Contents

Root numbers

David E. Rohrlich

IAS/Park City Mathematics Series
Volume XX, XXXX

Root numbers

David E. Rohrlich

Introduction

Starting with Riemann's derivation of an "explicit formula" for the number of primes below a given bound, the functional equation of an L-function has been an indispensable tool in analytic number theory, and in more recent years it has become a fundamental tool in automorphic forms as well via the method of converse theorems pioneered by Hamburger and Hecke. The present lectures are concerned with a third direction, naïve by comparison and more limited in scope, namely the use of the functional equation to determine the parity of the order of vanishing of an L-function at the center of the critical strip. While the insights gained from this type of information are often only conditional ("... granting the conjecture of Birch and Swinnerton-Dyer, we conclude that ..."), they are sometimes the first hint of interesting new phenomena in arithmetic geometry.

Given our focus in these lectures, the key invariant is the root number, and the first four lectures are devoted to issues that arise in computing it. The four lectures correspond respectively to four possibilities for the underlying Galois representation: global of dimension one, local of dimension one, global of arbitrary dimension, and local of arbitrary dimension. The fifth lecture addresses a question which is hinted at from the outset: To what extent, or under what circumstances, should one expect the order of vanishing of an L-function at the center of its critical strip to be the smallest value permitted by its functional equation? Very little is known about this question, and our remarks are largely speculative.

The main prerequisites for the lectures are basic algebraic number theory and a familiarity with Dirichlet L-functions. Some prior encounters with L-functions of elliptic curves are also desirable. More general classes of L-functions (Hecke L-functions, Artin L-functions, motivic L-functions) will be introduced from first principles as the lectures progress, but since references to "L-functions" in general appear right from the beginning, it is essential to have some notion of what is being talked about, namely an absolutely convergent Dirichlet series represented by an Euler product in some right half-plane (thus holomorphic and nonvanishing there) which is known or conjectured to extend to a meromorphic function on $\mathbb{C}$ and to satisfy a functional equation modeled on the functional equation of the Riemann zeta function. An acquaintance with Dirichlet L-functions and perhaps even with L-functions of elliptic curves provides an adequate intuition for absorbing the concept in general.

Department of Mathematics and Statistics, Boston University, Boston, MA 02215
E-mail address: rohrlich@math.bu.edu

Some vocabulary from group representation theory is also a prerequisite. Our conventions are as follows. A **representation** ρ of a group G is always understood to be finite-dimensional, and if G is a topological group then ρ is understood to be continuous as well. Continuity is meaningful because the field of scalars of ρ will be either $\mathbb{C}$ (the default) or else, where explicitly indicated, a λ-adic field. A **character** is either a one-dimensional representation or the trace of a representation of dimension greater than one, usually the former. Possible ambiguities, when they arise, will be resolved by referring to a **one-dimensional character.** A one-dimensional character is **unitary** if it takes values in the group of complex numbers of absolute value 1. Note that elsewhere in the literature, particularly in older treatments, the term *quasicharacter* is used for our "one-dimensional character" and the term *character* is reserved for our "unitary character." Also the "contragredient" of a representation ρ will be referred to as the **dual** of ρ and denoted $\rho^\vee$. To illustrate the definitions just made, note that if χ is a one-dimensional character then $\chi^\vee = \chi^{-1}$, but if χ is unitary then also $\chi^\vee = \overline{\chi}$. The trivial charcter of a group G will often be denoted by 1, or if $G = \mathrm{Gal}(\overline{K}/K)$ then by 1_K.

There is one simple fact about representations which comes up so frequently that it deserves to be emphasized at the outset: A complex representation of a profinite group is trivial on an open subgroup. To see why, observe first of all that $\mathrm{GL}_n(\mathbb{C})$ "has no small subgroups": in other words, there is an open neighborhood $\mathcal{U}$ of the identity in $\mathrm{GL}_n(C)$ such that the only subgroup of $\mathrm{GL}_n(\mathbb{C})$ which is contained in $\mathcal{U}$ is the trivial subgroup. This property is easily verified using the exponential map, and it actually characterizes real Lie groups among all locally compact groups (Hilbert's fifth problem). In any case, suppose we are given a profinite group G and a representation ρ of G on a complex vector space V. Choose $\mathcal{U} \subset \mathrm{GL}(V)$ as above. Since the open subgroups of G form a neighborhood basis at the identity, there is an open subgroup H contained in $\rho^{-1}(\mathcal{U})$. Then $\rho(H)$ is a subgroup of $\mathcal{U}$, hence trivial.

LECTURE 1

Trivial central zeros

Like many things in mathematics, the subject of root numbers begins with a theorem of Gauss, who proved in 1805 that if p is an odd prime then

$$\sum_{j=1}^{p-1} \lambda(j) e^{2\pi i j/p} = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \pmod 4 \\ i\sqrt{p} & \text{if } p \equiv 3 \pmod 4, \end{cases} \tag{1.1}$$

where λ is the Legendre symbol at p:

$$\lambda(j) = \left(\frac{j}{p}\right).$$

A crude restatement of (1.1), and one that is much easier to prove, is that the left-hand side is a square root of $\lambda(-1)p$. But by summarizing the result in this way we lose the information that the square root at issue is the one with *positive* real or imaginary part. In other words, the delicate point in (1.1) is precisely the determination of the sign in front of the square root – the "root number."

More generally, suppose that χ is any primitive Dirichlet character, say with conductor N. The **Gauss sum** attached to χ is the quantity

$$\tau(\chi) = \sum_{j=0}^{N-1} \chi(j) e^{2\pi i j/N} \tag{1.2}$$

and the associated **root number** is given by

$$W(\chi) = \frac{\tau(\chi)}{i^{m(\chi)}\sqrt{N}}, \tag{1.3}$$

where

$$m(\chi) = \begin{cases} 0 & \text{if } \chi(-1) = 1 \\ 1 & \text{if } \chi(-1) = -1. \end{cases} \tag{1.4}$$

If χ is quadratic then $\tau(\chi)$ is once again equal to $\sqrt{N}$ or $i\sqrt{N}$ according as χ is even or odd. Equivalently, we can formulate the preceding statement as an assertion about root numbers:

Theorem 1.1. *If χ is a primitive quadratic Dirichlet character then $W(\chi) = 1$.*

A proof of Theorem 1.1 will be given later, and in fact we will eventually prove a more general statement. But to begin with let us examine the implications of the theorem for Dirichlet L-functions.

