ADVANCES IN MATHEMATICS 21, 235–292 (1976)

Elliptic Curves and Automorphic Representations

STEPHEN GELBART

Department of Mathematics, Cornell University, Ithaca, New York 14853

CONTENTS

INTRODUCTION

The main purpose of this paper is to give a brief but relatively self-contained account of the recent refinements of Weil's conjecture and Eichler–Shimura theory due to Langlands and Deligne. A secondary goal is to interpret these relations between elliptic curves and representations of GL(2) from the broader perspective of Langlands' philosophy of L-series attached to automorphic forms.

Background material is collected in Parts I and II. Part I concerns the classical theory of the Hasse–Weil zeta-function and consequences of the theory of Eichler and Shimura. Part II develops the requisite representation theory and the notion of automorphic representation. The subject matter proper of the paper is treated in Part III.

I am indebted to R. P. Langlands, S. Lichtenbáum, and W. C. Waterhouse for several helpful conversations related to this material. I am also grateful to P. Cartier for suggesting I prepare this paper along the present lines.

I. Elliptic Curves and Their Zeta-Functions

1. *Preliminaries*

In this section we collect some basic facts about elliptic curves over an arbitrary field in general and a finite field in particular.

First suppose K is an arbitrary field. By *elliptic curve over* K we understand a nonsingular curve of genus 1 furnished with a K-rational point taken as the origin for the group law. Every such curve has an affine *Weierstrass model* of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\,, \tag{1}$$

with coefficients a_i in K. The *homogenization*

$$F(X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0 \tag{2}$$

is obtaining by setting x equal to X/Z and y equal to Y/Z.

Let E denote the projective curve defined by (2). The solution $0 = (0, 1, 0)$ of (2) corresponds to the "point at infinity" on (1). This is the distinguished point which we take to be the origin of the group law on E.

If the characteristic of K is not 2 or 3 we can replace x and y by

$$\mathfrak{p} = x + \frac{a_1{}^2 + 4a_2}{12} \qquad \text{and} \qquad \mathfrak{p}' = 2y + a_1x + a_3$$

to obtain from (1) the classical Weierstrass equation

$$(\mathfrak{p}')^2 = 4\mathfrak{p}^3 - g_2\mathfrak{p} - g_3 \tag{3}$$

with $g_2, g_3 \in K$. In this case the group law on E is particularly simple to describe. Indeed if (x_1, y_1) and (x_2, y_2) are two points satisfying (3) the formulas for the coordinates of their sum are

$$x_1 \dotplus x_2 = -x_1 - x_2 + \frac{1}{4}\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2$$

and

$$y_1 \dotplus y_2 = -\left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 \dotplus x_2) + \frac{y_2 x_1 - y_1 x_2}{x_2 - x_1}.$$

In particular it follows that the set of K-rational points of E, denoted $E(K)$, is a *subgroup* of E. Recall that E is regarded as the set of points in $\mathbb{P}^2(\bar{K})$ satisfying (the homogenization of) (3) with $\bar{K}$ an algebraic closure of K.

Now suppose E' is another elliptic curve over K and α is a map from E to E'. We say α is *K-rational* (or just rational) if it is induced from a backward homomorphism of the corresponding function fields $K(E)$ and $K(E')$. Equivalently, α is rational if it is given by rational functions of the coordinates with coefficients in K. In these terms E and E' are K-isomorphic (or just isomorphic) if there is a rational bijection between them which is an isomorphism in the sense of groups. A related but weaker notion is that of isogeny. Two elliptic curves are *K-isogenous* (or simply isogenous) if there is a *nontrivial* K-rational homomorphism between them.

The affine equation (1) is called a Weierstrass model for E because of the familiar form it takes in characteristic not equal to 2 or 3. The *discriminant* of the cubic (3) is simply $g_2^3 - 27g_3^2$. In general, for arbitrary K, the *discriminant* $\Delta(a_1, a_2, a_3, a_4, a_6)$ of (1) is given by [50, formula (2)]. In all cases, the nonvanishing of Δ is equivalent to the nonsingularity of E.

If E' is an elliptic curve over K with Weierstrass model

$$y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6', \tag{4}$$

then E and E' are K-isomorphic if and only if (4) is obtained from (1) by a coordinate change of the form

$$x = u^2x' + r \qquad \text{and} \qquad y = u^3y' + su^2x' + t, \tag{5}$$

with $r, s, t, u \in k$, and $u \neq 0$. Thus the Weierstrass model for an elliptic curve is unique up to a coordinate change of the form (5). The corresponding transformation formula for the discriminant is

$$\Delta(a_1, \ldots, a_6) = u^{12} \Delta(a_1', \ldots, a_6'). \tag{6}$$

Related formulas for the coefficients a_i are to be found in [50]. From (6) it already follows that an elliptic curve over K is one and the same thing as a cubic equation of the form (1) with coefficients in K and $\Delta \neq 0$.

The *j-invariant* of E is introduced through the formula

$$j(E) = (a_1^4 + 8a_1^2a_2 + 16a_2^2 - 24a_1a_3 - 48a_4)^3 \Delta^{-1}$$

or simply

$$j(E) = 1728\, g_2^3/(g_2^3 - 27g_3^2),$$

when char(K) $\neq$ 2 or 3. This is an invariant of E because it is of "weight zero" with respect to coordinate changes of the form (5), i.e., if E is K-isomorphic to E', then $j = j'$. Conversely, if $j = j'$, E and E' are isomorphic over some finite algebraic extension of K. In particular, if K is algebraically closed, j is a bijection between K and the set of isomorphism classes of elliptic curves over K.

For a detailed introduction to the general theory of elliptic curves over K and the classical Weierstrass theory over $\mathbb{C}$ see [35, Chaps. I, II]. For a less elementary account of the theory see [10] or [50].

EXAMPLE 1.1 (*Complex Multiplication*). Suppose E is an elliptic curve over $\mathbb{Q}$. Regarded as an elliptic curve over $\mathbb{C}$, E is isomorphic to $\mathbb{C}/L$ with L some lattice in $\mathbb{C}$ (see, for example, [35]). Each complex number which maps L into itself (by multiplication) then induces an endomorphism of E over $\mathbb{C}$ and all such endomorphisms so arise. In particular, End(E) $\supseteq \mathbb{Z}$. When this containment is proper, i.e., when End(E) contains "nontrivial" elements, E is said to possess *complex multiplication*. The terminology is apt since all "nontrivial" endomorphisms are actually induced by quadratic *imaginary* numbers. Applications of the theory of complex multiplication to the construction of class fields are described in [25, 37].

Now suppose K is a finite field. For simplicity, we actually suppose $K = \mathbb{F}_p$. Then we let $\overline{\mathbb{F}}_p$ denote an algebraic closure of $\mathbb{F}_p$, G the Galois group of $\overline{\mathbb{F}}_p$ over $\mathbb{F}_p$, and Π_p the Frobenius automorphism

$\alpha \to \alpha^p$. Recall that $\prod_p$ topologically generates G and $\mathbb{F}_{p_n} = \{\alpha \in \overline{\mathbb{F}}_p : \prod_p^n(\alpha) = \alpha\}$.

If E is an elliptic curve over $\mathbb{F}_p$, let N_n denote the cardinality of $E(\mathbb{F}_{p^n})$, i.e., the number of $\mathbb{F}_{p^n}$-rational points on E. Recall that E is viewed as the subset of $\mathbb{P}^2(\overline{\mathbb{F}}_p)$ satisfying the homogenization of some nonsingular cubic equation (1) with coefficients in $\mathbb{F}_p$. Thus N_n is (because of the point at infinity) one greater than the number of solutions of (1) with coordinates in $\mathbb{F}_{p^n}$.

One convenient way to record the diophantine data N_n is to introduce the *zeta-function of E*. This is given by the Dirichlet series

$$Z_E(s) = \sum_{\mathbf{d} \in \mathrm{Div}^+_{\mathbb{F}_p}(E)} \frac{1}{N(\mathbf{d})^s}, \tag{7}$$

where $\mathrm{Div}^+_{\mathbb{F}_p}(E)$ denotes the group of positive rational divisors of E and $N(\mathbf{d})$ is the norm of $\mathbf{d}$. (A divisor $\mathbf{d} = \sum d_P \cdot P$ is *positive* if each $d_P \geqslant 0$ and *rational* if $d_P = d_{P\sigma}$ for each $\sigma \in G$; the *norm* of $\mathbf{d}$ is $p^{\deg(\mathbf{d})}$, where $\deg(\mathbf{d}) = \sum_P d_P$.)

On a purely formal level,

$$Z_E(s) = \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1}, \tag{8}$$

where $\mathfrak{p}$ extends over the *prime* divisors in $\mathrm{Div}^+_{\mathbb{F}_p}(E)$ (those which cannot be expressed as the sum of two positive nonzero divisors). The logarithmic version of (8) is

$$\log Z_E(s) = \sum_{n \geqslant 1} \frac{N_n p^{-ns}}{n}. \tag{9}$$

But N_n cannot possibly be greater than the cardinality of $\mathbb{P}^2(\mathbb{F}_{p^n})$. Thus $N_n \leqslant p^{2n} + p^n + 1$, (9) converges for $\mathrm{Re}(s) > 2$, and *the series defining $Z_E(s)$ converges absolutely for* $\mathrm{Re}(s)$ *sufficiently large.*

THEOREM 1.2. (i) (*Analytic continuation and functional equation of $Z_E(s)$*). *The function $Z_E(s)$ has a meromorphic continuation to all of $\mathbb{C}$ and satisfies the functional equation*

$$Z_E(s) = Z_E(1 - s).$$

(ii) (*Rationality of $Z_E(s)$*). *If*

$$a_p = p + 1 - N_1$$

and

$$P(u) = 1 - a_p u + pu^2,$$

then

$$Z_E(s) = P(p^{-2})/(1 - p^{-s})(1 - p^{1-s}).$$

This theorem generalizes to higher-dimensional varieties as follows. Let V denote a nonsingular projective variety over $\mathbb{F}_p$ of dimension d and let $Z_V(s)$ denote its zeta-function (defined by (9)). In [51] (see also [55]) Weil conjectured that

$$Z_V(s) = \frac{P_1(u)\, P_3(u) \cdots P_{2d-1}(u)}{P_0(u)\, P_2(u) \cdots P_{2d}(u)} \qquad (u = p^{-s}),$$

with $P_0(u) = 1 - u$, $P_{2n}(u) = (1 - p^n u)$, and (for $1 \leqslant h \leqslant 2d - 1$)

$$P_h(u) = \prod_{i=1}^{\beta_h} (1 - \alpha_{h_i} u).$$

This was first established in its full generality by Dwork (cf. [17, 20, 39]). For elliptic curves (varieties of dimension 1 and genus 1) its proof is straightforward (see, for example, [35]).

In [51] Weil also conjectured a Riemann-hypothesis to the effect that the inverse roots α_{h_i} of $P_h(u)$ are of absolute value $p^{h/2}$. This was just recently proved in its full generality by Deligne [11]. Previously it had been proved by Hasse for elliptic curves and by Weil for arbitrary curves (varieties of dimension 1 and arbitrary genus). For elliptic curves, one gets

$$P_1(u) = P(u) = (1 - \alpha_1 u)(1 - \alpha_2 u) = 1 - a_p u + pu^2, \tag{10}$$

with

$$|\alpha_1| = |\alpha_2| = p^{1/2}. \tag{11}$$

Thus Hasse's result is equivalent to

THEOREM 1.3 (The Riemann-hypothesis for function fields of genus 1). *The zeros of $Z_E(s)$ lie on the line* $\mathrm{Re}(s) = \frac{1}{2}$.

Note that (10) implies $\alpha_1 + \alpha_2 = a_p$. Thus (11) says $|a_p| \leqslant 2p^{1/2}$; i.e., N_1 differs in absolute value from $p + 1$ by less than $2p^{1/2}$. Theorem 1.2 in turn relates N_n to N_1. Note also that even for elliptic curves the rationality result (Theorem 1.2) lies less deep than the estimate for N_1 (Theorem 1.3). For a sketch of the proof of Theorem 1.3, see [10] or [50].

Concluding Remarks. The Frobenius automorphism $\prod_p$ extends naturally to an endomorphism of E whose fixed point set is $E(\mathbb{F}_p)$. Thus $\prod_p$ can also be realized as a linear map on the so-called *Tate module* of E.

More precisely, for each $l \neq p$, and $n > 0$, elements of End(E) induce homomorphisms of the group of *l^n-division points* of E (the kernel of multiplication by l^n). The representations

$$\mathrm{End}(E) \rightarrow \mathrm{End}((\mathbb{Z}/l^n) \times (\mathbb{Z}/l^n)) \approx M_2(\mathbb{Z}/l^n)$$

corresponding to increasing n are compatible and hence yield an l-adic representation

$$\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q} \rightarrow \mathrm{End}(\mathbb{Q}_l \times \mathbb{Q}_l) \approx M_2(\mathbb{Q}_l)$$

after taking limits and tensoring with $\mathbb{Q}$. This is the standard l-adic representation of End(E). The free $\mathbb{Z}_l$-module of rank 2 which determines it is the *Tate-module* $T_l(E)$. For details, see [35, p. 178], [51], or [49, Chap. 9]. The crucial point is that the trace of $\prod_p$ on the vector space $V_l(E) = T_l(E) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ is independent of l and equal to a_p ; i.e.,

$$N_1 = p + 1 - \mathrm{tr}\left(\prod_p\right). \tag{12}$$

More generally, one can introduce the m-dimensional l-adic cohomology spaces $H^m(E, \mathbb{Q}_l)$ of Artin and Grothendieck (see, for example, [41]). The Frobenius automorphism then induces an endomorphism $\prod^l_{p,m}$ on $H^m(E, \mathbb{Q}_l)$ and

$$P_h(u) = \det\left(I - \prod_{p,h}^{l} u\right).$$

In particular, $H^1(E, \mathbb{Q}_l)$ is dual to the homology representation $V_l(E)$ and

$$Z_E(s) = \frac{1 - \mathrm{tr}(\prod^l_{p,1})\, p^{-s} + p^{1-2s}}{(1 - p^{-s})(1 - p^{1-s})}.$$

In general, if V is an n-dimensional variety over $\mathbb{F}_p$, and $P^l_{p,m}(u) = \det(I - \prod^l_{p,m} u)$, then

$$Z_V(s) = \prod_{m=0}^{2n} P^l_{p,m}(p^{-s})^{(-1)^{m+1}}.$$

In all cases, the middle-dimensional cohomology plays the crucial role.

Similar considerations hold for an abelian variety of arbitrary genus g. In this case, T_l has rank $2g$ over $\mathbb{Z}_l$.

2. *The Zeta-Function of an Elliptic Curve over* $\mathbb{Q}$

If E is an elliptic curve over $\mathbb{Q}$, choose a Weierstrass model for E of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{13}$$

so that

(i) $a_i \in \mathbb{Z}$; and

(ii) for each prime p, the p-order of $\Delta(a_1, \ldots, a_6)$ is minimal.

Such a model is called a *global minimal Weierstrass equation* for E.

The curve *over* $\mathbb{F}_p$ defined by (13) reduced mod p is denoted $\bar{E}_p$ and called the *reduction of* E mod p. If $\bar{E}_p$ is elliptic over $\mathbb{F}_p$, i.e., $\Delta(a_1, \ldots, a_6) \not\equiv 0 \bmod p$, we say *$E$ has good reduction at p.* Clearly E has "bad" reduction at only a finite number of primes. How bad the reduction is over all primes is measured by the *conductor*

$$\mathrm{Cond}(E) = N = \prod_p p^{f_p}.$$

Here $f_p = 0$ if $p \nmid \Delta$ and $f_p \geqslant 1$ otherwise.

More precisely, if $p \mid \Delta$, $\bar{E}_p$ is a curve of genus 0 whose unique singular point is either

(a) a node with both tangent directions defined over $\mathbb{F}_p$;

(b) a node with tangent directions *conjugate* over $\mathbb{F}_p$; or

(c) a cusp, where no tangent exists.

Characterizations of possibilities (a), (b), and (c) in terms of the coefficients a_i are given in [32, 50]. If the singularity of $\bar{E}_p$ is of type (a) or (b), then $f_p = 1$. On the other hand, if the singularity is a cusp, f_p is greater than or equal to 2 in general and equals 2 if $p > 3$ (for further details, see [32]). In all cases, f_p is invariant by isogeny.

Remark 2.1. If E has good reduction at p then its j-invariant is p-integral. Conversely, if $j(E)$ is p-integral, there is some finite extension L of $\mathbb{Q}$ such that $E \otimes_{\mathbb{Q}} L$ has good reduction at all places of L dividing p. This is "potential good reduction" in the sense of Serre and Tate [44].

EXAMPLE 2.2. Let E denote the elliptic curve with global minimal Weierstrass equation

$$y^2 + y = x^3 - x^2. \tag{14}$$

The discriminant of (14) is -11 and therefore E has good reduction at p if and only if $p \neq 11$. Moreover, the singular point of $\bar{E}_{11}$ is a node. Thus the conductor of E is 11.

In general, if E is an elliptic curve over $\mathbb{Q}$, let $N_1(p)$ denote the cardinality of $\bar{E}_p(\mathbb{F}_p)$. Equivalently, $N_1(p)$ is one more than the number of solutions of the congruence

$$y^2 + a_1xy + a_3y \equiv x^3 + a_2x^2 + a_4x + a_6 \pmod{p}$$

obtained from (13). The analytic object which stores this diophantine data is the *Hasse–Weil zeta-function of* E defined by

$$\begin{aligned} \zeta(E, s) &= \prod_{p<\infty} (1 - a_p p^{-s} + \psi(p) p^{1-2s})^{-1} \\ &= \prod_{p<\infty} L_p(p^{-s}). \end{aligned}$$

Here

$$a_p = 1 + p - N_1(p),$$

and $\psi(p)$ is 0 or 1 according as p does or does not divide Cond(E).

If p does not divide Cond(E), let α_1, α_2 denote the characteristic roots of the Frobenius map $\prod_p : (x, y) \to (x^p, y^p)$ regarded as an element of End$(\bar{E}_p)$. Then $L_p(u)^{-1} = 1 - a_pu + pu^2 = (1 - \alpha_1u)(1 - \alpha_2u) = (1 - u)(1 - pu) Z_{\bar{E}_p}(s)$. Consequently from (11) it follows that *the product defining* $\zeta(E, s)$ *converges for* Re$(s) > \frac{3}{2}$. In particular, *the product defining* $\zeta(E, s)$ *determines a holomorphic function of* s *in the right half-plane* Re$(s) > \frac{3}{2}$.

