $\rho(Frob_{\mathfrak{p}})$ is well defined and depends only on $\mathfrak{p}$.

An affine space of dimension n over a ring A is just the free module A^n. Actually we sometimes regard it as a covariant functor sending an algebra A to A^n. Any algebra homomorphism $\sigma \in \mathrm{Hom}_{ALG}(A, A')$ sends $(a_1, \ldots, a_n) \in A^n$ to $(\sigma(a_1), \ldots, \sigma(a_n)) \in A'^n$ giving covariant functoriality. When we emphasize that this is a functor, we write it as $\mathbb{G}_a^n : ALG \to SETS$ (and we write $\mathbb{G}_a$ when $n = 1$). Thus $\mathbb{G}_a(A) = A^n$.

The two-dimensional projective space $\mathbf{P}^2(K)$ for a field $A = K$ is the set of lines passing through the origin $(0, 0, 0)$ in the affine space K^3; therefore, the line $\ell \subset K^3$ is just $K \cdot (X, Y, Z) \subset K^3$ for a generator $(X, Y, Z) \neq (0, 0, 0)$. The generator (X, Y, Z) is unique up to scalar multiplication; so, the ratio really matters; so, we write $(X{:}Y{:}Z)$ for the equivalence class (up to scalar multiplication) of (X, Y, Z). For example, if $z \neq 0$, $(\frac{x}{z}, \frac{y}{z}, 1)$ is unique; so, writing $D_z = D_z(K) = \{(x{:}y{:}z) \in \mathbf{P}^2(K) | z \neq 0\}$, $D_z \cong K^2$, and $\mathbf{P}^2(K) = D_x \cup D_y \cup D_z$ (where if $K = \mathbb{C}$, $D_?$ gives a chart of the two dimensional complex manifold $\mathbf{P}^2(\mathbb{C})$). Give yourself a homogeneous equation, say, $Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3$ with $g_j \in K$. Note that writing $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$, the zero set

$$E(K) := \{(X{:}Y{:}Z) | Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3\} \subset \mathbf{P}^2(K)$$

intersected with $D_z \cong \mathbb{G}_a^2(K)$ is just $\{(x, y) \in K^2 | y^2 = 4x^3 - g_2x - g_3\}$. The point outside $E(K) \cap D_z$ has coordinate $(X{:}Y{:}0)$, which implies $X = 0$ by the equation; so, $E(K) = \{(0{:}1{:}0)\} \sqcup (E(K) \cap D_z)$. More generally, $P^j(K)$ is the set of lines in K^{j+1} passing through the origin, and writing the generator as $(x_0{:}\cdots{:}x_j)$, we call it the homogeneous coordinate of $\mathbf{P}^j(K)$. In particular, $\mathbf{P}^1(K) = K \sqcup \{\infty\}$ by $(x{:}y) \mapsto x/y$ (defining $x/y = \infty$ if $y = 0$).

Fix a base commutative ring B. For a general B-algebra A, a line ℓ in A^{j+1} is first of all an A-submodule of A^{j+1} and secondly is supposed to induce a line generated

by one element after localization $\ell_P = \ell \otimes_A A_P$ for each maximal ideal P of A (i.e, ℓ_P is A_P-free of rank 1 and A_P^{j+1}/ℓ_P is also A_P-free). Then again $\mathbf{P}^j(A)$ is the set of such lines in the affine space A^{j+1}, though each line may not have a single generator over A. The association $A \mapsto \mathbf{P}^j(A)$ is a covariant functor from B-algebras into sets. Here $\sigma \in \mathrm{Hom}_{ALG}(A, A')$ induces $\sigma : \mathbf{P}^j(A) \to \mathbf{P}^j(A')$ by $\ell \mapsto \sigma(\ell)$ giving covariant functoriality. We define

$$D_?(A) = \{\ell \in \mathbf{P}^2(A) | \text{the projection to ?-coordinate induces a surjection } \ell \to A\}$$

for $? = X, Y, Z$. Then $\ell \cong A$ by projection to the ?-coordinate; so, ℓ has a generator (X, Y, Z) over A. Thus on $D_?(A)$, the homogeneous coordinate has meaning (warning: $\mathbf{P}^2(A)$ may not be equal to $D_x(A) \cup D_y(A) \cup D_z(A)$ in general). Anyway, assuming $g_2, g_3 \in B$, we thus have

$$(D_z \cap E)(A) = \{(x, y, 1) | y^2 = 4x^3 - g_2x - g_3\},$$

which is a covariant functor from the category $ALG_{/B}$ of B-algebras into sets. Let $\mathrm{Hom}_{ALG_{/B}}(R, A)$ denote the set of B-algebra homomorphisms: $R \to A$ for B-algebras R and A. Then it is easy to see

$$\{(x, y) | y^2 = 4x^3 - g_2x - g_3\} \cong \mathrm{Hom}_{ALG_{/B}}(B[x, y]/(y^2 - (4x^3 - g_2x - g_3)), A)$$

by $(\phi(x), \phi(y)) \leftrightarrow \phi \in \mathrm{Hom}_{ALG_{/B}}(B[x, y]/(y^2 - (4x^3 - g_2x - g_3)), A)$, since

$$0 = \phi(y^2 - (4x^3 - g_2x - g_3)) = \phi(y^2) - 4\phi(x)^3 + g_2\phi(x) + g_3.$$

A covariant functor F from the category $ALG_{/B}$ into sets is called *representable* if $A \mapsto F(A)$ can be identified with $A \mapsto \mathrm{Hom}_{ALG_{/B}}(R, A)$, where $\mathrm{Hom}_{ALG_{/B}}(R, A)$ is the set of all B-linear algebra homomorphisms of R into A. This means that we have a bijection $\phi_A : F(A) \to h_R(A) := \mathrm{Hom}_{ALG_{/B}}(R, A)$ for each B-algebra A, and for any $\varphi \in \mathrm{Hom}_{ALG_{/B}}(A, A')$, the covariant functorial action $F(\varphi) : F(A) \to F(A')$ commutes with that of h_R; more precisely, the following diagram is commutative for each triple (A, A', φ) ($\varphi \in \mathrm{Hom}_{ALG_{/B}}(A, A')$):

$$\begin{array}{ccc} F(A) & \xrightarrow{\phi_A} & h_R(A) \\ {\scriptstyle F(\varphi)}\downarrow & & \downarrow{\scriptstyle h_R(\varphi)} \\ F(A') & \xrightarrow[\phi_{A'}]{} & h_R(A'), \end{array}$$

where $h_R(\varphi)(x) = \varphi \circ x : R \xrightarrow{x} A \xrightarrow{\varphi} A'$ (the composite) for $x \in h_R(A)$. The functor $\mathbb{G}^n_{a/B}$ is representable by $R = B[X_1, \ldots, X_n]$ (the n-variable polynomial ring), as

$$h_R(A) = \mathrm{Hom}_{ALG_{/B}}(B[X_1, \ldots, X_n], A) \cong \mathbb{G}^n_a(A) \text{ by } \phi \mapsto (\phi(X_1), \ldots, \phi(X_n)) \in A^n.$$

Because of this, we write $\mathbb{G}^n_{a/B} = \mathrm{Spec}(B[X_1, \ldots, X_n])$ as schemes (which just means that $\mathbb{G}^n_a$ is representable by the ring $B[X_1, \ldots, X_n]$). Thus $A \mapsto (D_z \cap E)(A)$ is representable by $R = B[x, y]/(y^2 - (4x^3 - g_2x - g_3))$; so,

$$D_z \cap E = \mathrm{Spec}(B[x, y]/(y^2 - (4x^3 - g_2x - g_3))).$$

In this course, Spec(R) just means the covariant functor $h_R : ALG_{/B} \to SETS$, nothing more.

A natural transformation $\psi : h_{R'} \to h_R$ is a collection of maps $\psi_A : h_{R'}(A) \to h_R(A)$ indexed by $A \in ALG_{/B}$ satisfying the above diagram replacing ϕ_A by ψ_A and F by $h_{R'}$. We write $\mathrm{Hom}_{COF}(h_{R'}, h_R)$ for the collection of all natural transformations. By Yoneda's lemma (covered by Math 210 series), $\psi \in \mathrm{Hom}_{COF}(h_{R'}, h_R)$ is induced by $\psi^* \in \mathrm{Hom}_{ALG_{/B}}(R, R')$ in the following way: $\psi_A(x) = x \circ \psi_*$. Thus $\mathrm{Hom}_{COF}(h_{R'}, h_R)$ is in bijection with $\mathrm{Hom}_{ALG_{/B}}(R, R')$ and hence is a set! This fact we can write as

$$\mathrm{Hom}_{COF}(\mathrm{Spec}(R'), \mathrm{Spec}(R)) = \mathrm{Hom}_{ALG_{/B}}(R, R').$$

This identification also gives a way of studying $\mathrm{Hom}_{ALG_{/B}}(R, R')$ from a quite different point of view; so, if you have not finished Math 210, just believe Yoneda's lemma (or find a proof of it), and please be attentive when your teacher covers Yoneda's lemma in Math 210 (as often new graduate students have weak understanding of this tautological lemma). If you have finished Math 210, take a look again at your notes about the lemma (possibly stated in a more genral setting) to recall the proof, as this will be used repeatedly in the course.

Contents

1. Overview

In the first two/three weeks, we describe different definitions of modular forms without going into technical details. We start analytic/classical definition (going back to Gauss/Eisenstein) and then convert it into an algebraic one valid over any base ring.

Starting with the third or fourth week, we go into the second part dealing with p-adic deformation theory of modular forms, and we start to fill in more details (trying to be at elementary levels of [LFE]). The word: "elementary level" include good knowledge of number fields (including its integer ring, Galois theory, ramification theory and non-archimedean completions; i.e., p-adic integers) and function theory (including compact/non-compact Riemann surfaces). We follow [LFE] Chapter 5–7.

Let $\mathfrak{H} = \{z \in \mathbb{C} | \operatorname{Im}(z) = \frac{z-\overline{z}}{2\sqrt{-1}} > 0\}$ and

$$GL_1(R) = \mathbb{G}_m(R) = R^\times \text{ and } GL_2(R) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) | ad - bc \in R^\times \right\}$$

for each commutative ring R. We embed GL_1 into GL_2 by sending a to the scalar matrix $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ and write its image as $Z(R)$ (the center of $GL_2(R)$). Thus these objects are not just groups but functors from the category of commutative rings into that of groups (so, group functors). If you do not know much about functors, for the moment, just take them as an association sending a ring R to a group (including compatibility with ring homomorphisms). Since $\operatorname{Hom}_{ALG}(\mathbb{Z}[t,t^{-1}], R) = R^\times$ by $\phi \mapsto \phi(t)$, we have $\mathbb{G}_m$ is representable and $\mathbb{G}_m = \operatorname{Spec}(\mathbb{Z}[t,t^{-1}])$ for a variable t. Similarly $GL_2 = \operatorname{Spec}(\mathbb{Z}[a,b,c,d,\frac{1}{ad-bc}])$. Category theory covered by Math 210 series is sufficient in this course.

Note that by sending $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ to $\frac{ai+b}{ci+d}$ for $i = \sqrt{-1} \in \mathfrak{H}$, we have $GL_2(\mathbb{R})/Z(\mathbb{R})O_2(\mathbb{R}) = SL_2(\mathbb{R})/SO_2(\mathbb{R}) \cong \mathfrak{H}$ (check this for yourself). Here $O_2(R) = \{x \in GL_2(R) | x^t x = 1\}$ and $SO_2(R) = \{x \in O_2(R) | ad - bc = 1\}$.

In some sense, class field theory for a given number field F is an analysis of continuous homomorphisms of $\pi : \operatorname{Gal}(\overline{\mathbb{Q}}/F) \to GL_1(R)$ for a profinite ring R. If R is finite and $F = \mathbb{Q}$, by composing with any homomorphism $\varphi : GL_1(R) \to GL_1(\mathbb{C})$, we get a Dirichlet character $\chi = \varphi \circ \pi$ and the associated Dirichlet L-function $L(s,\chi) = \sum_{n=1}^\infty \chi(n) n^{-s}$, regarding $\chi : \mathbb{Z} \to \mathbb{C}$ as a multiplicative map. Here for a prime l unramified for π (i.e., unramified in the fixed field K of $\operatorname{Ker}(\pi)$), $\chi(l) = \varphi(\pi(Frob_l))$ for the Frobenius substitution $Frob_l \in \operatorname{Gal}(K/\mathbb{Q})$ (see take a look at your algebraic number theory book about $Frob_l$). If l ramifies in $K/\mathbb{Q}$, we just put $\chi(l) = 0$. Then for any positive n with prime decomposition $n = \prod_l l^e$, $\chi(n) = \prod_l \chi(l)^e$. Note that $\chi(m) = \chi(n)$ if $m \equiv n \bmod N$ for some positive integer N (if you know class field theory, ask why). By the way, $(2\pi)^{-s}\Gamma(s)L(s,\chi) = \int_0^\infty \phi_\chi(\exp(-2\pi y)) y^{s-1} dy$ for a rational function ϕ_χ on $\mathbb{G}_m$ (a rational function on $\mathbb{G}_m = \operatorname{Spec}(\mathbb{Z}[t,t^{-1}])$ is an element in the field of fractions of $\mathbb{Z}[t,t^{-1}]$). Indeed, $\phi_\chi(t) = \sum_{n=1}^\infty \chi(n) t^n$ which is equal to $\frac{\sum_{a=1}^N \chi(n) t^a}{1-t^N}$ (a rational function of t; i.e., a ratio of polynomials in t).

Similarly to this, if we start with a Galois representation $\rho : \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(R)$ for a p-adic local ring R such that $\det(c) = -1$ for complex conjugation $c \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we can find a p-adic cusp form f on $GL(2)$, thanks to the solution of Serre's mod p modularity conjecture by Khare–Wintenberger in 2008–2010, such that the q-expansion of f is given by $\sum_{n=1} a_n q^n$ with $a_l = \operatorname{Tr}(\rho(Frob_l))$, for unramified primes l for ρ. If

further R is a $\mathbb{Z}_p$-algebra (free of finite rank over $\mathbb{Z}_p$) and ρ is geometric (of sufficiently high weight), in most cases, f is really classical coming from a line bundle over a modular curve $X_{/\mathbb{Q}}$ (thanks to the solution of Fontaine–Mazur conjecture by Kisin and Emerton after the solution of Serre's mod p modularity conjecture). Here a variety $V_{/\mathbb{Q}}$ is a zero set of a finitely many homogeneous polynomials in $\mathbb{Q}[X_0, \ldots, X_n]$ in a projective space $\mathbf{P}^n_{/\mathbb{Q}}$. If V has dimension 1; i.e., $V(\mathbb{C}) \subset \mathbf{P}^n(\mathbb{C})$ (the same zero set in the complex projective space) removed finitely many points is an open Riemann surface, we call V a curve. Note that as a complex Riemann surface, $X(\mathbb{C}) = \Gamma\backslash GL_2(\mathbb{R})/Z(\mathbb{R})SO_2(\mathbb{R})$ for a discrete subgroup $\Gamma \subset GL_2(\mathbb{Z})$, where $Z(R)$ is made of scalar matrices in $GL_2(R)$. The Riemann surface $X(\mathbb{C})$ can be canonically embedded into $\mathbf{P}^N(\mathbb{C})$ and actually defined over $\mathbb{Q}$ (see [IAT] Chapter 6).

Thus the theory of elliptic modular forms is a natural $GL(2)$-version of class field theory. Langlands (and others) made a precise conjecture for reductive general algebraic groups G, and for a (geometric) Galois representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to G^L(R)$ (for the Langlands dual group G^L), we expect to associate an automorphic form (classical or p-adic) on $G(F_{\mathbb{A}})$. We hope that all Galois representations with finite set of ramification primes would be obtained as a p-adic limit of automorphic Galois representation (deformation theory). If $G = GL(n)$, G is self dual; i.e, $G^L = G$. We have good portion of Langlands theory/conjectures established for $GL(2)_{/\mathbb{Q}}$ in the last decade (though it is far from completion).

In this course, we give first analytic definition of modular forms on GL_2, then make it somewhat algebraic and describe the p-adic deformation theory of modular forms and their Galois representations.

1.1. **Automorphic forms.** Classically, modular/automorphic forms are defined as an analytic function: $\mathfrak{H} \to \mathbb{C}$ with some invariance property under a discrete subgroup Γ of $GL_2(\mathbb{R})$. Note that $GL_1(\mathbb{R}) = \mathbb{R}_+ \sqcup \mathbb{R}_-$ is a disjoint union of positive/negative number lines $\mathbb{R}_\pm$; so, it has two connected components. Since the determinant map $\det : GL_n(\mathbb{R}) \to GL_1(\mathbb{R})$ is onto (and continuous), $GL_n(\mathbb{R}) = GL_n(\mathbb{R})^+ \sqcup GL_n(\mathbb{R})^-$ is a disjoint union of matrices with positive and negative determinants. Actually $GL_n(\mathbb{R})^\pm$ is connected (prove this fact).

For $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{R})$, we define $g(z) := \frac{az+b}{cz+d}$ for $z \in \mathbb{C} \setminus \mathbb{R} = \mathfrak{H} \sqcup \overline{\mathfrak{H}}$. Note that

$$g\left(\begin{smallmatrix} z \\ 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} az+b \\ cz+d \end{smallmatrix}\right) = \left(\begin{smallmatrix} g(z) \\ 1 \end{smallmatrix}\right) j(g,z) \text{ for } j(g,z) = cz + d. \tag{1.1}$$

Thus for $g, h \in GL_2(\mathbb{R})^+$,

$$\left(\begin{smallmatrix} g(h(z)) \\ 1 \end{smallmatrix}\right) j(g, h(z)) j(h,z) = g\left(\begin{smallmatrix} h(z) \\ 1 \end{smallmatrix}\right) j(h,z) = gh\left(\begin{smallmatrix} z \\ 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} gh(z) \\ 1 \end{smallmatrix}\right) j(gh,z).$$

So we get

$$(gh)(z) = g(h(z)) \quad \text{and} \quad j(gh,z) = j(g,h(z))j(h,z) \tag{1.2}$$

Thus $GL_2(\mathbb{R})$ acts on $\mathbb{C} \setminus \mathbb{R}$. The action is transitive on $\mathbb{C} \setminus \mathbb{R}$ as $\left(\begin{smallmatrix} y & x \\ 0 & 1 \end{smallmatrix}\right)(i) = x + iy$ with $y \neq 0$ ($i = \sqrt{-1}$). Here the action is transitive if any two points are sent each other by the action. The above equation tells us that any element in $\mathbb{C} \setminus \mathbb{R}$ is the image of i; so, the action is transitive. Thus $\mathbb{C} \setminus \mathbb{R} = GL_2(\mathbb{R})/K$ for $K = \{g \in GL_2(\mathbb{R}) | g(i) = i\}$.

Consider $SO_2(\mathbb{R}) = \{r(\theta)|\theta \in \mathbb{R}\}$ for $r(\theta) = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix}$ which is isomorphic to the unit circle $S^1 = \{e^{i\theta}|\theta \in \mathbb{R}\}$.

Exercise 1.1. *Verify $K = Z(\mathbb{R})SO_2(\mathbb{R})$, and by using this, prove $SL_2(\mathbb{R})$ is connected (as a real C^∞ manifold). Further prove that $GL_2(\mathbb{R})^+$ is connected.*

Let Γ be a discrete subgroup of $SL_2(\mathbb{R})$ such that $\Gamma\backslash\mathfrak{H}$ has finite volume under the measure $y^{-2}dxdy$ for the coordinate $z = x + iy$ of $\mathfrak{H}$. Any subgroup of finite index in $SL_2(\mathbb{Z})$ has this property, because, as is well known, $SL_2(\mathbb{Z})\backslash\mathfrak{H}$ is identical to the following set

$$\Phi = \{z \in \mathfrak{H} : |z| \geq 1, |\operatorname{Re}(z)| \leq 1\} \tag{1.3}$$

up to measure 0 set, and obviously $\int_\Phi y^{-2}dxdy < \infty$ (compute the exact value of $\int_\Phi y^{-2}dxdy$). If the group Γ contains $\Gamma(N) = \operatorname{Ker}(SL_2(\mathbb{Z}) \xrightarrow{\text{mod } N} SL_2(\mathbb{Z}/N\mathbb{Z}))$ for some integer N, Γ is called a congruence subgroup.

