Amer. Math. Soc. Transl.
(2) Vol. 160, 1994

Modular p-adic L-functions and p-adic Hecke Algebras

Haruzo Hida

§0

In this short article we discuss how the number of variables of modular L-functions is determined by the data from the algebraic group on which the modular forms are defined. To give you an idea about the L-functions before going into this main topic, we start with an interesting story of Euler about the values of the Riemann zeta function. This story provides a good introduction to the subject. The Riemann zeta function is defined by the following infinite series, which is absolutely convergent on the right half of the complex plane defined by $\mathrm{Re}(s) > 1$:

$$\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots + \frac{1}{n^s} + \cdots = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

This series must be a result of a naive question: What number can one get out of the sum of negative powers of all natural numbers? Then it is natural to think about the sum of positive powers of all natural numbers. Of course, one cannot compute the outrageous sum: $1^k + 2^k + 3^k + \cdots + n^k + \cdots$ of growing integers without some trick. Euler proposed the following trick to compute this sum in the mid 18th century. Euler first supposed that the value $\zeta(-k)$ $(0 \le k \in \mathbf{Z})$ actually exists. Then one is forced to have the following interesting identity:

$$\begin{aligned}(1 - 2^{k+1})\zeta(-k) &= \zeta(-k) - 2^{k+1}\zeta(-k) \\ &= (1^k + 2^k + 3^k + \cdots + n^k + \cdots) \\ &\quad - 2((2\cdot 1)^k + (2\cdot 2)^k + (2\cdot 3)^k + \cdots + (2\cdot n)^k + \cdots) \\ &= \{t - 2^k t^2 + 3^k t^3 - 4^k t^4 + \cdots + (-1)^{n+1} n^k t^n + \cdots\}|_{t=1}.\end{aligned}$$

When $k = 0$, we get

$$\begin{aligned}-\zeta(0) &= t\{1 - t + t^2 - t^3 + \cdots + (-t)^n + \cdots\}|_{t=1} \\ &= \left.\frac{t}{1+t}\right|_{t=1} \quad \text{(the sum of a geometric series).}\end{aligned}$$

1991 *Mathematics Subject Classification*. Primary 11G40.

This article originally appeared in Japanese in Sūgaku **44** (4) (1992), 289–305.
The author is partially supported by an NSF grant.

This would tell us that $\zeta(0) = -\frac{1}{2}$. In general, by the well-known formula: $t\frac{d}{dt}t^n = nt^n$, we have that

$$(1) \qquad Z(-k) = (1-2^{k+1})\zeta(-k) = \left(t\frac{d}{dt}\right)^k \left(\frac{t}{1+t}\right)\bigg|_{t=1}.$$

Euler was not playing an empty game, and he proved the following striking formula for m a positive integer:

$$(2) \qquad \begin{aligned} \zeta(2m) &= (-1)^m \frac{(2\pi)^{2m}}{2(2m-1)!}\zeta(1-2m) \\ &= (1-2^{2m})^{-1}(-1)^m \frac{(2\pi)^{2m}}{2(2m-1)!}\left(t\frac{d}{dt}\right)^{2m-1}\left(\frac{t}{1+t}\right)\bigg|_{t=1}. \end{aligned}$$

The left-hand side is the value of an actually converging infinite series and is the value of the complex analytic function $\zeta(s)$ which is well defined on the right half-plane given by $\mathrm{Re}(s) > 1$. The main part of the right-hand side is the value at $t = 1$ of the derivative of a simple rational function $t/(1+t)$. Thus, this is a formula connecting two fundamentally different objects, which was discovered by Euler almost 250 years ago. This formula looks even magical. To the author, the fun in studying number theory lies in learning and finding this sort of "magical relation" connecting two (or more) fundamentally different objects.

From today's view point, the Riemann zeta function has an analytic continuation to $\mathbf{C} - \{1\}$ having a simple pole at $s = 1$ (as proved by Riemann); the formula of Euler for $\zeta(-k)$ actually gives the value at $s = -k$ of the analytic continuation, and the formula (2) is a special case of the functional equation (proved by Riemann):

$$\zeta(s) = \frac{(2\pi)^s\zeta(1-s)}{2\Gamma(s)\cos(\pi s/2)}.$$

We refer to [**W84**] for historical matters about Euler and to [**K75**] and [**H93b**, §§2.1–2.2] for proofs of the above facts.

§1

There is another example of number-theoretic equality. Looking into the formula of Euler, Kummer found the following fact in the 19th century. He fixed a prime p (which we assume to be odd for simplicity). Then for two nonnegative integers k and k'

$$(3) \qquad k \equiv k' \bmod p^n(p-1) \Rightarrow (1-p^k)Z(-k) \equiv (1-p^{k'})Z(-k') \bmod p^{n+1}.$$

In other words, as long as k and k' stay in the same residue class modulo $p-1$, and if k and k' are close under the p-adic topology, then the values $(1-p^k)Z(-k)$ and $(1-p^{k'})Z(-k')$ are close to the same extent. This implies immediately that the function $k \mapsto (1-p^k)Z(-k)$ for positive integers $k \equiv -1 \bmod (p-1)$ extends to a continuous function defined on the p-adic integer ring $\mathbf{Z}_p$ having values in $\mathbf{Z}_p$. We write this function as Z_p (i.e., $Z_p(-k) = (1-p^k)Z(-k)$).

We give here a brief explanation of p-adic numbers. The reader who knows the subject well can skip this paragraph. For each integer n, we define its p-adic absolute value to be $|n|_p = p^{-e}$ if p^e divides n exactly (i.e., n/p^e is an integer but n/p^{e+1} is not an integer). We simply put $|0|_p = 0$. Then it is easy to check that this norm has all the basic properties of the usual absolute value:

(i) $|x|_p = 0 \Leftrightarrow x = 0$,

(ii) $|xy|_p = |x|_p|y|_p$,

and

(iii) $|x + y|_p \leq \max(|x|_p, |y|_p)$.

Then the function $\rho(x, y) = |x - y|_p$ is a metric and gives a structure of a metric space to $\mathbf{Z}$. For example, if $p = 5$, 5 is close to 0 ($|5|_5 = \frac{1}{5}$), $25 = 5^2$ is closer to 0 ($|25|_5 = \frac{1}{25}$) and $125 = 5^3$ is extremely close to 0 ($|125|_5 = \frac{1}{125}$). Thus, this p-adic space is an outrageous world hard to imagine for us living in the Euclidean world. We take the completion $\mathbf{Z}_p$ of $\mathbf{Z}$ under this metric (see [H93b, §1.3] for details of p-adic numbers). The ring $\mathbf{Z}_p$ is called the p-adic integer ring. We write $\mathbf{Q}_p$ for the field of fractions of $\mathbf{Z}_p$. Then $\mathbf{Q}_p$ naturally contains the rational numbers and

$$p^n\mathbf{Z}_p = \{p^n z \mid z \in \mathbf{Z}_p\} = \left\{z \in \mathbf{Q}_p \,\middle|\, |z|_p \leq p^{-n}\right\}: \quad \text{the disk of radius } p^{-n}.$$

The ring $\mathbf{Z}_p$ is then a closed unit disk in $\mathbf{Q}_p$, and hence, is a compact ring. The fact in (3) then implies that $|Z_p(-k) - Z_p(-k')| \leq |k - k'|_p$ as long as k and k' belong to the set of integers $I = \{n \mid n \equiv -1 \bmod (p-1) \text{ and } 0 < n \in \mathbf{Z}\}$. It is easy to check that I is a dense subset of $\mathbf{Z}_p$ (under the p-adic topology). Thus, $Z_p \colon I \to \mathbf{Q}$ extends to a continuous function on $\mathbf{Z}_p$ having values in $\mathbf{Q}_p$. We can verify that Z_p has values in $\mathbf{Z}_p$ using formula (1). The binomial polynomial

$$\binom{s}{n} = \begin{cases} \dfrac{s(s-1)\cdots(s-n+1)}{n!} & \text{if } n > 0, \\ 1 & \text{if } n = 0 \end{cases}$$

is a polynomial with rational coefficients. This can be thought of as a polynomial function of s on $\mathbf{Z}_p$ having values in $\mathbf{Z}$ on the set of all positive integers. Then by continuity, the values $\binom{s}{n}$ fall in $\mathbf{Z}_p$ for all $s \in \mathbf{Z}_p$, i.e., $|\binom{s}{n}|_p \leq 1$. Thus, the binomial expansion

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

converges in $\mathbf{Z}_p$ for all $s \in \mathbf{Z}_p$ if $|z|_p < 1$. That is, on the multiplicative group

$$W = \left\{z \in \mathbf{Z}_p \,\middle|\, |z - 1|_p < 1\right\} = 1 + p\mathbf{Z}_p \subset \mathbf{Z}_p^\times$$

the p-adic power $z^s = (1 + (z-1))^s = \sum_{n=0}^{\infty} \binom{s}{n}(z-1)^n$ is a well-defined p-adic analytic function in s. Here the "p-adic analyticity" means that the function can be expanded into an absolutely convergent power series at every $s \in \mathbf{Z}_p$. This p-adic power satisfies all the formal properties of the usual complex power: $z^{s+t} = z^s z^t$, $z^0 = 1$, and so on. As is well known, the series $\{z^{p^n}\}_n$ is a p-adic Cauchy sequence and obviously $\zeta = \omega(z) = \lim_{n\to\infty} z^{p^n} \in \mathbf{Z}_p$ satisfies $\zeta^p = \zeta$. Thus, ω is a character of $\mathbf{Z}_p^\times$ having values in the subgroup μ (of $\mathbf{Z}_p^\times$) of the $(p-1)$th roots of unity. It is also easy to check $\mathrm{Ker}(\omega) = W$ (here we remind the reader that we always assume p to be odd). Thus, we can define a canonical projection $z \mapsto \langle z \rangle$ of $\mathbf{Z}_p^\times$ onto W by $\langle z \rangle = \omega(z)^{-1}z$. Then we can think of the p-adic analytic function $s \mapsto \langle z \rangle^s$, and

$\langle z\rangle^n = z^n$ if $n \equiv 0 \bmod (p-1)$ for integers n. Then we define the p-adic function $\zeta_p(s)$ $(s \in \mathbf{Z}_p - \{1\})$ by

$$\zeta_p(-s) = (1 - \langle 2\rangle^{s+1})^{-1} Z_p(-s). \tag{4}$$

Obviously this function ζ_p has a singularity at $s = 1$. From (1) we know the following striking formula due basically to Kummer:

$$\zeta_p(k) = (1 - p^k)\zeta(-k) \quad \text{for all positive } k \equiv -1 \bmod (p-1). \tag{5}$$

Later it was shown by Kubota and Leopoldt that $\zeta_p(s)$ is actually a p-adic analytic function defined on $\mathbf{Z}_p - \{1\}$ and has a simple pole at $s = 1$. Moreover, Iwasawa showed the existence of a power series $\Phi \in \mathbf{Z}_p[[T]]$ such that $\zeta_p(s) = (u^s - 1)^{-1}\Phi(u^s - 1)$ for $u = 1 + p$ (which is a topological generator of $W \cong \mathbf{Z}_p$). A p-adic analytic function $f(s_1, \ldots, s_n)$ is called an Iwasawa function if there exists a power series Φ in $A[[X_1, \ldots, X_n]]$ for a p-adically complete valuation ring A over $\mathbf{Z}_p$ such that $f(s_1, \ldots, s_n) = \Phi(u^{s_1} - 1, \ldots, u^{s_n} - 1)$. Thus, $(u^s - 1)\zeta_p(s)$ is an Iwasawa function. The formula (5) connects the complex analytic function $\zeta(s)$ and the p-adic analytic function $\zeta_p(s)$ at positive integers $k \equiv -1 \bmod (p-1)$. Then it is natural to call ζ_p the p-adic Riemann zeta function. We again refer to **[H93b**, §§3.4–3.5] for the proof of these facts.

§2

Now we enter into the principal subject of the note. Although the L-functions we often encounter in number theory are functions of one complex or p-adic variable, there is no apparent reason not to have L-functions of several variables. Probably, we number theorists are too familiar with one-variable L-functions to notice the following fundamental question:

Why do L-functions have only one variable?

An explanation to this fact seems to have been offered first by A. Weil. To explain this, we consider the adèle ring $\mathbf{A}$ of $\mathbf{Q}$. The formal definition of $\mathbf{A}$ is as follows: $\mathbf{A}$ is the subring of $\mathbf{R} \times \prod_p \mathbf{Q}_p$ generated by the diagonal image of $\mathbf{Q}$ and $\widehat{\mathbf{Z}} \times \mathbf{R}$, where $\widehat{\mathbf{Z}} = \prod_p \mathbf{Z}_p$. Here p runs over all primes including 2. The field $\mathbf{Q}$ is considered to be a subring of the product $\mathbf{R} \times \prod_p \mathbf{Q}_p$ via the diagonal map $\mathbf{Q} \ni \alpha \mapsto (\alpha, \ldots, \alpha, \alpha, \ldots) \in \mathbf{R} \times \prod_p \mathbf{Q}_p$. The ring $\widehat{\mathbf{Z}}$ is a product of compact rings $\mathbf{Z}_p$, and hence, is compact. As is easily seen, $\mathbf{A} = \mathbf{Q} + \widehat{\mathbf{Z}} \times \mathbf{R}$ in the product $\mathbf{R} \times \prod_p \mathbf{Q}_p$. Since $\widehat{\mathbf{Z}} \times \mathbf{R} \cap \mathbf{Q} = \mathbf{Z}$, we know that

$$\mathbf{A}/\widehat{\mathbf{Z}} \times \mathbf{R} \cong \mathbf{Q}/\mathbf{Z}.$$

We put on $\widehat{\mathbf{Z}} \times \mathbf{R}$ the product topology of the compact ring $\widehat{\mathbf{Z}}$ and the number line $\mathbf{R}$. Then we extend this topology on $\widehat{\mathbf{Z}} \times \mathbf{R}$ to $\mathbf{A}$ by translation by elements in $\mathbf{Q}$. Thus $\mathbf{A}$ is a locally compact ring. Elements in $\mathbf{A}$ are called *adèles* (see **[H93b**, §8.1] for details of adèles). In particular, we look into the multiplicative group $\mathbf{A}^\times$ of this ring whose elements are called *idèles*. If $z = (z_p)$ is an idèle, then z can be written as $\alpha + z_0$ with $z_0 \in \widehat{\mathbf{Z}} \times \mathbf{R}$ and $\alpha \in \mathbf{Q}$. Thus, there are only finitely many primes p such that $|z_p|_p \neq 1$. By definition, $|z_p|_p$ is a power of p such that $|z_p|z_p|_p|_p = 1$. Thus, the rational number $\alpha = \prod_p |z_p|_p$ is well defined because $|z_p|_p = 1$ for all but finitely many primes p. Then $|\alpha z_p|_p = 1$, and thus, $\alpha z_p \in \mathbf{Z}_p^\times$. We can also replace α by $-\alpha$, if necessary, to ensure that $\alpha z_\infty \in \mathbf{R}_+^\times$, where z_∞ denotes the component of z in $\mathbf{R}$ and $\mathbf{R}_+^\times$ is the group of all positive real numbers. This implies $\alpha z \in \widehat{\mathbf{Z}}^\times \times \mathbf{R}_+^\times$, and thus, we have a natural surjective group homomorphism $\iota: \widehat{\mathbf{Z}}^\times \to \mathbf{A}^\times/\mathbf{Q}^\times\mathbf{R}_+^\times$, $(z \mapsto (z, 1))$. It is then immediate that

$$\widehat{\mathbf{Z}}^\times \cap \mathbf{Q}^\times\mathbf{R}_+^\times = \{1\}.$$

Thus, ι is an isomorphism $\widehat{\mathbf{Z}}^\times \cong \mathbf{A}^\times/\mathbf{Q}^\times\mathbf{R}_+^\times$. Defining the adèle norm $|z|_\mathbf{A}$ by $|z_\infty| \times \prod_p |z|_p$, we also have from the above argument the product formula

$$|\alpha|_\mathbf{A} = 1 \quad \text{for all } \alpha \in \mathbf{Q}.$$

The notion of adèles was created basically to supply a good tool to describe class field theory. We fix an algebraic closure $\overline{\mathbf{Q}}$ of $\mathbf{Q}$. We may identify $\overline{\mathbf{Q}}$ with the totality of all roots in $\mathbf{C}$ of polynomial equations with coefficients in $\mathbf{Q}$. A Galois extension K/F in $\overline{\mathbf{Q}}$ is called abelian if $\mathrm{Gal}(K/F)$ is an abelian group. Abelian extensions have a remarkable property that the composite of any two abelian extensions is again abelian. Thus, there exists the maximal abelian extension written $F_{ab}(\subset \overline{\mathbf{Q}})$ over F which is the composite of all abelian extensions of F. The extension F_{ab} is the fixed field of the commutator subgroup of $\mathrm{Gal}(\overline{\mathbf{Q}}/F)$. A typical example of an abelian extension of $\mathbf{Q}$ is the field generated by all Nth roots of unity for any given integer $N > 1$. If we write $\zeta = \exp(2\pi\sqrt{-1}/N)$, then the field is just $\mathbf{Q}(\zeta)$. Note that

$$\begin{aligned}\mu_N = \{x \in \overline{\mathbf{Q}}^\times \mid x^N = 1\} &= \{\zeta^n \mid n \in (\mathbf{Z}/N\mathbf{Z})\}\\ &\cong (\mathbf{Z}/N\mathbf{Z}): \quad \text{cyclic group of order } N.\end{aligned}$$

For each automorphism σ of $\mathbf{Q}(\zeta)$, σ^{-1} takes ζ to another Nth root of unity $\zeta^{\alpha(\sigma)}$ $(\alpha(\sigma) \in \mathbf{Z}/N\mathbf{Z})$. Since $\zeta^{\alpha(\sigma)}$ is again a generator of the cyclic group μ_N, $\alpha(\sigma)$ belongs to the unit group $(\mathbf{Z}/N\mathbf{Z})^\times$. Naturally, $\alpha(\sigma\tau) = \alpha(\sigma)\alpha(\tau)$, and σ is determined by the value $\alpha(\sigma)$. It is well known that α: $\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q}) \to (\mathbf{Z}/N\mathbf{Z})^\times$ is a surjective isomorphism. Thus, $\mathbf{Q}_{ab}$ contains Nth roots of unity for all n. We can identify the group μ_∞ of all roots of unity with $\mathbf{Q}/\mathbf{Z} = \mathbf{A}/\widehat{\mathbf{Z}} \times \mathbf{R}$ via $\mathbf{Q} \ni a \mapsto \exp(2\pi i a) \in \mu_\infty$. Although $\mathbf{Q}_{ab}$ is an infinite extension of $\mathbf{Q}$, we can still think of the huge abelian group $\mathrm{Gal}(\mathbf{Q}_{ab}/\mathbf{Q})$. Observing that $\mathrm{Aut}(\mathbf{A}/\widehat{\mathbf{Z}} \times \mathbf{R}) = \widehat{\mathbf{Z}}^\times$ via multiplication by elements of $\widehat{\mathbf{Z}}^\times$, we have a group homomorphism, called the cyclotomic character:

$$(6) \qquad \alpha: \mathrm{Gal}(\mathbf{Q}_{ab}/\mathbf{Q}) \to \mathrm{Aut}(\mu_\infty) = \mathrm{Aut}(\mathbf{A}/\widehat{\mathbf{Z}} \times \mathbf{R}) = \widehat{\mathbf{Z}}^\times \cong \mathbf{A}^\times/\mathbf{Q}^\times\mathbf{R}_+^\times$$

given by $\zeta^\sigma = \zeta^{\alpha(\sigma)}$. Class field theory claims that α is in fact a surjective isomorphism:

$$\mathrm{Gal}(\mathbf{Q}_{ab}/\mathbf{Q}) \cong \mathbf{A}^\times/\mathbf{Q}^\times\mathbf{R}_+^\times.$$

This fact was actually conceived, before the appearance of class field theory, by Kronecker as his famous theorem asserting that $\mathbf{Q}_{ab}$ is generated by roots of unity. The analogous fact is true for any number field (i.e., finite extensions of $\mathbf{Q}$). That is, defining a locally compact ring $F_\mathbf{A} = F \otimes_\mathbf{Q} \mathbf{A}$ $(\cong \mathbf{A}^{[F:\mathbf{Q}]}$ as topological spaces) and regarding F as a subfield of $F_\mathbf{A}$ by $F \ni a \mapsto a \otimes 1$, we have a canonical Artin reciprocity homomorphism: $F_\mathbf{A}^\times/F^\times \to \mathrm{Gal}(F_{ab}/F)$ whose kernel is the connected component of the idèle class group $C_F = F_\mathbf{A}^\times/F^\times$ and which is surjective. The above identity is another number-theoretic identity connecting quite different objects.