Hasse's conjecture is that $\zeta(E, s)$ has an analytic continuation to the whole plane and satisfies a functional equation relating its values at s

and $1 - s$. The exact form of the functional equation was conjectured by Weil [52]. The two examples given below are included to help motivate Weil's conjecture.

Remark 2.3. If $p \mid \Delta$, then $a_p = 1, -1$, or 0 according as the singularity of $\bar{E}_p$ is of type (a), (b), or (c). In any case,

$$\zeta(E, s) = \sum_{n=1}^{\infty} c_n n^{-s},$$

with $c_n \in \mathbb{Z}$ and $c_p = a_p$. Moreover, $\zeta(E, s) = \zeta(E', s)$ if E and E' are isogenous.

EXAMPLE 2.4. The elliptic curve with Weierstrass equation $y^2 = x^3 - x$ admits complex multiplication by i. Moreover [5] there exists a nontrivial grössencharacter χ of $\mathbb{Q}(i)$ (unramified outside 2) such that

$$\zeta(E, s) = L(s - \tfrac{1}{2}, \chi).$$

Here $L(s, \chi)$ is the Hecke L-series attached to χ (see [19]). The theory of Hecke thus implies Hasse's conjecture holds for E. More precisely, the entirety of $L(s, \chi)$ implies $\zeta(E, s)$ is actually entire and the functional equation for $L(s, \chi)$ implies

$$(2^r)^{s/2}(2\pi)^{-s}\,\Gamma(s)\,\zeta(E, s) = (-1)^n(2^r)^{(2-s)/2}(2\pi)^{s-2}\,\Gamma(2 - s)\,\zeta(E, 2 - s)$$

for some r and n.

The results of Example 2.4 generalize to arbitrary E with complex multiplication. In fact Deuring has shown that the zeta-function of any such curve is the translate of some $L(s, \chi)$ with χ an appropriate grössencharacter of $K = \mathrm{End}_{\mathbb{Q}}(E)$ (for details, see [25]).

EXAMPLE 2.5. Let E denote the curve of Example 2.2. Tate has shown that this curve is isogenous to Fricke's curve

$$y^2 = -44x^3 + 56x^2 - 20x + 1. \tag{15}$$

But Fricke's curve is a model for the modular variety $\Gamma_0(11)\backslash H$, obtained by factoring the upper half-plane H by

$$\Gamma_0(11) = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2, \mathbb{Z}) \colon c \equiv O(11)\right\};$$

i.e., the compactification of the set of complex points of (15) is (analytically) isomorphic to the compact Riemann surface determined by $\Gamma_0(11)\backslash H$.

Actually much more is known. If $\sum_{n=1}^{\infty} c_n e^{2\pi i n z}$ is the unique cusp form of weight 2 on $\Gamma_0(11)$ (with $c_1 = 1$) then

$$\zeta(E, s) = \sum_{n=1}^{\infty} c_n n^{-s}.$$

Thus from Hecke's theory of Dirichlet series attached to cusp forms it follows that $\zeta(E, s)\,\Gamma(s)$ is entire and satisfies the functional equation

$$(11)^{s/2}(2\pi)^{-s}\,\Gamma(s)\,\zeta(E, s) = (11)^{(2-s)/2}(2\pi)^{s-2}\,\Gamma(2-s)\,\zeta(E, 2-s).$$

In particular, Hasse's conjecture holds for E. We shall return to these notions in more detail in the next section. Note that the conductor of E equals the "level" of its corresponding modular form.

CONJECTURE A (Hasse–Weil). *If E is an elliptic curve over $\mathbb{Q}$ with conductor N put*

$$L(E, s) = N^{s/2}(2\pi)^{-s}\,\Gamma(s)\,\zeta(E, s).$$

Then $L(E, s)$ is entire and satisfies the functional equation

$$L(E, s) = wL(E, 2-s), \tag{16}$$

with $w = \pm 1$. More generally, for each primitive Dirichlet character χ defined modulo m, with $(m, N) = 1$, define

$$\zeta(E, \chi, s) = \sum_{n=1}^{\infty} c_n \chi(n)\, n^{-s}$$

and

$$L(E, \chi, s) = (m^2 N)^{s/2}(2\pi)^{-s}\,\Gamma(s)\, L(E, \chi, s).$$

Then $L(E, \chi, s)$ is entire, bounded in vertical strips of $\mathbb{C}$, and satisfies the functional equation

$$L(E, \chi, s) = w(g(\chi)/g(\bar{\chi}))\,\chi(-n)\, L(E, \bar{\chi}, 2-s) \tag{17}$$

with $g(\chi)$ the Gauss sum $\sum_{y=1}^{m} \chi(y)\, e^{2\pi i y/m}$.

Note that the modular curve of Example 2.5 satisfies (16) with $w = 1$. In fact Hecke's theory implies that $L(E, s)$ also satisfies (17) (cf. Sect. 3, Eq. (21)).

There are at least two possible interpretations for the sign of the constant w. On the one hand, the ultimate significance of Conjecture A is that Example 2.5 is not special, i.e., *every* elliptic curve over $\mathbb{Q}$ should be related to some modular form of weight 2. This being so, the sign of w should be explained by a particular transformation property of the corresponding modular form (see Sects. 3 and 5, especially (20) and Theorem 5.2).

On the other hand, the conjectures of Birch and Swinnerton-Dyer imply that the sign of w is also related to the parity of the rank of the group of rational points of E (for details, see [5, 6]).

Because there are numerous elliptic curves related to modular varieties for which Conjecture A can be checked directly it was natural (with hindsight) to ask if *all* E over $\mathbb{Q}$ are modular in this sense and satisfy Conjecture A. In one form or another, the remainder of this paper is devoted to a discussion of this single question.

Concluding Remark. Conjecture A is a special case of a vast conjecture about the zeta-functions attached to arbitrary algebraic varieties over arbitrary fields (cf. [41] and the concluding remarks of Sect. 1).

3. *The Zeta-Function of a Modular Form*

Let $\mathrm{GL}_2{}^+(\mathbb{R})$ denote the group $\{\alpha = [\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}] \in \mathrm{GL}_2(\mathbb{R})\colon \det(\alpha) > 0\}$. Then $\mathrm{GL}_2{}^+(R)$ acts on $\mathbb{C} \cap \{\infty\}$ by

$$\alpha(z) = (az + b)/(cz + d)$$

and preserves the upper half-plane H.

Set

$$\Gamma_0(N) = \left\{\alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z})\colon c \equiv 0(N)\right\}.$$

An element of $\Gamma_0(N)$ is called ***parabolic*** if it has only *one* fixed point in $\mathbb{C} \cap \{\infty\}$. The fixed point then belongs to $\mathbb{R} \cap \{\infty\}$ and is called a *cusp* of $\Gamma_0(N)$. If one such cusp is transformed into another by some α in $\Gamma_0(N)$ the two cusps are said to be *equivalent* with respect to $\Gamma_0(N)$; in general, $\Gamma_0(N)$ has only finitely many inequivalent cusps.

Let C denote the set of representatives for the cusps of $\Gamma_0(N)$ and put H^* equal to $H \cap C$. The quotient space $\Gamma_0(N)\backslash H^*$ has the structure of a compact Riemann surface. In fact $\Gamma_0(N)\backslash H^*$ is the set of complex points of a projective variety $X_0(N)$ defined over $\mathbb{Q}$ with good reduction outside N [22]. In particular, if $\Gamma_0(N)\backslash H^*$ has genus 1, $X_0(N)$ is elliptic with good reduction outside N. This is the case, for example, when $N = 11, 14, 15, 17$ or 19.

If $f(z)$ is a function on H, k is a nonnegative integer, and $\alpha = \begin{bmatrix} a & b \\ d & c \end{bmatrix}$ belongs to $\mathrm{GL}_2{}^+(\mathbb{R})$, define

$$(f|_k\alpha)(z) = (ad - bc)^{k/2}(cz + d)^{-k} f(\alpha(z)).$$

An *automorphic* (or *modular*) *form of weight k on* $\Gamma_0(N)$ is a function $f(z)$ satisfying the following conditions.

(i) $f|_k\gamma = f$ for all $\gamma \in \Gamma_0(N)$;

(ii) f is holomorphic on H;

(iii) f is holomorphic at the cusps of $\Gamma_0(N)$.

Condition (i) implies that $f|_k\sigma$ is periodic in z (with period 1) for all $\sigma \in \mathrm{SL}_2(\mathbb{Z})$; Condition (iii) means that the expansion of $f|_k\sigma$ in powers of

$$q = e^{2\pi iz}$$

has only *nonnegative* exponents (for all σ). If "nonnegative" is replaced by "positive." f is said to be *cuspidal*, or a *cusp form.*

Note that each cusp form has a Fourier expansion of the form

$$f(z) = \sum_{n=1}^{\infty} a_n q^n = \sum_{n=1}^{\infty} a_n e^{2\pi inz}.$$

The space of cusp forms of weight k on $\Gamma_0(N)$ is denoted by $S_k(\Gamma_0(N))$.

DEFINITION 3.1. Fix $f = \sum_{n=1}^{\infty} a_n q^n$ in $S_k(\Gamma_0(N))$ (with $q = e^{2\pi iz}$). For each prime number p the *Hecke operator* $T(p)$ takes f into

$$T(p) = \sum_{n=1}^{\infty} a_{pn} q^n + \psi(p)\, p^{k-1} \sum_{n=1}^{\infty} a_n q^{pn}.$$

Here $\psi(p)$ is 0 or 1 according as p does or does not divide N.

The Hecke operator $T(p)$ is Hermitian in $S_k(\Gamma_0(N))$ with respect to the Petersson inner product

$$(f, g)_k = \int\!\!\int_{\Gamma_0(N)\backslash H} f(z)\, \overline{g(z)}\, y^k \frac{dx\, dy}{y^2},$$

provided $p \nmid N$; if p does divide N, $T(p)$ need not even be normal. Therefore, although the family $\{T(p)\}$ is commutative, one cannot always find a basis for $S_k(\Gamma_0(N))$ consisting of simultaneous eigenfunctions for *all* the $T(p)$. The problem is that there may be "old forms" in $S_k(\Gamma_0(N))$, i.e., forms coming from $\Gamma_0(r)$ with r a proper divisor of N.

DEFINITION 3.2. For each integer m, let $\{T(p)\}^m$ denote the family of Hecke operators $T(p)$ with $(p, m) = 1$. Let $S_k^-(\Gamma_0(N))$ denote the subspace of $S_k(\Gamma_0(N))$ spanned by all possible functions of the form $g_j(\delta z)$ with $\{g_j\}$ a basis for $S_k(\Gamma_0(r))$ consisting of eigenfunctions for $\{T(p)\}^r$, r any proper divisor of N, and δ any divisor of N/r. The orthocomplement of $S_k^-(\Gamma_0(N))$ in $S_k(\Gamma_0(N))$ is preserved by $\{T(p)\}^N$ and has a basis consisting of eigenfunctions for $\{Y(p)\}^N$; a *primitive form* in $S_k(\Gamma_0(N))$ is any such basis element (see [31]).

The remainder of this section will be devoted to explaining the detailed significance of primitive forms.

Suppose $f = \sum_{n=1}^{\infty} a_n q^n$ is a *normalized* primitive form, i.e., $a_1 = 1$. Then f is an eigenfunction for *all* the $T(p)$ and the Dirichlet series

$$D(f, s) = \sum_{n=1}^{\infty} a_n n^{-s} \tag{18}$$

has an Eulerian expansion of the form

$$D(f, s) = \prod_p (1 - a_p p^{-s} + \psi(p)\, p^{k-1-2s})^{-1}. \tag{19}$$

Henceforth we shall deal almost exclusively with normalized primitive forms. For *any* primitive form, $a_1 \neq 0$.

The series (18) is *the zeta-function of f*. The zeta-function of an arbitrary form in $S_k(\Gamma_0(N))$ has an expansion of the form (19) *only if f* is an eigenfunction of all the $T(p)$.

If $(m, N) = 1$, and χ is a primitive Dirichlet character mod m, put

$$D(s, f, \chi) = \sum \chi(n)\, a_n n^{-s}$$

and

$$L(s, f, \chi) = (m^2 N)^{s/2} (2\pi)^{-s}\, \Gamma(s)\, D(s, f, \chi).$$

Suppose

$$f \mid_k \begin{bmatrix} 0 & -1 \\ N & 0 \end{bmatrix} = w i^k f, \tag{20}$$

with $w = \pm 1$; equivalently,

$$f(-1/Nz) = w\, i^k N^{k/2} z^k f(z).$$

Condition (20) is actually automatic for primitive forms (cf. [31]). In any case, $L(s, f, \chi)$ is entire, bounded in vertical strips of $\mathbb{C}$, and satisfies the (Hecke) functional equation

$$L(s, f, \chi) = w(g(\chi)/g(\bar{\chi}))\, \chi(-N) L(k - s, f, \bar{\chi}), \tag{21}$$

with $g(\chi)$ as in (17).

Remark 3.3. Suppose $f = \sum_{n=1}^{\infty} a_n q^n$ in $S_k(\Gamma_0(N))$ satisfies (20) and $D(s, f)$ satisfies (19). Then f is automatically a normalized primitive form [31, Theorem 7]. In this case,

$$a_p = 0 \tag{22}$$

if $p^2 \mid N$, and

$$| a_p | = p^{k/2-1} \tag{23}$$

if $p \,\|\, N$ (i.e., p divides N but p^2 does not).

Concluding Remark. Note that $L(s, f) = L(s, f, 1)$ is essentially the Mellin transform of f. Indeed

$$\int_0^{\infty} f(iy)\, y^{s-1}\, dy = (2\pi)^{-s}\, \Gamma(s)\, D(s, f).$$

4. *Eichler–Shimura Theory*

The modular curve $X_0(N)$ is a nonsingular projective curve over $\mathbb{Q}$ whose function field is the field of modular functions for $\Gamma_0(N)$. Although its zeta-function is initially defined only in some right half-plane, the general conjecture of Hasse–Weil asserts that it continues analytically to the whole plane and satisfies a simple functional equation. The thrust of Eichler–Shimura theory is that this already follows from Hecke's theory of Dirichlet series attached to modular forms (i.e., the zeta-function of $X_0(N)$ is determined by the action of the Hecke ring on $S_2(\Gamma_0(N))$).

Our exposition in this section follows [6] (for details, see [46–48]).

Fix p to be a prime which does not divide N. By Igusa [22] it is known that $X_0(N)$ has good reduction mod p, i.e., the reduced curve $\bar{X}_0(N)_p$

is nonsingular over $\mathbb{F}_p$. Thus we let $\prod_p$ denote its Frobenius correspondence and $\prod_p'$ the transpose of $\prod_p$ on $\bar{X}_0(N)_p \times \bar{X}_0(N)_p$.

The fundamental congruence relation of Eichler–Shimura theory relates $\prod_p$ to $T(p)$. Indeed $T(p)$ can be regarded as an algebraic correspondence on $\bar{X}_0(N)_p$ (cf. [46, Sect. 7.2]. What the congruence relation asserts is that

$$T_p = \prod_p + \prod_p{}' . \tag{24}$$

To explain the significance of (24) for the zeta-function of $X_0(N)$ let us recall some definitions. The *Jacobian* $J_0(N)$ is the group of divisors of degree 0 on $X_0(N)$ identified modulo principal divisors. If $X_0(N)$ has genus g, $J_0(N)$ defines an abelian variety over $\mathbb{Q}$ of dimension g. The reduced curve $X_0(N)_p$ also has genus g. Its zeta-function is

$$Z_p(s) = P_p(u)/(1-u)(1-pu),$$

where $u = p^{-s}$ and $P_p(u) = \prod_{i=1}^{2g}(1 - \alpha_i u)$ (cf. the remarks after Theorem 1.2). The zeta-function of $X_0(N)$ is obtained by taking products over the "good" primes. Thus

$$Z(X_0(N), s) = \prod_{p \nmid N} P_p(p^{-s})^{-1} = \prod_{p \nmid N} L_p(p^{-s}).$$

Now regard $T(p)$ as an endomorphism of the space $S_2(\Gamma_0(N))$. Since $S_2(\Gamma_0(N))$ is isomorphic to the space of differentials of the first kind on $X_0(N)$, its complex dimension is g. What keeps us from applying (24) directly is that the g-dimensional complex representation of $T(p)$ in $S_2(\Gamma_0(N))$ does not survive reduction mod p. Thus we consider the $2g$-dimensional representation coming from the standard *l-adic* representation of $\mathrm{End}(J_0(N))$ (cf. the concluding remarks of Sect. 1). This representation does survive reduction mod p.

If Δ_p denotes the diagonal on $\bar{X}_0(N)_p \times \bar{X}_0(N)_p$ then $\prod_p \circ \prod_p = p\Delta_p$. Note also that the l-adic representation just described is equivalent to two copies of the g-dimensional complex representation. Thus (24) implies

$$\det\left\{\left\{I_{2g} - u\prod_p\right\}\left\{I_{2g} - u\prod_p{}'\right\}\right\} = [\det\{I_g - uT(p) + pu^2 I_g\}]^2.$$

That is,

$$\det\left\{I_{2g} - u\prod_p\right\} = \det\{I_g - uT(p) + pu^2 I_g\} = \prod_{i=1}^{2g}(1 - \alpha_i u).$$

Thus one gets the desired relation between $Z(X_0(N), s)$ (defined up to a finite number of factors) and the action of the Hecke operators $T(p)$ in $S_2(\Gamma_0(N))$. Applications to elliptic curves are obtained as follows.

Suppose $J_0(N)$ is isogenous to the product of an elliptic curve E and an abelian variety A (both defined over $\mathbb{Q}$). Suppose also that there are no nontrivial $\mathbb{Q}$-rational homomorphisms between E and A. Since 1-forms on E and A lift back to 1-forms on $J_0(N)$ (hence $X_0(N)$) the decomposition of $J_0(N)$ corresponds to a direct sum decomposition of $S_2(\Gamma_0(N))$. It also corresponds to a direct sum decomposition of the standard complex representation of $T(p)$. (If $T(p)$ did not respect the decomposition of $S_2(\Gamma_0(N))$ it would induce a nontrivial homomorphism between E and A.)