Exercise 1.2. *Is there other examples of Γ as above, which are not inside $SL_2(\mathbb{Z})$?*

Note that for $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{R})$, we have

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} z & w \\ 1 & 1 \end{smallmatrix}\right) = \begin{pmatrix} g(z) & g(w) \\ 1 & 1 \end{pmatrix}\begin{pmatrix} j(g,z) & 0 \\ 0 & j(g,w) \end{pmatrix}.$$

Taking $w = \overline{z}$ and compuing the determinant of the above identity, we get

$$\det(g)\operatorname{Im}(g(z)) = \operatorname{Im}(z)|j(g,z)|^{-2}. \tag{1.4}$$

A holomorphic automorphic form on Γ of weight $k \in \mathbb{Z}$ is a holomorphic function $f : \mathfrak{H} \to \mathbb{C}$ such that

(M1) $f(\gamma(z)) = f(z)j(\gamma, z)^k$ for all $\gamma \in \Gamma$;
(M2) $|f(\alpha(z))\operatorname{Im}(\alpha(z))^{k/2}| = O(\operatorname{Im}(\alpha(z))^{k/2})$ for all $\alpha \in SL_2(\mathbb{Z})$.

Note by (1.4), $z \mapsto |f(z)\operatorname{Im}(z)^{k/2}|$ factors through $\Gamma\backslash\mathfrak{H}$ and hence (M2) makes sense.

Exercise 1.3. *Define $f|\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)(z) = \det\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)^w f(\frac{az+b}{cz+d})(cz+d)^{-k}$ for $w \in \mathbb{R}$. Prove the following facts:*

(1) $(f|\alpha)|\beta = f|(\alpha\beta)$ *for* $\alpha \in GL_2(\mathbb{R})^+$,
(2) *if f satisfies (M1), $f|\alpha$ satisfies (M1) replacing Γ by $\Gamma = \alpha^{-1}\Gamma\alpha$.*

If we impose on f the fast decreasing condition: $|f(\alpha(z))\operatorname{Im}(\alpha(z))^{k/2}| = O(1)$ as $\operatorname{Im}(z) \to \infty$ for all $\alpha \in SL_2(\mathbb{Z})$ in (2) above, we call f a cusp form.

Exercise 1.4. *Are there an example of Γ of finite index in $SL_2(\mathbb{Z})$ which is* **not** *a congruence subgroup?*

Write $S_k(\Gamma)$ (resp. $G_k(\Gamma)$) for the vector space of holomorphic cusp forms (resp. holomorphic automorphic forms) on Γ of weight k. If Γ is a congruence subgroup, we use the term "elliptic modular form" in place of "automorphic form" following the tradition started from Gauss. This is basically because elliptic modular form is a "function" defined over isomorphism classes of elliptic curves. So, general automorphic form is not

necessarily a function of isomorphism classes of specific algebro-geometric objects. This point is very important to define purely algebraically elliptic modular forms.

There is another diffeo-geometric interpretation of automorphic forms. If $f(z)$ is a cusp form of weight 2, then $\omega(f) = f(z)dz$ is invariant under Γ as $d\gamma(z) = j(\gamma, z)^{-2}dz$ by computation. If $Y(\Gamma) := \Gamma\backslash\mathfrak{H}$ is a Riemann sphere, then there are no non-trivial holomorphic differential forms on $Y(\Gamma)$ as $Y(\Gamma)$ is simply connected. Thus if $Y(\Gamma)$ is a Riemann sphere, $S_2(\Gamma) = 0$. There is a similar interpretation for higher weight modular forms as vector valued differential forms (see [IAT] Chapter 8).

Since $SL_2(\mathbb{Z})$ contains $\alpha = \alpha(1) = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, the side lines of Φ defined by $\mathrm{Re}(z) = \pm\frac{1}{2}$ are identified by α. Similarly by $\tau = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, the quarter unit circle left of the line $\mathrm{Re}(z) = 0$ is identified with the right one, $Y(1) := SL_2(\mathbb{Z})\backslash\mathfrak{H}$ is isomorphic to the Riemann sphere punctured at ∞; so, by filling ∞, we get $X(1) := Y(1) \sqcup \{\infty\} \cong \mathbf{P}^1(\mathbb{C})$; in other words, $SL_2(\mathbb{Z})\backslash\mathfrak{H} \cong \mathbf{P}^1(\mathbb{C}) \setminus \{\infty\}$. Since a cusp form on $SL_2(\mathbb{Z})$ extends to $X(1)$, again $S_2(SL_2(\mathbb{Z})) = 0$.

There is a function theoretic interpretation of automorphic forms. If you knows well homotopy theory of Riemann surfaces $\mathcal{R}$ (or more generally, theory of complex manifolds), $\mathcal{R} = \pi_1^{top}(\mathcal{R})\backslash U$ for the universal covering space U of $\mathcal{R}$. In our setting $U = \mathfrak{H}$, $\mathcal{R} = Y(\Gamma)$ and $\pi_1^{top}(Y(\Gamma)) = \Gamma$ (strictly speaking $\pi_1^{top}(Y(\Gamma)) = \overline{\Gamma} = \Gamma\{\pm 1\}/\{\pm 1\}$ but usually $\overline{\Gamma} \cong \Gamma$). Any non-vanishing function $J : \pi_1^{top}(\mathcal{R}) \times U \to \mathbb{C}^\times$ holomorphic in the variable $z \in U$ satisfies the cocycle relation $J(\alpha\beta, z) = J(\alpha, \beta(z))J(\beta, z)$ for all α, β in $\pi_1^{top}(\mathcal{R})$ and $z \in U$ gives rise to a line bundle in the following way. Let $\gamma \in \pi_1^{top}(\mathcal{R})$ act on $U \times \mathbb{C}$ by $\gamma(z, v) = (\gamma(z), J(\gamma, z)v)$. Then by the cocycle relation, $(\alpha\beta)(z, v) = \alpha(\beta(z, v))$ as easily verified; so, the quotient $L = \pi_1^{top}(\mathcal{R})\backslash(U \times \mathbb{C})$ gives rise to a covering $V \twoheadrightarrow \mathcal{R}$ by $(z, v) \mapsto z$ of complex manifolds whose fiber is isomorphic to $\mathbb{C}$; so, V is a line bundle over $\mathcal{R}$. Any section $f : \mathcal{R} \to V$ pulled back to a function on U satisfies $f(\alpha(z)) = f(z)J(\alpha, z)$ for all $\alpha \in \pi_1^{top}(\mathcal{R})$. Thus writing $\underline{\omega}^k$ for the invertible sheaf associated to $J(\gamma, z) = j(\gamma, z)^k$, we have $G_k(\Gamma) = H^0(X(\Gamma), \underline{\omega}^k)$, where the right-hand side is the collection of all global sections of the line bundle associated to $j(\cdot, z)^k$. By function theory, $\dim H^0(X, \mathcal{L}) < \infty$ for any Riemann surface and any line bundle $\mathcal{L}$ (e.g., see Riemann-Roch theorem in the notes of 207b Winter 12). In particular, we have

$$\dim G_k(\Gamma) < \infty. \tag{1.5}$$

1.2. **Elliptic modular forms of level N.** Let

$$\Gamma_0(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \middle| c \equiv 0 \mod N \right\},$$
$$\Gamma_1(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) \middle| d \equiv 1 \mod N \right\}.$$

These are congruence subgroups of finite index in $SL_2(\mathbb{Z})$.

Exercise 1.5. *Let $\mathbf{P}^1(A)$ be the projective space of dimension 1 over a ring A. Prove $[SL_2(\mathbb{Z}) : \Gamma_0(N)] = |\mathbf{P}^1(\mathbb{Z}/N\mathbb{Z})| = N\prod_{\ell|N}(1 + \frac{1}{\ell})$ if N is square-free, where ℓ runs over all prime factors of N.* Hint: Let $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ acts on $\mathbf{P}^1(A)$ by $z \mapsto \frac{az+b}{cz+d}$ and show that this is a transitive action if $A = \mathbb{Z}/N\mathbb{Z}$ and the stabilizer of ∞ is $\Gamma_0(N)$.

Moreover, sending $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$ to $(d \bmod N) \in (\mathbb{Z}/N\mathbb{Z})^\times$ is a homomorphism of groups, whose kernel is plainly $\Gamma_1(N)$. Thus for any Dirichlet character χ modulo N, $\Gamma_0(N) \ni \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto \chi(d)$ is a character of $\Gamma_0(N)$.

Exercise 1.6. *Prove that* $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^\times$.

We let $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{C})$ acts on $\mathbf{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$ by $z \mapsto \frac{az+b}{cz+d}$ (by linear fractional transformation).

Exercise 1.7. *Prove the following facts:*

(1) *there are two orbits of the action of* $GL_2(\mathbb{R})$ *on* $\mathbf{P}^1(\mathbb{C})$*:* $\mathbf{P}^1(\mathbb{R})$ *and* $\mathfrak{H} \sqcup \overline{\mathfrak{H}}$*, where* $\mathfrak{H} = \{z \in \mathbb{C} | \operatorname{Im}(z) > 0\}$ *and* $\overline{\mathfrak{H}} = \{z \in \mathbb{C} | \operatorname{Im}(z) < 0\}$.
(2) $\gamma \in GL_2(\mathbb{R})$ *with* $\det(\gamma) < 0$ *interchanges the upper half complex plane* $\mathfrak{H}$ *and lower half complex plane* $\overline{\mathfrak{H}}$,
(3) *the upper half complex plane is isomorphic to* $SL_2(\mathbb{R})/SO_2(\mathbb{R})$ *by* $SL_2(\mathbb{R}) \ni g \mapsto g(\sqrt{-1}) \in \mathfrak{H}$.

Then $Y_0(N) = \Gamma_0(N)\backslash\mathfrak{H}$ is an open Riemann surface with hole at cusps. In other words, $X_0(N) = \Gamma_0(N)\backslash(\mathfrak{H} \sqcup \mathbf{P}^1(\mathbb{Q}))$ is a compact Riemann surface.

Exercise 1.8. *Show that* $SL_2(K)$ *acts transitively on* $\mathbf{P}^1(K)$ *for any field* K *by linear fractional transformation.* Hint: $\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)(0) = a$.

Let $f : \mathfrak{H} \to \mathbb{C}$ be a holomorphic functions with $f(z+1) = f(z)$. Since $\mathfrak{H}/\mathbb{Z} \cong D = \left\{z \in \mathbb{C}^\times \middle| |z| < 1\right\}$ by $z \mapsto q = \mathbf{e}(z) = \exp(2\pi i z)$, we may regard f as a function of q undefined at $q = 0 \Leftrightarrow z = i\infty$. Then the Laurent expansion of f gives

$$f(z) = \sum_n a(n, f) q^n = \sum_n a(n, f) \exp(2\pi i n z).$$

In particular, we may assume that q is the coordinate of $X_0(N)$ around the infinity cusp ∞. We call f is *finite* (resp. *vanishing*) at ∞ if $a(n, f) = 0$ if $n < 0$ (resp. if $n \leq 0$). By Exercise 1.8, we can bring any point $c \in \mathbf{P}^1(\mathbb{Q})$ to ∞; so, the coordinate around the cusp c is given by $q \circ \alpha$ for $\alpha \in SL_2(\mathbb{Q})$ with $\alpha(c) = \infty$.

Exercise 1.9. *Show that the above* α *can be taken in* $SL_2(\mathbb{Z})$. Hint: write $c = \frac{a}{b}$ as a reduced fraction; then, we can find $x, y \in \mathbb{Z}$ such that $ax - by = 1$.

Let $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a Dirichlet character. We define the subspace $G_k(\Gamma_0(N), \chi)$ made up of modular forms $f \in G_k(\Gamma_1(N))$ satisfying the following conditions:

(χ) $f(\frac{az+b}{cz+d}) = \chi(d) f(z)(cz+d)^k$ for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$.

We put $S_k(\Gamma_0(N), \chi) = G_k(\Gamma_0(N), \chi) \cap S_k(\Gamma_1(N))$. If $f \in G_k(\Gamma_0(N), \chi)$, N is called the level of f and χ is called Neben character (or Nebentypus) of f following Hecke.

If f satisfies the above conditions, we find that $f(z+1) = f(z)$ because $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)(z) = z+1$; so, we can say that f is finite or not at the cusps by q-expansion.

Exercise 1.10. (1) *If* $\alpha \in SL_2(\mathbb{Z})$ *and* $\Gamma \supset \Gamma(N)$*, show that* $\alpha^{-1}\Gamma\alpha$ *contains* $\Gamma(N)$.

By the above exercise, for $\alpha \in SL_2(\mathbb{Z})$, we find $f|\alpha(z+N) = f|\alpha(z)$; thus, $f|\alpha$ has expansion $f|\alpha = \sum_n a(n, f|\alpha) q^{Nn}$. We call f is finite (resp. vanishing) at the cusp $\alpha^{-1}(\infty)$ if $f|\alpha$ is finite (resp. vanishing) at ∞. Thus (M2) is equivalent to

(M2′) f is finite at all cusps of $X_0(N)$.

Replace (M2) by

(S) f is vanishing at all cusps of $X_0(N)$.

Then the boundedness condition $|f(\alpha(z))\,\mathrm{Im}(\alpha(z))^{k/2}| = O(1)$ for all $\alpha \in SL_2(\mathbb{Z})$ is equivalent to (S); so,we may define the subspace $S_k(\Gamma_0(N)) \subset G_k(\Gamma_0(N))$ by imposing (S).

Exercise 1.11. *Prove that* $G_k(\Gamma_1(N)) = \bigoplus_\chi G_k(\Gamma_0(N), \chi)$, *where* χ *runs over all Dirichlet characters modulo* N *with* $\chi(-1) = (-1)^k$.

1.3. **Elliptic modular forms classify elliptic curves.** We give algebro-geometric interpretation of elliptic modular forms now without any real proof. First, we give another analytic definition of modular forms more classical than the one we have given (this definition goes back to Gauss). Writing $w = {}^t(w_1, w_2)$ for two linearly independent complex numbers (with $\mathrm{Im}(z) > 0$ ($z = w_1/w_2$)), a weight k modular form is a holomorphic function f of w satisfying $f\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) w\right) = f(w)$ for $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ and $f(aw) = a^{-k} f(w)$ for $a \in \mathbb{C}^\times$. In other words, f is a "holomorphic" function on the set Lat of lattices in $\mathbb{C}$ with $f(aL) = a^{-k} f(L)$, regarding

$$SL_2(\mathbb{Z})\backslash \left\{ w := \left(\begin{smallmatrix} w_1 \\ w_2 \end{smallmatrix}\right) \middle| z \in \mathfrak{H} \right\} = Lat$$

via $w \mapsto L_w = \mathbb{Z}w_1 + \mathbb{Z}w_2$. If we regard f as a function of $z \in \mathfrak{H} = \{z \in \mathbb{C} | \mathrm{Im}(z) > 0\}$ by $f(z) = f\left(2\pi i \left(\begin{smallmatrix} z \\ 1 \end{smallmatrix}\right)\right)$, the two relations can be stated as a single one:

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

for $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$.

Exercise 1.12. *Give details of the reason why the two properties defining* $f : Lat \to \mathbb{C}$ *gives modular functional equation of* $f : \mathfrak{H} \to \mathbb{C}$ *in (M1).*

This latter definition is the one given in (M1). Here we put $2\pi i$ to define $f(z)$ to make the q-expansion of f rational if f is algebro-geometrically rational (since $f(2\pi i w) = (2\pi i)^{-k} f(w)$, this is just the division by a power of $(2\pi i)$). This has to be done because $\exp : \mathbb{C}/2\pi i(\mathbb{Z} + \mathbb{Z}z) \cong \mathbb{C}^\times/q^{\mathbb{Z}}$ for $q = \exp(2\pi i z)$.

We nows give an algebraic interpretation of modular forms. Without going into technicalities, we give an outline of how to define modular forms algebraically. Pick a lattice L in $\mathbb{C}$ (so, $L \in Lat$). If necessary, we choose a $\mathbb{Z}$-basis $w = (w_1, w_2) \in \mathbb{C}^2$ of L; so, $L = L_w = \mathbb{Z}w_1 + \mathbb{Z}w_2$. Writing u for the variable on $\mathbb{C}$, the quotient $\mathbb{C}/L$ of $\mathbb{C}$ by the lattice L gives rise to a pair $(E(L) = \mathbb{C}/L_w, \omega)_{/\mathbb{C}}$ of a Riemann surface of genus 1 and the holomorphic differential $\omega = du$. The differential ω is nowhere vanishing; i.e., for any point $\alpha \in \mathbb{C}$, $du = d(u-\alpha) \neq 0$ for the coordinate $u - \alpha$ around α. The Riemann surface $E(L) \cong \mathbb{C}/L_w$ can be embedded into $\mathbf{P}^2$ via $u \mapsto (x(u), y(u), 1) \in \mathbf{P}^2(\mathbb{C})$ by Weierstrass $\wp$-functions

$$x(u) = \wp(u; L_w) = \frac{1}{u^2} + \sum_{0 \neq l \in L_w} \left\{ \frac{1}{(u-l)^2} - \frac{1}{l^2} \right\} = \frac{1}{u^2} + \frac{g_2}{20}u^2 + \frac{g_3}{28}u^4 + \cdots$$

and $y = \frac{dx}{du}$, where

$$g_2(w) = 60 \sum_{0 \neq l \in L_w} l^{-4} \text{ and } g_3(w) = 140 \sum_{0 \neq l \in L_w} l^{-6}.$$

By this formula, plainly $g_j(aL) = a^{-2j} g_j(L)$; so, g_j is a modular from of weight $2j$ ($j = 2, 3$) as we see soon its q-expansion. Then the equation satisfied by x and y is $y^2 = 4x^3 - g_2 x - g_3$ and $\omega = du = \frac{dx}{y}$. Indeed, the right-hand-side $4x^3 - g_2 x - g_3$ is made so that the difference $y^2 - (4x^3 - g_2 x - g_3)$ does not have pole at 0, and hence $\varphi = y^2 - (4x^3 - g_2 x - g_3)$ is everywhere holomorphic function on the compact Riemann surface $\mathbb{C}/L$ which has to be constant. The constant can be computed to be 0 by looking at the constant term of the explicit expansion as above. Thus as long as $x(u) \neq \infty$ (i.e., $u \neq 0$), the coordinate $(x(u), y(u)) \in \mathbb{C}^2$ satisfies $y^2 = 4x^3 - g_2(L)x - g_3(L)$. By $\omega = \frac{dx}{y} = du$, ω is a nowhere vanishing differential.

To add the point $u = 0$ in this picture, we homogenize the equation and consider the homogeneous equation $Y^2 Z = 4X^3 - g_2 X Z^2 - g_3 Z^3$. To make things slightly more general, we suppose $g_j \in K$ for a field K. The two-dimensional projective space $\mathbf{P}^2(K)$ for a field $A = K$ is the set of lines in the affine space K^3; i.e., a line $\ell \subset K^3$ is just $K(X, Y, Z) \subset K^3$ for $(X, Y, Z) \neq (0, 0, 0)$. The generator (X, Y, Z) is unique up to scalar multiplication; so, the ratio really matters; so, we write $(X{:}Y{:}Z)$ the equivalence class (up to scalar multiplication) of (X, Y, Z). For example, if $z \neq 0$, $(\frac{x}{z}, \frac{y}{z}, 1)$ is unique; so, writing $D_z = \{(x, y, z) | z \neq 0\}$, $D_z \cong K^2$, and $\mathbf{P}^2(K) = D_x \cup D_y \cup D_z$ (where if $K = \mathbb{C}$, $D_?$ gives a chart of complex manifold $\mathbf{P}^2(\mathbb{C})$). Note that writing $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$, for the zero set $E(K) = \{(X{:}Y{:}Z) | Y^2 Z = 4X^3 - g_2 X Z^2 - g_3 Z^3\} \subset \mathbf{P}^2(K)$, we have $E(K) \cap D_z = \{(x, y) \in K^2 | y^2 = 4x^3 - g_2 x - g_3\}$. More generally, $P^j(K)$ is the set of lines in K^{j+1}, and writing the generator as $(x_0{:}\ldots{:}x_n)$, we call it the homogeneous coordinate of $\mathbf{P}^j(K)$. In particular, $\mathbf{P}^1(K) = K \sqcup \{\infty\}$ by $(x{:}y) \mapsto x/y$ (defining $x/y = \infty$ if $y = 0$). The point outside $E(K) \cap D_z$ has coordinate $(X{:}Y{:}0)$, which implies $X = 0$ by the equation; so, $E(K) = \{(0{:}1{:}0)\} \sqcup (E(K) \cap D_z)$.

