LANGLANDS' CONJECTURES FOR PHYSICISTS

MARK GORESKY

1. INTRODUCTION

This is an expanded version of several lectures given to a group of physicists at the I.A.S. on March 8, 2004. It is a work in progress: check back in a few months to see if the empty sections at the end have been completed. This article is written on two levels. Many technical details that were not included in the original lectures, and which may be ignored on a first reading, are contained in the end-notes. The first few paragraphs of each section are designed to be accessible to a wide audience. The present article is, at best, an introduction to the many excellent survey articles ([Ar, F, G1, G2, Gr, Kn, K, R1, T] on automorphic forms and Langlands' program. Slightly more advanced surveys include ([BR]), the books [Ba, Be] and the review articles [M, R2, R3].

2. THE CONJECTURE FOR $\mathbf{GL}(n, \mathbb{Q})$

Very roughly, the conjecture is that there should exist a correspondence

$$(2.0.1) \qquad \left\{ \begin{matrix} \text{nice irreducible } n \text{ dimensional} \\ \text{representations of } \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \end{matrix} \right\} \longrightarrow \left\{ \begin{matrix} \text{nice automorphic representations} \\ \text{of } \mathbf{GL}(n, \mathbb{A}_{\mathbb{Q}}) \end{matrix} \right\}$$

such that

$$(2.0.2) \qquad \{\text{eigenvalues of Frobenius}\} \longrightarrow \{\text{eigenvalues of Hecke operators}\}$$

The purpose of the next few sections is to explain the meaning of the words in this statement. Then we will briefly examine the many generalizations of this statement to other fields besides $\mathbb{Q}$ and to other algebraic groups besides $\mathbf{GL}(n)$.

3. FIELDS

3.1. **Points in an algebraic variety.** If $E \subset F$ are fields, the Galois group $\mathrm{Gal}(F/E)$ is the set of field automorphisms $\phi : E \to E$ which fix every element of F. Let $E[x_1, x_2, \ldots, x_n]$ be the algebra of polynomials in n variables, with coefficients in E. If $f_1, f_2, \ldots, f_r \in E[x_1, x_2, \ldots, x_n]$ are polynomials, denote by $X(E)$ the set of solutions

$$\{x \in E^n | \ f_1(x) = f_2(x) = \cdots = f_r(x) = 0\}.$$

We may also view the f_i as polynomials with coefficients in F, so the set $X(F)$ of solutions with coordinates in F makes sense. The Galois group $\mathrm{Gal}(F/E)$ acts on $X(F)$, fixing $X(E)$.

Then $X(F)$ is called the set of points of the algebraic variety X in the field of F. We refer to the algebraic variety X as representing the set of solutions over all extension fields of E simultaneously, but we say that X is *defined over E*. The same applies to the case when the f_i are homogeneous polynomials and $X(E)$ is the corresponding set of solutions in projective space $\mathbb{P}^{r-1}(E)$.

In particular, if X is an algebraic variety defined over the integers $\mathbb{Z}$ then it lives in both worlds: $X(\mathbb{C})$ is a complex algebraic variety, and $X \pmod{p}$ is an algebraic variety defined over $\mathbb{F}_p$ (obtained by reducing the equations for X modulo p). Moreover, for any extension field $\mathbb{F}_{p^r}$ one may consider the set of points $X \pmod{p}(\mathbb{F}_{p^r})$ with coordinates in $\mathbb{F}_{p^r}$. The amazing relation between these two worlds will be described in §4.3.

3.2. **Finite fields.** For every prime number p and every positive integer n there is a unique field $\mathbb{F}_{p^n}$ with p^n elements. If $n = 1$ then $\mathbb{F}_p = \mathbb{Z}/(p)$ is the integers modulo p. If p_1 and p_2 are prime numbers then $\mathbb{F}_{p_1^n} \subset \mathbb{F}_{p_2^m}$ if and only if $p_1 = p_2$ and n divides m. Now let $q = p^n$ (with p a prime number). Then

$$px = 0 \text{ and } x^q = x$$

for every $x \in \mathbb{F}_q$. We say that $\mathbb{F}_q$ has *characteristic p*. The Galois group $\mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$ is isomorphic to $\mathbb{Z}/(r)$ and is generated by the Frobenius $\sigma_q(x) = x^q$. This is an automorphism, for

$$(x + y)^q = x^q + qx^{q-1}y + \binom{q}{2}x^{q-2}y^2 + \cdots + y^q.$$

Each of these binomial coefficients is divisible by p so $(x + y)^q = x^q + y^q$. As r varies, these Frobenius automorphisms are compatible. Taking $p = q$ we obtain a particular element

$$\sigma_p \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p).$$

3.3. **Number fields.** A *number field* is a finite extension of $\mathbb{Q}$. Each number field may be obtained by adjoining to $\mathbb{Q}$ the roots of a polynomial $f(x)$ with rational coefficients. The algebraic closure $\overline{\mathbb{Q}} \subset \mathbb{C}$ is the "union" of all number fields: it is the set of all roots of all polynomials with rational coefficients. Just as the rational numbers $\mathbb{Q}$ consists of all fractions a/b where $a, b \in \mathbb{Z}$, any number field E consists of all fractions a/b where $a, b \in \mathfrak{o}_E$ where $\mathfrak{o}_E$ is the *ring of integers* in E. For example, if $E = \mathbb{Q}[i]$ then $\mathfrak{o}_E$ is the set of all $a + bi$ where $a, b \in \mathbb{Z}$.

3.4. **Local function fields.** Let $\mathbb{F}_q$ be a finite field and let $\mathbb{F}_q[[t]]$ be the ring of formal power series with coefficients in $\mathbb{F}_q$, and with the obvious operations of addition and multiplication. An element $a = \sum_{n \geq 0} a_n t^n$ is invertible if and only if $a_0 \neq 0$. In this case the inverse may be found by writing $b = \sum_{m \geq 0} b_m t^m$, expanding the equation $ab = 1$ and solving the resulting linear equations for the coefficients b_m. The mapping $\mathbb{F}_q[[t]] \to \mathbb{F}_q$, which takes the above element a to its constant term a_0, is a surjective ring homomorphism, so F_q is referred to as the *residue field*.

2

The field $\mathbb{F}_q((t))$ consists of all fractions a/b where $a, b \in \mathbb{F}_q[[t]]$, and we refer to $\mathbb{F}_q[[t]]$ as the *ring of integers* in the field $\mathbb{F}_q((t))$. It is easy to see that any element $A \in \mathbb{F}_q((t))$ may be expressed as a formal Laurent series

$$A = \sum_{n=N}^{\infty} A_n t^n$$

(where $N \in \mathbb{Z}$ is any integer, possibly negative) with at most finitely many terms involving negative powers of t The *valuation* of such an element A is the smallest integer n such that $A_n \neq 0$.

Similarly one can form the function field $\mathbb{C}((t))$ and its ring of integers $\mathbb{C}[[t]]$, however this case is of less interest to number theorists (and of more interest to physicists).

3.5. p-adic fields. Fix a prime number p. A *p-adic integer* is a formal power series $a = a_0 + a_1 p + a_2 p^2 + \cdots$ where $0 \leq a_i \leq p - 1$. The set of such is denoted $\mathbb{Z}_p$. Addition and multiplication are performed using power series manipulations but with a "carry", meaning that whenever we come across a coefficient a that is greater than p, we write it as $a_0 + a_1 p$, keep the a_0 part, and carry the a_1 part on to the next term. As a consequence, the mapping $a \rightarrow a_0$ defines a surjective ring homomorphism $\mathbb{Z}_p \rightarrow \mathbb{Z}/(p)$, the *residue field*. The ring $\mathbb{Z}_p$ contains most of the rational numbers. It clearly contains the integers, but it also contains the fraction a/b whenever b is not divisible by p. For example, in $\mathbb{Z}_5$ the inverse of 3 is

$$3^{-1} = 2 + 3 \cdot 5 + 1 \cdot 5^2 + 3 \cdot 5^3 + 1 \cdot 5^4 + \cdots$$

as can be easily seen by multiplying the right hand side by 3.

However the number 5 is not invertible in $\mathbb{Z}_5$ so in order to make a field we need to include its inverse, as well as that of 5^2 and so on. This leads to two descriptions of $\mathbb{Q}_p$: as set of fractions a/b where $a, b \in \mathbb{Z}_p$, or as the set of *formal Laurent series*

$$c = \sum_{n=N}^{\infty} c_n p^n$$

consisting of all formal series with finitely many negative powers of p. The *valuation* $\mathrm{val}(c)$ of c is the "degree" of the leading term in this expansion. In particular, $\mathbb{Q}_p$ contains $\mathbb{Q}$. The p-adic numbers can also be realized as the (topological) completion[1] of the rational numbers $\mathbb{Q}$ with respect to a certain[2] norm $| \ |_p$. With this metric space structure, the field $\mathbb{Q}_p$ is locally compact.