For any infinite Galois extension $K/\mathbf{Q}$, there is a natural topology on $\mathrm{Gal}(K/\mathbf{Q})$, called the Krull topology. Its fundamental system of neighborhoods of 1 is given by the set of all subgroups that fix a finite extension of $\mathbf{Q}$. Under this topology, $\mathrm{Gal}(K/\mathbf{Q})$ is a compact group (see **[N86**, 1.1]). Then the isomorphism α is in fact an isomorphism of two compact groups.

Since $\mathrm{Gal}(\mathbf{Q}_{ab}/\mathbf{Q})$ is totally disconnected, it does not have many nontrivial complex (quasi) characters. However, the usefulness of characters for studying a given group is something everyone knows by experience. In particular, complex characters are easy to handle. Class field theory offers a way to get meaningful complex characters. The idea is to inflate the Galois group giving a nontrivial connected component. We consider $\mathbf{A}^\times/\mathbf{Q}^\times$ instead of $\mathrm{Gal}(\mathbf{Q}_{ab}/\mathbf{Q}) = \mathbf{A}^\times/\mathbf{Q}^\times\mathbf{R}_+^\times$. Then we have a nontrivial group of quasicharacters:

$$\mathrm{Hom}_{\mathrm{conti}}(\mathbf{A}^\times/\mathbf{Q}^\times, \mathbf{C}^\times).$$

There are infinitely many connected components in the space $\mathrm{Hom}_{\mathrm{conti}}(\mathbf{A}^\times/\mathbf{Q}^\times, \mathbf{C}^\times)$ which is represented by finite-order characters ξ of $\mathbf{A}^\times/\mathbf{Q}^\times$. The connected component containing ω is isomorphic to $\mathbf{C}$ via $\mathbf{C} \ni s \mapsto \xi(x)|x|_{\mathbf{A}}^s$. In particular, we look at the principal component corresponding to the trivial ξ:

$$\mathrm{Hom}_{\mathrm{conti}}(\mathbf{A}^\times/\widehat{\mathbf{Z}}^\times\mathbf{Q}^\times, \mathbf{C}^\times) = \{|x|_{\mathbf{A}}^s \mid s \in \mathbf{C}\} \cong \mathbf{C}.$$

For any idèle z, we define its finite part z_f by zz_∞^{-1}. Thus, z_f has the same component as z at each prime p, but its infinite component is equal to 1. Note that for each positive integer n, $|n_f|_{\mathbf{A}}^s = n^{-s}$, and

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \sum_{n=1}^{\infty} |n_f|_{\mathbf{A}}^s$$

can be considered to be a function on the principal connected component

$$\mathrm{Hom}_{\mathrm{conti}}(\mathbf{A}^\times/\widehat{\mathbf{Z}}^\times\mathbf{Q}^\times, \mathbf{C}^\times)$$

of $\mathrm{Hom}_{\mathrm{conti}}(\mathbf{A}^\times/\mathbf{Q}^\times, \mathbf{C}^\times)$ corresponding to the identity character. This is the reason that $\zeta(s)$ has only one complex variable. Note that $\mathbf{A}^\times/\widehat{\mathbf{Z}}^\times\mathbf{Q}^\times \cong \mathbf{R}_+^\times$ because $\mathbf{A}^\times = \widehat{\mathbf{Z}}^\times\mathbf{Q}^\times\mathbf{R}_+^\times$ and $\widehat{\mathbf{Z}}^\times\mathbf{Q}^\times \cap \mathbf{R}_+^\times = \{1\}$. Thus, we again obtain

$$\mathrm{Hom}_{\mathrm{conti}}(\mathbf{A}^\times/\widehat{\mathbf{Z}}^\times\mathbf{Q}^\times, \mathbf{C}^\times) \cong \mathrm{Hom}_{\mathrm{conti}}(\mathbf{R}_+^\times, \mathbf{C}^\times) \cong \mathbf{C} \quad \text{via } (x \mapsto x^s) \mapsto s$$

which is the domain on which $\zeta(s)$ is defined.

§3

We now argue in the same way to show that the p-adic Riemann zeta function necessarily has only one variable. When we considered the complex zeta function $\zeta(s)$, we removed the factor $\mathbf{R}_+^\times$ at infinity from the denominator of $\mathbf{A}^\times/\mathbf{Q}^\times\mathbf{R}_+^\times = \mathrm{Gal}(\mathbf{Q}_{ab}/\mathbf{Q})$ to obtain the right group on which L-functions are defined. Since the domain on which $\zeta(s)$ is defined is given by $\mathrm{Hom}_{\mathrm{conti}}(\mathbf{A}^\times/\widehat{\mathbf{Z}}^\times\mathbf{Q}^\times, \mathbf{C}^\times)$, we remove the factor $\mathbf{Z}_p^\times$ at p from the denominator $\widehat{\mathbf{Z}}^\times\mathbf{Q}^\times$ and insert $\mathbf{R}_+^\times$ to fill the infinity component. Then we expect to have $\mathrm{Hom}_{\mathrm{conti}}(\mathbf{A}^\times/U^{(p)}\mathbf{Q}^\times, \mathbf{Q}_p^\times)$ as the domain of the p-adic Riemann zeta function, where $U^{(p)} = \mathbf{R}_+^\times \times \prod_{\ell \neq p} \mathbf{Z}_\ell^\times$. Note here that the group $\mathbf{A}^\times/U^{(p)}\mathbf{Q}^\times$ is a quotient group of $\mathbf{A}^\times/\widehat{\mathbf{Z}}^\times\mathbf{Q}^\times = \mathrm{Gal}(\mathbf{Q}_{ab}/\mathbf{Q})$. Therefore, there is a subfield X of $\mathbf{Q}_{ab}$ such that $\mathrm{Gal}(X/\mathbf{Q}) \cong \mathbf{A}^\times/U^{(p)}\mathbf{Q}^\times$. The field X is given by $\mathbf{Q}(1^{1/p^\infty})$ which is the field generated by all p-power roots of unity as we see from the construction of α in (6). Thus, we have the cyclotomic character

$$\chi: \mathbf{A}^\times/U^{(p)}\mathbf{Q}^\times \cong \mathrm{Gal}(\mathbf{Q}(1^{1/p^\infty})/\mathbf{Q}) \cong \mathbf{Z}_p^\times, \tag{7}$$

which satisfies $\chi(z) = z$ for $z \in \mathbf{Z}_p^\times$. Since $\mathbf{Z}_p^\times$ is a compact group (it is a closed disk of radius p^{-1} centered at 1), the image of $\mathbf{Z}_p^\times$ under the continuous homomorphism lies in the maximal compact subgroup of $\mathbf{Q}_p^\times$, which is again $\mathbf{Z}_p^\times$. For each finite group G, writing $A[G]$ for the group algebra of G over a given commutative ring A, we know that

$$\mathrm{Hom}_{\mathrm{gr}}(G, A^\times) \cong \mathrm{Hom}_{A\text{-alg}}(A[G], A).$$

Similarly, any continuous homomorphism $\phi: \mathbf{Z}_p^\times \to \mathbf{Z}_p^\times$ induces modulo p^n a group homomorphism $\phi_n: \mathbf{Z}_p^\times \to (\mathbf{Z}/p^n\mathbf{Z})^\times$ such that $\phi_m \bmod p^n = \phi_n$ for all $m > n$. Note here that $\mathbf{Z}_p^\times = W \times \mu$, $\mathbf{Z}_p \cong W$ via $s \mapsto u^s$ $(u = 1 + p)$, and $(\mathbf{Z}/p^n\mathbf{Z})^\times$ is a cyclic group of order $p^{n-1}(p-1)$ (here we still assume that p is odd). Thus, any $x \in W^{p^{n-1}}$ is $y^{p^{n-1}(p-1)}$ for some $y \in \mathbf{Z}_p^\times$. That is, $\phi_n(x) = 1$ for all $x \in W^{p^{n-1}}$. Hence, ϕ_n must factor through $\mathbf{Z}_p^\times/W^{p^{n-1}} \cong (\mathbf{Z}/p^n\mathbf{Z})^\times$. As a consequence of this argument, we have

$$\begin{aligned}\mathrm{Hom}_{\mathrm{cont}}(\mathbf{Z}_p^\times, \mathbf{Z}_p^\times) &= \varprojlim_n \mathrm{Hom}_{\mathrm{gr}}((\mathbf{Z}/p^n\mathbf{Z})^\times, (\mathbf{Z}/p^n\mathbf{Z})^\times) \\ &= \varprojlim_n \mathrm{Hom}_{\mathbf{Z}_p\text{-alg}}(\mathbf{Z}_p[(\mathbf{Z}/p^n\mathbf{Z})^\times], (\mathbf{Z}/p^n\mathbf{Z})) \\ &= \mathrm{Hom}_{\mathbf{Z}_p\text{-alg}}(\mathbf{Z}_p[[\mathbf{Z}_p^\times]], \mathbf{Z}_p),\end{aligned}$$

where $\mathbf{Z}_p[[\mathbf{Z}_p^\times]] = \varprojlim_n \mathbf{Z}_p[(\mathbf{Z}/p^n\mathbf{Z})^\times]$ is called the continuous group algebra of $\mathbf{Z}_p^\times$. In general, for each profinite group $G = \varprojlim_n G_n$ for finite groups G_n, the continuous group algebra is defined by

$$\mathbf{Z}_p[[G]] = \varprojlim_n \mathbf{Z}_p[G_n],$$

where the transition map $\rho: \mathbf{Z}_p[G_m] \to \mathbf{Z}_p[G_n]$ $(m \geq n)$ is obtained by $\rho(\Sigma_g a_g g) = \Sigma_g a_g \rho(g)$ from the transition map $\rho: G_m \to G_n$.

Writing μ for the group of $(p-1)$th roots of unity in $\mathbf{Z}_p^\times$, we have, as already seen, $\mathbf{Z}_p^\times = W \times \mu$. If $p-1$ is invertible in an integral domain A (for example, in $\mathbf{Z}_p$, $(p-1)^{-1} = -(1 + p + p^2 + p^3 + \cdots) \in \mathbf{Z}_p$) and if A contains all $(p-1)$th roots of unity, then the group algebra $A[\mu]$ is isomorphic to the product of copies of A indexed by characters of μ having values in $A^\times$. We write $\hat{\mu}$ for the set of all characters of μ. Then $\hat{\mu} = \{\omega^a | a = 0, \dots, p-2\}$ for the inclusion $\omega: \mu \to A^\times$. Each projection of $A[\mu]$ onto the component A indexed by ω^a is actually given by the algebra homomorphism corresponding to ω^a. Note that $\mathbf{Z}_p^\times/W^{p^n} = \mu \times (W/W^{p^n})$, and hence,

$$\mathbf{Z}_p[\mu \times (W/W^{p^n})] = \mathbf{Z}_p[W/W^{p^n}][\mu] = \prod_{\xi \in \hat{\mu}} \mathbf{Z}_p[W/W^{p^n}]$$

and

$$\mathbf{Z}_p[[\mathbf{Z}_p^\times]] = \prod_{\xi \in \hat{\mu}} \mathbf{Z}_p[[W]].$$

Thus, we see that

$$\begin{aligned}\mathrm{Hom}_{\mathrm{conti}}(\mathbf{Z}_p^\times,\mathbf{Z}_p^\times) &= \mathrm{Hom}_{\mathbf{Z}_p\text{-alg}}(\mathbf{Z}_p[[\mathbf{Z}_p^\times]],\mathbf{Z}_p)\\ &= \coprod_{\xi\in\hat{\mu}} \mathrm{Hom}_{\mathbf{Z}_p\text{-alg}}(\mathbf{Z}_p[[W]],\mathbf{Z}_p).\end{aligned}$$

The last identification is given just because any $\mathbf{Z}_p$-algebra homomorphism of $\mathbf{Z}_p[[\mathbf{Z}_p^\times]]$ into $\mathbf{Z}_p$ must factor through a component $\mathbf{Z}_p[[W]]$ for a unique $\xi\in\hat{\mu}$. We know that W/W^{p^n} is a cyclic group of order p^n. Thus,

$$\mathbf{Z}_p[W/W^{p^n}]\cong\mathbf{Z}_p[t]/(t^{p^n}-1)\cong\mathbf{Z}_p[T]/((1+T)^{p^n}-1)\ (\text{by } t=1+T).$$

Then it is easy to see (cf. [**Wa82**, Theorem 7.1]) that

$$\Lambda=\mathbf{Z}_p[[W]]\cong\mathbf{Z}_p[[T]]=\varprojlim_n\mathbf{Z}_p[T]/((1+T)^{p^n}-1).$$

Thus, any continuous algebra homomorphism ϕ of Λ into $\mathbf{Z}_p$ is determined by its value at T. Since $\lim_{n\to\infty}T^{p^n}=0$ in Λ, $\lim_{n\to\infty}\phi(t)^{p^n}=1$, and hence, $\phi(t)=u^s\in W$. Thus,

$$\mathrm{Hom}_{\mathbf{Z}_p\text{-alg}}(\mathbf{Z}_p[[W]],\mathbf{Z}_p)\cong\mathbf{Z}_p\quad\text{via }\phi\leftrightarrow s\text{ for }\phi(T)=u^s.$$

In particular, the domain on which $\zeta_p(s)$ is defined is the component

$$\mathrm{Hom}_{\mathbf{Z}_p\text{-alg}}(\mathbf{Z}_p[[W]],\mathbf{Z}_p)$$

corresponding to the identity character $\xi=\omega^0$.

We now fix an algebraic closure $\overline{\mathbf{Q}}_p$ of $\mathbf{Q}_p$. Thus $\overline{\mathbf{Q}}$ is a subfield of $\mathbf{C}$ as well as $\overline{\mathbf{Q}}_p$. There is a natural p-adic norm $|\ |_p$ on $\overline{\mathbf{Q}}_p$ extending $|\ |_p$ on $\mathbf{Q}_p$. We can take $\mathrm{Hom}_{\mathbf{Z}_p\text{-alg,conti}}(\mathbf{Z}_p[[W]],\overline{\mathbf{Q}}_p)$ in place of $\mathrm{Hom}_{\mathbf{Z}_p\text{-alg}}(\mathbf{Z}_p[[W]],\mathbf{Z}_p)$. It is easy to see that

$$\text{(8)}\quad \mathrm{Hom}_{\mathbf{Z}_p\text{-alg,conti}}(\mathbf{Z}_p[[W]],\overline{\mathbf{Q}}_p)\cong\left\{x\in\overline{\mathbf{Q}}_p\,\middle|\,|x|_p<1\right\}=D\quad\text{via }\phi\leftrightarrow\phi(T).$$

As we have already noted, $(u^s-1)\zeta_p(s)$ is an Iwasawa function, i.e., $(u^s-1)\zeta_p(s)=\Phi(u^s-1)$ for $\Phi\in\mathbf{Z}_p[[T]]$. Thus in fact, we may regard $\zeta_p(x)$ as a function on D given by $x\zeta_p(x)=\Phi(x)$ for $x\in D$. This is the point of view taken in [**I72**]. In particular, the p-adic Riemann zeta function is legitimately of one variable.

§4

The principle behind our argument in §2 and §3 is to regard each L-function as a function of characters. Then the values of characters can be considered as eigenvalues of the regular representation on a suitable space of functions on $\mathbf{Q}^\times\backslash\mathbf{A}^\times=\mathrm{GL}_1(\mathbf{Q})\backslash\mathrm{GL}_1(\mathbf{A})$. That is, for each function ϕ: $\mathrm{GL}_1(\mathbf{Q})\backslash\mathrm{GL}_1(\mathbf{A})\to\mathbf{C}$, we define the representation R of $\mathrm{GL}_1(\mathbf{A})$ by $(R(g)\phi)(x)=\phi(xg)$. A typical choice of such spaces is the L_2-space on $\mathrm{GL}_1(\mathbf{Q})\backslash\mathrm{GL}_1(\mathbf{A})$ with respect to the Haar measure on $\mathrm{GL}_1(\mathbf{Q})\backslash\mathrm{GL}_1(\mathbf{A})$. Actually, for each Hecke character ξ, we may regard ξ as the eigenvector of the operators $R(g)$: $R(g)\xi=\xi(g)\xi$ with eigenvalue $\xi(g)$.

