Centre de Recherches Mathématiques
CRM Proceedings & Lecture Notes
Volume 4, 1994

Elliptic Curves and the Weil-Deligne Group

David E. Rohrlich

Given an elliptic curve E over a non-Archimedean local field K, one associates to E over K a two-dimensional complex representation $\sigma'_{E/K}$ of the Weil-Deligne group of K, derived from the ℓ-adic Galois representations on the Tate modules of E. We shall define $\sigma'_{E/K}$ precisely, and shall also explain how the local factors associated to $\sigma'_{E/K}$ encode certain data about E. Intended for a reader familiar with elliptic curves but not with the Weil-Deligne group, our exposition amounts to a glossed transcription (possibly marred by interpolation) of portions of the papers of Tate [**13**] and Deligne [**3**]. For rectifications and omitted proofs the reader will have to consult the original texts.

ACKNOWLEDGEMENT. In preparing this work I have benefited from discussions with Steve Kudla concerning a preliminary version of his article *The local Langlands correspondence: The non-Archimedean case.*

Part I: The Weil-Deligne Group

1. The Weil group

Let k be a finite field of characteristic p and cardinality q, and let $\bar{k}$ denote an algebraic closure of k. The Weil group $\mathcal{W}(\bar{k}/k)$ of k is the infinite cyclic subgroup of $\mathrm{Gal}(\bar{k}/k)$ generated by the Frobenius automorphism $x \mapsto x^q$. Nowadays it is actually the inverse of the Frobenius automorphism which is regarded as the canonical generator of $\mathcal{W}(\bar{k}/k)$, and so it is the latter which will get a special notation: φ. Thus if n is a positive integer and k_n is the unique subfield of $\bar{k}$ of degree n over k then $\varphi(x) = x^{q^{n-1}}$ for $x \in k_n$. We make $\mathcal{W}(\bar{k}/k)$ into a topological group by giving it the discrete topology.

Next consider a non-Archimedean local field K with residue class field k. Write $\overline{K}$ for a separable algebraic closure of K and K_{unr} for the maximal unramified extension of K contained in $\overline{K}$. The inertia subgroup of $\mathrm{Gal}(\overline{K}/K)$ is the group $I = \mathrm{Gal}(\overline{K}/K_{\mathrm{unr}})$. Identifying $\bar{k}$ with the residue class field of $\overline{K}$ (or of K_{unr}), we have an exact sequence

$$1 \longrightarrow I \longrightarrow \mathrm{Gal}(\overline{K}/K) \xrightarrow{\pi} \mathrm{Gal}(\bar{k}/k) \longrightarrow 1,$$

1991 *Mathematics Subject Classification.* Primary:11G07; Secondary: 11G05, 11F70.

The author gratefully acknowledges the support of the National Science Foundation (NSF grant DMS-9114603).

This is the final form of the paper.

where $\pi : \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{Gal}(\bar{k}/k)$ is the decomposition map. We define $\mathcal{W}(\overline{K}/K)$ to be the inverse image of $\mathcal{W}(\bar{k}/k)$ under π:

$$\mathcal{W}(\overline{K}/K) = \pi^{-1}(\mathcal{W}(\bar{k}/k)).$$

Thus $\mathcal{W}(\overline{K}/K)$ fits into an exact sequence

$$1 \longrightarrow I \longrightarrow \mathcal{W}(\overline{K}/K) \longrightarrow \mathcal{W}(\bar{k}/k) \longrightarrow 1,$$

and we have

$$\mathcal{W}(\overline{K}/K) = \bigcup_{n\in\mathbb{Z}} \Phi^n I$$

for any $\Phi \in \mathrm{Gal}(\overline{K}/K)$ such that $\pi(\Phi) = \varphi$. Such an element Φ is called an inverse Frobenius element of $\mathrm{Gal}(\overline{K}/K)$; unlike φ, it is not unique but only unique up to multiplication by an element of I. We define a topology on $\mathcal{W}(\overline{K}/K)$ by requiring that I be open in $\mathcal{W}(\overline{K}/K)$, that the relative topology on I from $\mathcal{W}(\overline{K}/K)$ coincide with the relative topology from $\mathrm{Gal}(\overline{K}/K)$, and that left multiplication by Φ be a homeomorphism. Thus $\mathcal{W}(\overline{K}/K)$ has the coarsest topology for which the projection $\pi : \mathcal{W}(\overline{K}/K) \longrightarrow \mathcal{W}(\bar{k}/k)$ and the inclusion $I \longrightarrow \mathrm{Gal}(\overline{K}/K)$ are both continuous, and for which $\mathcal{W}(\overline{K}/K)$ is a topological group. The key point to keep in mind about this topology is that while the identity in $\mathcal{W}(\overline{K}/K)$ has a neighborhood basis consisting of open subgroups of I, the open subgroups *of finite index* in $\mathcal{W}(\overline{K}/K)$ are the subgroups $\mathcal{W}(\overline{K}/L)$ $(= \mathcal{W}(\overline{K}/K) \cap \mathrm{Gal}(\overline{K}/L))$, where L runs over finite extensions of K in $\overline{K}$. This should be contrasted with the fact that for a compact group like I or $\mathrm{Gal}(\overline{K}/K)$, every open subgroup has finite index.

2. Representations of the Weil group

By a representation of $\mathcal{W}(\overline{K}/K)$ we mean a continuous homomorphism $\sigma : \mathcal{W}(\overline{K}/K) \longrightarrow \mathrm{GL}(V)$, where V is a finite-dimensional complex vector space. We say that σ is ramified or unramified according as $\sigma|I$ is nontrivial or trivial. If V is one-dimensional then we call σ a character (or a quasicharacter, if we wish to emphasize that σ is not necessarily unitary). We freely identify characters of $\mathcal{W}(\overline{K}/K)$ with characters of $K^\times$ by composing with the Artin isomorphism

$$K^\times \cong \mathcal{W}(\overline{K}/K)^{\mathrm{ab}},$$

where $\mathcal{W}(\overline{K}/K)^{\mathrm{ab}}$ stands for $\mathcal{W}(\overline{K}/K)$ modulo the closure of its commutator subgroup. It should be added that the "Artin isomorphism" referred to here is the Artin automorphism of [**3**], equal to the classical Artin isomorphism precomposed with the automorphism $x \mapsto x^{-1}$ of $K^\times$: thus a uniformizer of K is sent to the image in $\mathcal{W}(\overline{K}/K)^{\mathrm{ab}}$ of an *inverse* Frobenius element of $\mathcal{W}(\overline{K}/K)$.

The requirement that a representation $\sigma : \mathcal{W}(\overline{K}/K) \longrightarrow \mathrm{GL}(V)$ be continuous has the following significance: By a standard property of real or complex Lie groups, there is an open neighborhood $\mathcal{U}$ of the identity in $\mathrm{GL}(V)$ which contains no nontrivial subgroups of $\mathrm{GL}(V)$. Since σ is continuous, $\sigma^{-1}(\mathcal{U})$ is an open neighborhood of the identity in $\mathcal{W}(\overline{K}/K)$ and so contains an open subgroup J of I. Then $\sigma(J)$ is a subgroup of $\mathrm{GL}(V)$ contained in $\mathcal{U}$, hence equal to the trivial subgroup. Thus the continuity of σ implies that σ is trivial on an open subgroup of I. Conversely, if $\sigma : \mathcal{W}(\overline{K}/K) \longrightarrow \mathrm{GL}(V)$ is an arbitrary homomorphism which is trivial on an open subgroup J of I, then the inverse image of *any* subset of $\mathrm{GL}(V)$ is a union of cosets of J and is therefore open. Hence σ is continuous.

To summarize, a homomorphism $\sigma : \mathcal{W}(\overline{K}/K) \longrightarrow \mathrm{GL}(V)$ is a representation if and only if it is trivial on an open subgroup of I. By way of illustration, suppose that L is a finite Galois extension of K. Then $I \cap \mathcal{W}(\overline{K}/L)$ is an open subgroup of I and

$$W(\overline{K}/K)/\mathcal{W}(\overline{K}/L) = \mathrm{Gal}(L/K),$$

so that any representation of $\mathrm{Gal}(L/K)$ can be viewed as a representation of $\mathcal{W}(\overline{K}/K)$. Such representations of $\mathcal{W}(\overline{K}/K)$ are said to be of "Galois type"; they are precisely the representations of $\mathcal{W}(\overline{K}/K)$ with finite image. As an example of a representation which is not of Galois type we have the quasicharacter

$$\omega : \mathcal{W}(\overline{K}/K) \longrightarrow \mathbb{C}^\times,$$

defined by the conditions $\omega(I) = \{1\}$ (i.e. ω is unramified) and $\omega(\Phi) = q^{-1}$. More generally, for $s \in \mathbb{C}$ the quasicharacter ω^s is of Galois type if and only if q^s is a root of unity.

PROPOSITION. *An irreducible representation σ of $\mathcal{W}(\overline{K}/K)$ has the form $\sigma \cong \rho \otimes \omega^s$, where ρ is of Galois type and $s \in \mathbb{C}$.*

PROOF. [**3**, 4.10].

Given a finite extension L of K, we write $\mathrm{ind}_{L/K}$ and $\mathrm{res}_{L/K}$ for the induction and restriction functors corresponding to $\mathcal{W}(\overline{K}/K)$ and its subgroup of finite index $\mathcal{W}(\overline{K}/L)$. Also, if σ is any representation of $\mathcal{W}(\overline{K}/K)$ then we denote by $[\sigma]$ the class of σ in the Grothendieck group of virtual representations of $\mathcal{W}(\overline{K}/K)$. Since not all representations of $\mathcal{W}(\overline{K}/K)$ are semisimple, we should add that the equivalence relation defining the Grothendieck group is here understood to be additivity across short exact sequences, not additivity across direct sums. Thus $[\sigma]$ is equal to the sum of the classes of the irreducible constituents in a Jordan-Hölder series for σ, and the Grothendieck group is isomorphic to the free abelian group on the set of isomorphism classes of irreducible representations.

If ρ is a representation of $\mathcal{W}(\overline{K}/K)$ of Galois type, then the Brauer induction theorem allows one to write $[\rho]$ as an integral linear combination of classes of the form $[\mathrm{ind}_{L/K}\,\xi]$, with ξ one-dimensional. On the other hand, according to the proposition just stated, every *irreducible* representation has the form $\rho \otimes \omega^s$ with ρ of Galois type. Since $\mathrm{ind}_{L/K}(\xi) \otimes \omega^s = \mathrm{ind}_{L/K}(\xi\, \mathrm{res}_{L/K}\, \omega^s)$, and since the classes of irreducible representations span the Grothendieck group of $\mathcal{W}(\overline{K}/K)$, one deduces a version of Brauer induction for $\mathcal{W}(\overline{K}/K)$:

COROLLARY 1. *Let σ be any representation of $\mathcal{W}(\overline{K}/K)$. Then we can write*

$$[\sigma] = \sum_{(L,\chi)} c_{L,\chi}[\mathrm{ind}_{L/K}\,\chi],$$

where (L, χ) runs over pairs consisting of a finite extension L of K and a quasicharacter χ of $\mathcal{W}(\overline{K}/L)$, and where $c_{L,\chi}$ is an integer ($= 0$ for almost all (L, χ)).

Let us denote the trivial representation of $\mathcal{W}(\overline{K}/K)$ by 1_K, and an expression such as $[\mathrm{ind}_{L/K}\,\chi] - [\mathrm{ind}_{L/K}\,\chi']$ simply by $[\mathrm{ind}_{L/K}(\chi - \chi')]$. The following variant of Corollary 1 is due to Deligne:

COROLLARY 2. *Let σ be any representation of $\mathcal{W}(\overline{K}/K)$. Then we can write*

$$[\sigma] = \dim(\sigma)[1_K] + \sum_{(L,\chi,\chi')} c_{L,\chi,\chi'}[\mathrm{ind}_{L/K}(\chi - \chi')],$$

where (L, χ, χ') runs over triples consisting of a finite extension L of K and a pair of quasicharacters χ, χ' of $\mathcal{W}(\overline{K}/L)$, and where $c_{L,\chi,\chi'}$ is an integer ($= 0$ for almost all (L, χ, χ')).

PROOF. [**3**, 1.5].

3. The Weil-Deligne group and its representations

The Tate modules of an elliptic curve over K with potential multiplicative reduction afford ℓ-adic representations of $\mathrm{Gal}(\overline{K}/K)$ which are *not* trivial on an open subgroup of I and which therefore do not correspond to a complex representation of $\mathcal{W}(\overline{K}/K)$. Thus one is forced to consider representations of a larger group, the Weil-Deligne group $\mathcal{W}'(\overline{K}/K)$.

Recall that ω denotes the unramified character of $\mathcal{W}(\overline{K}/K)$ taking the value q^{-1} on any inverse Frobenius element. We define $\mathcal{W}'(\overline{K}/K)$ to be the semidirect product

$$\mathcal{W}'(\overline{K}/K) = \mathcal{W}(\overline{K}/K) \ltimes \mathbb{C},$$

where the action of $\mathcal{W}(\overline{K}/K)$ on $\mathbb{C}$ is

$$gzg^{-1} = \omega(g)z \qquad (g \in \mathcal{W}(\overline{K}/K), z \in \mathbb{C}). \tag{3.1}$$

We give $\mathcal{W}'(\overline{K}/K)$ the product topology corresponding to its set-theoretic structure as a cartesian product.

If $L \subset \overline{K}$ is a finite extension of K and Φ_L is an inverse Frobenius element of $\mathcal{W}(\overline{K}/L)$, then

$$\Phi_L \in \Phi^{f(L/K)} I,$$

where $f(L/K)$ is the residue class degree of L over K. Hence

$$\omega(\Phi_L) = q_L^{-1}$$

with $q_L = q^{f(L/K)}$. Thus in a self-explanatory notation we can write

$$\omega | \mathcal{W}(\overline{K}/L) = \omega_L,$$

and we may view $\mathcal{W}'(\overline{K}/L)$ as a subgroup of $\mathcal{W}'(\overline{K}/K)$.

By a representation of $\mathcal{W}'(\overline{K}/K)$ on a finite-dimensional complex vector space V we mean a continuous homomorphism

$$\sigma' : \mathcal{W}'(\overline{K}/K) \longrightarrow \mathrm{GL}(V)$$

such that the restriction of σ' to the subgroup $\mathbb{C}$ of $\mathcal{W}'(\overline{K}/K)$ is complex analytic. To give such a representation σ' is the same as to give a pair (σ, N), where σ is a representation of $\mathcal{W}(\overline{K}/K)$ on V and N is a nilpotent endomorphism of V satisfying

$$\sigma(g)N\sigma(g)^{-1} = \omega(g)N \qquad (g \in \mathcal{W}(\overline{K}/K)). \tag{3.2}$$

One obtains σ' from (σ, N) by putting

$$\sigma'(gz) = \sigma(g)\exp(zN) \qquad (g \in \mathcal{W}(\overline{K}/K), z \in \mathbb{C}), \tag{3.3}$$

the function so defined being a homomorphism by virtue of (3.1) and (3.2). In the other direction, we recover (σ, N) from σ' via the formulas

$$\sigma = \sigma' | \mathcal{W}(\overline{K}/K) \tag{3.4}$$

and

$$N = (\log \sigma'(z))/z \qquad (z \in \mathbb{C}^\times \text{ arbitrary}). \tag{3.5}$$

The latter formula requires some words of explanation:

First, if U is any unipotent automorphism of V, then by $\log U$ we mean the usual power series in $U - 1$, so that $\log U$ is nilpotent. We shall verify in a moment that $\sigma'(z)$ is in fact unipotent for every $z \in \mathbb{C}$.