Now note that differentials of the first kind on E pull back to a one-dimensional space of differential on $X_0(N)$. Equivalently, differentials of the first kind pull back to a one-dimensional subspace of $S_2(\Gamma_0(N))$. Thus if $f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}$ belongs to this subspace, it is automatically an eigenfunction for *all* the $T(p)$. Normalize f so that $a_1 = 1$. If $p \nmid N$, then $T(p)f = a_p f$. Thus restricting the arguments used above to the one-dimensional subspace of $S_2(\Gamma_0(N))$ belonging to f (or E) yields

THEOREM 4.1. *Suppose E is an elliptic modular curve, i.e., an elliptic curve over $\mathbb{Q}$ isogenous to an isolated factor of $J_0(N)$. Then there is a cusp form f_E in $S_2(\Gamma_0(N))$ (the form corresponding to the unique differential of the first kind on E) with the property that the p-factor of its zeta-function coincides with the p-factor of $L(E, s)$ for all p not dividing N.*

With "almost all p" in place of "$p \nmid N$" this theorem is due to Eichler and Shimura. That one can deal with all $p \nmid N$ results from [22]. Actually, from recent work of Deligne and Langlands it follows that the p-factors of $L(s, f)$ and $L(E, s)$ agree *for all p*. In this sense the theory of Eichler–Shimura is now complete. We shall come back to this work of Deligne and Langlands in Part III after recasting the theory in the mold of representation theory. In the meantime, we take it for granted that

$$L(E, s) = L(s, f_E).$$

5. *Weil's Conjecture*

According to Theorem 4.1 and the remarks immediately following it, the zeta-function of an elliptic modular curve is the Mellin transform of an appropriate cusp of weight 2. More generally, if $k = 2$, the functional equations of Hasse and Weil (17) and Hecke (21) coincide. This is probably no accident. For any elliptic curve over $\mathbb{Q}$ the conjecture of Hasse and Weil ultimately implies $L(E, s)$ is $L(f, s)$ for some appropriate (normalized primitive) form in $S_2(\Gamma_0(N))$.

EXAMPLE 5.1. Recall the curve E (of Examples 2.2 and 2.5) defined by

$$y^2 + y = x^3 - x^2.$$

Its zeta-function is

$$\zeta(E, s) = (1 - a_{11} p^{-s})^{-1} \prod_{p \neq 11} (1 - a_p p^{-s} + p^{1-2s})^{-1},$$

with $a_{11} = 1$. Furthermore its conductor is 11. On the other hand, $S_2(\Gamma_0(11))$ is one-dimensional and spanned by the normalized primitive form

$$\begin{aligned} f(z) &= e^{2\pi i n z} \prod_{n=1}^{\infty} (1 - e^{2\pi i n z})^2 \prod_{n=1}^{\infty} (1 - e^{22\pi i n z})^2 \\ &= (\Delta(z)\, \Delta(11z))^{1/12} \\ &= \sum_{n=1}^{\infty} a_n' e^{2\pi i n z}, \end{aligned}$$

with $a_p' = a_p$; here $\Delta(z)$ is the unique (normalized) cusp form of weight 12 for $\Gamma_0(1)$. Thus

$$L(E, s) \equiv L(f, s).$$

CONJECTURE B (Weil's conjecture). *If E is a elliptic curve over $\mathbb{Q}$ of conductor N there exists a (normalized primitive) cusp form f in $S_2(\Gamma_0(N))$ such that*

$$L(f, s) = L(E, s).$$

Note Conjecture B implies that the pth Fourier coefficient of f should be 0 or ± 1 when p divides N. This is consistent with (22) and (23). The conjecture also implies (by the Riemann-hypothesis for function fields of genus 1) that

$$| a_p | \leqslant 2p^{1/2}.$$

This is consistent with the Ramanujan–Petersson conjecture for forms of weight 2 proved by Igusa, Eichler, and Shimura (cf. Theorem 4.1 and (11)).

Note too that Conjecture B obviously implies Conjecture A (cf. (21) and (17)). That Conjecture A also implies Conjecture B results from the characterization of the zeta-function of a cusp form in terms of its functional equations (21). By establishing this characterization Weil simultaneously filled an important gap in Hecke's theory and unearthed the (conjectured) relation between elliptic curves and modular forms.

THEOREM 5.2 [52]. *Suppose the sequence of complex numbers* a_1, $a_2, \ldots, a_n, \ldots$ *is such that*

(i) $|a_n| = O(n^\sigma)$ *for some* $\sigma > 0$;

(ii) *the Dirichlet series* $\sum_{n=1}^{\infty} a_n n^{-s}$ *converges absolutely at* $s = k - \delta$ *for some* $k > \delta > 0$;

(iii) *for each* $(m, N) = 1$, *and primitive character* χ *modulo* m, $L(s, \chi) = \sum_{n=1}^{\infty} a_n \chi(n) n^{-s}$ *is entire, bounded in vertical strips, and satisfies the functional equation* (21).

Then $\sum_{n=1}^{\infty} a_n e^{2.inz} = f(z)$ *belongs to* $S_k(\Gamma_0(N))$ *and satisfies* (20).

COROLLARY 5.3. *Conjectures* A *and* B *are equivalent.*

Recall that $L(E, s) = \sum_{n=1}^{\infty} a_n n^{-s}$ converges for $\mathrm{Re}(s) > \frac{3}{2}$. Thus in applying Theorem 5.2, $k = 2$ and δ can be taken to be $\frac{1}{2} + \epsilon$.

Now let $E \rightarrow^{W} f_E$ denote the correspondence which Weil's conjecture establishes between elliptic curves over $\mathbb{Q}$ and cusp forms of weight 2. An arbitrary form in $S_2(\Gamma_0(N))$ is in the image of W *only if* it is a normalized primitive form with Fourier coefficients in $\mathbb{Z}$. We call such a form a "rational" normalized primitive form. The natural question to ask is, Do the above conditions *characterize* the image of W? In other words, given such a form f can we produce an elliptic curve E such that $f_E = f$? This is a question which is essentially resolved by Section 4 but more carefully considered by Shimura [48].

Briefly, since each a_p is assumed to be integral, each $T(p) - a_p$ may be regarded as an element of $\mathrm{End}(J_0(N))$. So let Y denote the subvariety of $J_0(N)$ defined by the union of the images of these endormorphisms. The resulting quotient $J_0(N)/Y$ is then an elliptic curve (call it E_f). Moreover, from Eichler–Shimura theory (as refined by Deligne and Langlands) it follows that $L(E_f, s) = L(f, s)$.

Actually, Conjecture B already implies (without Deligne and Langlands) that the p-factors of the zeta-functions of E_f and f agree for all p. To see this, compose the map $f \rightarrow E_f$ just described with Weil's map $E_f \rightarrow f'$. Since $L(f', s) = L(f, s)$ up to a finite number of factors in the Euler product, the normalized new forms f and f' must coincide. Thus $L(f, s) = L(f', s) = L(E_f, s)$, as desired. In particular, E_f has conductor N. The image of the conjectured correspondence $E \rightarrow f_E$ is precisely the set of rational normalized primitive forms in $S_2(\Gamma_0(N))$ and its inverse is the correspondence $f \rightarrow E_f$ just described.

Conjecture C. *The map $f \rightarrow E_f$ is one-to-one* onto *the set of isogeny classes of rational elliptic curves.*

The one-to-one-ness of $f \rightarrow E_f$ is obvious since $L(f, s)$ completely determines f. The onto-ness, however, is not. It asserts that *any* E over $\mathbb{Q}$ is isogenous to some E_f with f a rational primitive form of weight 2 such that $L(f, s) = L(E)$.

One consequence of Conjecture C is Conjecture B. Indeed suppose E has conductor N. By Conjecture C, there exists an f in $S_2(\Gamma_0(N))$ with E_f isogenous to E. Thus $L(E_f, s) = L(E, s)$ and Conjecture B follows.

Another consequence of Conjecture C is the *Isogeny Conjecture*. This asserts that $L(E, s) = L(E', s)$ *only if* E is isogenous to E'. Indeed Conjecture C produces an f and f' such that E(resp. E') is isogenous to E_f (resp. $E_{f'}$). Thus $L(E, s) = L(E', s)$ implies $L(E_f, s) = L(E_{f'}, s)$ which implies $L(f', s) = L(f, s)$, i.e., $f = f'$. Thus $E_f = E_{f'}$ and E is isogenous to E'. Serre [42] proves the Isogeny Conjecture (for arbitrary number fields) assuming only that the j-invariant of E or E' is not integral.

Remark 5.4. Conjecture C says there is a one-to-one correspondence between isogeny classes of rational elliptic curves of conductor N and rational normalized primitive forms in $S_2(\Gamma_0(N))$. The existence of this correspondence has not yet been established in general but all available experimental evidence supports it. For example there are no curves over $\mathbb{Q}$ of conductor N if $g_N = 0$. Furthermore computer searches for elliptic curves of small conductor have produced the right number of isogeny classes in all cases (cf. [2]).

Recent theoretical work on the classification of curves of given conductor also supports Conjecture C. In fact for certain N this classification essentially establishes the conjecture (cf. [33, 58]).

Note finally that Conjecture C follows from Conjecture B *if* the

Isogeny Conjecture is assumed. Indeed for E over $\mathbb{Q}$ Conjecture B produces an f in $S_2(\Gamma_0(N))$ with $L(E, s) = L(f, s)$. Thus $L(E, s) = L(E_f, s)$ and (by the Isogeny Conjecture) E is isogenous to E_f. Conjecture C also follows from Conjecture B if the map $E \to f_E$ is one-to-one. Indeed the one-to-one-ness of *this* map is equivalent to the Isogeny Conjecture.

Concluding Remark. Elliptic curves with complex multiplication are known to satisfy Conjecture B because Deuring showed they satisfy Conjecture A. Shimura [47] proves that such curves also arise as factors of the Jacobian $J_0(N)$; i.e., curves of "C.M. type" are "modular."

Further evidence for Conjectures B and C is described in Part III. There Conjecture B is reformulated and generalized in terms of the representation theory of GL(2) over an arbitrary global field.

II. Automorphic Forms and Cuspidal Representations

We explain somewhat leisurely how a representation π^f of $\mathrm{GL}(2, \mathbb{A})$ is attached to a cusp form f and how the zeta-function of f is understood in terms of Euler-factors attached to the local components of π^f. Much of this development is due to Jacquet and Langlands [23] (for more background and details, see [18]).

6. *Archimedean Theory*

We deal only with $\mathrm{GL}(2, \mathbb{R})$. Our point of departure is the well-known fact that every irreducible unitary representation of $\mathrm{SL}(2, \mathbb{R})$ is "admissible" in the following sense.

Consider the universal enveloping algebra of the complexification of the Lie algebra of $\mathrm{SL}(2, \mathbb{R})$. If π is realized on the Hilbert space H, and σ is an irreducible representation of $K = \mathrm{SO}(2)$, let $H(\sigma)$ denote the subspace of vectors v in H which transform according to σ. (Thus $\pi(K)v$ spans a finite-dimensional subspace of H equivalent to a finite number of copies of σ.) The algebraic direct sum

$$H^0 = \bigoplus_{\sigma} H(\sigma)$$

is dense in H and comprises the subspace of K-finite vectors. The crucial fact is that by differentiation π induces a representation of the enveloping algebra on the space H^0. This representation is algebraically irreducible since the unitary representation π is topologically irreducible. *It is* *"admissible" in the sense that its restriction to the Lie algebra of K decomposes into finite-dimensional representations with finite multiplicities.* (Equivalently, the dimension of $H(\sigma)$ is finite for each σ.)

Following Harish and Chandra and Jacquet and Langlands one focuses attention not on irreducible *unitary* representations of $G = \mathrm{GL}(2, \mathbb{R})$ but rather on irreducible *admissible* representations of an appropriate group algebra of G.

DEFINITION 6.1. Let $\mathscr{J}$ denote the universal enveloping algebra of the complexification of the Lie algebra of G. Let ϵ_- denote the Dirac measure at $\left[\begin{smallmatrix}-1 & 0\\ 0 & 1\end{smallmatrix}\right]$. Then the *Hecke group algebra of G* is by definition the direct sum

$$(G) = \mathscr{J} \oplus (\epsilon_-)*\mathscr{J}.$$

Observe that $\mathscr{H}(G)$ is an algebra (under convolution product) of distributions supported in the subgroup $\{\left[\begin{smallmatrix}\pm 1 & 0\\ 0 & 1\end{smallmatrix}\right]\}$ of G. It is the simplest substitute for the enveloping algebra of G which takes into account the fact that G has *two* connected components.

DEFINITION 6.2. Suppose π is a representation of the algebra $\mathscr{H}(G)$ on a complex vector space V. Then π is said to be *admissible* if its restriction to the Lie algebra of $K = O(2, \mathbb{R})$ decomposes into finite-dimensional representations with finite multiplicities.

Remark 6.3. Almost all the irreducible representations of $K = O(2, \mathbb{R})$ are two-dimensional. Suppose σ is any such representation of (the Lie algebra of) K and $V(\sigma)$ denotes the subspace of vectors in V which transform according to some multiple of σ. Then admissibility of (π, V) amounts to the assertion that

$$V = \underset{\substack{\sigma \\ (algebraic\ sum)}}{\bigoplus} V(\sigma)$$

with each $V(\sigma)$ *finite-dimensional.*

Our task now is to describe all the *irreducible* admissible representations up to equivalence. This task is simplified by the fact that all such representations are known to be subquotients of the following basic representations of $\mathscr{H}(G)$, the so-called *principal series representations.*

Let μ_1, μ_2 denote any quasi (i.e., not necessarily unitary) characters of $\mathbb{R}^\times$. Let $\mathscr{B}(\mu_1, \mu_2)$ denote the vector space of functions $\varphi(g)$ on G which are right K-finite and such that

$$\varphi\left(\begin{bmatrix} t_1 & * \\ 0 & t_2 \end{bmatrix} g\right) = \mu_1(t_1)\,\mu_2(t_2) |\, t_1/t_2 \,|^{1/2}\, \varphi(g)$$

for all $t_1, t_2 \in \mathbb{R}^\times$. According to the Iwasawa decomposition,

$$G = NA\,\mathrm{SO}(2),$$

where $A = \{[\begin{smallmatrix} t_1 & 0 \\ 0 & t_2 \end{smallmatrix}]\}$ and $N = \{[\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}]\}$. Therefore, each φ in $\mathscr{B}(\mu_1, \mu_2)$ is completely determined by its restriction to $\mathrm{SO}(2, \mathbb{R})$ (and in particular is infinitely differentiable since this restriction must be a trigonometric polynomial).

If X belongs to $\mathscr{J}$ we define (as usual)

$$\varphi * X(g) = (d/dt)\, \varphi(g \exp(-tX))|_{t=0}$$

and let $\check{X}$ denote $-X$. By $\rho(\mu_1, \mu_2)$ we denote the representation of $\mathscr{H}(G)$ on $\mathscr{B}(\mu_1, \mu_2)$ determined by

$$\rho(\mu_1, \mu_2)(X)\, \varphi = \varphi * \check{X}.$$

This representation is essentially induced from the one-dimensional representation

$$\begin{bmatrix} t_1 & * \\ 0 & t_2 \end{bmatrix} \to \mu_1(t)\, \mu_2(t)$$

of $B = NA$. It is admissible precisely because each φ in $\mathscr{B}(\mu_1, \mu_2)$ restricts to a trigonometric polynomial on $\mathrm{SO}(2, \mathbb{R})$. What is remarkable is that *every irreducible admissible representation of* $\mathscr{H}(G)$ *is a subquotient of some such* $\rho(\mu_1, \mu_2)$. Therefore the classification of irreducible admissible representations is reduced to the study of how (and when) these $\rho(\mu_1, \mu_2)$ decompose.

To analyze the reducibility of $\rho(\mu_1, \mu_2)$ one computes the action of certain Lie algebra elements on convenient basis elements of $\mathscr{B}(\mu_1, \mu_2)$. To this end, write $\mu_i(t) = (t)^{s_i}[\mathrm{sgn}(t)]^{m_i}$, where $m_i = 0$ or 1, and $s_i \in \mathbb{C}$. Then

$$\mu(t) = \mu_1\mu_2^{-1}(t) = |\, t \,|^s[\mathrm{sgn}(t)]^m,$$

with $s = s_1 - s_2$ and $m = m_1 - m_2$. For each $n \equiv m \pmod 2$, the function

$$\varphi_n\left(\begin{bmatrix} t_1 & * \\ 0 & t_2 \end{bmatrix}\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}\right) = \mu_1(t_1)\,\mu_2(t_2)|\,t_1/t_2\,|^{1/2}\, e^{-in\theta}$$

belongs to $\mathscr{B}(\mu_1, \mu_2)$ and the set $\{\varphi_n\}$ is obviously a basis for $\mathscr{B}(\mu_1, \mu_2)$.

Theorem 6.4. (a) *If* $\mu_1\mu_2^{-1}$ *is not of the form* $t \to t^p \operatorname{sgn}(t)$, *with* p *a nonzero integer, then* $\mathscr{B}(\mu_1, \mu_2)$ *is* irreducible *under the action of* $\mathscr{H}(G)$;

(b) *If* $\mu_1\mu_2^{-1}(t) = t^p \operatorname{sgn}(t)$, with $p > 0$, *then* $\mathscr{B}(\mu_1, \mu_2)$ *contains exactly one invariant subspace, namely,*

$$\mathscr{B}^s(\mu_1, \mu_2) = \{\ldots, \varphi_{-p-3}, \varphi_{-p-1}, \varphi_{p+1}, \varphi_{p+3}, \ldots\},$$

and the quotient $\mathscr{B}^f(\mu_1, \mu_2) = \mathscr{B}(\mu_1, \mu_2)/\mathscr{B}^s(\mu_1, \mu_2)$ *is finite-dimensional*;

(c) *If* $\mu(t) = t^p \operatorname{sgn}(t)$ with $p > 0$ *then the only invariant subspace of* $\mathscr{B}(\mu_1, \mu_2)$ *is*

$$\mathscr{B}^f(\mu_1, \mu_2) = \{\varphi_{p+1}, \varphi_{p+3}, \ldots, \varphi_{-p-3}, \varphi_{-p-1}\}.$$

The representation $\rho(\mu_1, \mu_2)$ will be denoted by $\pi(\mu_1, \mu_2)$ if it is irreducible; in case it is not, the obvious representation on the finite-dimensional space $\mathscr{B}^f(\mu_1, \mu_2)$ will still be denoted by $\pi(\mu_1, \mu_2)$. The representation on the *infinite*-dimensional subspace (or quotient) $\mathscr{B}^s(\mu_1, \mu_2)$ will be denoted by $\sigma(\mu_1, \mu_2)$ and viewed as a member of the *discrete series* for G. It is defined only when $\mu(t) = t^p \operatorname{sgn}(t)$ for some nonzero integer p. The representations $\pi(\mu_1, \mu_2)$ exhaust the so-called *principal series* for G.