Now we explore the same question for nonabelian L-functions. The idea of Langlands is to use the topological space $\mathrm{GL}_n(\mathbf{Q})\backslash\mathrm{GL}_n(\mathbf{A})$. The group $\mathrm{GL}_n(\mathbf{A})/\mathbf{R}_+^\times$ is a locally compact group having a Haar measure $d\mu_n(x)$. Since $\mathrm{GL}_n(\mathbf{Q})$ acts discretely on $\mathrm{GL}_n(\mathbf{A})/\mathbf{R}_+^\times$, we have a fundamental domain Φ in $\mathrm{GL}_n(\mathbf{A})/\mathbf{R}_+^\times$ of

$\mathrm{GL}_n(\mathbf{Q})$. We then define the invariant measure $d\mu$ on $X = \mathrm{GL}_n(\mathbf{Q})\backslash \mathrm{GL}_n(\mathbf{A})/\mathbf{R}_+^\times$ by $\int_X \phi\, d\mu(x) = \int_{\mathfrak{D}} \phi\, d\mu_0(x)$. We fix a Hecke character ξ of $\mathbf{A}^\times/\mathbf{Q}^\times$ and consider measurable functions $\phi\colon \mathrm{GL}_n(\mathbf{A}) \to \mathbf{C}$ satisfying

(1) $\quad \phi(\alpha z x) = \xi(z)\phi(x)$ for all scalar matrices $z \in \mathbf{A}^\times$ and $\alpha \in \mathrm{GL}_n(\mathbf{Q})$.

For two functions ϕ and ϕ' satisfying (1), the function $x \mapsto \overline{\phi(x)}\phi'(x)|\xi(\det(x))|^{-1}$ is invariant under left multiplication by $\mathbf{R}_+^\times$ and right multiplication by $\mathrm{GL}_n(\mathbf{Q})$. Thus, we can define the inner product of such functions by

$$(\phi, \phi') = \int_X \overline{\phi(x)}\phi'(x)|\xi(\det(x))|^{-1}\, d\mu(x).$$

Then the L_2-space $L_2(\xi)$ is defined with respect to this inner product. We can let $\mathrm{GL}_n(\mathbf{A})$ act on $L_2(\xi)$ by $(R_\xi(g)\phi)(x) = \phi(xg)$. We thus have a representation R_ξ that satisfies $(R_\xi(g)\phi, R_\xi(g)\phi') = |\xi(\det(g))|(\phi, \phi')$. Thus, the twisted representation $R_\xi \otimes |\xi|^{-1/2}((R_\xi \otimes |\xi|^{-1/2})(g) = |\xi(\det(g))|^{-1/2} R_\xi(g))$ is unitary and has a spectral decomposition. It is known by Langlands' theory of Eisenstein series **[L76]** that we have

$$R_\xi = \widehat{\bigoplus}_{\pi:\ \text{irreducible}} \pi \oplus \left\{\bigoplus \text{continuous sum}\right\}.$$

The continuous sum is at most $(n-1)$-dimensional. We may also consider the regular representation R on $L_2(\mathrm{GL}_n(\mathbf{Q})\backslash \mathrm{GL}_n(\mathbf{A}))$ defined in a way similar to R_ξ. Thus, the regular representation R on $L_2(\mathrm{GL}_n(\mathbf{Q})\backslash \mathrm{GL}_n(\mathbf{A}))$ has at most an n-dimensional continuous spectrum, and we write this fact *symbolically* as

$$R = \widehat{\bigoplus} \int_{\widehat{G}} \pi \otimes \eta\, d\eta \oplus \left\{\bigoplus \int_{\widehat{G}} (\text{continuous sum})\, d\eta\right\} \quad \text{for a fixed } \xi,$$

where $\widehat{G}$ is the space of unitary characters of $G = \mathbf{A}^\times/\mathbf{Q}^\times$ (which is isomorphic to the disjoint union of $\sqrt{-1}\mathbf{R}$ because $\mathrm{Hom}_{\mathrm{conti}}(\mathbf{A}^\times/\mathbf{Q}^\times, \mathbf{C}^\times)$ is a disjoint union of $\mathbf{C}$). Now we assume that π is cuspidal, i.e., π is realized on the subspace

$$L_2^0(\xi) = \left\{\phi \in L_2(\xi) \mid \int_{N(\mathbf{Q})\backslash N(\mathbf{A})} \phi(xn)\, dn = 0 \text{ for almost all } x \in \mathrm{GL}_n(\mathbf{A})\right\},$$

where in the above definition N runs over all standard unipotent subgroups in $\mathrm{GL}_n(\mathbf{Q})$. The representation on the space $L_2^0(\xi)$ is known to be decomposed into a discrete sum of irreducible representations in which each irreducible representation occurs at most once. We then know that π as above can be decomposed as $\bigotimes_p \pi_p \otimes \pi_\infty$ for local representations π_p of $\mathrm{GL}_n(\mathbf{Q}_p)$ and π_∞ of $\mathrm{GL}_n(\mathbf{R})$. Moreover, for all but finitely many p, the representation π_p has a vector in its representation space fixed by $K_p = \mathrm{GL}_n(\mathbf{Z}_p)$. Such representations having a nontrivial fixed vector by $K_p = \mathrm{GL}_n(\mathbf{Z}_p)$ are called spherical (or unramified). If π_p is spherical and irreducible, then the vectors fixed by K_p form a one-dimensional space $V(\pi_p)$. We then define an action of the double coset $K_p g K_p$ for $g \in M_n(\mathbf{Z}_p) \cap \mathrm{GL}_n(\mathbf{Q}_p)$ on $V(\pi_p)$ by

$$\pi(K_p g K_p)v = \sum_{g_i} \pi(g_i)v \quad \text{for any disjoint decomposition } K_p g K_p = \coprod_i g_i K_p.$$

Since $\pi(K_p g K_p)v$ is an average of $\pi(g)v$ over a double coset $K_p g K_p$, it again falls in $V(\pi_p)$. Thus, v is an eigenvector of all operators of the form of $T = \sum_g \pi(K_p g K_p)$.

We write $\lambda(T)$ for the eigenvalue of T. We specify these operators as follows: first, decomposing the set $\{g \in M_n(\mathbf{Z}_p) \mid \det(g)\mathbf{Z}_p = p^m\mathbf{Z}_p^\times\}$ into a disjoint union of double cosets $K_p g K_p$, we define the Hecke operator T_{p^m} by $\Sigma_g \pi(K_p g K_p)$. We write $T_i(p) = \pi(K_p \varpi_i K_p)$ for the diagonal matrix ϖ_i having i p's and $n-i$ 1's as diagonal entries. Then we can show [**Sh71**, Theorem 3.21] that the formal power series $\sum_{m=0}^{+\infty} \lambda(T_{p^m})X^m$ is a rational function, and in fact, we have

$$\text{(L)} \quad \sum_{m=0}^{\infty} \lambda(T_{p^m})X^m = L_{\pi_p}(X)^{-1} \quad \text{for } L_{\pi_p}(X) = \sum_{i=0}^{n} (-1)^i p^{i(i-1)/2} \lambda(T_i(p))X^i.$$

We define $L(s, \pi_p \otimes \eta_p) = L_{\pi_p \otimes \eta_p}(p^{-s})^{-1}$ if $\pi \otimes \eta_p$ is spherical for each quasicharacter η_p of $\mathbf{Q}_p^\times$. There is a representation theoretic way of defining a polynomial $L_{\pi_p \otimes \eta_p}(X)$ of degree $\leq n$ with $L_{\pi \otimes \eta_p}(0) = 1$ even for nonspherical $\pi_p \otimes \eta_p$ [**GJ72**]. We define $L(s, \pi_p) = L_{\pi \otimes \eta_p}(p^{-s})^{-1}$ for such π_p and η_p, and we set

$$L(s, \pi \otimes \eta) = \prod_p L(s, \pi_p \otimes \eta_p) \quad \text{for each Hecke character } \eta: \mathbf{Q}^\times \backslash \mathbf{A}^\times \to \mathbf{C}^\times,$$

which converges absolutely if $\mathrm{Re}(s)$ is sufficiently large, has an analytic continuation to the entire complex plane, and satisfies a good functional equation [**GJ72**]. Thus, we may regard $L(s, \pi \otimes \eta)$ as a function defined on the connected component of the spectrum, which is isomorphic to the connected component of the space of Hecke characters $\mathrm{Hom}_{\mathrm{cont}}(\mathbf{Q}^\times \backslash \mathbf{A}^\times, \mathbf{C}^\times)$ via $\pi \otimes \eta \leftrightarrow \eta$. Thus, $L(s, \pi \otimes \eta)$ is of one variable.

§5

When we consider the commutative algebraic group $G = \mathrm{GL}(1)$, there is a surjective homomorphism $\mathrm{GL}_1(\mathbf{Q}) \backslash \mathrm{GL}_1(\mathbf{A})$ onto $\mathrm{Gal}(\mathbf{Q}_{ab}/\mathbf{Q})$. Thus, the automorphic side $\mathrm{GL}_1(\mathbf{Q}) \backslash \mathrm{GL}_1(\mathbf{A})$ and the Galois side $\mathrm{Gal}(\mathbf{Q}_{ab}/\mathbf{Q})$ are directly linked. In the nonabelian case, the automorphic side is just a topological space $\mathrm{GL}_n(\mathbf{Q}) \backslash \mathrm{GL}_n(\mathbf{A})$, and at the Galois side there is no way to define naively an extension $\mathbf{Q}_{\mathrm{GL}(n)}$ of $\mathbf{Q}$ which replaces $\mathbf{Q}_{ab} = \mathbf{Q}_{\mathrm{GL}(1)}$ in the sense that the irreducible factors of the regular representation of $\mathrm{GL}_n(\mathbf{A})$ on $L_2(\mathrm{GL}_n(\mathbf{Q}) \backslash \mathrm{GL}_n(\mathbf{A}))$ correspond to the irreducible representations of $\mathrm{Gal}(\mathbf{Q}_{\mathrm{GL}(n)}/\mathbf{Q})$. Thus, the automorphic side and the Galois side seem to come apart in the nonabelian case.

Even in the abelian case, we need to replace the actual Galois group by $\mathbf{Q}^\times \backslash \mathbf{A}^\times$ to get many complex quasicharacters. Thus, we need to find a good group extending $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ for the Galois side. The first attempt to find such a group was made by A. Weil. He found, up to isomorphism, a system of groups called the Weil groups [W51] (see also [T79]): To get $\mathbf{Q}^\times \backslash \mathbf{A}^\times$, we extended the Galois group $\mathrm{Gal}(\mathbf{Q}_{ab}/\mathbf{Q})$ by the connected component of $\mathbf{Q}^\times \backslash \mathbf{A}^\times$. Thus, to get the nonabelian version of $\mathbf{Q}^\times \backslash \mathbf{A}^\times$, we need to inflate the total Galois group $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ by a suitable connected component which has to be compatible with class field theory over all finite extensions $F/\mathbf{Q}$. Thus, the Weil groups W_F are indexed by finite extensions $F/\mathbf{Q}$ and are in fact a system of triples $(W_F, \varphi, \{r_F\})$ consisting of a locally compact topological group W_F satisfying $W_F \supset W_E$ if $E \supset F$, a surjective homomorphism $\varphi: W_Q \to \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ of topological groups inducing $W_F/W_E \cong \mathrm{Hom}_F(E, \overline{\mathbf{Q}})$ *for all finite extensions* $E/F/\mathbf{Q}$ and another isomorphism of topological groups $r_E: C_E \cong W_E^{ab} = W_E/\overline{[W_E : W_E]}$ for each finite extension E/F in $\overline{\mathbf{Q}}$, where $\overline{[W_E : W_E]}$ is the closure of the commutator subgroup $[W_E : W_E]$. The system is characterized by the following properties:

(W1) The composite: $C_E \xrightarrow{r_E} W_E^{ab} \xrightarrow{\varphi} \mathrm{Gal}(E_{ab}/E)$ gives the Artin reciprocity map of class field theory for E;

(W2) The following diagrams are commutative: for $\sigma = \varphi(w) \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ and for E/F

$$\begin{array}{ccc} x & \longmapsto & x^{\sigma} \\ C_E & \longrightarrow & C_{E^\sigma} \\ {\scriptstyle r_E}\downarrow & & \downarrow{\scriptstyle r_{E^\sigma}} \\ W_E^{ab} & \longrightarrow & W_{E^\sigma}^{ab} \\ v & \longmapsto & wvw^{-1} \end{array}$$

$$\begin{array}{ccc} C_F & \xrightarrow{r_F} & W_F^{ab} \\ {\scriptstyle \text{inclusion}}\downarrow & & \downarrow{\scriptstyle \text{transfer},} \\ C_E & \xrightarrow{r_E} & W_E^{ab} \end{array} \qquad \begin{array}{ccc} C_E & \xrightarrow{r_E} & W_E^{ab} \ni v \\ {\scriptstyle \text{norm}}\downarrow & & \downarrow \quad \downarrow \\ C_F & \xrightarrow{r_F} & W_F^{ab} \ni v \end{array}$$

where the transfer map is defined as follows: For each group G and its subgroup, choosing a complete representative set R for $H \backslash G$, we define the transfer $t : G/[G:G] \to H/[H:H]$ by $t(g[G:G]) = \prod_{x \in R} h_x \mod [H:H]$;

(W3) Writing $W_{F/\mathbf{Q}} = W_Q/\overline{[W_F : W_F]}$, we have that groups. $W_Q = \varprojlim_F W_{F/Q}$ as topological

The existence of the system $\{W_F\}$ is shown by using the data of the "canonical 2-cocycle" appearing in class field theory, and hence, is highly artificial (see **[T79]** for the construction). Similarly, we can also construct the local Weil group by replacing finite extensions $F/\mathbf{Q}$ (resp. C_F) by finite extensions $F/\mathbf{Q}_p$ (resp. $F^\times$) and by using local class field theory in place of global class field theory. In this local case, we can actually see the group in an explicit manner. Write k_E for the residue field of an algebraic extension $E/\mathbf{Q}_p$; in particular, $k_{\overline{\mathbf{Q}}_p} = \overline{k}$ is an algebraic closure of k_F. Then Frob: $x \mapsto x^q$ for $q = \# k_F$ is a topological generator of $\mathrm{Gal}(\overline{k}/k_F)$. Then W_F is canonically given by the subgroup of $\mathrm{Gal}(\overline{\mathbf{Q}}_p/F)$ consisting of automorphisms σ which induce on $\overline{k}$ a power of Frob. The kernel of the natural map: $W_F \to \mathrm{Gal}(\overline{k}/k_F)$ (with dense image) is called the inertia subgroup of W_F. We write I_p for the inertia group of W_{Q_p}. Then we define $r_F : F^\times \to W_F^{ab}$ by the reciprocity map such that $r_F(a)$ induces $x \mapsto x^{|a|_p^{-d}}$ on $\overline{k}$ for $a \in F^\times$ and $d = [F : \mathbf{Q}_p]$. Then the compatibility of local and global class field theory implies the existence of a natural morphism $\theta_p : W_{Q_p} \to W_Q$ making the following diagram commutative:

$$\begin{array}{ccc} W_{Q_p} & \xrightarrow{\text{Inc}} & \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p) \\ {\scriptstyle \theta_p}\downarrow & & \cap \\ W_Q & \xrightarrow[\varphi]{} & \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}). \end{array}$$

Of course, the last vertical inclusion map depends on our embedding of $\overline{\mathbf{Q}}$ into $\overline{\mathbf{Q}}_p$. We have a natural Frobenius element $\mathrm{Frob}_p = \theta_p(\mathrm{Frob})$ in W_Q modulo I_p. For any continuous representation $\xi : W_Q \to \mathrm{End}_C(V)$ for a finite-dimensional $\mathbf{C}$-vector space V, we consider the subspace V^{I_p} fixed by the inertia group I_p. Then $\xi(\mathrm{Frob}_p)$ has meaning on V^{I_p} because Frob is determined modulo I_p. Then we define the L-function of ξ by

$$L(s,\xi) = \prod_p \det((\mathrm{id} - p^{-s}\xi(\mathrm{Frob}_p))|_{V^{I_p}})^{-1}.$$

As A. Weil proved, these L-functions (which converge on a suitable right half-plane) have meromorphic continuations on the whole complex plane and satisfy a good functional equation. Our desire is to find a good classification map

$$\imath : \{\text{isomorphism classes of continuous irreducible representations of } W_Q \text{ into } \mathrm{GL}_n(\mathbf{C})\} \to \left\{\text{irreducible representations occurring on } \bigoplus_{\xi} L^0_2(\xi)\right\}$$

preserving L-functions (i.e., $L(s,\imath(\sigma)) = L(s,\sigma)$) and to describe its image. We can think of the corresponding problem for W_{Q_p}. This problem is called the local Langlands conjecture [**T79**, 4.1.7]), which has been proven for many values of n (see [**He85**] and [**Ku87**]), that is, supercuspidal representations of $\mathrm{GL}_n(\mathbf{Q}_p)$ are classified by representations of the local Weil group via L-functions and its ε-factors. Actually, enlarging the Weil group a little (the enlarged group is called the Deligne-Weil group W'_{Q_p}), we can extend this conjecture to a correspondence between all semisimple representations of W'_{Q_p} and local admissible representations of $\mathrm{GL}_n(\mathbf{Q}_p)$ (see [**T79**, §4]). The local conjecture is successfully solved because the local Galois group is solvable (that is, it can be approximated by abelian groups). The Weil group, constructed out of all known abelian data from class field theory, tries to describe nonabelian objects. Therefore, it is like peering into the whole nonabelian world through a small hole of the established abelian theory. Since the global Galois group is highly nonabelian, the image of $\imath$ is small [**T79**, (2.1–2.3)]. The representations of W_Q consist of representations of Artin type, i.e., those having finite image (factoring through $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$), representations of Hecke type, i.e., twists of representations of Artin type by Hecke characters, and induced representations of previous types. We call automorphic representations in the image representations of Weil type. Even the Hasse-Weil zeta function of modular elliptic curves without complex multiplication cannot be associated to an automorphic representation of Weil type. Thus, we need to look at all the algebraic objects, simultaneously, which yield "good" (abelian and nonabelian) Galois representations. This idea is first conceived by Grothendieck as his theory of motives and is later elaborated by Deligne [**DMOS82**]. Admitting the standard conjectures, we see that the category of motives is (Tannakian and) equivalent to the (Tannakian) category of algebraic representations of a huge proalgebraic group $\mathscr{G}$ which is an extension of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. All irreducible algebraic representations of the motivic Galois group $\mathscr{G}$ should be somehow classified by algebraic automorphic representations (Langlands' hypothesis), but even the formulation of this expectation is not yet clear (see [**C90**]). Here the word "algebraic" means, on the Galois side, a morphism of the proalgebraic group $\mathscr{G}$ into the algebraic group $\mathrm{GL}(n)$ and, on the automorphic side, that the finite part of the automorphic representation is defined over a number field.