1. Nonexistence of trivial central zeros for Dirichlet L-functions

A **trivial zero** of an L-function is a zero which is immediately apparent from the functional equation. Any L-function worthy of the name has infinitely many trivial zeros, as one sees by playing off the holomorphy of the L-function in some right half-plane against the poles of $\Gamma(s)$ at nonpositive integers. For example, consider the functional equation of the Riemann zeta function:

$$\pi^{-s/2}\Gamma(s/2)\zeta(s) = \pi^{-(1-s)/2}\Gamma((1-s)/2)\zeta(1-s). \tag{1.5}$$

At $s = -2, -4, -6, \dots$ the factor $\Gamma(s/2)$ on the left-hand side has a simple pole, whereas the right-hand side is holomorphic and nonvanishing. It follows that $\zeta(s)$ has a zero (in fact a simple zero) at the negative even integers, whence these points are trivial zeros of $\zeta(s)$.

On the other hand, $\zeta(s)$ does not have a **trivial central zero**. The latter term refers to a trivial zero of an L-function at $s = k/2$, where the functional equation of the L-function in question is a transformation law relative to $s \mapsto k - s$. In the case of $\zeta(s)$ we have $k = 1$; indeed if we write $Z(s)$ for the left-hand side of (1.5), then (1.5) becomes $Z(s) = Z(1-s)$. Thus a trivial central zero of $\zeta(s)$ would be a zero at $s = 1/2$ inherent in the equation $Z(s) = Z(1-s)$; but the latter equation says merely that the function $f(s) = Z(s+1/2)$ is even, and even functions, unlike odd functions, need not vanish at $s = 0$. Thus there is no trivial reason why $Z(s)$ must vanish at $s = 1/2$ and hence none why $\zeta(s)$ itself must vanish there. The expansion

$$\zeta(s) = (1 - 2^{1-s})^{-1}(1 - 2^{-s} + 3^{-s} - 4^{-s} + \dots) \qquad (\Re(s) > 0)$$

shows that in fact $\zeta(1/2) \neq 0$.

More generally, no Dirichlet L-function has a trivial central zero. To verify this statement, consider a primitive Dirichlet character χ of conductor N. The functional equation of $L(s, \chi)$ is

$$\Lambda(s, \chi) = W(\chi)\Lambda(1 - s, \overline{\chi}) \tag{1.6}$$

with $\Lambda(s, \chi) = N^{s/2}\,\Gamma_{\mathbb{R}}(s + m(\chi))L(s, \chi)$. Here $W(\chi)$ and $m(\chi)$ are as in (1.3) and (1.4) respectively, and

$$\Gamma_{\mathbb{R}}(s) = \pi^{-s/2}\Gamma(s/2). \tag{1.7}$$

We mention in passing that in addition to this "real gamma factor" there is also a "complex gamma factor"

$$\Gamma_{\mathbb{C}}(s) = 2 \cdot (2\pi)^{-s}\Gamma(s), \tag{1.8}$$

and with this notation the duplication formula takes the attractive form

$$\Gamma_{\mathbb{R}}(s)\Gamma_{\mathbb{R}}(s+1) = \Gamma_{\mathbb{C}}(s). \tag{1.9}$$

Returning to the matter at hand, we consider three cases, namely (i) χ has order $\geqslant 3$, (ii) $\chi = 1$, and (iii) χ has order 2. In case (i), $L(s, \chi) \neq L(s, \overline{\chi})$, whence $\Lambda(s, \chi) \neq \Lambda(s, \overline{\chi})$ and (1.6) has no direct bearing on the possible vanishing of $L(s, \chi)$ at $s = 1/2$. In case (ii), $L(s, \chi) = \zeta(s)$, and we have already seen that $\zeta(s)$ does not have a trivial central zero. Finally, suppose that χ is quadratic. Then (1.6) becomes $\Lambda(s, \chi) = W(\chi)\Lambda(1 - s, \chi)$, and since $W(\chi)$ is 1 rather than -1 the function $f(s) = \Lambda(s + 1/2, \chi)$ is even rather than odd. Hence in case (iii) there is again no trivial central zero.

Of course it is one thing to say that there is no trivial reason for $L(s,\chi)$ to vanish at $s = 1/2$ and quite another to prove that $L(1/2,\chi)$ is not in fact zero. The latter problem is the subject of an extensive literature (see for example [**4**], [**33**], [**34**], and [**60**]), and while the state of the art does not yet permit us to assert that $L(1/2,\chi) \neq 0$ for every Dirichlet character χ, that is certainly the conjecture to which the evidence points.

2. Hecke characters and Hecke L-functions

While they do not occur for Dirichlet L-functions, trivial central zeros of L-functions do exist. The first examples were found in 1966 by Birch and Stephens [**6**] and arose in connection with elliptic curves over $\mathbb{Q}$ with complex multiplication by an imaginary quadratic field. The L-function of such an elliptic curve is a Hecke L-function, and Hecke's functional equation allows one to exhibit cases in which an analogue of (1.6) holds but with $L(s,\chi) = L(s,\overline{\chi})$ and $W(\chi) = -1$, so that the L-function vanishes at the center of its critical strip. Here this phenomenon will be illustrated not using elliptic curves with complex multiplication by $\mathbb{Q}(i)$ as in Birch and Stephens but rather with the "$\mathbb{Q}$-curves" of Gross [**26**], for which the field of complex multiplication varies. But first of all we review some background on Hecke characters and Hecke L-functions. Throughout, K denotes a number field and $\mathcal{O}$ its ring of integers. We also write I for the multiplicative group of nonzero fractional ideals of K and P for the subgroup of principal fractional ideals. As usual, a "prime ideal of K" is a nonzero prime ideal of $\mathcal{O}$, and an "integral ideal of K" is any nonzero ideal of $\mathcal{O}$.