Going back to the case $K = \mathbb{C}$, $u \mapsto (x(u), y(u))$ is not well defined at $u = 0$. However, for the homogeneous coordinate $(x(u){:}y(u){:}1) = (u^3 x(u){:}u^3 y(u){:}u^3)$ is defined for all $u \neq 0$ and the right-hand-side has meaning even when $u = 0$. Then from the explicit expansion, we see $(u^3 x{:}u^3 y{:}u^3)|_{u=0} = (0{:}-2{:}0) = (0{:}1{:}0)$. Thus $E(\mathbb{C})$ inside $\mathbf{P}^2(\mathbb{C})$ is exactly defined by the homogenized Weierstrass equation, and isomorphic to $\mathbb{C}/L$ as complex manifolds by $u \mapsto (u^3 x{:}u^3 y{:}u^3)$. In other words, $E(\mathbb{C})$ is the compactification adding one point $\mathbf{0} = (0{:}1{:}0)$ to the affine curve $E(\mathbb{C}) \cap D_z$ defined by $y^2 = 4x^3 - g_2 x - g_3$. An important point is that $E(\mathbb{C}) = \mathbb{C}/L$ is a compact abelian group with identity $\mathbf{0}$. Since $Y^2 Z = 4X^3 - g_2 X Z^2 - g_3 Z^3$ has degree 3, $E(\mathbb{C})$ has three intersection points P, Q, R with any line ℓ defined in $aX + bY + cZ = 0$ in $\mathbf{P}^2(\mathbb{C})$. The great discovery of Gauss and Abel in the early 19th century is that under the above setting, $P + Q + R = \mathbf{0}$. We can take this (along with $(x(-P), y(-P)) = (x(P), -y(P))$) to be the definition of the group law on $E(\mathbb{C})$.

For a more general field K, consider the zero set $E(K) \subset \mathbf{P}^2(K)$ of

$$Y^2 Z - (4X^3 - g_2 X Z^2 - g_3 Z^3) \quad (g_j \in K).$$

As long as $4X^3 - g_2XZ^2 - g_3Z^3 = 0$ has three distinct roots (in an algebraic closure K; i.e, its discriminant $\Delta = g_2^3 - 27g_3^2 \neq 0$), we can define an abelian group structure by putting $P + Q + R = \mathbf{0}$ (and $(x(-P), y(-P)) = (x(P), -y(P))$) if $\{P, Q, R\}$ is the intersection of a line with E (Abel's theorem; see 12W 207b lecture notes Section 2.1).

Fix a base ring B. Any homogeneous equation $f(X, Y, Z) \in B[X, Y, Z]$ gives rise to its zero set $C(A) = \{\ell \in \mathbf{P}^2(A) | f(\ell) = 0\}$ for any B-algebra A. Here $f(\ell) = 0$ means that $f(x, y, z) = 0$ for all $(x, y, z) \in \ell$. The association $A \mapsto C(A)$ is again a covariant functor from B-algebras to sets. Any B-algebra homomorphism $\sigma : A \to A'$ induces $\mathbf{P}^2(A) \xrightarrow{\sigma_*} \mathbf{P}^2(A')$ and brings $C(A)$ into $C(A')$. Since A is a B-algebra, we have the structure algebra homomorphism $i : B \to A$; so, applying i_* to any point $P \in C(B)$, we get a point $i_*P \in C(A)$ (which we just write P again). For any B-algebra homomorphism $\varphi : B \to B'$, we may regard f as a polynomial $\varphi_* f$ with coefficients in B' applying φ to coefficients of f. The curve defined by $\varphi_* f$ is written as $C \otimes_{B,\varphi} B'$ (the scalar extension of C to B' with respect to φ). We say C is geometrically irreducible if $\varphi_* f$ is irreducible for any algebra homomorphism $\varphi : B \to k$ into an algebraically closed field k. For a pair $(C, \mathbf{0} \in C(B))$ for geometrically irreducible C, the functor $A \mapsto C(A)$ is actually a functor from B-algebras into groups (in place of sets) with identity $\mathbf{0}$, C is called an elliptic curve. Geometrically, C is an elliptic curve if and only if it is a geometrically irreducible smooth curve of genus 1 (if we fix a point $\mathbf{0} \in C(B)$). Here smoothness is equivalent to $\Delta \in B^\times$ if C is defined by (the homogenized form of) the equation $y^2 - 4x^3 + g_2x + g_3 \in B[x, y]$ (assuming $\frac{1}{6} \in B$).

Over $\mathbb{C}$, we get $Lat \hookrightarrow \{(E, \omega)_{/\mathbb{C}}\}/\cong$ sending L to $E(\mathbb{C}) = \mathbb{C}/L$ defined by $Y^2Z = 4X^3 - g_2(L)XZ^2 - g_3(L)Z^3$. Here $(E, \omega) \cong (E', \omega')$ if we have an isomorphism $\varphi : E \to E'$ (of schemes) inducing $E \cap D_z \cong E' \cap D_z$ such that $\varphi^*\omega' = \omega$. The pair w (or lattice $L = L_w$) can be recovered by ω so that $w_i = \int_{\gamma_i} \omega$ for a basis (γ_1, γ_2) of the Betti homology group $H_1(E(\mathbb{C}), \mathbb{Z}) = \pi_1^{top}(E(\mathbb{C}))$. For a given $(E, \omega)_{/\mathbb{C}}$, we write L_E for its lattice. Thus by $E_{/\mathbb{C}} \mapsto L_E$, we confirm

$$Lat \cong \{(E, \omega)_{/\mathbb{C}}\}/\cong$$

Here $\mathbb{C}/L_w$ is an additive group, and this is the canonical group structure of $E(\mathbb{C})$. Thus $(E(L), a\omega)$ $(a \in \mathbb{C}^\times)$ corresponds to $aL \in Lat$; so, $g_j(E, a\omega) = a^{-2j} g_j(E, \omega)$ regarding g_j as a function of the pair (E, ω).

Conversely, start with a pair $(E, \omega)_{/B}$ with $\mathbf{0} = \mathbf{0}_E \in E(B)$ defined over the base ring B made of an elliptic curve and a nowhere vanishing differential ω. By smoothness, we have an algebraic parameter u around $\mathbf{0}$ so that $\omega = du$. If $6^{-1} \in B$, there is a unique way of finding a rational function $x : E \to \mathbf{P}^1$ with pole of order 2 at 0 such that $x(u) = u^{-2} +$ higher terms and for $y = \frac{dx}{du}$ (algebraic derivative), we find that the equation $y^2 = 4x^3 - g_2x - g_3$ defines $E(A) \subset \mathbf{P}^1(A)$ with $g_2, g_3 \in B$ for a unique pair $(g_2 = g_2(E, \omega), g_3 = g_3(E, \omega)) \in B^2$ (see §2.2 of the lecture notes of 207B in 2012 Winter or [GME] §2.2.6). Since $E_{/B}$ is smooth, this pair (g_2, g_3) has to satisfy $\Delta = g_2^3 - 27g_3^2 \in B^\times$ (the smoothness criterion of Weierstrass). If we change ω by $a\omega$ for $a \in B^\times$, $a\omega = d(au)$; and hence, (x, y) is replaced by $(x', y') = (a^{-2}x, a^{-3}y)$ whose expansion starting with $(qu)^{-2}$ and $-2(au)^{-3}$ respectively, and hence the equation of

(x', y') has to be

$$y'^2 = 4x'^3 - g_2 a^{-2} x' - a^{-6} g_3 \Leftrightarrow (a^{-3}y)^2 = 4(a^{-2}x)^3 - g_2 a^{-4} a^{-2} x - a^{-6} g_3.$$

This shows $g_j(E, a\omega) = a^{-2j} g_j(E, \omega)$ and

$$\wp(A) := [(E,\omega)_{/A}] \overset{\text{one-to-one and onto}}{\leftrightarrow} \{(g_2, g_3) \in A^2 | \Delta \in A^\times\} = \mathrm{Hom}_{ALG}(B[g_2, g_3, \frac{1}{\Delta}], A). \tag{1.6}$$

Here the ring $\mathbb{Z}[\frac{1}{6}][g_2, g_3]$ is a polynomial ring with variables g_2, g_3, and the straight brackets $[\cdot]$ indicates the set of isomorphism classes of the objects inside; so, $[(E,\omega)_{/A}] = \{(E,\omega)_{/A}\}/\cong$. The association $\wp : ALG_{/B} \to SETS$ is a covariant functor for a B-algebra homomorphism $\varphi : A \to A'$ with $\wp(\varphi)(E) = E \otimes_{A,\varphi} A'$ (and ω is sent to corresponding differential on $E \otimes_{A,\varphi} A'$). In other word, for any algebra homomorphism $A \overset{\phi}{\to} A'$, $\wp(A) \overset{\phi}{\to} \wp(A')$ is just induced by $\phi : \mathbf{P}^2(A) \to \mathbf{P}^2(A')$ as $\mathbf{P}^2(A)$ is the set of "lines" in the affine space A^3. Thus $A \mapsto \wp(A) = [(E,\omega)_{/A}]$ are isomorphic to $A \mapsto \mathrm{Hom}_{ALG}(\mathbb{Z}[\frac{1}{6}, g_2, g_3, \frac{1}{\Delta}], A)$ as covariant functors from B-algebras into sets; so, $\wp = \mathrm{Spec}(\mathcal{R})$ for $\mathcal{R} = B[g_2, g_3, \frac{1}{\Delta}]$. Note that $\mathrm{Hom}_{COF}(\wp, \mathbb{G}_a)$ is made of $f_A : \wp(A) \to A$ such that $f_A((E,\omega)_{/A}) \in A$ which only depends on the A-isomorphism class of (E,ω) and $f_A(\wp(\varphi)(E,\omega)) = \varphi(f_A(E,\omega))$ for any $\varphi \in \mathrm{Hom}_{ALG}(A, A')$. By Yoneda's lemma, $f \in \mathrm{Hom}_{ALG_{/B}}(B[X], \mathcal{R}) = \mathcal{R}$ by $\phi \mapsto \phi(X)$. In other words, $f = f(g_2, g_3) \in \mathcal{R}$ and $f(E,\omega) = f(g_2(E,\omega), g_3(E,\omega))$.

Returning to $A = \mathbb{C}$, an important fact is that all these functions g_2, g_3 and Δ have Fourier expansions in $\mathbb{Z}[\frac{1}{6}][[q]]$ for $q = \exp(2\pi i z)$. Indeed, g_2 and g_3 are rational multiple of the following Eisenstein series for $k > 2$:

$$E_k(z) := \frac{(k-1)!}{2(2\pi i)^k} \sum_{(m,n)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{(mz+n)^k} = \frac{1}{2}\zeta(1-k) + \sum_{n=1}^{\infty} q^n \sum_{0<d|n} d^{k-1} = \frac{1}{2}\zeta(1-k) + \sum_{(m,n)\in\mathbb{Z}^2\setminus\{(0,0)\}/\mathbb{Z}^\times, mn>0} q^{mn} \tag{1.7}$$

for even integers $2 < k \in \mathbb{Z}$. By this, $E_k \in G_k(SL_2(\mathbb{Z}))$. This follows from the partial fraction expansion of the cotangent function for $z = \frac{\log q}{2\pi i}$ (see any function theory book):

$$\frac{1}{z} + \sum_{n=1}^{\infty} \left\{ \frac{1}{(z+n)} + \frac{1}{(z+n)} \right\} = \pi \cot(\pi z) = \pi i \left\{ 1 - 2\sum_{n=1}^{\infty} q^n \right\}, \tag{1.8}$$

and its derivatives by $\left((2\pi i)^{-1}\frac{d}{dz}\right)^k = \left(q\frac{d}{dq}\right)^k$:

$$\sum_{n=-\infty}^{\infty} \frac{1}{(z+n)^k} = \frac{(-1)^k (2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} n^{k-1} q^n. \tag{1.9}$$

In particular, keeping the fact that $g_k(z) = g_k(2\pi i \left(\begin{smallmatrix} z \\ 1 \end{smallmatrix}\right))$, we find

$$g_2(q) = \frac{1}{12} + 20\sum_{n=1}^{\infty}\left\{\sum_{0<d|n} d^3\right\}q^n = \frac{1}{12} + 20\sum_{n=1}^{\infty}\frac{n^3q^n}{1-q^n},$$

$$g_3(q) = -\frac{1}{216} + \frac{7}{3}\sum_{n=1}^{\infty}\left\{\sum_{0<d|n} d^5\right\}q^n = -\frac{1}{216} + \frac{7}{3}\sum_{n=1}^{\infty}\frac{n^5q^n}{1-q^n}, \tag{1.10}$$

$$\Delta(q) = q\prod_{n=1}^{\infty}(1-q^n)^{24} \text{ (so, } \Delta(z) \neq 0 \text{ for all } z \in \mathfrak{H}).$$

To obtain the product expansion of Δ, one need to work a little more (see [IAT] (4.6.1)).

Similarly, by the same computation, for a primitive Dirichlet character $\chi \neq 1$ modulo N, a suitable constant multiple of

$$\sum_{(m,n)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{\chi(n)}{(mNz+n)^k|mNz+n|^{-2s}}|_{s=0}$$

has q-expansion

$$E_k(\chi) = \frac{1}{2}L(1-k,\chi) + \sum_{n=1}^{\infty} q^n \sum_{0<d|n}\chi(d)d^{k-1} \tag{1.11}$$

and gives an element in $G_k(\Gamma_0(N),\chi)$ for all $k \geq 1$ (see [MFM] Chapter 7). We can show the existence of $E_k(\chi) \in G_k(\Gamma_0(Np),\chi)$ even for imprimitive characters χ' modulo Np for a prime $p \nmid N$. Writing χ regarded defined modulo Np as χ_{Np} (so, $\chi_{Np}(n) = 0$ if $p|n$) First note, if $p|n$

$$\sum_{0<d|n}\chi_{Np}(d)d^{k-1} = \sum_{0<d|n,p\nmid d}\chi(d)d^{k-1} = \sum_{0<d|n}\chi(d)d^{k-1} - \chi(p)p^{k-1}\sum_{p|d|n}\chi(d)d^{k-1}$$

and

$$L(s,\chi_{Np}) = \prod_{l:\text{primes}}(1-\chi_{Np}(l)l^{-s})^{-1} = (1-\chi(p)p^{-s})L(s,\chi).$$

These facts tell us that $E_k(\chi_{Np}) := E_k(\chi)(z) - \chi(p)p^{k-1}E_k(\chi)(pz) \in G_k(\Gamma_0(Np),\chi)$, since $E_k(\chi)(pz) = E_k(\chi)|\alpha$ for $\alpha = \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$ (taking $w = 0$ in the notation of Exercise 1.3) and $\alpha^{-1}\Gamma_0(N)\alpha \supset \Gamma_0(Np) = \alpha^{-1}\Gamma_0(N)\alpha \cap \Gamma_0(N)$.

We can then think of the *Tate curve* $\mathrm{Tate}(q)$ defined over $\mathbb{Z}[\frac{1}{6}][[q]][q^{-1}]$ by the equation $Y^2Z - (4X^3 - g_2(q)XZ^2 - g_3(q)Z^3))$ with nowhere vanishing differential $\omega_{can} = \frac{dX}{Y}$. Let μ_N is the group of N-th roots of unity; so, as a functor, $\mu_N(R) = \{\zeta \in R^\times | \zeta^N = 1_R\}$ for any commutative ring R. Note that $\mathrm{Hom}_{ALG}(\mathbb{Z}[t,t^{-1}]/(t^N-1),R) = \mu_N(R)$ by sending t to $\phi(t) \in \mu_N(R)$; so, $\mu_N = \mathrm{Spec}(\mathbb{Z}[t,t^{-1}]/(t^N-1))$. As shown by Tate (see [GME] Section 2.5), we have a canonical embedding

$$\mathrm{Tate}(q)(\overline{\mathbb{Q}}_p[[q]]) \supset (\overline{\mathbb{Q}}_p[[q]])^\times/q^{\mathbb{Z}},$$

we have therefore a natural inclusion $\phi_{N,can} : \mu_N(\overline{\mathbb{Q}}_p) \hookrightarrow \mathrm{Tate}(q)[N]$, (which comes from a natural transformation of group functors $\mu_N \to \mathrm{Tate}(q)$; see [GME] §1.6.4). Tate curve is not an elliptic curve over $\mathbb{Z}[\frac{1}{6}][[q]]$ but is an elliptic curve over $\mathbb{Z}[\frac{1}{6}][[q]][q^{-1}]$ because the non-unit q is a factor of the discriminant $\Delta(q)$ of the elliptic curve.

For general elliptic curve E over a B-algebra A, a *level* $\Gamma_1(N)$ *structure* is an embedding $\phi_N : \mu_N \hookrightarrow E[N]$ of finite flat group schemes (i.e., a group embedding of functors). For the first reading, if the reader is not familiar with the theory of group schemes, just assume $N = 1$ to forget about ϕ_N. If the triple (E, ϕ_N, ω) is all defined over A, we call $(E, \phi_N, \omega)_{/A}$ a *test object* over A. The elements g_2, g_3, Δ in $\mathbb{Z}[g_2, g_3]$ is a function of pairs $(E, \omega)_{/A}$ of an elliptic curve E and a differential ω defined over A with values in A and can be considered as a function of test objects (E, ϕ_N, ω) disregarding ϕ_N. This motivates the following algebraic definition of B-integral elliptic modular forms of level $\Gamma_1(N)$ as functions of test objects $(E, \phi_N : \mu_N \hookrightarrow E[N], \omega)$ satisfying the following conditions:

(G0) f assigns a value $f((E, \phi_N, \omega)_{/A}) \in A$ for each test object

$$(E, \phi_N : \mu_N \hookrightarrow E[N], \omega)_{/A}$$

defined over an B-algebra A. Here A is also a variable (running over the category of B-algebras).

(G1) $f((E, \phi_N, \omega)_{/A}) \in A$ depends only on the isomorphism class of $(E, \phi_N, \omega)_{/A}$.

(G2) If $\varphi : A \to A'$ is an B-algebra homomorphism, we have

$$f((E, \phi_N, \omega)_{/A} \otimes A') = \varphi(f((E, \phi_N, \omega)_{/A})),$$

where $(E, \phi_N, \omega)_{/A} \otimes A'$ means that we regard $(E, \phi_N, \omega)_{/A}$ as defined over A' via φ (so, for example, if $N = 1$, $(E, \omega) \otimes A'$ is defined by the equation $y^2 = 4x^3 - \varphi(g_2(E, \omega))x - \varphi(g_3(E, \omega))$).

(G3) $f((E, \phi_N, a \cdot \omega)_{/A}) = a^{-k} f(E, \phi_N, \omega)$ for $a \in A^\times$.

(G4) $f(q) = f((\mathrm{Tate}(q), \phi_N, \omega_{can})_{/A[[q^{1/d}]][q^{-1/d}]}) \in A[[q^{1/d}]]$ for any level N-structures ϕ_N on $\mathrm{Tate}(q)$ defined over $A[[q^{1/d}]][q^{-1/d}]$ with $d|N$. In particular, we have

$$f(q) = f((\mathrm{Tate}(q), \phi_{N,can}, \omega_{can})_{/B[[q]][q^{-1}]}) \in B[[q]].$$

Here, if N is invertible in B and B contains all N-th roots of unity, $\mathbb{Z}/N\mathbb{Z} \cong \mu_N$ over B, and we can think of a level $\Gamma_1(N)$-structure $\phi_N^{\mathrm{et}} : \mathbb{Z}/N\mathbb{Z} = \mu_N \cong q^{1/N\mathbb{Z}}/q^{\mathbb{Z}} \subset \mathrm{Tate}(q)[N]$, which is defined over $B[[q^{1/N}]][q^{-1/N}]$. More generally, if $N = dN'$ with d prime to N', assuming $\frac{1}{d} \in B$ and that B contains all d-th roots of unity, we can think of

$$\phi_N = \phi_d^{\mathrm{et}} \times \phi_{N',can} : \mu_N = \mathbb{Z}/d\mathbb{Z} \times \mu_{N'} \hookrightarrow \mathrm{Tate}(q),$$

which is defined over $B[[q^{1/d}]][q^{-1/d}]$.

The space of modular forms defined by the conditions (G0–4) will be written as $G_k(N; B) = G_k(\Gamma_1(N); B)$. By definition, for $f \in G_k(N; B)$ and $g \in G_l(N; B)$, the product $f \cdot g(E, \phi_N, \omega) = f(E, \phi_N, \omega) \cdot g(E, \phi_N, \omega)$ belongs to $G_{k+l}(N; B)$. Thus $G_N(B) = \bigoplus_k G_k(N; B)$ is a graded ring. For $f \in G_k(1; B)$, just putting $f(E, \phi_N, \omega) = f(E, \omega)$ forgetting ϕ_N, we may consider $G_k(1; B)$ as a subspace of $G_k(N; B)$. Put $\mathcal{R}_N(B) =$

$G_N(B)[\frac{1}{\Delta}]$. Then $\mathcal{R}_N(B)$ is a ring containing $\mathcal{R}$ as a subalgebra. The following fact is known (e.g., [GME] §2.6.2):

Theorem 1.13. *The functor $\wp_N : ALG_{/\mathbb{Z}[\frac{1}{n(N)}]} \to SETS$ given by*

$$\wp_N(A) = \left[(E, \phi_N, \omega)_{/A}\right]$$

is representable by $\mathcal{R}_N(\mathbb{Z}[\frac{1}{n(N)}])$, where $n(N) = 6N$ if $N \le 3$ and otherwise $n(N) = N$.