Second, a unipotent automorphism has a unique unipotent n-th root for every integer $n \geq 1$, and hence a unique unipotent t-th power for every $t \in \mathbb{Q}$. Since σ' is a homomorphism we have

$$\log \sigma'(tz_0) = \log(\sigma'(z_0)^t) = t \log \sigma'(z_0)$$

for $t \in \mathbb{Q}$ and $z_0 \in \mathbb{C}$. By continuity, the identity $\log \sigma'(tz_0) = t \log \sigma'(z_0)$ holds for all $t \in \mathbb{R}$, and in fact for all $t \in \mathbb{C}$ by complex analyticity. Taking $z_0 = 1$ and $t = z$, we see that the right-hand side of (3.5) is independent of z, as claimed.

It remains to check that $\sigma'(z)$ is unipotent. Taking $g = \Phi^{-1}$ in (3.1), we see that the linear transformations $\sigma'(z)$ and $\sigma'(z)^q$ are similar. It follows by iteration that if λ is an eigenvalue of $\sigma'(z)$, then so is λ^{q^n} for every integer $n \geq 0$. Now $\sigma'(z)$ has at most d distinct eigenvalues, where $d = \dim \sigma'$, so that

$$\lambda^{q^{m_0}} = \lambda^{q^{n_0}}$$

for some pair of integers (m_0, n_0) satisfying $0 \leq m_0 < n_0 \leq d$. Thus

$$r = \prod_{0 \leq m < n \leq d} (q^n - q^m)$$

is a positive integer independent of z such that every eigenvalue of $\sigma'(z)$ is an r-th root of unity. Applying this remark to $\sigma'(z/r)$ in place of $\sigma'(z)$, and writing $\sigma'(z) = \sigma'(z/r)^r$, we conclude that every eigenvalue of $\sigma'(z)$ is 1, as desired.

This completes our verification that representations σ' of $\mathcal{W}'(\overline{K}/K)$ are in one-to-one correspondence with pairs (σ, N) satisfying (3.2). Henceforth we simply identify σ' with the corresponding pair (σ, N) and write $\sigma' = (\sigma, N)$. We say that σ' is unramified if σ is unramified and $N = 0$. Otherwise we say that σ' is ramified. Also, if σ is any representation of $W(\overline{K}/K)$ then we identify σ with the representation $(\sigma, 0)$ of $\mathcal{W}'(\overline{K}/K)$.

In the following proposition we record the effect on (σ, N) of some standard operations on σ'.

PROPOSITION. *Let $\sigma' = (\sigma, N)$ and $\tau' = (\tau, P)$ be representations of $\mathcal{W}'(\overline{K}/K)$ on vector spaces V and W respectively.*

(i) $\sigma' \oplus \tau' = (\sigma \oplus \tau, N \oplus P)$.

(ii) $\sigma' \otimes \tau' = (\sigma \otimes \tau, N \otimes 1 + 1 \otimes P)$, *where* 1 *denotes the identity automorphism of V or W.*

(iii) *Let σ'^* denote the contragredient representation on the dual space V^* of V. Then $\sigma'^* = (\sigma^*, N^*)$, where*

$$(\sigma^*(g)f)(v) = f(\sigma(g^{-1})v)$$

and

$$(N^*f)(v) = -f(Nv)$$

for $g \in \mathcal{W}(\overline{K}/K)$, $f \in V^*$, and $v \in V$.

(iv) *Let L denote a finite extension of K, and write $\mathrm{res}_{L/K}$ and $\mathrm{ind}_{L/K}$ for the restriction and induction functors corresponding to the group $\mathcal{W}'(\overline{K}/K)$ and its subgroup of finite index $\mathcal{W}'(\overline{K}/L)$ (or to the group $\mathcal{W}(\overline{K}/K)$ and its subgroup of finite index $\mathcal{W}(\overline{K}/L)$, as appropriate). Let $\rho' = (\rho, M)$ be a representation of $\mathcal{W}'(\overline{K}/L)$ on a vector space U. Then*

$$\mathrm{res}_{L/K}\,\sigma' = (\mathrm{res}_{L/K}\,\sigma, N)$$

and

$$\mathrm{ind}_{L/K}\,\rho' = (\mathrm{ind}_{L/K}\,\rho, M_{L/K}),$$

where $M_{L/K}$ is defined as follows: Put $G = \mathcal{W}(\overline{K}/K)$ and $H = \mathcal{W}(\overline{K}/L)$, and view U as a $\mathbb{C}[H]$-module via the representation ρ. Take $\mathbb{C}[G] \otimes_{\mathbb{C}[H]} U$ as the space of $\mathrm{ind}_{L/K}\,\rho$. Then

$$M_{L/K}(g \otimes u) = \omega(g)^{-1}(g \otimes Mu)$$

for $g \in G$ and $u \in U$.

Proof. The formulas are a straightforward consequence of the definitions. As an example, let us verify (ii). Put $S = \exp N$ and $T = \exp P$. Then

$$\log(S \otimes T) = \log\left((S \otimes 1)(1 \otimes T)\right) = \log(S \otimes 1) + \log(1 \otimes T). \tag{3.6}$$

Writing the identity automorphism of $V \otimes W$ as $1 \otimes 1$, we have

$$\log(S \otimes 1) = \sum_{n \geq 1} \frac{(-1)^{n+1}}{n}(S \otimes 1 - 1 \otimes 1)^n = (\log S) \otimes 1 = N \otimes 1;$$

similarly, $\log(1 \otimes T) = 1 \otimes P$. Substitution in (3.6) gives (ii).

4. The Weil-Deligne group and ℓ-adic representations

Let ℓ denote a prime different from p. By an ℓ-adic representation of $\mathrm{Gal}(\overline{K}/K)$ we mean a continuous homomorphism

$$\sigma'_\ell : \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{GL}(V_\ell),$$

where V_ℓ is a finite-dimensional vector space over $\mathbb{Q}_\ell$. In the first instance it is ℓ-adic representations of $\mathrm{Gal}(\overline{K}/K)$, not complex representations of $\mathcal{W}'(\overline{K}/K)$, which are the representation-theoretic output of arithmetical algebraic geometry. However, if we fix a field embedding $\iota : \mathbb{Q}_\ell \hookrightarrow \mathbb{C}$, then there is a simple recipe for converting an ℓ-adic representation σ'_ℓ of $\mathrm{Gal}(\overline{K}/K)$ into a complex representation $\sigma'_{\ell,\iota}$ of $\mathcal{W}'(\overline{K}/K)$. The construction, due to Grothendieck and Deligne, is summarized in the next proposition. The essential point is that there is a canonical way to associate to σ'_ℓ a pair (σ_ℓ, N_ℓ) consisting of a homomorphism $\sigma_\ell : \mathcal{W}(\overline{K}/K) \longrightarrow \mathrm{GL}(V_\ell)$ *trivial on an open subgroup of* I and a nilpotent endomorphism N_ℓ of V_ℓ such that

$$\sigma_\ell(g)N_\ell\sigma_\ell(g)^{-1} = \omega(g)N_\ell \tag{4.1}$$

for $g \in \mathcal{W}(\overline{K}/K)$. Composing σ_ℓ with the extension-of-scalars map $\mathrm{GL}(V_\ell) \hookrightarrow \mathrm{GL}(\mathbb{C} \otimes_\iota V_\ell)$, we obtain

$$\sigma_{\ell,\iota} : \mathcal{W}(\overline{K}/K) \longrightarrow \mathrm{GL}(\mathbb{C} \otimes_\iota V_\ell);$$

and applying the extension-of-scalars map $\mathrm{End}(V_\ell) \hookrightarrow \mathrm{End}(\mathbb{C}\otimes_\iota V_\ell)$ to N_ℓ we obtain

$$N_{\ell,\iota} \in \mathrm{End}(\mathbb{C} \otimes_\iota V_\ell).$$

Since $\sigma_{\ell,\iota}$ is continuous by construction and the compatibility relation (3.2) follows from (4.1), we see that the pair $(\sigma_{\ell,\iota}, N_{\ell,\iota})$ is actually a representation of $\mathcal{W}'(\overline{K}/K)$. This is $\sigma'_{\ell,\iota}$.

In practice, if one starts with a smooth projective variety X over K and takes σ'_ℓ to be the representation associated to ℓ-adic cohomology of X in some dimension, then neither ι nor ℓ can be chosen canonically, and one would therefore like to verify that the isomorphism class of $\sigma'_{\ell,\iota}$ is independent of ℓ and ι. In the case where X is an elliptic curve this verification is elementary and will be carried out in Sections 14 and 15. But to start with, we would like to describe the correspondence $\sigma'_\ell \mapsto (\sigma_\ell, N_\ell)$ more precisely, and for this we need to make two further choices: The choice of an inverse Frobenius element Φ and the choice of a nontrivial continuous homomorphism $t_\ell : I \to \mathbb{Q}_\ell$. Such a homomorphism is unique up to multiplication by an element of $\mathbb{Q}_\ell^\times$, for if K_{tame} is the maximal tamely ramified extension of K_{unr} inside $\overline{K}$ then the group $P = \mathrm{Gal}(\overline{K}/K_{\mathrm{tame}})$ is a pro-p-group, and

$$I/P \cong \prod_{r \neq p} \mathbb{Z}_r.$$

Hence up to a scalar multiple t_ℓ is just projection on the factor $\mathbb{Z}_\ell$. By Kummer theory we have

$$gig^{-1} = i^{\omega(g)} \pmod{P}$$

for $g \in \mathcal{W}(\overline{K}/K)$ and $i \in I$, whence

$$t_\ell(gig^{-1}) = \omega(g)t_\ell(i). \tag{4.2}$$

Proposition. *Let* $\sigma'_\ell : \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{GL}(V_\ell)$ *be an* ℓ*-adic representation.*

(i) *There is a unique nilpotent endomorphism* N_ℓ *of* V_ℓ *such that*

$$\sigma'_\ell(i) = \exp(t_\ell(i)N_\ell)$$

for i *in some open subgroup of* I. *Furthermore,*

$$\sigma'_\ell(g)N_\ell\sigma'_\ell(g)^{-1} = \omega(g)N_\ell$$

for $g \in \mathcal{W}(\overline{K}/K)$. *We have* $N_\ell = 0$ *if and only if* σ'_ℓ *is trivial on an open subgroup of* I.

(ii) *The function* $\sigma_\ell : \mathcal{W}(\overline{K}/K) \longrightarrow \mathrm{GL}(V_\ell)$ *defined by*

$$\sigma_\ell(g) = \sigma'_\ell(g)\exp(-t_\ell(i)N_\ell) \qquad (g = \Phi^m i, m \in \mathbb{Z}, i \in I)$$

is a homomorphism and is trivial on an open subgroup of I.

(iii) $\sigma_\ell(g)N_\ell\sigma_\ell(g)^{-1} = \omega(g)N_\ell$ *for* $g \in \mathcal{W}(\overline{K}/K)$.

(iv) *The isomorphism class of the representation*

$$\sigma'_{\ell,\iota} = (\sigma_{\ell,\iota}, N_{\ell,\iota})$$

is independent of the choice of Φ and t_ℓ.

PROOF.

(i) For the first statement see [**11**, **p. 515**]. The second statement follows from (4.2) and the uniqueness of N_ℓ, while the third statement also follows from the uniqueness of N_ℓ.

(ii) Direct calculation using the given formula. Of course the triviality of σ_ℓ on an open subgroup of I follows from the first statement in (i).

(iii) To prove this identity substitute the formula for $\sigma_\ell(g)$ given in (ii) and apply the second statement in (i).

(iv) [**3**, Lemma 8.4.3].

GENERALIZATION. By a λ-adic representation of $\mathrm{Gal}(\overline{K}/K)$ we mean a continuous homomorphism $\sigma'_\lambda : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}(V_\lambda)$, where V_λ is a finite-dimensional vector space over a finite extension $\mathbf{E}_\lambda$ of $\mathbb{Q}_\ell$. Let ι be an embedding of $\mathbf{E}_\lambda$ in $\mathbb{C}$ and let t_ℓ be as before. The preceding proposition remains true if we replace the subscript ℓ on V_ℓ, σ'_ℓ, σ_ℓ, N_ℓ, $\sigma'_{\ell,\iota}$, $\sigma_{\ell,\iota}$, and $N_{\ell,\iota}$ by λ.

5. Indecomposable representations and special representations

A representation $\sigma' = (\sigma, N)$ of $\mathcal{W}'(\overline{K}/K)$ is called *admissible* (or *Φ-semisimple*) if σ is semisimple; it is called *indecomposable* if the space of σ' cannot be written as a direct sum of proper subspaces invariant under $\mathcal{W}'(\overline{K}/K)$. Of course a subspace is invariant under $\mathcal{W}'(\overline{K}/K)$ if and only if it is invariant under both $\mathcal{W}(\overline{K}/K)$ and N.

We mention in passing that σ' is admissible if and only if $\sigma(\Phi)$ is a semisimple linear transformation for some inverse Frobenius element Φ. Indeed the latter condition means that the restriction of σ to the subgroup generated by Φ is semisimple; but Φ generates a subgroup of finite index in $\mathcal{W}(\overline{K}/K)/\ker\sigma$, and if G is any group and H a subgroup of finite index then a finite-dimensional complex representation of G is semisimple if and only if its restriction to H is semisimple ([**2**, Ch. IV, §5, Prop. 1, p. 82]). This is the reason for the terminology "Φ-semisimple".

Let n be a positive integer, and let $e_0, e_1, \ldots, e_{n-1}$ denote the standard basis for $\mathbb{C}^n$. The *special representation of dimension* n, denoted $\mathrm{sp}(n)$, is the representation $\sigma' = (\sigma, N)$ defined by the formulas

$$\sigma(g)e_j = \omega(g)^j e_j \qquad (g \in \mathcal{W}(\overline{K}/K);\ 0 \le j \le n-1)$$

and

$$Ne_j = e_{j+1} \qquad (0 \le j \le n-2),$$
$$Ne_{n-1} = 0.$$

The kernel of N, namely $\mathbb{C}e_{n-1}$, is an invariant subspace, so that $\mathrm{sp}(n)$ is reducible if $n > 1$. However, precisely because $\ker N$ has dimension one, $\mathrm{sp}(n)$ is indecomposable: if $\mathbb{C}^n = U \oplus W$ were a nontrivial decomposition of $\mathbb{C}^n$, then both $U \cap \ker N$ and $W \cap \ker N$ would be nontrivial, because N is nilpotent. Thus $\mathrm{sp}(n)$ is an example of an admissible, indecomposable, n-dimensional representation which for $n > 1$ is reducible.

More generally, let π be an irreducible representation of $\mathcal{W}(\overline{K}/K)$, and consider the representation $\pi \otimes \mathrm{sp}(n)$ of $\mathcal{W}'(\overline{K}/K)$. (Recall that π is identified with the representation $(\pi, 0)$ of $\mathcal{W}'(\overline{K}/K)$, and that a formula for the tensor product is given in part (ii) of the proposition of Section 3.) If we write $\pi \otimes \mathrm{sp}(n) = (\rho, M)$, then ρ is the direct sum of the irreducible representations $\pi \otimes \omega^j$ $(0 \leq j \leq n-1)$ and therefore $\pi \otimes \mathrm{sp}(n)$ is admissible. We claim that it is also indecomposable. Indeed, if V is the space of $\pi \otimes \mathrm{sp}(n)$, then a nontrivial decomposition $V = U \oplus W$ would give a decomposition

$$\ker M = (U \cap \ker M) \oplus (W \cap \ker M), \tag{5.1}$$

necessarily nontrivial because N is nilpotent. But the representation of $\mathcal{W}(\overline{K}/K)$ on $\ker M$ afforded by ρ is isomorphic to $\pi \otimes \omega^{n-1}$, which is irreducible. Hence (5.1) gives a contradiction. Therefore $\pi \otimes \mathrm{sp}(n)$ is an admissible indecomposable representation, and in fact the most general such:

PROPOSITION. *Every admissible indecomposable representation of $\mathcal{W}'(\overline{K}/K)$ is equivalent to a representation of the form $\pi \otimes \mathrm{sp}(n)$, where π is an irreducible representation of $\mathcal{W}(\overline{K}/K)$ and n is a positive integer.*

PROOF. [**4**, Prop. 3.1.3].