Theorem 6.5. *Every irreducible admissible representation of* $\mathscr{H}(G)$ *is either a* $\pi(\mu_1, \mu_2)$ *or a* $\sigma(\mu_1, \mu_2)$; *the only equivalences between these representations are the following.*

$$\pi(\mu_1, \mu_2) \approx (\mu_2, \mu_1)$$

and

$$\sigma(\mu_1, \mu_2) \approx \sigma(\mu_2, \mu_1) \approx \sigma(\mu_1\eta, \mu_2\eta) \approx \sigma(\mu_2\eta, \mu_1\eta),$$

where $\eta(t) = \operatorname{sgn}(t)$.

Remark 6.6. If π is equivalent to the discrete series representation $\sigma(\mu_1, \mu_2)$ it can conveniently be indexed by the parameters $p = s_1 - s_2$ and $t = s_1 + s_2$. The significance of p is that the space of $\sigma(p, t)$ will contain the functions $\varphi_{p+1}, \varphi_{p+3}, \ldots$, but not the function φ_{p-1}. Thus $\sigma(p, t)$ is said to have *lowest weight* $p + 1$. The significance of t is that $\sigma(p, t)$ will be unitary (i.e., correspond to a unitary representation of G) if and only if t is pure imaginary. By contrast, a given principal series representation $\pi(\mu_1, \mu_2)$ will be unitary (in this same sense) iff both μ_1 and μ_2 are unitary, *or* just $s_1 + s_2$ is pure imaginary and $s_1 - s_2$ is real, nonzero, and between -1 and 1; $\pi(\mu_1, \mu_2)$ is then called a *continuous* series or a *complementary* series representation according as the first or second possibility occurs.

Concluding Remarks. To attach an L-factor to each admissible representation π of $\mathscr{H}(G)$ one introduces the *Whittaker model* of π. This is a space of functions $W(g)$ on G such that $W([\begin{smallmatrix}1 & x\\ 0 & 1\end{smallmatrix}]g) = e^{2\pi ix}W(g)$ for all $x \in \mathbb{R}$ and such that in this space the natural action of $\mathscr{H}(G)$ is equivalent to π. The terminology is apt since each function $f_W(t) = W([\begin{smallmatrix}t & 0\\ 0 & 1\end{smallmatrix}])$ actually defines a classical Whittaker function on $\mathbb{R}^x$. How the corresponding L and ϵ factors arise is explained in Section 8.

If π belongs to the discrete series it is often convenient to parametrize π by a complex quasi-character $\omega(z) = | z |^{2r-(m+n)} z^m\bar{z}^n$ with r complex and m and n two integers, one zero and the other nonnegative. Thus if π corresponds to ω, $\pi(\omega) = \sigma(\mu_1, \mu_2)$ with $\mu_1\mu_2(x) = | x |^{2r} \operatorname{sgn}(x)^{m+n+1}$ and $\mu_1\mu_2^{-1}(x) = x^{m+n} \operatorname{sgn}(x)$. In particular, $\pi(\omega)$ has lowest weight $m + n + 1$. The analog of this construction for p-adic fields (and their quadratic extensions) is explained in detail in Section 7 (cf. Theorem 7.3 in particular).

7. *p-Adic Theory*

Our purpose is to describe the irreducible admissible representations of GL$(2, F)$, where F is a local nonarchimedean field. We also collect some basic facts concerning these representations.

We start with some notation. Throughout this section, F will be a finite extension of the p-adic number field *or* a field of formal power series in one variable over a finite field. The symbol O_F will denote the ring of integers of F. The absolute value on F is defined by the relation $d(ax) = | a | \, dx$, where dx is an invariant measure on the additive group of F. The prime ideal of O_F, defined by $| a | < 1$, will be denoted by P_F. It is generated (say) by $\tilde{\omega}$, and O_F/P_F is a finite field with q

elements, q some power of p. The standard maximal compact (open) subgroup of G is

$$K = \mathrm{GL}(2, O_F).$$

Now G has no enveloping algebra of differential operators but there is a natural group algebra for G which is fundamental for its representation theory, namely the (*Hecke*) *group algebra* $\mathscr{H}(G)$ consisting of all locally constant compactly supported functions on G. (This is an algebra for the group convolution product

$$f*g(x) = \int_G f(xy^{-1})\, g(y)\, d^*y,$$

where d^*y denotes the Haar measure for G which assigns the measure 1 to K.)

Following Jacquet and Langlands [23], we say that a representation π of $\mathscr{H}(G)$ on a complex vector space V is *admissible* if for every v in V there is an f in $\mathscr{H}(H)$ such that $\pi(f)v = v$, and if every $\pi(f)$ maps V onto a finite-dimensional space. This definition of admissibility is motivated by the following considerations.

Suppose π is an irreducible *unitary* representation *of* G on some Hilbert space H. Then π induces a representation of $\mathscr{H}(G)$ through the formula

$$\pi(f) = \int_G f(g)\, \pi(g)\, d^*g,$$

and, as in the real case, $\pi(f)$ defines a representation of $\mathscr{H}(G)$ in the subspace of K-finite functions of H which is admissible in the above sense. However, *in contrast to the real case*, $\pi(g)$ itself acts in the space of K-finite vectors. Therefore it should not seem surprising that *for p-adic groups* (*and admissible representations*) *the correspondence between representations of G and representations of the group algebra of G is completely transparent*. Thus the following definition.

DEFINITION 7.1. Suppose π is a representation *of* G on a complex vector space V (the space of K-finite vectors of some unitary G-space, for example). Then π is said to be *admissible* if (i) the stabilizer in G of each v in V is an open subgroup of K, and (ii) the subspace of V fixed by any open subgroup of K is finite-dimensional. Equivalently, the restriction of π to K contains any given irreducible representation of K at most finitely many times.

Schur's lemma holds for all irreducible admissible representations, unitary or not. In particular, the restriction of π to the center Z of $\mathrm{GL}(2, F)$ defines a quasi-character of F, the so-called *central character of* π. Every finite-dimensional irreducible admissible representation is automatically one-dimensional and of the form $\chi(\det g)$ with χ a quasi-character of F^x.

The infinite-dimensional irreducible admissible representations of $G = \mathrm{GL}(2, F)$ are either subrepresentations of some principal series representation or else supercuspidal representations. To describe the principal series, let μ_1, μ_2 be any two quasi-characters of $F^\times$ and let $\mathscr{B}(\mu_1, \mu_2)$ denote the space of all locally constant functions φ on G such that

$$\varphi\left(\begin{bmatrix} t_1 & * \\ 0 & t_2 \end{bmatrix} g\right) = \mu_1(t_1)\, \mu_2(t_2) | \, t_1/t_2 \, |^{1/2} \varphi(g)$$

for all $t_1, t_2 \in F^\times$. The group G acts on $\mathscr{B}(\mu_1, \mu_2)$ through right translations and the resulting representation of G is called a *principal series representation* (at least when it is irreducible) and denoted by $\rho(\mu_1, \mu_2)$. Each such representation is seen to be admissible.

THEOREM 7.2. *The representation $\rho(\mu_1, \mu_2)$ is irreducible except when $\mu(x) = \mu_1\mu_2^{-1}(x) = | \, x \, |$ or $| \, x \, |^{-1}$. If $\mu(x) = | \, x \, |^{-1}$, then $\mathscr{B}(\mu_1, \mu_2)$ contains a one-dimensional invariant subspace and the representation induced on the resulting factor space is irreducible. If $\mu(x) = | \, x \, |$, then $\mathscr{B}(\mu_1, \mu_2)$ contains an irreducible invariant subspace of codimension* 1. (*The* irreducible *representations $\rho(\mu_1, \mu_2)$ are denoted by $\pi(\mu_1, \mu_2)$ and called* principal series representations; *if $\mu_1\mu_2^{-1}(x) = | \, x \, |$ or $| \, x \, |^{-1}$, the resulting irreducible infinite-dimensional subquotients of $\rho(\mu_1, \mu_2)$ are denoted by $\sigma(\mu_1, \mu_2)$ and called* special representations; *the one-dimensional quotients are denoted by $\pi(\mu_1, \mu_2)$.*)

Two representations $\pi(\mu_1, \mu_2)$ and $\pi(\nu_1, \nu_2)$ are equivalent if and only if $(\mu_1, \mu_2) = (\nu_1, \nu_2)$ or (ν_2, ν_1). An analogous result holds for the special representations. The question remains: How are the *supercuspidal* representations of G obtained (those which do not appear as subrepresentations of $\rho(\mu_1, \mu_2)$)? The answer is that (almost all) these representations arise as subrepresentations of the various *Weil representations* of G defined as follows.

Fix a nontrivial additive character τ of F. For each separable quadratic extension L of F, let $x \to x^\sigma$ denote the nontrivial element of $\mathrm{Gal}(L/F)$,

$q(x) = xx^\sigma$ the corresponding norm, and $\mathrm{tr}(x) = x + x^\sigma$. Let $\mathscr{S}(L)$ denote the Schwartz–Bruhat space of locally constant compactly supported functions on L and $r^\tau(s)$ the (unique) representation of $\mathrm{SL}(2, F)$ in $\mathscr{S}(L)$ such that

$$r^\tau\left(\begin{bmatrix} 1 & u \\ 0 & 1 \end{bmatrix}\right) \Phi(x) = \tau(uq(x))\, \Phi(x)$$

and

$$r^\tau\left(\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\right) \Phi(x) = \gamma \int_L \Phi(y)\, \tau(\mathrm{tr}(x^\sigma y))\, dy.$$

Here γ is a Gauss sum and dy is a suitably normalized Haar measure on L. Since $r^\tau(s)$ commutes with the natural action of the norm 1 group of L in $\mathscr{S}(V)$, $r^\tau(s)$ decomposes according to the characters of $L^\times$.

More precisely, for each quasi-character ω of L the subspace of functions in $\mathscr{S}(L)$ satisfying

$$\Phi(xh) = \omega^{-1}(h)\, \Phi(x)$$

for all $h \in L$ with $q(h) = 1$ is invariant for $r^\tau(s)$ and the resulting representation $r_\omega{}^\tau(s)$ extends to a representation of $G_+ = \{g \in \mathrm{GL}(2, F)\colon \det(g) \in q(L^\times)\}$. Note that G_+ has index 2 in $\mathrm{GL}(2, F)$.

THEOREM 7.3. *Let $\pi(\omega)$ denote the representation of* $\mathrm{GL}(2, F)$ *induced from $r_\omega{}^\tau$. Then*

(i) *$\pi(\omega)$ is irreducible, admissible, and independent of τ;*

(ii) *$\pi(\omega)$ is supercuspidal if there is no character δ of $F^\times$ such that $\omega = \delta \circ q$;*

(iii) *if the residual characteristic of F is odd, and ω and L vary as above,* all *supercuspidal representations of* $\mathrm{GL}(2, F)$ *thus arise.*

For further details see [18] or [23]. If the residual characteristic of F is even, supercuspidal representations of $\mathrm{GL}(2, F)$ which are not of the form $\pi(\omega)$ will be called "irregular." In general, supercuspidal representations are often also called *absolutely cuspidal.* They are characterized among the irreducible admissible representations of $\mathrm{GL}(2, F)$ as those whose matrix coefficients are compactly supported modulo the center Z. They can also be characterized in terms of their Whittaker models (cf. Sect. 8 below).

We close this section with some facts relating to the decomposition of the restriction to K of an arbitrary irreducible admissible representation of G. Of course one knows a priori that any such decomposition contains a given irreducible of K at most finitely many times. But it is a more delicate question to ask *exactly* how many times.

DEFINITION 7.4. An irreducible admissible representation π of G is called *class* 1 or *spherical* if its restriction to K contains the identity representation at least once.

THEOREM 7.5. *An (infinite-dimensional) irreducible admissible representation π of G is class* 1 *if and only if $\pi = \pi(\mu_1, \mu_2)$ for some pair of unramified characters μ_1, μ_2 of $F^\times$ and π is not a special representation. In this case the identity representation is contained* exactly *once in π. Furthermore, if $\varphi_0(g)$ denotes any function in the (one-dimensional) subspace of K-invariant vectors in $\mathscr{B}(\mu_1, \mu_2)$, and $\tau_{\tilde{\omega}}$ denotes the Hecke operator corresponding to convolution over G with the characteristic function of the double coset $K\left[\begin{smallmatrix}\tilde{\omega} & 0\\ 0 & 1\end{smallmatrix}\right]K$, then $\varphi_0(g)$ is an eigenfunction of $\tau_{\tilde{\omega}}$, and*

$$\varphi_0 * \tau_{\tilde{\omega}}(g) = q^{1/2}(q^{s_1} + q^{s_2})\, \varphi_0(g)$$

if $\mu_i(x) = |x|^{s_i}$. (Recall that $|\tilde{\omega}| = q^{-1}$.)

If π is not class 1 there is the following useful result (due to Miyake and Casselman; see, for example, [18]).

THEOREM 7.6. *Let π denote any irreducible admissible (infinite-dimensional) representation of G with central character ψ. Then there is a largest ideal $c(\pi)$ of O_F such that the space of vectors v with*

$$\pi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) v = \psi(a) v$$

for all

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(c(\pi)) = \left\{ \begin{bmatrix} a & b \\ c & a \end{bmatrix} \in K : c \equiv 0 \ (\mathrm{mod}\ c(\pi)) \right\}$$

is not empty. Furthermore, this space has dimension 1. *The ideal $c(\pi)$ is called the* conductor *of π.*

If π is class 1, then $c(\pi)$ is O_F. In general, we have the table:

Representation	Conductor
$\pi = \pi(\mu_1, \mu_2)$ (principal series)	(Conductor of μ_1) (Conductor of μ_2)
$\pi = \sigma(\mu_1, \mu_2)$ (special representations)	(Conductor of $\mu)^2$ *or* ωO_F
π supercuspidal	$(\tilde{\omega}^N O)$, $\quad N \geqslant 2$

Recall that the conductor of any quasi-character μ of $F^\times$ is the largest ideal $\tilde{\omega}^n O_F$ such that μ is trivial on the subgroup $1 + \tilde{\omega}^n O_F$ of $O_F{}^\times$. For the special representation $\pi(\mu_1, \mu_2)$, the conductor is $\tilde{\omega} O_F$ if and only if μ is unramified.

Definition 7.7. An admissible representation π of G on a complex space V will be called *preunitary* (or simply *unitary*) if there exists on V an invariant positive-definite hermitian form.

If π is preunitary, the operators $\pi(g)$ can be extended to unitary operators on the Hilbert space obtained by completing V with respect to this form and the result is a unitary representation in the classical sense. Furthermore, this completion will be topologically irreducible if and only if (π, V) is algebraically irreducible.

Theorem 7.8. *The* (*pre*-)unitary *irreducible admissible representations of G are*

(i) *the supercuspidal representation with* unitary *central character*;

(ii) *the principal series representations* $\pi(\mu_1, \mu_2)$ *with both* μ_1 *and* μ_2 *unitary*;

(iii) *the representations* $\pi(\mu_1, \mu_2)$ *of the principal series for which* $\mu_2(x) = \overline{\mu_1(x)}^{-1}$ *and* $\mu(x) = | x |^\sigma$, $0 < \sigma < 1$;

(iv) *the special representations with unitary central character.*

This result is entirely analagous to the real situation. Therefore the representations in (ii) and (iii) are called *continuous* (respectively, *complementary*) series representations of G.

8. *L-Functions and ε-Factors*

Suppose F is $\mathbb{R}$ or $\mathbb{Q}_p$, ψ is a nontrivial character of F, and π is an irreducible admissible representation of $\mathrm{GL}(2, F)$. The factors $L(s, \pi)$ and $\epsilon(s, \pi, \psi)$ defined in this section play a crucial role in the global functional equation of Hecke. One way to introduce them is to study the zeta-functions attached to the Whittaker model of π.

THEOREM 8.1 (Existence and Uniqueness of the Local Whittaker Model). *Suppose π is an irreducible admissible (infinite-dimensional) representation of* GL(2, F). *Then in the space of locally constant functions on G such that*

$$W\left(\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} g\right) = \psi(x)\, W(g) \tag{25}$$

($x \in F$, $g \in G$), *there is a* unique *subspace $\mathscr{W}(\pi)$* (*the* Whittaker space) *which is invariant for the right action of G and equivalent* (*as a G-module*) *to π.*

Theorem 8.1 is also valid for $F = \mathbb{R}$ (cf. the concluding remarks of Sect. 6). In this case one considers irreducible admissible representations of the group algebra $\mathscr{H}(G)$ and solutions of (25) which are C^∞ and such that $W(\left[\begin{smallmatrix} t & 0 \\ 0 & 1 \end{smallmatrix}\right]) = O(|\,t\,|)^N$ as $t \to \infty$.

For F nonarchimedean, the functions $f_W(t) = W(\left[\begin{smallmatrix} t & 0 \\ 0 & 1 \end{smallmatrix}\right])$ are locally constant on F^x and vanish outside some compact subset of F. The space they comprise is called the *Kirillov space of π*. It contains the space of locally constant compactly supported functions *on F^x* with codimension 2 if π belongs to the principal series, codimension 1 if π is special, and codimension zero if π is supercuspidal. In general, if $\xi(x)$ belongs to the Kirillov space of π, $\pi(\left[\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right])\, \xi(x) = \psi(bx)\, \xi(ax)$.

Let π denote an irreducible admissible representation of G and $\mathscr{W}(\pi)$ its Whittaker space. Suppose χ is a unitary character of $F^\times$, $g \in G$, $W \in \mathscr{W}(\pi)$, and s a complex number. Then the *local zeta-function* attached to (g, χ, W) is defined by the formula

$$\zeta(g, \chi, W, s) = \int_{F^x} W\left(\begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} g\right) \chi(a) |\, a\,|^{s-1/2}\, d^x a. \tag{26}$$

Caution. Although $\xi(a) = W(\left[\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right] g)$ is a relatively well-behaved function on $F^\times$, it is not necessarily locally constant of F. Therefore the function of s defined by (26) is *not* necessarily a zeta-function of the type studied by Tate (cf. [19, Chap. 8.1]).

In the Theorem below, $\pi \otimes \chi$ denotes the tensor product of π with the one-dimensional representation $\chi(\det g)$. Also $\check{\pi}$ denotes the contragredient of π defined by $\check{\pi}(g) = {}^t\pi(g^{-1})$ (for vectors $\check{v}$ in the dual space of π fixed by an open subgroup of G).