Note that $\mathbb{Q}_p$ has characteristic 0 and in fact it is possible to embed $\mathbb{Q}_p$ into the complex numbers $\mathbb{C}$, which, from now on, we will assume to have been done[3].

There are also many finite extensions of $\mathbb{Q}_p$ and these are referred to as *p-adic fields*. Each such may be obtained by "completing" a number field E at a prime ideal $\mathfrak{p}$ which contains (or "lies over") p. The p-adic field $E_{\mathfrak{p}}$ contains a ring of integers $\mathfrak{o}$ which then projects to a *residue field* $\mathfrak{o}_E \rightarrow F$ which is a finite extension of $\mathbb{F}_p$. If $\deg(E_{\mathfrak{p}}/\mathbb{Q}_p) = \deg(F/\mathbb{F}_p)$ then $E_{\mathfrak{p}}$

is said to be an *unramified* extension of $\mathbb{Q}_p$. The field $\mathbb{Q}_p$ has a unique unramified extension of each degree, but there are other extensions as well. The p-adic fields are referred to as *local fields*.

3.6. Global Function fields.
Let Y be a compact Riemann surface. Then the meromorphic functions $\mathbb{C}(Y)$ on Y form a field. Such a Y admits the structure of a (smooth) complex projective algebraic variety which may be realized as a subvariety of $\mathbb{P}^2(\mathbb{C})$. As such, it has a field of "rational functions", and this also coincides with $\mathbb{C}(Y)$. If $Y = \mathbb{P}^1(\mathbb{C})$ then its function field is the field $\mathbb{C}(x)$ of "rational functions", consisting of quotients $p(x)/q(x)$ where p, q are polynomials. If $Y' \to Y$ is a (possibly ramified) finite covering of compact Riemann surfaces then $\mathbb{C}(Y')$ is a finite extension of $\mathbb{C}(Y)$.

Similarly, suppose Y is a smooth projective algebraic curve defined over a finite field $\mathbb{F}(q)$. Let $\mathbb{F}_q(Y)$ be its field of ("rational") functions. If $Y = \mathbb{P}^1$ then $\mathbb{F}_q(Y) = \mathbb{F}_q(x)$ is the set of quotients $p(x)/q(x)$ where $p, q \in \mathbb{F}_q[x]$ are polynomimals with coefficients in $\mathbb{F}_q$. For any point $y \in Y(\mathbb{F}_q)$ a choice of coordinate t_y at y determines a completion of $\mathbb{F}_q(Y)$ which is isomorphic to the local function field $\mathbb{F}_q((t))$. For this reason the points $y \in Y$ are called *places*.

3.7. Higher dimensional fields.
The above collection of fields (together with their finite extensions and various sorts of algebraic closures) pretty much exhausts the list of fields that people have traditionally been interested in. But it is possible to construct an endless variety of new fields K from old fields k by iterating the following: two constructions (a) completing the ring of integers $\mathfrak{o}_k$ with respect to a norm, or (b) forming a field of functions, $K = k((t))$ or $K = k(Y)$. So, for example there is a function field

$$\mathbb{Q}_p(Y)((t))$$

consisting of formal Laurent polynomials with coefficients in the function field $\mathbb{Q}_p(Y)$ of p-adic functions on an n-dimensional algebraic variety Y defined over $\mathbb{Q}_p$.

3.8. The big picture.
In summary the fields of primary interest to number theorists fit into a chart (where E is a number field and $E_{\mathfrak{p}}$ is a p-adic field obtained by completing E at a prime ideal; where p is a prime number and $q = p^r$ is a power of p).

	base field	extension	base field	extension
global	$\mathbb{Q}$	E	$\mathbb{F}_p(X)$	$\mathbb{F}_q(X)$
local	$\mathbb{Q}_p$	$E_{\mathfrak{p}}$	$\mathbb{F}_p((t))$	$\mathbb{F}_q((t))$
integers	$\mathbb{Z}_p$	$\mathcal{O}_{\mathfrak{p}}$	$\mathbb{F}_p[[t]]$	$\mathbb{F}_q[[t]]$
residue	$\mathbb{F}_p$	$\mathbb{F}_q$	$\mathbb{F}_p$	$\mathbb{F}_q$

The number fields $\mathbb{Q}$ and E also have completions "at infinity" which give local fields $\mathbb{R}$ (as the only infinite completion of $\mathbb{Q}$) and $\mathbb{R}, \mathbb{C}$ (as possible infinite completions of E).

4

4. Galois representations

4.1. **How they arise.** We wish to consider representations of the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and similar things. These arise naturally in the theory of étale cohomology, a truly marvellous theory that we will now briefly describe.

Suppose Y is an d-dimensional algebraic variety defined over a field E. Let ℓ be a prime number, $\ell \neq \mathrm{char}(E)$. Then for $0 \leq i \leq 2d$ the étale cohomology

$$H^i_{\text{ét}}(Y, \mathbb{Q}_\ell)$$

is defined. It is a $\mathbb{Q}_\ell$ vector space on which $\mathrm{Gal}(\overline{E}/E)$ acts. (Originally, attempts were made to find an good cohomology theory with "coefficients" in the rational numbers $\mathbb{Q}$. It was later discovered that this was impossible.)

4.2. The étale cohomology enables us to think about a variety Y defined over a finite field (such as may occur in the study of coding theory or cryptography) as if it were a complex variety. And in this case, the Galois module structure on the étale cohomology has some amazing properties. Suppose the algebraic variety Y is defined over $\mathbb{F}_q$ (of characteristic p) and that it is nonsingular and projective. Then a series of conjectures of A. Weil, eventually proven by P. Deligne states that

(1) The eigenvalues α_j of the Frobenius σ_q on $H^{2i}(Y, \mathbb{Q}_\ell)$ have absolute value $|\alpha_j| = q^i$.
(2) The eigenvalues β_k of σ_q on $H^{2i+1}(Y, \mathbb{Q}_\ell)$ have absolute value $|\beta_k| = q^i\sqrt{q}$.
(3) The number of points

$$(4.2.1) \qquad \#(Y(\mathbb{F}_{q^r})) = \sum_j \alpha_j^r - \sum_k \beta_k^r$$

(the sum being over all eigenvalues of σ_q on all étale cohomology groups).
(4) The eigenvalues $\alpha_j, \beta_k \in \mathbb{C}$ are uniquely determined by this equation.

In particular, $\mathrm{rank} H^{2i}_{\text{ét}}(Y, \mathbb{Q}_\ell)$ is the number of α occurring in (4.2.1) with $|\alpha| = q^i$ and $\mathrm{rank} H^{2i+1}_{\text{ét}}(Y, \mathbb{Q}_\ell)$ is the number of β occurring in (4.2.1) with $|\beta| = q^i\sqrt{q}$.

The elementary symmetric functions of the eigenvalues of σ_q on $H^i_{\text{ét}}(Y, \mathbb{Q}_\ell)$ are the coefficients of the characteristic polynomial of the action of σ_q on H^i. It is common to encode the eigenvalues in a ζ function,

$$\zeta_q(Y, t) = \frac{\prod_{i \text{ odd}} \det(1 - t\sigma_q) \text{ on } H^i_{\text{ét}}(Y, \mathbb{Q}_\ell)}{\prod_{i \text{ even}} \det(1 - t\sigma_q) \text{ on } H^i_{\text{ét}}(Y, \mathbb{Q}_\ell)}.$$

Another way to express part(3) of Deligne's theorem is:

$$\zeta_q(Y, t) = \exp\left(\sum_{n=1}^\infty \#(Y(\mathbb{F}_{q^n})) \frac{t^n}{n}\right).$$

5

The zeta function is independent of the choice of ℓ (for almost all ℓ). It satisfies the following functional equation, which may be interpreted as the statement of Poincaré duality for the étale cohomology,

$$\zeta\left(\frac{1}{q^d t}\right) = \pm q^{\frac{d}{2}\chi(Y)} t^{\chi(Y)} \zeta(t)$$

where $d = dim(Y)$ and $\chi(Y)$ is the Euler characteristic,

$$\chi(Y) = \sum_{i=0}^{d} (-1)^i \mathrm{rank} H_{\text{ét}}^i(Y, \mathbb{Q}_\ell).$$

4.3. **Varying the** p**.** Now suppose Y is an algebraic variety defined over $\mathbb{Z}$. The equations defining Y can be reduced modulo p, to give an algebraic variety $Y \ (\mathrm{mod}\,p)$ (sometimes denoted $Y/\mathbb{F}_p$) defined over $\mathbb{F}_p$. In this case, it turns out that for almost all primes p (and for $\ell \neq p$),

$$H^i(Y(\mathbb{C}), \mathbb{Q}) \otimes_{\mathbb{Q}_\ell} \mathbb{Q}_\ell \cong H_{\text{ét}}^i(Y/\mathbb{F}_p, \mathbb{Q}_\ell)$$

where the cohomology on the left hand side denotes the usual (singular, or simplicial) cohomology for $Y(\mathbb{C})$. For example, complex projective space is obtained as the quotient $\mathbb{P}^n(\mathbb{C}) = \mathbb{C}^{n+1} - \{0\}/\mathbb{C}^*$. So the analogous construction over $\mathbb{F}_q$ has

$$\#\mathbb{P}^n(\mathbb{F}_q) = \frac{q^{n+1} - 1}{q - 1} = 1 + q + q^2 + \ldots + q^n$$

which is the polynomial that describes the singular cohomology of projective space. (They're not all this easy, but it always seems like magic whenever you are able to count points.)