As an application, let us prove that Schur's Lemma holds in this context.

COROLLARY 1. *Suppose that σ' is an admissible indecomposable representation of $\mathcal{W}'(\overline{K}/K)$ on a vector space V. Let T be a linear endomorphism of V commuting with the action of $\mathcal{W}'(\overline{K}/K)$. Then T is a scalar multiplication.*

PROOF. Write $\sigma' = (\sigma, N) = \pi \otimes \mathrm{sp}(n)$ and $V = U \otimes W$, where U is the space of π and $W = \mathbb{C}^n$ is the space of $\mathrm{sp}(n)$. Then σ is the direct sum of the irreducible representations $\pi \otimes \omega^j$ for $0 \leq j \leq n-1$, corresponding to the subspaces $U \otimes e_j$ of $U \otimes W$. Since the representations $\pi \otimes \omega^j$ are pairwise nonisomorphic, the usual form of Schur's Lemma shows that $T|U \otimes e_j$ is a scalar c_j. The equation $TN = NT$ then implies that $c_j = c_{j+1}$ for $0 \leq j \leq n-2$, whence all the c_j are equal.

COROLLARY 2. *Let σ' be an admissible representation of $\mathcal{W}'(\overline{K}/K)$. Then σ' has a decomposition of the form*

$$\sigma' = \bigoplus_{j=1}^{s} \pi_j \otimes \mathrm{sp}(n_j),$$

where π_j is an irreducible representation of $\mathcal{W}(\overline{K}/K)$ and n_j is a positive integer. Furthermore, if

$$\sigma' = \bigoplus_{j=1}^{t} \rho_j \otimes \mathrm{sp}(m_j)$$

is another such decomposition, then $s = t$, and after renumbering the summands we have $\pi_j \cong \rho_j$ and $n_j = m_j$.

PROOF. Induction on the dimension of σ' shows that σ' is a direct sum of indecomposables. For uniqueness, write $\sigma' = (\sigma, N)$ and put $n = \inf\{m \in \mathbb{Z}, m \geq 1 : N^m = 0\}$. If $n = 1$ then $N = 0$, σ' is semisimple, and the uniqueness is immediate. If $n > 1$, then in the Grothendieck group of virtual representations of $\mathcal{W}(\overline{K}/K)$ we can write

$$[\sigma] - [\ker N^{n-1}] = \sum_{n_j = n} [\pi_j]$$

and

$$[\sigma] - [\ker N^{n-1}] = \sum_{m_j=n} [\rho_j],$$

where we identify $\ker N^{n-1}$ with the corresponding representation of $\mathcal{W}(\overline{K}/K)$. After renumbering, we conclude that $n_j = n$ if and only if $m_j = n$ and that $\pi_j \cong \rho_j$ whenever $n_j = m_j = n$. Next consider the decompositions

$$[\ker N^{n-1}] - [\ker N^{n-2}] = \left(\sum_{n_j=n-1} [\pi_j]\right) + \left(\sum_{n_j=n} [\pi_j \otimes \omega]\right)$$

and

$$[\ker N^{n-1}] - [\ker N^{n-2}] = \left(\sum_{m_j=n-1} [\rho_j]\right) + \left(\sum_{m_j=n} [\rho_j \otimes \omega]\right).$$

Since we already know that $\pi_j \cong \rho_j$ when n_j or m_j is n, we now conclude (after renumbering) that $n_j = n-1$ if and only if $m_j = n-1$, and that $\pi_j \cong \rho_j$ whenever $n_j = m_j = n-1$. Continuing in this way, we see that the decomposition is unique.

6. A second point of view on the Weil-Deligne group

In the automorphic forms literature, the Weil-Deligne group is sometimes considered to be $\mathcal{W}(\overline{K}/K) \times \mathrm{SL}(2,\mathbb{C})$. While this is not the same thing as $\mathcal{W}'(\overline{K}/K)$, let us explain how *representations* of the two groups can be identified.

We define a representation of $\mathcal{W}(\overline{K}/K) \times \mathrm{SL}(2,\mathbb{C})$ to be a continuous homomorphism $\eta : \mathcal{W}(\overline{K}/K) \times \mathrm{SL}(2,\mathbb{C}) \longrightarrow \mathrm{GL}(V)$ (V a finite-dimensional complex vector space) such that the restriction of η to $\mathrm{SL}(2,\mathbb{C})$ is complex analytic. Note that η is semisimple if and only if its restriction to $\mathcal{W}(\overline{K}/K)$ is semisimple: for the restriction of η to $\mathrm{SL}(2,\mathbb{C})$ is in any case semisimple, and a finite-dimensional complex representation of the direct product of two groups is semisimple if and only if its restriction to each factor is.

For $n \geq 1$ let us write $\mathrm{sym}(n)$ for the n-dimensional representation τ of $\mathrm{SL}(2,\mathbb{C})$ given as follows: The space of τ is the vector space V of homogeneous polynomials of degree $n-1$ in two variables x and y. Given

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{C})$$

and $f \in V$, we define

$$(\tau(g)f)(x,y) = f(ax+cy, bx+dy).$$

PROPOSITION. *There is a bijection $\sigma' \mapsto \eta$ between isomorphism classes of admissible representations $\sigma' = (\sigma, N)$ of $\mathcal{W}'(\overline{K}/K)$ and isomorphism classes of semisimple representations η of $\mathcal{W}(\overline{K}/K) \times \mathrm{SL}(2,\mathbb{C})$ given as follows: If σ' is indecomposable and hence of the form $\pi \otimes \mathrm{sp}(n)$ for some irreducible representation π of $\mathcal{W}(\overline{K}/K)$ then we let $\eta = \pi \boxtimes \mathrm{sym}(n)$ (external tensor product). In the general case, where σ' is a direct sum $\sigma' = \sigma'_1 \oplus \cdots \oplus \sigma'_t$ with each σ'_j indecomposable, we let $\eta = \eta_1 \oplus \cdots \oplus \eta_t$, where η_j corresponds to σ'_j as above.*

PROOF. It suffices to check that the map $\sigma' \mapsto \eta$ is a bijection from indecomposables to irreducibles. Now if we are given $\eta = \pi \boxtimes \mathrm{sym}(n)$, then we can recover π and n by restricting to $\mathcal{W}(\overline{K}/K)$: π is the only irreducible representation of $\mathcal{W}(\overline{K}/K)$ occurring in η, and it occurs with multiplicity n. As for surjectivity, since the group $\mathcal{W}(\overline{K}/K) \times \mathrm{SL}(2, \mathbb{C})$ is a direct product, its irreducible representations are external tensor products of irreducible representations of $\mathcal{W}(\overline{K}/K)$ and $\mathrm{SL}(2, \mathbb{C})$. Thus surjectivity follows from the fact that any irreducible complex analytic representation of $\mathrm{SL}(2, \mathbb{C})$ is equivalent to $\mathrm{sym}(n)$ for some n.

One point about the correspondence

$$\sigma' = \pi \otimes \mathrm{sp}(n) \mapsto \eta = \pi \boxtimes \mathrm{sym}(n)$$

should be noted: if we write σ' in the form $\sigma' = (\sigma, N)$, then σ is *not* isomorphic to $\eta|\mathcal{W}(\overline{K}/K)$ but rather to the representation

$$g \mapsto \omega(g)^{(n-1)/2}\, \eta\left(g, \begin{pmatrix} \omega(g)^{-1/2} & 0 \\ 0 & \omega(g)^{1/2} \end{pmatrix}\right).$$

NORMALIZATION. In the literature the map $\sigma' \mapsto \eta$ is usually normalized in such a way that $\pi \otimes \mathrm{sp}(n)$ is sent to $(\pi \otimes \omega^{(n-1)/2}) \boxtimes \mathrm{sym}(n)$, not to $\pi \boxtimes \mathrm{sym}(n)$ as here. The factor $\omega(g)^{(n-1)/2}$ then disappears from the preceding displayed formula.

7. Invariant forms

Let $\sigma' : \mathcal{W}'(\overline{K}/K) \longrightarrow \mathrm{GL}(V)$ be a representation. By a *σ'-invariant form* on V we mean a nondegenerate bilinear or sesquilinear form $\langle -, - \rangle$ on V such that

$$\langle \sigma'(g)v, \sigma'(g)w \rangle = \langle v, w \rangle \tag{7.1}$$

for $g \in \mathcal{W}'(\overline{K}/K)$. It is readily verified that (7.1) holds for $g \in \mathcal{W}'(\overline{K}/K)$ if and only if

$$\langle \sigma(g)v, \sigma(g)w \rangle = \langle v, w \rangle \tag{7.2}$$

for $g \in \mathcal{W}(\overline{K}/K)$ and

$$\langle Nv, w \rangle = -\langle v, Nw \rangle. \tag{7.3}$$

We say that σ' is *unitary, orthogonal,* or *symplectic* if V admits a σ'-invariant form which is hermitian, symmetric, or symplectic respectively. Note that in the case of a unitary representation we do not require the hermitian form to be positive definite. All that we require is nondegeneracy.

More generally, given a real number t, we say that σ' is *essentially unitary of weight t* if $\sigma' \otimes \omega^{t/2}$ is unitary. Similarly, we say that σ' is *essentially orthogonal of weight t* or *essentially symplectic of weight t* if $\sigma' \otimes \omega^{t/2}$ is orthogonal or symplectic. Finally, σ' is *essentially unitary* (*essentially orthogonal, essentially symplectic*) if it is essentially unitary (orthogonal, symplectic) of some weight.

We can illustrate these definitions using the representation $\mathrm{sp}(n)$. Consider the nondegenerate hermitian form $\langle -, - \rangle$ on $\mathbb{C}^n$ given by

$$\langle z, w \rangle = i^{n-1} \sum_{j=0}^{n-1} (-1)^j z_j \overline{w}_{n-1-j},$$

where $z = (z_0, z_1, \dots, z_{n-1})$ and $w = (w_0, w_1, \dots, w_{n-1})$. Let $\sigma' = \mathrm{sp}(n) = (\sigma, N)$. Then (7.2) and (7.3) hold with σ replaced by $\sigma \otimes \omega^{-(n-1)/2}$. Therefore $\mathrm{sp}(n) \otimes \omega^{-(n-1)/2}$ is unitary and $\mathrm{sp}(n)$ is essentially unitary of weight $1-n$.

One can also consider the nondegenerate bilinear form

$$\langle z, w\rangle = \sum_{j=0}^{n-1} (-1)^j z_j w_{n-1-j}$$

on $\mathbb{C}^n$. This is symmetric if n is odd and symplectic if n is even; in both cases it is invariant under $\mathrm{sp}(n) \otimes \omega^{-(n-1)/2}$. Hence $\mathrm{sp}(n)$ is essentially orthogonal of weight $1-n$ if n is odd and essentially symplectic of weight $1-n$ if n is even.

The following proposition is the analogue for representations of $\mathcal{W}'(\overline{K}/K)$ of a familiar fact about representations of finite groups.

PROPOSITION. *Suppose that σ' is an admissible indecomposable representation of $\mathcal{W}'(\overline{K}/K)$. Then σ' is essentially unitary, and if in addition* $\operatorname{tr}\sigma'$ *is real-valued then σ' is either essentially orthogonal or essentially symplectic (but not both). Conversely, if σ' is essentially orthogonal or essentially symplectic then* $\operatorname{tr}\sigma'$ *is real-valued.*

PROOF. Write $\sigma' = \pi \otimes \mathrm{sp}(n)$, where π is an irreducible representation of $\mathcal{W}(\overline{K}/K)$. Then $\pi = \rho \otimes \omega^s$ with ρ of Galois type and $s \in \mathbb{C}$. Write $s = t + i\theta$ with $t, \theta \in \mathbb{R}$, and let V be the space of ρ. Since ρ has finite image, V admits a ρ-invariant positive definite hermitian form $\langle -, -\rangle_V$, and by virtue of its sesquilinearity this form is also invariant under $\rho \otimes \omega^{i\theta}$. Consequently, the tensor product of $\langle -, -\rangle_V$ with the nondegenerate hermitian form on $\mathbb{C}^n$ exhibited above is invariant under $\pi \otimes \mathrm{sp}(n) \otimes \omega^{(-2t+1-n)/2}$. Hence $\pi \otimes \mathrm{sp}(n)$ is essentially unitary of weight $-2t+1-n$.

Next suppose that $\operatorname{tr}\pi \otimes \mathrm{sp}(n)$ is real-valued. Then so is its restriction to $\mathcal{W}(\overline{K}/K)$, namely $(\operatorname{tr}\pi)(1 + \omega + \cdots + \omega^{n-1})$. Therefore $\operatorname{tr}\pi$ $(= \omega^{t+i\theta} \operatorname{tr}\rho)$ is real-valued. In particular, if Φ is an inverse Frobenius and m is the order of $\rho(\Phi)$, then $q^{im\theta} = \pm 1$. Thus $q^{i\theta}$ is a root of unity, and consequently $\rho \otimes \omega^{i\theta}$ is also of Galois type. Hence without loss of generality we may assume that $\theta = 0$. Therefore $\operatorname{tr}\rho$ is real-valued, so that V admits a ρ-invariant nondegenerate bilinear form which is either orthogonal or symplectic. The tensor product of this form with the orthogonal or symplectic form on $\mathbb{C}^n$ exhibited above is invariant under $\pi \otimes \mathrm{sp}(n) \otimes \omega^{(-2t+1-n)/2}$ and is either orthogonal or symplectic. Hence $\pi \otimes \mathrm{sp}(n)$ is essentially orthogonal or essentially symplectic of weight $-2t+1-n$.

Conversely, suppose that $\pi \otimes \mathrm{sp}(n)$ is essentially orthogonal or essentially symplectic of some weight u. Then $\sigma' \otimes \omega^{u/2}$ is self-contragredient. Hence if an irreducible representation of $\mathcal{W}(\overline{K}/K)$ occurs in $\sigma' \otimes \omega^{u/2}$ so does its contragredient. It follows that $\pi^* \otimes \omega^{-u/2}$ is isomorphic to $\pi \otimes \omega^{j+u/2}$ for some j $(0 \le j \le n-1)$. Writing $\pi = \rho \otimes \omega^{t+i\theta}$ and equating $|\det \pi^* \otimes \omega^{-u/2}|$ with $|\det \pi \otimes \omega^{j+u/2}|$, we find that $j = -2t-u$, whence $\rho \otimes \omega^{i\theta}$ is self-contragredient. In particular, $(\det(\rho \otimes \omega^{i\theta}))^2 = 1$, and since the values of $\det\rho$ are roots of unity, we see that $q^{i\theta}$ is also a root of unity. Hence after replacing ρ by $\rho \otimes \omega^{i\theta}$ we may assume that $\theta = 0$. Then ρ, being both self-contragedient and of finite image, has real-valued trace. Consequently, so do $\pi = \rho \otimes \omega^t$ and $\sigma = \pi \otimes (1 \oplus \omega \oplus \cdots \oplus \omega^{n-1})$. Now $\operatorname{tr}\sigma'(gz) = \operatorname{tr}\sigma(g)$ for $g \in \mathcal{W}(\overline{K}/K)$ and $z \in \mathbb{C}$, as one sees by taking $\sigma' = \pi \otimes \mathrm{sp}(n)$ in (3.3). Hence $\operatorname{tr}\sigma'$ is also real-valued.