2.1. Hecke characters

Given an integral ideal $\mathfrak{f}$ of K, we say that a fractional ideal $\mathfrak{a} \in I$ is **relatively prime** to $\mathfrak{f}$ if no prime ideal dividing $\mathfrak{f}$ occurs in the factorization of $\mathfrak{a}$ as a product of prime ideals to nonzero integral powers. The multiplicative group of such $\mathfrak{a}$ will be denoted $I(\mathfrak{f})$, and we also put $P(\mathfrak{f}) = P \cap I(\mathfrak{f})$. Note that if $\mathfrak{f} = \mathcal{O}$ then $I(\mathfrak{f}) = I$ and $P(\mathfrak{f}) = P$. We say that an element $\alpha \in K^\times$ is relatively prime to $\mathfrak{f}$ if the principal ideal (α) is – in other words, if $(\alpha) \in P(\mathfrak{f})$ – and we write $K(\mathfrak{f})$ for the subgroup of $K^\times$ consisting of such α. Equivalently, $K(\mathfrak{f}) = \mathcal{O}_T^\times$, where $\mathcal{O}_T$ is the localization of $\mathcal{O}$ at the multiplicative set $T = \cap_{\mathfrak{p}|\mathfrak{f}}(\mathcal{O} \smallsetminus \mathfrak{p})$. Finally, we write $K_\mathfrak{f}$ for the subgroup of $K(\mathfrak{f})$ consisting of elements $\alpha \equiv 1 \bmod^* \mathfrak{f}$: recall that a congruence $\bmod^* \mathfrak{f}$ means a congruence mod $\mathfrak{f}\mathcal{O}_T$. Alternatively, we can say that an element $\alpha \in K^\times$ satisfies the congruence $\alpha \equiv 1 \bmod^* \mathfrak{f}$ if for every prime ideal $\mathfrak{p}$ dividing $\mathfrak{f}$ we have $v_\mathfrak{p}(\alpha - 1) \geqslant \mathrm{ord}_\mathfrak{p}\mathfrak{f}$, where $v_\mathfrak{p}$ denotes the valuation associated to $\mathfrak{p}$ and $\mathrm{ord}_\mathfrak{p}\mathfrak{f}$ the multiplicity of $\mathfrak{p}$ in $\mathfrak{f}$. Note that with the latter definition it still follows that $K_\mathfrak{f}$ is a subgroup of $K(\mathfrak{f})$. To complete our suite of parallel notations, let $P_\mathfrak{f}$ be the subgroup of $P(\mathfrak{f})$ consisting of principal ideals (α) with $\alpha \in K_\mathfrak{f}$.

By a **Hecke character of K to the modulus $\mathfrak{f}$** we mean a group homomorphism $\chi : I(\mathfrak{f}) \to \mathbb{C}^\times$ satisfying the following condition: There exists a continuous homomorphism $\chi_\infty : (\mathbb{R} \otimes_\mathbb{Q} K)^\times \to \mathbb{C}^\times$ such that if $\alpha \in K_\mathfrak{f}$ then $\chi((\alpha)) = 1/\chi_\infty(\alpha)$. Here $\alpha \in K^\times$ is identified with $1 \otimes \alpha \in (\mathbb{R} \otimes_\mathbb{Q} K)^\times$, so an equivalent formulation is

$$\chi(\alpha\mathcal{O}) = \chi_\infty^{-1}(1 \otimes \alpha) \qquad (\alpha \in K_\mathfrak{f}). \tag{1.10}$$

We call χ_∞ the **infinity type** of χ. Thus a Hecke character to the modulus $\mathfrak{f}$ is a character of $I(\mathfrak{f})$ which is completely determined on $P_\mathfrak{f}$ by its infinity type.

Two points should be noted. First of all, χ_∞ is a continuous homomorphism if and only its reciprocal is, so the content of the definition would not change if we omitted the exponent -1 on the right-hand side of (1.10). Nonetheless we retain it for the sake of the correspondence between Hecke characters and idele class characters to be discussed later. The second point is that the continuity of χ_∞ is an unambiguous concept, because all norms on the finite-dimensional real vector space

$$\mathbb{R} \otimes_{\mathbb{Q}} K \cong \mathbb{R}^{r_1} \otimes \mathbb{C}^{r_2} \tag{1.11}$$

are equivalent. Here r_1 and r_2 have the usual meanings; in fact we may specify the isomorphism in (1.11) – call it ι – by requiring that for $\alpha \in K$ we have

$$\iota(1 \otimes \alpha) = (\sigma_1(\alpha), \sigma_2(\alpha), \dots, \sigma_{r_1+r_2}(\alpha)), \tag{1.12}$$

where $\sigma_1, \dots, \sigma_{r_1}$ are the distinct real embeddings of K and $\sigma_{r_1+1}, \dots, \sigma_{r_1+r_2}$ are chosen from the distinct pairs of conjugate complex embeddings. Using (1.11) and (1.12), we may view χ_∞ as a continuous homomorphism $\mathbb{R}^{\times r_1} \otimes \mathbb{C}^{\times r_2} \to \mathbb{C}^\times$. Since $\iota(K_\mathfrak{f})$ is dense in $\mathbb{R}^{\times r_1} \otimes \mathbb{C}^{\times r_2}$ we see that χ_∞ is uniquely determined by (1.10).

As with Dirichlet characters, there is a notion of primitivity: A Hecke character χ to the modulus $\mathfrak{f}$ is **primitive** if there does not exist an integral ideal $\mathfrak{f}'$ properly dividing $\mathfrak{f}$ such that χ extends to a Hecke character to the modulus $\mathfrak{f}'$. Note that $I(\mathfrak{f}) \subset I(\mathfrak{f}')$, so that the definition is meaningful. Given a Hecke character χ to the modulus $\mathfrak{f}$, there exists a unique pair $(\chi', \mathfrak{f}')$ such that $\mathfrak{f}'$ is an integral ideal dividing $\mathfrak{f}$ and χ' is a primitive Hecke character to the modulus $\mathfrak{f}'$ extending χ. We call $\mathfrak{f}'$ and χ' the **conductor** of χ and the **primitive Hecke character determined by** χ respectively. Thus a Hecke character is primitive if and only its modulus equals its conductor. If χ is primitive, as we shall usually assume, then its conductor will be denoted $\mathfrak{f}(\chi)$.