The Frobenius eigenvalues for different p can then be encoded in the L-function,

(4.3.1) $$L(Y, s) = \prod_p \zeta_p(Y, p^{-s}).$$

(In practice, finitely many primes are "bad". The factors corresponding to bad primes must be defined in a different way.)

4.4. **Frobenius eigenvalues of a Galois representation.** If Y is a nonsingular algebraic variety defined over the integers then $H_{\text{ét}}^i(Y, \mathbb{Q}_\ell)$ has an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. It is possible to recover the eigenvalues of σ_q on $H_{\text{ét}}^i(Y/\mathbb{F}_p, \mathbb{Q}_\ell)$ from this Galois module directly, and this leads to a definition of an L function for an abstract Galois representation.

First note that there is a diagram

$$\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \xrightarrow{\ r\ } \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$$
$$\downarrow \pi$$
$$\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$$

where π is surjective and r is injective. The mapping r exists because $\mathbb{Q} \subset \mathbb{Q}_p$ and $\overline{\mathbb{Q}} \subset \overline{\mathbb{Q}}_p$; any automorphism of $\overline{\mathbb{Q}}_p$ which fixes $\mathbb{Q}_p$ restricts to an automorphism of $\overline{\mathbb{Q}}$ which fixes $\mathbb{Q}$.

The mapping π is similarly induced from the projection $(\mathrm{mod}\, p) : \mathbb{Z}_p \to \mathbb{F}_p$. One would like to say that there is a canonical lift of the Frobenius $\sigma_p \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ whose image in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is denoted Fr_p and is called the *Frobenius element* at p. Unfortunately this is not quite true, due to the existence of "ramification".

Let H be a finite dimensional vector space over $\mathbb{Q}_\ell$. A representation[4] $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbf{GL}(H)$ is said to be *unramified at* p (where $\ell \neq p$) if its restriction to $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ factors through $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. So in this case we have a mapping

$$\rho_p : \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \to \mathbf{GL}(H)$$

and we define the Frobenius element $Fr_p = \rho_p(\sigma_p) \in \mathbf{GL}(H)$. The inverse of the characteristic polynomial of the action of Fr_p on H defines a function,

$$\zeta_p(\rho, t) = \frac{1}{\det(I - tFr_p)}.$$

Using the embedding $\mathbb{Q}_\ell \to \mathbb{C}$ we may consider this to be a rational function with complex coefficients. The coefficients of the characteristic polynomial are the eigenvalues of Fr_p, so this function "encodes" the Frobenius eigenvalues, which may be combined for different values of p by defining

$$(4.4.1) \qquad\qquad\qquad L(\rho, s) = \prod_p \zeta_p(p^{-s}).$$

(For ramified primes p a slight modification[5] is needed.) If ρ is the trivial 1-dimensional representation then

$$L(\rho, s) = \prod_p \frac{1}{1 - p^{-s}}$$

which is the Riemann zeta function.

If Y is a nonsingular algebraic variety defined over the integers $\mathbb{Z}$ and if p is a "good" prime (which excludes only finitely many primes) then the repesentation of $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ on $H^i_{\text{ét}}(Y/\mathbb{F}_p, \mathbb{Q}_\ell)$ (obtained by reducing Y modulo p) coincides with the representation on $H^i_{\text{ét}}(Y, \mathbb{Q}_\ell)$ determined by the Frobenius element so the L function (4.3.1) is

$$L(Y, s) = \frac{\prod_{i\ \text{odd}} L(H^i, s)}{\prod_{i\ \text{even}} L(H^i, s)}$$

where H^i is the representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the étale cohomology $H^i_{\text{ét}}(Y, \mathbb{Q}_\ell)$.

An excellent survey article on Galois representations is [T].

5. Modular forms for $\mathbf{SL}(2)$

5.1. The purpose of this section and the next is to show that each modular form f gives rise to a representation of $\mathbf{GL}(2, \mathbb{A})$ such that the action of the Hecke operators (on modular forms) translates into an action of the Hecke algebra. We will also describe three ways

to view a Hecke operator: as a geometrically defined correspondence, as an operator on modular forms given by a certain equation, and as an integral operator on functions.

The group that we wish to study, $\mathbf{GL}(2, \mathbb{R})$, has two connected components, and it has a nontrivial center $Z(\mathbb{R})$ consisting of the scalar matrices. These properties are responsible for several technicalities that we would just as soon avoid. So in this section we will instead consider the theory of modular forms for $\mathbf{SL}(2, \mathbb{R})$, which is similar but simpler.

5.2. **Classical theory.** The group $\mathbf{SL}(2, \mathbb{R})$ acts on the upper half plane $\mathfrak{h}$ by fractional linear transformations:
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az + b}{cz + d}.$$
The stabilizer of the "basepoint" i is the maximal compact subgroup $\mathbf{SO}(2)$ which can be identified with the circle group by $e^{i\theta} \mapsto \left(\begin{smallmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{smallmatrix} \right)$.

A *modular form* f of weight k is a holomorphic mapping $f : \mathfrak{h} \to \mathbb{C}$, meromorphic at infinity, such that for every $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \in \mathbf{SL}(2, \mathbb{Z})$,
$$f(g \cdot z) = (cz + d)^{-k} f(z).$$
The modular form f is *cuspidal* if $f(z) \to 0$ as $z \to \infty$. The space $\mathcal{S}_k$ of cuspidal modular forms of weight k is finite dimensional. Each modular form $f : \mathfrak{h} \to \mathbb{C}$ of weight k may be interpreted as a section of a certain line bundle E_k on the quotient
$$X = \mathbf{SL}(2, \mathbb{Z}) \backslash \mathfrak{h}.$$

This quotient, not coincidentally, may be interpreted as the moduli space of elliptic curves, and as such, it carries the natural structure of a complex algebraic variety defined over $\mathbb{Q}$.

In [Se] a few of the many marvelous number theoretic properties of individual modular forms are described in an elementary way.

5.3. **Modular forms give representations.** Each integer k corresponds to a representation $j : \mathbf{SO}(2) \to \mathbf{GL}(1, \mathbb{C}) = \mathbb{C}^*$, namely

(5.3.1)
$$j \begin{pmatrix} a & b \\ c & d \end{pmatrix} = (ci + d)^k.$$

There is a simple trick[6], perhaps first expressed in [GF], for converting a modular form f of weight k into a function $\widehat{f} : \mathbf{SL}(2, \mathbb{R}) \to \mathbb{C}$ such that
$$\widehat{f}(\gamma g h) = j(h)^{-1} \widehat{f}(g)$$
for all $\gamma \in \mathbf{SL}(2, \mathbb{Z})$, all $g \in \mathbf{SL}(2, \mathbb{R})$ and all $h \in \mathbf{SO}(2)$, namely
$$\widehat{f} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = (ci + d)^{-k} f \left(\frac{ai + b}{ci + d} \right).$$
In other words, view (5.3.1) as a function on $\mathbf{SL}(2, \mathbb{R})$ and set $\widehat{f}(g) = j(g)f(g \cdot i)$.

Then we may also view $\widehat{f}$ as a function

$$\widehat{f} : \mathbf{SL}(2,\mathbb{Z})\backslash\mathbf{SL}(2,\mathbb{R}) \to \mathbb{C}.$$

The group $\mathbf{SL}(2,\mathbb{R})$ acts on the space of such functions by the "regular" representation, that is, the action of $g \in \mathbf{SL}(2,\mathbb{R})$ on such a function ϕ is the function

$$R_g(\phi)(x) = \phi(g^{-1}x).$$

The collection of all translates $R_g(\widehat{f})$ of $\widehat{f}$ by elements $g \in \mathbf{SL}(2,\mathbb{R})$ span a sub-representation of $\mathbf{SL}(2,\mathbb{R})$. If f is a cuspidal Hecke eigenform (see below) of weight k then $\widehat{f}$ is an L^2 function, and the resulting representation turns out to be irreducible and isomorphic to the discrete series representation (with trivial central character) of weight k.