Finally, suppose that σ' is both essentially orthogonal and essentially symplectic. Then there exist $u, u' \in \mathbb{R}$ such that $\sigma' \otimes \omega^{u/2}$ is orthogonal and $\sigma' \otimes \omega^{u'/2}$ is symplectic. In particular, the square of the determinant of both representations is 1, whence $u = u'$. Thus $\sigma' \otimes \omega^{u/2}$ is both orthogonal and symplectic. Since Schur's Lemma holds for an admissible indecomposable representation, the usual argument shows that an invariant bilinear form is unique up to scalar multiples, and we get a contradiction.

TERMINOLOGY. One usually defines a representation σ' to be essentially unitary if there is a quasicharacter χ of $\mathcal{W}(\overline{K}/K)$ such that $\sigma' \otimes \chi$ is unitary. However, if such a quasicharacter exists then one can choose it to be of the form $\chi = \omega^{t/2}$ for some $t \in \mathbb{R}$. Therefore the definition of "essentially unitary" given here agrees with the usual notion.

On the other hand, the requirement that $\sigma' \otimes \omega^t$ be orthogonal or symplectic for some $t \in \mathbb{R}$ is strictly stronger than the requirement that $\sigma' \otimes \chi$ be orthogonal or symplectic for some quasicharacter χ.

8. The L-factor

Let $\sigma' = (\sigma, N)$ be a representation of $\mathcal{W}'(\overline{K}/K)$ on a vector space V. Put

$$V^I = V^{\sigma(I)} = \{v \in V : \sigma(g)v = v \text{ for all } g \in I\},$$

$$V_N = \ker N,$$

and

$$V_N^I = V^I \cap V_N.$$

The compatibility relation (3.2) and the fact that I is normal in $\mathcal{W}(\overline{K}/K)$ together imply that V^I and V_N^I are invariant subspaces of V. Furthermore, if Φ is an inverse Frobenius element, then the restriction of $\sigma(\Phi)$ to V^I or to V_N^I is independent of the choice of Φ. For simplicity let us write $\sigma(\Phi)|V_N^I$ as $\Phi|V_N^I$. The L-factor of σ' is the meromorphic function

$$L(\sigma', s) = \det(1 - q^{-s}\Phi|V_N^I)^{-1}.$$

Its properties are as follows:

($L1$) $L(\sigma' \oplus \tau', s) = L(\sigma', s)L(\tau', s)$.

($L2$) $L(\mathrm{ind}_{L/K}\, \rho', s) = L(\rho', s)$.

Here τ' is another representation of $\mathcal{W}'(\overline{K}/K)$ and ρ' is a representation of $\mathcal{W}'(\overline{K}/L)$, with L a finite extension of K. Property ($L1$) is immediate, and in fact a stronger property holds if we restrict ourselves to representations with $N = 0$: on such representations $L(*, s)$ is multiplicative in short exact sequences, i.e. the map $\sigma = (\sigma, 0) \mapsto L(\sigma, s)$ determines a homomorphism from the Grothendieck group of virtual representations of $\mathcal{W}(\overline{K}/K)$ into the group of nonzero meromorphic functions on $\mathbb{C}$. In general, though, all we can assert is ($L1$), because unlike $V \mapsto V^I$, the functor $V \mapsto V_N$ is not exact. As for ($L2$), it can be deduced from two elementary lemmas (cf. [**3**, Prop. 3.8]):

LEMMA 1. *Let W be a finite-dimensional vector space over $\mathbb{C}$, T an endomorphism of W, f a positive integer, and T_f the endomorphism of $\mathbb{C}^f \otimes W$ given by*

$$T_f(e_j \otimes w) = e_{j+1} \otimes w \qquad (w \in W,\ 0 \le j \le f-2),$$
$$T_f(e_{f-1} \otimes w) = e_0 \otimes T(w).$$

Then

$$\det(1 - xT_f) = \det(1 - x^f T).$$

For the statement of the next lemma it is convenient to employ the language of "$\mathbb{C}[G]$-modules" rather than of "representations".

LEMMA 2. *Let G be a group, H a subgroup of G of finite index, and I a normal subgroup of G. Put $J = I \cap H$. Given a $\mathbb{C}[H]$-module U, we have an isomorphism of G/I-modules*

$$(\operatorname{ind}_H^G U)^I \cong \operatorname{ind}_{H/J}^{G/I} U^J,$$

where H/J is identified with the subgroup HI/I of G/I.

Let us recall Deligne's argument deducing $(L2)$ from Lemmas 1 and 2. Put $G = \mathcal{W}(\overline{K}/K)$, $H = \mathcal{W}(\overline{K}/L)$, and $J = I \cap H = I_L$. Write U for the space of the representation $\rho' = (\rho, M)$ of H and $\sigma' = (\sigma, N)$ for the induced representation on $V = \mathbb{C}[G] \otimes_{\mathbb{C}[H]} U$. The explicit formula for N in part (iv) of the proposition of Section 3 gives identifications

$$V_N = \mathbb{C}[G] \otimes_{\mathbb{C}[H]} U_M = \operatorname{ind}_{L/K} U_M,$$

so that

$$V_N^I = \operatorname{ind}_{H/J}^{G/I} U_M^J \tag{8.1}$$

by Lemma 2. Hence

$$L(\sigma', s) = \det(1 - q^{-s}\Phi | \operatorname{ind}_{H/J}^{G/I} U_M^J)^{-1}. \tag{8.2}$$

On the other hand, if we put $W = U_M^J$, then

$$\operatorname{ind}_{H/J}^{G/I} U_M^J = \mathbb{C}[G/I] \otimes_{\mathbb{C}[H/J]} W. \tag{8.3}$$

Denoting the residue class degree $f(L/K)$ simply by f, we can identify the right-hand side of (8.3) with $\mathbb{C}^f \otimes W$ by making the coset of Φ^j in G/I correspond to the standard basis vector e_j in $\mathbb{C}^f$. Hence if Φ_L is an inverse Frobenius element of L (equal to $\Phi^f i$ for some $i \in I$) and $T = \Phi_L | W$, then Lemma 1 gives

$$\det(1 - x\Phi | \operatorname{ind}_{H/J}^{G/I} U_M^J) = \det(1 - xT_f) = \det(1 - x^f T).$$

Taking $x = q^{-s}$ and referring to (8.2), we obtain $(L2)$.

Property $(L1)$ reduces the computation of L-factors of admissible representations to the case of admissible indecomposable representations. The latter computation reduces in turn to the case of irreducible representations:

PROPOSITION. *Suppose that $\sigma' = \pi \otimes \mathrm{sp}(n)$, where π is an irreducible representation of $\mathcal{W}(\overline{K}/K)$ and n is a positive integer. Then*

$$L(\sigma', s) = L(\pi, s + n - 1).$$

PROOF. Let W be the space of π, so that $V = W \otimes \mathbb{C}^n$ is the space of σ'. Then $V_N^I = W^I \otimes e_{n-1}$, and Φ acts on $W^I \otimes e_{n-1}$ via the automorphism $(\pi(\Phi)|W^I) \otimes q^{1-n}$.

9. L-factors and ℓ-adic representations

Let ℓ be a prime different from p and let $\sigma'_\ell : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}(V_\ell)$ be an ℓ-adic representation. Given an embedding $\iota : \mathbb{Q}_\ell \hookrightarrow \mathbb{C}$ (and hence an embedding $\iota : \mathbb{Q}_\ell(x) \hookrightarrow \mathbb{C}(x)$ satisfying $\iota(x) = x$) we can define an L-factor $L(\sigma'_\ell, \iota, s)$ by putting

$$L(\sigma'_\ell, \iota, s) = \iota(\det(1 - x\sigma'_\ell(\Phi)|V_\ell^I)^{-1})|_{x=q^{-s}}.$$

On the other hand, we have seen how to associate to σ'_ℓ and ι a representation $\sigma'_{\ell,\iota} = (\sigma_{\ell,\iota}, N_{\ell,\iota})$ of $\mathcal{W}'(\overline{K}/K)$, whence an L-factor $L(\sigma'_{\ell,\iota}, s)$. These two L-factors are equal:

PROPOSITION. $L(\sigma'_\ell, \iota, s) = L(\sigma'_{\ell,\iota}, s)$.

PROOF. Put $V = \mathbb{C} \otimes_\iota V_\ell$. In the notation of Section 4 we have

$$N_{\ell,\iota} = 1_{\mathbb{C}} \otimes N_\ell$$

and

$$\sigma_{\ell,\iota}(g) = 1_{\mathbb{C}} \otimes \sigma_\ell(g) = 1_{\mathbb{C}} \otimes (\sigma'_\ell(g)\exp(-t_\ell(i)N_\ell))$$

$(g = \Phi^m i \in \mathcal{W}(\overline{K}/K),\ m \in \mathbb{Z},\ i \in I)$. Hence $V_N = \mathbb{C} \otimes \ker N_\ell$ and

$$\sigma_{\ell,\iota}(g)|V_N = 1_{\mathbb{C}} \otimes (\sigma'_\ell(g)|\ker N_\ell). \tag{9.1}$$

It follows that

$$V_N^I = \mathbb{C} \otimes ((\ker N_\ell) \cap V_\ell^I). \tag{9.2}$$

But V_ℓ^I is contained in $\ker N_\ell$, because σ'_ℓ coincides with the map $i \mapsto \exp(t_\ell(i)N_\ell)$ on an open subgroup of I. Therefore (9.2) can be rewritten $V_N^I = \mathbb{C} \otimes V_\ell^I$, and then (9.1) gives

$$\sigma_{\ell,\iota}(\Phi)|V_N^I = 1_{\mathbb{C}} \otimes (\sigma'_\ell(\Phi)|V_\ell^I).$$

10. The conductor

We let $\mathcal{O}$ and ϖ denote respectively the ring of integers and a uniformizer of K, and if R is any extension of K inside $\overline{K}$ we let $\mathcal{O}_R$ denote the ring of integers of R. If RK_{unr} has finite degree over K_{unr} then it is also meaningful to speak of a uniformizer ϖ_R of R.

Let $\sigma' = (\sigma, N)$ be a representation of $\mathcal{W}'(\overline{K}/K)$. We would like to define the conductor $\mathfrak{N}(\sigma')$ of σ'. It is to be a nonzero ideal of $\mathcal{O}$, hence of the form

$$\mathfrak{N}(\sigma') = \varpi^{a(\sigma')}\mathcal{O}$$

for some nonnegative integer $a(\sigma')$. This integer is the sum of two terms,

$$a(\sigma') = a(\sigma) + b(\sigma'),$$

and as the notation indicates, the first term depends only on σ, not on N. Furthermore, if $N = 0$ then $b(\sigma') = 0$, so that $a((\sigma, 0)) = a(\sigma)$; thus the notation is consistent with our practice of identifying σ with $(\sigma, 0)$.

The term $b(\sigma')$ is the simpler of the two to define: writing V for the space of σ' we have

$$b(\sigma') = \dim V^I/V_N^I.$$

This quantity has the following properties (notation as in ($L1$) and ($L2$)):

($b1$) $b(\sigma' \oplus \tau') = b(\sigma') + b(\tau')$.

($b2$) $b(\mathrm{ind}_{L/K}\,\rho') = f(L/K)b(\rho')$.

For insight into this formalism, observe that since V_N^I is an invariant subspace of V^I, the characteristic polynomial of Φ on V_N^I divides its characteristic polynomial on V^I. Thus if we think of the L-factor as the reciprocal of a characteristic polynomial, then we see that $L(\sigma', s)/L(\sigma, s)$ is a polynomial in q^{-s}, and in fact that

$$b(\sigma') = \text{ degree in } q^{-s} \text{ of } \frac{L(\sigma', s)}{L(\sigma, s)}.$$

Hence $(b1)$ and $(b2)$ follow from $(L1)$ and $(L2)$ (of course one must also note that $q_L^{-s} = (q^{-s})^{f(L/K)}$).

The definition of $a(\sigma)$ is slightly more involved. Choose a finite Galois extension R of K_{unr} such that σ is trivial on the subgroup $\mathrm{Gal}(\overline{K}/R)$ of I, and put $G = \mathrm{Gal}(R/K_{\mathrm{unr}})$. Let v_R be the valuation on R and $G = G_0 \supset G_1 \supset G_2 \supset \dots$ the higher ramification groups, defined by

$$G_j = \{g \in G : v_R(g(\varpi_R) - \varpi_R) \geq j + 1\}.$$

Then

$$a(\sigma) = \sum_{j=0}^{\infty} \frac{|G_j|}{|G|} \dim(V/V^{G_j}), \tag{10.1}$$

where V is the space of σ and V^{G_j} the subspace of vectors fixed by G_j. It is easily verified that all but finitely many terms in the sum are 0, that the definition is independent of the choice of R, and that $a(\sigma)$ is a nonnegative rational number which is positive if and only if σ is ramified. Furthermore, it is known that $a(\sigma)$ is a nonnegative *integer* (cf. [**10**, p. 99, Thm. 1′; p. 100, Cor. 1′]) and that the following properties hold:

$(a1)$ $a(*)$ is additive in short exact sequences, i.e. the map $\sigma \mapsto a(\sigma)$ determines a homomorphism from the Grothendieck group of virtual representations of $\mathcal{W}(\overline{K}/K)$ into $\mathbb{Z}$.

$(a2)$ Let L be a finite extension of K in $\overline{K}$ and ρ a representation of $\mathcal{W}(\overline{K}/L)$. Write the relative discriminant of L/K as $\varpi^{d(L/K)}\mathcal{O}$. Then

$$a(\mathrm{ind}_{L/K}\,\rho) = \dim(\rho)d(L/K) + f(L/K)a(\rho).$$

$(a3)$ Let χ be a quasicharacter of $L^\times$, identified with a one-dimensional representation of $\mathcal{W}(\overline{K}/L)$ by local class field theory. If χ is unramified, then $a(\chi) = 0$; otherwise $a(\chi)$ is the smallest positive integer m such that χ is trivial on $1 + \varpi_L^m \mathcal{O}_L$.

Property $(a1)$ is straightforward; for proofs of the other two assertions see [**10**, pp. 101–102, Prop. 5 and Cor. to Prop. 4]. What is important here is that if we grant the existence of a function $a(*)$ satisfying $(a1)$, $(a2)$, and $(a3)$, then these properties actually serve to define $a(\sigma)$ for every representation σ of $\mathcal{W}(\overline{K}/K)$, and we can dispense with the explicit formula (10.1): indeed if we write $[\sigma]$ as in Corollary 2 of Section 2, then

$$a(\sigma) = \sum_{(L,\chi,\chi')} c_{L,\chi,\chi'} f(L/K)(a(\chi) - a(\chi')), \tag{10.2}$$

and the right-hand side is uniquely determined by property $(a3)$. The remark will become important in Section 11.

Let us return now to $\sigma' = (\sigma, N)$ and to $a(\sigma') = a(\sigma) + b(\sigma')$. Recall that σ' is said to be unramified if σ is unramified and $N = 0$. These conditions being equivalent to the vanishing of $a(\sigma)$ and of $b(\sigma')$, it follows that σ' is unramified if and only if $a(\sigma') = 0$. Furthermore, from the properties of $b(\sigma')$ and $a(\sigma)$ listed above we obtain:

($a'1$) $a(\sigma' \oplus \tau') = a(\sigma') + a(\tau')$.