Under the isomorphism $\alpha\colon \mathrm{Gal}(\mathbf{Q}_{ab}/\mathbf{Q}) \cong \mathbf{A}^\times/\mathbf{Q}^\times\mathbf{R}_+^\times$, the group $\mathbf{Z}_p^\times$ corresponds to the image of the inertia group I_p at p in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Thus, it is natural to call a Hecke character $\xi\colon \mathbf{Q}^\times\backslash\mathbf{A}^\times \to \mathbf{C}^\times$ unramified at p if ξ is trivial on $\mathbf{Z}_p^\times$. A Hecke character ξ is unramified at all but finitely many primes p. A Hecke character ξ is called algebraic if $\xi(z_\infty) = z_\infty^m$ for $z_\infty \in \mathbf{R}_+^\times$. This definition is compatible with the definition of algebraic automorphic representations, i.e., ξ is algebraic in the above sense if and only if $\xi(z)$ stays in a number field E for all $z \in \mathbf{A}_f^\times$. According to Weil, we can attach to an algebraic ξ a (continuous) Galois character $\xi_{\mathscr{P}}$ into $E_{\mathscr{P}}^\times$ for the $\mathscr{P}$-adic completion $E_{\mathscr{P}}$ of E for each prime ideal $\mathscr{P}$ of E. The character $\xi_{\mathscr{P}}$ is characterized by the following properties:

(i) If p is prime to $\mathscr{P}$ then $\xi_{\mathscr{P}}$ is unramified at p if and only if ξ is unramified at p;

(ii) If p is prime to $\mathscr{P}$ and ξ is unramified at p, then $\xi_{\mathscr{P}}(\mathrm{Frob}_p) = \xi(p_p)$, where p_p is the image of $p \in \mathbf{Q}_p^\times$ (but not the image of $p \in \mathbf{Q}^\times$) in $\mathbf{A}^\times$.

We then define

$$L(s,\xi) = \prod_{p \text{ unramified}} (1-\xi(p_p)p^{-s})^{-1} = \prod_{p \text{ unramified}} (1-\xi_{\mathscr{P}}(\mathrm{Frob}_p)p^{-s})^{-1}.$$

Thus, if we consider Galois characters having values in an $\mathscr{P}$-adic field, then we do not need to enlarge the Galois group. This fact is partially true in the nonabelian case. To each (Grothendieck) motive $M_{/\mathbf{Q}}$ of rank n with coefficients in a number field E, we can associate a compatible system $\xi = \{\xi_{\mathscr{P}}\}_{\mathscr{P}}$ of $\mathscr{P}$-adic Galois representations indexed by prime ideals of E. Without referring to motives, we can define a compatible system ξ of $\xi_{\mathscr{P}}\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_n(E_{\mathscr{P}})$ as follows. First of all, $\xi_{\mathscr{P}}$ is unramified outside Nl for an integer N independent of $\mathscr{P}$ (l is the residual characteristic of $\mathscr{P}$). Let $V(\xi_{\mathscr{P}})$ be the representation space of $\xi_{\mathscr{P}}$ and consider the subspace $V(\xi_{\mathscr{P}})^{I_p}$ fixed by I_p. Then $\xi(\mathrm{Frob}_p)$ actually acts on $V(\xi_{\mathscr{P}})^{I_p}$. Here the system $\xi = \{\xi_{\mathscr{P}}\}_{\mathscr{P}}$ is called compatible if

$$L_{\xi,p}(X) = \det((1 - X\xi_{\mathscr{P}}(\mathrm{Frob}_p))|_{V(\xi_{\mathscr{P}})^{I_p}}) \in E[X] \text{ for all } p \text{ outside } Nl$$

is independent of $\mathscr{P}$. We then define

$$L(s,\xi) = \prod_p L_{\xi,p}(p^{-s})^{-1}.$$

When ξ is attached to a motive M, this L-function is called the L-function of the motive M and is written as $L(s,M)$. If the classification map referred to as the Langlands hypothesis

$$\iota\colon \{\text{simple motives}\} \to \{\text{algebraic irreducible cuspidal automorphic representations}\}$$

exists, then it must satisfy the identity of L-functions: $L(s,\iota(M)) = L(s,M)$.

§6

We now turn to the p-adic case. Hereafter, unless otherwise mentioned, we suppose that $p > 2$ and $n = 2$ (i.e., we consider the algebraic group $\mathrm{GL}(2)_{/\mathbf{Q}}$). The fundamental question is:

What type of space should we take as a p-adic analog of $L_2^0(\xi)$?

Here we only think about automorphic representations of p-power conductors to make our argument simple. Such representations always possess a vector invariant under the group $U(p^\infty)$ of the matrices in $GL_2(\widehat{\mathbf{Z}})$ which are unipotent at p. Thus, even in the complex case, we can replace $L_2^0(\xi)$ by invariant vectors under $U(p^\infty)$. There are several different choices of such analogs. A naive (algebro-geometric) definition of the space of p-adic modular forms is possible **[K78]**, but here we give a cohomological definition of a p-adic analog of $L_2^0(\xi)$ which can be easily extended to $GL(2)_{/F}$ for all number fields F. We consider the following open compact subgroups of $GL_2(\mathbf{A}_f)$:

$$(9)\qquad U(p^r) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in U_1(N) \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod p^r\widehat{\mathbf{Z}} \right\} \quad \text{and} \quad U(p^\infty) = \bigcap_r U(p^r).$$

The group $GL_2(\mathbf{R})$ acts on $\mathbf{C}$-$\mathbf{R}$ via $\gamma(z) = \frac{az+b}{cz+d}$ for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. We then set $GL_2^+(\mathbf{R}) = \{\gamma \in GL_2(\mathbf{R}) \mid \gamma(H) = H\}$ for the upper half complex plane $H = \{z \in \mathbf{C} \mid \mathrm{Im}(z) > 0\}$. Then for $GL_2^+(\mathbf{R}) = \{x \in GL_2(\mathbf{R}) \mid \det(x) > 0\}$, we have $GL_2^+(\mathbf{R})/C_\infty \cong H$ via $g \mapsto g(\sqrt{-1})$, where $C_\infty = SO_2(\mathbf{R})\mathbf{R}^\times$ is the pull-back image of the standard maximal compact subgroup of $PGL_2(\mathbf{R})$. For each open compact subgroup S of $GL_2(\mathbf{A}_f)$, we consider the quotient topological space

$$X(S) = GL_2(\mathbf{Q})\backslash GL_2(\mathbf{A})/SC_\infty \cong GL_2^+(\mathbf{Q})\backslash GL_2^+(\mathbf{A})/SC_\infty,$$

where $GL_2^+(\mathbf{A}) = GL_2(\mathbf{A}_f) \times GL_2^+(\mathbf{R})$ and $GL_2^+(\mathbf{Q}) = GL_2(\mathbf{Q}) \cap GL_2^+(\mathbf{A})$. If S is sufficiently small so that $S \subset U(p^r)$ for some $p^r \geq 4$, then $X(S)$ is an open Riemann surface with finitely many connected components which are isomorphic to $\Gamma\backslash H$ for some congruence subgroup Γ ($\cong SL_2(\mathbf{Z}) \cap S$) of $SL_2(\mathbf{Z})$ (**[Sh71**, Chapter 6] and **[H93b]**). In particular, we write $X(p^r)$ for $X(U(p^r))$.

Let A be a complete valuation ring in $\overline{\mathbf{Q}}_p$ with finite residue field, and let K be its quotient field. Assume that $[K : \mathbf{Q}_p] < +\infty$. Take an A-module M with an action of

$$S'_p = \{u'_p = \det(u_p)u_p^{-1} \in GL_2(\mathbf{Z}_p) \mid u \in S\}.$$

Then we let $GL_2(\mathbf{Q})$ (resp., SC_∞) act on $GL_2(\mathbf{A}) \times M$ from the left (resp., from the right) as follows: $\alpha(x, m)u = (\alpha xu, u'_p m)$. This action is a discrete action if we use the discrete topology on M and the product topology on $GL_2(\mathbf{A}) \times M$. We then define the quotient space $\underline{M} = GL_2(\mathbf{Q})\backslash\{GL_2(\mathbf{A}) \times M\}/SC_\infty$. This space $\underline{M}$ is a covering space of the Riemann surface $X(S)$ which is locally homeomorphic to $X(S)$. We consider the sheaf of continuous sections of $\underline{M} = \underline{M}_S$ on $X(S)$. We also write $\underline{M}$ for this sheaf. Then we can consider the cohomology groups

$$H^1(X(S), \underline{M}), \qquad H^1_c(X(S), \underline{M}), \quad \text{and} \quad H^1_P(X(S), \underline{M}),$$

where $H^1_c(X(S), \underline{M})$ is the usual cohomology group of compact support and $H^1_P(X(S), \underline{M})$ is the natural image of $H^1_c(X(S), \underline{M})$ in the usual cohomology group $H^1(X(S), \underline{M})$ (see **[H93b**, Chapter 6]). Then if $S \supset W$ are two open compact subgroups, writing H^1_* for any one of H^1, H^1_c, and H^1_P, we have the restriction map and the trace map [**H93b**, §6.3]:

$$\mathrm{res}_{S/V}: H^1_*(X(S), \underline{M}) \to H^1_*(X(W), \underline{M})$$

and

$$\mathrm{Tr}_{S/V}: H^1_*(X(W), \underline{M}) \to H^1_*(X(S), \underline{M}).$$

Take two open subgroups S and V. Let $W = \alpha S \alpha^{-1} \cap V$, and let $W^\alpha = \alpha^{-1} W \alpha = S \cap \alpha^{-1} V \alpha$ for $\alpha \in \mathrm{GL}_2(\mathbf{A}_f)$. Suppose that M is actually a module over the semigroup generated by α^ι_p, S^ι_p, and V^ι_p in $\mathrm{GL}_2(\mathbf{Q}_p)$. Then we can define a morphism of sheaves $[\alpha]: \underline{M}_W \to \underline{M}_{W^\alpha}$ by $[\alpha](x, m) = (x\alpha, \alpha^\iota_p m)$. It is easy to see that this is well defined. Then by the functoriality of cohomology theory, $[\alpha]$ induces a morphism

$$[\alpha]: H^1_*(X(W), \underline{M}) \to H^1_*(X(W^\alpha), \underline{M}).$$

Then we can define the Hecke operator $[S\alpha V]: H^1_*(X(S), \underline{M}) \to H^1_*(X(V), \underline{M})$ by

$$[S\alpha V] = \mathrm{Tr}_{V/W^\alpha} \circ [\alpha] \circ \mathrm{res}_{S/W}.$$

It is easy to see that the operator $[S\alpha V]$ depends only on the double coset $S\alpha V$ but not on the choice of α. We now apply the above argument to the following modules. Let $\xi: (\mathbf{Z}/p^r\mathbf{Z})^\times \to A^\times$ be a character. Let B be any A-module. Let $M = L(n, v, \xi; B)$ for $(n, v) \in \mathbf{Z}^2$ $(n \geq 0)$ be the A-module of homogeneous polynomials in $B[X, Y]$ of degree n. Here $B[X, Y]$ denotes the polynomial module (in X and Y) with coefficients in B. We let $S(p^r)^\iota_p$ act on $P(X, Y)$ by

$$\text{(S)} \qquad uP(X, Y) = \xi(d)\det(u)^v P((X, Y)^t u^\iota) \quad \text{for } u = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Then we write $\mathcal{L}(n, v, \xi; B)$ for $\underline{M}$. For the semigroup

$$(\Delta) \qquad \Delta = \left\{ \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbf{A}_f) \mid \alpha_p \in M_2(\mathbf{Z}_p), a_p \in \mathbf{Z}_p^\times, c \in p^r\mathbf{Z}_p \right\},$$

we let Δ^ι act on $L(n, v, \xi; A)$ by setting

$$\alpha^\iota P(X, Y) = \xi(a_p)\det(\alpha)^v P((X, Y)^t \alpha^\iota_p).$$

Thus, we have the operator $[S\alpha S]$ for $\alpha \in \Delta$. To the triple (n, v, ξ), we attach a character of the group $\mathbf{Z}_p^\times \times \mathbf{Z}_p^\times$ given by $(w, z) \mapsto w^v z^{n+2v} \xi(z)$. Then it is known that $H^1_P(X(p^r), \mathcal{L}(n, v, \xi; K)) = 0$ if the character attached to (n, v, ξ) does not factor through $\mathbf{G} = \mathbf{Z}_p^\times \times (\mathbf{A}^\times/\mathbf{Q}^\times U^{(p)}\mathbf{R}^\times)$, where we consider $\mathbf{G}$ as a quotient of $\mathbf{Z}_p^\times \times \mathbf{Z}_p^\times$ via the isomorphism $\chi: \mathbf{A}^\times/\mathbf{Q}^\times U^{(p)}\mathbf{R}^\times \cong \mathbf{Z}_p^\times/\{\pm 1\}$ (see (7)). We call a character φ of $\mathbf{G}$ arithmetic if there exist integers $n \geq 0$ and v such that in a small neighborhood of 1 in $\mathbf{G}$, φ coincides with the character: $(w, z) \mapsto w^v z^{n+2v}$.

An arithmetic character φ of $\mathbf{G}$ determines the data (n, v, ξ). Thus, we shall hereafter write $\mathcal{L}(\varphi; B)$ for $\mathcal{L}(n, v, \xi; B)$. Using this action, we define the operator

$$T(z) = z_p^{-v} \left[S \begin{pmatrix} 1 & 0 \\ 0 & z \end{pmatrix} S \right] \qquad (S = U(p^r))(z \in \mathcal{Z} = \mathbf{A}_f^\times \cap \widehat{\mathbf{Z}}).$$

There is another set of operators acting on $H^1_P(X(p^r), \mathcal{L}(\varphi; B))$ for $X(p^r) = X(U(p^r))$. For each $z \in \mathcal{Z}$ with $z_p \in \mathbf{Z}_p^\times$, we can think of the action $\langle z \rangle = \varphi(1, z_p)^{-1}[SzS]$. We have written $T(q)$ (resp., $\langle q \rangle$) as $T_1(q)$ (resp., $T_2(q)$) for primes

q prime to p in paragraph 4 (see (L)). These operators $\{T(n), \langle z \rangle\}$ are mutually commutative and compatible with the restriction map

$$\mathrm{res}_{r,s}: H^1_P(X(p^r), \mathscr{L}(\varphi; B)) \to H^1_P(X(p^s), \mathscr{L}(\varphi; B)) \quad \text{for } s \geq r.$$

Therefore, we have

$$T(z) \circ \mathrm{res}_{r,s} = \mathrm{res}_{r,s} \circ T(z) \quad \text{and} \quad \langle z \rangle \circ \mathrm{res}_{r,s} = \mathrm{res}_{r,s} \circ \langle z \rangle.$$

To define a Hecke algebra, we can take as B either K or K/A. The two choices of B yield the same result. We define the Hecke algebra $\mathbf{h}_\varphi(p^r; A)$ to be the A-subalgebra of the A-linear endomorphism algebra of $H^1_P(X(p^r), \mathscr{L}(\varphi; B))$ ($B = K$ or K/A) generated by $T(z)$ and $\langle z \rangle$ for all $z \in \mathscr{Z}$. The algebra $\mathbf{h}_\varphi(p^r; A)$ is commutative with identity $T(1)$ and is free of finite rank over A. Therefore, it is a compact ring. The restriction of these operators acting on $H^1_P(X(p^s), \mathscr{L}(\varphi; K))$ to $H^1_P(X(p^r), \mathscr{L}(\varphi; K))$ yields an A-algebra homomorphism of $\mathbf{h}_\varphi(p^s; A)$ onto $\mathbf{h}_\varphi(p^r; A)$ for $s > r$. We then take the following two limits

$$\mathscr{V}(B)_{/\mathbf{Q}} = H^1_P(X(p^\infty), \mathscr{L}(\varphi; B)) = \varinjlim_n H^1_P(X(p^n), \mathscr{L}(\varphi; B))$$

and

$$\mathbf{h}_\varphi(p^\infty; A) = \varprojlim_n \mathbf{h}_\varphi(p^n; A).$$

Then the Hecke algebra $\mathbf{h}_\varphi(p^\infty; A)$ is a compact ring and naturally acts on $\mathscr{V}(B)$. In fact, we can define the p-adic topology on $\mathscr{V}(K)$ so that the natural images of $\{p^n \mathscr{V}(A)\}$ form a fundamental system of neighborhoods of 0. Then the Hecke algebra acts on $\mathscr{V}(K)$ via bounded operators. We may take the p-adic completion $\overline{\mathscr{V}}(K)$ of $\mathscr{V}(K)$ as a p-adic analog of the subspace of $L^0_2(\xi)$ (or even the symbolic continuous sum $\int L^0_2(\xi)\, d\xi$) fixed by $U(p^\infty) = \bigcap_r U(p^r)$. The important fact is that the pair

$$(\mathbf{h}_\varphi(p^\infty; A), \{T(z), \langle z \rangle\})$$

is independent of φ. Hence, there exists an isomorphism of $\mathbf{h}_\varphi(p^\infty; A)$ onto $\mathbf{h}_\psi(p^\infty; A)$ for any two arithmetic characters φ and ψ of $\mathbf{G}$ which takes $T(z)$ to $T(z)$ and $\langle z \rangle$ to $\langle z \rangle$ **[H89b]**. Thus, we may write this universal object as $\mathbf{h}_{/\mathbf{Q}} = \mathbf{h}(p^\infty; A)_{/\mathbf{Q}}$. Then the algebro-geometric spectrum Spec($\mathbf{h}$) is a p-adic analog of the complex spectrum of $\int L^0_2(\xi)\, d\xi$. It seems that in the p-adic case the spectrum is large compared to the complex case. We have two continuous characters

$$\langle\ \rangle: \mathbf{A}^\times / U^{(p)} \mathbf{Q}^\times \mathbf{R}^\times_+ = \mathbf{Z}^\times_p / \{\pm 1\} \to \mathbf{h}_{/\mathbf{Q}}: z \mapsto \langle z \rangle$$

and

$$T: \mathbf{Z}^\times_p \to \mathbf{h}_{/\mathbf{Q}}: u \mapsto T(u).$$

This extends to an algebra homomorphism

$$T \times \langle\ \rangle: \mathbf{Z}_p[[\mathbf{G}]] \to \mathbf{h}_{/\mathbf{Q}} \quad (\text{and } T \times \langle\ \rangle: \mathbf{Z}_p[[W \times W]] \to \mathbf{h}_{/\mathbf{Q}}). \tag{10}$$