When $N = 1$, we forget about ϕ_N as μ_1 is the trivial group. Thus there is no need to worry about the level structure ϕ_N of Tate(q). The condition (G0-2) implies $f \in \mathrm{Hom}_{COF}(\wp, \mathbb{G}_a)$; so, $f \in \mathcal{R}$. Then f is of the form $h(g_2, g_3)/\Delta^d$ for a polynomial $h \in B[g_2, g_3]$ for $g_j(q)$ and $\Delta(q)$ as in (1.10). The condition (G4) implies $d = 0$ since $f(q) \in B[[q]]$. Indeed, otherwise, $f(q)$ involves negative power of q. Thus $f = h(g_2, g_3)$. By (G3) and $g_j(E, a\omega) = a^{-2j} g_j(E, \omega)$, we find $h(g_2, g_s) = \sum_{4a+6b=k} b_{a,b} g_2^a g_3^b$ with $b_{a,b} \in B$. Since g_2 and g_3 in $\mathcal{R}$ are variables and $\mathcal{R} \hookrightarrow \mathbb{Z}[\frac{1}{6}][[q]]$ (by q-expansion), the set $\{g_2^a g_3^b | 0 \le a, b \in \mathbb{Z}\}$ in $B[[q]]$ is linearly independent. This shows that $G_k(1; B) = \oplus_{4a+6b=k} B g_2^a g_3^b$.

We can show more generally

Theorem 1.14. *The B-module $G_k(N; B)$ is free of finite rank over B, and $G_k(1, B) = \oplus_{4a+6b=k} B g_2^a g_3^b$. In particular, we have*

$$\mathrm{rank}_B\, G_k(1; B) = \#\{(a, b) \in \mathbb{Z}^2_{\ge 0} | 4a + 6b = k\},$$

$G_k(N; B) \otimes_B A = G_k(N; A)$ if $k \ge 2$ and $G_k(N; B) \otimes_B \mathbb{C} = G_k(\Gamma_1(N))$ whenever B as above is inside $\mathbb{C}$. Also, if $f \in G_k(\Gamma_1(N); B)$ with $B \subset \mathbb{C}$, $f(q)$ with $q = \exp(2\pi i z)$ gives the Fourier expansion of f at the cusp ∞.

For the moment, we admit this (except for the case $N = 1$).

Exercise 1.15. *For even $k \ge 0$, show that*

$$r(k) := \mathrm{rank}_B\, G_k(1; B) = \begin{cases} \left[\frac{k}{12}\right] + 1 & \text{if } k \not\equiv 2 \mod 12 \\ \left[\frac{k}{12}\right] & \text{if } k \equiv 2 \mod 12. \end{cases}$$

Show also that $4a + 6b = k - 12(r(k) - 1)$ has only one non-negative integer solution for each even integer $k \ge 0$.

In addition to (G1-4), if f satisfies the following condition, we call f a *cusp form*:

(s) $f(q) = f((\mathrm{Tate}(q), \phi_N, \omega_{can})_{/R[[q^{1/d}]][q^{-1/d}]}) \in q^{1/d} R[[q^{1/d}]]$ for any level structures ϕ_N on Tate(q) defined over $R[[q^{1/d}]][q^{-1/d}]$ with $d|N$. This means that the constant term of f vanishes at all cusps.

We write $S_k(N; B) = S_k(\Gamma_1(N); B) \subset G_k(N; B)$ for the subspace of cusp forms.

In terms of $L \in Lat$, the corresponding elliptic curve is given by $E(\mathbb{C}) = \mathbb{C}/L$; so, identifying $\mu_N(\mathbb{C})$ with $N^{-1}\mathbb{Z}/\mathbb{Z}$ by $N^{-1}\mathbb{Z}/Z \ni a \mapsto \exp(2\pi i a) \in \mu_N(\mathbb{C})$, the level structure ϕ_N is a homomorphism $\phi_N : N^{-1}\mathbb{Z}/\mathbb{Z} \hookrightarrow N^{-1}L/L$. Using coordinate $w = \left(\begin{smallmatrix} w_1 \\ w_2 \end{smallmatrix}\right)$, we can normalize ϕ_N so that $\phi_{w,N}(a) = a w_2$. Then plainly $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$ acts on $\phi_{w,N}$ by $\phi_{w,N} \mapsto \phi_{w,N} \circ d$. Assuming that B contains the values of χ (i.e., B is an algebra

over $\mathbb{Z}[\frac{1}{6},\chi]$ for the subring $\mathbb{Z}[\chi]$ in $\overline{\mathbb{Q}}$ generated by the values of χ). Thus we can define for $f \in G_k(\Gamma_1(N);B)$ (for $\mathbb{Z}[\frac{1}{6},\chi]$-algebra B)

$$f \in G_k(\Gamma_0(N),\chi;B) \Leftrightarrow f(E,\phi_N \circ d,\omega) = \chi(d) f(E,\phi_N,\omega)$$

for all $d \in (\mathbb{Z}/N\mathbb{Z})^\times$, where $\phi_N \circ d(\zeta) = \phi_N(\zeta^d)$. Then we put $S_k(\Gamma_0(N),\chi;B) = G_k(\Gamma_0(N),\chi;B) \cap S_k(\Gamma_1(N),;B)$. Again we can prove, as long as B is $\mathbb{Z}[\frac{1}{6N},\chi]$-algebra,

$$S_k(\Gamma_0(N),\chi;B[\chi]) \otimes_B A = S_k(\Gamma_0(N),\chi;A)$$
$$\text{and} \quad G_k(\Gamma_0(N),\chi;B[\chi]) \otimes_B A = G_k(\Gamma_0(N),\chi;A).$$

Here is a more elementary proof of (a part of) Theorem 1.16 for $N = 1$. By a well known value of $\zeta(1-2k)$ for $k \geq 2$, if we put $e_{2k} = \frac{2}{\zeta(1-2k)} E_k$, we have

$$e_{2k} = 1 + C_k \sum_{n=1}^{\infty} \sum_{0<d|n} d^{k-1} q^n \in \mathbb{Z}[[q]].$$

For the value of C_k, see [LFE] §5.2. Let $s(k) = k - 12(r(k)-1)$. Take a unique solution (a,b) of $s(k) = 4a+6b$ as in (1.15). Put $h_i = e_4^a e_6^{b+2(r-1-i)} \Delta^i \in G_k(SL_2(\mathbb{Z}))$ for $r = r(k)$. By definition $h_i(q) \in \mathbb{Z}[[q]]$. Define $G_k(N;\mathbb{Z}) = \{f \in G_k(N;\mathbb{Z}[\frac{1}{6N}]) | f(q) \in \mathbb{Z}[[q]]\}$; so, $h_i \in G_k(1;\mathbb{Z})$. Then for $i = 0,1,\cdots,r(k)-1$, the $r \times r$ matrix $U = U(k) := (a(i,h_j))_{(i,j)\in[0,r-1]\cap\mathbb{Z}}$ is a unipotent matrix with coefficients in $\mathbb{Z}$; so, U^{-1} has coefficients in $\mathbb{Z}$, since Δ^i starts with q^i. Thus h_i is linearly independent over $\mathbb{Z}$ giving a basis of $G_k(N;\mathbb{Z})$. Solving $Ux = \mathbf{a}(f)$ for the column vector

$$\mathbf{a}(f) = {}^t(a(0,f), a(1,f), \ldots, a(r-1,f)),$$

we find $f = \sum_i x_i h_i$. Thus $G_k(1;\mathbb{Z}) = \bigoplus_{i=0}^{r(k)-1} \mathbb{Z} h_i$, which shows the following fact for $N = 1$.

Theorem 1.16. *$G_k(N;B) = G_k(N;\mathbb{Z}) \otimes_{\mathbb{Z}} B$ and $S_k(N;B) = S_k(N;\mathbb{Z}) \otimes_{\mathbb{Z}} B$ for any commutative ring B as long as $k \geq 2$.*

The case for cusp forms for $N = 1$ follows from the same argument, since $h_1, \ldots, h_{r(k)-1}$ gives a basis of $S_k(1;\mathbb{Z})$.

2. Deformation theory of modular forms

We study p-adic deformation of modular forms. This means for a given cusp form f of level N, we want to know the totality of all modular forms congruent modulo some power of p in $\bigcup_k S_k(N;W) \subset W[[q]]$ for a p-adically complete valuation ring containing the p-adic integer ring $\mathbb{Z}_p$. Indeed, this set often has geometric structure of the form $\mathrm{Spec}(R)$ for a p-profinite ring R made out of Hecke operators.

First, without going into technical details, we describe a prototypical example of a p-adic analytic families of modular forms. Then give a definition of p-adic analytic families of modular forms, and give details of how to construct them.

2.1. **p-adic integers.** We recall briefly the construction of the p-adic integer ring $\mathbb{Z}_p$ (cf. [PAI]). By definition, we have $\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} \cong \{x = \sum_{n=0}^{\infty} c_n p^n | c_n \in [0, p-1] \cap \mathbb{Z}\}$ with p-adic absolute value $|x|_p = p^{-v(x)}$ for $v(x) = \min_n(n|c_n \neq 0)$. Here $v : \mathbb{Z}_p \to \mathbb{Z} \cup \{\infty\}$ is a discrete valuation of $\mathbb{Z}_p$; so, $\mathbb{Z}_p$ is a discrete valuation ring with only maximal ideal (p). Embedding $\mathbb{Z}_{\geq 0} = \{0 \leq n \in \mathbb{Z}\}$ into $\mathbb{Z}_p$ by p-adic expansion, then we see that $\mathbb{Z}_{\geq 0}$ is made up of elements in $\mathbb{Z}_p$ with finite p-adic expansion. Thus $\mathbb{Z}_p$ is the completion of $\mathbb{Z}_{\geq 0}$ under the absolute value $|\cdot|_p$ given by $|x|_p = p^{-v(x)}$. The field $\mathbb{Q}_p$ of p-adic numbers is the field of fraction of the discrete valuation ring $\mathbb{Z}_p$ with valuation v with $v(p) = 1$, and the norm $|\cdot|_p$ and v naturally extend to $\mathbb{Q}_p$ by $v(\frac{a}{b}) = v(a) - v(b)$. Let $\overline{\mathbb{Q}}_p$ be an algebraic closure of $\mathbb{Q}_p$. Note that $\overline{\mathbb{Q}}_p/\mathbb{Q}_p$ is an infinite extension with $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ having continuous cardinality (why?). The p-adic absolute value $|\cdot|_p$ extends uniquely to $\overline{\mathbb{Q}}_p$ (so the valuation v to $v : \overline{\mathbb{Q}}_p \to \mathbb{Q} \cup \{\infty\}$ (taking a suitable logarithm of $|\cdot|_p$). See any book on algebraic number theory for these facts.

The ring $\mathbb{Z}_p$ is the unit closed disk centered at 0 in $\mathbb{Q}_p$; so, $\mathbb{Z}_p$ is a closed compact subring of the locally compact field $\mathbb{Q}_p$ (so, $\mathbb{Q} \subset \mathbb{Q}_p$ and $\mathbb{Q} \cap \mathbb{Z}_p = \{\frac{a}{b} \in \mathbb{Q} | v(b) = 0\}$). Plainly $\mathbb{Z}_{\geq 0}$ is dense in $\mathbb{Z}_p$, and any polynomial function $f(x) \in \mathbb{Q}_p[x]$ gives rise to a continuous function $f : \mathbb{Z}_p \to \mathbb{Q}_p$. Consider the binomial polynomial $\binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!}$ for $n \in \mathbb{Z}_+ = \{0 < m \in \mathbb{Z}_{\geq 0}\}$ and $\binom{x}{0} = 1$. If one plug in positive integers m in $\binom{x}{n}$, we get the binomial numbers $\binom{m}{n}$ if $m \geq n$, and otherwise $\binom{m}{n} = 0$; so, $\binom{x}{n} : \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$ is a p-adically continuous function; so, its extends to $\binom{x}{n} : \mathbb{Z}_p \to \mathbb{Z}_p$. Consider the binomial power series $(1+T)^x = \sum_{n=0}^{\infty} \binom{x}{n} T^n$. Plainly this series converge under $|\cdot|_p$ for any $x \in \mathbb{Z}_p$ on the open unit disk $p\mathbb{Z}_p$ centered at 0 giving rise to an isomorphism $\mathbb{Z}_p \cong (1 + \mathbf{p}\mathbb{Z}_p)$ by $x \mapsto \gamma^x = (1+\mathbf{p})^x$, where $\mathbf{p}$ is 4 if $p = 2$ and $\mathbf{p} = p$ is $p > 2$.

Exercise 2.1. *Why do we need to take $\mathbf{p}\mathbb{Z}_p$ if $p = 2$ in the above isomorphism?*

In any way, $1 + \mathbf{p}\mathbb{Z}_p = \gamma^{\mathbb{Z}_p} = \{\gamma^x | x \in \mathbb{Z}_p\}$ is a multiplicative (topologically) cyclic group generated by $\gamma = 1 + \mathbf{p}$.

Note that $p^r\mathbb{Z}_p = \{\sum_{n \geq r} c_n p^n\}$; so, $\mathbb{Z}/p^r\mathbb{Z} \cong \mathbb{Z}_p/p^r\mathbb{Z}_p$ canonically. Similarly, we have ${\mathbb{Z}_p}^\times/(1 + p^r\mathbb{Z}_p) = (\mathbb{Z}_p/p^r\mathbb{Z}_p)^\times$. In particular, $(\mathbb{Z}_p/p^r\mathbb{Z}_p)^\times$ has $\varphi(p^r) = p^r - p^{r-1}$ elements. By Lagrange theorem, we find that $x^{p^r - p^{r-1}} \equiv 1 \mod p^r$; in other words, $|x^{p^r} - x^{p^{r-1}}|_p \leq |p^r|_p = p^{-r}$; so, we have $\omega(x) = \lim_{n\to\infty} x^{p^r}$ in $\mathbb{Z}_p$.

Exercise 2.2. *Let $A = \varprojlim_n A_n$ for finite rings A_n of p-power order with projections $\pi_n : A \to A_n$, prove that $\lim_{n\to\infty} x^{d_n}$ converges into A for $d_n = |A_n|$, where A is equipped with the projective limit of discrete topology on A_n (called p-profinite topology) such that open-closed set is given by $\pi_n^{-1}(x)$ for all $x \in A_n$ and $n < \infty$.*

By definition, $\omega(x)^p = \omega(x)$; so, either $\omega(x) = 0$ or $\omega(x)^{p-1} = 1$. Since $(\mathbb{Z}/p\mathbb{Z})^\times$ is made up of $(p-1)$-th roots of unity (Fermat's little theorem) and $\omega(x) \equiv x \mod p\mathbb{Z}_p$, all $(p-1)$-th roots of unity shows up. Thus we have ${\mathbb{Z}_p}^\times = \mu_{p-1}(\mathbb{Z}_p) \times (1 + p\mathbb{Z}_p)$ and $\mathbb{Z}_2^\times = \mu_2 \times (1 + 4\mathbb{Z}_p)$. We define the p-profinite projection $\langle\cdot\rangle : {\mathbb{Z}_p}^\times \twoheadrightarrow 1 + \mathbf{p}\mathbb{Z}_p$; so, $z = \langle z\rangle\omega(z)$ if $p > 2$ and we change the definition of ω if $p = 2$ so that the above formula is valid; so, if $p = 2$, $\omega : \mathbb{Z}_2^\times \to \{\pm 1\}$ is a unique character factoring through $(\mathbb{Z}/4\mathbb{Z})^\times$; i.e., $\omega(x) \equiv \pm 1 \mod 4$. In particular, writing $\langle z\rangle = \gamma^{s_z}$ with $s_z \in \mathbb{Z}_p$, we find for $A_z(T) = (1+T)^{s_z} = \sum_{n=0}^\infty \binom{s_z}{n} T^n$, $A_z(\gamma^k - 1) = \langle z\rangle^k = z^k\omega^{-k}(z)$ for all $k \in \mathbb{Z}_p$. If we use the power series $\log_p(1+x) = \sum_{n=1}^\infty (-1)^{n+1}\frac{x^n}{n}$ convergent on $\mathbf{p}\mathbb{Z}_p$ (and extends $\log_p$ to ${\mathbb{Z}_p}^\times$ by $\log_p(\omega(z)\langle z\rangle) = \log_p(\langle z\rangle)$, we find $s_z = \log_p(z)/\log_p(\gamma)$.

Exercise 2.3. *Prove the convergence of $\log_p$, $\log_p(xy) = \log_p(x) + \log_p(y)$ and $s_z = \log_p(z)/\log_p(\gamma)$.*

2.2. **Eisenstein family.** Fix a positive integer N prime to p. For each character χ modulo Np, let $\mathbb{Z}_p[\chi]$ be the subring generated over $\mathbb{Z}_p$ by the values of χ inside $\overline{\mathbb{Q}}_p$.

Exercise 2.4. *Prove that $\mathbb{Z}_p[\chi]$ is a discrete valuation ring.*

Take a discrete valuation ring W inside $\overline{\mathbb{Q}}_p$ containing $\mathbb{Z}_p[\chi]$. Define $\Lambda = \Lambda_W = W[[T]]$ (the one variable power series ring). We often write t for $1 + T$ which is invertible in Λ_W. Assume that $\chi(-1) = 1$, and put

$$\mathcal{E}_\chi(T) = \sum_{n=0} a_{n,\chi}(T)q^n \in \Lambda_W[[q]],$$

where $a_n(T) = \sum_{0<d|n,p\nmid d} \chi_{Np}(d)d^{-1}A_d(T)$ and $a_0(T) = \frac{1}{2}\Phi_\chi(T)$ for the power series giving the Kubota–Leopoldt Dirichlet p–adic L-function $L_p(s,\chi)$ of $\chi\omega$ in the following way. By the theory of p-adic L-function (see [LFE] §3.4 and §3.5 and Chapter 4 for details), there exists a power series $\Phi_\chi(T) \in T^{-1}\Lambda_W$ such that $\Phi_\chi(\gamma^s - 1) = L_p(1-s,\chi)$ and $L_p(1-k,\chi) = (1 - \chi\omega^{-k}(p)p^{k-1})L(1-k,\chi\omega^{-k})$ for all positive integers k. We have $\Phi_\chi \in \Lambda_W$ unless $\chi = 1$ and $N = 1$. If $N = 1$ and $\chi = 1$, $L_p(s,\chi)$ has a simple pole at $s = 1$ (so, $\Phi_\chi \notin \Lambda_W$ and its denominator is T).

By definition, $\mathcal{E}_\chi(\gamma^k - 1) = E_k(\chi_{Np})$ for all $k \geq 1$. This $\{\mathcal{E}_\chi(\gamma^k - 1)|1 \leq k \in \mathbb{Z}\}$ is the p-adic Eisenstein family first proposed by Serre. A formal q-expansion $\mathcal{F}(T) \in \Lambda_W[[q]]$ is called a Λ-adic form (of Neben character χ) if the weight k specialization $\mathcal{F}(\gamma^k - 1) \in G_k(\Gamma_0(N\mathbf{p}, \chi\omega^{-k}; W)$ for all $k \gg 1$. We call the Λ-adic form a Λ-adic cusp form if its weight k-specializations for $k \gg 1$ are cusp forms for except for finitely many $k's$. Write $\mathcal{G}_\chi(\Gamma_0(N\mathbf{p}); \Lambda)$ (resp. $\mathcal{S}_\chi(\Gamma_0(N\mathbf{p}); \Lambda)$ for the space of Λ-adic modular forms (resp. Λ-adic cusp forms).

The family of modular forms $\{\mathcal{F}(\gamma^k - 1)|k \gg 1\}$ is called a p-adic analytic family of modular forms. Plainly $\mathcal{G}_\chi(\Gamma_0(N\mathbf{p}); \Lambda)$ and $\mathcal{S}_\chi(\Gamma_0(N\mathbf{p}); \Lambda)$ are Λ-modules. Thus

$\mathcal{E}_\chi$ for $\chi \neq 1$ and $T\mathcal{E}_1$ are called Λ-adic Eisenstein series. The Von Staut-Clausen theorem saying that $B_{2n} \equiv -\sum_{l-1|2n} \frac{1}{l} \mod \mathbb{Z}$ tells us $T\Phi_{\mathbf{1}}(T)|_{T=\gamma^k-1} = \frac{\zeta(1-k)}{2} = p^k(1-p^{k-1})\frac{B_k}{k} \in {\mathbb{Z}_p}^\times$ for even integer $k \equiv 0 \mod (p-1)$. This shows $\Phi_1(T) = \frac{\nu(T)}{T}$ with $\nu(T) \in \Lambda_W^\times$.