($a'2$) $a(\mathrm{ind}_{L/K}\, \rho') = \dim(\rho')d(L/K) + f(L/K)a(\rho')$.

($a'3$) If $\dim \sigma' = 1$, so that $\sigma' = (\sigma, 0)$, then $a(\sigma') = a(\sigma)$ is given by ($a3$).

Property ($a'1$) reduces the calculation of $a(\sigma')$ for an arbitrary admissible representation to the case of an admissible indecomposable representation. As with the L-factor, we can further reduce to the case of an irreducible representation of $\mathcal{W}(\overline{K}/K)$:

PROPOSITION. *Suppose that $\sigma' = \pi \otimes \mathrm{sp}(n)$, where π is an irreducible representation of $\mathcal{W}(\overline{K}/K)$ and n is a positive integer. Then*

$$a(\sigma') = \begin{cases} na(\pi) & \text{if } \pi \text{ is ramified,} \\ n-1 & \text{if } \pi \text{ is unramified.} \end{cases}$$

PROOF. Let W be the space of π, so that $V = W \otimes \mathbb{C}^n$ is the space of σ'. Then $V^I = W^I \otimes \mathbb{C}^n$ and $V_N^I = W^I \otimes e_{n-1}$. Since π is irreducible we have either $W^I = \{0\}$ (if π is ramified) or $W^I = W$ (if π is unramified). In the latter case W is one-dimensional, because $\mathcal{W}(\overline{K}/K)/I$ is abelian. It follows that $b(\sigma')$ is 0 or $n-1$ according as π is ramified or unramified. On the other hand, σ is the direct sum of the representations $\pi \otimes \omega^j$ for $0 \leq j \leq n-1$, and it is immediate from (10.1) that $a(\pi \otimes \omega^j) = a(\pi)$. Therefore $a(\sigma) = na(\pi)$.

Finally, let us mention an alternative formulation of ($a'1$) and ($a'2$) in the case where K has characteristic 0. In this case K contains $\mathbb{Q}_p$, and we can speak of the absolute discriminant of K, an ideal of $\mathbb{Z}_p$ with a unique positive rational integral generator D. Putting

$$A(\sigma') = D^{\dim \sigma'} q^{a(\sigma')} = \mathrm{N}(\mathfrak{D}^{\dim \sigma'} \mathfrak{N}(\sigma')),$$

where $\mathfrak{D}$ is the different ideal of K, we have

($A1$) $A(\sigma' \oplus \tau') = A(\sigma')A(\tau')$.

($A2$) $A(\mathrm{ind}_{L/K}\, \rho') = A(\rho')$.

For ($A2$) one uses the standard formula $D_L = D^{[L:K]} q^{d(L/K)}$, where D_L denotes the discriminant of L.

11. The epsilon factor

By an *additive character* of K we mean a nontrivial unitary character of the additive group of K, i.e. a continuous homomorphism $\psi : K \longrightarrow \mathbb{C}^\times$ which is nontrivial and of absolute value 1. The first point to make about the epsilon factor of a representation $\sigma' = (\sigma, N)$ of $\mathcal{W}'(\overline{K}/K)$ is that it depends on more than just σ': it also depends on the choice of an additive character ψ of K and of a Haar measure dx on K. Hence we denote the epsilon factor $\epsilon(\sigma', \psi, dx)$. If K has characteristic 0 then there is a nearly canonical choice of ψ and dx given by

$$\psi_{\mathrm{can}}(x) = e^{2\pi i \lambda(\mathrm{tr}_{K/\mathbb{Q}_p}(x))} \tag{11.1}$$

and

$$\int_{\mathcal{O}} dx_{\text{can}} = D^{-1/2}, \tag{11.2}$$

where $\lambda : \mathbb{Q}_p \to \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow \mathbb{Q}/\mathbb{Z} \hookrightarrow \mathbb{R}/\mathbb{Z}$ is the composition of natural maps. But the choice $\overline{\psi}_{\text{can}}$ is also canonical, and we shall avoid premature specialization.

The second point about the epsilon factor is that it is really the product of two factors:

$$\epsilon(\sigma', \psi, dx) = \epsilon(\sigma, \psi, dx)\delta(\sigma').$$

As the notation suggests, the second factor is independent of ψ and dx, while the first is independent of N. The factors are defined in such a way that if $N = 0$ then $\delta(\sigma') = 1$; equivalently, $\epsilon((\sigma, 0), \psi, dx) = \epsilon(\sigma, \psi, dx)$, as one would hope.

The delta factor is the simpler factor to define. If V is the space of σ' then the action of an inverse Frobenius element Φ on the quotient space V^I/V_N^I is independent of the choice of Φ, and we put

$$\delta(\sigma') = \det(-\Phi | V^I/V_N^I).$$

This satisfies a familiar formalism:

($\delta 1$) $\delta(\sigma' \oplus \tau') = \delta(\sigma')\delta(\tau')$.

($\delta 2$) $\delta(\operatorname{ind}_{L/K} \rho') = \delta(\rho')$.

The similarity between these properties and those of the L-factor is not coincidental, for we have

$$\delta(\sigma') = \frac{\det(-\Phi|V^I)}{\det(-\Phi|V_N^I)} = \lim_{s\to-\infty} \frac{q^{s \dim V^I} L(\sigma, s)^{-1}}{q^{s \dim V_N^I} L(\sigma', s)^{-1}} = \lim_{s\to-\infty} q^{b(\sigma')s} \frac{L(\sigma', s)}{L(\sigma, s)}.$$

Hence ($\delta 1$) and ($\delta 2$) follow from ($L1$), ($L2$), ($b1$), and ($b2$).

We come next to the definition of $\epsilon(\sigma)$. In contrast to $a(\sigma)$, for which we have the explicit formula (10.1), $\epsilon(\sigma, \psi, dx)$ has no known definition other than by the analogues of properties ($a1$), ($a2$), and ($a3$). More precisely, Langlands and Deligne **[3]** have proved the existence of a function $\epsilon(*, *, *)$ satisfying the following conditions:

($\epsilon 1$) $\epsilon(*, \psi, dx)$ is multiplicative in short exact sequences, i.e. the map $\sigma \mapsto \epsilon(\sigma, \psi, dx)$ determines a homomorphism from the Grothendieck group of virtual representations of $\mathcal{W}(\overline{K}/K)$ to $\mathbb{C}^\times$.

($\epsilon 2$) Let L be a finite extension of K in $\overline{K}$ and ρ a virtual representation of $\mathcal{W}(\overline{K}/L)$. Then for any choice of Haar measure dx_L on L,

$$\epsilon(\operatorname{ind}_{L/K} \rho, \psi, dx) = \epsilon(\rho, \psi \circ \operatorname{tr}_{L/K}, dx_L)\, \theta(L/K, \psi, dx, dx_L)^{\dim \rho},$$

where

$$\theta(L/K, \psi, dx, dx_L) = \frac{\epsilon(\operatorname{ind}_{L/K} 1_L, \psi, dx)}{\epsilon(1_L, \psi \circ \operatorname{tr}_{L/K}, dx_L)}.$$

($\epsilon 3$) Let χ be a quasicharacter of $L^\times$, identified with a representation of dimension 1 of $\mathcal{W}(\overline{K}/L)$ by local class field theory. Let ψ_L be an additive character of L, and write $n(\psi_L)$ for the largest integer n such that ψ_L is trivial on $\varpi_L^{-n}\mathcal{O}_L$. Let $c \in L^\times$ be any element of valuation $n(\psi_L) + a(\chi)$. Then

$$\epsilon(\chi, \psi_L, dx_L) = \begin{cases} \int_{c^{-1}\mathcal{O}_L^\times} \chi^{-1}(x)\psi_L(x)\, dx_L & \text{if } \chi \text{ is ramified,} \\ \chi\omega^{-1}(c) \int_{\mathcal{O}_L} dx_L & \text{if } \chi \text{ is unramified.} \end{cases}$$

The formulas in (ϵ3) are those imposed by Tate's local functional equation for L-functions of quasicharacters [**14**]. Now if $[\sigma]$ is written as in Corollary 2 of Section 2 then (ϵ1) and (ϵ2) give

$$\epsilon(\sigma, \psi, dx) = \epsilon(1_K, \psi, dx)^{\dim\sigma} \prod_{(L,\chi,\chi')} \left(\frac{\epsilon(\chi, \psi \circ \mathrm{tr}_{L/K}, dx_L)}{\epsilon(\chi', \psi \circ \mathrm{tr}_{L/K}, dx_L)} \right)^{c_{L,\chi,\chi'}}, \tag{11.3}$$

and the right-hand side is uniquely determined by (ϵ3).

With this definition of $\epsilon(\sigma, \psi, dx)$ in hand, let us return to $\epsilon(\sigma', \psi, dx) = \epsilon(\sigma, \psi, dx)\delta(\sigma')$. Its properties follow from those of its factors:

(ϵ'1) $\epsilon(\sigma' \oplus \tau', \psi, dx) = \epsilon(\sigma', \psi, dx)\epsilon(\tau', \psi, dx)$.

(ϵ'2) $\epsilon(\mathrm{ind}_{L/K}\, \rho', \psi, dx) = \epsilon(\rho', \psi \circ \mathrm{tr}_{L/K}, dx_L)\, \theta(L/K, \psi, dx, dx_L)^{\dim\rho}$, where the factor $\theta(L/K, \psi, dx, dx_L)$ is as in (ϵ2).

(ϵ'3) If $\dim\sigma' = 1$, so that $\sigma' = (\sigma, 0)$, then $\epsilon(\sigma', \psi, dx) = \epsilon(\sigma, \psi, dx)$ is as in (ϵ3).

As with (L1) and (a'1), property (ϵ'1) reduces the calculation of $\epsilon(\sigma', \psi, dx)$ for admissible σ' to the case of admissible indecomposable σ'. A further reduction to the case of irreducible σ will be given in Section 12. But for this and other applications we must first record the dependence of $\epsilon(\sigma, \psi, dx)$ on the choice of ψ and dx, and the effect on $\epsilon(\sigma, \psi, dx)$ of twisting σ by ω^s.

Given $\alpha \in K^\times$, write ψ_α for the additive character $x \mapsto \psi(\alpha x)$. Any additive character of K is equal to ψ_α for some α, and any Haar measure on K has the form $r dx$ for some positive real number r. Recall that $\det\sigma$ and ω can be viewed as characters of $K^\times$.

PROPOSITION.
(i) $\epsilon(\sigma, \psi_\alpha, dx) = \det\sigma(\alpha)\omega(\alpha)^{-\dim\sigma}\epsilon(\sigma, \psi, dx)$.
(ii) $\epsilon(\sigma, \psi, r dx) = r^{\dim\sigma}\epsilon(\sigma, \psi, dx)$.
(iii) $\epsilon(\sigma \otimes \omega^s, \psi, dx) = \epsilon(\sigma, \psi, dx) q^{-s(n(\psi)\dim(\sigma) + a(\sigma))}$.

PROOF. When $\dim\sigma = 1$, all three statements are readily deduced from the explicit formulas in (ϵ3). Property (ii) then follows in general from (11.3). For (iii) one uses (10.2) as well as (11.3). For (i) one also needs the fact that if $[\sigma]$ is written as in Corollary 2 of Section 2, then

$$\det\sigma = \prod_{(L,\chi,\chi')} \left(\frac{\chi}{\chi'} \,\Big|\, K^\times \right)^{c_{L,\chi,\chi'}}. \tag{11.4}$$

This follows from the general identity

$$\det(\mathrm{ind}_H^G \chi) = (\mathrm{sign}_H^G)(\chi \circ \mathrm{trans}_H^G), \tag{11.5}$$

where G is any group, H a subgroup of finite index, χ a one-dimensional character of H, sign_H^G the determinant of the permutation representation of G on the left cosets of H, and trans_H^G the transfer from G^{ab} to H^{ab} (see [**3**, Prop. 1.2], or [**6**]). Of course if G is a topological group and χ is continuous, then (11.5) is still valid if we interpret G^{ab} and H^{ab} to be the group modulo the *closure* of its commutator subgroup. Hence to deduce (11.4) from (11.5) one need only recall that in the class-field-theoretic identification of multiplicative groups of local fields with abelianized Weil groups, the transfer from $\mathcal{W}(\overline{K}/K)^{\mathrm{ab}}$ to $\mathcal{W}(\overline{K}/L)^{\mathrm{ab}}$ corresponds to the inclusion of $K^\times$ in $L^\times$.

REMARK. It follows from (ii) that on virtual representations of dimension 0, $\epsilon(*, \psi, dx)$ is independent of dx, which can therefore be omitted from the notation. Thus if ρ is a virtual representation of $\mathcal{W}(\overline{K}/L)$ of dimension 0, then ($\epsilon 2$) takes the form

$$\epsilon(\mathrm{ind}_{L/K}\,\rho, \psi) = \epsilon(\rho, \psi \circ \mathrm{tr}_{L/K}).$$

This property is described in the literature by saying that the epsilon factor is "inductive in degree 0".

12. The root number

The root number associated to a representation σ' of $\mathcal{W}'(\overline{K}/K)$ and an additive character ψ of K is

$$W(\sigma', \psi) = \frac{\epsilon(\sigma', \psi, dx)}{|\epsilon(\sigma', \psi, dx)|},$$

where dx is any Haar measure on K. As the notation suggests, the value of $W(\sigma', \psi)$ is independent of the choice of dx (Section 11, Prop. (ii)). If σ' is an essentially symplectic representation then $W(\sigma', \psi)$ is even independent of ψ (Section 11, Prop. (i)), for the determinant of a symplectic representation is trivial, and therefore the determinant of an essentially symplectic representation is ω^u for some $u \in \mathbb{R}$. Thus if σ' is essentially symplectic we shall denote the root number simply by $W(\sigma')$.

We begin with a lemma which is valid for any σ'. Let $\mathcal{S}(K)$ be the Schwartz space of K, i.e. the space of locally constant complex-valued functions on K with compact support. If ψ is an additive character of K then the self-dual measure relative to ψ is the unique Haar measure dx_ψ on K such that the Fourier transform

$$\hat{f}(y) = \int_K f(x)\psi(xy)dx_\psi$$

is an isometry of the L^2-norm on $\mathcal{S}(K)$.

LEMMA.
(i) $\epsilon(\sigma, \psi, dx_\psi)\epsilon(\sigma^*, \psi, dx_\psi) = \det\sigma(-1)q^{n(\psi)\dim(\sigma)+a(\sigma)}$.
(ii) $\delta(\sigma')\delta(\sigma'^*) = q^{b(\sigma')}$.
(iii) $\epsilon(\sigma', \psi, dx_\psi)\epsilon(\sigma'^*, \psi, dx_\psi) = \det\sigma(-1)q^{n(\psi)\dim(\sigma')+a(\sigma')}$.

PROOF.
(i) If σ is a quasicharacter χ, then (i) follows from ($\epsilon 3$) by an elementary calculation, familiar from the theory of Gauss sums. Alternatively, we can appeal directly to Tate's local functional equation [**14**], which is after all the source of ($\epsilon 3$):

$$\frac{\int \hat{f}(x)\chi^{-1}\omega^{1-s}(x)d^\times x}{L(\chi^{-1}, 1-s)} = \epsilon(\chi\omega^s, \psi, dx_\psi)\frac{\int f(x)\chi\omega^s(x)d^\times x}{L(\chi, s)}.$$

Here $f \in \mathcal{S}(K)$ is arbitrary, $d^\times x$ is any Haar measure on $K^\times$, and the equation is to be understood by analytic continuation in s (i.e. each side makes sense on some nonempty open subset of $\mathbb{C}$ and the two sides are equal as meromorphic functions on $\mathbb{C}$). Choosing f so that the integrals do not vanish identically, we deduce that

$$\epsilon(\chi\omega^s, \psi, dx_\psi)\epsilon(\chi^{-1}\omega^{1-s}, \psi, dx_\psi) = \chi(-1),$$

because $\hat{\hat{f}}(x) = f(-x)$. Hence the formula follows from part (iii) of the proposition of Section 11.