We thus propose to take the space $\mathrm{Spec}(\mathbf{h})(\overline{\mathbf{Q}}_p) = \mathrm{Hom}_{A\text{-alg}}(\mathbf{h}, \overline{\mathbf{Q}}_p)$ (or its irreducible components) as a natural domain on which modular p-adic L-functions should be defined. As was already seen in §3, the connected and irreducible component of $\mathrm{Spec}(\mathbf{Z}_p[[\mathbf{G}]])$ is given by $\mathrm{Spec}(\mathbf{Z}_p[[W]])$, and $\mathrm{Spec}(\mathbf{Z}_p[[W]])(\overline{\mathbf{Q}}_p)$ is isomorphic to the p-adic open unit disk D (see (8)). Since the morphism (10) induces a covering map $\mathrm{Spec}(\mathbf{h})(\overline{\mathbf{Q}}_p) \to D \times D$, we are tempted to conjecture

CONJECTURE. *The dimension of each irreducible component of* $\mathrm{Spec}(\mathbf{h})(\overline{\mathbf{Q}}_p)$ *as a p-adic space is greater than or equal to 2. Moreover, the natural covering* $\mathrm{Spec}(\mathbf{h}) \to \mathrm{Spec}(\mathbf{Z}_p[[W \times W]])$ *is dominant on each irreducible component.*

Here we implicitly assumed that $\mathbf{h}$ is Noetherian. We will discuss this question later (Corollary 3). The conjecture also implies that the Krull dimension of the coordinate ring of each irreducible component is greater than or equal to 3. Here for the first time we encounter the situation where the dimension of the space on which a p-adic L-function should be defined is larger than 1. We will later see that some irreducible components are finite coverings of $D \times D$, and therefore, have dimension 2 (Theorem 6 and [**H93b**, §7.6]).

We can almost automatically extend the above definition of $\mathbf{h}$ to any number field F. We briefly explain how to define the p-adic Hecke algebra for $\mathrm{GL}(2)_{/F}$. Since $\mathbf{A} = \mathbf{A}_f \times \mathbf{R}$ for $\mathbf{A}_f = \{z \in \mathbf{A} \mid z_\infty = 0\}$, we have $F_{\mathbf{A}} = F_{\mathbf{A}_f} \times F_{\mathbf{R}}$ for $F_{\mathbf{A}_f} = F \otimes_{\mathbf{Q}} \mathbf{A}_f$ and $F_{\mathbf{R}} = F \otimes_{\mathbf{Q}} \mathbf{R}$. Let I be the set of all fields embedding F into $\overline{\mathbf{Q}}$ and fix two embeddings $i_\infty : \overline{\mathbf{Q}} \to \mathbf{C}$ and $i_p : \overline{\mathbf{Q}} \to \overline{\mathbf{Q}}_p$. Let A and K be as above, but we assume that K contains F^σ for all $\sigma \in I$. Let O be the integer ring of F, and set $\mathcal{O}_p = \mathcal{O} \otimes_{\mathbf{Z}} \mathbf{Z}_p$ and $\widehat{\mathcal{O}} = \mathcal{O} \otimes_{\mathbf{Z}} \widehat{\mathbf{Z}}$, which will be regarded as a subring of $F_{\mathbf{A}_f}$. Then we define subgroups $U(p^r)$ of $\mathrm{GL}_2(F_{\mathbf{A}_f})$ in the same way as (9) replacing $\widehat{\mathbf{Z}}$ by $\widehat{\mathcal{O}}$. Similarly, we write C_∞ for the pull-back image of the standard maximal compact subgroup of $\mathrm{PGL}_2(F_{\mathbf{R}})$ in the identity (connected) component $\mathrm{GL}_2^+(F_{\mathbf{R}})$. We define a topological group $\mathbf{G}$ and G by

$$\mathbf{G} = \mathcal{O}_p^\times \times (F_{\mathbf{A}}^\times / \overline{F^\times U^{(p)} F_{\mathbf{R}}^\times}) \supset \mathcal{O}_p^\times \times (\mathcal{O}_p^\times / \overline{\mathcal{O}^\times}) = G,$$

where $U^{(p)} = \{z \in \widehat{\mathcal{O}}^\times \mid z_p = 1\}$. It is easy to see that G is an open compact subgroup of $\mathbf{G}$. A character $\varphi : \mathbf{G} \to K^\times$ is called arithmetic if there exist I-tuples of integers $n = (n_\sigma \geq 0)_{\sigma \in I}$ and $v = (v_\sigma)_{\sigma \in I}$ such that on a small open neighborhood of the identity of G, φ coincides with $(w, z) \mapsto w^v z^{n+2v}$, where $w^v = \prod_{\sigma \in I} w^{\sigma v_\sigma}$. From an arithmetic φ, we recover the data (n, v, ξ) (which we write as $(n(\varphi), v(\varphi), \xi(\varphi))$ if necessary), where ξ is a finite-order character of $\mathcal{O}_p^\times$ given by $\xi(z) = \varphi(1, z) z^{-n-2v}$. For any A-module B, we consider the polynomial module $B[X_\sigma, Y_\sigma]_{\sigma \in I}$ with indeterminate $(X_\sigma, Y_\sigma)_{\sigma \in I}$. We write $L(\varphi; B)$ for the space of polynomials homogeneous in each pair (X_σ, Y_σ) of degree n_σ for the I-tuple $n = n(\varphi)$. If ξ factors through $(\mathcal{O}/p^r\mathcal{O})^\times$, then we get $U(p^r)_p^t$ act on $L(\varphi; B)$ by

$$\text{(U)} \qquad uP(X_\sigma, Y_\sigma) = \xi(d) \det(u)^v P((X_\sigma, Y_\sigma)^t u^\iota) \quad \text{for } u = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

For the semigroup

$$(\Delta) \qquad \Delta = \left\{ \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(F_{\mathbf{A}_f}) \mid \alpha_p \in M_2(O_p), a_p \in \mathcal{O}_p^\times, c \in p^r \mathcal{O}_p \right\},$$

we let Δ^t act on $L(\varphi; B)$ by

$$\alpha^t P(X_\sigma, Y_\sigma) = \xi(a_p) \det(\alpha_p)^v P((X_\sigma, Y_\sigma)^t \alpha_p^\sigma).$$

Then for each r, we can define a sheaf $\mathscr{L}(\varphi; B)$ of locally constant sections of the covering space

$$\mathrm{GL}_2(F)\backslash(\mathrm{GL}_2(F_A) \times L(\varphi; B))/U(p^r)C_\infty$$

over

$$X(p^r) = \mathrm{GL}_2(F)\backslash \mathrm{GL}_2(F_A)/U(p^r)C_\infty.$$

The topological space $X(p^r)$ is a Riemannian manifold of (real) dimension $2r_1 + 3r_2$ if r is sufficiently large, where r_1 (resp., r_2) is the number of real (resp., complex) places of F. We then consider $H^j_P(X(p^r), \mathscr{L}(\varphi; B))$. We can define Hecke operators acting on the cohomology group for $S = U(p^r)$ by

$$T(z) = z_p^{-1}\left[S\begin{pmatrix}1 & 0\\ 0 & z\end{pmatrix}S\right] \quad \text{for } z \in \mathscr{Z} = \hat{\mathscr{O}} \cap F_A^\times,$$

and

$$\langle z\rangle = \varphi(1, z_p)^{-1}[SzS] \quad \text{for } z \in \mathscr{Z} \text{ with } z_p \in \mathscr{O}_p^\times$$

in the same manner as in the case of $F = \mathbf{Q}$. For each prime ideal $\mathscr{P}$ of $\mathscr{O}$ prime to p, we write $T(\mathscr{P})$ (resp., $\langle\mathscr{P}\rangle$) for $T(\varpi)$ for a prime element ϖ of the $\mathscr{P}$-adic completion $\mathscr{O}_\mathscr{P}$ regarded as an element of F_A. The operators $T(\mathscr{P})$ and $\langle\mathscr{P}\rangle$ are well defined independently of the choice of ϖ. We know (see **[Ha87]** and **[H93a]**) that

$$H^j_P(X(S), \mathscr{L}(\varphi; K)) = \{0\} \quad \text{if } n(\varphi) \neq 0 \text{ and } j \notin [r_1 + r_2, r_1 + 2r_2],$$

and for all $j \in [r_1 + r_2, r_1 + 2r_2]$, the A-subalgebras $h_\varphi(p^r; A)_{/F}$ of

$$\mathrm{End}_K(H^j_P(X(p^r), \mathscr{L}(\varphi; K)))$$

generated by all $T(z)$ and $\langle z\rangle$ are canonically isomorphic to each other. Thus, we may concentrate our attention on $H^q_P(X(S), \mathscr{L}(\varphi; B))$ for $q = r_1 + r_2$ when B is a field of characteristic 0. We may also define $\mathbf{h}_\varphi(p^r; A)$ by the A-subalgebra of $\mathrm{End}_K(H^q_P(X(p^r), \mathscr{L}(\varphi; K/A)))$ generated by all $T(z)$ and $\langle z\rangle$. For this algebra, we actually need to consider H^j_P for general j, but for simplicity, we discuss only the qth cohomology group. Since we have a natural map of sheaves $\pi: \mathscr{L}(\varphi; K) \to \mathscr{L}(\varphi; K/A)$, we have an A-algebra homomorphism

$$\rho: \mathbf{h}_\varphi(p^r; A) \to h_\varphi(p^r; A) \quad \text{determined by } h \circ \pi = \pi \circ \rho(h).$$

Naturally ρ takes $T(z)$ and $\langle z\rangle$ to $T(z)$ and $\langle z\rangle$, and hence, ρ is surjective. In the same manner as in the case of $F = \mathbf{Q}$, we have two natural projective systems of triples: $\{h_\varphi(p^r; A), T(z), \langle z\rangle\}_r$ and $\{\mathbf{h}_\varphi(p^r; A), T(z), \langle z\rangle\}_r$. We form the following two limits:

$$\{h_\varphi(p^\infty; A), T(z), \langle z\rangle\} = \varprojlim_n \{h_\varphi(p^n; A), T(z), \langle z\rangle\}$$

and

$$\{\mathbf{h}_\varphi(p^\infty; A), T(z), \langle z\rangle\} = \varprojlim_n \{\mathbf{h}_\varphi(p^n; A), T(z), \langle z\rangle\}.$$

We then ask

QUESTION 1. Is ρ an isomorphism for $r = 1, 2, \ldots, \infty$?

It is known that ρ is an isomorphism when $F = \mathbf{Q}$ because $H^1(X(p^r), K/A)$ is divisible. When F is totally real, it is expected that $\mathrm{Ker}(\rho)$ is small (for example, is torsion or even pseudonull over $\Lambda[[\mathbf{G}]]$), but the pseudonullity is not yet proven. If F has complex places, the answer to Question 1 is known to be negative in some cases. Writing c for complex conjugation, it is known **[Ha87]** that $H_p^1(X(S), \mathscr{L}(\varphi; K)) = \{0\}$ if $n_\sigma \neq n_{\sigma c}$ for some $\sigma \in I$ (see also **[H93a]**). However, there are plenty of examples of nonvanishing of $H_p^1(X(S), \mathscr{L}(\varphi; K/A))$ even if $n \neq 0$ (**[Ta]**, **[H93a]**).

QUESTION 2. Are the algebras $\mathbf{h}_\varphi(p^\infty; A)$ and $h_\varphi(p^\infty; A)$ independent of φ if $n(\varphi) \neq 0$?

When F is totally real, it is seen in **[H89b]** that $h_\varphi(p^\infty; A)$ is independent of φ. There is a partial result of this type for the nearly ordinary part of the ring $\mathbf{h}_\varphi(p^\infty; A)$ valid for arbitrary F (Theorem 4).

QUESTION 3. How many connected components does $\mathrm{Spec}(\mathbf{h}_\varphi(p^\infty; A))$ have?

This can be interpreted as asking: how many congruence classes modulo p are there of the eigenvalues of Hecke operators of p-power level? It is classically known **[Se75]** that there are only finitely many connected components when $F = \mathbf{Q}$, and it is not hard to extend the proof of the finiteness in **[Se75]** to totally real F, because we can now attach a Galois representation to such a system of eigenvalues (**[Ta89]**, **[BR89]**).

We decompose $\mathbf{G} = \mu \times \mathbf{W}$ for a finite group μ and $\mathbf{W}$ isomorphic to $\mathbf{Z}_p^d$ for some $d = d(F) > 0$. We always have $d(F) = [F : \mathbf{Q}] + r_2 + 1 + \delta(p, F)$ for $\delta(p, F) \geq 0$ and $\delta(p, F) = 0$ if the Leopoldt conjecture is true for p and F. Each irreducible component of $\mathrm{Spec}(\Lambda[[\mathbf{G}]])$ is isomorphic to $\mathrm{Spec}(\Lambda[[\mathbf{W}]])$ whose space of $\overline{\mathbf{Q}}_p$-valued points is isomorphic to the product of d copies of the open unit disk: $D \times \cdots \times D$. In particular, the (Krull) dimension of $\Lambda[[\mathbf{W}]]$ is $d + 1$. We have a natural algebra homomorphism

$$T \times (\ ) : \Lambda[[\mathbf{G}]] \to \mathbf{h}_\varphi(p^\infty; A) \quad \text{and} \quad T \times (\ ) : \Lambda[[\mathbf{G}]] \to h_\varphi(p^\infty; A).$$

Thus, $\mathrm{Spec}(\mathbf{h}_\varphi(p^\infty; A))$ and $\mathrm{Spec}(h_\varphi(p^\infty; A))$ are covering spaces of $\mathrm{Spec}(\Lambda[[\mathbf{W}]])$.

QUESTION 4. Are there some irreducible components of $\mathrm{Spec}(h_\varphi(p^\infty; A))$ or $\mathrm{Spec}(\mathbf{h}_\varphi(p^\infty; A))$ that dominate $\mathrm{Spec}(\Lambda[[\mathbf{W}]])$?

When F is totally real, there are such components: the irreducible components of the nearly ordinary part (Theorem 6). When F has some complex places, the answer is probably negative (see Theorem 6 and **[H93a**, Theorem 5.2]).

§7

We now speculate why we expect that $\mathbf{h}_\varphi(p^\infty; A)_{/F}$ is independent of φ (as long as $n(\varphi) \neq 0$), and at the same time we explain how to construct the maximal GL(2)-extension $F_{\mathrm{GL}(2),p}$ unramified outside p which is the GL(2) analog of $\mathbf{Q}_{\mathrm{GL}(1),p} = \mathbf{Q}(1^{1/p^\infty})$. Let $h_\varphi^{(F)}(p^r; A)_{/F}$ $(r = 1, 2, \ldots, \infty)$ be the closed subalgebra of $h_\varphi(p^r; A)_{/F}$ generated over $\Lambda[[\mathbf{W}]]$ by $T(z)$ with $z_p = 1$. It is well known from the theory of primitive (or new) forms (see **[Mi89**, Chapter 4] for $F = \mathbf{Q}$) that $h_\varphi^{(F)}(p^r; A)$ is reduced (i.e., has no nontrivial nilpotent elements). Since $h_\varphi^{(F)}(p^\infty; A)$ is the projective limit of $\{h_\varphi^{(F)}(p^r; A)\}_r$, $h^{(F)} = h_\varphi^{(F)}(p^\infty; A)$ is also reduced. For any profinite local algebra R over $\Lambda[[\mathbf{W}]]$ and an $\Lambda[[\mathbf{W}]]$-algebra homomorphism $\lambda : h_\varphi^{(F)}(p^\infty; A)_{/F} \to R$, a continuous Galois representation $\pi: \mathrm{Gal}(\overline{\mathbf{Q}}/F) \to \mathrm{GL}_2(R)$ is called λ-residual if the following conditions are satisfied:

(R1) π is unramified outside p;

(R2) for the Frobenius element $\mathrm{Frob}_{\mathscr{P}}$ for each prime ideal $\mathscr{P}$ prime to p, we have

$$\det(1_2 - \pi(\mathrm{Frob}_{\mathscr{P}})X) = 1 - \lambda(T(\mathscr{P}))X + N(\mathscr{P})\lambda((\mathscr{P}))X^2.$$

The existence of a λ-residual representation is known, when F is totally real, in the following cases (**[M89]**, **[Gv88]**, **[Wi88]**, **[Ta89]**, **[BR89]**, **[H89c]**, **[HT93b]**, **[H93b, §7.5]**):

(i) R is a field;

(ii) R is an integral domain and for the maximal ideal $\mathfrak{m}$ of R, the ($\lambda \bmod \mathfrak{m}$)-residual representation is irreducible (see Corollary 1 below);

(iii) the ($\lambda \bmod \mathfrak{m}$)-residual representation is absolutely irreducible.