THEOREM 8.2. (i) *The integral defining* $\zeta(g, \chi, W, s)$ *converges for* s *with sufficiently large real part*;

(ii) *There exists an* Euler factor $L(x, \chi \otimes \pi)$ *with the property that*

$$\zeta(g, \chi, W, s)/L(s, \chi \otimes \pi)$$

is an entire function of s for every g, χ, and W, *and such that*

$$\zeta(1, \chi, W^0, s) = L(s, \chi \otimes \pi) \tag{27}$$

for an appropriate choice *of* $W^0 \in \mathscr{W}(\pi)$;

(iii) *The function* $\zeta(g, \chi, W, s)$ *possesses an analytic continuation to the whole s-plane and satisfies the functional equation*

$$\frac{\zeta(g, \chi, W, s)}{L(s, \chi \otimes \pi)} \epsilon(s, \psi, \pi \otimes \chi) = \frac{\zeta(wg, \chi^{-1}\omega_\pi^{-1}, W, 1-s)}{L(1-s, \chi^{-1} \otimes \pi)},$$

where $\epsilon(s, \psi, \chi \otimes \pi)$ *is independent of* g *and* W, ω_π *is the central character of* π, *and* $w = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$.

Remarks 8.3 (*Concerning the Statement of Theorem* 8.2).

(i) By an *Euler factor* we understand a function of s of the form $P^{-1}(q)$ where P is a polynomial such that $P(0) = 1$ and $q = |\tilde{\omega}|^{-1}$ if v is finite. For archimedean places v, the factor $L(s, \pi)$ will be a product of certain gamma functions to be specified below. In either case $L(s, \pi)$ *is unique*. (Indeed if $L(s, \pi)$ and $L^*(s, \pi)$ are two Euler factors satisfying the conditions of the theorem their quotient is an entire function without zeros.)

(ii) Suppose two irreducible admissible representations π^1 and π^2 of G induce the same central character. Then π^1 and π^2 are equivalent if and only if

$$\frac{\epsilon(s, \psi, \chi \otimes \pi^1) L(1-s, \chi^{-1} \otimes \check{\pi}^1)}{L(s, \chi \otimes \pi^1)} = \frac{\epsilon(s, \psi, \chi \otimes \pi^2) L(1-s, \chi^{-1} \otimes \check{\pi}^2)}{L(s, \chi \otimes \pi^2)}$$

for all χ. In other words, the factors $L(s, \chi \otimes \pi)$ and $\epsilon(s, \psi, \chi \otimes \pi)$ uniquely determine π among all representations with given central character. Some of these factors can be explicitly described as follows.

Suppose first that F is nonarchimedean. If μ is a quasi-character of $F^\times$, set $L(s, \mu)$ equal to $(1 - \mu(\tilde{\omega})q^{-s})^{-1}$ if μ is unramified, and equal to 1, otherwise.

TABLE A

π	$L(s, \pi)$	$\epsilon(s, \psi, \pi)$
$\pi = \pi(\mu_1, \mu_2)$ (principal series or one-dimensional)	$L(s, \mu_1)L(s, \mu_2)$	$\epsilon(s, \mu_1)\epsilon(s, \mu_2)$ (equals 1 if μ_1 and μ_2 are unramified!)
$\pi = \sigma(\mu_1, \mu_2)$ (special representation)	$L(\mu_1, s)$	$\dfrac{\epsilon(s, \mu_1)\epsilon(s, \mu_2)L(1 - s, \mu_1^{-1})}{L(s, \mu_2)}$
π supercuspidal	1	unimportant to us

Now suppose $F = \mathbb{R}$. If $\mu(x) = |x|^r(\operatorname{sgn}(x))^m$ is a quasi-character of $\mathbb{R}^\times$, set $L(s, \mu)$ equal to $\pi^{-1/2(s+r+m)} \Gamma^{(s+r+m)/2}$; set $\epsilon(s, \psi, \mu)$ equal to $(i \operatorname{sgn}(u))^m |u|^{s+r-1/2}$ if $\psi(x) = 2^{\pi i x}$. If $\omega(z) = |z|^{2r} z^m \bar{z}^n$ is a quasi-character of $\mathbb{C}^x$ (as at the end of Sect. 6) set $L(s, \omega)$ equal to $2(2\pi)^{-(s+r+m+n)}$ $\Gamma(s + r + m + n)$, and $\epsilon(s, \psi, \omega)$ equal to $i^{m+n}\omega(u) |u|^{2s-1}$.

TABLE B

π	$L(s, \pi)$	$\epsilon(s, \psi, \pi)$
$\pi = \pi(\mu_1, \mu_2)$ (principal series or finite-dimensional)	$L(s, \mu_1)L(s, \mu_2)$	$\epsilon(s, \psi, \mu_1)\epsilon(s, \psi, \mu_2)$
$\pi = \sigma(p, t)$ (discrete series representation of the form $\pi(\omega)$)	$L(s, \omega)$	$i \operatorname{sgn}(u)\epsilon(s, \psi, \omega)$

Concluding Remarks. (i) One can regard $L(s, \chi \otimes \pi)$ as the g.c.d. for the family of meromorphic local zeta-functions $\zeta(g, W, \chi, s)$. The privileged Whittaker function whose Mellin transform is *precisely* $L(s, \chi \otimes \pi)$ (in the sense of Eq. (27)) is (roughly speaking) the "lowest weight" vector in $\mathscr{W}(\pi)$. More precisely, if F is nonarchimedean, $W^0(g)$ corresponds to the vector v in Theorem 7.6; if $F = \mathbb{R}$, and $\pi = \pi(p, t)$, $W^0(g)$ is the function with weight vector $p + 1$.

(ii) Tables A and B include L and ϵ-factors for the *finite*-dimensional representations $\pi(\mu_1, \mu_2)$. However, since Whittaker models do not exist for such representations, the assignment of these factors results from other considerations (cf. [23, Sect. 13]; and Sect. 11 of this paper).

9. *Cuspidal Representations*

Our task is to realize primitive cusp forms on $\Gamma_0(N)$ as privileged representations of GL(2).

Let $\mathbb{A}$ denote the ring of adeles of $\mathbb{Q}$ and $Z_\infty{}^+$ the subgroup of $G_\mathbb{A} = \mathrm{GL}(2, \mathbb{A})$ consisting of positive real scalar matrices at infinity and the identity elsewhere. For each prime p and integer N let $K_p(N)$ denote the compact subgroup of $G_p = \mathrm{GL}_2(\mathbb{Q}_p)$ defined by

$$K_p(N) = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z}_p) \colon c \equiv O(N)\right\}.$$

The quotient space

$$X = Z_\infty{}^+ G_\mathbb{Q} \backslash G_A$$

has finite volume with respect to the natural right-invariant measure inherited from the unimodular group $G_\mathbb{A}$. In fact, the map

$$x + iy \leftrightarrow \begin{bmatrix} y^{1/2} & xy^{-1/2} \\ 0 & y^{-1/2} \end{bmatrix} \tag{28}$$

provides an isomorphism from $Z_\infty{}^+ G_\mathbb{Q} \backslash G_\mathbb{A} / \mathrm{SO}_2(\mathbb{R}) \prod_{p<\infty} K_p(N)$ to the modular variety $\Gamma_0(N) \backslash H$ and $\mathrm{SO}_2(\mathbb{R}) \prod_{p<\infty} K_p(N)$ is compact.

Let T denote the right regular representation of $G_\mathbb{A}$ in $L^2(X)$. Since the measure on X is right invariant T is a *unitary* representation of $G_\mathbb{A}$. Let T_0 denote the restriction of T to the subspace $L_0{}^2(X)$ consisting of functions in $L^2(X)$ satisfying the cuspidal condition

$$\int_\mathbb{A} \varphi\left(\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} g\right) dx = 0$$

for almost every $g \in G_\mathbb{A}$. Roughly speaking, T_0 exhausts the discrete spectrum of T.

More precisely, let $L_E{}^2(X)$ denote the subspace of $L^2(X)$ spanned by functions of the form $\chi(g) = \chi(\det g)$ with χ a character of $\mathbb{R}_+{}^\times \mathbb{Q}^\times \backslash \mathbb{A}^\times$ (recall X has finite measure). Then the restriction of T to $L_0{}^2(X) \oplus L_E{}^2(X)$ exhausts the discrete spectrum of T (i.e., the orthocomplement of $L_0{}^2(X) \oplus L_E{}^2(X)$ has no *minimally* invariant subspace for the action of $G_\mathbb{A}$ and T restricted to this orthocomplement decomposes *continuously*).

We say that an irreducible unitary representation π of $G_\mathbb{A}$ is *automorphic* if π occurs in T and *cuspidal* if it occurs in T_0. This terminology is chosen because certain special cuspidal representations of $G_{\mathbb{A}}$ correspond one-one to normalized primitive forms of weight k.

Indeed any irreducible unitary representation π of $\mathrm{GL}(2, \mathbb{A}) = \prod_{p\leqslant\infty} \mathrm{GL}(2, \mathbb{Q}_p)$ can be factored as an infinite tensor product of local representations π_p of $\mathrm{GL}(2, \mathbb{Q}_p)$ almost all of which are class 1. Moreover, these local representations are completely determined by π. Thus we write $\pi = \bigotimes_{p\leqslant\infty} \pi_p$, a restricted infinite tensor product. This factorizability of irreducible unitary representations of $G_{\mathbb{A}}$ was first established by Gelfand, Graev, and Pyatetskii-Shapiro and later generalized by Jacquet and Langlands [23] (see [18, Sect. 4.C] for further discussion).

Now suppose π is an irreducible unitary representation of $G_{\mathbb{A}}$ satisfying the following properties.

(a) $\pi = \bigotimes_{p\leqslant\infty} \pi_p$ occurs in T_0;

(b) the "conductor" $\prod_{p\leqslant\infty} c(\pi_p)$ of π is N;

(c) π_∞ is the unique discrete series representation $\pi_\infty{}^k$ of $\mathrm{GL}(2, \mathbb{R})$ which is trivial on the center and has lowest weight vector k; and

(d) for all $p \nmid N$, π_p is equivalent to the class 1 representation $\pi_p(\mu_1, \mu_2)$.

Then in the space of π in $L^2(X)$ there is (essentially) one function $\varphi(g)$ which, via the isomorphism (28), corresponds to a primitive form f_φ in $S_k(\Gamma_0(N))$. Moreover, $T(p)f_\varphi = p^{(k-1)/2}(\mu_1^{-1}(p) + \mu_2^{-1}(p))f_\varphi$ for each $p \nmid N$. Thus certain cuspidal representations indeed correspond to classical forms in $S_k(\Gamma_0(N))$. The Ramanujan–Petersson conjecture (cf. [11, 16]) asserts that μ_1 and μ_2 above are actually unitary, i.e., $\pi_p(\mu_1, \mu_2)$ is a continuous (as opposed to complementary) series representation of $\mathrm{GL}(2, \mathbb{Q}_p)$ (see [18, Sect. 5.B] for details).

In general, an arbitrary cuspidal representation π of $G_{\mathbb{A}}$ no longer corresponds to a form in $S_k(\Gamma_0(N))$, or even $S_k(\Gamma_0(N), \psi)$, because π_∞ need not belong to the discrete series. At worst, however, π will correspond to a real-analytic cusp form in the sense of Maass. In particular, if π has conductor N, the function $f(z)$ corresponding to the priviledged one-dimensional subspace of the space of π will be a form on $\Gamma_0(N)$. It is by considering arbitrary cuspidal representations that Jacquet and Langlands [23] simultaneously treat real analytic *and* holomorphic forms of *arbitrary* level.

Now suppose

$$f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}$$

is an arbitrary normalized primitive form in $S_k(\Gamma_0(N))$. Then $f(z)$ lifts to a function $\varphi_f(g)$ on X via the isomorphism (28). More precisely, suppose $g = \gamma g_\infty k_0$ with $g \in G_{\mathbb{A}}$, $\gamma \in G_{\mathbb{Q}}$, $g_\infty = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{GL}^+(2, \mathbb{R}) = \{g \in \mathrm{GL}(2, \mathbb{R})\colon \det(g) > 0\}$, and $k_0 \in \prod_{p<\infty} K_p(N)$. Then $\varphi_f(g) = f(g_\infty(i))\, j(g_\infty, i)^{-k}$, with $g_\infty(i) = (ai + b)/(ci + d)$, and $j(g_\infty, i) = (ci + d)(\det g_\infty)^{-1/2}$.

The fact that $f(z)$ is automorphic of weight k and level N implies that $\varphi_f(g)$ is right invariant for $\prod_{p<\infty} K_p(N)$ and that is transforms under $\mathrm{SO}_2(\mathbb{Q}) = \{\left[\begin{smallmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{smallmatrix}\right]\}$ according to the character $e^{ik\theta}$. The fact that $f(z)$ is cuspidal in the classical sense implies that $\varphi_f(g)$ belongs to $L_0^2(X)$. What remains to show is that the right translates of $\varphi_f(g)$ span an infinite-dimensional subspace $H(f)$ of $L^2(X)$ isomorphic to some cuspidal representation.

Let π_f denote the unitary representation of $G_{\mathbb{A}}$ generated by $H(f)$. Then π_f is the direct sum of irreducible unitary representations π^i each one of which occurs in T_0. Moreover, according to the factorizability result quoted above, each π^i can be written as $\bigotimes_{p<\infty} \pi_p{}^i$.

Since every right translate of $\varphi_f(g)$ shares the same eigenvalue for the so-called Casimir operator of $G_\infty = \mathrm{GL}(2, \mathbb{R})$, the infinite component of each summand π^i of π_f is completely determined. Indeed this component must be the discrete series representation $\sigma(p, t)$ with $p = k - 1$ and $t = 0$. On the other hand, for each $p \nmid N$, the Hecke operator $T(p)$ acting on f corresponds to the convolution operator τ_p acting on $\varphi_f(g)$ (cf. Theorem 7.3 with $\tilde{\omega} = p$). Therefore, since each π^i contains a function which is right $K_p(N)$-invariant and an eigenfunction of τ_p with eigenvalue a_p, the p-component of each summand of π_f (with $p \nmid N$) is the unique class 1 representation $\pi_p(\mu_1, \mu_2)$ of $\mathrm{GL}(2, \mathbb{Q}_p)$ which has trivial central character and satisfies

$$a_p = p^{(k-1)/2}(\mu_1^{-1}(p) + \mu_2^{-1}(p)). \tag{29}$$

We know now that each summand of π_f has the same local factor for $p = \infty$ and all p not dividing N. But according to the discussion above, each distinct summand corresponds to a distinct form in $S_k(\Gamma_0(N))$. Therefore, since $S_k(\Gamma_0(N))$ is well known to be finite-dimensional, π_f has only finitely many summands. To conclude that π_f is actually irreducible we need only apply the following two "multiplicity 1" results. The first, due to Casselman and Miyake, asserts that two irreducible constituents of T_0 coincide as soon as they agree at all but finitely many *finite* places (cf. [18, Theorem 5.14]). The second, due to

Jacquet and Langlands [23], says that any given irreducible π occurs *at most once* in T_0.

A detailed discussion of the correspondence $f \leftrightarrow \pi_f$ appears in [18]; numerous examples are given there as well as in [9, 13].

10. *Hecke Theory à la Jacquet and Langlands*

Let G denote (for the moment only) an arbitrary reductive algebraic group defined over $\mathbb{Q}$. Following Langlands [26], one attaches to G, and each finite Galois extension E of $\mathbb{Q}$, a complex group ${}^LG^0$, and a semidirect product ${}^LG = {}^LG^0 \times \mathrm{Gal}(E/\mathbb{Q})$, the "$L$-group" of G. One also introduces the notion of "cuspidal representation" for G. For $G = \mathrm{GL}(2)$, "cuspidal representation" is as in Section 9, and ${}^LG^0 = \mathrm{GL}(2, \mathbb{C})$.

In general, one conjecture of [26] is that one can attach to each cuspidal representation $\pi = \otimes_p \pi_p$ of G, and each finite-dimensional holomorphic representation r of ${}^LG^0$, an eulerian product

$$L(s, \pi, r) = \prod_p L(s, \pi_p, r),$$

indexed by the primes of $\mathbb{Q}$. If $\check{r}$ denotes the contragradient of r, one wants $L(s, \pi, r)$ and $L(s, \pi, \check{r})$ to admit meromorphic continuations to the whole s-plane. Moreover, if $\psi = \prod \psi_p$ is any nontrivial additive character of $\mathbb{A}$ trivial on $\mathbb{Q}$, one wants to introduce factors $\epsilon(s, \pi_p, r, \psi_p)$, almost always equal to 1, so that $\epsilon(s, \pi, r) = \prod_p \epsilon(s, \pi_p, r, \psi_p)$ is independent of ψ, and $L(s, \pi, r)$ satisfies the functional equation

$$L(s, \pi, r) = \epsilon(s, \pi, r) L(1 - s, \pi, \check{r}).$$

If r is irreducible and nontrivial, $L(s, \pi, r)$ should actually be entire (at least when $G = GL(n)$, $n > 1$).

It is precisely these conjecture (among others) which Jacquet and Langlands resolve affirmatively for $G = \mathrm{GL}(2)$ and r the standard representation of $\mathrm{GL}(2, \mathbb{C})$ by itself. Our purpose here is to summarize their results and quickly indicate their connection with the classical theory of Hecke.

How does Hecke's theory attach a Dirichlet series to f in $S_k(N, \psi)$? According to the concluding remark of Section 3, one simply takes the Mellin transform of f along the line $\{iy : y > 0\}$. That is,

$$L(s, f) = \int_0^\infty f(iy)\, y^{s-1}\, dy. \tag{30}$$

(Strictly speaking, the *Dirichlet series* attached to f is $D(s, f) = (2\pi)^s \Gamma(s)^{-1} L(s, f)$. However, our interest is in the *L-function* $F(s, f)$, a simple modification of $D(s, f)$.)