In general, we write $\epsilon(\sigma, \psi, dx_\psi)$ as in (11.3). Then $\epsilon(\sigma^*, \psi, dx_\psi)$ is expressed by the same formula, but with each quasicharacter replaced by its inverse. Hence we obtain (i) from (10.2), (11.4), and the one-dimensional case.

(ii) Write $\sigma' = (\sigma, N)$ and $\sigma'^* = (\sigma^*, N^*)$, and let V and V^* be the respective spaces. Since the subspace $N(V)$ of V is invariant under $\mathcal{W}(\overline{K}/K)$, its dual space $N(V)^*$ is a representation space for $\mathcal{W}(\overline{K}/K)$ via the contragredient action. In what follows we shall mingle "$\mathcal{W}(\overline{K}/K)$-modules" and "representations of $\mathcal{W}(\overline{K}/K)$" freely, writing for example $N^*(V^*)\otimes\omega^{-1}$ to indicate the tensor product of the representation of $\mathcal{W}(\overline{K}/K)$ on $N^*(V^*)$ with ω^{-1}. The map $N^*(V^*)\otimes\omega^{-1} \to N(V)^*$ given by $N^*f \mapsto f|N(V)$ is a well-defined isomorphism intertwining the action of $\mathcal{W}(\overline{K}/K)$, so that

$$N^*(V^*)\otimes\omega^{-1} \cong N(V)^*. \tag{12.1}$$

Taking I-invariants on both sides of (12.1), we find

$$N^*(V^{*I})\otimes\omega^{-1} \cong N(V^I)^*. \tag{12.2}$$

Now N and N^* determine $\mathcal{W}(\overline{K}/K)$-isomorphisms

$$(V^I/V_N^I)\otimes\omega \cong N(V^I)$$

and

$$V^{*I}/V_{N^*}^{*I} \cong N^*(V^{*I})\otimes\omega^{-1}$$

respectively, and substitution in (12.2) gives

$$V^{*I}/V_{N^*}^{*I} \cong (V^I/V_N^I)^*\otimes\omega^{-1}. \tag{12.3}$$

In particular, (12.3) implies that

$$\det\left(-\sigma^*(\Phi)|V^{*I}/V_{N^*}^{*I}\right) = \det\left(-q\sigma(\Phi^{-1})|V^I/V_N^I\right),$$

proving (ii).

(iii) This follows from (i) and (ii).

Recall that if K has characteristic 0 we put $A(\sigma') = D^{\dim\sigma'}q^{a(\sigma')}$ and define ψ_{can} and dx_{can} by (11.1) and (11.2).

PROPOSITION. *Suppose that for some $t \in \mathbb{R}$ the representation σ' is essentially unitary, essentially orthogonal, or essentially symplectic of weight t. Let ψ be an additive character of K.*

(i) $|\epsilon(\sigma', \psi, dx_\psi)| = q^{\frac{t+1}{2}(n(\psi)\dim(\sigma')+a(\sigma'))}$.

(ii) *If K has characteristic 0 and ψ is either ψ_{can} or $\overline{\psi}_{\mathrm{can}}$, then*

$$\epsilon(\sigma', \psi, dx_{\mathrm{can}}) = W(\sigma', \psi)A(\sigma')^{(t+1)/2}.$$

(iii) *If σ' is essentially orthogonal then $W(\sigma', \psi)^4 = 1$.*

(iv) *If σ' is essentially symplectic then $W(\sigma') = \pm 1$.*

PROOF. First suppose that σ' is either essentially orthogonal or essentially symplectic of weight t. Then the space of $\sigma'\otimes\omega^{t/2}$ admits a nondegenerate invariant bilinear form, so that $\sigma'\otimes\omega^{t/2}$ is isomorphic to its contragredient. Thus σ'^* is isomorphic to $\sigma'\otimes\omega^t$. Applying part (iii) of the lemma as well as part (iii) of the proposition of Section 11, we see that

$$\epsilon(\sigma',\psi,dx_\psi)^2 = \det\sigma(-1)q^{(t+1)(n(\psi)\dim(\sigma')+a(\sigma'))}.$$

Parts (i), (iii), and (iv) of the proposition follow immediately from this equation. So does (ii), for if ψ is either ψ_{can} or $\overline{\psi}_{\mathrm{can}}$, then $dx_\psi = dx_{\mathrm{can}}$ and $q^{n(\psi)} = D$.

Next suppose that σ' is essentially unitary of weight t, so that the space of $\sigma'\otimes\omega^{t/2}$ admits a nondegenerate invariant hermitian form. Then σ'^* is isomophic to $\overline{\sigma'}\otimes\omega^t$, where $\overline{\sigma'}$ is defined up to isomorphism by viewing σ' as a map $\mathcal{W}'(\overline{K}/K)\to \mathrm{GL}(d,\mathbb{C})$ for some d and composing with complex conjugation. Hence this time the lemma gives

$$\epsilon(\sigma',\psi,dx_\psi)\epsilon(\overline{\sigma'},\psi,dx_\psi) = \det\sigma(-1)q^{(t+1)(n(\psi)\dim(\sigma')+a(\sigma'))},$$

or equivalently (Section 11, Prop. (i)),

$$\epsilon(\sigma',\psi,dx_\psi)\epsilon(\overline{\sigma'},\psi_{-1},dx_\psi) = q^{(t+1)(n(\psi)\dim(\sigma')+a(\sigma'))}. \tag{12.4}$$

We claim that

$$\epsilon(\overline{\sigma'},\psi_{-1},dx_\psi) = \overline{\epsilon(\sigma',\psi,dx_\psi)}, \tag{12.5}$$

or more precisely, that

$$\delta(\overline{\sigma'}) = \overline{\delta(\sigma')} \tag{12.6}$$

and

$$\epsilon(\overline{\sigma},\psi_{-1},dx_\psi) = \overline{\epsilon(\sigma,\psi,dx_\psi)}. \tag{12.7}$$

Indeed (12.6) is immediate, while (12.7) follows from (ϵ3) for $\dim\sigma = 1$ and from (11.4) in general. Therefore (12.5) holds, and substitution in (12.4) gives (i) and (ii).

REMARK. Deligne has proved a formula relating root numbers of orthogonal representations of $\mathcal{W}(\overline{K}/K)$ to Stiefel-Whitney classes ([**5**, Prop. 5.2]).

We can now make good on our promise to express epsilon factors of admissible indecomposable representations in terms of epsilon factors of irreducible representations.

COROLLARY. *Suppose that $\sigma' = \pi\otimes\mathrm{sp}(n)$, where π is an irreducible representation of $\mathcal{W}(\overline{K}/K)$ and n is a positive integer. Write $\pi = \rho\otimes\omega^{t+i\theta}$ with ρ of Galois type and $t,\theta\in\mathbb{R}$. If π is unramified and hence one-dimensional, put $\chi = \rho\omega^{i\theta}$.*

(i) $|\epsilon(\sigma',\psi,dx_\psi)| = q^{(-t+1-n/2)(n(\psi)\dim(\sigma')+a(\sigma'))}$.

(ii) *If K has characteristic 0 and ψ is either ψ_{can} or $\overline{\psi}_{\mathrm{can}}$ then*

$$\epsilon(\sigma',\psi,dx_{\mathrm{can}}) = W(\sigma',\psi)A(\sigma')^{-t+1-n/2}.$$

(iii)

$$W(\sigma',\psi) = \begin{cases} W(\pi,\psi)^n & \text{if } \pi \text{ is ramified,}\\ (-1)^{n-1}\chi(\Phi)^{n(n(\psi)+1)-1} & \text{if } \pi \text{ is unramified.}\end{cases}$$

PROOF. Since σ' is essentially unitary of weight $-2t+1-n$ (Section 7), both (i) and (ii) follow from the proposition. To prove (iii), let W be the space of π, so that $V = W \otimes \mathbb{C}^n$ is the space of σ'. Then $V^I = W^I \otimes \mathbb{C}^n$ and $V_N^I = W^I \otimes e_{n-1}$.

Suppose first that π is ramified. Then $W^I = \{0\}$, so $V^I = \{0\}$. Hence $\delta(\sigma') = 1$. On the other hand, σ is the direct sum of the representations $\pi \otimes \omega^j$ for $0 \le j \le n-1$, so that $\epsilon(\sigma, \psi, dx)$ has the form $\epsilon(\pi, \psi, dx)^n q^*$ with $* \in \mathbb{Z}$ (Section 11, Prop. (iii)). Hence $\epsilon(\sigma', \psi, dx)$ has the same form, and $W(\sigma', \psi) = W(\pi, \psi)^n$.

Next suppose that π is unramified. Then $W = W^I$ is one-dimensional, and V^I/V_N^I is isomorphic to the direct sum of the lines $W \otimes e_j$ $(0 \le j \le n-2)$, with $-\Phi$ acting by the scalar $-\chi(\Phi)q^{-t-j}$. Therefore, computing in $\mathbb{C}^\times/\mathbb{R}_+^\times$, we have

$$\delta(\sigma') \equiv (-\chi(\Phi))^{n-1} \pmod{\mathbb{R}_+^\times}. \tag{12.8}$$

On the other hand, σ is the direct sum of the unramified characters $\chi\omega^{t+j}$ for $0 \le j \le n-1$, so that $(\epsilon 3)$ gives

$$\epsilon(\sigma, \psi, dx) \equiv \chi(\Phi)^{n(\psi)n} \pmod{\mathbb{R}_+^\times}. \tag{12.9}$$

Combining (12.8) and (12.9), we obtain the stated formula.

Part II: Elliptic Curves

13. The representation associated to an elliptic curve

Now let E be an elliptic curve over K and ℓ a prime different from p. The ℓ-adic Tate module of E is a free $\mathbb{Z}_\ell$-module of rank 2 with a natural action of $\mathrm{Gal}(\overline{K}/K)$. Quite generally, if A is any abelian group, then by the ℓ-adic Tate module of A we mean the inverse limit of the system of multiplication-by-ℓ maps $A_{\ell^{n+1}} \longrightarrow A_{\ell^n}$ $(n \ge 1)$, where A_m denotes the kernel of multiplication by m on A. We use the standard notations $T_\ell(A) = \varprojlim A_{\ell^n}$, $V_\ell(A) = \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_\ell(A)$ as well as the standard abbreviations $T_\ell(E) = T_\ell(E(\overline{K}))$, $V_\ell(E) = V_\ell(E(\overline{K}))$. However, we shall write $\sigma'_{E/K,\ell}$ for the *contragredient* of the natural representation of $\mathrm{Gal}(\overline{K}/K)$ on $V_\ell(E)$. Thus for us $\sigma'_{E/K,\ell}$ is a map

$$\sigma'_{E/K,\ell} : \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{GL}(V_\ell(E)^*),$$

where $V_\ell(E)^*$ is the dual of $V_\ell(E)$.

The reason that we take the contragredient of the natural action rather than the natural action itself is that for an arbitrary smooth projective variety X over K there is no Tate module, but only the Galois representations afforded by the ℓ-adic cohomology groups of X. In the case of an elliptic curve, $H^1_\ell(E)$ is actually dual to $V_\ell(E)$, and so it is the dual of $V_\ell(E)$ which is properly viewed as a part of the general picture. Since we have also replaced a Frobenius element by its inverse, the L-factors which we end up with will be the traditional ones.

Now let $\iota : \mathbb{Q}_\ell \hookrightarrow \mathbb{C}$ be a field embedding. As we have seen in Section 4, we can associate to $\sigma'_{E/K,\ell}$ a complex representation $\sigma'_{E/K,\ell,\iota} = (\sigma_{E/K,\ell,\iota}, N_{E/K,\ell,\iota})$ of $\mathcal{W}'(\overline{K}/K)$. We would like to write simply $\sigma'_{E/K} = (\sigma_{E/K}, N_{E/K})$, and so we must verify that the isomorphism class of $\sigma'_{E/K,\ell,\iota}$ is independent of the choice of ℓ and ι. The verification breaks naturally into two cases: the case of potential good and the case of potential multiplicative reduction.

14. The case of potential good reduction

First suppose that E has potential good reduction. Let $L \subset \overline{K}$ be a finite extension of K over which E acquires good reduction, and let I_L be the inertia subgroup of $\mathrm{Gal}(\overline{K}/L)$. The criterion of Néron-Ogg-Shafarevich implies that $\sigma'_{E/K,\ell}$ is trivial on I_L. Since I_L is open in I, it follows that $N_{E/K,\ell} = 0$. Hence it is merely the isomorphism class of $\sigma_{E/K,\ell,\iota}$ which must be proved independent of ℓ and ι. But the isomorphism class of a finite-dimensional semisimple complex representation of a group is determined by its character ([**8**, p. I-11], [**1**, Ch. 8, Chapter 12, no. 1, Prop. 3]), and according to the theory of Serre-Tate, $\mathrm{tr}\,\sigma_{E/K,\ell}(g)$ is a rational number independent of ℓ for every $g \in \mathcal{W}(\overline{K}/K)$ ([**11**, p. 499, Cor. to Thm. 3]). Hence it suffices to see that $\sigma_{E/K,\ell,\iota}$ is semisimple. In fact it suffices to see that $\sigma_{E/L,\ell,\iota}$ is semisimple, for as we have already recalled in Section 5, a finite-dimensional complex representation of a group is semisimple if and only if its restriction to some subgroup of finite index is semisimple. Thus without loss of generality we may assume that E has good reduction over K itself. By the remark in Section 5 just referred to, it suffices to show that for some inverse Frobenius element Φ, the linear transformation $\sigma_{E/K,\ell,\iota}(\Phi)$ is semisimple.

Let $\widetilde{E}$ be the reduction of E over K. The algebra $\mathbb{Q} \otimes \mathrm{End}(\widetilde{E})$ is an imaginary quadratic field or a quaternion division algebra over $\mathbb{Q}$ and therefore contains no nonzero nilpotent elements. It follows that if $B \in \mathbb{Q} \otimes \mathrm{End}(\widetilde{E})$, then the image of B under the natural embedding

$$\eta_\ell : \mathbb{Q} \otimes \mathrm{End}(\widetilde{E}) \hookrightarrow \mathrm{End}(V_\ell(\widetilde{E})) = \mathrm{End}(V_\ell(E))$$

is semisimple: for if $\eta_\ell(B)$ were not semisimple, then $B - \frac{1}{2}\,\mathrm{tr}\,\eta_\ell(B) \cdot 1$ would be a nonzero nilpotent element of $\mathbb{Q}_\ell \otimes \mathrm{End}(\widetilde{E})$, and in fact of $\mathbb{Q} \otimes \mathrm{End}(\widetilde{E})$ because $\mathrm{tr}\,\eta_\ell(B) \in \mathbb{Q}$ ([**12**, p. 134, Prop. 2.3]). In particular let us take $B = F$, the Frobenius endomorphism of $\widetilde{E}$. The image of F under the contragredient of the natural representation

$$(\mathbb{Q} \otimes \mathrm{End}(\widetilde{E}))^\times \hookrightarrow \mathrm{GL}(V_\ell(\widetilde{E})) \cong \mathrm{GL}(V_\ell(E))$$

coincides with $\sigma_{E/K,\ell}(\Phi^{-1})$, and therefore $\sigma_{E/K,\ell}(\Phi)$ is semisimple. Consequently so is $\sigma_{E/K,\ell,\iota}$, and dropping the subscripts ℓ and ι, as we are now entitled to do, we may summarize our conclusion as follows:

PROPOSITION. *Suppose that E has potential good reduction. Then $N_{E/K} = 0$ and $\sigma_{E/K}$ is semisimple. Furthermore, E has good reduction if and only if $\sigma_{E/K}$ is unramified.*

Of course the final assertion is just the criterion of Néron-Ogg-Shafarevich.