Exercise 2.5. *Prove that $\Phi(T) \in \Lambda_W^\times$ if and only if $\Phi(\gamma^k - 1) \in {\mathbb{Z}_p}^\times$ for some $k \in \mathbb{Z}$.*

Thus defining $\mathcal{E} = a_0(T)^{-1}\mathcal{E}_1$, by the above exercise, $\mathcal{E}$ is still a Λ-adic form and satisfies $\mathcal{E}(0) = 1$.

Proposition 2.6. *For any $f \in G_k(\Gamma_0(N\mathfrak{p}), \chi\omega^{-k}; W)$, we can find a Λ-adic form $\mathcal{F} \in \mathcal{G}_\chi(\Gamma_0(N\mathfrak{p}), \Lambda)$ such that $f = \mathcal{F}(\gamma^k - 1)$. In particular, $\mathcal{G}_\chi(\Gamma_0(N\mathfrak{p}); \Lambda) \otimes_\Lambda \Lambda/(t - \gamma^k)$ canonically contains $G_k(\Gamma_0(N), \chi\omega^{-k}; W)$.*

Even if a non-zero Λ-adic form $\mathcal{F}(T)$ vanishes at $t := 1 + T = \gamma^k$ $(k \geq 2)$, there is no guarantee that for $\mathcal{F}' = \mathcal{F}/(t - \gamma^k)$ specializes at $t = \gamma^k$ to a classical modular form. Therefore, we cannot prove that $\mathcal{G}_\chi(\Gamma_0(N\mathfrak{p}), \Lambda) \otimes_\Lambda \Lambda/(1 + T - \gamma^k) \cong G_k(\Gamma_0(N\mathfrak{p}), \chi\omega^{-k}; W)$.

Proof. Consider $\mathcal{E}_k(T) = \mathcal{E}(\gamma^{-k}(1+T)-1)$. Then it is easy to check that $a(n, \mathcal{E}_k) \in \Lambda_W$ for all n. Then $\mathcal{E}_k(0) = 1$ and $\mathcal{E}_k(\gamma^l - 1) = \mathcal{E}(\gamma^{l-k} - 1) \in G_{k-l}(\Gamma_0(N\mathfrak{p}), \omega^{k-l}; W)$; so, $\mathcal{F} := (f \cdot \mathcal{E}_k)(\gamma^l - 1) = \mathcal{E}(\gamma^{l-k} - 1)f \in G_l(\Gamma_0(N\mathfrak{p}), \chi\omega^{-k}\omega^{k-l}; W) = G_l(\Gamma_0(N\mathfrak{p}), \chi\omega^{-l}; W)$ for all $l \geq k$. Thus $\mathcal{F} \in \mathcal{G}_\chi(\Gamma_0(N\mathfrak{p}); \Lambda)$ as desired. □

2.3. **Hecke operators.** Let $\Gamma = \Gamma_0(N)$ or $\Gamma_1(N)$. For $\alpha \in GL_2(\mathbb{Q})$ for which $f \mapsto f|\alpha$ is well defined, if $\Gamma\alpha\Gamma$ can be decomposed into a disjoint union of finite left cosets $\Gamma\alpha\Gamma = \bigsqcup_{j=1}^h \Gamma\alpha_j$, we can think of the finite sum $g = \sum_j f|\alpha_j$ for $f : \mathfrak{H} \to \mathbb{C}$. If $\gamma \in \Gamma$, then $\alpha_j\gamma \in \Gamma\alpha_{\sigma(j)}$ for a unique index $1 \leq \sigma(j) \leq h$ and σ is a permutation of $1, 2, \ldots, h$. If further, $f|\gamma = f$ for all $\gamma \in \Gamma$, we have

$$g|\gamma = \sum_j f|\alpha_j\gamma = \sum_j f|\gamma_j\alpha_{\sigma(j)} = \sum_j (f|\gamma_j)|\alpha_{\sigma(j)} = \sum_j f|\alpha_{\sigma(j)} = g.$$

Thus under the condition that $f|\gamma = f$ for all $\gamma \in \Gamma$, $f \mapsto g$ is a linear operator only dependent on the double coset $\Gamma\alpha\Gamma$; so, we write $g = f|[\Gamma\alpha\Gamma]$. If we define

$$f|\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = f|_{k,k-1,\chi}\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \chi(a)(ad-bc)^{k-1} f\left(\frac{az+b}{cz+d}\right)(cz+d)^{-k}$$

for $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $N|c$ and a prime to N, we find $f \in G_k(\Gamma_0(N), \chi)$ satisfies $f|\gamma = f$ for all $\gamma \in \Gamma_0(N)$.

Exercise 2.7. *Prove that $f \in G_k(\Gamma_0(N), \chi)$ satisfies $f|\gamma = f$ for all $\gamma \in \Gamma_0(N)$. Use the fact that $ad \equiv 1 \mod N$ if $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$.*

More generally, if we have a set $T \subset GL_2^+(\mathbb{R})$ such that $\Gamma T\Gamma = T$ with finite $|\Gamma\backslash T|$, we can define the operator $[T]$ by $f \mapsto \sum_j f|\tau_j$ if $T = \bigsqcup_j \Gamma\tau_j$. We define

$$\Delta_0(N) = \left\{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{Z}) \cap GL_2^+(\mathbb{R}) \middle| c \equiv 0 \mod N,\ a\mathbb{Z} + N\mathbb{Z} = \mathbb{Z}\right\}.$$

Exercise 2.8. *Prove that $\Gamma\Delta_0(N)\Gamma = \Delta_0(N)$ for $\Gamma = \Gamma_0(N)$.*

Lemma 2.9. *Let $\Gamma = \Gamma_0(N)$.*

(1) *If $\alpha \in M_2(\mathbb{Z})$ with positive determinant, $|\Gamma\backslash(\Gamma\alpha\Gamma)| < \infty$;*
(2) *If p is a prime,*

$$\Gamma \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) \Gamma = \left\{\alpha \in \Delta_0(N) \middle| \det(\alpha) = p\right\} = \begin{cases} \Gamma \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) \sqcup \bigsqcup_{j=0}^{p-1} \Gamma \left(\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right) & \text{if } p \nmid N, \\ \bigsqcup_{j=0}^{p-1} \Gamma \left(\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right) & \text{if } p|N. \end{cases}$$

(3) *for an integer $n > 0$,*

$$T_n := \left\{\alpha \in \Delta_0(N) \middle| \det(\alpha) = n\right\} = \bigsqcup_a \bigsqcup_{b=0}^{d-1} \Gamma_0(N) \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \quad (a > 0,\ ad = n,\ (a, N) = 1,\ a, b, d \in \mathbb{Z}),$$

(4) *Write $T(n)$ for the operator corresponding to T_n. Then we get the following identity of Hecke operators for $f \in G_k(\Gamma_0(N), \chi)$:*

$$a(m, f|T(n)) = \sum_{0<d|(m,n),(d,N)=1} \chi(d) d^{k-1} \cdot a(\frac{mn}{d^2}, f).$$

(5) *$T(m)T(n) = T(n)T(m)$ for all integers m and n.*

By (4), $a(n, f|T(l)) = a(ln, f)$ if l is a prime factor of N and $a(n, f|T(l)) = a(ln, f) + \chi(l)l^{k-1}a(\frac{n}{l}, f)$ otherwise (here $a(m, f) = 0$ for $m \notin \mathbb{Z}_{\geq 0}$). Because of this, we write often $U(l)$ for $T(l)$ if $l|N$. By this formula, $U(l)^n = U(l^n)$.

Proof. Note that (1) and (2) are particular cases of (3). We only prove (2), (4) when $n = p$ for a prime p and (5), leaving the other cases as an exercise (see [IAT] Proposition 3.36 and (3.5.10) for a detailed proof of (3) and (4)).

We first deal with (2). Since the argument in each case is essentially the same, we only deal with the case where $p \nmid N$ and $\Gamma = \Gamma_0(N)$. Take any $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{Z})$ and $ad - bc = p$. If c is divisible by p, then ad is divisible by p; so, one of a and d has a factor p. We then have

$$\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} a/p & b \\ c/p & d \end{smallmatrix}\right) \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_0(N) \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$$

if a is divisible by p. If d is divisible by p and a is prime to p, choosing an integer j with $0 \leq j \leq p-1$ with $ja \equiv b \mod p$, we have $\gamma \left(\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right)^{-1} \in GL_2(\mathbb{Z})$. If c is not divisible by p but a is divisible by p, we can interchange a and c via multiplication by $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ from the left-side. If a and c are not divisible by p, choosing an integer j so that $ja \equiv -c \mod p$, we find that the lower left corner of $\left(\begin{smallmatrix} 1 & 0 \\ j & 1 \end{smallmatrix}\right) \gamma$ is equal to $ja + c$ and is divisible by p. This finishes the proof of (2).

We now deal with (4) assuming $n = p$. By (2), we have

$$f|T(p)(z) = \begin{cases} \chi(p)p^{k-1} \cdot f(pz) + \sum_{j=0}^{p-1} f\left(\frac{z+j}{p}\right) & \text{if } p \nmid N, \\ \sum_{j=0}^{p-1} f\left(\frac{z+j}{p}\right) & \text{if } p|N. \end{cases} \tag{2.1}$$

Writing $f = \sum_{n=1}^{\infty} a(n,f)q^n$ for $q = \mathbf{e}(z)$, we find

$$a(m, f|T(p)) = a(mp, f) + \chi(p)p^{k-1} \cdot a(\frac{m}{p}, f).$$

Here we put $a(r,f) = 0$ unless r is a non-negative integer.

The formula of Lemma 2.9 (4) is symmetric with respect to m and n; so, we conclude $T(m)T(n) = T(n)T(m)$. This proves (5). □

Exercise 2.10. *Give a detailed proof of the above lemma.*

The following exercise is more difficult:

Exercise 2.11. *Let $\Gamma = SL_2(\mathbb{Z})$. Prove that $|\Gamma\backslash(\Gamma\alpha\Gamma)| < \infty$ for $\alpha \in GL_2(\mathbb{R})$ if and only if then $\alpha \in M_2(\mathbb{Q})$ modulo real scalar matrices.*

If we regard $f \in G_k(SL_2(\mathbb{Z}))$ as a function of lattices L, for example, for $\alpha \in \Gamma \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) \Gamma$, $p^k f(\alpha \cdot L) = f(p^{-1}\alpha L)$. Note that $\mathbb{C}/p^{-1}\alpha L$ is a quotient of $E(L)$ ($E(L)(\mathbb{C}) = \mathbb{C}/L$) by order p subgroup $p^{-1}\alpha L/L$. Since $E(L)[p]$ (the kernel of $x \mapsto px$) is two dimensional vector space over $\mathbb{F}_p$, it has $|\mathbf{P}^1(\mathbb{F}_p)| = |\mathbb{F}_p \cup \{\infty\}|$ subgroup of order p. This corresponds to the representatives $\Gamma\backslash\Gamma \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) \Gamma$. Thus $f|T(p) = \frac{1}{p}\sum_{L' \supset L, [L':L]=p} f(L')$. Here the factor $\frac{1}{p}$ in front is the difference of p^k and the factor $p^{k-1} = \det(\alpha)^{k-1}$ of $f|\alpha = \det(\alpha)^{k-1} f(\alpha(z))j(\alpha,z)^{-k}$. Note that $E(L') = E(L)/(L'/L)$ (i.e., $E(L')$ running over all quotients of $E(L)$ by subgroups of order p). More generally, $f|T(n) = \frac{1}{n}\sum_{L' \supset L, [L':L]=n} f(L')$. If $\Gamma = \Gamma_0(N)$ or $\Gamma_1(N)$, we can verify $f|U(l)$ for $l|N$ is the sum of $f(L', \phi_N)$ where $[L' : L] = l$ and $L'/L \cap \mathrm{Im}(\phi_N) = \{0\}$ inside $E(L)$ (so, the summation is different from $T(l)$ fro $SL_2(\mathbb{Z})$).

If we regard algebraically $f \in G_k(\Gamma_1(N); B)$ as a function $(E, \phi_N, \omega) \mapsto f(E, \phi_N, \omega)$, the Hecke operators can be interpreted using the above quotient process:

$$f|T(n)(E, \phi_N, \omega) = \frac{1}{n} \sum_{C:\text{subgroups of } E \text{ of order } n} f(E/C, \pi_C \circ \phi_N, \pi_{C,*}\omega),$$

where $\pi_C : E \to E/C$ is the projection and $\pi_{C,*}\omega$ is the push-forward of ω (see [GME] §3.2.3 for more details). Similarly,

$$f|U(l)(E, \phi_N, \omega) = \frac{1}{l} \sum_{C:\text{subgroups of } E \text{ of order } l,\ C \cap \mathrm{Im}(\phi_N) = \{0\}} f(E/C, \pi_C \circ \phi_N, \pi_{C,*}\omega).$$

We extend the definition of Hecke operators on $\mathcal{F} \in \mathcal{G}_\chi(\Gamma_0(N\mathbf{p}); \Lambda)$ by the following formula:

$$a(m, \mathcal{F}|T(n)) = \sum_{0<d|(m,n),(d,N)=1} \chi(d)d^{-1}A_d(T) \cdot a(\frac{mn}{d^2}, \mathcal{F}). \tag{2.2}$$

Since $A_d(\gamma^k - 1) = d^k\omega^{-k}(d)$, the specialization of the above formula gives rise to the formula in Lemma 2.9 (4) for the Neben character $\chi\omega^{-k}$; so, $\mathcal{F}|T(n)(\gamma^k - 1) = \mathcal{F}(\gamma^k - 1)|T(n)$. Thus, $\mathcal{F}(\gamma^k - 1) \in G_k(\Gamma_0(N\mathbf{p}), \chi\omega^{-k}; W)$ implies $\mathcal{F}|T(n)(\gamma^k - 1) \in G_k(\Gamma_0(N\mathbf{p}), \chi\omega^{-k}; W)$; so, the above operator acts on $\mathcal{G}_\chi(\Gamma_0(N\mathbf{p}); \Lambda)$.

Thus we defined Λ-adic forms in an ad-hoc manner, for any local ring $R = \varprojlim_n R/\mathfrak{m}_R^n$ with a continuous algebra homomorphism $\varphi : \Lambda \to R$, the image f_R of $\mathcal{F}$ under φ gives a q-expansion of a "p-adic modular form" defined over R (i.e., roughly/morally speaking, f_R is a p-adic limit of a sequence $\{f_n \in G_{k_n}(\Gamma_1(N\mathbf{p}); R)\}$), and one can give a more intrinsic definition of Λ-adic forms which we do not touch in this course.

2.4. **Ordinarity.** Let V be a free W-module of finite rank with a W-linear operator $U : V \to V$. Then $W[U] \subset \mathrm{End}_W(V)$ is free of finite rank r over W; so, the algebra $W[U]$ is a p-profinite semi-local ring (i.e., $W[U]$ has only finitely many maximal ideals; why?). Writing $W[U] = \varprojlim_n W[U]/p^n W[U]$ and $d_n = |W[U]/p^n W[U]| = p^{rn \operatorname{rank} W}$, we have the p-adic limit $\omega(U) = \lim_n U^{d_n}$ exists by Exercise 2.2. Since $d_n | m!$ for some m depending on n, the limit $e = \lim_n U^{n!}$ exists in $W[U]$, which plainly satisfies $e^2 = e$ (i.e., an idempotent of $W[U]$). The operator e is called the projector associated to U. For any commutative subalgebra $A \subset \mathrm{End}_W(V)$ containing $W[U]$, eA is the direct summand of A in which eU is a unit and $(1-e)A$ is the complementary direct summand such that $(1-e)U$ is topologically nilpotent (i.e., $\lim_{n\to\infty}(1-e)U^n = 0$).

We apply this argument to the $U(p)$-operator. Since $G_k(\Gamma_0(N\mathbf{p}), \chi; W)$ is free of finite rank over W, we have the limit idempotent $e = \lim_n U(p)^{n!}$. We write the subspace $e(G_k(\Gamma_0(N\mathbf{p}), \chi; W))$ as $G_k^{ord}(\Gamma_0(N\mathbf{p}), \chi; W)$, and we call forms in $G_k^{ord}(\Gamma_0(N\mathbf{p}), \chi; W)$ ordinary (or p-ordinary) modular forms.

Let

$$\mathcal{G}_\chi^k(\Gamma_0(N\mathbf{p}); \Lambda) = \{\mathcal{F} \in \mathcal{G}_\chi(\Gamma_0(N\mathbf{p}); \Lambda) | \mathcal{F}(\gamma^j - 1) \in G_k(\Gamma_0(N\mathbf{p}), \chi\omega^{-j}; W) \text{ for all } j \geq k\}.$$

Then $\mathcal{G}_\chi(\Gamma_0(N\mathbf{p}); \Lambda) = \bigcup_k \mathcal{G}_\chi^k(\Gamma_0(N\mathbf{p}); \Lambda) \subset \Lambda_W[[q]]$.

Theorem 2.12. *There exists an idempotent $e \in \mathrm{End}_\Lambda(\mathcal{G}_\chi(\Gamma_0(N\mathbf{p}); \Lambda))$ commuting with $U(p)$ such that $eU(p)$ is invertible in $e\Lambda[U] \subset \mathrm{End}_\Lambda(\mathcal{G}_\chi(\Gamma_0(N\mathbf{p}); \Lambda))$ and $(1-e)U(p)$ is topologically nilpotent.*

Proof. Since $\mathcal{G}_\chi(\Gamma_0(N\mathbf{p}); \Lambda) = \bigcup_k \mathcal{G}_\chi^k(\Gamma_0(N\mathbf{p}); \Lambda) \subset \Lambda_W[[q]]$, we only need to prove that e exists in $\mathrm{End}_\Lambda(\mathcal{G}_\chi^k(\Gamma_0(N\mathbf{p}); \Lambda))$ for each $k \geq 2$. If the map $\mathcal{G}_\chi^k(\Gamma_0(N\mathbf{p}); \Lambda) \ni \mathcal{F} \mapsto (\mathcal{F}(\gamma^j - 1))_{j \geq k} \in \prod_j G_j(\Gamma_0(N\mathbf{p}), \chi\omega^{-j}; W)$ is an injection, the product operator of $U(p)$ on each $G_j(\Gamma_0(N\mathbf{p}), \chi\omega^{-j}; W)$ induces $U(p)$ on $\mathcal{G}_\chi^k(\Gamma_0(N\mathbf{p}); \Lambda)$ since $\mathcal{F}(\gamma^j - 1)|U(p) = \mathcal{F}|U(p)(\gamma^j - 1)$. Then in the product on the right-hand-side $\lim_{n\to\infty} U(p)^{n!}$ exists and preserves the image of $\mathcal{G}_\chi^k(\Gamma_0(N\mathbf{p}); \Lambda)$, and the assertion follows. So we show the injectivity. If $\mathcal{F}(\gamma^j - 1) = 0$ for all $j \geq k$, writing $\mathcal{F} = \sum_{n=0}^\infty a(n, \mathcal{F})(T) q^n$, we have $a(n, \mathcal{F})(T) \in (t - \gamma^j)$. Note that $W[[T]] = \Lambda$ is a unique factorization domain (why?). Thus $a(n, \mathcal{F})(T)$ is divisible by infinitely many prime $t - \gamma^j$ (for $j \geq k$) implies $a(n, \mathcal{F}) = 0$; so, $\mathcal{F} = 0$. □

We define

$$\mathcal{G}_\chi^{ord}(\Gamma_0(N\mathbf{p}), \Lambda) = e(\mathcal{G}_\chi^{ord}(\Gamma_0(N\mathbf{p}), \Lambda)) \text{ and } \mathcal{S}_\chi^{ord}(\Gamma_0(N\mathbf{p}), \Lambda) = e(\mathcal{S}_\chi^{ord}(\Gamma_0(N\mathbf{p}), \Lambda)),$$

and call them the space of ordinary Λ-adic modular/cusp forms.

We have proven that for any $f \in G_k^{ord}(\Gamma_0(N\mathbf{p}), \chi\omega^{-k}; W)$, we can find a Λ-adic form $\mathcal{F} \in \mathcal{G}_\chi(\Gamma_0(N\mathbf{p}); \Lambda)$ such that $\mathcal{F}(\gamma^k - 1) = f$. Applying e, we find $\mathcal{F}|e(\gamma^k - 1) =$

$\mathcal{F}(\gamma^k-1)|e=f|e=f$; so, any $f\in G_k^{ord}(\Gamma_0(N\mathbf{p}),\chi\omega^{-k};W)$ can be lifted to $\mathcal{F}\in\mathcal{G}_\chi^{ord}(\Gamma_0(N\mathbf{p});\Lambda)$. For example, we can take $\mathcal{F}=\mathcal{E}_kf|e$ for $\mathcal{E}_k$ as in the proof of Proposition 2.6.