To understand how one might generalize Hecke's construction, it is helpful to rewrite (30) in the framework of the adele group of GL(2). As in Section 9, let $\varphi_f(g)$ denote the function on $G_{\mathbb{A}} = \mathrm{GL}(2, \mathbb{A})$ corresponding to f in $S_k(\Gamma_0(N))$. Then

$$L(s + ((k-1)/2), f) = \int_{\mathbb{Q}^x \backslash \mathbb{A}^x} \varphi\left(\begin{bmatrix} y & 0 \\ 0 & 1 \end{bmatrix}\right) |\, y\,|^s \, d^*y.$$

(Recall $\mathbb{A}^\times \,\|\, \mathbb{Q}^\times \mathbb{R}_+ (\prod_{p<\infty} 0_p{}^\times)$.) Now exploit the Fourier expansion of $f(iy)$. Using adeles,

$$\varphi\left(\begin{bmatrix} y & 0 \\ 0 & 1 \end{bmatrix}\right) = \sum_{\xi \in \mathbb{Q}^x} W_\varphi\left(\begin{bmatrix} \xi y & 0 \\ 0 & 1 \end{bmatrix}\right). \tag{31}$$

Here $W_\varphi(g)$, the "first" Fourier coefficient of $\varphi([\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}] g)$, is defined by the integral $\int_{\mathbb{Q}\backslash\mathbb{A}} \varphi([\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}] g)\, \overline{\psi(x)}\, dx$. Substituting (31) in (30) yields

$$L(s + ((k-1)/2), f) = \int_{\mathbb{A}^x} W_\varphi\left(\begin{bmatrix} y & 0 \\ 0 & 1 \end{bmatrix}\right) |\, y\,|^s \, d^*y.$$

But $W_\varphi(g)$ is right K-finite, C^∞ as a function of G_∞, satisfies

$$W_\varphi \left[\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} g\right) = \psi(x)\, W(g)$$

for all $x \in \mathbb{A}$, and generates a space of functions on which the (convolution) action of $G_{\mathbb{A}}$ is equivalent to π_f (i.e., $L(s, f)$ is the Mellin transform of a privileged function in the *global Whittaker space* $\mathscr{W}(\pi_f)$ of π_f).

So suppose now that $\pi = \otimes \pi_p$ is an *arbitrary* irreducible unitary representation of $G_{\mathbb{A}}$. By the local theory of Section 8, each π_p possesses a unique Whittaker model $\mathscr{W}(\pi_p)$. Thus the space of functions on $G_{\mathbb{A}}$ generated by those of the form $W(g) = \prod W_p(g_p)$, with $W_p = W_p{}^0$ for almost every p, provides a Whittaker model $\mathscr{W}(\pi)$ for π. Following Hecke, Jacquet and Langlands [23] essentially introduce $L(s, \pi, 1)$ (henceforth denoted $L(s, \pi)$) as the Mellin transform of an appropriate W in $\mathscr{W}(\pi)$. What they actually do to get this privileged W is piece together the local functions $W_p{}^0$ of Theorem 8.2.

To state the main theorem of Jacquet and Langlands we set

$$\epsilon(\pi, \chi, s) = \Pi \epsilon(\pi_p, \chi_p, s)$$

for each grössencharacter $\chi = \prod \chi_p$ of F. Since π_p is almost always class 1 this product is actually a finite product by Table A. We also put

$$L(s, \chi \otimes \pi) = \prod_p L(s, \chi_p \otimes \pi_p).$$

This product converges for Re(s) sufficiently large since for almost every v, $L(s, \chi_p \otimes \pi_p)$ is of the form

$$[1 - \mu_p \chi_p(\tilde{\omega}_p)\, p^{-s}]^{-1}[1 - \nu_p \chi_p(\tilde{\omega}_v)\, q^{-s}]^{-1},$$

with $| \mu_p(x)| = | \nu_p(x)| = | x |^{\pm\sigma/2}$, $0 \leqslant \sigma \leqslant 1$.

THEOREM 10.1. *Suppose* $\pi = \otimes \pi_p$ *has central character* ψ. *Then* π *occurs in* T_0 if and only if $L(s, \chi \otimes \pi)$ *satisfies the following properties for every grossencharacter* χ *of* F:

(i) $L(s, \chi \otimes \pi)$ *extends to an entire function bounded in vertical strips*; *and*

(ii) $L(s, \chi \otimes \pi)$ *satisfies the functional equation*

$$L(s, \chi \otimes \pi) = \epsilon(\pi, \chi, s) L(1 - s, \chi^{-1} \otimes \check{\pi}), \tag{32}$$

where $\check{\pi}(g) = \psi^{-1}(g)\, \pi(g)$.

The thrust of this theorem is more than that the L-functions attached to constituents of T_0 enjoy the properties listed above. It is that these properties characterize the constituents of T_0 among the arbitrary irreducible representations of $G_{\mathbb{A}}$. In other words, both Hecke's theorem and Weil's "converse theorem" are generalized in one fell swoop. The precise connection is this. If π is the cuspidal representation of $G_{\mathbb{A}}$ corresponding to the normalized primitive form f in $S_k(\Gamma_0(N))$ then

$$L(s, \pi) = L(s + ((k - 1)/2), f) \tag{33}$$

and (32) reduces to (21).

Note that $1/L(\pi_p, s)$ is a polynomial of degree 2 in p^{-s} if and only if π_p has conductor 0. The group theoretic significance of f in (33) is that φ_f generates the one-dimensional space of functions in the space of π which transform under $K(N) = \prod_{p<\infty} K_p(N)$ according to the central character of π and transform under $\mathrm{SO}_2(\mathbb{R})$ according to the character $e^{ik\theta}$.

Since we have discussed only the case of $\mathbb{Q}$ we hasten to add that Jacquet and Langlands work over *arbitrary* global fields. Of course in this generality their results need no longer have significant classical content. Nevertheless, it is in this context that Weil's conjecture can be attacked most successfully.

III. Elliptic Curves and Cuspidal Representations

Let K now denote a global field and G the group GL(2) regarded as an algebraic group over K. Let $G_{\mathbb{A}}$ and G_K denote the adelic and K-rational points of G. The right regular action of $G_{\mathbb{A}}$ in $L^2(G_K\backslash G_{\mathbb{A}})$ then provides a unitary representation of $G_{\mathbb{A}}$ which decomposes as a generalized direct sum of irreducible constituents.

Let $\bar{K}$ denote an algebraic closure of K and $\mathrm{Gal}(\bar{K}/K)$ the corresponding Galois group (below we deal with Weil groups). The general reciprocity laws conjectured by Langlands asserts that to any two-dimensional representation σ of $\mathrm{Gal}(\bar{K}/K)$ there should be associated an irreducible constituent $\pi(\sigma)$ of $L^2(G_K\backslash G_{\mathbb{A}})$. Moreover, this correspondence should be a product of local correspondences.

To see this, for each place v of K, let K_v and G_v denote the corresponding completions of K and G. Let $\mathrm{Gal}(\bar{K}_v/K_v)$ denote the corresponding Galois group (again, it should be the Weil group). To each two-dimensional representation σ_v of $\mathrm{Gal}(\bar{K}_v/K_v)$ one should be able to associate an irreducible representation $\pi_v(\sigma_v)$ of G_v. But there are embeddings of $\mathrm{Gal}(\bar{K}_v/K_v)$ into $\mathrm{Gal}(\bar{K}/K)$ (unique up to conjugation). Thus a representation σ of $\mathrm{Gal}(\bar{K}/K)$ gives rise to a σ_v for each v and $\pi(\sigma)$ should be the restricted tensor product $\bigotimes \pi_v(\sigma_v)$.

The correspondences $\sigma_v \leftrightarrow \pi_v(\sigma_v)$ and $\sigma \leftrightarrow \pi(\sigma)$ are natural in that they preserve Euler factors. Nevertheless, one might hope for a more profound realization of them. This is what much of the recent work of Deligne and Langlands concerns. Indeed the fundamental result of Eichler–Shimura theory, recast in the mold of representation theory, says precisely that a correspondence which arises naturally in the arithmetic of elliptic modular curves coincides with the correspondence $\sigma \leftrightarrow \pi(\sigma)$ just described.

For simplicity we deal primarily with the field $K = \mathbb{Q}$. This case already suffices for a treatment of the classical theory and at times considerably eases our exposition. Nevertheless, if it is appropriate to deal, say, with a function field, or a local field with positive characteristic, we shall not hesitate to do so even if some of the terms involved have not been carefully defined.

11. *Weil Groups and the Galois Classification of Representations of* GL(2)

Let K denote $\mathbb{Q}_p$ or $\mathbb{R}$. Roughly speaking, according to Langlands, the set of n-dimensional representations of the *Weil group* of K should correspond one-to-one to the set of irreducible admissible representations of $\mathrm{GL}(n, K)$. Moreover, the corresponding L and ϵ factors (defined for the unramified representations by Artin and Hecke (at least when $n = 2$)) should coincide.

If $n = 1$ this conjecture amounts to the fundamental reciprocity law of local abelian class field theory. For $n = 2$ the situation is already considerably more complicated and not yet completely resolved. The difficulty is that p-adic fields possess many nontrivial extensions. Since the corresponding theory for the reals is almost transparent by comparison we sketch this case first.

The only extension of $K = \mathbb{R}$ is $\mathbb{C} = \bar{K}$. In this case the *Weil group* W_K is the group generated by $\bar{K}^\times$ and an element e with $e^2 = -1$ and $eze^{-1} = \bar{z}$ for $z \in \mathbb{C}^\times = \bar{K}^\times$. If ν denotes the homomorphism of W_K to $\mathbb{R}^\times$ given by $\nu(e) = -1$, $\nu(z) = z\bar{z}$, the quasi-characters of W_K are all of the form $\mu \circ \nu$ for μ some quasi-character of $\mathbb{R}^\times$.

An arbitrary *two*-dimensional representation σ of W_K is then either

(1) reducible and the direct sum of two one-dimensional representations of the form $\mu_i \circ \nu$; or

(2) irreducible and induced from a quasi-character ω of $\mathbb{C}^\times$ with $\omega \neq \omega \circ c$ for c complex conjugation in $\mathbb{C}$.

In case (2) we have $\omega(z) = | z |^{2r-(m+n)} z^m z^n$, with r complex and m and n two integers one zero and the other nonnegative. The corresponding L-functions are $L(\sigma, s) = L(\mu_1, s) L(\mu_2, s)$ and $L(\sigma, s) = L(\omega, s)$, respectively. Recall that $L(\mu_i, s) = \pi^{-1/2(s+r_i+m_j)} \Gamma((s + r_i + m_i)/2)$ if $\mu_i(x) = | x |^{r_i} \operatorname{sgn}(x)^{m_i}$ and $L(\omega, s) = (2\pi)^{-(s+r+((m+n)/2))} \Gamma(s + r + ((m + n)/2))$ if $\omega(z) = | z |^{2r-(m+n)} z^m \bar{z}^n$. Similarly, if $\psi(x) = \exp(2\pi(-1)^{1/2} ux)$, $\epsilon(s, \sigma, \psi)$ equals $\epsilon(s, \mu_1, \psi) \epsilon(s, \mu_2, \psi)$ if $\sigma = \mu_1 \circ \nu \oplus \mu_2 \nu$, and equals $((-1)^{1/2} \operatorname{sgn} u) \epsilon(s, \omega, \psi \circ tr)$, otherwise. Here $\epsilon(s, \mu_j, \psi) = ((-1)^{1/2} \operatorname{sgn} u)^m \times | u |^{s+r-1/2}$ and $\epsilon(s, \omega, \psi \circ tr) = i^{m+n} \omega(u) | u |^{2s+2r-1}$ (cf. [18, p. 194] and Sect. 8 of this paper).

For each possible σ above one can define an irreducible admissible representation $\pi(\sigma)$ of $\mathrm{GL}(2, K)$ whose corresponding L and ϵ factors coincide with those of σ and whose central character is $\det \sigma$. Namely, in case (1) above, $\pi(\sigma)$ is the (possibly finite-dimensional) principal series representation $\pi(\mu_1, \mu_2)$. In case (2), $\pi(\sigma)$ is $\pi(\omega)$, the discrete series representation belonging to the ω-component of the basic Weil representation; more precisely, in the notation of Section 6, $\pi(\omega) = \sigma(\mu_1, \mu_2)$, with $\mu_1\mu_2(x) = |x|^{2r}(\operatorname{sgn} x)^{m+n+1}$ and $\mu_1\mu_2^{-1}(x) = x^{m+n}(\operatorname{sgn} x)$. Thus $\pi(\omega)$ is a discrete series representation with lowest weight vector $m + n + 1$.

As already noted, the situation for a p-adic field K is more complicated precisely because K possesses many nontrivial finite extensions. Let us therefore fix K to be $\mathbb{Q}_p$ and let k denote the residue class field of $\mathbb{Q}_p$. Let $\bar{K}$ denote an algebraic closure of K, $\bar{k}$ the closure of k, and φ the automorphism $x \mapsto x^p$. Recall that $\mathrm{Gal}(\bar{k}/k)$ is isomorphic to $\hat{\mathbb{Z}}$ and topologically generated by φ.

To deal simultaneously with all finite extensions of K we introduce the (*absolute*) *Weil group* W_K. This is the (dense) subgroup of $\mathrm{Gal}(\bar{K}/K)$ consisting of all elements whose image in $\mathrm{Gal}(\bar{k}/k)$ is a power of φ. The *inertia* subgroup of $\mathrm{Gal}(\bar{K}/K)$ is the subgroup of W_K whose image in $\mathrm{Gal}(\bar{k}/k)$ is trivial. To topologize W_K we require that I be an *open* subgroup and that it have induced on it the usual (profinite topology). In particular, if $W(\bar{k}/k)$ denotes the subgroup of $\mathrm{Gal}(\bar{k}/k)$ generated by φ, we have

$$\begin{tikzcd}
0 \arrow[r] & I \arrow[r] \arrow[dd, equal] & W_K \arrow[r] \arrow[dd, hook] & W(\bar{k}/k) \arrow[r] \arrow[dd, hook] \arrow[rrd, no head, "\cong"] & 0 & \\
& & & & & \mathbb{Z} \arrow[dd, hook] \\
0 \arrow[r] & I \arrow[r] & \mathrm{Gal}(\bar{K}/K) \arrow[r] & \mathrm{Gal}(\bar{k}/k) \arrow[r] \arrow[rrd, no head, "\cong"'] & 0 & \\
& & & & & \hat{\mathbb{Z}}.
\end{tikzcd}$$

For more details, see [15].

Note that the topology for W_K just described is stronger than the topology it inherits from $\mathrm{Gal}(\bar{K}/K)$. Thus W_K has more continuous n-dimensional representations than $\mathrm{Gal}(\bar{K}/K)$. Following Deligne, we call any element of W_K or $\mathrm{Gal}(\bar{K}/K)$ whose image in $\mathrm{Gal}(\bar{k}/k)$ is φ^{-1} the *geometric Frobenius*. We denote such an automorphism by F.

Definition 11.1. By an n-dimensional representation of W_K we understand a pair (σ, N) such that

(i) σ is a *continuous* homomorphism from W_K to $\mathrm{GL}(n, \mathbb{C})$, in particular, σ is trivial on some open (finite-index) subgroup of I;

(ii) σ is *semi-simple*, i.e., $\sigma(F)$ is diagonalizable for each Frobenius F; and

(iii) N is a nilpotent element of $M(n, \mathbb{C})$ such that $\sigma(w)\, N\sigma(w)^{-1} = \omega_1(w)N$ for all $w \in W_K$.

Here ω_1 denotes the quasi-character of W_K which via the isomorphism of class field theory corresponds to the normalized absolute value on $K^\times$. Since we normalize this isomorphism to take F to a uniformizing variable $\tilde{\omega}$, $\omega_1(F) = p^{-1}$.

The notions of equivalence, irreducibility, direct sum, quotient and tensor product for W_F-representations are defined in the usual way; in particular, $(\sigma, N) \otimes (\sigma', N') = (\sigma \otimes \sigma', N \otimes 1 + 1 \otimes N')$. If σ is trivial on I, σ is said to be *unramified.*

PROPOSITION 11.2 [15, p. 93]. *All irreducible representations* (σ, N) *of* W_K *are of the form* $(\sigma, 0)$ *with* σ *irreducible.*

Note that one-dimensional representations of W_K are just quasi-characters. But by class field theory, W_K^{ab} is isomorphic to $K^\times$, i.e., one-dimensional representations of W_K are indistinguishable from quasi-characters *of* $K^\times$.

In general, when σ is n-dimensional, we shall often abbreviate (σ, N) by σ even when σ is not irreducible. This notation will be abusive because the pair (σ, N) may be indecomposable even when σ itself is completely reducible. A case in point is the n-dimensional *special representation* $\mathrm{sp}(n) = (\sigma, N)$ defined as follows. Fix a canonical basis $\{e_0, e_1, \ldots, e_{n-1}\}$ for $\mathbb{C}^n$ and define (σ, N) by $\sigma(w)e_i = \omega_1{}^i(w)e_i$, $Ne_{n-1} = 0$, and $Ne_i = e_{i+1}$ $(0 \leqslant i < n - 1)$. Then (σ, N) is indecomposable even though σ is completely reducible. In fact, we have

PROPOSITION 11.3 [13, p. 93]. *Every indecomposable representation of* W_K *is of the form* $\rho \otimes \mathrm{sp}(n)$ *with* ρ *irreducible.*

Remark 11.4. The notion of W_K-representation given by Definition 11.1 seems first to have been made explicit by Deligne. Why this sophisticated notion is needed will become clear below. Roughly speaking, the usual notion of W_K-representation is too restrictive to bring into play the *special representations* of GL(2, K). Indeed these representations correspond naturally to two-dimensional *l-adic* representations of W_K and such representations correspond not to complex representations of W_K in the familiar sense but rather to complex representations of the form $\rho \otimes \mathrm{sp}(2)$. Thus Langlands' conjecture relating each representation of GL(2, K) to one of W_K fails unless "W_K-representation" is understood in the sense of Definition 11.1. The precise conjecture is

CONJECTURE 11.5. (a) *There is a one-to-one correspondence* $\sigma \leftrightarrow \pi(\sigma)$ *between the set of equivalence classes of all two-dimensional representations of* W_K *and the set of equivalence classes of all irreducible admissible representations of* GL(2, K);

(b) *The correspondence* $\sigma \leftrightarrow \pi(\sigma)$ *preserves L and* ϵ *factors in the obvious sense.*

Although the L-factor attached to (σ, N) is simple to describe, the ϵ-factor is not. The L-factor is $\det(Id - \sigma_I(F)\, p^{-s})^{-1}$ with σ_I the restriction of σ to the subspace of ker N left fixed by $\sigma(I)$. In particular, $L(\sigma, s)$ has degree 2 if $N = 0$ and σ is unramified. To define $\epsilon(s, \sigma, \psi)$ one first introduces a function $\epsilon(\sigma, \psi)$ depending only on (σ, N) and ψ (for details, see [9, Sect. 2; 15, Sects. 4, 5, 8]). The complete condition of part (b) of Conjecture 11.5 is then that for each quasi-character χ of $K^\times$,

$$\begin{aligned}
\pi(\sigma)\left(\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}\right) &= \det \sigma(a) I, \\
L(s, \chi \otimes \pi(\sigma)) &= L(s, \chi \otimes \sigma), \\
L(s, \chi^{-1} \otimes \check{\pi}(\sigma)) &= L(s, \chi^{-1} \otimes \check{\sigma}), \\
\epsilon(s, \chi \otimes \pi(\sigma), \psi) &= \epsilon(s, \chi \otimes \sigma, \psi).
\end{aligned}$$

The remainder of this section is devoted to summarizing all that is known (at the moment) concerning Conjecture 11.5. Note that the above conditions (by virtue of Remark 8.3(ii)) imply that $\pi(\sigma)$ is uniquely determined by σ.