2.2. Examples

The simplest examples are primitive Hecke characters χ with $\mathfrak{f}(\chi) = \mathcal{O}$, for then the requirement in (1.10) is simply that $\chi(\alpha\mathcal{O}) = \chi^{-1}(1 \otimes \alpha)$ for all $\alpha \in K^\times$. Consider for instance the **power-of-the-norm** map $\chi : I \to \mathbb{C}^\times$ given by $\chi(\mathfrak{a}) = (\mathbf{N}\mathfrak{a})^c$, where $c \in \mathbb{C}$ is fixed and $\mathbf{N}\mathfrak{a}$ is the absolute norm of $\mathfrak{a}$. Viewing χ_∞ as a character $\mathbb{R}^{\times r_1} \otimes \mathbb{C}^{\times r_2} \to \mathbb{C}^\times$, we see that (1.10) holds with

$$\chi_\infty(u_1, u_2, \dots, u_{r_1+r_2}) = |u_1 u_2 \cdots u_{r_1}|^{-c} \cdot |u_{r_1+1} u_{r_1+2} \cdots u_{r_1+r_2}|^{-2c}. \tag{1.13}$$

Note that apart from the trivial Hecke character (i. e. the case $s_0 = 0$), the power-of-the-norm map has infinite order.

Another example with $\mathfrak{f}(\chi) = \mathcal{O}$, this time of finite order, is an **ideal class character**, in other words a character χ of the ideal class group I/P of K: if we view χ as a character of I trivial on P then (1.10) holds with χ_∞ equal to the trivial character. Now if $\mathfrak{f}$ is a nonzero integral ideal of K then the natural map $I(\mathfrak{f})/P(\mathfrak{f}) \to I/P$ is an isomorphism, and therefore an ideal class character becomes a Hecke character to the modulus $\mathfrak{f}$ by restriction to $I(\mathfrak{f})$. In particular, if χ is any Hecke character to the modulus $\mathfrak{f}$ then so is $\chi\varphi$, where φ is an ideal class character of K. Note that $(\chi\varphi)_\infty = \chi_\infty$ and that $\chi\varphi$ is primitive if and only if χ is. The upshot is that whenever we have an example of a primitive Hecke character of a given infinity type then we automatically have h such examples, where h is the class number of K.

2.3. A nonexample

It may also be instructive to see a character of I which is not a Hecke character. Since I is the free abelian group on the nonzero prime ideals of $\mathcal{O}$, we can define a homomorphism $I \to \mathbb{C}^\times$ simply by specifying its values on prime ideals. Thus we get a character $\chi : I \to \{\pm\}$ (the "Liouville function" of K) by specifying that $\chi(\mathfrak{p}) = -1$ for every prime ideal $\mathfrak{p}$. Equivalently, $\chi(\mathfrak{a}) = (-1)^{\tau(\mathfrak{a})}$, where $\tau(\mathfrak{a})$ is the total number of prime ideals (taking account of multiplicities) occurring in a factorization of $\mathfrak{a}$ into prime ideals. But the set of $\alpha \in K^\times$ such that $\tau(\alpha\mathcal{O})$ is even and the set of α such that $\tau(\alpha\mathcal{O})$ is odd are both dense in $(\mathbb{R} \otimes_{\mathbb{Q}} K)^\times$. Hence there does not exist a continuous homomorphism $\chi_\infty : (\mathbb{R} \otimes_{\mathbb{Q}} K)^\times \to \mathbb{C}^\times$ such that $\chi(\alpha\mathcal{O}) = \chi_\infty^{-1}(1 \otimes \alpha)$ for $\alpha \in K^\times$, and consequently χ is not a Hecke character.

2.4. Unitary Hecke characters

The L-function associated to a Hecke character is defined by a Dirichlet series, and in preparation for writing down this Dirichlet series explicitly we prove a result which will assure us that the series does converge in some right half-plane. If χ is a one-dimensional character of a group then the associated unitary character $\chi/|\chi|$ will be denoted χ_{u}, so that $\chi = \chi_{\mathrm{u}} \cdot |\chi|$.

Proposition 1.1. *If χ is a Hecke character of K then there exists $c \in \mathbb{R}$ such that $|\chi| = \mathbf{N}^c$ on $I(\mathfrak{f})$, where $\mathfrak{f}$ is the modulus of χ. Thus*

$$\chi = \chi_{\mathrm{u}} \cdot \mathbf{N}^c.$$

In particular, every Hecke character is a unitary Hecke character times a real power of the norm.

Proof. Let $\mathbb{R}_+$ denote the multiplicative group of positive real numbers. The point requiring proof is that a Hecke character with values in $\mathbb{R}_+$ coincides on its domain with a real power of the norm. So after changing notation we may suppose that we are given a Hecke character $\chi : I(\mathfrak{f}) \to \mathbb{R}_+$. It suffices to see that χ_∞ has the form (1.13) with $c \in \mathbb{R}$, for then $\chi \cdot \mathbf{N}^{-c}$ is a character with values in $\mathbb{R}_+$ which factors through the finite group $I(\mathfrak{f})/P_{\mathfrak{f}}$, and consequently $\chi \cdot \mathbf{N}^{-c}$ is trivial.

Now the absolute value function and the polar coordinate map give topological group isomorphisms $\mathbb{R}^\times \cong \{\pm 1\} \times \mathbb{R}_+$ and $\mathbb{C}^\times \cong \mathbf{T} \times \mathbb{R}_+$ respectively, where $\mathbf{T} = \{e^{i\theta} : \theta \in \mathbb{R}\}$. Furthermore any continuous homomorphism $\mathbb{R}^+ \to \mathbb{R}^+$ raises the elements of $\mathbb{R}_+$ to some fixed real exponent, which we choose to write as twice another exponent in the case of the complex places. Thus χ_∞ has the form

$$\chi_\infty(u_1, u_2, \dots, u_{r_1+r_2}) = \prod_{j=1}^{r_1} |u_j|^{c_j} \cdot \prod_{j=r_1+1}^{r_1+r_2} |u_j|^{2c_j} \tag{1.14}$$

with $c_j \in \mathbb{R}$ for $1 \leqslant j \leqslant r_1+r_2$. Now if $\varepsilon \in \mathcal{O}^\times \cap K_{\mathfrak{f}}$ then $\chi(\mathcal{O}) = \chi(\varepsilon\mathcal{O}) = \chi_\infty^{-1}(1 \otimes \varepsilon)$, so

$$\prod_{j=1}^{r_1} |\sigma_j(\varepsilon)|^{c_j} \cdot \prod_{j=r_1+1}^{r_1+r_2} |\sigma_j(\varepsilon)|^{2c_j} = 1. \tag{1.15}$$