Thus, the points of $\mathrm{Spec}(h^{(p)})$ parametrize residual representations. However, there may be several λ-residual representations for a given point λ. To get objects that are parametrized exactly by points of $\mathrm{Spec}(h^{(p)})$, we introduce the notion of pseudorepresentations first given by Wiles **[Wi88]**. Let $G = G_F$ be the Galois group of the maximal extension of F unramified outside p. Let π be a (continuous) representation of G into $\mathrm{GL}_2(R)$. We assume the existence of an element $c \in G$ of order 2 such that $\det(\pi(c)) = -1$. If F has a real place v, the complex conjugation at v is often taken as c. Then by the assumption that $p > 2$, we may assume that

$$\pi(c) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

For each $\sigma \in G$, we write $\pi(\sigma) = \begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix}$ and define a function $x: G \times G \to R$ by $x(\sigma, \tau) = b(\sigma)c(\tau)$. Then these functions satisfy the following properties:

(PR1) As functions on G or G^2, a, d, and x are continuous,

(PR2) $a(\sigma\tau) = a(\sigma)a(\tau) + x(\sigma, \tau)$, $d(\sigma\tau) = d(\sigma)d(\tau) + x(\tau, \sigma)$, and

$$\begin{aligned} x(\sigma\tau, \rho\gamma) = {} & a(\sigma)a(\gamma)x(\tau, \rho) + a(\gamma)d(\tau)x(\sigma, \rho) \\ & + a(\sigma)d(\rho)x(\tau, \gamma) + d(\tau)d(\rho)x(\sigma, \gamma), \end{aligned}$$

(PR3) $a(1) = d(1) = d(c) = 1$, $a(c) = -1$, and

$$x(\sigma, \rho) = x(\rho, \tau) = 0 \text{ if } \rho = 1 \text{ or } c,$$

(PR4) $x(\sigma, \tau)x(\rho, \eta) = x(\sigma, \eta)x(\rho, \tau)$.

The properties (PR3) and (PR4) follow directly from the definition, and the first half of (PR2) can be proven by computing directly the multiplicative formula

$$\begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix} \begin{pmatrix} a(\tau) & b(\tau) \\ c(\tau) & d(\tau) \end{pmatrix} = \begin{pmatrix} a(\sigma\tau) & b(\sigma\tau) \\ c(\sigma\tau) & d(\sigma\tau) \end{pmatrix}.$$

Then in addition to the first two formulas of (PR2), we also have

$$b(\sigma\tau) = a(\sigma)b(\tau) + b(\sigma)d(\tau) \quad \text{and} \quad c(\sigma\tau) = c(\sigma)a(\tau) + d(\sigma)c(\tau).$$

Thus, we know that

$$\begin{aligned} x(\sigma\tau, \rho\gamma) &= b(\sigma\tau)c(\rho\gamma) = (a(\sigma)b(\tau) + b(\sigma)d(\tau))(c(\rho)a(\gamma) + d(\rho)c(\gamma)) \\ &= a(\sigma)a(\gamma)x(\tau, \rho) + a(\gamma)d(\tau)x(\sigma, \rho) + a(\sigma)d(\rho)x(\tau, \gamma) \\ &\quad + d(\tau)d(\rho)x(\sigma, \gamma). \end{aligned}$$

For any topological algebra R, we now define a *pseudorepresentation* of G into R to be a triple $\pi' = (a, d, x)$ consisting of continuous functions on G and G^2 satisfying the conditions (PR1–4). We define the trace $\mathrm{Tr}(\pi')$ (resp., the determinant $\det(\pi')$) of the pseudorepresentation π' to be a function on G given by

$$\mathrm{Tr}(\pi')(\sigma) = a(\sigma) + d(\sigma) \quad (\text{resp., } \det(\pi')(\sigma) = a(\sigma)d(\sigma) - x(\sigma, \sigma)).$$

Then we have

PROPOSITION 1 (Wiles). *Let $\pi' = (a, d, x)$ be a pseudorepresentation of G into an integral domain R with quotient field Q. Then there exists a continuous representation $\pi: G \to \mathrm{GL}_2(Q)$ with the same trace and determinant as π'.*

Here we only point out how to construct the representation π out of π' (see **[Wi88]**, **[H93b**, §7.5] for a detailed proof). We divide our argument into two cases:

CASE 1. there exist ρ and $\gamma \in G$ such that $x(\rho, \gamma) \neq 0$,
and

CASE 2. $x(\sigma, \tau) = 0$ for all σ, τ in G.

CASE 1. We define $\pi(\sigma) = \begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix}$ by setting

$$c(\sigma) = x(\rho, \sigma) \quad \text{and} \quad b(\sigma) = x(\sigma, \gamma)/x(\rho, \gamma).$$

Then it is easy to check using (PR2, 4) that π actually gives a representation.

CASE 2. In this case, by (PR2) we have $a(\sigma)a(\tau) = a(\sigma\tau)$ and $d(\sigma)d(\tau) = d(\sigma\tau)$ for all $\sigma, \tau \in G$.

Then we simply put $\pi(\sigma) = \begin{pmatrix} a(\sigma) & 0 \\ 0 & d(\sigma) \end{pmatrix}$ which does the job.

The following corollary is obvious from the above explanation.

COROLLARY 1. *Let R be a profinite local $\mathbf{Z}_p$-algebra with maximal ideal $\mathfrak{m}$. Let $\pi' = (a, d, x)$ be a pseudorepresentation of G into R. Suppose there exist $\rho, \gamma \in G$ such that $x(\rho, \gamma) \in R^\times$. Then there exists a continuous representation $\pi: G \to \mathrm{GL}_2(R)$ with the same trace and determinant as π'. In particular, if the Galois representation into $\mathrm{GL}_2(R/\mathfrak{m})$ associated to π' mod $\mathfrak{m}$ exists and is irreducible, then we have a continuous representation $\pi: G \to \mathrm{GL}_2(R)$ with the same trace and determinant as π'.*

We write κ for the residue field of A. We consider the category $\mathscr{C}$ consisting of all profinite local A-algebras with residue field κ. For two maps $\alpha: X \to Z$ and $\beta: Y \to Z$ of sets, their fiber product is defined by $X \times_Z Y = \{(x, y) \in X \times Y \mid \alpha(x) = \beta(y)\}$. For three objects R, R_1, and R_2 in $\mathscr{C}$ and morphisms $\alpha_i: R_i \to R$, there exists a fiber product $R_1 \times_R R_2$ in $\mathscr{C}$ that is given by the set-theoretic fiber product. We write $p_i: R_1 \times_R R_2 \to R_i$ for the projection map. Let $\mathscr{PR}(R)$ be the set of all pseudorepresentations (with respect to c) of G_F having values in the ring R. Then we have a natural map

(11)
$$\gamma\colon \mathcal{PR}(R_1 \times_R R_2) \to \mathcal{PR}(R_1) \times_{\mathcal{PR}(R)} \mathcal{PR}(R_2) \quad \text{given by } \gamma(\pi) = p_1 \circ \pi \times p_2 \circ \pi.$$

PROPOSITION 2.

(i) *The canonical morphism* $\gamma\colon \mathcal{PR}(R_1 \times_R R_2) \to \mathcal{PR}(R_1) \times_{\mathcal{PR}(R)} \mathcal{PR}(R_2)$ *is a bijection.*

(ii) (Wiles) *Let* $\mathfrak{a}$ *and* $\mathfrak{b}$ *be two ideals of* R. *Let* $\pi(\mathfrak{a})$ *and* $\pi(\mathfrak{b})$ *be pseudorepresentations into* $R/\mathfrak{a}$ *and* $R/\mathfrak{b}$, *respectively. Suppose that* $\pi(\mathfrak{a})$ *and* $\pi(\mathfrak{b})$ *are compatible; that is, there exist functions* tr *and* det *on a dense subset* Σ *of* G *with values in* $R/\mathfrak{a} \cap \mathfrak{b}$ *such that for all* $\sigma \in \Sigma$,

$$\mathrm{Tr}(\pi(\mathfrak{a})(\sigma)) \equiv \mathrm{tr}(\sigma) \bmod \mathfrak{a} \quad \textit{and} \quad \mathrm{Tr}(\pi(\mathfrak{b})(\sigma)) \equiv \mathrm{tr}(\sigma) \bmod \mathfrak{b},$$
$$\det(\pi(\mathfrak{a})(\sigma)) \equiv \det(\sigma) \bmod \mathfrak{a} \quad \textit{and} \quad \det(\pi(\mathfrak{b})(\sigma)) \equiv \det(\sigma) \bmod \mathfrak{b}.$$

Then there exists a pseudorepresentation $\pi(\mathfrak{a} \cap \mathfrak{b})$*of* G *into* $R/\mathfrak{a} \cap \mathfrak{b}$ *such that*

$$\mathrm{Tr}(\pi(\mathfrak{a} \cap \mathfrak{b})(\sigma)) = \mathrm{tr}(\sigma) \quad \textit{and} \quad \det(\pi(\mathfrak{a} \cap \mathfrak{b})(\sigma)) = \det(\sigma) \quad \textit{on } \Sigma.$$

PROOF. The first assertion is obvious from the definition. To prove (ii), we consider the exact sequence

$$0 \to R/\mathfrak{a} \cap \mathfrak{b} \to R/\mathfrak{a} \oplus R/\mathfrak{b} \xrightarrow{\alpha} R/\mathfrak{a} + \mathfrak{b} \to 0,$$
$$a \mapsto a \bmod \mathfrak{a} \oplus a \bmod \mathfrak{b}, \qquad a \oplus b \mapsto (a-b) \bmod (\mathfrak{a} + \mathfrak{b}).$$

We consider the pseudorepresentation $\pi = \pi(\mathfrak{a}) \oplus \pi(\mathfrak{b})$ with values in $R/\mathfrak{a} \oplus R/\mathfrak{b}$. The function $\alpha \circ \mathrm{Tr}(\pi)$ vanishes identically on Σ. Since this function is continuous on G and Σ is dense in G, $\alpha \circ \mathrm{Tr}(\pi)$ vanishes on G. Thus, $\mathrm{Tr}(\pi)$ has values in $R/\mathfrak{a} \cap \mathfrak{b}$. If we write $\pi = (a, d, x)$, then

$$a(\sigma) = 2^{-1}(\mathrm{Tr}(\pi(\sigma)) - \mathrm{Tr}(\pi(\sigma c))), \qquad d(\sigma) = 2^{-1}(\mathrm{Tr}(\pi(\sigma)) + \mathrm{Tr}(\pi(\sigma c))),$$

and

$$x(\sigma, \tau) = a(\sigma\tau) - a(\sigma)a(\tau).$$

Thus π itself has values in $R/\mathfrak{a} \cap \mathfrak{b}$ and gives the desired pseudorepresentation. □

A point $\lambda\colon h_{\mathcal{F}}^{(P)}(p^\infty; A) \to \overline{\mathbf{Q}}_p$ of $\mathrm{Spec}(h_{\mathcal{F}}^{(P)}(p^\infty; A))(\overline{\mathbf{Q}}_p)$ is called *algebraic* if it factors through $h_{\mathcal{F}}^{(P)}(p^r; A)$ for some finite r. Then the following theorem follows immediately from Propositions 1 and 2.

THEOREM 1 (WILES **[Wi88]**). *Let* R *be a local ring of* $h_{\mathcal{F}}^{(P)}(p^\infty; A)$. *If a* λ*-residual representation exists for every algebraic* λ *factoring through* R, *then there exist a pseudorepresentation* $\pi'\colon G_F \to R$ *and a continuous representation* $\pi\colon G_F \to \mathrm{GL}_2(Q)$ *such that* $\mathrm{Tr}(\pi(\mathrm{Frob}_{\mathcal{J}})) = \mathrm{Tr}(\pi'(\mathrm{Frob}_{\mathcal{J}})) = T(\mathcal{J})$ *and* $\det(\pi(\mathrm{Frob}_{\mathcal{J}})) = \det(\pi'(\mathrm{Frob}_{\mathcal{J}})) = N(\mathcal{J})(\mathcal{J})$ *for all prime ideals* $\mathcal{J}$ *prime to* p, *where* Q *is the total quotient ring of* R.

PROOF. Since G is unramified outside p, the set Σ of Frobenius elements for primes outside p is dense in G (Tchebotarev density theorem). We set $\mathrm{tr}(\mathrm{Frob}_q) = \lambda(T(q))$ and $\det(\mathrm{Frob}_q) = \chi(q)\kappa(\langle q\rangle)q^{-1}$. Let S be the subset of $\mathrm{Spec}(R)$ consisting of algebraic points. We identify $\lambda \in S$ with the prime ideal $P = \mathrm{Ker}(\lambda)$, i.e., $\lambda\colon R \to R/P$. We number each element of S and write $S = \{P_i\}_{i=1}^\infty$ and π_i for the residual representation attached to P_i. We construct out of each residual representation π_i for $P \in S$, a pseudorepresentation π_i'. Then all the π_i''s are compatible. Then by the above proposition, we can construct a pseudo-representation π' into $R/\bigcap_{j=1}^{i} P_j$ so that

$$\mathrm{Tr}(\pi^{i'}(\sigma)) \equiv \mathrm{Tr}(\pi^{i-1'}(\sigma)) \bmod \bigcap_{j=1}^{i-1} P_j \quad \text{on } \Sigma.$$

Both sides of this congruence are continuous functions, and hence,

$$\mathrm{Tr}(\pi^{i'}(\sigma)) \equiv \mathrm{Tr}(\pi^{i-1'}(\sigma)) \bmod P_1 \cap \cdots \cap P_{i-1} \quad \text{on } G.$$

Note that, by definition, if $\pi^{i'} = (a_i, d_i, x_i)$, then $a_i(\sigma) = \frac{1}{2}(\mathrm{Tr}(\pi^{i'}(\sigma)) - \mathrm{Tr}(\pi^{i'}(\sigma c)))$, $d_i(\sigma) = \frac{1}{2}(\mathrm{Tr}(\pi^{i'}(\sigma)) + \mathrm{Tr}(\pi^{i'}(\sigma c)))$, and $x_i(\sigma, \tau) = a_i(\sigma\tau) - a_i(\sigma)a_i(\tau)$. Therefore, we have

$$a_i(\sigma) \equiv a_{i-1}(\sigma) \bmod P_1 \cap \cdots \cap P_{i-1}, \qquad d_i(\sigma) \equiv d_{i-1}(\sigma) \bmod P_1 \cap \cdots \cap P_{i-1}$$

and

$$x_i(\sigma, \tau) \equiv x_{i-1}(\sigma, \tau) \bmod P_1 \cap \cdots \cap P_{i-1}.$$

Thus, we can define a pseudorepresentation π' into $R = \varprojlim_i R/P_1 \cap \cdots \cap P_i$ by

$$\pi'(\sigma) = \varprojlim_i \pi^{i'}(\sigma).$$

Then we can construct the representation π out of π' by Proposition 1, because we already know that Q is a direct sum of fields (i.e., R is reduced). □

For any given continuous pseudorepresentation $\pi' \colon G_F \to R$ for a profinite algebra R over $\mathbf{Z}_p$, there exists the largest closed normal subgroup $H(\pi')$ among closed normal subgroups H such that π' factors through G/H. In fact, $H(\pi')$ is the maximal closed normal subgroup in $\{\sigma \in G \mid \pi'(\sigma\eta) = \pi'(\sigma) = \pi'(\eta\sigma)$ for all $\sigma \in G\}$. If R is an integral domain and if there exists an absolutely irreducible Galois representation π attached to π', then $\mathrm{Ker}(\pi') = \mathrm{Ker}(\pi)$, because the isomorphism class of such representations over the quotient field of R is unique. Theorem 1 shows the existence of a big pseudorepresentation $\pi' \colon G_F \to h_{\mathscr{I}}^{[P]}(p^\infty; A)$ such that $\mathrm{Tr}(\pi'(\mathrm{Frob}_{\mathscr{J}})) = T(\mathscr{J})$ and $\det(\pi'(\mathrm{Frob}_{\mathscr{J}})) = N(\mathscr{J})\langle\mathscr{J}\rangle$ *for all prime ideals* $\mathscr{J}$ *prime to* p, as long as there exist pseudorepresentations attached to algebraic points of $\mathrm{Spec}(h_{\mathscr{I}}^{[P]}(p^\infty; A))$. We write $F_{\mathrm{GL}(2),p}^{\mathrm{mod}}$ for the fixed field of $H(\pi')$ for the pseudorepresentation $\pi' \colon G_F \to h_{\mathscr{I}}^{[P]}(p^\infty; A)$ if π' exists. This is one of the candidates for the maximal p-ramified GL(2)-extension. For each homomorphism $\lambda \colon h_{\mathscr{I}}^{[P]}(p^\infty; A) \to R$ of profinite A-algebras, we call a pseudorepresentation $\pi_\lambda \colon G_F \to R$ λ*-residual* if $\mathrm{Tr}(\pi_\lambda(\mathrm{Frob}_{\mathscr{J}})) = \lambda(T(\mathscr{J}))$ for all primes $\mathscr{J}$ prime to p.

To describe a more theoretical candidate for $F_{\mathrm{GL}(2),p}$ found by Mazur **[M89]**, we assume the existence of a $\bar{\lambda}$-residual pseudorepresentation $\bar{\pi}$ for an algebra homomorphism $\bar{\lambda} \colon h_{\mathscr{I}}^{[P]}(p^\infty; A) \to \kappa$. In **[M89]**, Mazur studied the universal deformation of each $\overline{\lambda}$-residual representation. Following his argument, we study here the universal deformation of each $\overline{\lambda}$-residual pseudorepresentation. We consider the functor

$$\mathcal{PR}_{\overline{\pi}}: \mathcal{C} \to \mathcal{S}ets \quad \text{given by } \mathcal{PR}_{\overline{\pi}}(R) = \{\pi \in \mathcal{PR}(R) \mid \pi \bmod \mathfrak{m}_R = \overline{\pi}\},$$

where $\mathfrak{m}_R$ is the maximal ideal of R and $(\pi \bmod \mathfrak{m}_R) = (a', d', x')$ given by $a'(\sigma) = a(\sigma) \bmod \mathfrak{m}_R$, $d'(\sigma) = d(\sigma) \bmod \mathfrak{m}_R$, $x'(\sigma,\tau) = x(\sigma,\tau) \bmod \mathfrak{m}_R$ for $\pi = (a, d, x)$. Then we have

THEOREM 2. *The functor $\mathcal{PR}_{\overline{\pi}}$ is representable in $\mathcal{C}$. That is, there exists a unique pair (R^{pr}, π^{pr}) (up to isomorphisms) consisting of a Noetherian profinite A-algebra R^{pr} and a pseudorepresentation $\pi^{pr}: G_F \to R^{pr}$ such that*

$$\mathrm{Hom}_{\mathcal{C}}(R^{pr}, R) \ni \varphi \mapsto \varphi \circ \pi^{pr} \in \mathcal{PR}_{\overline{\pi}}(R)$$

induces an isomorphism $\mathrm{Hom}_{\mathcal{C}}(R^{pr}, R) \cong \mathcal{PR}_{\overline{\pi}}(R)$ for all objects R of $\mathcal{C}$.