15. The case of potential multiplicative reduction

Next suppose that E has potential multiplicative reduction. Then E acquires split multiplicative reduction over some finite extension of K, which can be chosen to be quadratic and separable. Equivalently, there exists a character χ of $\mathrm{Gal}(\overline{K}/K)$ with $\chi^2 = 1$ such that the twist of E by χ has split multiplicative reduction over K itself. Let E^χ denote the twist of E by χ, so that we have a $\mathrm{Gal}(\overline{K}/K)$-equivariant group isomorphism

$$E(\overline{K}) \otimes \chi \cong E^\chi(\overline{K}). \tag{15.1}$$

As an elliptic curve over K with split multiplicative reduction, E^χ is isomorphic to a Tate curve over K. Hence for some $q \in K^\times$ of positive valuation there is a $\mathrm{Gal}(\overline{K}/K)$-equivariant isomorphism

$$E^\chi(\overline{K}) \cong \overline{K}^\times/q^{\mathbb{Z}}, \tag{15.2}$$

where $q^{\mathbb{Z}}$ denotes the infinite cyclic subgroup of $K^\times$ generated by q. Together, (15.1) and (15.2) yield a $\mathrm{Gal}(\overline{K}/K)$-equivariant isomorphism

$$E(\overline{K}) \cong \overline{K}^\times/q^{\mathbb{Z}} \otimes \chi,$$

and therefore an isomorphism of ℓ-adic representations

$$V_\ell(E) \cong V_\ell(\overline{K}^\times/q^{\mathbb{Z}}) \otimes \chi. \tag{15.3}$$

Now as a basis for $V_\ell(\overline{K}^\times/q^{\mathbb{Z}})$ over $\mathbb{Q}_\ell$ we can choose the vectors

$$e_0 = (\zeta_1, \zeta_2, \ldots, \zeta_n, \ldots) \quad \text{and} \quad e_1 = (q_1, q_2, \ldots, q_n, \ldots),$$

where ζ_n is a primitive ℓ^n-th root of unity, $\zeta_{n+1}^\ell = \zeta_n$, $q_n^{\ell^n} = q$, and $q_{n+1}^\ell = q_n$. Using this basis and (15.3), let us identify the natural action of $\mathrm{Gal}(\overline{K}/K)$ on $V_\ell(E)$ with a representation $\mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}(2, \mathbb{Q}_\ell)$. By our conventions $\sigma'_{E/K,\ell}$ is the *transpose-inverse* of this representation, so that

$$\sigma'_{E/K,\ell}(g) = \begin{pmatrix} \omega(g)^{-1} & 0 \\ * & 1 \end{pmatrix} \otimes \chi(g) = \begin{pmatrix} \omega^{-1}\chi(g) & 0 \\ * & \chi(g) \end{pmatrix}$$

for $g \in \mathrm{Gal}(\overline{K}/K)$. In particular, $\sigma'_{E/K,\ell}(I)$ is infinite because q has positive valuation.

Now write

$$\begin{aligned} \sigma_{E/K,\ell}(g) = \sigma'_{E/K,\ell}(g)\exp(-t_\ell(i)N_{E/K,\ell}) \\ (g = \Phi^m i \in \mathcal{W}(\overline{K}/K), m \in \mathbb{Z}, i \in I) \end{aligned} \tag{15.4}$$

as in Section 4. Since $\sigma'_{E/K,\ell}(I)$ is infinite, $N_{E/K,\ell} \neq 0$. Furthermore, using (15.4) we find

$$\sigma_{E/K,\ell}(\Phi) = \pm \begin{pmatrix} q & 0 \\ * & 1 \end{pmatrix},$$

so that $\sigma_{E/K,\ell}(\Phi)$ has distinct eigenvalues and is therefore semisimple. Hence $\sigma_{E/K,\ell,\iota}$ is semisimple as a representation, i.e. $\sigma'_{E/K,\ell,\iota}$ is admissible. Since $\sigma'_{E/K,\ell,\iota}$ is two-dimensional and $N_{E/K,\ell,\iota} \neq 0$ we see that $\sigma'_{E/K,\ell,\iota}$ is indecomposable as well. The classification of admissible indecomposable representations (Section 5) now shows that $\sigma'_{E/K,\ell,\iota}$ is isomorphic to $\xi \otimes \mathrm{sp}(2)$ for some character ξ of $\mathcal{W}(\overline{K}/K)$. Comparing the traces of these two representations, we find that $\chi(g)(\omega^{-1}(g)+1) = \xi(g)(1+\omega(g))$ for $g \in \mathcal{W}(\overline{K}/K)$. Hence $\xi = \chi\omega^{-1}$, where χ is now viewed as a character of $\mathcal{W}(\overline{K}/K)$ rather than of $\mathrm{Gal}(\overline{K}/K)$.

We conclude that $\sigma'_{E/K,\ell,\iota}$ is isomorphic to $\chi\omega^{-1} \otimes \mathrm{sp}(2)$, which is independent of ℓ and ι. Dropping these subscripts, we may summarize the conclusion as follows:

PROPOSITION. *Suppose that E has potential multiplicative reduction, and let χ be a character of $\mathcal{W}(\overline{K}/K)$ such that $\chi^2 = 1$ and E^χ has split multiplicative reduction. Then $\sigma'_{E/K} \cong \chi\omega^{-1} \otimes \mathrm{sp}(2)$. In particular, $N_{E/K} \neq 0$, so that $\sigma'_{E/K}$ is ramified. Furthermore, χ is trivial, unramified but nontrivial, or ramified according as E/K has split multiplicative reduction, nonsplit multiplicative reduction, or additive reduction.*

The final statement follows from the reduction theory of elliptic curves (cf. [**12**, p. 181, Prop. 5.4 (a)]).

16. The Weil pairing

Let μ denote the group of all roots of unity in $\overline{K}$. We have an identification of $\mathrm{Gal}(\overline{K}/K)$-modules

$$T_\ell(\mu) = \mathbb{Z}_\ell \otimes \omega_\ell,$$

where ω_ℓ is the ℓ-adic cyclotomic character of $\mathrm{Gal}(\overline{K}/K)$ (the unique ℓ-adic character of $\mathrm{Gal}(\overline{K}/K)$ which coincides with ω on $\mathcal{W}(\overline{K}/K)$). Hence the Weil pairing on E_{ℓ^n} $(n \geq 1)$ determines a nondegenerate, symplectic, $\mathrm{Gal}(\overline{K}/K)$-equivariant pairing

$$\langle -, - \rangle : T_\ell(E) \times T_\ell(E) \longrightarrow \mathbb{Z}_\ell \otimes \omega_\ell. \tag{16.1}$$

After extending scalars to $\mathbb{Q}_\ell$ and taking duals, we get

$$\langle -, - \rangle : V_\ell(E)^* \times V_\ell(E)^* \longrightarrow \mathbb{Q}_\ell \otimes \omega_\ell^{-1},$$

and the $\mathrm{Gal}(\overline{K}/K)$-equivariance means that

$$\langle \sigma'_{E/K,\ell}(g)v, \sigma'_{E/K,\ell}(g)w \rangle = \omega_\ell(g)^{-1}\langle v, w \rangle$$

for $g \in \mathrm{Gal}(\overline{K}/K)$. This implies first that

$$\langle N_{E/K,\ell}v, w \rangle = -\langle v, N_{E/K,\ell}w \rangle \tag{16.2}$$

and second that

$$\langle \sigma_{E/K,\ell}(g)v, \sigma_{E/K,\ell}(g)w \rangle = \omega(g)^{-1}\langle v, w \rangle \tag{16.3}$$

for $g \in \mathcal{W}(\overline{K}/K)$. If we extend scalars to $\mathbb{C}$ via an embedding $\iota : \mathbb{Q}_\ell \hookrightarrow \mathbb{C}$, then (16.2) and (16.3) imply that

$$\langle \sigma'_{E/K,\ell,\iota}(g)v, \sigma'_{E/K,\ell,\iota}(g)w \rangle = \omega(g)^{-1}\langle v, w \rangle$$

for $g \in \mathcal{W}'(\overline{K}/K)$, and we conclude that $\sigma'_{E/K} \otimes \omega^{1/2}$ is symplectic. In other words:

PROPOSITION. *The representation $\sigma'_{E/K}$ is essentially symplectic of weight* 1.

Since a symplectic representation has trivial determinant, this statement contains the fact that

$$\det \sigma'_{E/K} = \omega^{-1}.$$

Conversely, any *two-dimensional* representation with determinant ω^{-t} $(t \in \mathbb{R})$ is essentially symplectic of weight t, because in dimension two the symplectic group is just $\mathrm{SL}(2, \mathbb{C})$.

17. The L-factor

We define the L-factor of E over K to be the L-factor of the associated representation:

$$L(E/K, s) = L(\sigma'_{E/K}, s).$$

Let us check that this definition gives the familiar result.

PROPOSITION.

(i) *Suppose that E has good reduction. Let $\widetilde{E}$ denote the reduced curve over k, and put $a = 1 - |\widetilde{E}(k)| + q$. Then*

$$L(E/K, s) = (1 - aq^{-s} + q^{1-2s})^{-1}.$$

(ii) *If E has multiplicative reduction, then*

$$L(E/K, s) = (1 - \alpha q^{-s})^{-1},$$

where α is 1 or -1 according as E has split or nonsplit multiplicative reduction.

(iii) *If E has additive reduction, then $L(E/K, s) = 1$.*

PROOF.

(i) From Section 9 we know that $L(\sigma'_{E/K}, s) = P(q^{-s})^{-1}$ with

$$P(x) = \det(1 - x\sigma'_{E/K,\ell}(\Phi)|V_\ell(E)^{*I}).$$

In the case at hand I acts trivially on $V_\ell(E)^*$, and $P(x)$ is *a priori* of the form

$$P(x) = \det(1 - x\Phi|V_\ell(E)^*) = 1 - {*}x + qx^2 \tag{17.1}$$

because $\det \sigma'_{E/K,\ell}(\Phi) = \omega_\ell^{-1}(\Phi) = q$. Let F denote the Frobenius endomorphism of $\widetilde{E}$. In the identification $V_\ell(\widetilde{E}) = V_\ell(E)$, the natural action of F on the left-hand side coincides with the natural action of Φ^{-1} on the right. Hence

$$P(x) = \det(1 - xF|V_\ell(\widetilde{E})),$$

so that

$$P(1) = \det(1 - F|V_\ell(\widetilde{E})) = \deg(1 - F) = |\widetilde{E}(k)|$$

(cf. [**12**, p. 134, Prop. 2.3]). In view of (17.1) this pins down $P(x)$ completely.

(ii) Suppose more generally that E has *potential* multiplicative reduction, and let χ be a character of $\mathcal{W}(\overline{K}/K)$ such that $\chi^2 = 1$ and E^χ has split multiplicative reduction. Then $\sigma'_{E/K} \cong \chi\omega^{-1} \otimes \mathrm{sp}(2)$. Hence

$$L(\sigma'_{E/K}, s) = L(\chi\omega^{-1}, s + 1) = L(\chi, s)$$

(Section 8, Prop.). Now if E has multiplicative reduction over K, then χ is unramified, so that

$$L(\chi, s) = (1 - \chi(\Phi)q^{-s})^{-1} = (1 - \alpha q^{-s})^{-1}$$

with α as stated. On the other hand, if E has additive reduction then χ is ramified, so that $L(\chi, s) = 1$ in agreement with (iii).

(iii) Since we have just handled the case where E has potential multiplicative reduction, we may assume that E has bad but potentially good reduction. Thus $\sigma'_{E/K} = (\sigma_{E/K}, 0)$, with $\sigma_{E/K}$ ramified: if V is the space of $\sigma_{E/K}$, then $V^I \neq V$. Hence V^I has dimension 0 or 1. Suppose that V^I has dimension 1, and choose a basis $\{e_0, e_1\}$ for V such that e_0 spans V^I. Let us use this basis to view $\sigma_{E/K}$ as a map $\mathcal{W}(\overline{K}/K) \longrightarrow \mathrm{GL}(2, \mathbb{C})$. Since $\det \sigma_{E/K} = \omega^{-1}$ is trivial on I, we find that $\sigma_{E/K}(I)$ is a finite but nontrivial subgroup of the group

$$\left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} : * \in \mathbb{C} \right\}.$$

But this group has no finite nontrivial subgroups. Hence V^I has dimension 0, and consequently $L(\sigma'_{E/K}, s) = 1$.

18. The conductor

Put $a(E/K) = a(\sigma'_{E/K})$. The conductor of E over K is the ideal

$$\mathfrak{N}(E/K) = \mathfrak{N}(\sigma'_{E/K}) = \varpi^{a(E/K)}\mathcal{O}.$$

If K has characteristic 0 then one can also put

$$A(E/K) = A(\sigma'_{E/K}) = D^2 \mathrm{N}(\mathfrak{N}(E/K)).$$

PROPOSITION.

(i) *E has good reduction over K if and only if $a(E/K) = 0$.*

(ii) *Suppose that E has potential multiplicative reduction. If E has multiplicative reduction over K itself, then*

$$a(E/K) = 1.$$

If E has additive reduction, let ξ be a quadratic character of $\mathcal{W}(\overline{K}/K)$ such that E^ξ has multiplicative reduction. Then

$$a(E/K) = 2a(\xi).$$

(iii) *Suppose that $p \geq 5$ and that E has bad but potentially good reduction. Then*

$$a(E/K) = 2.$$

PROOF.

(i) A representation σ' of $\mathcal{W}'(\overline{K}/K)$ is unramified if and only if $a(\sigma') = 0$, and $\sigma'_{E/K}$ is unramified if and only if E has good reduction.

(ii) Choose a character χ of $\mathcal{W}(\overline{K}/K)$ such that $\chi^2 = 1$ and E^χ has split multiplicative reduction. Then $\sigma'_{E/K} \cong \chi\omega^{-1} \otimes \mathrm{sp}(2)$. Hence $a(\sigma'_{E/K})$ is $2a(\chi)$ or 1 according as χ is ramified or unramified (Section 10, Prop.), i.e. according as E has additive or multiplicative reduction. If E has additive reduction then $a(\chi) = a(\xi)$, because both E^χ and E^ξ have multiplicative reduction and therefore χ/ξ is unramified.

(iii) Let R be the minimal extension of K_{unr} inside $\overline{K}$ over which E acquires good reduction (cf. [**11**, p. 498, Cor. 3]). Then $\mathrm{Gal}(\overline{K}/R)$ is the kernel of $\sigma_{E/K}$, and we may view $\sigma_{E/K}$ as a faithful representation of

$$\mathcal{W}(R/K) = \mathcal{W}(\overline{K}/K)/\,\mathrm{Gal}(\overline{K}/R).$$

Denoting the image of Φ in $\mathcal{W}(R/K)$ simply by Φ, we can write $\mathcal{W}(R/K)$ as a semidirect product

$$\mathcal{W}(R/K) = \mathrm{Gal}(R/K_{\mathrm{unr}}) \rtimes \langle \Phi \rangle,$$

and since $p \geq 5$ we know that $\mathrm{Gal}(R/K_{\mathrm{unr}})$ is cyclic of order 2, 3, 4, or 6 (cf. [**9**, p. 312]). We now consider two cases, according as the above semidirect product is or is not direct.