But $\mathcal{O}^\times \cap K_{\mathfrak{f}}$ has finite index in $\mathcal{O}^\times$. Hence on taking the log of both sides of (1.15) and applying the Dirichlet unit theorem, we deduce that the linear form on $\mathbb{R}^{r_1+r_2}$

given by

$$(t_1, t_2, \dots, t_{r_1+r_2}) \mapsto \sum_{j=1}^{r_1} c_j t_j + \sum_{j=r_1+1}^{r_1+r_2} 2c_j t_j$$

vanishes identically on the hyperplane $\sum_{j=1}^{r_1} t_j + \sum_{j=r_1+1}^{r_1+r_2} 2t_j = 0$, whence c_j is independent of j. So (1.14) is indeed of the form (1.13) with $c \in \mathbb{R}$, as indeed. $\square$

2.5. Hecke L-functions

If χ is a Dirichlet character to the modulus N then $\chi(n) = 0$ whenever $\gcd(n, N) > 1$, and by virtue of this convention the Dirichlet series for $L(s, \chi)$ can be written either as a sum over integers prime to N or as a sum over all positive integers. In the same way, given a Hecke character χ to the modulus $\mathfrak{f}$, one sets $\chi(\mathfrak{a}) = 0$ whenever $\mathfrak{a} + \mathfrak{f} \neq \mathcal{O}$, and one defines the associated L-series $L(s, \chi)$ by

$$L(s, \chi) = \sum_{\mathfrak{a}} \chi(\mathfrak{a})(\mathbf{N}\mathfrak{a})^{-s}, \tag{1.16}$$

where $\mathfrak{a}$ runs over all nonzero integral ideals of K or alternatively over the subset of ideals relatively prime to $\mathfrak{f}$. For example, if χ is the trivial Hecke character to the modulus $\mathcal{O}$ then $L(s, \chi)$ is the Dedekind zeta function

$$\zeta_K(s) = \sum_{\mathfrak{a}} (\mathbf{N}\mathfrak{a})^{-s} \tag{1.17}$$

of K, while if χ is more generally the power-of-the-norm character $\mathfrak{a} \mapsto (\mathbf{N}\mathfrak{a})^c$ then $L(s, \chi) = \zeta_K(s - c)$. For any χ, the definition (1.16) is meaningful in the sense that the given Dirichlet series converges in some right half-plane. Indeed by writing χ as in Proposition 1.1 we see that the Dirichlet series is absolutely convergent for $\Re(s) > c + 1$.

The basic analytic fact about $L(s, \chi)$, proved by Hecke, is that $L(s, \chi)$ extends to a meromorphic function on $\mathbb{C}$ which is either entire (if χ is not a power of the norm) or holomorphic except for a simple pole at $s = c + 1$ (if $\chi = \mathbf{N}^c$) satisfying a functional equation relative to the transformation $s \mapsto 2c + 1$. More about the functional equation later: For the moment we return to the right half-plane of absolute convergence and observet that $L(s, \chi)$ can be written there as an Euler product,

$$L(s, \chi) = \prod_{\mathfrak{p}} (1 - \chi(\mathfrak{p})\mathbf{N}(\mathfrak{p})^{-s})^{-1} \tag{1.18}$$

where $\mathfrak{p}$ runs over the prime ideals of K or over the subset of prime ideals not dividing $\mathfrak{f}$. The fact that the Dirichlet series in (1.16) is equal to the Euler product in (1.18) is proved in much the same way as the corresponding equality for Dirichlet L-functions. In the latter case, the key fact needed is the unique factorization of positive integers into primes; in the case of Hecke L-functions one uses instead the fact that every nonzero ideal of $\mathcal{O}$ has a unique factorization into prime ideals.

2.6. Dirichlet characters as Hecke characters

The analogy between Dirichlet L-functions and Hecke L-functions is no coincidence, for in the case $K = \mathbb{Q}$ there is a bijection $\chi \mapsto \chi_{\mathrm{Hec}}$ from the set of Dirichlet characters to the set of Hecke characters of $\mathbb{Q}$ of finite order. The map $\chi \mapsto \chi_{\mathrm{Hec}}$ is

defined as follows: Given a Dirichlet character χ to the modulus N, take $\mathfrak{f} = (N)$ and set

$$\chi_{\mathrm{Hec}}(\mathfrak{a}) = \chi(a) \tag{1.19}$$

for $\mathfrak{a} \in I(\mathfrak{f})$, where a is the unique positive generator of $\mathfrak{a}$. Contemplating (1.19), we recognize that the subscript on χ_{Hec} is superfluous, because the left-hand side of (1.19) is a function of ideals whereas the right-hand side is a function of numbers. Hence without risk of confusion we can write (1.19) in the form $\chi(\mathfrak{a}) = \chi(a)$. Furthemore, on making the identification $(\mathbb{R} \otimes_{\mathbb{Q}} K)^\times = \mathbb{R}^\times$ one readily verifies that (1.10) holds with χ_∞ equal to the trivial character or the sign character $x \mapsto x/|x|$ according as χ is even or odd as a Dirichlet character. Thus χ_{Hec} is indeed a Hecke character. One can also check that $L(s, \chi) = L(s, \chi_{\mathrm{Hec}})$ and that χ is primitive if and only if χ_{Hec} is. Henceforth we drop the subscript on χ_{Hec}.

2.7. Hecke characters on principal ideals

While the defining property (1.10) of a Hecke χ refers only to $\chi|P_{\mathfrak{f}}$, the following proposition shows that one can also deduce something about $\chi|P(\mathfrak{f})$. For an integer $n \geqslant 1$ let $\boldsymbol{\mu}_n \subset \mathbb{C}^\times$ be the subgroup of nth roots of unity.