2.5. **Control theorem.** For a while, we admit the following innocuous looking theorem:

Theorem 2.13. *Suppose that $p\nmid N$. Then for all $k\geq 2$, we have*

$$\operatorname{rank}_{\mathbb{Z}_p} G_k^{ord}(\Gamma_0(N\mathbf{p}),\chi\omega^{-k})\leq \operatorname{rank}_{\mathbb{Z}_p} G_2^{ord}(\Gamma_0(N\mathbf{p}),\chi\omega^{-2}).$$

The same inequality holds for cusp forms.

We will give a sketch of the proof of this theorem later if time allows. We prove the following consequence of the above theorem.

Corollary 2.14. *The Λ-modules $\mathcal{G}_\chi^{ord}(\Gamma_0(N\mathbf{p});\Lambda)$ and $\mathcal{S}_\chi^{ord}(\Gamma_0(N\mathbf{p});\Lambda)$ is Λ-free of finite rank. Moreover for any $k\geq 2$, we have*

$$\mathcal{G}_\chi^{ord}(\Gamma_0(N\mathbf{p});\Lambda)\otimes_\Lambda \Lambda/(t-\gamma^k)\cong G_k^{ord}(\Gamma_0(N\mathbf{p}),\chi\omega^{-k};W)$$

and

$$\mathcal{S}_\chi^{ord}(\Gamma_0(N\mathbf{p});\Lambda)\otimes_\Lambda \Lambda/(t-\gamma^k)\cong S_k^{ord}(\Gamma_0(N\mathbf{p}),\chi\omega^{-k};W)$$

by the specialization map. In particular, the W-rank of the right-hand-side of the above equation is independent of $k\geq 2$.

Proof. Since the proof is the same, we prove it for modular forms. For simplicity, write $\mathcal{G}=\mathcal{G}_\chi^{ord}(\Gamma_0(N\mathbf{p});\Lambda)$. We have $E=\mathcal{E}(\gamma^{k-2}-1)\equiv 1 \mod \mathfrak{m}\Lambda$ for the maximal ideal $\mathfrak{m}$ of W. Multiplying $\overline{E}:=E \mod \mathfrak{m}\Lambda\in\mathbb{F}[[q]]$ for $\mathbb{F}=W/\mathfrak{m}$, we get $G_2^{ord}(\Gamma_0(N\mathbf{p}),\chi\omega^{-2};\mathbb{F})\hookrightarrow G_k^{ord}(\Gamma_0(N\mathbf{p}),\chi\omega^{-k};\mathbb{F})$. Since we get

$$\begin{aligned}\operatorname{rank} G_k^{ord}(\Gamma_0(N\mathbf{p}),\chi\omega^{-k};W)&=\dim_{\mathbb{F}} G_k^{ord}(\Gamma_0(N\mathbf{p}),\chi\omega^{-k};W)\otimes_W\mathbb{F}\\&=\dim_{\mathbb{F}} G_k^{ord}(\Gamma_0(N\mathbf{p}),\chi\omega^{-k};\mathbb{F})\end{aligned}$$

from $G_k(\Gamma_0(N\mathbf{p}),\chi\omega^{-k};W)\otimes_W\mathbb{F}\cong G_k(\Gamma_0(N\mathbf{p}),\chi\omega^{-k};\mathbb{F})$, we have

$$\operatorname{rank} G_k^{ord}(\Gamma_0(N\mathbf{p}),\chi\omega^{-k};W)\geq \operatorname{rank} G_2^{ord}(\Gamma_0(N\mathbf{p}),\chi\omega^{-2};W)$$

for all $k\geq 2$. The reverse inequality follows from the theorem; so, the rank is independent of $k\geq 2$.

Let $M\subset\mathcal{G}$ be the free Λ-module of rank r generated by $\mathcal{F}_1,\dots,\mathcal{F}_r$. Thus we can find a sequence of integer $0\leq n_1\leq\cdots\leq n_r$ such that $D=\det(A)\neq 0$ for the $r\times r$-matrix $A=(a(n_i,\mathcal{F}_j))$ in Λ. By Weierstrass preparation theorem (cf. [ICF] Theorem 7.3), any non-zero power series in $\Lambda=W[[T]]$ has finitely many zeros in the unit disk (in $\overline{\mathbb{Q}}_p$). For sufficiently large $k\gg 0$, we find $D(\gamma^k-1)\neq 0$ and that all $f_j=\mathcal{F}_j(\gamma^k-1)$ are in $G_k^{ord}(\Gamma_0(N\mathbf{p}),\chi\omega^{-k};W)$. Thus any Λ-free submodule of $\mathcal{G}$ has rank bounded by $\operatorname{rank}_W G_k^{ord}(\Gamma_0(N\mathbf{p}),\chi\omega^{-k};W)$. Let r is the maximal of the rank of Λ-free submodules. We may assume that the Λ-free submodule $M\subset\mathcal{G}$ has rank r. Thus $f_j=\mathcal{F}_j(\gamma^k-1)$ $(j=1,\dots,r)$ are linearly independent over W, and hence

$$r\leq \operatorname{rank} G_k^{ord}(\Gamma_0(N\mathbf{p}),\chi\omega^{-k};W)=:R,$$

which is independent of k. Since $M \subset \mathcal{G} \subset \Lambda[[q]]$ by definition, M and $\mathcal{G}$ are Λ–torsion-free. Therefore $\mathcal{F}_1, \dots, \mathcal{F}_r$ is the set of maximally linearly independent elements in $\mathcal{G}$. Writing Q for the quotient field of Λ, we find the identity of Q-span $Q \cdot M = Q \cdot \mathcal{G}$ in $Q[[q]]$. Pick an $\mathcal{F} \in \mathcal{G}$. Then $\mathcal{F} = \sum_i x_i \mathcal{F}_i$ for $x_i \in Q$. The elements $x_i \in Q$ are the solution of $A\mathbf{x} = \mathbf{a}(\mathcal{F})$, where $\mathbf{x} = {}^t(x_1, \dots, x_r)$ and $\mathbf{a}(\mathcal{F}) = {}^t(a(n_1, \mathcal{F}), \dots, a(n_r, \mathcal{F}))$. Therefore by linear algebra, $Dx_i \in \Lambda$. This shows $D\mathcal{G} \subset M$. In particular, $\mathcal{G}$ is finitely generated over Λ as Λ is noetherian. We now use the following facts:

(u) Λ is a unique factorization domain (any power series ring over a regular UFD is UFD; see, [CRT] 20.8).
(r) For $x \in \mathbb{Z}_p$, $\Phi(x) = 0 \Leftrightarrow \Phi(T) = (T - x)\Psi(T)$ with $\Psi(T) \in \Lambda$ (an exercise).

Since $\mathcal{G}$ is finitely generated, choosing a set of generators $\Phi_1, \dots, \Phi_m$. By definition, for $k \gg 2$, $\Phi_j(\gamma^k - 1) \in G_k^{ord}(\Gamma_0(N\mathbf{p}), \chi\omega^{-k}; W)$ for all j. Then every $\mathcal{F} \in \mathcal{G}$, $\mathcal{F}(\gamma^k - 1)$ is a linear combination of $\Phi_j(\gamma^k - 1)$, and hence $\mathcal{F}(\gamma^k - 1) \in G_k^{ord}(\Gamma_0(N\mathbf{p}), \chi\omega^{-k}; W)$. If $\mathcal{F}(\gamma^k - 1) = 0$, by (u), $a(n, \mathcal{F})/(t - \gamma^k) \in \Lambda$ for any integer $n \geq 0$, and we have $\mathcal{F}' = \mathcal{F}/(t - \gamma^k) \in \mathcal{G}$. However, $\mathcal{F}'(\gamma^k - 1) \in G_k^{ord}(\Gamma_0(N\mathbf{p}), \chi\omega^{-k}; W)$ as this is true for any elements in $\mathcal{G}$; so, $\mathcal{F} = (t - \gamma^k)\mathcal{F}'$. Thus the kernel of the specialization map $\Phi \mapsto \Phi(\gamma^k - 1)$ is $(t - \gamma^k)\mathcal{G}$. We have therefore an exact sequence:

$$0 \to (t - \gamma^k)\mathcal{G} \to \mathcal{G} \to G_k^{ord}(\Gamma_0(N\mathbf{p}), \chi\omega^{-k}; W) \to 0.$$

Now set $r = R$. Choose a basis $f_1, \dots, f_r$ of $G_k^{ord}(\Gamma_0(N\mathbf{p}), \chi\omega^{-k}; W)$ and pick $\mathcal{F}_j$ with $\mathcal{F}_j(\gamma^k - 1) = f_j$. The existence of $\{\mathcal{F}_1, \dots, \mathcal{F}_r\}$ is guaranteed by the above exact sequence. If $\sum_i a_i \mathcal{F}_i = 0$ for $a_i \in \Lambda$, then $\sum_i a_i(\gamma^k - 1) f_i = 0$; so, $a_i = (t - \gamma^k)a_i'$ with $a_i' \in \Lambda$ for all i. Dividing the equation $\sum_i a_i \mathcal{F}_i = 0$ by $(t - \gamma^k)$, we get $\sum_i a_i' \mathcal{F}_i = 0$; so, $(t - \gamma^k)|a_i'$, repeating this, we find any power of $(t - \gamma^k)$ is a factor of a_i; so, $a_i = 0$ for all i; i.e., $\mathcal{F}_i$ are linearly independent. By Nakayama's lemma below, we find $\{\mathcal{F}_i\}_i$ is a basis of $\mathcal{G}$, and hence $\mathcal{G}$ is Λ-free of rank $r = \operatorname{rank} G_k^{ord}(\Gamma_0(N\mathbf{p}), \chi\omega^{-k}; W)$. As we have seen already, for any $f \in G_l^{ord}(\Gamma_0(N\mathbf{p}), \chi\omega^{-2}; W)$, we can find $\mathcal{F} \in \mathcal{G}$ such that $\mathcal{F}(\gamma^l - 1) = f$; i.e., $G_l^{ord}(\Gamma_0(N\mathbf{p}), \chi\omega^{-l}; W) \hookrightarrow \mathcal{G}/(t - \gamma^l)\mathcal{G}$. This shows $r = R = \operatorname{rank}_\Lambda \mathcal{G} \geq \operatorname{rank}_W G_l^{ord}(\Gamma_0(N\mathbf{p}), \chi\omega^{-l}; W) = R$ for any $l \geq 2$. Therefore $r = \operatorname{rank}_W G_l^{ord}(\Gamma_0(N\mathbf{p}), \chi\omega^{-l}; W)$, and hence

$$\mathcal{G}/(t - \gamma^l)\mathcal{G} \cong G_l^{ord}(\Gamma_0(N\mathbf{p}), \chi\omega^{-l}; W)$$

for any $l \geq 2$. This finishes the proof. □

Lemma 2.15 (NAK). *Let R be a local ring with maximal ideal $\mathfrak{m}$. For any ideal P of R, suppose that an R-module M is finitely generated over R. Then if M/PM is generated by $f_1 \mod P, \dots, f_j \mod P$ over R/P, then M is generated by $f_1, \dots, f_r$ over R.*

This lemma can be found in any book on commutative rings (e.g. [CRT] Theorem 2.3).

2.6. **Duality.** We suppose the following axiom for a character ϕ of $(\mathbb{Z}/N\mathbb{Z})^\times \times {\mathbb{Z}_p}^\times$ with values in $R^\times$ for a profinite ring R:

(d1) We have an R–free module E of finite rank with commuting R-linear operator $T(n)$ $(n = 1, 2, \dots)$, $T(1)$ giving the identity operator;

(d2) We have an embedding $E \hookrightarrow qR[[q]]$ for a power series ring $R[[q]]$ given by $E \ni f \mapsto \sum_{n=1}^{\infty} a(n,f)q^n \in qR[[q]]$;
(d3) We have $a(m, f|T(n)) = \sum_{0<d|(m,n),(d,Np)=1} \phi(d)a(\frac{mn}{d^2}, f)$ for all positive integer m, n, where N is a fixed positive integer.

Here ϕ can be a character $z \mapsto \chi(z)z_p^{k-1}$ for the projection z_p of $z \in {\mathbb{Z}_p}^\times \times (\mathbb{Z}/\mathbb{Z})^\times$ to ${\mathbb{Z}_p}^\times$ or $\phi(z) = \chi(z)z_p^{-1}A_{z_p}(T)$.

Let $\mathcal{H}(E)$ be the closed subring of R-linear endomorphism algebra $\mathrm{End}_R(E)$ topologically generated by $T(n)$ $(n = 1, 2, \dots)$ under the profinite topology of R, E and $\mathrm{End}_R(E)$. Using (d3), we leave the reader to show that $\mathcal{H}(E)$ is a commutative algebra. For any Λ-algebra $\mathbb{I}$, we define $\mathcal{G}_\chi(\Gamma_0(N\mathbf{p}); \mathbb{I}) = \mathcal{G}_\chi(\Gamma_0(N\mathbf{p}); \Lambda) \otimes_\Lambda \mathbb{I}$ and $\mathcal{S}_\chi(\Gamma_0(N\mathbf{p}); \mathbb{I}) = \mathcal{S}_\chi(\Gamma_0(N\mathbf{p}); \Lambda) \otimes_\Lambda \mathbb{I}$ which are submodules of $\mathbb{I}[[q]]$.

Definition 2.1. We write $H_k(\Gamma_0(Np^r), \chi; R)$ (resp. $h_k(\Gamma_0(Np^r), \chi; R)$) for $\mathcal{H}(E)$ if $E = G_k(\Gamma_0(Np^r), \chi; R)$ (resp. $E = S_k(\Gamma_0(Np^r), \chi; R)$) for an algebra R finite over W. Similarly, we write $H_k^{ord}(\Gamma_0(Np^r), \chi; R)$ (resp. $\mathbf{h}_k^{ord}(\Gamma_0(Np^r), \chi; R)$) for $\mathcal{H}(E)$ if $E = G_k^{ord}(\Gamma_0(Np^r), \chi; R)$ (resp. $E = S_k^{ord}(\Gamma_0(Np^r), \chi; R)$). If $E = \mathcal{G}_\chi(\Gamma_0(N\mathbf{p}); \mathbb{I})$, we write $\mathbf{H}_\chi(\Gamma_0(N\mathbf{p}); \mathbb{I})$ for $\mathcal{H}(E)$, where $\chi : (\mathbb{Z}/Np^r\mathbb{Z})^\times \to W^\times$ is a character. If $E = \mathcal{S}_\chi(\Gamma_0(N\mathbf{p}); \mathbb{I})$, we write $\mathbf{h}_\chi(\Gamma_0(N\mathbf{p}); \mathbb{I})$ for $\mathcal{H}(E)$.

We define a pairing $\langle \cdot, \cdot \rangle : E \times \mathcal{H}(E) \to R$ by $\langle f, h \rangle = a(1, f|h)$. By (d3), we have $\langle f, T(n) \rangle = a(n, f)$. Then by (d2), $\langle f, T(n) \rangle = 0$ for all n implies $f = 0$. On the other hand, if we assume that $\langle f, h \rangle = 0$ for all $f \in E$, we have

$$0 = \langle f|T(n), h \rangle = \langle f, hT(n) \rangle = a(1, f|hT(n)) = \langle f|h, T(n) \rangle = a(n, f|h).$$

This shows that $f|h = 0$ for all $f \in E$, and by definition $h = 0$; so, the pairing is non-degenerate.

Lemma 2.16. *If R is a field or a discrete valuation ring and E is free of finite rank over R, we have $\mathrm{Hom}_R(\mathcal{H}(E), R) \cong E$ and $\mathcal{H}(E) = \mathrm{Hom}_R(E, R)$ under the above pairing. If $\lambda \in \mathrm{Hom}_R(\mathcal{H}(E), R)$, the isomorphism: $\mathrm{Hom}_R(\mathcal{H}(E), R) \cong E$ sends λ to $\sum_{n=1}^{\infty} \lambda(T(n))q^n \in E$.*

Proposition 2.17. *If $\mathbb{I}$ is a Λ-algebra and E is either $S(\chi; \mathbb{I})$ or $S(\Gamma_0(N), \chi; \mathbb{I})$, we have $\mathrm{Hom}_\mathbb{I}(\mathcal{H}(E), \mathbb{I}) \cong E$ and $\mathcal{H}(E) = \mathrm{Hom}_\mathbb{I}(E, \mathbb{I})$ under the above pairing. If $\lambda \in \mathrm{Hom}_\mathbb{I}(\mathcal{H}(E), \mathbb{I})$, the isomorphism: $\mathrm{Hom}_\mathbb{I}(\mathcal{H}(E), \mathbb{I}) \cong E$ sends λ to $\sum_{n=1}^{\infty} \lambda(T(n))q^n \in E$.*

Proof. Since the space over $\mathbb{I}$ is the scalar extension of the space over Λ, we may assume that $\mathbb{I} = \Lambda$. For simplicity, we write $S = \mathcal{S}_\chi(\Gamma_0(N\mathbf{p}); \Lambda)$ and $\mathbf{h} = \mathbf{h}_\chi(\Gamma_0(N\mathbf{p}); \Lambda)$. Let $\mathfrak{m}$ be the maximal ideal of Λ with $\mathbb{F} = \Lambda/\mathfrak{m}$. By definition, $\mathbf{h}/\mathfrak{m}\mathbf{h}$ surjects down to $\mathcal{H}(S/\mathfrak{m}S)$ as the two algebras are generated by $T(n)$. This shows the morphism: $\mathbf{h} \to \mathrm{Hom}_\Lambda(S, \Lambda)$ induced by the pairing gives rise to

$$\mathbf{h}/\mathfrak{m}\mathbf{h} \xrightarrow{i} \mathrm{Hom}_\Lambda(S, \Lambda) \otimes_\Lambda \Lambda/\mathfrak{m} \cong \mathrm{Hom}_\mathbb{F}(S/\mathfrak{m}S, \mathbb{F}).$$

The last identity follows as the Λ-module S is Λ-free of finite rank. Since

$$\mathrm{Hom}_\mathbb{F}(S/\mathfrak{m}S, \mathbb{F}) \cong \mathcal{H}(S/\mathfrak{m}S)$$

by the non-degeneracy over the field $\mathbb{F}$, i factors through $\mathcal{H}(S/\mathfrak{m}S)$. Then by Nakayama's lemma, $i : \mathbf{h} \to \mathrm{Hom}_\Lambda(S, \Lambda)$ is surjective. Tensoring the quotient field Q of Λ,

$$i \otimes 1 : \mathbf{h}_\chi(\Gamma_0(N\mathbf{p}); Q) = \mathbf{h} \otimes_\Lambda Q \to S \otimes_\Lambda Q = \mathcal{S}_\chi(\Gamma_0(N\mathbf{p}); Q)$$

again by the result over now the field Q. Thus i is an isomorphism. Since $\mathbf{h}$ is the Λ-dual of the Λ-free module S, $\mathbf{h}$ is Λ-free. Then by applying $\mathrm{Hom}_\Lambda(?, \Lambda)$ to $\mathbf{h} \cong \mathrm{Hom}_\Lambda(S, \Lambda)$, we recover

$$S = \mathrm{Hom}_\Lambda(\mathrm{Hom}_\Lambda(S, \Lambda), \Lambda) \cong \mathrm{Hom}_\Lambda(\mathbf{h}, \Lambda),$$

as desired. □

We get the following control theorem for Hecke algebras from Theorem 2.13 and Corollary 2.14.

Corollary 2.18. *We have a canonical isomorphism for $k \geq 2$:*

$$\mathbf{h}/(t - \gamma^k)\mathbf{h} \cong h_k^{ord}(\Gamma_0(N\mathbf{p}), \chi\omega^{-k}; W)$$

sending $T(n)$ to $T(n)$ and $U(\ell)$ to $U(\ell)$.