5.4. **Hecke operators.** Write $\Gamma = \mathbf{SL}(2,\mathbb{Z})$. Each $g \in \mathbf{GL}(2,\mathbb{Q})$ defines a *Hecke correspondence* whose action on functions (or on modular forms) is called a *Hecke operator*, as follows. Let $\Gamma' = \Gamma \cap g\Gamma g^{-1}$. It has finite index in both Γ and Γ' so the following mappings are finite coverings:

$$
\begin{array}{ccc}
\Gamma'\backslash\mathfrak{h} & \longrightarrow & (g\Gamma g^{-1})\backslash\mathfrak{h} \\
s\downarrow & \swarrow & \\
\Gamma\backslash\mathfrak{h} & &
\end{array}
$$

where the diagonal isomorphism is given by multiplication by g^{-1}. Setting $X' = \Gamma'\backslash\mathfrak{h}$ we obtain two mappings $(s,t) : X' \rightrightarrows X$ or, equivalently, a mapping $X' \to X \times X$, which turns out to be an embedding whose image may be thought of as the graph of a multi-valued mapping (or *correspondence*) $X \to X$. It turns out that this correspondence $X' \rightrightarrows X$ depends only on the double coset $\Gamma g\Gamma$. This correspondence acts on a function $f : \Gamma\backslash\mathfrak{h} \to \mathbb{C}$ to give the function[7]

(5.4.1) $$T_g(f) = s_* t^* f.$$

5.5. **Hecke algebra.** If $(s_1,t_1) : Y_1 \rightrightarrows X$ and $(s_2,t_2) : Y_2 \rightrightarrows X$ are two correspondences, their composition is the correspondence Y_3 defined to be the fiber product,

$$
\begin{array}{ccc}
Y_3 & \longrightarrow & Y_2 \xrightarrow{\ t_2\ } X \\
\downarrow & & \downarrow {\scriptstyle s_2} \\
Y_1 & \xrightarrow{\ t_1\ } & X \\
{\scriptstyle s_1}\downarrow & & \\
X & &
\end{array}
$$

that is, $Y_3 = \{(y_1, y_2) \in Y_1 \times Y_2 | \ t_1(y_1) = s_2(y_2)\}$. If $Y_1 = \Gamma_1 \backslash \mathfrak{h}$ and $Y_2 = \Gamma_2 \backslash \mathfrak{h}$ are Hecke correspondences associated to elements $g_1, g_2 \in \mathbf{GL}(2, \mathbb{Q})$ then $Y_3 = \Gamma_3 \backslash \mathfrak{h}$ with $\Gamma_3 = \Gamma_2 \cap g_1 \Gamma_2 g_1^{-1}$. The action of the composition Y_3 on functions is given by the composition $T_{g_2} \circ T_{g_1}$. However this does not necessarily coincide with the action of $T_{g_2 g_1}$. Rather, the product of double cosets $(\Gamma g_1 \Gamma)(\Gamma g_2 \Gamma)$ decomposes into a union of finitely many double cosets $\Gamma h_i \Gamma$ with multiplicities m_i ($1 \le i \le k$ for some k), and

$$(5.5.1) \qquad\qquad T_{g_1} \circ T_{g_2} = \sum_{i=1}^{k} m_i T_{h_i}.$$

Thus we are led to define the *Hecke algebra* to be the set of all finite formal linear combinations (with rational coefficients) of double cosets

$$\Gamma g \Gamma \in \mathbf{SL}(2, \mathbb{Z}) \backslash \mathbf{GL}(2, \mathbb{Q}) / \mathbf{SL}(2, \mathbb{Z}),$$

with the composition law (5.5.1) and an action on functions given either by (5.4.1) or by (8.7.1). Variations on this construction are obtained by replacing $\mathbf{GL}(2, \mathbb{Q})$ with its identity component $\mathbf{GL}(2, \mathbb{Q})^{+}$, (the elements of positive determinant) or with integer matrices with positive determinant $M_2(\mathbb{Z})^{+}$; or by replacing $\mathbf{SL}(2, \mathbb{Z})$ with $\mathbf{GL}(2, \mathbb{Z})$.

The structure of such a Hecke algebra is completely understood. It has no zero divisors, it is abelian, and it decomposes into a sum of algebras $\mathcal{H}_p$ for each prime number p. Each $\mathcal{H}_p$ is isomorphic to the ring of polynomials on certain generators [8].

Returning to $\mathbf{GL}(2)$, let $T(n)$ be the Hecke operator corresponding to the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & n \end{smallmatrix} \right)$. A modular form f is a *Hecke eigenform* if it is a simultaneous eigenvector for all elements of the Hecke algebra. Each modular form f is automatically an eigenfunction for the Hecke correspondences corresponding to scalar matrices, so f is a Hecke eigenform iff there exist $\lambda_p \in \mathbb{C}$ so that $T(p)f = \lambda_p f$ for all primes p, from which it also follows that f is an eigenform for all $T(n)$.

5.6. **Fourier coefficients.** If $f : \mathfrak{h} \to \mathbb{C}$ is a modular form, then it is periodic near infinity, so it admits a Fourier expansion

$$f(z) = \sum_{i=0}^{\infty} a_i e^{2\pi i z}.$$

The form f is cuspidal if $a_0 = 0$ or equivalently, if $f(z) \to 0$ as $z \to \infty$. Suppose, moreover, that f is a simultaneous eigenfunction for all Hecke operators: $T_n(f) = \lambda_n f$, and that f is normalized so that $a_1 = 1$. Then $a_n = \lambda_n$, that is, the Fourier coefficients of f coincide with its Hecke eigenvalues.

5.7. **Summary.** In summary, the vector space $\mathcal{S}_k$ of cuspidal modular forms of weight k decomposes under the Hecke algebra into 1-dimensional subspaces consisting of Hecke eigenforms. The Hecke eigenvalues of such a cusp form coincide with its Fourier coefficients. Such a cusp form gives rise to a discrete series representation of $\mathbf{SL}(2, \mathbb{R})$.

6. ADELIC POINT OF VIEW

6.1. The concept of a modular form may be generalized by a two step procedure: (a) to that of an *automorphic form* and (b) to that of an *automorphic representation*. An automorphic representation (of $\mathbf{GL}(n)$) is an irreducible representation of $\mathbf{GL}(n, \mathbb{A})$ occurring in a space of complex valued functions (on $\mathbf{GL}(n, \mathbb{A})$) having certain growth, smoothness, and equivariance properties. Langlands, and Jacquet-Langlands [JL] discovered how to assign Hecke eigenvalues to such a representation so that the following diagram commutes:

$$\text{modular form} \quad \longrightarrow \quad \text{automorphic form}$$
$$\downarrow \qquad\qquad\qquad\qquad \downarrow$$
$$\text{Hecke eigenvalues} \longleftarrow \text{automorphic representation}$$

These constructions involve the adèles,

$$\mathbb{A} = \mathbb{A}_{\mathbb{Q}} = \mathbb{R} \times \underset{p}{\Pi'}\mathbb{Q}_p.$$

This is the *restricted* product of the real numbers with the p-adic numbers for all primes p, meaning that a sequence $(a_\infty, a_2, a_3, a_5, \cdots)$ of elemenets $a_p \in \mathbb{Q}_p$ is in $\mathbf{A}$ if there exists $N > 0$ so that $a_p \in \mathbb{Z}_p$ for all $p \geq N$. The object $\mathbb{A}$ forms a locally compact ring under coordinate-wise multiplication, and it contains the rational numbers $\mathbb{Q}$, embedded diagonally, as a discrete subring. (That is, each $q \in \mathbb{Q}$ corresponds to the sequence $(q, q, q, \cdots)$.) We refer to the real numbers $\mathbb{R}$ as the *infinite* component and the remainder $\mathbb{A}_f = \Pi'_p \mathbb{Q}_p$ as the *finite* adeles.

The group $\mathbf{GL}(2, \mathbb{A})$ is locally compact and it breaks into a restricted product

$$\mathbf{GL}(2, \mathbb{A}) = \mathbf{GL}(2, \mathbb{R}) \times \underset{p}{\Pi'}\mathbf{GL}(2, \mathbb{Q}_p)$$

meaning that a sequence $g_\infty, g_2, g_3, g_5, \cdots$ is in $\mathbf{GL}(2, \mathbb{A})$ if, for all p sufficiently large, $g_p \in \mathbf{GL}(2, \mathbb{Z}_p)$. The diagonally embedded subgroup $\mathbf{GL}(2, \mathbb{Q})$ is discrete in $\mathbf{GL}(2, \mathbb{A})$ and we may form the quotient $\mathbf{GL}(2, \mathbb{Q})\backslash\mathbf{GL}(2, \mathbb{A})$. A modular form may be considered as a function on this quotient. In fact, there is a natural (although not entirely obvious) identification

$$\mathbf{GL}(2, \mathbb{Z})\backslash\mathbf{GL}(2, \mathbb{R}) \cong \mathbf{GL}(2, \mathbb{Q})\backslash\mathbf{GL}(2, \mathbb{A})/K_f$$

where

$$K_f = \underset{p}{\Pi}\, \mathbf{GL}(2, \mathbb{Z}_p)$$

is a compact open subgroup of the finite adelic group $\mathbf{GL}(2, \mathbb{A}_f)$. This identification induces an isomorphism

(6.1.1) $$X = \mathbf{SL}(2, \mathbb{Z})\backslash\mathfrak{h} \cong \mathbf{GL}(2, \mathbb{Q})Z(\mathbb{A})\backslash\mathbf{GL}(2, \mathbb{A})/\mathbf{O}(2) \times K_f.$$

Moreover the manifold X admits the structure of a complex algebraic variety defined over the rational numbers $\mathbb{Q}$. With this algebraic strucutre, X is referred to as a *Shimura variety*[9].