Proposition 1.2. *Let $\chi : I(\mathfrak{f}) \to \mathbb{C}^\times$ be a homomorphism and $\chi_\infty : (\mathbb{R} \otimes_{\mathbb{Q}} K)^\times \to \mathbb{C}^\times$ a continuous homomorphism. Then χ is a Hecke character with infinity type χ_∞ if and only if there is an integer $n \geqslant 1$ and a homomorphism $\varepsilon : (\mathcal{O}/\mathfrak{f})^\times \to \boldsymbol{\mu}_n$ such that*

$$\chi(\alpha\mathcal{O}) = \varepsilon(\alpha)\chi_\infty^{-1}(1 \otimes \alpha)$$

for $\alpha \in K(\mathfrak{f})$. Here ε is viewed as a character of $K(\mathfrak{f})$ by composition with

$$K(\mathfrak{f}) \longrightarrow K(\mathfrak{f})/K_{\mathfrak{f}} \longrightarrow (\mathcal{O}/\mathfrak{f})^\times,$$

the first arrow being the quotient map and the second the natural isomorphism.

Proof. Sufficiency is immediate, because ε is trivial on $K_{\mathfrak{f}}$. To prove necessity let n be the order of $K(\mathfrak{f})/K_{\mathfrak{f}}$. If χ is a Hecke character with infinity type χ_∞ and $\alpha \in K(\mathfrak{f})$ then $\alpha^n \in K_{\mathfrak{f}}$, whence $\chi(\alpha^n\mathcal{O}) = \chi_\infty^{-1}(1 \otimes \alpha^n)$ or in other words $\chi((\alpha\mathcal{O})^n) = \chi_\infty^{-1}((1 \otimes \alpha)^n)$. As both χ and χ_∞ are homomorphisms it follows that $\chi(\alpha\mathcal{O}) = \varepsilon(\alpha)\chi_\infty^{-1}(1 \otimes \alpha)$ with an nth root of unity $\varepsilon(\alpha)$. It follows immediately that $\varepsilon : K \to \mathbb{C}^\times$ is a homomorphism trivial on $K_{\mathfrak{f}}$ and may therefore be viewed as a character of $K(\mathfrak{f})/K_{\mathfrak{f}} \cong (\mathcal{O}/\mathfrak{f})^\times$ □

Proposition 1.2 completes our discussion of Hecke characters in general. Next we specialize to the case of imaginary quadratic fields.

3. A family of Hecke L-functions with trivial central zeros

Let K be an imaginary quadratic field. Then $\mathbb{R} \otimes_{\mathbb{Q}} K \cong \mathbb{C}$, and after fixing an embedding of K in $\mathbb{C}$ we may use the preceding isomorphism to identify $\mathbb{R} \otimes_{\mathbb{Q}} K$ with $\mathbb{C}$ and hence $(\mathbb{R} \otimes_{\mathbb{Q}} K)^\times$ with $\mathbb{C}^\times$. The map χ_∞ of (1.10) then becomes a continuous homomorphism from $\mathbb{C}^\times$ to itself, whence it is in particular meaningful to ask for Hecke characters χ of K such that $\chi_\infty(z) = z^{-1}$. When χ_∞ has this form we say that χ is of type $(1, 0)$. To demystify this terminology we add that if $\chi_\infty(z) = z^{-p}\overline{z}^{-q}$ with $p, q \in \mathbb{Z}$ then χ is said to be of type (p, q).

Write D for the absolute value of the discriminant of K, and let κ be the primitive quadratic Dirichlet character of conductor D defined by

$$\kappa(n) = \left(\frac{-D}{n}\right). \tag{1.20}$$

Here we follow the convention that the Kronecker symbol on the right has the value -1 when $n = -1$ (in other words, the Kronecker symbol is viewed as a Dirichlet character rather than as a norm residue symbol). We would like to exhibit a canonical choice of a Hecke character of K of type (1,0) as in Gross [**26**]. Thus we consider the set $X(D)$ of primitive Hecke characters χ of K of type (1,0) satisfying the following conditions:

(a) $\mathfrak{f}(\chi)|D^\infty$.
(b) $\chi(n\mathcal{O}) = \kappa(n)n$ for $n \in \mathbb{Z}$ prime to D.
(c) The values of χ on $P(\mathfrak{f}(\chi))$ lie in K.

Let Φ be the set of ideal class characters of K. If $\chi \in X(D)$ then $\chi\varphi \in X(D)$ for every $\varphi \in \Phi$, so the cardinality of $X(D)$ is a multiple of $h(D)$, the class number of K. Henceforth we assume that $D \neq 3, 4$.

Proposition 1.3.

$$|X(D)| = \begin{cases} h(D) & \text{if } D \text{ is odd,} \\ 0 & \text{if } 4||D, \\ 2h(D) & \text{if } 8|D. \end{cases}$$

Proof. Writing $\mathfrak{f}$ to denote an ideal dividing D^∞, let E be the set of all characters of the form $\varepsilon : (\mathcal{O}/\mathfrak{f})^\times \to \{\pm 1\}$ which satisfy two conditions: First, $\varepsilon(n) = \kappa(n)$ for $n \in \mathbb{Z}$ relatively prime to D, and second, ε is primitive, in other words ε does not factor through $(\mathcal{O}/\mathfrak{f}')^\times$ for any ideal $\mathfrak{f}'$ properly dividing $\mathfrak{f}$. We claim that the proposition is equivalent to the assertion

$$|E| = \begin{cases} 1 & \text{if } D \text{ is odd,} \\ 0 & \text{if } 4||D, \\ 2 & \text{if } 8|D. \end{cases} \tag{1.21}$$

In other words, we claim that $|X(D)| = |E|h(D)$.