PROOF. Let $\mathcal{C}_0$ be the category of Artinian local A-algebras with residue field κ. We only need to show the prorepresentability of $\mathcal{PR}_{\overline{\pi}}$ restricted to $\mathcal{C}_0$. Let $\alpha_i: R_i \to R$ $(i = 1, 2)$ be morphisms in $\mathcal{C}_0$, and let $\gamma: \mathcal{PR}_{\overline{\pi}}(R_1 \times_R R_2) \to \mathcal{PR}_{\overline{\pi}}(R_1) \times_{\mathcal{PR}_{\overline{\pi}}(R)} \mathcal{PR}_{\overline{\pi}}(R_2)$ be the natural map as in (11). To show the representability by a Noetherian ring in $\mathcal{C}$ of the covariant functor $\mathcal{PR}_{\overline{\pi}}$, we need to check the four criteria of Schlessinger **[Sch68]**. However, the three criteria denoted as (H_1), (H_2), and (H_4) in **[Sch68]** automatically follow from Proposition 2(i). The remaining criterion (H_3) follows immediately from

$$\text{(F)} \qquad \mathcal{PR}_{\overline{\pi}}(\kappa[T]/(T^2)) \quad \text{is a finite set.}$$

We now prove (F). We write $\kappa[T]/(T^2)$ as $\kappa[\varepsilon]$ with $\varepsilon^2 = 0$ (i.e., ε is the image of T). Write $\overline{\pi} = (\overline{a}, \overline{d}, \overline{x})$, and take $\pi = (a, d, x) \in \mathcal{PR}_{\overline{\pi}}(\kappa[\varepsilon])$. If there exist $\rho, \eta \in G_F$ such that $\overline{x}(\rho,\eta) \neq 0$, then one defines a representation $\varphi: G_F \to GL_2(\kappa)$ as in Proposition 1 using $\overline{x}(\rho,\eta)$. If there are no $\rho, \eta \in G_F$ as above, we set $\varphi(\sigma) = \left(\begin{smallmatrix} \overline{a}(\sigma) & 0 \\ 0 & \overline{d}(\sigma) \end{smallmatrix}\right)$. Set $H = \mathrm{Ker}(\varphi)$. If $\sigma \in H$, $\varphi(\sigma) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, and therefore, $\overline{x}(\sigma,\eta) = \overline{x}(\rho,\sigma) = 0$ for all $\sigma \in H$. For all $\tau \in G$, we have by (PR4) that $\overline{x}(\sigma,\tau)\overline{x}(\rho,\eta) = \overline{x}(\sigma,\eta)\overline{x}(\rho,\tau) = 0$. This shows $\overline{x}(\sigma,\tau) = 0$ for all $\sigma \in H$ because $\overline{x}(\rho,\eta) \neq 0$. From $\overline{x}(\tau,\sigma)\overline{x}(\rho,\eta) = \overline{x}(\tau,\eta)\overline{x}(\rho,\sigma) = 0$, we conclude

$$\text{(12a)} \qquad \overline{x}(\sigma,\tau) = \overline{x}(\tau,\sigma) = 0 \quad \text{for all } \tau \in G \text{ and } \sigma \in H.$$

We also have

$$\text{(12b)} \qquad \overline{a}(\sigma) = \overline{d}(\sigma) = 1 \quad \text{if } \sigma \in H.$$

Then by (PR2), we have

$$\begin{aligned} x(\sigma\tau, \delta\gamma) &= a(\sigma)a(\gamma)x(\tau,\delta) + a(\gamma)d(\tau)x(\sigma,\delta) \\ \text{(12c)} \qquad &+ a(\sigma)d(\delta)x(\tau,\gamma) + d(\tau)d(\delta)x(\sigma,\gamma). \end{aligned}$$

We see, observing $x(1,*) = x(*,1) = 0$, that

$$x(\sigma, \delta\gamma) = a(\gamma)x(\sigma,\delta) + d(\delta)x(\sigma,\gamma) \qquad (\tau = 1 \text{ in (12c)}),$$

$$x(\sigma\tau, \delta) = a(\sigma)x(\tau,\delta) + d(\tau)x(\sigma,\delta) \qquad (\gamma = 1 \text{ in (12c)}).$$

Therefore by (12a, b, c), we have, writing $a = \overline{a} \oplus a'\varepsilon$, $d = \overline{d} \oplus d'\varepsilon$, and $x = \overline{x} \oplus x'\varepsilon$,

$$x'(\sigma, \delta\gamma) = x'(\sigma, \delta) + x'(\sigma, \gamma) \quad \text{if } \delta, \gamma \in H \text{ and } \sigma \in G,$$
$$x'(\sigma\tau, \delta) = x'(\sigma, \delta) + x'(\tau, \delta) \quad \text{if } \sigma, \tau \in H \text{ and } \delta \in G.$$

Therefore, for each $\sigma \in G$ the maps ${}_\sigma x \colon H \ni \delta \mapsto x'(\sigma, \delta) \in \kappa$ and $x_\sigma \colon H \ni \delta \mapsto x'(\delta, \sigma) \in \kappa$ are homomorphisms of groups. Thus, if we write H' for the closed subgroup of H topologically generated by $H^p(H, H)$, then $\#(H/H') < +\infty$ by class field theory, and $x'(\sigma, \tau) = 0$ for all $\sigma, \tau \in H'$. By (12a),

(12d) $\quad x(\sigma, \tau) = 0 \quad$ and $\quad x(\delta\sigma, \gamma\tau) = a(\tau)d(\sigma)x(\delta, \gamma) \quad$ for all $\sigma, \tau \in H'$.

Then by (12d) and (PR2), we see that

(12e) $\quad a'(\sigma\tau) = a'(\sigma) + a'(\tau), \qquad d'(\sigma\tau) = d'(\sigma) + d'(\tau) \quad$ for all $\sigma, \tau \in H'$.

Let H'' be the subgroup of H' topologically generated by $H'^p(H', H')$. Then again, we have $\#(H/H'') < +\infty$ and

(12f) $$a'(H'') = 0 \quad \text{and} \quad d'(H'') = 0.$$

Then we have

(12g) $\quad a(\gamma\sigma) = a(\gamma), \qquad d(\gamma\sigma) = d(\gamma), \quad$ and $\quad x(\delta\sigma, \gamma\tau) = x(\delta, \gamma) \quad$ if $\sigma, \tau \in H''$.

Note that H'' does not depend on the choice of π. Therefore, all the elements of $\mathcal{PR}_{\overline{\pi}}(\kappa[\varepsilon])$ are functions of the finite group G/H'', and thus, $\#(\mathcal{PR}_{\overline{\pi}}(\kappa[\varepsilon])) < +\infty$. □

PROPOSITION 3. *R^{pr} is generated by* $\mathrm{Tr}(\pi^{\mathrm{pr}})(G_F)$ *over A.*

PROOF. Let R_{tr} be the A-subalgebra topologically generated by $\mathrm{Tr}(\pi^{\mathrm{pr}}(G_F))$. Since π^{pr} is determined by its trace, π^{pr} has values in R_{tr}. Therefore, we have a deformation $(R_{\mathrm{tr}}, \pi^{\mathrm{pr}})$. For each deformation (A, π) of $(\kappa, \overline{\pi})$, we have a morphism $\varphi_\pi \colon R_{\mathrm{tr}} \to A$ such that $\pi = \varphi_\pi \circ \pi^{\mathrm{pr}}$. The morphism φ_π is unique because R_{tr} is generated by the traces. Therefore, $(R_{\mathrm{tr}}, \pi^{\mathrm{pr}})$ is already universal and hence $R^{\mathrm{pr}} = R_{\mathrm{tr}}$. □

Let $\overline{\rho}$ be a $\overline{\lambda}$-residual representation. In [M89], Mazur considered instead of $\mathcal{PR}_{\overline{\pi}}$ the following functor

$$\mathcal{R}_{\overline{\rho}}(R) = \{\rho \colon G \to \mathrm{GL}_2(R) \mid \rho \bmod \mathfrak{m}_R = \overline{\rho}\}/\approx,$$

where ρ is assumed to be a continuous homomorphism and $\rho \approx \rho'$ if there exists a matrix $\alpha \in \mathrm{GL}_2(R)$ with $\alpha \equiv \left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right) \bmod \mathfrak{m}_R$ such that $\rho(\sigma) = \alpha\rho'(\sigma)\alpha^{-1}$ for all $\sigma \in G$. Then Mazur proved

THEOREM 3 (Mazur). *If $\overline{\rho}$ is absolutely irreducible, then $\mathcal{R}_{\overline{\rho}}$ is representable by a unique pair $(R^{\mathrm{rep}}, \rho^{\mathrm{rep}})$ up to isomorphisms for a Noetherian local ring R^{rep} in $\mathcal{C}$ and $\rho^{\mathrm{rep}} \in \mathcal{R}_{\overline{\rho}}(R^{\mathrm{rep}})$.*

It is easy to show

COROLLARY 2. *Let $\overline{\pi}$ be the pseudorepresentation attached to $\overline{\rho}$. Then R^{pr} is canonically isomorphic to the subalgebra of R^{rep} topologically generated by traces of ρ^{rep} over A.*

Assuming that there are only finitely many connected components of $h_\chi^{\mathrm{ord}}(p^\infty; A)$ and that Questions 1 and 2 have affirmative answers, we write $\mathbf{h}$ (resp., $\mathbf{h}^{(p)}$) for

$h_\varphi(p^\infty; A)$ (resp., $h_\varphi^{\mathscr{L}}(p^\infty; A)$). We further assume, extending by scalar if necessary, that all the local rings of $\mathbf{h}^{(p)}$ have κ as their residue field. We further assume that there exists a pseudorepresentation $\pi\colon G_F \to \mathbf{h}$ such that $\mathrm{Tr}(\pi)(\mathrm{Frob}_{\mathscr{L}}) = T(\mathscr{L})$ for all primes $\mathscr{L}$ prime to p. Let π_0 be the set of local rings of $\mathbf{h}^{(p)}$ (= the set of connected components of $\mathrm{Spec}(\mathbf{h}^{(p)})$). For each $S \in \pi_0$, we have a pseudorepresentation $\overline{\pi}_S = \pi \bmod \mathfrak{m}_S$. To $\overline{\pi}_S$ we can attach, by Theorem 2, the universal deformation $(R_S^{\mathrm{ps}}, \pi_S^{\mathrm{ps}})$. Let π_S be the projected image of π to S. Then (S, π_S) is a deformation of $\overline{\pi}_S$, and hence, there exists a natural ring homomorphism $\varphi_S\colon R_S^{\mathrm{ps}} \to S$ satisfying $\varphi_S \circ \pi_S^{\mathrm{ps}} = \pi_S$. We set $\mathbf{H} = \bigoplus_{S \in \pi_0} R_S^{\mathrm{ps}}$. Then we have a surjective ring homomorphism $\Phi\colon \mathbf{H} \to \mathbf{h}^{(p)}$. Then by Proposition 3, the following fact is clear:

Corollary 3. *The ring homomorphism $\Phi\colon \mathbf{H} \to \mathbf{h}^{(p)}$ is surjective, and hence, $\mathbf{h}^{(p)}$ is Noetherian. The algebra $\mathbf{h}$ is generated topologically over $\mathbf{h}^{(p)}$ by $T(\varpi_{\mathfrak{p}})$ for all prime ideals $\mathfrak{p}$ above p in F, and hence, is Noetherian, where $\varpi_{\mathfrak{p}}$ is a prime element in $F_{\mathfrak{p}}$.*

Then we ask in the spirit of **[M89]** and **[MT90]**

Question 5. Is Φ injective?

We can think of the field $F_{\mathrm{GL}(2),p}$ fixed by $\mathrm{Ker}(\bigoplus_S \pi_S^{\mathrm{ps}})$, which is an extension of $F^{\mathrm{mod}}_{\mathrm{GL}(2),p}$. Then Question 5 is just asking whether or not $F^{\mathrm{mod}}_{\mathrm{GL}(2),p} = F_{\mathrm{GL}(2),p}$.

§8

In the discussion of the previous paragraph, we only used the Hecke operators $T(z)$ with $z_p = 1$. The existence of $T(p)$ in $\mathbf{h}_\varphi(p^\infty; A)$ plays a key role in the definition of the ordinary part of $\mathbf{h}_\varphi(p^\infty; A)$, which is the most manageable part of the algebra. Since $\mathbf{h}_\varphi(p^\infty; A)$ is a profinite algebra, we can find two idempotents e_h and $e^h = 1 - e_h$ in $\mathbf{h}_\varphi(p^\infty; A)$ for any given element h in $\mathbf{h}_\varphi(p^\infty; A)$ such that $e_h h \in (e_h\mathbf{h}_\varphi(p^\infty; A))^\times$ and $\lim_{n\to\infty}(e^h h)^n = 0$ (see **[H89a**, §4] and **[H93b**, §7.2]). We apply this argument to $h = T(p)$. We write $e = e_{T(p)}$ and put $\mathbf{h}_\varphi^{n.\mathrm{ord}} = \mathbf{h}_\varphi^{n.\mathrm{ord}}(p^\infty; A) = e\mathbf{h}_\varphi(p^\infty; A)$. Similarly, we define $h_\varphi^{n.\mathrm{ord}} = h_\varphi^{n.\mathrm{ord}}(p^\infty; A)$ out of $h_\varphi(p^\infty; A)$ and $T(p)$. We write again $T(z)$ and $\langle z\rangle \in \mathbf{h}_\varphi^{n.\mathrm{ord}}$ for $eT(z)$ and $e\langle z\rangle$. Then we can prove **[H93a]**, **[H94b]**:

Theorem 4. *The triple $\{\mathbf{h}_\varphi^{n.\mathrm{ord}}(p^\infty; A)_{/F}, (T(z), \langle z\rangle)_{z\in\mathscr{Z}}\}$ is independent of φ (as long as $n(\varphi) \neq 0$). The same assertion holds for $\{h_\varphi^{n.\mathrm{ord}}(p^\infty; A)_{/F}, (T(z), \langle z\rangle)\}$ if F is totally real.*

We write $(\mathbf{h}^{n.\mathrm{ord}}_{/F}, T(z), \langle z\rangle)$ (resp., $(h^{n.\mathrm{ord}}_{/F}, T(z), \langle z\rangle)$) for the universal triple $(\mathbf{h}_\varphi^{n.\mathrm{ord}}(p^\infty; A)_{/F}, T(z), \langle z\rangle)$ (resp., $(h_\varphi^{n.\mathrm{ord}}(p^\infty; A)_{/F}, T(z), \langle z\rangle)$ when F is totally real). A point $P \in \mathrm{Hom}_{A\text{-alg}}(\mathbf{h}^{n.\mathrm{ord}}, \overline{\mathbf{Q}}_p) = \mathrm{Spec}(h^{n.\mathrm{ord}})(\overline{\mathbf{Q}}_p)$ is called *arithmetic* if the composition $\varphi(P) = P \circ (T \times \langle\ \rangle)\colon \mathbf{G} \to \overline{\mathbf{Q}}_p$ is arithmetic. Of course, $\varphi(P)$ may be different from φ. We write $r(P) = r(\varphi(P))$, $n(P) = n(\varphi(P))$, and $v(P) = v(\varphi(P))$. Then

Theorem 5. *Each arithmetic point $P \in \mathrm{Spec}(\mathbf{h}^{n.\mathrm{ord}})(\overline{\mathbf{Q}}_p)$ factors through $h_{\varphi(P)}^{n.\mathrm{ord}}(p^\infty; A)$. For each arithmetic point $P \in \mathrm{Hom}_{A\text{-alg}}(\mathbf{h}^{n.\mathrm{ord}}, \overline{\mathbf{Q}}_p)$, we have $P(T(\mathscr{L})) \in \overline{\mathbf{Q}}$ and $P(\langle\mathscr{L}\rangle) \in \overline{\mathbf{Q}}$ for all prime ideals $\mathscr{L}$ prime to p, and there exist a Hecke* *character ξ whose infinity type is given by $n(P) + 2v(P)$ and a unique algebraic cuspidal automorphic representation $\pi(P)$ occurring in $L_2^0(\xi)$ such that $\pi(P) = \otimes_{\mathscr{J}} \pi_{\mathscr{J}}(P)$ and*

$$L(s, \pi_{\mathscr{J}}(P))^{-1} = 1 - P(T(\mathscr{J}))N(\mathscr{J})^{-s} + P(\langle\mathscr{J}\rangle)N(\mathscr{J})^{1-2s} \quad \textit{for all } \mathscr{J} \textit{ prime to } p.$$

When F is totally real, the above two theorems are proven in **[H89b**, 2.5] (see also **[H89a**, §4] and **[H93b**, §7.3]). In general, the results follow from the main result in **[H93a]** (see **[H94b]** for the proof).