2.7. **Hecke eigenforms and algebra homomorphisms.** If $0 \neq f \in E \subset R[[q]]$ as in (d1-3) the previous section and $f|T(n) = \lambda(T(n))f$ with scalar $\lambda(T(n)) \in R$, then we have an R-algebra homomorphism $\lambda : \mathcal{H}(E) \to R$ given by $f|h = \lambda(h)f$. Then $\lambda(T(n))a(1, f) = a(1, f|T(n)) = \langle T(n), f\rangle = a(n, f)$. If $a(1, f) = 0$, this implies $f = 0$; so, we conclude $a(1, f) \neq 0$. Thus dividing by $a(1, f)$, we may assume that $a(n, f) = \lambda(T(n)) \in R$ (in particular $a(1, f) = 1$). We call f a Hecke eigenform if f is an eigenvector of all $T(n)$ and $a(1, f) = 1$. Write $\mathcal{E}(E)$ for the set of all Hecke eigenforms in E. Then Theorem 1.16 implies

Corollary 2.19. *Let the notation be as in* (d1–3). *We have a canonical identity $\mathcal{E}(E) \cong \mathrm{Hom}_{ALG_{/R}}(\mathcal{H}(E), R) = \mathrm{Spec}(\mathcal{H}(E))(R)$ by $f \leftrightarrow \lambda$ with $a(n, f) = \lambda(T(n))$ for all $n > 0$.*

Taking $R = B$ and $E = S_k(\Gamma_1(N); B)$, put $h_k(\Gamma_1(N); B) = \mathcal{H}(S_k(\Gamma_1(N); b))$. Then $h_k(\Gamma_1(N); B) = h_k(\Gamma_1(N); \mathbb{Z}) \otimes_{\mathbb{Z}} B$. Since

$$\mathrm{Hom}_{ALG}(h_k(\Gamma_1(N); \mathbb{Z}), \overline{\mathbb{Z}}) = \mathrm{Hom}_{ALG}(h_k(\Gamma_1(N); \mathbb{Z}) \otimes_{\mathbb{Z}} \overline{\mathbb{Z}}, \overline{\mathbb{Z}}) = \mathrm{Hom}_{ALG}(h_k(\Gamma_1(N); \overline{\mathbb{Z}}), \overline{\mathbb{Z}})$$

for any $f = \sum_{n=1}^\infty \lambda(T(n))q^n \in \mathcal{E}(S_k(\Gamma_1(N), \overline{\mathbb{Z}}))$ and $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, $\sigma \circ \lambda$ is associated another $f^\sigma \in \mathcal{E}(S_k(\Gamma_1(N), \overline{\mathbb{Z}}))$. Thus $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the set of Hecke eigenforms. This is also true for $\mathcal{E}(G_k(\Gamma_1(N); \overline{\mathbb{Q}}))$ even if $\lambda(T(n))$ only determine the q-expansion coefficients $a(n, f)$ with $n > 0$. Indeed, first of all, f^σ exists for any $f \in G_k(\Gamma_1(N))$ and $\sigma \in \mathrm{Aut}(\mathbb{C}/\mathbb{Q})$, as f is a linear combination of a basis $\{f_i\}$ of $G_k(\Gamma_1(N); \mathbb{Q})$. Secondly, if $a(n, f') = \sigma(a(n, f))$ for all $n > 0$ with $f' \in G_k(\Gamma_1(N))$, $f^\sigma - f'$ is a constant in $G_k(\Gamma_1(N))$ which has to be 0 (why?). Thus $f' = f^\sigma$. This prove rationality of the constant term in a number field K if $a(n, f) \in K$ for all $n > 0$ (in particular, $L(1-k, \chi) \in \mathbb{Q}[\chi]$ if a Dirichlet character χ satisfies $\chi(-1) = (-1)^k$). Similarly, writing $\overline{Q}$ for an algebraic closure of $Q = Frac(\Lambda)$ and $\overline{\Lambda}$ for integral closure of Λ in $\overline{Q}$, $\mathrm{Gal}(\overline{Q}/Q)$ acts on $\mathcal{E}(\mathcal{S}_\chi(\Gamma_0(N\mathbf{p}); \overline{\Lambda}))$

3. Galois representations

We describe modular two dimensional galois representations and its Λ-adic version. Since the field $\mathbb{Q}[\mu_N]$ generated by a primitive N-th root of unity ζ has Galois group canonically isomorphic to $(\mathbb{Z}/N\mathbb{Z})^\times$. Indeed, fro $\sigma \in \mathrm{Gal}(\mathbb{Q}[\mu_N]/\mathbb{Q})$, we have $\zeta^\sigma = \zeta^d$ with some $d \in \mathbb{Z}$, and the association $\sigma \mapsto (d \bmod N)$ gives an isomorphism $\mathrm{Gal}(\mathbb{Q}[\mu_N]/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times$. This any Dirichlet character χ can be regarded as a Galois character $\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \overline{\mathbb{Q}}^\times$ factoring through $\mathrm{Gal}(\mathbb{Q}[\mu_N]/\mathbb{Q})$. Since $\mathbb{Q}[\mu_N]$ is unramified outside N, we have well defined $Frob_p \in \mathrm{Gal}(\mathbb{Q}[\mu_N]/\mathbb{Q})$ if $p \nmid N$, and we haves $\chi(Frob_p) = p$

3.1. **Modular two dimensional Galois representations.** Since

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

by duality we have $h_k(\Gamma_1(N); \mathbb{C}) = \bigoplus_\chi h_k(\Gamma_0(N), \chi; \mathbb{C})$. Thus any Hecke eigenform in $S_k(\Gamma_1(N))$ belongs $S_k(\Gamma_0(N), \chi)$ for some χ and the cofrresponding algebra homomorphism $\lambda : h_k(\Gamma_1(N); \mathbb{Z}) \to \mathbb{C}$ factors through $h_k(\Gamma_0(N), \chi; \mathbb{Z}[\chi])$. In this case, we say that λ has Neben character χ. Here is an important theorem we admit (cf. [GME] Section 4.2):

Theorem 3.1. *Let $\lambda : h_k(\Gamma_1(N); \mathbb{Z}) \to \overline{\mathbb{Q}}$ be an algebra homomorphism, with Neben character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{Q}}^\times$. Then for the finite extension $\mathbb{Q}[\lambda]$ generated over $\mathbb{Q}$ by $\lambda(T(n))$ and a prime ideal $\mathfrak{l}$ of $O := O_{\mathbb{Q}[\lambda]}$ with completion $O_\mathfrak{l} = \varprojlim_n O/\mathfrak{l}^n$, there exists a unique absolutely irreducible Galois representations $\rho_{\lambda,\mathfrak{l}}$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ into $GL_2(O_\mathfrak{l})$ such that*

1. *$\rho_{\lambda,\mathfrak{l}}$ is unramified outside Nl for the rational prime $l \in \mathfrak{l}$;*
2. *For each prime p outside Nl,*

$$\det(1 - \rho_{\lambda,\mathfrak{l}}(Frob_p)T) = 1 - \lambda(T(p))T + p^{k-1}\chi(p)T^2;$$

3. *We have $\det(\rho_{\lambda,\mathfrak{l}}(c)) = -1$ for each complex conjugation c (such a representation is called an "odd" representation);*
4. *For the l–adic cyclotomic character ν_l, we have $\det \rho_{\lambda,\mathfrak{l}} = \chi\nu_l^{k-1}$, where we regard χ as a Galois character given by $\chi(Frob_p) = \chi(p)$ for primes p outside Nl as above.*

This theorem is due to Eichler for $N = 11$, $\chi = 1$ and $k = 2$, to Shimura for all cases of $k = 2$, to Deligne for all cases of $k \geq 2$ and to Deligne–Serre for $k = 1$.

If a system of Galois representations $\rho = \{\rho_\mathfrak{l} : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to GL_n(O_{T,\mathfrak{l}})\}$ for a finite extension F and T over $\mathbb{Q}$ satisfies

1. There exists a finite set S of primes of O_K such that $\rho_\mathfrak{l}$ is unramified outside S and any prime ideal over $\mathfrak{l} \cap \mathbb{Z} = (l)$;
2. For any prime $\mathfrak{p} \notin S \cup \{\mathfrak{l}'|l\}$, $H_\mathfrak{p}(X) := \det(1_n - \rho_\mathfrak{l}(Frob_\mathfrak{p})X)$ is in $T[X]$ and is independent of $\mathfrak{l}$,

we call $\{\rho_\mathfrak{l}\}_\mathfrak{l}$ a (weak) compatible system of n-dimensional Galois representations with coefficients in T. We define the L-function of ρ to be

$$L(s,\rho)=\prod_{\mathfrak{p}} H_\mathfrak{p}(N(\mathfrak{p}^{-s})^{-1}.$$

Thus $\rho_\lambda := \{\rho_{\lambda,\mathfrak{l}}\}$ give a modular two dimensional compatible system with coefficients in $\mathbb{Q}[\lambda]$ associated to a Hecke eigenform on $GL(2)$, and one can prove $L(s,\rho_\lambda) = \sum_{n=1}^\infty \lambda(T(n)n^{-s}$ which has Euler factor as in the above theorem (see [IAT] §3.2).

The cyclotomic character ν_l is given by the Galois action on $\mu_{l^\infty}(\overline{\mathbb{Q}})$. For any l-adic integer z with l-adic expansion $z=\sum_{n=0} c_n l^n$ ($c_n\in[0,l-1]\cap\mathbb{Z}$), writing $z_m=\sum_{n=0}^m c_n l^n\in\mathbb{Z}$, if $\zeta\in\mu_{l^r}(\overline{\mathbb{Q}})$, we can define $\zeta^z=\lim_{n=0}^\infty \zeta^{z_n}=\zeta^{z_r}$ as $z_m\equiv z_r \mod l^r$ for all $m\ge r$. Then $\zeta^\sigma=\zeta^{\chi(\sigma)}$ with $\chi(\sigma)\in\mathbb{Z}_l^\times$ for all $\zeta\in\mu_{l^\infty}(\overline{\mathbb{Q}})$. Since $\mu_{l^\infty}(\overline{\mathbb{Q}})\cong\mu_{l^\infty}(\overline{\mathbb{F}}_p)$ (as long as $p\nmid l$) by $\zeta\mapsto(\zeta \mod \mathfrak{P})$ for a fixed prime $\mathfrak{P}$ over (p) in $\overline{\mathbb{Z}}$), we have $\zeta^{Frob_p}=\zeta^p$ for all $\zeta\in\mu_{l^\infty}(\overline{\mathbb{Q}})$ (as $Frob_p$ acts on $\overline{\mathbb{F}}_p$ by $x\mapsto x^p$). Thus $\nu_l(Frob_p)=p$, and $\chi\nu^k:=\{\chi\nu_l^k\}_l$ is a one dimensional compatible system (coming from $GL(1)$).

Exercise 3.2. *Identify the fixed field K_l of* $\mathrm{Ker}(\nu_l)$ *in $\overline{\mathbb{Q}}$, and prove that $K_l\cap K_q=\mathbb{Q}$ if q is a prime different from l (even if $\nu_q(Frob_p)=\nu_l(Frob_p)$ as long as $p\nmid ql$). In addition, prove that $\nu_l(c)=-1$ for complex conjugation c.*

For a given $\lambda\in\mathrm{Hom}_{ALG}(\mathbf{h}_k(\Gamma_1(N);\mathbb{Z}),\overline{\mathbb{Q}})$, we consider

$$\mathcal{E}_\lambda=\{f\in\bigcup_M \mathcal{E}(S_k(\Gamma_1(M))) : f|T(n)=\lambda(T(l))f \text{ for almost all primes } l\}.$$

By Chebotarev density theorem (in algebraic number theory), the compatible system associated to any Hecke eigenform $f\in\mathcal{E}_\lambda$ is isomorphic to ρ_λ. Therefore we may assume that N is the minimal level appearing in the levels of forms in $\mathcal{E}_\lambda$. We call such λ *primitive*. The level of primitive λ is alled the conductor of any of the member of $\mathcal{E}_\lambda$. By the theory of new/old forms described in [MFM] Chapter 4, Hecke eigenform in $\mathcal{E}_\lambda$ associated to a primitive λ is unique, and the form is also called a primitive form. For a primitive from f associated to a primitive λ, its Hecke L-function $L(s,f)=L(s,\rho_\lambda)$ satisfies a functional equation of the form $s\leftrightarrow k-s$.

Here is a more close information about ramification:

Theorem 3.3. *Let $\lambda: h_k(\Gamma_1(N);\mathbb{Z})\to\overline{\mathbb{Q}}$ be a primitive algebra homomorphism with Neben character χ and conductor N. Then we have*

(1) (Deligne, Mazur–Wiles) *Suppose $k\ge 2$ and that $\lambda(T(p))$ or $\lambda(U(p))$ is a unit in the $\mathfrak{p}$-adic integer ring of $\mathbb{Q}[\lambda]$ for a prime $\mathfrak{p}|p$. Then the restriction of $\rho_{\lambda,\mathfrak{p}}$ to the decomposition group $D_{\mathfrak{P}/p}$ is isomorphic to an upper triangular representation*

$$\sigma\mapsto\begin{pmatrix}\epsilon(\sigma) & *\\ 0 & \delta(\sigma)\end{pmatrix},$$

where δ is unramified and $\delta(Frob_p)$ is the unique $\mathfrak{p}$–adic unit root of $X^2-\lambda(T)X+\chi(p)p^{k-1}=0$ for $T=T(p)$ or $U(p)$ according as $p\nmid N$ or $p|N$. Here we have used the convention that $\chi(p)=0$ if $p|N$.

(2) (Langlands, Carayol) *Let p be a prime different from l, and let C be the conductor of χ. Write $N = p^e N'$ (resp. $C = p^{e'} C'$) so that $p \nmid N'$ (resp. $p \nmid C'$).*
   (a) If $e = e' > 0$, $\rho_{\lambda,\mathfrak{l}}$ restricted to the inertia group $I_{\mathfrak{P}/p}$ is equivalent to:

$$\sigma \mapsto \left(\begin{smallmatrix} \chi(\sigma) & 0 \\ 0 & 1 \end{smallmatrix}\right).$$

   Moreover ρ restricted to the decomposition group $D_{\mathfrak{P}/p}$ is still diagonal, and writing δ_p for the unique unramified character appearing in $\rho_{\lambda,\mathfrak{l}}|_{D_{\mathfrak{P}/p}}$, we have $\delta_p(Frob_{\mathfrak{P}}) = \lambda(U(p))$.
   (b) If $e = 1$ and $e' = 0$, $\rho_{\lambda,\mathfrak{l}}$ restricted to the decomposition group $D_{\mathfrak{P}/p}$ for $\mathfrak{P}|p$ is ramified and is equivalent to an upper triangular representation:

$$\sigma \mapsto \begin{pmatrix} \eta(\sigma)\nu_\ell(\sigma) & * \\ 0 & \eta(\sigma) \end{pmatrix},$$

   where $\nu_\ell : D_{\mathfrak{P}/p} \to \mathbb{Z}_\ell^\times$ is the ℓ–adic cyclotomic character and η is an unramified character taking $Frob_{\mathfrak{P}}$ to $\lambda(U(p))$.

(4) (Deligne-Serre) *If $k = 1$, then there exists a complex continuous representation $\rho_0 : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Q}(\lambda)) \subset GL_2(\mathbb{C})$ unramified outside N with finite image, which is isomorphic to $\rho_{\lambda,\mathfrak{l}}$ over $\mathbb{Q}_\ell(\lambda)$ for all $\mathfrak{l}$.*

Here is a big theorem of Khare–Wintenberger (we state it in some particular cases treated above):

Theorem 3.4 (Khare–Wintenberger)**.** *If a two dimensional odd compatible system $\rho = \{\rho_{\mathfrak{l}}\}_{\mathfrak{l}}$ with coefficients T satisfies*

(1) $\det(\rho) = \chi\nu^{k-1}$ *for a Dirichlet character χ with $\chi(-1) = (-1)^k$ for an integer $k \geq 1$,*
(2) *for some prime $\mathfrak{p}|p$ of O_T, $\rho_{\mathfrak{p}}|_{D_{\mathfrak{P}/p}} \cong \left(\begin{smallmatrix} \epsilon & * \\ 0 & \delta \end{smallmatrix}\right)$ for an unramified character δ,*

then there exists a primitive $\lambda : h_k(\Gamma_1(N); \mathbb{Z}) \to \overline{\mathbb{Q}}$ such that $\rho \cong \rho_\lambda$.

This is in their celebrated sequnce of papers proving Serre's mod p modularity conjecture. Try find it in that long papers! For any two dimensional compatible system ρ, $\det(\rho)$ is forced to be of the form $\chi\nu^{k-1}$ for some integer k (not necessarily positive). Replacing ρ by $\rho \otimes \nu^m$ given by $(\rho \otimes \nu^m(\sigma) = \nu(\sigma)^m\rho(\sigma)$, we can achieve $k \geq 1$; so, the first condition is not something restrictive. If ρ is geometric (i.e., coming from cohomology theory of projective varieties), choosing minimal m making $k \geq 1$, it is expected to find $\mathfrak{p}$ satisfying the second condition (if ρ comes from an abelian variety, this is true). Indeed, the theorem of Khare-Wintenberger only requires this "geometricity" not really the second condition.

3.2. **Pseudo representations.** In order to make Galois representation attached to Λ-adic eigenform, pseudo representations are very useful. We recall the definition of pseudo representations (due to Wiles) when $n = 2$. See [MFG] §2.2.2 for a higher dimensional generalization due to R. Taylor.

In this subsection, the coefficient ring A is always a local ring with maximal ideal $\mathfrak{m}_A$. We write $\kappa = A/\mathfrak{m}_A$. For simplicity, we assume that 2 is invertible in A. We would like to characterize the trace of a representation of a group G.

We describe in detail traces of degree 2 representations $\rho : G \to GL_2(A)$ when G contains c such that $c^2 = 1$ and $\det\rho(c) = -1$. Let $V(\rho) = A^2$ on which G acts by ρ. Since 2 is invertible in A, we know that $V = V(\rho) = V_+ \oplus V_-$ for $V_\pm = \frac{1\pm c}{2}V$. For $\overline{\rho} = \rho \mod \mathfrak{m}_A$, we write $\overline{V} = V(\overline{\rho}) = \kappa^2$. Then similarly as above, $\overline{V} = \overline{V}_+ \oplus \overline{V}_-$ and $\overline{V}_\pm = V_\pm/\mathfrak{m}_A V_\pm$. Since $\dim_\kappa \overline{V} = 2$ and $\det\overline{\rho}(c) = -1$, $\dim_\kappa \overline{V}_\pm = 1$. This shows that $\overline{V}_\pm = \kappa\overline{v}_\pm$ for $\overline{v}_\pm \in \overline{V}_\pm$. Take $v_\pm \in V_\pm$ such that $v_\pm \mod \mathfrak{m}_A V_\pm = \overline{v}_\pm$, and define $\phi_\pm : A \to V_\pm$ by $\phi(a) = av_\pm$. Then $\phi_\pm \mod \mathfrak{m}_A V$ is surjective by Nakayama's lemma. Note that $\phi_\pm : A \cong V_\pm$ as A-modules. In other words, $\{v_-, v_+\}$ is an A–base of V. We write $\rho(r) = \begin{pmatrix} a(r) & b(r) \\ c(r) & d(r) \end{pmatrix}$ with respect to this base. Thus $\rho(c) = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Define another function $x : G \times G \to A$ by $x(r,s) = b(r)c(s)$. Then we have

(W1) $a(rs) = a(r)a(s) + x(r,s)$, $d(rs) = d(r)d(s) + x(s,r)$ and
$$x(rs,tu) = a(r)a(u)x(s,t) + a(u)d(s)x(r,t) + a(r)d(t)x(s,u) + d(s)d(t)x(r,u);$$
(W2) $a(1) = d(1) = d(c) = 1$, $a(c) = -1$ and $x(r,s) = x(s,t) = 0$ if $s = 1, c$;
(W3) $$x(r,s)x(t,u) = x(r,u)x(t,s).$$

These are easy to check: We have
$$\begin{pmatrix} a(r) & b(r) \\ c(r) & d(r) \end{pmatrix}\begin{pmatrix} a(s) & b(s) \\ c(s) & d(s) \end{pmatrix} = \begin{pmatrix} a(rs) & b(rs) \\ c(rs) & d(rs) \end{pmatrix}.$$
Then by computation, $a(rs) = a(r)a(s) + b(r)c(s) = a(r)a(s) + x(r,s)$. Similarly, we have $b(rs) = a(r)b(s) + b(r)d(s)$ and $c(rs) = c(r)a(s) + d(r)c(s)$. Thus

$$\begin{aligned} x(rs,tu) = b(rs)c(tu) &= (a(r)b(s) + b(r)d(s))(c(t)a(u) + d(t)c(u)) \\ &= a(r)a(u)x(s,t) + a(r)d(t)x(s,u) + a(u)d(s)x(r,t) + d(s)d(t)x(r,u). \end{aligned}$$

A triple $\{a, d, x\}$ satisfying the three conditions (W1-3) is called a *pseudo representation* of Wiles of (G, c). For each pseudo-representation $\tau = \{a, d, x\}$, we define
$$\mathrm{Tr}(\tau)(r) = a(r) + d(r) \quad \text{and} \quad \det(\tau)(r) = a(r)d(r) - x(r,r).$$
By a direct computation using (W1-3), we see
$$a(r) = \frac{1}{2}(\mathrm{Tr}(\tau)(r) - \mathrm{Tr}(\tau)(rc)), \quad d(r) = \frac{1}{2}(\mathrm{Tr}(\tau)(r) + \mathrm{Tr}(\tau)(rc))$$
and
$$x(r,s) = a(rs) - a(r)a(s), \quad \det(\tau)(rs) = \det(\tau)(r)\det(\tau)(s).$$
Thus the pseudo-representation τ is determined by the trace of τ as long as 2 is invertible in A.