To verify the claim, we use Proposition 1.2: The restriction to $P(\mathfrak{f}(\chi))$ of any $\chi \in X(D)$ has the form $\chi(\alpha\mathcal{O}) = \varepsilon(\alpha)\alpha$ for some character ε of $(\mathcal{O}/\mathfrak{f}(\chi))^\times$ with values in the nth roots of unity. As the values of χ on $P(\mathfrak{f}(\chi))$ lie in K and $K \neq \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-4})$ it follows that n can be taken to be 2. Thus we may view ε as a character $(\mathcal{O}/\mathfrak{f}(\chi))^\times \to \{\pm 1\}$, necessarily primitive since χ is primitive. Since $\chi(n\mathcal{O}) = \kappa(n)n$ for $n \in \mathbb{Z}$ prime to D we deduce that $\varepsilon \in E$, and thus we obtain a map $X(D) \to E$. The fibers of the map have cardinality $h(D)$, because there are $h(D)$ ways to extend a character of $P(\mathfrak{f}(\chi))$ to a character of $I(\mathfrak{f}(\chi))$. To see that the map $\chi \mapsto \varepsilon$ is surjective, let $\varepsilon : (\mathcal{O}/\mathfrak{f})^\times \to \{\pm 1\}$ be a a given element of E. We would like to define a character χ of $P(\mathfrak{f})$ by setting

$$\chi(\alpha\mathcal{O}) = \varepsilon(\alpha)\alpha \tag{1.22}$$

for $\alpha \in K(\mathfrak{f})$, but we must check that the right-hand side of (1.22) depends only on the principal ideal $\alpha\mathcal{O}$ and not on the choice of generator α. Since $K \neq \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-4})$, the only other generator is $-\alpha$; but $\varepsilon(-\alpha) = \kappa(-1)\varepsilon(\alpha) = -\varepsilon(\alpha)$

by (1.20). Hence if α is replaced by $-\alpha$ then the right-hand side of (1.22) is unchanged, so we obtain a well-defined character χ of $P(\mathfrak{f})$. Extending it arbitarily to $I(\mathfrak{f})$ we obtain an element of $X(D)$.

Having established the claim, we must now prove (1.21). Given $\varepsilon \in E$, let us write $\mathfrak{f}(\varepsilon)$ for the ideal $\mathfrak{f}$ such that ε is a primitive character of $(\mathcal{O}/\mathfrak{f})^\times$. (Thus $\mathfrak{f}(\varepsilon) = \mathfrak{f}(\chi)$.) If $D||4$ write $\mathfrak{T}$ for the prime ideal of $\mathcal{O}$ lying over 2. It is helpful to note at the outset that if $\varepsilon \in E$ then

$$\mathfrak{f}(\varepsilon) \text{ is divisible by } \begin{cases} \sqrt{-D}\mathcal{O} & \text{if } D \text{ is odd,} \\ \sqrt{-D}\mathfrak{T} & \text{if } 4||D, \\ 2\sqrt{-D}\mathcal{O} & \text{if } 8|D. \end{cases} \tag{1.23}$$

To verify (1.23) use the fact $\varepsilon(n) = \kappa(n)$ for $n \in \mathbb{Z}$ prime to D. Since κ is primitive of conductor D, it follows that D divides $\mathbb{Z} \cap \mathfrak{f}(\varepsilon)$, but one readily checks that an ideal $\mathfrak{a}$ of $\mathcal{O}$ with the property that D divides $\mathbb{Z} \cap \mathfrak{a}$ is divisible by the right-hand side of (1.23).

We now consider the three cases in (1.21) one by one. Suppose first that D is odd. If $\varepsilon \in E$ then $\sqrt{-D}\mathcal{O}|\mathfrak{f}(\varepsilon)$ by (1.23), but also $\mathfrak{f}(\varepsilon)|D^\infty$ by assumption. Thus if $\mathfrak{f}(\varepsilon)$ is *properly* divisible by $\sqrt{-D}\mathcal{O}$ then $(\mathcal{O}/\mathfrak{f}(\varepsilon))^\times$ is a nontrivial extension of $\mathcal{O}/\sqrt{-D}\mathcal{O})^\times$ by a group of odd order, contradicting the fact that ε is both quadratic and primitive. It follows that $\mathfrak{f}(\varepsilon) = \sqrt{-D}\mathcal{O}$. But the natural map $(\mathbb{Z}/D\mathbb{Z})^\times \to (\mathcal{O}/\sqrt{-D}\mathcal{O})^\times$ is an isomorphism, and $\varepsilon(n) = \kappa(n)$ for $n \in (\mathbb{Z}/D\mathbb{Z})^\times$. Hence there is a unique choice for ε, and $|E| = 1$. At the same time we have proved that if D is odd then

$$\mathfrak{f}(\chi) = \sqrt{-D}\mathcal{O} \tag{1.24}$$

for $\chi \in X(D)$.

Next suppose that $4||D$. Then $D = 4C$ with $C \equiv 1 \bmod 4$. If there exists an $\varepsilon \in E$, then $\sqrt{-C}\mathfrak{T}^4|\mathfrak{f}(\varepsilon)$ by (1.23); we claim that in fact

$$\mathfrak{f}(\varepsilon) = \sqrt{-C}\mathfrak{T}^4. \tag{1.25}$$

To see this, we first argue as in the case D odd: Since ε is quadratic and primitive, the kernel of the reduction map $(\mathcal{O}/\mathfrak{f}(\varepsilon))^\times \to (\mathcal{O}/\sqrt{-C}\mathfrak{T}^4)^\times$ has 2-power order. As $\mathfrak{f}(\varepsilon)|D^\infty$ this already implies that $\mathfrak{f}(\varepsilon) = \sqrt{-C}\mathfrak{T}^k$ with $k \geqslant 4$. But it is easily verified by induction that if $k \geqslant 5$ then every element of the kernel of $(\mathcal{O}/\mathfrak{T}^k)^\times \to (\mathcal{O}/\mathfrak{T}^5)^\times$ is a square in $(\mathcal{O}/\mathfrak{T}^k)^\times$, so again, the fact that ε is quadratic and primitive ensures that $k = 4$ or 5. Now choose a rational integer n such that $n \equiv 5 \bmod 8$ and $n \equiv 1 \bmod C$. Then n represents the nontrivial element of the kernel of $(\mathcal{O}/\mathfrak{T}^5)^\times \to (\mathcal{O}/\mathfrak{T}^4)^\times$; but $\varepsilon(n) = \kappa(n) = 1$. Since ε is primitive, (1.25) follows.

To obtain a contradiction from (1.25), write

$$(\mathcal{O}/\sqrt{-C}\mathfrak{T}^4)^\times \cong (\mathcal{O}/4\mathcal{O})^\times \times (\mathcal{O}/\sqrt{-C}\mathcal{O})^\times$$

and $\varepsilon = \varepsilon'\varepsilon''$ with quadratic characters ε' and ε'' of $(\mathcal{O}/4\mathcal{O})^\times$ and $(\mathcal{O}/\sqrt{-C}\mathcal{O})^\times$ respectively. Then $\varepsilon(-1) = \kappa(-1) = -1$, but $\varepsilon''(-1) = 1$ because $C \equiv 1 \bmod 4$, so $\varepsilon'(-1) = -1$. This is a contradiction, because -1 is a square in $(\mathcal{O}/4\mathcal{O})^\times$: indeed $(2 + \sqrt{-C})^2 \equiv -1 \bmod 4O$.