11

6.2. **Automorphic forms in the adelic setting.** As in §5.3, each (holomorphic) cuspidal modular form f lifts to a function

(6.2.1) $$\widehat{f} : \mathbf{GL}(2, \mathbb{Q})Z(\mathbb{A})\backslash\mathbf{GL}(2, \mathbb{A}) \to \mathbb{C}.$$

The functions obtained this way satisfy certain growth[10], smoothness[11], and equivariance[12] properties. The cuspidality condition for f can be rephrased in terms of certain integrals[13] of $\widehat{f}$. In general, a *cuspidal automorphic form* ϕ on $\mathbf{GL}(n, \mathbb{A})$ is a function

(6.2.2) $$\phi : \mathbf{GL}(n, \mathbb{Q})Z(\mathbb{A})\backslash\mathbf{GL}(n, \mathbb{A}) \to \mathbb{C}$$

which satisies the analogous growth[14], smoothness[15], equivariance[16], and cuspidal conditions[17]. Denote the vector space of cuspidal automorphic forms by $\mathcal{A}_0 = \mathcal{A}_0(\mathbf{GL}(n, \mathbb{A}))$.

6.3. **Automorphic representations.** Elementary references for this section include [K], [G1] and [G2]. A more complete reference is [Bu] §3.2. Given an automorphic form ϕ (6.2.2), the collection of all translates $R_g(\phi)$ (as g varies in $\mathbf{GL}(n, \mathbb{A})$) spans a vector subspace of

(6.3.1) $$L^2(\mathbf{GL}(n, \mathbb{Q})Z(\mathbb{A})\backslash\mathbf{GL}(n, \mathbb{A}))$$

whose closure we denote by V_ϕ. The group $\mathbf{GL}(n, \mathbb{A})$ acts on V_ϕ. If the automorphic form ϕ arose from a cuspidal modular Hecke eigenform (for $n = 2$) then the representation V_ϕ is irreducible. So one would like to define an automorphic representation to be any irreducible representation that occurs in (6.3.1). There are two problems with this plan. The first is that any reasonable decomposition of (6.3.1) will have a continuous spectrum. This creates enormous difficulties that must eventually be addressed, however for the present purpose we will avoid these difficulties by restricting to the Hilbert space

(6.3.2) $$L_0^2(\mathbf{GL}(n, \mathbb{A})Z(\mathbb{A})\backslash\mathbf{GL}(n, \mathbb{A}))$$

consisting of L^2 measurable functions that satisfy the cuspidal condition. This space decomposes into a discrete sum[18] of irreducible unitary representations of $\mathbf{GL}(n, \mathbb{A})$.

Each irreducible constituent π of (6.3.2) decomposes as a product $\pi = \pi_\infty \otimes \otimes_p \pi_p$ of irreducible unitary representations of $\mathbf{GL}(n, \mathbb{R})$ and $\mathbf{GL}(n, \mathbb{Q}_p)$ respectively, and each π_p has eigenvalues associated to the Hecke algebra $\mathcal{H}_p$ (see below) associated to the group $\mathbf{GL}(n, \mathbb{Q}_p)$. Here is how these eigenvalues are constructed. The space

(6.3.3) $$\mathcal{A}_0 = \mathcal{A}_0(\mathbf{GL}(n, \mathbb{A}))$$

of cuspidal automorphic forms is a subspace of (6.3.2) which also admits a decomposition into a (Hilbert space direct) sum of irreducibles, each of which we refer to as a *cuspidal automorphic representation*[19]. Moreover, there is a natural one to one correspondence between the irreducibles appearing in (6.3.2) and the irreducibles appearing in (6.3.3): if

$$\pi : \mathbf{GL}(n, \mathbb{A}) \to \mathbf{GL}(V)$$

is an irreducible unitary representation occurring in (6.3.2) then the subspace $V^{(K)}$ of K-finite vectors[20] constitutes an irreducible cuspidal automorphic representation π' appearing

12

in (6.3.3). Moreover, this automorphic representation π' decomposes as a restricted[21] tensor product,

$$\pi' = \pi'_\infty \otimes \otimes_p \pi'_p$$

where π'_p is an irreducible (admissible[22]) representation of $\mathbf{GL}(n, \mathbb{Q}_p)$ and π'_∞ is an irreducible $(\mathfrak{g}_\infty, K_\infty)$ module (see note 20). The plan, now, is to assign Hecke eigenvalues to each component π'_p.

Not every such tensor product of irreducibles appears in (6.3.2). The manner in which the various factors appear in the irreducible constituents of (6.3.2) is believed to reflect deep number-theoretic facts.

6.4. **Hecke eigenvalues of an automorphic representation.** Throughout this section let us fix a prime number $p < \infty$ and set $G_p = \mathbf{GL}(n, \mathbb{Q}_p)$ and $K_p = \mathbf{GL}(n, \mathbb{Z}_p)$. The Hecke algebra $\mathcal{H}_p$ is the vector space of all finite formal linear combinations of double cosets

(6.4.1) $$K_p g K_p \in K_p \backslash G_p / K_p$$

or equivalently, it is the vector space of smooth (= locally constant) compactly supported K_p- bi-invariant functions on G_p. It has a basis consisting of characteristic functions of double cosets (6.4.1). Multiplication in $\mathcal{H}_p$ may be expressed as convolution[23]:

$$(f * h)(z) = \int_{G_p} f(x) h(x^{-1} z) dx.$$

The Hecke algebra $\mathcal{H}_p$ acts on K_p-finite locally constant functions ϕ by

$$(h\phi)(z) = \int_{G_p} h(g) \phi(zg) dg.$$

Fix an irreducible (admissible) representation $\pi_p : G_p \to \mathbf{GL}(V)$ that occurs as the p-component of a cuspidal automorphic representation π. We say that π_p is *unramified* or *spherical* (or that π is *unramified at p*) if the subgroup K_p acts on V with a nontrivial fixed subspace V^{K_p}. In this case the subspace of vectors fixed under K_p is 1-dimensional, which may be interpreted as an eigenspace for the Hecke operators at p. In fact[24] the Hecke algebra $\mathcal{H}_p$ acts on this 1-dimensional space through some $\lambda : \mathcal{H}_p \to \mathbb{C}$, which turns out to be a homomorphism of algebras, and which we refer to as the Hecke eigenvalue corresponding to the representation π_p.

Satake showed[25] that the collection of such homomorphisms can be naturally identified with equivalence classes of diagonal $n \times n$ matrices of nonzero complex numbers; two being considered equivalent if they differ by a permutation of the entries (that is, with $T(\mathbb{C})$ where T is the torus of diagonal matrices in $\mathbf{GL}(n)$). Moreover this *Satake parameter* determines the representation π_p. If $\text{diag}(t_1, t_2, \cdots, t_n)$ is a diagonal matrix of n nonzero complex

numbers, let $\mu : T(\mathbb{Q}_p) \to \mathbb{C}^\times$ be the homomorphism

$$\mu \begin{pmatrix} x_1 & & & \\ & x_2 & & \\ & & \cdots & \\ & & & x_n \end{pmatrix} = \prod_{i=1}^{n} t_i^{\mathrm{val}(x_i)}$$

Then $\pi_p = \mathrm{ind}_T^{G_p}(\mu)$ is obtained by inducing this character up to G_p. See the survey article [K] for details.

The Satake parameter $t = \mathrm{diag}(t_1, t_2, \cdots, t_n) \in T(\mathbb{C})$ may also be identified with a semisimple conjugacy class in $\mathbf{GL}(n, \mathbb{C})$. Any element in this class has the same eigenvalues $t_1, t_2, \cdots, t_n$, possibly permuted, (with respect to the standard representation of $\mathbf{GL}(n, \mathbb{C})$), which we consider to be the desired "Hecke eigenvalues" attached[26] to π_p. We may form a zeta function in the usual way,

$$\zeta_p(y) = \frac{1}{\det(I - yt)}.$$

If π is an automorphic representation of $\mathbf{GL}(n, \mathbb{A})$ then define

$$L(\pi, s) = \prod_p \zeta_p(p^{-s})$$

where the product is taken over all primes p such that π_p is unramified[27].