If the product is actually direct, then $W(R/K)$ is abelian. Since $\sigma_{E/K}$ is semisimple, we can write it as a direct sum of quasicharacters of $\mathcal{W}(\overline{K}/K)$ trivial on $\mathrm{Gal}(\overline{K}/R)$: $\sigma_{E/K} = \chi \oplus \chi'$. In fact $\chi' = \omega^{-1}\chi^{-1}$, because $\det \sigma_{E/K} = \omega^{-1}$. Thus $a(\sigma_{E/K}) = a(\chi) + a(\chi') = 2a(\chi)$. But the restriction of χ to I has order 2, 3, 4, or 6, while $p \geq 5$. Thus χ is tamely ramified, i.e. $a(\chi) = 1$.

Next suppose that $W(R/K)$ is nonabelian. Since $\mathrm{Gal}(R/K_{\mathrm{unr}})$ is cyclic of order 3, 4, or 6, its automorphism group has order 2, so that Φ^2 centralizes $\mathrm{Gal}(R/K_{\mathrm{unr}})$. Let L denote the quadratic extension of K inside K_{unr}. It follows that the group

$$\mathcal{W}(R/L) = \mathrm{Gal}(R/K_{\mathrm{unr}}) \times \langle \Phi^2 \rangle$$

is an abelian normal subgroup of $\mathcal{W}(R/K)$ and consequently that $\sigma_{E/K}$ is induced from a one-dimensional character of $\mathcal{W}(R/L)$: $\sigma_{E/K} = \mathrm{ind}_{L/K}\,\chi$. Let us view χ as a character of $\mathcal{W}(\overline{K}/L)$ trivial on $\mathrm{Gal}(\overline{K}/R)$. Since the restriction of χ to I has order 3, 4, or 6, χ is tamely ramified. Hence formula $(a2)$ in Section 10 gives $a(\sigma_{E/K}) = a(\mathrm{ind}_{L/K}\,\chi) = 2a(\chi) = 2$.

19. The root number

The root number of E over K is

$$W(E/K) = W(\sigma'_{E/K}).$$

Since $\sigma'_{E/K}$ is essentially symplectic, the right-hand side does not depend on the choice of an additive character of K, and $W(E/K) = \pm 1$.

PROPOSITION.

(i) *If E has good reduction over K, then $W(E/K) = 1$.*

(ii) *Suppose that E has potential multiplicative reduction. If E has multiplicative reduction over K itself, then*

$$W(E/K) = \begin{cases} -1 & \text{if } E \text{ has split multiplicative reduction,} \\ 1 & \text{if } E \text{ has nonsplit multiplicative reduction.} \end{cases}$$

If E has additive reduction, let ξ be a quadratic character of $\mathcal{W}(\overline{K}/K)$ such that E^{ξ} has multiplicative reduction. Then

$$W(E/K) = \xi(-1),$$

where ξ is viewed as a character of $K^\times$ by local class field theory.

(iii) *Suppose that E has potential good reduction and that $K = \mathbb{Q}_p$, with $p \geq 5$. Let $\Delta \in \mathbb{Q}_p^\times$ be the discriminant of any generalized Weierstrass equation for E over $\mathbb{Q}_p$, and put*

$$e = \frac{12}{\gcd(\operatorname{ord}_p \Delta, 12)} = 1, 2, 3, 4, \text{ or } 6.$$

Then

$$W(E/\mathbb{Q}_p) = \begin{cases} 1, & \text{if } e = 1 \\ \left(\frac{-1}{p}\right), & \text{if } e = 2 \text{ or } 6 \\ \left(\frac{-3}{p}\right), & \text{if } e = 3 \\ \left(\frac{-2}{p}\right), & \text{if } e = 4 \end{cases}$$

PROOF.

(i) Here $N_{E/K} = 0$ and $\sigma_{E/K}$ factors through the abelian group $\mathcal{W}(\overline{K}/K)/I$. Since $\sigma_{E/K}$ is semisimple, it is the direct sum of two quasicharacters:

$$\sigma_{E/K} \cong \chi \oplus \chi'.$$

We have in fact $\chi' = \omega^{-1}\chi^{-1}$, because $\det \sigma_{E/K} = \omega^{-1}$. Hence if ψ is an additive character of K then

$$W(\sigma_{E/K}) = W(\chi, \psi)W(\chi', \psi) = W(\chi, \psi)W(\chi^{-1}, \psi) = \chi(-1)$$

(Section 11, Prop. (iii); Section 12, Lemma (i)), and since χ is unramified, $\chi(-1) = 1$.

(ii) Let χ be a character of $\mathcal{W}(\overline{K}/K)$ such that $\chi^2 = 1$ and E^χ has split multiplicative reduction. Then $\sigma'_{E/K} \cong \chi\omega^{-1} \otimes \mathrm{sp}(2)$. Hence we have

$$W(\sigma'_{E/K}) = \begin{cases} W(\chi\omega^{-1}, \psi)^2 & \text{if } \chi \text{ is ramified,} \\ -\chi(\Phi) & \text{if } \chi \text{ is unramified} \end{cases}$$

(Section 12, Cor.), where ψ is an arbitrary additive character of K. If E has multiplicative reduction, then χ is unramified and is trivial or nontrivial according as E/K has split or nonsplit reduction. On the other hand, if E has additive reduction, then χ is ramified and we get

$$W(\sigma'_{E/K}) = W(\chi\omega^{-1}, \psi)^2 = W(\chi, \psi)^2 = \chi(-1)$$

(Section 11, Prop. (iii); Section 12, Lemma (i)). Since both E^χ and E^ξ have multiplicative reduction, χ/ξ is unramified, whence $\chi(-1) = \xi(-1)$.

(iii) [**7**, Prop. 2].

20. The Archimedean case

We would still like to fit in a brief word about the global setting, or at least about the "number field case". To do so, however, we must make some mention of the representation associated to an elliptic curve over $\mathbb{R}$ or $\mathbb{C}$. In these Archimedean cases there is no distinction between the Weil group and the Weil-Deligne group; one puts .

$$\mathcal{W}'(\mathbb{C}/\mathbb{C}) = \mathcal{W}(\mathbb{C}/\mathbb{C}) = \mathbb{C}^\times$$

and

$$\mathcal{W}'(\mathbb{C}/\mathbb{R}) = \mathcal{W}(\mathbb{C}/\mathbb{R}) = \mathbb{C}^\times \cup J\mathbb{C}^\times,$$

where

$$J^2 = -1 \text{ and } JzJ^{-1} = \overline{z} \qquad (z \in \mathbb{C}^\times).$$

The subgroup $\mathbb{C}^\times$ of $\mathcal{W}(\mathbb{C}/\mathbb{R})$ is identified with $\mathcal{W}(\mathbb{C}/\mathbb{C})$. Now if E is an elliptic curve over $\mathbb{C}$, then one associates to $E/\mathbb{C}$ the representation

$$\sigma'_{E/\mathbb{C}} = \sigma_{E/\mathbb{C}} = \varphi_{1,0} \oplus \varphi_{0,1},$$

where

$$\varphi_{p,q} : \mathcal{W}(\mathbb{C}/\mathbb{C}) = \mathbb{C}^\times \longrightarrow \mathbb{C}^\times \qquad (p,q \in \mathbb{Z})$$

is the character

$$\varphi_{p,q}(z) = z^{-p}\,\overline{z}^{-q}.$$

Note in particular that $\sigma_{E/\mathbb{C}} \circ c \cong \sigma_{E/\mathbb{C}}$, where c denotes complex conjugation. Thus if K is a number field with a complex place v and we identify the completion K_v with $\mathbb{C}$ in one of the two possible ways, then for an elliptic curve E over K, the isomorphism class of the representation $\sigma_{E/\mathbb{C}}$ is independent of the identification chosen. If E is an elliptic curve over $\mathbb{R}$ then we put

$$\sigma'_{E/\mathbb{R}} = \sigma_{E/\mathbb{R}} = \mathrm{ind}_{\mathbb{C}/\mathbb{R}}\, \varphi_{1,0} = \mathrm{ind}_{\mathbb{C}/\mathbb{R}}\, \varphi_{0,1}.$$

With these definitions one has

$$\mathrm{res}_{\mathbb{C}/\mathbb{R}}\, \sigma_{E/\mathbb{R}} = \sigma_{E/\mathbb{C}}.$$

As in the non-Archimedean case, one can now attach local factors to E through the intermediary of the associated representation of the Weil group. For our present purpose it is enough simply to record the formulas

$$L(E/\mathbb{C}, s) = (2(2\pi)^{-s}\Gamma(s))^2, \quad W(E/\mathbb{C}) = -1$$

for an elliptic curve over $\mathbb{C}$ and

$$L(E/\mathbb{R}, s) = 2(2\pi)^{-s}\Gamma(s), \quad W(E/\mathbb{R}) = -1$$

for an elliptic curve over $\mathbb{R}$. But for the sake of perspective we should at least mention how one associates a representation of the Weil group to the cohomology in some dimension n of an *arbitrary* smooth projective variety X over $\mathbb{R}$ or $\mathbb{C}$. The key ingredient is the Hodge decomposition

$$H^n(X(\mathbb{C}), \mathbb{C}) = \bigoplus_{p+q=n} H^{p,q}.$$

If X is a variety over $\mathbb{C}$ then we define

$$\sigma_{X/\mathbb{C}} = \bigoplus_{p+q=n} \varphi_{p,q} \otimes H^{p,q},$$

where $H^{p,q}$ is regarded as a vector space with trivial action. If X is a variety over $\mathbb{R}$ then we define

$$\begin{aligned}\sigma_{X/\mathbb{R}} = &\left(\bigoplus_{\substack{p+q=n \\ p<q}} (\mathrm{ind}_{\mathbb{C}/\mathbb{R}}\, \varphi_{p,q}) \otimes H^{p,q}\right) \\ &\oplus \left((\omega^{-n/2}\epsilon^{n/2}) \otimes H^{n/2,n/2,+}\right) \\ &\oplus \left((\omega^{-n/2}\epsilon^{n/2+1}) \otimes H^{n/2,n/2,-}\right),\end{aligned}$$

where the second and third summands occur only for n even, and the meaning of the new notation is as follows: Since X is defined over $\mathbb{R}$, there is a natural action of complex conjugation on $X(\mathbb{C})$ and hence an induced $\mathbb{C}$-linear automorphism Φ_∞ of $H^n(X(\mathbb{C}), \mathbb{C})$. This satisfies $\Phi_\infty(H^{p,q}) = H^{q,p}$; in particular, $H^{n/2,n/2}$ is invariant under Φ_∞. We let $H^{n/2,n/2,+}$ and $H^{n/2,n/2,-}$ denote the $(+1)$- and (-1)-eigenspaces of Φ_∞ on $H^{n/2,n/2}$. We also let ω denote the character of $\mathcal{W}(\mathbb{C}/R)$ given by $\omega(J) = 1$ and $\omega(z) = z\bar{z}$ for $z \in \mathbb{C}^\times$. As for ϵ, it denotes the quadratic character of $\mathcal{W}(\mathbb{C}/\mathbb{R})$ with kernel $\mathcal{W}(\mathbb{C}/\mathbb{C})$. Specializing now to the case where $X = E$ is an elliptic curve and $n = 1$, we obtain the representations indicated previously, because in this case the Hodge decomposition is simply

$$H^1(E(\mathbb{C}), \mathbb{C}) = H^{1,0} \oplus H^{0,1},$$

and both $H^{1,0}$ and $H^{0,1}$ are one-dimensional.

21. The global case

We conclude with a peek at the global setting. Let K be a number field of degree n over $\mathbb{Q}$ with r_1 real and $2r_2$ complex embeddings. Write D for the absolute value of the discriminant of K and K_v for the completion of K at a place v. Given an elliptic curve E over K, we define its conductor $\mathfrak{N}(E/K)$ by

$$\mathfrak{N}(E/K) = \prod_{v \text{ finite}} \mathfrak{N}(E/K_v),$$

the right-hand side being interpreted as an ideal of the ring of integers of K in the usual way. We also put

$$A(E/K) = \prod_{v \text{ finite}} A(E/K_v) = D^2 \mathrm{N}(\mathfrak{N}(E/K))$$

and

$$W(E/K) = \prod_v W(E/K_v) = (-1)^{r_1+r_2} \prod_{v \text{ finite}} W(E/K_v).$$

Originally one defined the L-function of E to be the Euler product

$$L(E/K, s) = \prod_{v \text{ finite}} L(E/K_v, s),$$

absolutely convergent for $\Re(s) > 3/2$. Nowadays one often includes the Archimedean L-factors in this product as well; alternatively, one incorporates them into

$$\Lambda(E/K, s) = A(E/K)^{s/2} (2(2\pi)^{-s}\Gamma(s))^n L(E/K, s).$$

Now $\Lambda(E/K,s)$ is conjectured to have an analytic continuation to an entire function and to satisfy the functional equation

$$\Lambda(E/K,s) = W(E/K)\Lambda(E/K,2-s). \tag{21.1}$$

This implies in particular that

$$W(E/K) = (-1)^{\operatorname{ord}_{s=1} L(E/K,s)}. \tag{21.2}$$

In conjunction with the Birch-Swinnerton-Dyer Conjecture, (21.2) would give

$$W(E/K) = (-1)^{\operatorname{rank} E(K)}. \tag{21.3}$$

If $K = \mathbb{Q}$ and E occurs as an isogeny factor in the jacobian variety of some modular curve, then (21.1) and hence also (21.2) — but not yet (21.3) — are known, as a consequence of work of Eichler, Shimura, Igusa, Ihara, Deligne, Langlands, and Carayol.

References

1. N. Bourbaki, *Algebra*, Springer-Verlag, New York, 1988.
2. C. Chevalley, *Théorie des groupes de Lie* III, Hermann, Paris, 1955.
3. P. Deligne, *Les constantes des équations fonctionnelles des fonctions L*, Modular Functions of One Variable II, SLN 349, Springer-Verlag, New York, 1973, pp. 501–595.
4. ——, *Formes modulaires et représentations de GL(2)*, Modular Functions of One Variable, II, SLN 349, Springer-Verlag, New York, 1973, pp. 55–105.
5. ——, *Les constantes locales de l'équation fonctionnelle de la fonction L d'Artin d'une représentation orthogonale*, Invent. Math. **35** (1976), 299–316.
6. P.X. Gallagher, *Determinants of representations of finite groups*, Abh. Math. Sem. Univ. Hamburg **28** (1965), 162–167.
7. D.E. Rohrlich, *Variation of the root number in families of elliptic curves*, Compos. Math. (to appear).
8. J.-P. Serre, *Abelian ℓ-adic representations and elliptic curves*, W.A. Benjamin, New York, 1968.
9. ——, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.
10. ——, *Local fields*, Graduate Texts in Math., vol. 67, Springer-Verlag, New York, 1979.
11. J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. Math. **68** (1968), 492–517.
12. J.H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Math., vol. 106, Springer-Verlag, New York, 1985.
13. J. Tate, *Number theoretic background*, Automorphic Forms, Representations, and L-Functions, Proc. Symp. Pure Math. Vol. 33 — Part 2, Amer. Math. Soc., Providence, 1979.
14. ——, *Fourier analysis in number fields and Hecke's zeta functions*, Algebraic Number Theory, J.W.S. Cassels and A. Fröhlich eds., Academic Press, London, 1967.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MARYLAND, COLLEGE PARK, MD 20742, USA

E-mail address: der@lakisis.umd.edu