The significance of the continuity assumption on (σ, N) in Definition 11.1 is that σ must factor through a *finite* extension of K. More precisely, if E is a finite Galois extension E of K, there is a *fundamental class* in $H^2(\mathrm{Gal}(E/K), E^\times)$ and a canonical extension

$$1 \to E^x \to W_{E/K} \to \mathrm{Gal}(E/K) \to 1,$$

with $W_{E/K}$ the *relative Weil group of E over K* (for details, see [3, 54]). According to Shafarevich [38, 45, 57] this extension satisfies (and is determined by) the following property. There is a homomorphism s from $W_{E/K}$ to $\mathrm{Gal}(E_{ab}/K)$ such that the diagram

$$\begin{tikzcd}
E^x \arrow[r] \arrow[d, "c"] & W_{E/K} \arrow[r] \arrow[d, "s"] & \mathrm{Gal}(E/K) \arrow[d] \\
\mathrm{Gal}(E_{ab}/E) \arrow[r] & \mathrm{Gal}(E_{ab}/K) \arrow[r] & \mathrm{Gal}(E/K)
\end{tikzcd}$$

commutes. Here E_{ab} denotes the maximal abelian extension of E and c is the injection of local class field theory. From this description of $W_{E/K}$ it follows that there is a canonical surjection

$$\alpha_E : W_K \rightarrow W_{E/K}.$$

Moreover, every (continuous) representation of W_K determines one of $W_{E/K}$ for E sufficiently large. In particular, from the point of view of representation theory, it suffices to deal with the *relative* Weil groups over K. Note that $W_{K/K} = K^\times$.

EXAMPLE 11.6. (i) Suppose μ_1, μ_2 are two quasi-characters of $K^\times$ and σ is a representation of W_K equivalent to the representation

$$w \rightarrow \begin{bmatrix} \mu_1(\alpha_K(w)) & 0 \\ 0 & \mu_2(\alpha_K(w)) \end{bmatrix}.$$

Then set $\pi(\sigma)$ equal to $\pi(\mu_1, \mu_2)$. Recall that $\pi(\sigma)$ will be one-dimensional if $\mu_1\mu_2^{-1}(x) = |x|$ or $|x|^{-1}$.

(ii) Suppose E is a quadratic extension of K, ω is a quasi-character of $E^\times = W_{E/E} \subset W_{E/K}$ which does not factor through the norm map $N_{E/K}$, and σ is the two-dimensional representation of $W_{E/K}$ induced from ω. Then set $\pi(\sigma)$ equal to the absolutely cuspidal representation $\pi(\omega)$ referred to in Section 7.

The correspondence $\sigma \leftrightarrow \pi(\sigma)$ described in Example 11.6 is easily seen to preserve L- and ϵ-factors. Thus it is natural to ask: Which representations σ and $\pi(\sigma)$ are excluded from it? According to [15, Proposition 3.1.4] every irreducible two-dimensional representation of W_K is induced (as above) from a quasi-character ω of a quadratic extension *provided the residual characteristic of K is odd.* On the other hand, this same restriction on K implies that every absolutely cuspidal representation of GL(2, K) is of the form $\pi(\omega)$. Thus we have

PROPOSITION 11.7. *Suppose $K = \mathbb{Q}_p$ with $p \neq 2$. Then Conjecture 11.5 is true.*

Indeed in this case the correspondonce $\sigma \leftrightarrow \pi(\sigma)$ provided by Example 11.6 misses only the "special" representations, i.e., the representations $\mu \otimes \mathrm{sp}(2)$ of W_K and the representations $\sigma(\mu, \mu \mid x \mid^{-1})$ of GL(2, K). Thus pairing these representations in the obvious way yields the proposition.

For $\mathbb{Q}_2$ the problem is that there exist "irregular" absolutely cuspidal representations, i.e., absolutely cuspidal representations *not* of the form $\pi(\omega)$. Equivalently, there exist two-dimensional irreducible W_K-representations *not* induced from a quasi-character of a quadratic extension. In either case, these "extraordinary" representations are only finite in number. Thus one should be able to inspect them case by case to reach the desired conclusion. On the Galois side the requisite classification was essentially obtained by Weil [56]. The "extraordinary" representations are apparently now being carefully studied by Henniart (work in progress).

On the GL(2) side a complete classification of the absolutely cuspidal representations has been obtained by Kutzko [24] (see all Casselman [8]). The representations of the compact subgroups of $GL(2, K)$ needed to induce these representations have all recently been investigated by Nobs and Wolfhart and Kutzko. According to Cartier, the entire question should be settled soon. A description of the extraordinary representations of PGL(2, $\mathbb{Q}_2$) has been announced by E. A. Neklyudova (*Functional Anal. Appl.* **9** (1975), 75–77).

Concluding Remarks. Jacquet and Langlands [23] prove that one can indeed attach to each two-dimensional representation σ of $W_{\mathbb{Q}_2}$ the appropriate $\pi(\sigma)$ *provided* Artin's conjecture is true. Their methods are global and are explained in Section 12 below. Tying this together with results of Drinfeld (*Math. Sbornik* **94** (1974), 594–627), Deligne subsequently established the desired bijection.

12. *Conjectures of Artin and Langlands*

Suppose K is a global field, $\bar{K}$ is a separable closure of K, and E is a finite Galois extension of K. The (*absolute*) *Weil group* W_K is defined in [54]. In the function field case it is described as in the local theory but in the number field case its construction is less straightforward. Suffice it to say that in the latter case W_K is disconnected and its quotient by the connected component of the identity is precisely Gal($\bar{K}/K$).

The (*relative*) *Weil group* $W_{E/K}$ is an extension of Gal(E/K) by the idele class group of E. As in the local theory, $W_{E/K}$ is a canonical quotient of the absolute Weil group W_K . In particular, each continuous finite-dimensional representation of W_K actually defines a representation of

$W_{E/K}$ for some appropriate E. So once again, from the point of view of representation theory, it suffices to deal with the relative Weil groups $W_{E/K}$.

If v is any place of K, let any extension of v to E also be denoted by v. For each place v there is a homomorphism from $W(E_v/K_v)$ to $W_{E/K}$ which is completely determined up to inner automorphism. Thus a continuous finite-dimensional representation σ of W_K defines a representation σ_v of W_{E_v/K_v} which is uniquely determined up to isomorphism.

Using the local factors of Section 8 one can follow Artin and Weil by attaching to σ a global L-function

$$L(s, \sigma) = \prod_v L(s, \sigma_v).$$

This function is initially defined only in some right half-plane $\operatorname{Re}(s) > s_0$. However, according to Artin [3] and Brauer (*Ann. of Math.* **48** (1947), 502–514) it extends to a meromorphic function defined on all of $\mathbb{C}$ and it satisfies a functional equation of the form

$$L(s, \sigma) = \epsilon(s, \sigma) L(1 - s, \check{\sigma}). \tag{34}$$

Here σ is the contragredient of σ.

The crucial result of Langlands [27] is that the "root number" $\epsilon(s, \sigma)$ can be expressed as a product of local constants. More precisely, given σ, and a nontrivial character $\psi = \prod_v \psi_v$ of $K\backslash\mathbb{A}$, the factors $\epsilon(\sigma_v, \psi_v, s)$ are such that $\epsilon(\sigma_v, \psi_v, s) = 1$ for almost all v, the product $\prod_v \epsilon(\sigma_v, \psi_v, s)$ is independent of ψ, and

$$\epsilon(\sigma, s) = \prod_v \epsilon(\sigma_v, \psi_v, s). \tag{35}$$

CONJECTURE 12.1 (Artin). *$L(\sigma, s)$ is entire if σ is irreducible and nontrivial.*

CONJECTURE 12.2 (Langlands). *If σ is a two-dimensional irreducible representation of W_K,*

$$\pi(\sigma) = \bigotimes_v \pi_v(\sigma_v)$$

is a cuspidal representation of $G_{\mathbb{A}}$.

The correspondence alluded to in Conjecture 12.2 has already been established for σ induced from quasi-characters of a quadratic extension of K. This is [23, Proposition 12.1]. The corresponding form $\pi(\sigma)$ is a generalization of the theta-series attached to binary quadratic forms in the classical theory of Hecke and Maass (for more details and references, see [18, Sect. 7]).

For arbitrary σ the representation $\pi(\sigma)$ is not even defined unless Conjecture 11.5 is assumed. Also implicit in Conjecture 12.2 is the fact that for almost all v, σ_v is unramified and $\pi_v(\sigma_v)$ is class 1 for almost all v. In [23], Conjecture 12.2 is proved *assuming* the truth of Artin's conjecture. The proof uses (34), (35), and a refinement of Jacquet and Langlands' converse to Hecke theory (cf. [23, Corollary 11.6, Theorem 12.2]). Note that Artin's conjecture *is* true *for function fields* (this was proved along with the Riemann-hypothesis). Therefore Conjecture 12.2 is a real theorem in this case. In fact, what falls out of the proof of this result is the following.

PROPOSITION 12.3 (cf. [23, Proposition 12.6]). *Suppose Artin's conjecture is true for K. Then to each place v of K, and each two-dimensional representation of W_{K_v}, one can associate an irreducible representation of* GL$(2, K_v)$ *so that the corresponding ϵ and L factors are preserved. In particular, if K_v is a local field of positive characteristic, the correspondence $\sigma_v \to \pi_v(\sigma_v)$ (alluded to in Conjecture* 11.5) *exists.*

As already noted, it follows from subsequent (unpublished) work of Deligne's that Conjecture 11.5 is true for local fields of positive characteristic, and indeed for arbitrary fields, provided Artin's conjecture is always true.

In general, the conjectured correspondence $\sigma \to \pi(\sigma)$ provides an analog of the abelian reciprocity law for nonabelian extensions of $\mathbb{Q}$ whose Galois group has a faithful two-dimensional representation. Thus the goal is to prove Conjecture 12.2 *directly* and then deduce Artin's conjecture *from it* (rather than the other way around). This is what Artin did for GL(1). Dramatic progress in this direction for GL(2) has recently been made by Deligne and Serre [16] and Langlands [29] but much remains to be done (see Sect. 15 for further discussion of this problem).

13. *Weil's Conjecture Reformulated*

For K an arbitrary global field, and E an elliptic curve over K, the zeta-function of E has been defined in [53]. When gamma factors for the (possibly nonexistent) archimedean places of K are included this zeta-function will be denoted $L(E, s)$.

CONJECTURE D. *If E is an elliptic curve over K there exists a cuspidal representation $\pi(E)$ of $G_{\mathbb{A}}$ with the property that*

$$L(\pi(E), s - 1/2) = L(E, s).$$

In case K is a function field this conjecture has already been proved by Deligne [15]. In this case $L(E, s)$ can be shown to be entire by some general results of Grothendieck. The difficult step is to establish the correct functional equations so that the converse theorem to Hecke theory can be applied (as in the proof of Conjecture 12.2). The idea is that $L(E, s)$ may be regarded as an Artin L-function attached not to a complex representation of W_K but to a strictly compatible system of *l-adic* representations. These representations arise naturally from the arithmetic of E (see below). Moreover, their ϵ- and L-factors piece together as desired to recapture the global data (for details, see [15]).

In general, Conjecture D generalizes Conjecture B. Indeed from (33) with $k = 2$ it follows that Conjecture D reduces to Conjecture B when E is elliptic over $\mathbb{Q}$. But if Conjecture B is true, and $\zeta(E, s) = \sum_{n=1}^{\infty} a_n n^{-s}$, then the primitive form corresponding to $\pi(E)$ must be $f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}$. Thus Conjecture B can be restated as follows.

CONJECTURE B′. *Let E be elliptic over $\mathbb{Q}$ with conductor N and zeta-function $\sum_{n=1}^{\infty} a_n n^{-s}$. Then the function*

$$f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}$$

is a normalized primitive form in $S_2(\Gamma_0(N))$.

To formulate a representation theoretic version of this conjecture one needs to define $\pi(E)$ directly in terms of the reduced curves $\bar{E}_p$. This is what Langlands does in [26]. Since the construction is significant in its own right and useful in Section 14 of this paper we sketch it briefly below. For simplicity, we once again suppose $K = \mathbb{Q}$. For the case of an arbitrary number field, see [26].

Suppose first that p is such that the j-invariant of E is p-integral. For precisely such primes E has "potential good reduction" in the sense of

Serre and Tate, i.e., good reduction over some extension K_p of $\mathbb{Q}_p$. For $l \neq p$, let $V_l(E)$ denote the Tate module of E over $\mathbb{C}_l$ and let $\sigma_{p,l}$ denote the corresponding l-adic representation of W_{K_p}. From [44] it follows that $\sigma_{p,l}$ lifts to a two-dimensional *complex* representation σ_p which is independent of l. In this case $\pi_p(E)$ may be defined to be the representation $\pi_p(\sigma_p)$ given by Conjecture 11.5. Note that if E actually has good reduction at p, then $\pi_p(E)$ will be class 1. More precisely, good reduction at p implies that σ_p is the direct sum of two *unramified* characters μ_1, μ_2, with $\mu_1\mu_2^{-1}(x) \neq | x |$ or $| x |^{-1}$; consequently $\pi(\sigma_p) = \pi(\mu_1, \mu_2)$. (In general, good reduction at p is equivalent to the fact that $V_l(E)$ is unramified at p for all $l \neq p$; cf. [50, Theorem 4].)

Now suppose p is such that $j(E)$ is *not* p-integral (this is possible for only finitely many p, but is automatic if $\bar{E}_p$ has a node). The corresponding l-adic representation $\sigma_{p,l}$ of W_{K_p} in $H_l^1(E)$ (the l-adic cohomology space dual to $V_l(E)$) is then of the form

$$w \to \begin{bmatrix} \mu_1(w) & * \\ 0 & \mu_2(w) \end{bmatrix}.$$

Here μ_1 and μ_2 are quasi-characters of $K_p^\times$ which take values in $\mathbb{Q}$ (hence $\mathbb{C}$) and satisfy $\mu_1\mu_2^{-1}(x) = | x |^{-1}$ (for details, see [42, Appendix]). The crucial ingredient is Tate's theory of ultrametric theta-functions, i.e., Tate's model for an elliptic curve with nonintegral j-invariant.

In case p is such that $j(E)$ is not p-integral set $\pi_p(E)$ equal to the special representation $\sigma_p(\mu_1, \mu_2)$. Note that this correspondence is consistent with Conjecture 11.5. Indeed the l-adic representation $\sigma_{p,l}$ (which is reducible but not indecomposable) may be replaced by the complex representation $\sigma_p = (\sigma_p, N) = \mathrm{sp}(2) \otimes \mu_1 | x |^{-1}$. Thus $\pi_p(E)$ is just $\pi_p(\sigma_p)$ in the sense of Conjecture 11.5. Note too that $L(\sigma_p, s) = L(\sigma_{p,l}, s) = L(\pi_p(\sigma_p), s) = L(\pi_p(E), s)$ is always of the form $(1 - a_p p^{-s})^{-1}$.

Finally suppose $p = \infty$. In this case set $\pi_p(E)$ equal to $\pi_p(\sigma_p)$, where σ_p is the representation of $W_{\mathbb{R}}$ induced from the character $z \to | z |^{-1}z$ of $\mathbb{C}^\times$. According to Section 6, $\pi_p(\sigma_p)$ is then a discrete series representation π_∞^2 with lowest weight vector 2.

If we now piece together the local maps

$$E \to \pi_p(E)$$

just defined in terms of the local correspondences $\sigma_p \leftrightarrow \pi_p(\sigma_p)$, we obtain a global correspondence

$$E \to \pi(E) = \bigotimes_p \pi_p(E)$$

and a representation–theoretic interpretation of Conjecture B'.

CONJECTURE D′. *If E is an elliptic curve over $\mathbb{Q}$, then the representation $\pi(E)$ is a cuspidal representation of* GL(2, $\mathbb{A}$) *and*

$$L(\pi(E), s - \tfrac{1}{2}) = L(E, s).$$

Clearly $\pi(E)$ corresponds to a normalized primitive form of *weight* 2. Additional conditions on $\pi(E)$ are imposed by the rationality of E and the Riemann-hypothesis for $\bar{E}_p$.

If f is the primitive form associated to E by Conjecture B it is natural to ask how the corresponding cuspidal representation of $G_{\mathbb{A}}$ is related to $\pi(E)$. Of course if Conjectures B′ and D′ are true these representations must coincide because their L-functions do. But without assuming this it does not seem to be a trivial matter to compare these representations locally. One problem is that if σ_2 is an "extraordinary" irreducible representation of $W_{\mathbb{Q}_2}$, $\pi(\sigma_2)$ is an irregular supercuspidal representation of GL(2, $\mathbb{Q}_2$). Perhaps work in progress will soon resolve this ambiguity.

14. *Eichler–Shimura Theory Revisited*

Recall Shimura's correspondence between rational primitive forms in $S_2(\Gamma_0(N))$ and elliptic curve over $\mathbb{Q}$. The principal result is that the zeta-function of the curve agrees with the zeta-function of the form at all places not dividing N. What happens at the remaining places was essentially left open because too little was known about the reduction of $X_0(N)$ at these places.

In 1970 Deligne obtained the first general results about the bad reduction of $X_0(N)$. Encouraged by these results Langlands proposed the refinement of Eichler–Shimura theory described below. Experts can consult [28] for the original statement of results (such people should not be reading this paper). Others should see [9, 21].