6.5. **Summary.** Finally, Langlands' conjecture states that there should be a way to associate, to any representation ρ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ an automorphic representation π of $\mathbf{GL}(n, \mathbb{A})$ such that (up to constant factors and a shift in s) the resulting L functions coincide:

$$L(\rho, s) = L(\pi, s).$$

In other words, the eigenvalues of Fr_p on the representation ρ should coincide with the eigenvalues of the Hecke algebra $\mathcal{H}_p$ on the p-component π_p of the representation π.

7. COMPARING BOTH SIDES

7.1. **The case** $n = 2$. The Eichler-Shimura theorem may be reinterpreted as a proof of the conjecture for $n = 2$. There are several ways to associate Galois representations and modular forms. Shimura's original description [Sh1] associates to any modular form f a certain elliptic curve E_f. Then he shows that the Galois group acts on the torsion points of E_f, giving rise to the desired Galois representation which can be interpereted as the Galois representation on the étale cohomology $H^1_{\text{ét}}(E_f, \mathbb{Q}_\ell)$. However the modern approach consists of identifying this Galois representation in the cohomology $H^1_{\text{ét}}(X, \mathbb{Q}_\ell)$ of the Shimura variety

$$X = \mathbf{GL}(2, \mathbb{Q})Z(\mathbb{A})\backslash\mathbf{GL}(2, \mathbb{A})/\mathbf{O}(2)K_f$$

described in (6.1.1). In fact, Eichler and Shimura showed that there is a local coefficient system $\mathcal{E}_k$ on X such that

(7.1.1)
$$H^1_P(X, \mathcal{E}_k; \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{C} \cong \mathcal{S}_k \oplus \overline{\mathcal{S}}_k$$

where S_k denotes the (finite dimensional) vector space of cusp forms of weight k. Here, $H^1_P(X, \mathcal{E}_k)$ denotes the image of the mapping $H^1_c(X, \mathcal{E}_k) \to H^1(X, \mathcal{E}_k)$, where H^1_c denotes cohomology with compact supports[28]. Under the isomorphism (7.1.1) the action of Hecke correspondences on the left side coincides with the action of the Hecke operators on the right side. If a cusp form f is a Hecke eigenform then its complex conjugate $\overline{f}$ is also an eigenfunction of all Hecke operators, and it has the same Hecke eigenvalues. So the action of the Hecke algebra decomposes the cohomology group on the left side into two dimensional subspaces. It follows that the étale cohomology $H^1_{\text{ét},P}(\overline{X}, \mathcal{E}_k; \mathbb{Q}_\ell)$ is decomposed into two dimensional subspaces (under the action of the Hecke correspondences), each of which corresponds to a unique cuspidal Hecke eigenform f, and hence to an automorphic representation. This, finally, gives a correspondence between (certain) two dimensional representations of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and (certain) cuspidal automorphic representations of $\mathbf{GL}(2, \mathbb{A})$. It turns out (and this is the difficult part) that under this correspondence, the Galois eigenvalues do indeed correspond to the Hecke eigenvalues. In order to prove this, one needs some relation between the Galois action and the Hecke action on the étale cohomology, and this is provided by the *Eichler-Shimura relation* which says, approximately, that the correspondence T_p is isomorphic (as a correspondence) to the sum of σ_p and its transpose.

7.2. **The case $n \geq 3$.** The above argument is so compelling that one might ask why it doesn't just work in general. The problem is that the procedure breaks down entirely for $n \geq 3$ because the required Shimura varieties do not exist. For example, when $n = 3$ the analogous object

$$\mathbf{GL}(3, \mathbb{Q})Z(\mathbb{A})\backslash\mathbf{GL}(3, \mathbb{A})/\mathbf{O}(3)K_f$$

is not an algebraic variety at all, and in fact it is a manifold of (real) dimension 5. This issue is one of the great puzzles of the subject.

7.3. **What about $\mathbf{GL}(1)$?**

8. Other groups and fields

8.1. Roughly speaking, for any algebraic group $\mathbf{G}$ defined over $\mathbb{Q}$, Langlands conjectures that there should exist a correspondence

(8.1.1)
$$\left\{ \begin{array}{l} \text{nice homomorphism} \\ \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to {}^L\mathbf{G}(\mathbb{C}) \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \text{nice automorphic representations} \\ \text{of } \mathbf{G}(\mathbb{A}_{\mathbb{Q}}) \end{array} \right\}$$

such that

(8.1.2)
$$\{\text{eigenvalues of Frobenius}\} \longrightarrow \{\text{eigenvalues of Hecke operators}\}$$

8.2. The dual group.

8.3. The Hermitian case.

8.4. Local fields.

8.5. Geometric Langlands.

8.6. Langlands' functoriality conjecture.

8.7. A sampling of major results.

<div align="center">NOTES</div>

[1]In other words, it is the set of equivalence classes of Cauchy sequences; two such sequences $\{x_n\}$, $\{y_n\}$ being considered equivalent if $|x_n - y_n|_p \to 0$.

[2]The norm $|\ |_p$ is defined as follows. Suppose a/b is a fraction in lowest terms. If neither a nor b is divisible by p then $|a/b|_p = 1$. If a is divisible by p, say $a = p^m a'$ then $|a/b|_p = p^{-m}$. If b is divisible by p, say $b = p^n b'$ then $|a/b|_p = p^n$. If $c = a/b$ is expanded as a power series in p, then $|a/b|_p = p^{-\text{valc}}$.

[3]There are many such embeddings, and they are never continuous with respect to the usual topology on $\mathbb{C}$.

[4]A Galois representation ρ is always assumed to be continuous with respect to the natural topology on $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ that arises from its structure as a pro-finite group; see [T] §1.

[5]More generally, for any prime $p \neq \ell$, let $I_p = \ker(\pi_p)$ be the "inertia group" and let H^{I_p} be the subspace of H that is fixed under I_P. If H is unramified at p then $H^{I_p} = H$. But in general, the quotient $\text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)/I_p \cong \text{Gal}(\overline{\mathbb{F}}_p/\mathbb{F})$ acts on H^{I_p}. So we obtain a " Frobenius element" $Fr_p \in \mathbf{GL}(H^{I_p})$. Then the zeta function "at p" is defined to be $\frac{1}{\det(I - tFr_p)}$, where $I - Fr_p$ acts on the subspace H^{I_p}. Then equation (4.4.1) makes sense as a product of local factors over all primes $p \neq \ell$. If $p = \ell$ then the corresponding local factor involves more technical considerations.

[6]In general if G is a Lie group and K is a closed subgroup then any representation $\rho : K \to \mathbf{GL}(V)$ of K (on a complex vector space V) determines a homogeneous vector bundle $E = G \times_K V$ on $D = G/K$, consisting of equivalence classes $[g, v]$ where $[gk, v] \sim [g, \lambda(k)v]$ for all $k \in K$, which admits an action of G by $g \cdot [h, v] = [gh, v]$. Each (smooth) section of E is given by a (smooth) function $\widehat{f} : G \to \mathbb{C}$ such that $\widehat{f}(gk) = \lambda(k^{-1})\widehat{f}(g)$. A (smooth) *automorphy factor* for E is a smooth mapping $J : G \times D \to \mathbf{GL}(V)$ such that

(1) $J(gg', x) = J(g, g'x)J(g', x)$ for all $g, g' \in G$ and all $x \in D$,
(2) $J(k, x_0) = \rho(k)$ for all $k \in K$

where $x_0 \in D$ is the basepoint determined by K. The automorphy factor J is determined by its values $J(g, x_0)$ at the basepoint: any smooth mapping $j : G \to \mathbf{GL}(V)$ such that $j(gk) = j(g)\rho(k)$ (for all $k \in K$ and $g \in G$) extends in a unique way to an automorphy factor J by setting $J(g, hx_0) = j(gh)j(h)^{-1}$.

An automorphy factor for E, if one exists, determines a smooth trivialization $\Phi_J : G \times_K V \to D \times V$ of E, by $[g, v] \mapsto (gK, J(g, x_0)v)$ which is G-equivariant with respect to the *J-automorphic action* of G on $D \times V$ given by $g \cdot (x, v) = (gx, J(g, x)v)$. (Conversely, any smooth trivialization $\Psi : E \to D \times V$ of E determines a unique automorphy factor J such that $\Psi = \Phi_J$.) An automorphy factor allows one to identify smooth mappings $f : D \to V$ with smooth sections $\widehat{f} : G \to V$ of E by setting $\widehat{f}(g) = J(g, x_0)^{-1}f(gK)$. Sections $\widehat{f}$ that are invariant under some $\gamma \in G$ (meaning that $\widehat{f}(\gamma g) = \widehat{f}(g)$ for all $g \in G$) then correspond to

<div align="center">16</div>

mappings $f : D \to V$ such that $f(\gamma x) = J(\gamma, x) f(x)$ for all $x \in D$. In the case of $\mathbf{SL}(2)$, the one dimensional representation of $K = \mathbf{SO}(2)$,

$$\rho \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix} \right) = (a + ib)^k$$

admits an automorphy factor $J \left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right), z \right) = (cz + d)^k$ where $z \in \mathfrak{h} = G/K$. See [GP] for more details.