Let $L(s, \pi(P))$ be the standard L-function of $\pi(P)$ introduced in §3. Let $\pi(P)^\vee$ be the contragredient representation of $\pi(P)$. For two arithmetic points P and Q, we consider the external tensor product representation $\pi(P) \times \pi(Q)^\vee$ of $GL_2(F_A) \times GL_2(F_A)$. We write $L(s, \pi(P) \times \pi(Q)^\vee)$ for the standard L-function of $\pi(R) \times \pi(Q)^\vee$ **[H91a]**. Writing

$$L(s, \pi_{\mathscr{J}}(P)) = \{(1 - \alpha N(\mathscr{J})^{-s})(1 - \beta N(\mathscr{J})^{-s})\}^{-1}$$

and

$$L(s, \pi_{\mathscr{J}}(Q)^\vee) = \{(1 - \alpha' N(\mathscr{J})^{-s})(1 - \beta' N(\mathscr{J})^{-s})\}^{-1},$$

we have the following local Euler factor:

$$\begin{aligned} &L(s, \pi_{\mathscr{J}}(P) \times \pi_{\mathscr{J}}(Q)^\vee) \\ &\quad = \{(1 - \alpha\alpha' N(\mathscr{J})^{-s})(1 - \alpha\beta' N(\mathscr{J})^{-s})(1 - \beta\alpha' N(\mathscr{J})^{-s})(1 - \beta\beta' N(\mathscr{J})^{-s})\}^{-1}. \end{aligned}$$

Write $L(s)$ for one of the above L-functions and $L_\infty(s)$ for the Γ-factor of $L(s)$. We suppose that the functional equation of $L(s)$ is given by $s \mapsto w + 1 - s$. Then w is an integer. We call $L(1)$ critical if $L_\infty(s)$ is finite at $s = 1$ and $s = w$. We call $\pi(P)$ (resp., $\pi(P) \times \pi(Q)^\vee$) critical, if $L(1, \pi(P))$ (resp., $L(1, \pi(P) \times \pi(Q)^\vee)$) is critical. Note that our automorphic representations $\pi(P)$ and $\pi(Q)$ are algebraic. Thus, there should exist corresponding motives $M(P)$ and $M(Q)$ (see **[BR93]**). If $\pi(P)$ (resp., $\pi(P) \times \pi(Q)^\vee$) is critical, then $M(P)(1)$ (resp., $M(P) \otimes M(Q)^\vee(1)$) is critical in the sense of Deligne **[D79]**, where $M(Q)^\vee$ is the dual of $M(Q)$. Thus, we have well-defined motivic periods $c^+(M(P)(1))$ and $c^+(M(P) \otimes M(Q)^\vee(1))$, which are nonzero complex numbers. We write $c^+(P)$ (resp., $c^+(P, Q)$) for the identity component of $c^+(M(P)(1))$ (resp., $c^+(M(P) \otimes M(Q)^\vee(1))$. Then the algebraicity conjecture [D] tells us

$$\frac{L(1, \pi(P))}{c^+(P)} \in \mathbf{Q}(\pi(P)) \quad \text{and} \quad \frac{L(1, \pi(P) \times \pi(Q)^\vee)}{c^+(P, Q)} \in \mathbf{Q}(\pi(P) \otimes \pi(Q)^\vee),$$

where $\mathbf{Q}(\pi(P))$ (resp., $\mathbf{Q}(\pi(P) \otimes \pi(Q)^\vee)$ is the number field generated by $P(T(\mathscr{J}))$ (resp., $P(T(\mathscr{J}))$ and $Q(T(\mathscr{J}))$) for all $\mathscr{J}$ prime to p (which is the field of definition of the finite part of $\pi(P)$ (resp., $\pi(P) \otimes \pi(Q)^\vee$).

If an element L of the total quotient ring of $\mathbf{h}^{n.\mathrm{ord}}$ (resp., $\mathbf{h}^{n.\mathrm{ord}} \widehat{\otimes}_A \mathbf{h}^{n.\mathrm{ord}}$) is given, then we can think of L as a (p-adic meromorphic) function on $\mathrm{Spec}(\mathbf{h}^{n.\mathrm{ord}})(\overline{\mathbf{Q}}_p)$ (resp., $\mathrm{Spec}(\mathbf{h}^{n.\mathrm{ord}}) \times \mathrm{Spec}(\mathbf{h}^{n.\mathrm{ord}})(\overline{\mathbf{Q}}_p)$) by $L(P) = P(L)$ (resp., $L(P, Q) = P \widehat{\otimes} Q(L)$) as long as the value is well defined. Here we have regarded $P : \mathbf{h}^{n.\mathrm{ord}} \to \overline{\mathbf{Q}}_p$ (resp., $P \widehat{\otimes} Q : \mathbf{h}^{n.\mathrm{ord}} \widehat{\otimes}_A \mathbf{h}^{n.\mathrm{ord}} \to \overline{\mathbf{Q}}_p$) as an A-algebra homomorphism, and if sL for $s \in \mathbf{h}^{n.\mathrm{ord}}$ (resp., $s \in \mathbf{h}^{n.\mathrm{ord}} \widehat{\otimes}_A \mathbf{h}^{n.\mathrm{ord}}$) is in $\mathbf{h}^{n.\mathrm{ord}}$ (resp., $\mathbf{h}^{n.\mathrm{ord}} \widehat{\otimes}_A \mathbf{h}^{n.\mathrm{ord}}$) and $P(s) \neq 0$ (resp.,

$P\hat{\otimes}Q(s)\neq 0$), then $P(L)=P(sL)/P(s)$ (resp., $P\hat{\otimes}Q(L)=(P\hat{\otimes}Q(sL))/(P\hat{\otimes}Q(s))$). Then we can ask

QUESTION 6. Can we find a p-adic meromorphic function $L_p(P)$ (resp., $L_p(P,Q)$) on $\mathrm{Spec}(\mathbf{h}^{n.\mathrm{ord}})(\overline{\mathbf{Q}}_p)$ (resp., $\mathrm{Spec}(\mathbf{h}^{n.\mathrm{ord}}\hat{\otimes}_A\mathbf{h}^{n.\mathrm{ord}})(\overline{\mathbf{Q}}_p)$) interpolating the values $L(1,\pi(P))/c^+(P)\in\mathbf{Q}(\pi(P))$ (resp., $L(1,\pi(P)\times\pi(Q)^\vee)/c^+(P,Q)\in\mathbf{Q}(\pi(P)\otimes\pi(Q)^\vee)$) as long as $\pi(P)$ (resp., $\pi(P)\times\pi(Q)^\vee$) is critical.

When F is totally real, the algebraicity conjecture is known for $L(1,\pi(P))$ by Mazur and Manin (see [**H93b**, §6.4]) and also by Shimura [**Sh88**, 90] and for $L(1,\pi(P)\times\pi(Q)^\vee)$ by Shimura [**Sh88**] (see also [**H93b**, §10.4]). When F has complex places, an approximation of the algebraicity conjecture for $L(s,\pi(P))$ is known ([**H94a**]). When F contains CM-fields, a partial result is given for the algebraicity conjecture for $L(1,\pi(P)\times\pi(Q)^\vee)$ in [**H94a**]. When $F\neq\mathbf{Q}$, the transcendental factors vary depending on $n(P)$ and $v(P)$ for $L(1,\pi(P))$ and on $n(P)$, $n(Q)$, $v(P)$, and $v(Q)$ for $L(1,\pi(P)\times\pi(Q)^\vee)$ (cf. [**Sh88**], [**H94a**])). Thus, when $F\neq\mathbf{Q}$, there might be several p-adic L-functions interpolating different combinations of special values. In any case, the answer to the above question is affirmative when $F=\mathbf{Q}$ ([**Ki91**], [**GS92**], and [**H93b**, §§7.4 and 10.4]). When F is totally real, the answer is known, so far, to be partially affirmative [**H91**]. We can ask similar questions for various Langlands L-functions of the polynomial representations of the L-group of $\mathrm{GL}(2)_{/F}$. For example, the adjoint lift p-adic L-function exists on $\mathrm{Spec}(\mathbf{h}^{n.\mathrm{ord}}_{/\mathbf{Q}})$ [**H90a**].

As for Question 4, we have the following partial answer.

THEOREM 6. *The algebra $\mathbf{h}^{n.\mathrm{ord}}$ is of finite type over $A[[\mathbf{W}]]$. If F is totally real and $h^{n.\mathrm{ord}}\neq 0$, then $h^{n.\mathrm{ord}}$ is a torsion-free $A[[\mathbf{W}]]$-module. In particular, in this case the natural map $\mathrm{Spec}(h^{n.\mathrm{ord}})\to\mathrm{Spec}(A[[\mathbf{W}]])$ is dominant. If F has some complex places, then the image of $\mathrm{Spec}(h^{n.\mathrm{ord}})$ is contained in a proper closed subscheme of $\mathrm{Spec}(A[[\mathbf{W}]])$.*

The above fact is proven in [**H89b**] for totally real fields F. Thus, the p-adic space attached to each irreducible component of $h^{n.\mathrm{ord}}$ has dimension equal to $[F:\mathbf{Q}]+1+\delta(p,F)$, which grows at least linearly with respect to the degree $[F:\mathbf{Q}]$. For general number fields, it follows from the main result of [**H93a**] (see [**H94b**] for the proof). Thus, we may ask

QUESTION 7. Characterize the image of $\mathrm{Spec}(h^{n.\mathrm{ord}})$ in $\mathrm{Spec}(A[[\mathbf{W}]])$.

If F is totally real and if the Leopoldt conjecture is true for F and p, the dimension of the scheme $\mathrm{Spec}(h^{n.\mathrm{ord}})\times_{\mathbf{Z}_p}\mathbf{Q}_p$ is $[F:\mathbf{Q}]+1$. In particular, it is equal to 2 when $F=\mathbf{Q}$. This value coincides with the dimension of the continuous spectrum in the complex case. We may thus ask

QUESTION 8. Is the dimension (over $\mathbf{Q}_p$) of the irreducible components of the p-adic nearly ordinary Hecke algebra for $\mathrm{GL}(n)_{/\mathbf{Q}}$ (suitably defined) equal to the maximum of the dimension of the continuous complex spectrum for $\mathrm{GL}(n)_{/\mathbf{Q}}$ (which is equal to n)?

It is quite plausible that the dimension is less than or equal to n. However, there is no compelling reason to expect that the answer is exactly n. The final point we would like to make explicit is

Question 9. What kind of arithmetic of $F^{\mathrm{mod}}_{\mathrm{GL}(2),p}$ do the above p-adic L-functions describe?

For the connected component of $\mathrm{Spec}(h^{n.\mathrm{ord}})$ corresponding to the representation of Weil type (§6), there might be some chance to relate these p-adic L-functions to a certain main conjecture of the Iwasawa theory. Partial results are obtained in this direction when F is totally real (**[MT90]**, **[Ti89]**, **[HT91]**, **[HT93a, b]**). When the representation attached to the connected component is not of Weil type, there are some speculations but their meaning is not yet clear **[MT90]**.

References

[BR89] D. Blasius and J. D. Rogawski, *Galois representations for Hilbert modular forms*, Bull. Amer. Math. Soc. **21** (1989), 65–69.

[BR93] ———, *Motives for Hilbert modular forms*, Invent. Math. **114** (1993), 55–87.

[C90] L. Clozel, *Motifs et formes automorphes: Applications du principe de fonctorialité*, Automorphic Forms, Shimura Varieties, and L-functions, Perspectives in Math., vol. 10, Academic Press, New York, 1990, pp. 77–159.

[D79] P. Deligne, *Valeurs de fonctions L et périodes d'intégrales*, Proc. Sympos. Pure Math., vol. 33, part 2, Amer. Math. Soc., Providence, R.I., 1979, pp. 313–346.

[DMOS82] P. Deligne, J. S. Milne, A. Ogus, and K-y Shih, *Hodge cycles, motives and Shimura varieties*, Lecture Notes in Math., vol. 900, Springer-Verlag, Berlin and New York, 1982.

[GJ72] R. Godement and H. Jacquet, *Zeta functions of simple algebras*, Lecture Notes in Math., vol. 260, Springer-Verlag, Berlin and New York, 1972.

[Gv88] F. Q. Gouvêa, *Arithmetic of p-adic modular forms*, Lecture Notes in Math., vol. 1304, Springer-Verlag, Berlin and New York, 1988.

[Gv90] ———, *Deforming Galois representations: Controlling the conductor*, J. Number Theory **34** (1990), 95–113.

[GS92] R. Greenberg and G. Stevens, *p-adic L-functions and p-adic periods of modular forms*, preprint.

[Ha87] G. Harder, *Eisenstein cohomology of arithmetic groups, the case* GL_2, Invent. Math. **89** (1987), 37–118.

[He85] G. Henniart, *Le point sur la conjecture de Langlands pour* $\mathrm{GL}(n)$, Sém. Théorie des Nombres, Paris **1983–84** (1985), 115–131.

[H89a] H. Hida, *Theory of p-adic Hecke algebras and Galois representations*, Sûgaku **39** (1987), 124–139; English transl., Sûgaku Expositions **2** (1989), 75–102.

[H89b] ———, *On nearly ordinary Hecke algebras for* $\mathrm{GL}(2)$ *over totally real fields*, Adv. Stud. Pure Math., vol. 17, Academic Press, Boston, MA, 1989, pp. 139–169.

[H89c] ———, *Nearly ordinary Hecke algebras and Galois representations of several variables*, in supplement to the Amer. J. Math., Algebraic Analysis, Geometry and Number Theory, Johns Hopkins Univ. Press, Baltimore, MD, 1989, pp. 115–134.

[H90a] ———, *p-adic L-functions for base change lifts of* GL_2 *to* GL_3, Proceedings of the Conference on Automorphic Forms, Shimura Varieties, and L-functions, Ann Arbor, Michigan, July 1988, Perspectives in Math., vol. 11, Academic Press, Boston, MA, 1990, pp. 93–142.

[H90b] ———, *Le produit de Petersson et de Rankin p-adique*, Sém. Théorie de Nombre de Paris **1988–89** (1990), 87–102.

[H91] ———, *On p-adic L-functions of* $\mathrm{GL}(2) \times \mathrm{GL}(2)$ *over totally real fields*, Ann. Institut Fourier **41**, No. 2 (1991), 311–391.

[H93a] ———, *p-ordinary cohomology groups for* $\mathrm{SL}(2)$ *over number fields*, Duke Math. J. **69** (1993), 259–314.

[H93b] ———, *Elementary theory of L-functions and Eisenstein series*, Student Texts in Mathematics, No. 26, Cambridge University Press, London and New York, 1993.

[H94a] H. Hida, *On the critical values of L-functions of* $\mathrm{GL}(2)$ *and* $\mathrm{GL}(2) \times \mathrm{GL}(2)$, Duke Math. J. **74** (1994), 431–530.

[H94b] ———, *p-adic ordinary Hecke algebras for* $\mathrm{GL}(2)$, Ann. Inst. Fourier (to appear).

[HT91] H. Hida and J. Tilouine, *Katz p-adic L-functions, congruence modules and deformation of Galois representations*, Proceedings of the London Math. Soc. Symposium on L-functions and arithmetic, Durham, England, July 1989, London Math. Soc. Lecture Note Ser., vol. 153, Cambridge Univ. Press, London and New York, 1991, pp. 271–293.

[HT93a] ———, *Anti-cyclotomic Katz p-adic L-functions and congruence modules*, Ann. Sci. École Norm. Sup. (4) **26** (1993), 189–259.

[HT93b] ———, *On the anticyclotomic main conjecture for CM fields*, Invent. Math. **117** (1994), 89–147.

[I72] K. Iwasawa, *Lectures on p-adic L-functions*, Ann. of Math. Stud., vol. 74, Princeton University Press, Princeton, NJ, 1972.

[K75] N. M. Katz, *p-adic L-functions via moduli of elliptic curves*, Proc. Sympos. Pure Math., vol. 29, Amer. Math. Soc., Providence, RI, 1975, pp. 479–506.

[K78] ———, *p-adic L-functions for CM fields*, Invent. Math. **49** (1978), 199–297.

[Ki91] K. Kitagawa, *On standard p-adic L-functions of families of elliptic cusp forms*, Ph.D. thesis, Univ. of California, Los Angeles, CA, 1991 (to appear in Contemporary Math.).

[Ku87] P. C. Kutzko, *On the supercuspidal representation of GL_N and other p-adic groups*, Proc. Internat. Congress Math. 1986, Berkeley, I, Amer. Math. Soc., Providence, RI, 1987, pp. 853–861.

[L76] R. P. Langlands, *On the functional equations satisfied by Eisenstein series*, Lecture Notes in Math., vol. 544, Springer-Verlag, Berlin and New York, 1976.

[M89] B. Mazur, *Deforming Galois representations*, Galois Groups over **Q**, Springer-Verlag, Berlin and New York, 1989, pp. 385–437.

[MT90] B. Mazur and J. Tilouine, *Représentations Galoisiennes, différentielles de Kähler et conjectures principales*, Inst. Hautes Études Sci. Publ. Math. **71** (1990), 65–103.

[Mi89] T. Miyake, *Modular forms*, Springer-Verlag, Berlin and New York, 1989.

[N86] J. Neukirch, *Class field theory*, Grundlehren Math. Wiss. 280, Springer, 1986.

[Sch68] M. Schlessinger, *Functors on Artin rings*, Trans. Amer. Math. Soc. **130** (1968), 208–222.

[Se75] J.-P. Serre, *Valeurs propres des opérateurs de Hecke modulo ℓ*, Astérisque **24–25** (1975), 109–117.

[Sh71] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Iwanami Shoten and Princeton University Press, Princeton, NJ, 1971.

[Sh88] ———, *On the critical values of certain Dirichlet series and the periods of automorphic forms*, Invent. Math. **94** (1988), 245–305.

[Sh90] G. Shimura, *On the fundamental periods of automorphic forms of arithmetic type*, Invent. Math. **102** (1990), 399–428.

[Ta89] R. Taylor, *On Galois representations associated to Hilbert modular forms*, Invent. Math. **98** (1989), 265–280.

[Ta] ———, *Congruences between modular forms on GL_2 over imaginary quadratic fields*, preprint.

[T79] J. Tate, *Number theoretic background*, Proc. Sympos. Pure Math., vol. 33, part 2, Amer. Math. Soc., Providence, RI, 1979, pp. 3–26.

[Ti89] J. Tilouine, *Sur la conjecture principale anticyclotomique*, Duke Math. J. **59** (1989), 629–673.

[Wa82] L. C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Math., vol. 83, Springer, New York, 1982.

[W84] A. Weil, *Number Theory, An approach through history from Hammurapi to Legendre*, Birkhäuser, Boston, 1984.

[W51] ———, *Sur la théorie du corps de classes*, J. Math. Soc. Japan **3** (1951), 1–35.

[Wi88] A. Wiles, *On ordinary λ-adic representations associated to modular forms*, Invent. Math. **94** (1988), 529–573.

Department of Mathematics, University of California at Los Angeles, Los Angeles, CA 90024

Translated by HARUZO HIDA