Suppose $\pi = \otimes_p \pi_p$ is the cuspidal representation of $G_{\mathbb{A}}$ corresponding to the rational normalized primitive form f in $S_2(\Gamma_0(N))$. Following Shimura, one associates to f the rational elliptic curve E_π, and following Langlands, one associates to E_π the representation $\pi(E_\pi) = \otimes_p \pi_p(E_\pi)$

as in Section 13. What then is the relation between $\pi(E_\pi)$ and the original representation π? In particular, what is the relation between the local factors at the ends of the path below?

$$\begin{tikzcd}
 & \pi_f = \bigotimes \pi_p \arrow[r, "\textit{Conjecture 11.5}", "(\textit{Section 11})"'] & \{\sigma_p\} \\
f \arrow[ur] \arrow[dr] & & \\
 & E_f \arrow[r, "\textit{Serre-Tate}", "(\textit{Section 13})"'] & \{\sigma_p{}'\}.
\end{tikzcd}$$

CONJECTURE 14.1. *The local representations $\{\sigma_p\}$ and $\{\sigma_p{}'\}$ coincide; i.e., for each prime p,*

$$\pi_p = \pi_p(E_\pi). \tag{36}$$

Note that $\pi_\infty = \pi_\infty(E_\pi)$ by definition.

The full thrust of this conjecture is that the correspondence $\pi_p \leftrightarrow \sigma_p$ is completely natural from the point of view of geometry and the arithmetic of elliptic curves.

For $p \nmid N$, Conjecture 14.1 is equivalent to the Eichler–Shimura theory. Indeed $p \nmid N$ implies π_p is a class 1 representation of GL(2, $\mathbb{Q}_p$) corresponding to some pair of unramified quasi-characters (μ_1, μ_2) of $\mathbb{Q}_p{}^\times$. Thus from (29) it follows that

$$T(p) f_\pi = a_p f = p^{1/2}(\mu_1^{-1}(p) + \mu_2^{-1}(p)) f_\pi ,$$

i.e., the p-factor of the zeta-function of π is $(1 - a_p p^{-s} + p^{1-2s})^{-1}$. But $p \nmid N$ also implies that E_π has good reduction at p. Thus the corresponding representation $\sigma_p{}'$ of the Weil group is the direct sum of two unramified characters ν_1, ν_2, which by Eichler–Shimura theory must be μ_1, μ_2 (i.e., the representation $\pi_p(\sigma_p{}')$ is precisely π_p). A comprehensive treatment of Eichler–Shimura theory from the point of view of representation theory and modern algebraic geometry is given by Pyatetskii-Shapiro [34].

One can also verify Conjecture 14.1 directly in case π corresponds to the unique normalized primitive form in $S_2(\Gamma_0(11))$. In this case π_{11} is the special representation associated to the pair of quasi-characters $(|x|^{-1/2}, |x|^{1/2})$ and π_p is class 1 for all $p \neq 11$. The representation $\pi_{11}(E_\pi)$ of Section 10 is a special representation equivalent to π_{11} because the reduction of E_π modulo 11 has a node with rational tangents (cf. Example 2.5).

In general, Conjecture 14.1 has now been proved for all π_p and p except π_2 an irregular supercuspidal representation of $\mathrm{GL}_2(\mathbb{Q}_2)$. The case of an arbitrary principal series representation or special representation is due to Langlands [28]. The proof for "regular" supercuspidals is due to Deligne (unpublished). The method of Langlands is completely new in that it is based on the Selberg trace formula for GL(2) and a strong form of the Lefshetz fixed point formula of algebraic geometry.

More examples and consequences of Conjecture 14.1 (including the earlier results of Deligne on bad reduction) are discussed in [9]. According to Langlands it already follows from the current state of Conjecture 14.1 that the p-factors of $L(f, s)$ and $L(E_f, s)$ coincide *for all p* (without verifying (36) for irregular supercuspidal representations π_2). Although Langlands has convinced me of this fact I am unable to reproduce the arguments here.

Concluding Remark. In Section 4 (and the present section) we assumed f (and π_f) to be "rational." We made this assumption purely to simplify the discussion. Without it the eigenvalues of f generate a finite algebraic extension K of $\mathbb{Q}$ and the corresponding E_f is no longer an elliptic curve but rather an abelian variety of dimension $n = [K: \mathbb{Q}]$ (cf. [48]). In this case the zeta-function of the variety E_f is a *product* of the zeta-functions of f and certain "twistings" of f. The corresponding modification in the statement of Conjecture 14.1 is explained in [9, 28].

15. *Odds and Ends*

In Sections 12 and 13 we described two correspondences with image in the set of cuspidal representations of $G_{\mathbb{A}(\mathbb{Q})}$. The first, given by Conjecture 12.2, is defined for two-dimensional semi-simple representations of the Weil group $W_{\mathbb{Q}}$. The second, given by Conjecture D′, is defined for isogeny classes of elliptic curves over $\mathbb{Q}$. We denote these correspondences by $\pi(\sigma)$ and $\pi(E)$, respectively. Both are predicted by special cases of the conjectures of [26].

In [23] a correspondence is defined for the nontrivial automorphic representations of the adelization of the multiplicative group of a quaternion algebra. We denote this correspondence by $\pi(\pi')$. It too takes values in the set of cuspidal representations of $G_{\mathbb{A}}$ and preserves L-functions. Since $\pi(\sigma)$, $\pi(E)$, and $\pi(\pi')$ share the same range space it is natural to ask: When do the corresponding L-functions $L(\sigma, s)$, $L(E, s)$, $L(\pi', s)$, and $L(\pi, s)$ coincide?

Relations between these L-functions are of particular number–theoretical interest when the Euler factors defining them are determined in an elementary way. This is the case, for example, for $L(\sigma, s)$, $L(E, s)$ and $L(\pi', s)$, at least when the quaternion algebra does not split at infinity (cf. [30]).

To obtain relations between these functions, [23, Theorem 16.1] is particularly useful. This theorem gives a simple criterion for π be in the image of $\pi(\pi')$ and it can easily be applied to $\pi(\sigma)$ and $\pi(E)$. Thus one obtains a general result about the relations between $L(\sigma, s)$, $L(E, s)$ and $L(\pi', s)$. Previously, only isolated examples of such relations were known.

A criterion for π to be in the image of $\pi(E)$ is not difficult to give in terms of the weight and rationality of the primitive form corresponding to π (see Sect. 13). For such π the construction of Shimura described in Section 5 produces an elliptic curve which inverts the correspondence $\pi(E)$.

In general it is *not* easy to characterize the image of $\pi(\sigma)$. Suppose, however, that σ defines an irreducible representation of the *Galois* group, i.e., σ is trivial on the connected component of the neutral element of $W_{\mathbb{Q}}$. Then σ_∞ is the direct sum of two one-dimensional representations of Gal($\mathbb{C}/\mathbb{R}$). Moreover, assuming that the determinant of σ is odd, $\pi(\sigma)$ corresponds to a normalized primitive form in $S_1(\Gamma_0(N), \epsilon)$ with $\epsilon(-1) = -1$ and all such cuspidal representations of $G_{\mathbb{A}}$ thus arise. (See [31] for the definition of primitive form with nontrivial character and [16] for the definition of odd σ.)

What Deligne and Serre do in [16] is invert the correspondence

$$\sigma \longrightarrow \pi(\sigma)$$

restricted to "Galois representations" of the above type. In particular, they produce for each π belonging to some f in $S_1(\Gamma_0(N), \epsilon)$ a σ such that $\pi(\sigma) = \sigma$. Thus from Conjecture 12.2 there results a bijection between certain primitive cusp forms *of weight* 1 and certain two-dimensional representations of Gal($\overline{\mathbb{Q}}/\mathbb{Q}$).

The results of Deligne and Serre also make it possible to prove Artin's conjecture for a wide variety of nontrivial σ. Indeed, the image of σ(Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) in PGL$_2(\mathbb{C})$ is either dihedral, tetrahedral (A_4), octahedral (S_4), or icosahedral (A_5). The dihedral case is trivial in the sense that σ is then induced from a quasi-character of some quadratic extension. Thus $L(\sigma, s) = L(\pi(\sigma), s)$ with $\pi(\sigma)$ a cuspidal representation of GL(2, $\mathbb{A}$)

(cf. Conjecture 12.2 and the remarks immediately following it). What Langlands does in [29] is prove Conjecture 12.2 for a wide range of tetrahedral and octahedral σ by combining the result of Deligne and Serre with a generalization of the recent theory of "lifting" automorphic forms due to Saito and Shintani. In particular, Artin's conjecture is proved for these σ. It is interesting to note that Selberg's trace formula once again plays a crucial role in this work.

Suppose finally that $\pi = \otimes \pi_p$ is a cuspidal representation of $G_{\mathbb{A}}$ with π_∞ a discrete series representation of weight $k \geqslant 2$. Rather than worry about whether π is in the image of $\pi(\sigma)$ it is more profitable to follow the path initiated by Eichler and Shimura. As in [28, 34], a crucial step is to associate to π an appropriate two-dimensional l-adic representation σ of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ (cf. [15, Theorem 6.1]). The refinement of Eichler–Shimura theory described in Section 14 amounts to the assertion that the L- and ϵ-factors of π_p coincide with those of σ for all p.

In the classical context of cusp forms of weight $k \geqslant 2$, the l-adic representations also play a crucial role in [14] (see also [43]). For p not dividing the level of f Deligne shows that a_p is the trace of the Frobenius on $H^{k-1}(V, \mathbb{Q}_l)$, V an appropriate $(k - 1)$-dimensional variety defined over $\mathbb{F}_p$. The Ramanujan–Petersson conjecture for forms of weight $k \geqslant 2$ is thus proved using Weil's conjectures (cf. [11] and the concluding remarks of Sect. 1). The Ramanujan–Petersson conjecture for forms *of weight* 1 is a consequence of [15].

For further examples of results in this area the reader is referred to Borel's account [7] of what is now called the "philosophy of Langlands."

Note added in proof. Langlands has now sketched a proof of Artin's conjecture for all two-dimensional tetrahedral representations of the Galois group of an arbitrary number field. Among other things, his proof uses the recently established fact that cusp forms on $GL(2)$ "lift" to $GL(3)$ (see [18b]). This fact also implies that $L(s, \pi, r)$ is entire when π is cuspidal and r is the symmetric square of the standard representation of $GL(2, \mathbb{C})$ (cf. the remarks at the beginning of Sect. 10).

References

1. "Proceedings of the Antwerp Conference on Modular Functions of One Variable," Vol. 2, Lecture Notes in Mathematics, No. 349, Springer–Verlag New York/Berlin, 1973.
2. "Proceedings of the Antwerp Conference on Modular Functions of One Variable," Vol. 4, Lecture Notes in Mathematics, No. 476, Springer–Verlag, New York/Berlin, 1975.

3. A. Artin, Theorie der L-Riehen mit allgemeinen Gruppencharakteren, *Abh. Math. Sem. Univ. Hamburg* 8 (1930), 292–306.
4. A. Atkin and J. Lehner, Hecke operators on $\Gamma_0(m)$, *Math. Ann.* **185** (1970), 134–160.
5. B. J. Birch and H. P. F. Swinnerton-Dyer, Notes on elliptic curves, II, *J. Reine Angew. Math.* 218 (1962), 79–108.
6. B. J. Birch and H. P. F. Swinnerton-Dyer, Elliptic curves and modular functions, *in* [2, pp. 2–32].
7. A. Borel, Formes automorphes et séries de Dirichlet, *Sem. Bourbaki,* No. 466, Juin (1975).
8. W. Casselman, An assortment of results on representations of $\mathrm{GL}_2(k)$, *in* [1, pp. 1–54].
9. W. Casselman, On representations of GL_2 and the arithmetic of modular curves, *in* [1, pp. 107–142].
10. J. W. S. Cassels, Diophantine equations with special reference to elliptic curves, *J. London Math. Soc.* 41 (1966), 193–291.
11. P. Deligne, La conjecture de Weil, I, *Publ. I.H.E.S.* 43 (1974), 273–307.
12. P. Deligne, Les constantes des équations fonctionnelles, *Sem. Delange-Pisot-Poitou,* No. 19 bis, Mai (1970).
13. P. Deligne, Formes modulaires et représentations de GL_2, *in* [1, pp. 55–107].
14. P. Deligne, Formes modulaires et représentations l-adiques, *Sem. Bourbaki,* No. 355; Lecture Notes in Mathematics, No. 244, pp. 139–186, Springer–Verlag, New York/Berlin, 1971.
15. P. Deligne, Les constantes des équations fonctionnelles des fonctions L, *in* [1, pp. 501–598].
16. P. Deligne and J.-P. Serre, Formes modulaires de poids, 1, *Ann. Sci. École Norm. Sup., 4^e^ sér.* 4 (1974), 507–530.
17. B. Dwork, On the rationality of the zeta-function of an algebraic variety, *Amer. J. Math.* 82 (1960), 631–648.
18a. S. Gelbart, "Automorphic Forms on Adele Groups," *Annals of Mathematical Studies,* No. 83, Princeton Univ. Press, Princeton, N. J., 1975.
18b. S. Gelbart and H. Jacquet, The relation between automorphic forms on $GL(2)$ and $GL(3)$, *Proc. Nat. Acad. Sci. U.S.A.,* in press; also paper in preparation.
19. L. Goldstein, "Analytic Number Theory," Prentice–Hall, Englewood Cliffs, N. J., 1973.
20. A. Grothendieck, Formule de Lefschetz et rationalité des fonctions L, *Sem. Bourbaki,* No. 279, December (1964).
21. R. Howe, Review of [28], *Zentralblatt für Math.* **279**, Review 14007 (1974), 94–96.
22. J. Igusa, Kroneckerian models of fields of elliptic modular functions, *Amer. J. Math.* 81 (1959), 561–577.
23. H. Jacquet and R. P. Langlands, "Automorphic Forms on GL(2)," Lecture Notes in Mathematics, No. 114, Springer–Verlag, New York/Berlin, 1970.
24. Kutzko, On the supercuspidal representations of GL_2, *Amer. J. Math.,* to appear.
25. S. Lang, "Elliptic Functions," Addison–Wesley, Reading, Mass., 1973.
26. R. P. Langlands, "Problems in the Theory of Automorphic Forms," Lecture Notes in Mathematics, No. 170, Springer–Verlag, New York/Berlin, 1970.
27. R. P. Langlands, On the functional equation of the Artin L-functions, mimeographed notes, Yale University.
28. R. P. Langlands, Modular forms and l-adic representations, *in* [1], pp. 361–500.

29. R. P. LANGLANDS, Base change for GL(2): The theory of Saito–Shintani with applications, preprint, Institute for Advanced Study, Princeton, N. J., 1975.
30. R. P. LANGLANDS, Automorphic forms on GL(2), *Actes*, *Congrès Intern. Math.* **2** (1970), 327–329.
31. W. LI, New forms and functional equations, *Math. Ann.* **212** (1975), 285–315.
32. A. P. OGG, Elliptic curves with wild ramification, *Amer. J. Math.* **89** (1967), 1–21.
33. A. P. OGG, Abelian curves of small conductor, *J. Reine Angew. Math.* **226** (1967), 204–215.
34. I. I. PYATETSKII-SHAPIRO, Zeta-functions of modular curves, *in* [1, pp. 317–360].
35. A. ROBERT, "Elliptic curves," Lecture Notes in Mathematics, No. 326, Springer–Verlag, New York/Berlin, 1973.
36. P. J. SALLY AND J. SHALIKA, Characters of the discrete series of representations of SL(2) over a local field, *Proc. Nat. Acad. Sci. U.S.A.* **63** (1969), 1231–1237.
37. "Seminar on Complex Multiplication," Lecture Notes in Mathematics, No. 21, Springer–Verlag, New York/Berlin, 1966.
38. S. SEN AND J. TATE, Ramification groups of local fields, *J. Indian Math. Soc.* **27** (1963), 197–202.
39. J.-P. SERRE, "Rationalité des Fonctions zêta des variétés algébriques (d'après Dwork), *Sem. Bourbaki*, No. 198 (1960).
40. J.-P. SERRE, "Course in Arithmetic," Springer–Verlag, New York/Berlin, 1973.
41. J.-P. SERRE. Facteurs locaux des fonctions zêta des variétés algébriques, *Sem. Delange-Pisot-Poitou*, No. 19, Mai (1970).
42. J.-P. SERRE, "Abelian l-adic Representations and Elliptic Curves," Benjamin, New York, 1968.
43. J.-P. SERRE, Une interprétation des congruences relative à la fonction τ de Ramanujan, *Sem. Delange-Pisot-Poitou*, No. 14, Février (1968).
44. J.-P. SERRE AND J. TATE, Gcod reduction of abelian varieties, *Ann. Math.* **88** (1968), 492–517.
45. I. R. SHAFAREVICH, On Galois groups of p-adic fields, *C. R. Dokl. Acad. Sci. USSR* (*N. S.*) **53** (1946), 15–16.
46. G. SHIMURA, "Introduction to the Arithmetic Theory of Automorphic Functions," Iwanami Shoten, Tokyo, and Princeton Univ. Press, Princeton, N. J., 1971.
47. G. SHIMURA, On elliptic curves with complex multiplication as factors of the Jacobians of modular functions fields, *Nagoya Math. J.* **43** (1971), 199–208.
48. G. SHIMURA, On the factors of the Jacobian variety of a modular function field, *J. Math. Soc. Japan* **25** (1973), 523–544.
49. H. P. F. SWINNERTON-DYER, "Analytic Theory of Abelian Varieties," London Mathematical Society Lecture Note Series 14, Cambridge Univ. Press, London/New York, 1974.
50. J. TATE, The arithmetic of elliptic curves, *Invent. Math.* **23** (1974), 179–206.
51. A. WEIL, Number of solutions of equations in finite fields, *Bull. Amer. Math. Soc.* **55** (1949), 497–508.
52. A. WEIL, Über die Bestimmung Dirichletscher Reiken durch Funktionalgleichungen, *Math. Ann.* **168** (1967), 149–156.
53. A. WEIL, "Dirichlet Series and Automorphic Forms," Lecture Notes in Mathematics, No. 189, Springer–Verlag, New York/Berlin, 1971.
54. A. WEIL, Sur la théorie du corps de classes, *J. Math. Soc. Japan* **3** (1951), 1–35.
55. A. WEIL, Number theory and algebraic geometry, *in* "Proceedings of the International

Congress of Mathematics 1950," pp. 90–100, American Mathematical Society, Provicence, R. I., 1952.

56. A. Weil, Exercices dyadiques, *Invent. Math.* **29** (1975).
57. A. Weil, "Basic Number Theory," 2nd ed., Springer–Verlag, New York/Berlin, 1973.
58. Yamamoto, Elliptic curves of prime power conductor, presented at the 1975 U.S.–Japan Number Theory Conference, Ann Arbor, Mich.