[7]The Hecke operator may also be described as the action of the double coset $\Gamma g \Gamma$ on f as follows. Choose coset representatives $\gamma_1, \cdots, \gamma_t$ for $\Gamma' \backslash \Gamma$ so that $\Gamma = \coprod_{i=1}^{t} \Gamma' \gamma_i$. Then

$$(8.7.1) \qquad\qquad T_g(f)(\Gamma x) = \sum_{i=1}^{t} f(\Gamma g^{-1} \gamma_i x)$$

for any $x \in \mathfrak{h}$.

[8]The Hecke algebra for $\mathbf{SL}(n)$ differs slightly from that of $\mathbf{GL}(n)$. Here are a few examples.

Let $M_n(\mathbb{Z})^+$ be the ring of all $n \times n$ matrices with integer entries and positive determinant. Then ([Sh1], Thm. 3.20) the Hecke algebra for $\mathbf{SL}_n(\mathbb{Z}) \backslash M_n(\mathbb{Z})^+ / \mathbf{SL}_n(\mathbb{Z})$ is the sum of $\mathcal{H}_p$ (for p prime), each of which is isomorphic to a polynomial algebra on n generators

$$(8.7.2) \qquad\qquad \mathrm{diag}(1, p, \cdots, p), \mathrm{diag}(1, 1, p, \cdots, p), \cdots, \mathrm{diag}(p, p, \cdots, p).$$

The Hecke algebra for $\mathbf{GL}(n, \mathbb{Z}) \backslash \mathbf{GL}(n, \mathbb{Q}) / \mathbf{GL}(n, \mathbb{Z})$ is a sum of $\mathcal{H}_p$, each of which ([A] Thm. 3.2.17) is isomorphic to a polynomial algebra on $n + 1$ generators: those in (8.7.2) and $\mathrm{diag}(p, p, \cdots, p)^{-1}$.

[9] Other quotients $\Gamma_1 \backslash \mathfrak{h}$ (where Γ_1 is an arithmetic subgroup of $\mathbf{GL}(2, \mathbb{Q})$) may similarly be expressed as quotients $\mathbf{GL}(2, \mathbb{Q}) Z(\mathbb{R}) \backslash \mathbf{GL}(2, \mathbb{A}) / \mathbf{O}(2) K_{1f}$ for appropriate choice of compact open subgroup K_{1f} of the finite adèlic group $\mathbf{GL}(2, \mathbb{A}_f)$.

[10]The function ϕ should be *slowly increasing*, or have *moderate growth*, meaning that for any $c > 0$ and any compact subset $T \subset \mathbf{GL}(n, \mathbb{A})$ there exist constants C, N such that

$$\phi \left(\left(\begin{smallmatrix} 1 & 0 \\ 0 & a \end{smallmatrix} \right) g \right) \leq C |a|^N$$

whenever $a \in \mathbb{A}^\times$ and $|a| > c$, cf. note 14.

[11]The function $\widehat{f}$, viewed as a function on $\mathbf{GL}(2, \mathbb{R})$, turns out to be an eigenfunction of the Laplace operator, with eigenvalue $-\frac{k}{2} \left(\frac{k}{2} - 1 \right)$.

[12]The fact that $\widehat{f}$ is defined on the quotient space (6.2.1) means that $\widehat{f}$ may be considered to be a function on $\mathbf{GL}(2, \mathbb{A})$ such that $f(z\gamma g) = f(g)$ for all $z \in Z(\mathbb{A})$ and all $\gamma \in \mathbf{GL}(2, \mathbb{Q})$. Equivariance with respect to $K_\infty = \mathbf{O}(2)$ is expressed by $\widehat{f}(gu) = e^{-ik\theta} f(g)$ where $u = \left(\begin{smallmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{smallmatrix} \right)$.

[13]$\int_{\mathbb{Q} \backslash \mathbb{A}} \widehat{f} \left(\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix} \right) g \right) dx = 0$ for all $g \in \mathbf{GL}(2, \mathbb{A})$.

[14]The function ϕ should be slowly increasing, meaning that there exist constants C, N such that $|\phi(g)| \leq C \|g\|^N$ where $\| \ \|$ is a "height function", [Bu] p. 300. (It may be taken to be the length of the vector $(g, \det(g)^{-1}) \in \mathbb{A}^{2n} \oplus \mathbb{A}$, using the embedding of $\mathbf{GL}(n, \mathbb{A})$ in the space $M_n(\mathbb{A})$ of all $n \times n$ matrices.) If ϕ is slowly increasing then it is square integrable.

[15]The function ϕ should be $\mathfrak{z}(\mathfrak{g})$-finite, meaning that there is an ideal of finite codimension in the center $\mathfrak{z}$ of the universal enveloping algebra of $\mathfrak{g} = \mathfrak{gl}(n, \mathbb{R})$ that kills the function ϕ (viewed as a function on $\mathbf{GL}(n, \mathbb{R})$).

[16]The function ϕ should be K-finite, meaning that its translates by K span a finite dimensional vector space of functions. Here, $K = \mathbf{O}(n) \times K_f$ where $K_f = \prod_p \mathbf{GL}(n, \mathbb{Z}_p)$ as above.

[17]More generally, for any character $\psi : \mathbb{A}^\times \to \mathbb{C}^\times$ a cuspidal automorphic form of type ψ is a function

$$\phi : \mathbf{GL}(n, \mathbb{Q}) \backslash \mathbf{GL}(n, \mathbb{A}) \to \mathbb{C}$$

which satisfies $\phi(zg) = \psi(z)\phi(g)$ for all $z \in Z(\mathbb{A}) \cong \mathbb{A}^\times$, along with the growth, smoothness, equivariance, and cuspidal conditions.

[18] A special feature of the group $\mathbf{GL}(n)$ is that each irreducible representation occurs at most once in this decomposition.

[19] Actually the group $\mathbf{GL}(n, \mathbb{A})$ does not act on $\mathcal{A}_0$ because the K-finiteness condition is not preserved under the translation operator R_g. However $\mathcal{A}_0$ is both a $(\mathfrak{g}_\infty, K_\infty)$ module (where $\mathfrak{g}_\infty = \mathrm{Lie}(\mathbf{GL}(n, \mathbb{R})$ and $K_\infty = \mathbf{O}(n)$) and a $\mathbf{GL}(n, \mathbb{A}_f)$ module. As such, it decomposes into irreducibles and in particular, each automorphic representation is not really a representation of $\mathbf{GL}(n, \mathbb{A})$ but rather it is a

$$(\mathfrak{g}_\infty, K_\infty) \times \mathbf{GL}(n, \mathbb{A}_f)$$

module.

[20] It turns out that $V^{(K)}$ consists of eigenvectors (or eigenfunctions) of $Z(\mathfrak{g}_\infty)$, relative to some homomorphism $Z(\mathfrak{g}_\infty) \to \mathbb{C}$, and that each such vector also satisfies the "slow growth" hypothesis of note 14; in fact it is even rapidly decreasing. See [Kn] Thm. 7.3.

[21] meaning that for p sufficiently large, the component π'_p is the trivial one dimensional representation

[22] A representation of $\mathbf{GL}(n, \mathbb{Q}_p)$ is admissible if it decomposes under $K_p = \mathbf{GL}(n, \mathbb{Z}_p)$ into a direct sum of finite dimensional representations, each of which occurs at most finitely many times.

[23] with respect to a naturally defined Haar measure on G_p

[24] If $h \in \mathcal{H}_p$ is a smooth compactly supported complex valued K_p-bi-invariant function, and if $v \in V^{K_p}$ then

$$\pi_p(h)(v) = \int_{G_p} h(g)\pi_p(g)v\,dg.$$

If h is the characteristic function of a single double coset $K_p a K_p$ then this gives

$$\pi_p(h)(v) = \int_{K_p} \pi(k)\pi(a)v\,dk$$

which is easily seen to be fixed under K_p again. Consequently,

$$\pi_p(h)(v) = \lambda(h)v$$

for some number $\lambda(h) \in \mathbb{C}$. It is easily seen that in fact, λ is a homomorphism $\lambda : \mathcal{H}_p \to \mathbb{C}$ of algebras.