Proposition 3.5 (A. Wiles, 1988)**.** *Let G be a group and $R = A[G]$. Let $\tau = \{a, d, x\}$ be a pseudo-representation (of Wiles) of (G, c). Suppose either that there exists at least one pair $(r, s) \in G \times G$ such that $x(r, s) \in A^\times$ or that $x(r, s) = 0$ for all $r, s \in G$. Then there exists a representation $\rho : R \to M_2(A)$ such that $\mathrm{Tr}(\rho) = \mathrm{Tr}(\tau)$ and $\det(\rho) = \det(\tau)$ on G. If A is a topological ring, G is a topological group and all maps in τ are continuous on G, then ρ is a continuous representation of G into $GL_2(A)$ under the topology on $GL_2(A)$ induced by the product topology on $M_2(A)$.*

Proof. When $x(r,s)=0$ for all $r,s\in G$, we see from (W1) that $a,d:G\to A$ satisfies $a(rs)=a(r)a(s)$ and $d(rs)=d(r)d(s)$. Thus a,d are characters of G, and we define $\rho:G\to GL_2(A)$ by $\rho(g)=\begin{pmatrix} a(g) & 0\\ 0 & d(g)\end{pmatrix}$, which satisfies the required property.

We now suppose $x(r,s)\in A^\times$ for $r,s\in G$. Then we define $b(g)=x(g,s)/x(r,s)$ and $c(g)=x(r,g)$ for $g\in G$. Then by (W3), $b(g)c(h)=x(r,h)x(g,s)/x(r,s)=x(g,h)$. Put $\rho(g)=\begin{pmatrix} a(g) & b(g)\\ c(g) & d(g)\end{pmatrix}$. By (W2), we see that $\rho(1)$ is the identity matrix and $\rho(c)=\left(\begin{smallmatrix}-1 & 0\\ 0 & 1\end{smallmatrix}\right)$. By computation,

$$\rho(g)\rho(h)=\begin{pmatrix} a(g) & b(g)\\ c(g) & d(g)\end{pmatrix}\begin{pmatrix} a(h) & b(h)\\ c(h) & d(h)\end{pmatrix}=\begin{pmatrix} a(g)a(h)+b(g)c(h) & a(g)b(h)+b(g)d(h)\\ c(g)a(h)+d(g)c(h) & d(g)d(h)+c(g)b(h)\end{pmatrix}.$$

By (W1), $a(gh)=a(g)a(h)+x(g,h)=a(g)a(h)+b(g)c(h)$ and $d(gh)=d(g)d(h)+x(h,g)=d(g)d(h)+b(h)c(g)$. Now let us look at the lower left corner:

$$c(g)a(h)+d(g)c(h)=x(r,g)a(h)+d(g)x(r,h).$$

Now apply (W1) to $(1,r,g,h)$ in place of (r,s,t,u), and we get

$$c(gh)=x(r,gh)=a(h)x(r,g)+d(g)x(r,h),$$

because $x(1,g)=x(1,h)=0$. As for the upper right corner, we apply (W1) to $(g,h,1,s)$ in place of (r,s,t,u). Then we get

$$b(gh)x(r,s)=x(gh,s)=a(g)x(h,s)+d(h)x(g,s)=(a(g)b(h)+d(h)b(g))x(r,s),$$

which shows that $\rho(gh)=\rho(g)\rho(h)$. We now extends ρ linearly to $R=A[G]$. This shows the first assertion. The continuity of ρ follows from the continuity of each entries, which follows from the continuity of τ. □

Start from an absolutely irreducible representation $\overline{\rho}:G\to GL_n(\kappa)$. Here a representation of a group into $GL_n(K)$ for a field K is called *absolutely irreducible* if it is irreducible as a representation into $GL_n(\overline{K})$ for an algebraic closure $\overline{K}$ of K.

Exercise 3.6. *Give an example of irreducible representations of a group G into $GL_2(\mathbb{Q})$ which is not absolutely irreducible.*

We fix an absolutely irreducible representation $\overline{\rho}:G\to GL_2(\kappa)$ with $\det(\overline{\rho})(c)=-1$. If we have a representation $\rho:G\to GL_2(A)$ with $\rho \mod \mathfrak{m}_A\sim\overline{\rho}$, then $\det(\rho(c))\equiv\det(\overline{\rho}(c))\equiv -1 \mod \mathfrak{m}_A$. Since $c^2=1$, if 2 is invertible in A ($\Leftrightarrow$ the characteristic of κ is different from 2), $\det(\rho(c))=-1$. This is a requirement to have a pseudo-representation τ_ρ of Wiles associated to ρ. Since $\overline{\rho}$ is absolutely irreducible, we find $r,s\in G$ such that $b(r)\not\equiv 0 \mod \mathfrak{m}_A$ and $c(s)\not\equiv 0 \mod \mathfrak{m}_A$. Thus τ_ρ satisfies the condition of Proposition 3.5. Conversely if we have a pseudo representation $\tau:G\to A$ such that $\tau\equiv\overline{\tau} \mod \mathfrak{m}_A$ for $\overline{\tau}=\tau_{\overline{\rho}}$, again we find $r,s\in G$ such that $x(r,s)\in A^\times$. The correspondence $\rho\mapsto\tau_\rho$ induces a bijection:

$$\{\rho:G\to GL_2(A):\text{representation}|\rho \mod \mathfrak{m}_A\sim\overline{\rho}\}/\sim\ \leftrightarrow \{\tau:G\to A:\text{pseudo-representation}|\tau \mod \mathfrak{m}_A=\overline{\tau}\}, \tag{3.1}$$

where $\overline{\tau} = \tau_{\overline{\rho}}$ and "$\sim$" is the conjugation under $GL_2(A)$. The map is surjective by Proposition 3.5 combined with Proposition 3.7 and one to one by Proposition 3.7 we admit, because a pseudo-representation is determined by its trace.

Proposition 3.7 (Carayol, Serre, 1994)**.** *Let A be an pro-artinian local ring with finite residue field κ. Let $R = A[G]$ for a profinite group G. Let $\rho : R \to M_n(A)$ and $\rho' : R \to M_{n'}(A)$ be two continuous representations. If $\overline{\rho} = \rho \mod \mathfrak{m}_A$ is absolutely irreducible and $\mathrm{Tr}(\rho(\sigma)) = \mathrm{Tr}(\rho'(\sigma))$ for all $\sigma \in G$, then $\rho \sim \rho'$.*

See [MFG] Proposition 2.13 for a proof of this result.

3.3. **Λ-adic Galois representations.** Let $\mathbf{h} = \mathbf{h}_\chi(\Gamma_0(N\mathbf{p}); \Lambda)$ and $S = \mathcal{S}_\chi(\Gamma_0(N\mathbf{p}); \overline{Q})$. Then $\mathcal{E}(S) \cong \mathrm{Hom}_{ALG_{/\Lambda}}(\mathbf{h}, \overline{Q})$. Since $\mathrm{rank}_\Lambda \mathbf{h} < \infty$, for each $\lambda \in \mathcal{E}(S)$, $Q(\lambda) := \mathrm{Im}(\lambda)\cdot Q$ is a finite extension of Q and $\Lambda[\lambda] = \mathrm{Im}(\lambda)$ is an integral extension of Λ. Write $\widetilde{\Lambda}[\lambda]$ for the integral closure of Λ in $Q(\lambda)$; so, $\widetilde{\Lambda}[\lambda] \supset \Lambda[\lambda]$. Here facts from commutative ring theory we admit:

Lemma 3.8. (0) *$\Lambda[\lambda]$ is noetherian;*
(1) *$\widetilde{\Lambda}[\lambda]$ and $\Lambda[\lambda]$ are local rings;*
(2) *$\widetilde{\Lambda}[\lambda]/\Lambda[\lambda]$ is a torsion Λ-module of finite type;*
(3) *$\widetilde{\Lambda}[\lambda]$ is Λ-free of rank equal to $\dim_Q Q(\lambda)$.*

Since $\mathbf{h}$ is free of finite rank over noetherian Λ, it is noetherian; so, its image $\Lambda[\lambda]$ is noetherian, showing (0). Since the going-up and going-down theorems hold for $\widetilde{\Lambda}[\lambda]/\Lambda[\lambda]/\Lambda$, the assertion (1) holds (as Λ is a local ring with $\mathfrak{m}_\Lambda = \mathfrak{m}_W\Lambda + (T)$).

Exercise 3.9. *prove that $\mathfrak{m} = (p) + (T)$ is the unique maximal ideal of $\Lambda_{\mathbb{Z}_p} = \mathbb{Z}_p[[T]]$.*

If you do not know the going-up/down theorems, take a look at any commutative ring theory book (e.g., [CRT] Theorem 9.4). In algebraic number theory, if any subring R in a finite extension field F of $\mathbb{Q}$ (resp. $\mathbb{Q}_p$) is finitely generated as modules over $\mathbb{Z}$ (resp. $\mathbb{Z}_p$), O_F/R is a torsion module over $\mathbb{Z}$ (resp. $\mathbb{Z}_p$). The assertion (2) is its analogue replacing $(\mathbb{Z}, F)$ (or $(\mathbb{Z}_p, F)$) by $(\Lambda, Q(\lambda))$, and the proof is essentially the same in the three cases); so, try prove yourself. The assertion (3) is more difficult and follows from, for example, [CRT] Theorem 23.1 and 23.8 combined.

Again in

$$\{\varphi \in \mathrm{Hom}_{ALG_{/\Lambda}}(\mathbf{h}_\chi(\Gamma_0(N\mathbf{p}); \Lambda), \overline{Q}) | \varphi(T(l)) = \lambda(T(l)) \text{ for almost all primes } l\},$$

there is a unique φ with minimal N. We call such φ *primitive*. Hereafter, we suppose that $\lambda \in \mathrm{Hom}_{ALG_{/\Lambda}}(\mathbf{h}, \overline{Q})$ is primitive.

Exercise 3.10. *Is $\mathrm{Im}(\lambda)$-free over Λ?*

A point $P \in \mathrm{Spec}(\Lambda[\lambda])(\overline{\mathbb{Q}}_p) = \mathrm{Hom}_{ALG_{/W}}(\Lambda[\lambda], \overline{\mathbb{Q}}_p)$ is called *arithmetic* if $P(t - \gamma^k) = 0$ for some $k \geq 2$. From time to time, we write P for a prime ideal of $\Lambda[\lambda]$ given by $\mathrm{Ker}(P : \Lambda[\lambda], \overline{\mathbb{Q}}_p)$. If P is arithmetic, $\lambda_P = P \circ \lambda$ kills $(t - \gamma^k)\mathbf{h}$; so, it factors through $h_k^{ord}(\Gamma_0(N\mathbf{p}), \chi\omega^{-k}; W) = \mathbf{h}/(t - \gamma^k)\mathbf{h}$. Therefore we get an algebra homomorphism

$\lambda_P : h_k^{ord}(\Gamma_0(N\mathbf{p}), \chi\omega^{-k}; W) \to \overline{\mathbb{Q}}_p$ with $\lambda(T(n)) = \lambda_P(T(n))$ for all n; so, we have Galois representation $\rho_P = \rho_{\lambda_P,\mathfrak{p}}$ as in and Theorems 3.1 and 3.12 associated to λ_P. Here $\mathfrak{p}$ is the prime ideal of $\mathbb{Q}(\lambda_P)$ induced by $\mathbb{Q}(\lambda_P) \hookrightarrow \mathbb{Q}_p(\lambda_P)$. Consider $\mathrm{Tr}(\rho_P)$ which satisfies $\mathrm{Tr}(\rho_P)(Frob_l) = \lambda_P(T(l))$ for all primes $l \nmid Np$.

Exercise 3.11. *Let $P_1, P_2, \ldots$ be an infinite sequence of distinct primes of $\Lambda[\lambda]$. prove $\bigcap_n P_n = (0)$ in $\Lambda[\lambda]$.*

By this exercise, we have

$$\bigcap_{P:\text{arithmetic}} \mathrm{Ker}(P) = (0).$$

Therefore by $i := \prod_{P:\text{arithmetic}} P : \Lambda[\lambda] \to \prod_P \mathbb{Q}_p(\lambda_P)$ is an embedding, where $\mathbb{Q}_p(\lambda)$ is the subfield of $\overline{\mathbb{Q}}_p$ generated by $\lambda_P(T(n))$ for all n. For a finite set S inside $\{P : \text{arithmetic}\} \subset \mathrm{Spec}(\Lambda[\lambda])(\overline{\mathbb{Q}}_p)$, we consider also $i_S : \prod_{P\in S} P : \Lambda[\lambda] \to \prod_{P\in S} \mathbb{Q}_p(\lambda_P)$. Then $\mathrm{Im}(i_S) \cong \Lambda/P_S\Lambda$ for $P_S = \bigcap_{P\in S} \mathrm{Ker}(P)$, and $\Lambda[\lambda] = \varprojlim_S \lambda[\lambda]/P_S$ by the above lemma.

Put $\varphi = \prod_{P:\text{arithmetic}} \rho_P : \mathrm{Gal}(\mathbb{Q}^{(Np)}/\mathbb{Q}) \to GL_2(\prod_{P:\text{arithmetic}} \mathbb{Q}_p(\lambda_P))$ and $\varphi_S = \prod_{P\in S} \rho_P \to GL_2(\prod_{P\in S} \mathbb{Q}_p(\lambda_P))$, where $\mathbb{Q}^{(Np)}$ is the maximal extension unramified outside Np (i.e., fixed field of the closed subgroup generated by all conjugates of $I_{\mathfrak{L}/l}$ for all $l|Np$). The map φ and φ_S are representations. Note that

$$\mathrm{Tr}(\varphi_S(Frob_l)) = \prod_{P\in S} \lambda_P(T(l)) = i_S(\lambda(T(l)))$$

for all primes $l \nmid Np$. Since φ_S is continuous under the p-profinite topology (which is equal to the p-adic topology) of the target, by the Chebotarev density theorem asserting that $\{Frob_l : l \nmid Np\} \subset \mathrm{Gal}(\mathbb{Q}^{(Np)}/\mathbb{Q})$ is dense, we conclude $\mathrm{Tr}(\varphi_S)(\sigma) \in \mathrm{Im}(i_S) \cong \Lambda[\lambda]/P_S$. Taking the projective limit with respect to S (and inclusion relation $S \subset S'$), we find that

$$\mathrm{Tr}(\varphi)(\sigma) = \varprojlim_S \mathrm{Tr}(\varphi_S)(\sigma) \in \varprojlim_S \mathrm{Im}(i_S) \cong \varprojlim_S \Lambda[\lambda/P_S] = \Lambda[\lambda]/\bigcap_{P:\text{arithmetic}} \mathrm{Ker}(P) = \Lambda[\lambda].$$

Since the projective limit of p-profinite topology of $\mathrm{Im}(i_S)$ is equal to the p-profinite topology of $\Lambda[\lambda]$ (which is the $\mathfrak{m}_{\Lambda[\lambda]}$-adic topology), the trace map $\mathrm{Tr}(\varphi) : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \Lambda[\lambda]$ is continuous; so, the pseudo-representation $\tau = (a, d, x)$ associated to $\mathrm{Tr}(\varphi)$ has values in $\Lambda[\lambda]$. As we will see later, ρ_P is always irreducible; so, we can find σ, τ in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $\xi = x(\sigma, \tau) \neq 0$. Thus inverting ξ and taking $\Lambda[\lambda][\frac{1}{\xi}]$, we get a Galois representation $\rho_\lambda : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\Lambda[\lambda][\frac{1}{\xi}])$ which is a projective limit of φ_S. Since φ_S is unramified outside Np, ρ_λ is unramified outside Np, and by construction $\mathrm{Tr}(\rho_\lambda)(Frob_l)) = \lambda(T(l)) \in \Lambda[\lambda]$ for all primes $l \nmid Np$. By Theorem 3.12, the maximal quotient of the space $H_0(I_{\mathfrak{P}/p}, \varphi_S)$ of φ_S on which $I_{\mathfrak{P}/p}$ acts trivially is free of rank 1 over $\Lambda[\lambda][\frac{1}{\xi}]/P_S$, again bu the limit, we have $H_0(I_{\mathfrak{P}/p}, \rho_\lambda) \cong \Lambda[\lambda][\frac{1}{\xi}]$. Since the ramification description at $l \neq p$ is independent of P (i.e., $\chi\omega^{-k}|_{I_{\mathfrak{L}/l}} = \chi|_{I_{\mathfrak{L}/l}}$), we have the same description for ρ_λ. Thus we get

Theorem 3.12. *Let $\lambda : \mathbf{h}_\chi(\Gamma_0(N);\Lambda) \to \overline{Q}$ be a primitive algebra homomorphism with Neben character χ. Then we have*

(0) There exists a continuous semi-simple Galois representation $\rho_\lambda : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\Lambda[\lambda][\frac{1}{\xi}])$ unramified outside Np for some $0 \neq \xi \in \Lambda[\lambda]$ such that

$$\mathrm{Tr}(\rho_\lambda(Frob_l)) = \lambda(T(l))$$

for all primes $l \nmid Np$ and $\det(\rho_\lambda(\sigma)) = \chi(\sigma)\nu_p(\sigma)^{-1}\boldsymbol{\nu}(\sigma)$, where $\boldsymbol{\nu} : D_{\mathfrak{P}/p} \to \Lambda^\times$ is given by $\boldsymbol{\nu}(\sigma) = A_{\nu_p(\sigma)}(T) \in \Lambda^\times$.

(1) The restriction of ρ_λ to the decomposition group $D_{\mathfrak{P}/p}$ is isomorphic to an upper triangular representation

$$\sigma \mapsto \begin{pmatrix} \epsilon(\sigma) & * \\ 0 & \delta(\sigma) \end{pmatrix},$$

where δ is unramified and $\delta(Frob_p) = \lambda(U(p))$.

(2) Let l be a prime different from p, and let C be the conductor of χ. Write $N = l^e N'$ (resp. $C = l^{e'}C'$) so that $l \nmid N'$ (resp. $l \nmid C'$).

(a) If $e = e' > 0$, ρ_λ restricted to the inertia group $I_{\mathfrak{L}/l}$ is equivalent to:

$$\sigma \mapsto \begin{pmatrix} \chi(\sigma) & 0 \\ 0 & 1 \end{pmatrix}.$$

Moreover ρ_λ restricted to the decomposition group $D_{\mathfrak{L}/l}$ is still diagonal, and writing δ_l for the unique unramified character appearing in $\rho_\lambda|_{D_{\mathfrak{L}/l}}$, we have $\delta_l(Frob_l) = \lambda(U(l))$.

(b) If $e = 1$ and $e' = 0$, ρ_λ restricted to the decomposition group $D_{\mathfrak{L}/l}$ for $\mathfrak{L}|l$ is ramified and is equivalent to an upper triangular representation:

$$\sigma \mapsto \begin{pmatrix} \eta(\sigma)\nu_l & * \\ 0 & \eta(\sigma) \end{pmatrix},$$

where η is an unramified character taking $Frob_{\mathfrak{P}}$ to $\lambda(U(l))$.

References

Books

[CGP] K. S. Brown, *Cohomology of Groups*, Graduate texts in Math. **87**, Springer, 1982

[CRT] H. Matsumura, *Commutative Ring Theory*, Cambridge studies in advanced mathematics **8**, Cambridge Univ. Press, 1986

[GME] H. Hida, *Geometric Modular Forms and Elliptic Curves*, 2000, World Scientific Publishing Co., Singapore (a list of errata posted at www.math.ucla.edu/~hida)

[IAT] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press and Iwanami Shoten, 1971, Princeton-Tokyo

[ICF] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Text in Mathematics, **83**, Springer, 1980

[LFE] H. Hida, *Elementary Theory of L–functions and Eisenstein Series*, LMSST **26**, Cambridge University Press, Cambridge, 1993

[MFG] H. Hida, *Modular Forms and Galois Cohomology*, Cambridge Studies in Advanced Mathematics **69**, 2000, Cambridge University Press

[MFM] T. Miyake, *Modular Forms*, Springer, New York-Tokyo, 1989.

[PAI] F. Q. Gouvea, *p-adic Numbers, an introduction*, Universitext, Springer, 1997