[25] In general, if $\mathbf{G}$ is a reductive linear algebraic group defined over $\mathbb{Q}_p$ the spherical Hecke algebra $\mathcal{H}_{\mathbf{G}}$ is the collection of formal finite linear combinations of double cosets

$$h \in \mathbf{G}(\mathbb{Z}_p)\backslash \mathbf{G}(\mathbb{Q}_p)/\mathbf{G}(\mathbb{Z}_p)$$

or, equivalently, the collection of all localy constant compactly supported complex valued functions $\phi : \mathbf{G}(\mathbb{Q}_p) \to \mathbb{C}$ that are $\mathbf{G}(\mathbb{Z}_p)$-bi-invariant, together with its convolution product. It is commutative. In the case that $\mathbf{G} = \mathbf{T}$ is a split torus with cocharacter group $X_*(\mathbf{T}) = \mathrm{Hom}(\mathbf{G_m}, \mathbf{T})$, the homomorphism $\mathrm{val} : \mathbb{Q}_p \to \mathbb{Z}$ extends to an isomorphism

$$\mathbf{T}(\mathbb{Q}_p)/\mathbf{T}(\mathbb{Z}_p) \cong X_*(\mathbf{T})$$

which, in turn, induces an isomorphism $\mathcal{H}_{\mathbf{T}} \cong \mathbb{C}[X_*(\mathbf{T})]$ between the Hecke algebra and the group algebra of $X_*(\mathbf{T})$. Let $\mathbf{T}^\wedge$ be the dual torus with

$$X_*(\mathbf{T}^\wedge) = X^*(\mathbf{T}) = \mathrm{Hom}(\mathbf{T}, \mathbf{G_m}).$$

In summary there is a natural identification

$$\mathrm{Hom}_{\mathrm{alg}}(\mathcal{H}_{\mathbf{T}}, \mathbb{C}) \cong \mathrm{Hom}_{\mathrm{alg}}(\mathbb{C}[X_*(\mathbf{T})], \mathbb{C}) \cong X^*(\mathbf{T}) \otimes_{\mathbb{Z}} \mathbb{C} = X_*(\mathbf{T}^\wedge) \otimes_{\mathbb{Z}} \mathbb{C} = \mathbf{T}^\wedge(\mathbb{C})$$

between the group of algebra homomorphism $\mathbb{C}[X_*(\mathbf{T})] \to \mathbb{C}$ and the complex points of the dual torus. Now suppose $\mathbf{G}$ as above is split over $\mathbb{Q}_p$. If $\mathbf{T}$ is a maximal torus in $\mathbf{G}$ then the Satake transform (see the survey article [Gr]) gives an isomorphism $\mathcal{H}_{\mathbf{G}} \cong \mathcal{H}_{\mathbf{T}}^W$ between the Hecke algebra for G and the Weyl group invariants in $\mathcal{H}_{\mathbf{T}}$ and hence induces an identification

$$\mathrm{Hom}_{\mathrm{alg}}(\mathcal{H}_{\mathbf{G}}, \mathbb{C}) \cong \mathrm{Hom}_{\mathrm{alg}}(\mathcal{H}_{\mathbf{T}}, \mathbb{C})/W \cong \mathbf{T}^{\wedge}(\mathbb{C})/W$$

between the group of algebra homomorphism $\mathcal{H}_{\mathbf{G}} \to \mathbb{C}$ and orbits of the Weyl group in the group of complex points of the dual torus $\mathbf{T}^{\wedge}(\mathbb{C})$. The set $\mathbf{T}^{\wedge}(\mathbb{C})/W$ also parametrizes semisimple conjugacy classes in the group of complex points $\mathbf{G}^{\wedge}(\mathbb{C})$ of the dual group $\mathbf{G}^{\wedge}$. In the case $\mathbf{G} = \mathbf{GL}(n)$ the maximal torus $\mathbf{T}$ and the dual torus $\mathbf{T}^{\wedge}$ can be identified, as can $\mathbf{G}$ and $\mathbf{G}^{\wedge}$.

[26]These numbers turn out to be essentially the elementary symmetric functions in the eigenvalues of the action of $T(1, \cdots, 1, p, \cdots, p)$ on the corresponding "classical" modular form f; see [K].

[27]It is a theorem that π_p will be unramified for all but finitely many primes p. However the L function for π should contain contributions from all primes, and something else must be done for the ramified primes.

[28]In modern language, this is the intersection cohomology

$$IH^1(\overline{X}, \mathcal{E}_k; \mathbb{Q}) \cong H_P^1(X, \mathcal{E}_k; \mathbb{Q})$$

of the Baily-Borel compactification $\overline{X}$ of X. The intersection cohomology with coefficients in $\mathcal{E}_k$ makes sense, even though the local system $\mathcal{E}_k$ may fail to extend over the Baily-Borel compactification of X. There is also an étale version of intersection cohomology and a comparison isomorphism

$$IH_{\text{ét}}^i(\overline{X}, \mathcal{E}_k; \mathbb{Q}_\ell) \cong IH^i(\overline{X}, \mathcal{E}_k; \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$$

between the étale intersection cohomology of $\overline{X}$ (viewed as an algebraic variety defined over the rational numbers) and the (topological) intersection cohomology of $\overline{X}$. .

References

[A] A. N. Andrianov, **Quadratic Forms and Hecke Operators**, Grundlehren der mathematischen Wissenschaften **286**, Springer Verlag, Berlin, 1987.

[Ar] J. Arthur, The principle of functoriality, Bull. Amer. Math. Soc. **40** (2002), p. 39-53.

[Ba] T. Bailey and A. Knapp, ed., **Representation Theory and Automorphic Forms**, Proc. Symp. Pure Math. **61**, Amer. Math. Soc., Providence, R. I., 1977.

[Be] J. Bernstein and S. Gelbart, ed., **An Introduction to the Langlands Program**, Birkhauser, Boston MA, 2003.

[Bu] D. Bump, **Automorphic Forms and Representations**, Cambridge Studies in Advanced Mathematics **55** (1997), Cambridge University Press, New York.

[BR] D. Blasius and J. Rogawski, Zeta functions of Shimura varieties, in *Motives*, Proc. Symp. Pure Math. **55** (part 2), 525-572, Amer. Math. Soc., Providence R. I., 1994.

[F] E. Frenkel, Recent advances in the Langlands program, Bull. Amer. Math. Soc. **41** (2004), p. 151-184.

[G1] S. Gelbart, **Automorphic Forms on Adele Groups**, Annals of Math Studies **83**, Princeton University Press, Princeton NJ, 1975.

[G2] S. Gelbart, An elementary introduction to the Langlands Program, Bull. Amer. Math. Soc. bf 10 (1984), 177-219.

[GF] I. M. Gelfand and S. Fomin, Geodesic flows on manifolds of constant negative curvature, Uspekhi Mat. Nauk **7** (1952), 118–137; English translation in Amer. Math. Soc. Transl. **1** (1965), 49–65.

[GP] M. Goresky and W. Pardon, Chern classes of automorphic vector bundles, Inv. Math. **147** (2002), 561-612.

[Gr] B. Gross, On the Satake isomorphism, in **Galois Representations in Arithmetic Algebraic Geometry**, A. Scholl and R. Taylor, ed., Cambridge University Press, New York, 1998, p.223-237.

[JL] H. Jacquet and R. Langlands, **Automorphic Forms on GL**(2), Lecture Notes in Mathematics **114**, Springer Verlag, New York, 1970.

[Kn] A. Knapp, Introduction to the Langlands Program, Proc. Symp. Pure Math. **61** (1997), 245-302.

[K] S. Kudla, From modular forms to automorphic representations, in **An Introduction to the Langlands Program**, J. Bernstein and S. Gelbart, ed., Birkhauser, Boston Ma, 2003, p. 133-151.

[M] J. Milne, review of book by M. Harris and R. Taylor, Math Reviews 2002m:11050.

[R1] J. Rogawski, The nonabelian reciprocity law for local fields, Notices of the A. M. S., **47** (2000), 35-41.

[R2] J. Rogawski, review of books by Borel, Bump, and Iwaniec, Bull. A. M. S. **35** (1998), 253-263.

[R3] J. Rogawski, review of books by Laumon, Math Reviews MR 98C:11045a, 98C:11045b.

[Se] J. P. Serre, **A Course in Arithmetic**, Graduate Texts in Mathematics **7**, Springer Verlag, New York, 1973.

[Sh1] G. Shimura, **Introduction to the Arithmetic Theory of Automorphic Forms**, Math. Soc. Jap., 1971, reprinted Princeton University Press, Princeton NJ, 1994.

[T] R. Taylor, Galois representations, Proceedings of the International Congress of Mathematicians, Beijing, 2002, vol I. World Scientific, New York, p. 449-474. See also longer version, to appear in Annales de la Faculte des Sciences de Toulouse.