Finally, suppose that $8|D$. Write $\mathfrak{T}$ for the prime ideal of $\mathcal{O}$ lying over 2. As in the case $4||D$, if $k \geqslant 5$, then every element of the kernel of $(\mathcal{O}/\mathfrak{T}^k)^\times \to (\mathcal{O}/\mathfrak{T}^5)^\times$ is a square in $(\mathcal{O}/\mathfrak{T}^k)^\times$. Appealing to (1.23) and arguing as before, we deduce that $(\varepsilon) = 2\sqrt{-D}\mathcal{O}$. Now write $D = 8C$, and as in the case $4||D$, consider the

decompositions $(\mathcal{O}/2\sqrt{-D}\mathcal{O})^\times \cong (\mathcal{O}/4\mathfrak{T})^\times \times (\mathcal{O}/\sqrt{-C}\mathcal{O})^\times$ and $\varepsilon = \varepsilon'\varepsilon''$. Also write $(\mathbb{Z}/D\mathbb{Z})^\times \cong (Z/8\mathbb{Z})^\times \times (Z/C\mathbb{Z})^\times$ and $\kappa = \kappa'\kappa''$. Using the natural embedding of $(Z/C\mathbb{Z})^\times$ in $(\mathcal{O}/\sqrt{-C}\mathcal{O})^\times$ to identify these two groups, we have $\varepsilon'' = \kappa''$, so ε'' is uniquely determined and $|E|$ is equal to the number of possibilities for ε'. Now the natural embedding of $(\mathbb{Z}/8\mathbb{Z})^\times$ in $(\mathcal{O}/4\mathfrak{T})^\times$ realizes $(\mathbb{Z}/8\mathbb{Z})^\times$ as one summand in a direct sum decomposition of $(\mathcal{O}/4\mathfrak{T})^\times$, the complementary summand being the cyclic group of order 4 generated by the coset of $1+\sqrt{-2C}$. On the factor $(\mathbb{Z}/8\mathbb{Z})^\times$ the character ε' coincides with κ', and since ε is quadratic there are exactly two possibilites for the value of ε' on the coset of $1+\sqrt{-2C}$, namely ± 1. Thus $|E| = 2$. In the process we have proved that if $8|D$ then

$$\mathfrak{f}(\chi) = 2\sqrt{-D}\mathcal{O} \tag{1.26}$$

for $\chi \in X(D)$. □

3.1. The functional equation

While we have not yet discussed the functional equation of Hecke L-functions over arbitrary number fields, if K is imaginary quadratic and χ a Hecke character of K of type $(1,0)$ then the functional equation is easily stated:

$$\Lambda(s,\chi) = W(\chi)\Lambda(2-s,\overline{\chi}) \tag{1.27}$$

with $|W(\chi)| = 1$ and

$$\Lambda(s,\chi) = (D\mathbf{N}\mathfrak{f}(\chi))^{s/2}\Gamma_{\mathbb{C}}(s)L(s,\chi). \tag{1.28}$$

Since $\overline{\chi}$ is of type $(0,1)$, the definition of $\Lambda(s,\overline{\chi})$ is technically not covered by (1.28), but it offers no surprises:

$$\Lambda(s,\overline{\chi}) = (D\mathbf{N}\mathfrak{f}(\chi))^{s/2}\Gamma_{\mathbb{C}}(s)L(s,\overline{\chi}). \tag{1.29}$$

The appearance of $\mathfrak{f}(\chi)$ in place of $\mathfrak{f}(\overline{\chi})$ on the right-hand side of (1.29) is not a misprint; one readily checks that $\mathfrak{f}(\overline{\chi}) = \mathfrak{f}(\chi)$. Now take $\chi \in X(D)$ with D either odd or divisible by 8. We shall give explicit formulas for the factors that go into the functional equation. One factor has already been made explicit (cf. (1.24) and (1.26)):

Proposition 1.4. *If $\chi \in X(D)$ then*

$$\mathfrak{f}(\chi) = \begin{cases} \sqrt{-D}\mathcal{O} & \text{if } D \text{ is odd,} \\ 2\sqrt{-D}\mathcal{O} & \text{if } 8|D. \end{cases}$$

The root number $W(\chi)$ can also be computed. First consider the case D odd. The proof of the following proposition is as in Gross ([**26**], pp. 60 – 63) and will be reproduced in Lecture 2.

Proposition 1.5. *If D is odd and $\chi \in X(D)$ then*

$$W(\chi) = \left(\frac{2}{D}\right).$$

Next recall that if $8|D$ then $|X(D)| = 2h(D)$. The following statement is proved in [**48**], pp. 538, and a proof will also be outlined in Exercise 2.3.

Proposition 1.6. *Suppose that* $8|D$*, and put*

$$X^{\pm}(D) = \{\chi \in X(D) : W(\chi) = \pm 1\}.$$

Then $|X^{\pm}(D)| = h(D)$*. In fact if* $\chi \in X^{\pm}(D)$ *then* $X^{\pm}(D) = \{\chi\varphi : \varphi \in \Phi\}$*, where* Φ *is the set of ideal class characters of* K*.*

In spite of Propositions (1.5) and (1.6), we cannot conclude that our "canonical" family of Hecke L-functions exhibits trivial central zeros until we have verified that $\Lambda(s, \overline{\chi}) = \Lambda(s, \chi)$. But if we think of $L(s, \chi)$ as the Dirichlet series $\sum \chi(\mathfrak{a})(\mathbf{N}\mathfrak{a})^{-s}$ then the desired identity $L(s, \overline{\chi}) = L(s, \chi)$ is an immediate consequence of the equivariance of χ with respect to complex conjugation:

Proposition 1.7. *If* $\chi \in X(D)$ *then*

$$\chi(\overline{\mathfrak{a}}) = \overline{\chi(\mathfrak{a})}$$

for $\mathfrak{a} \in I(\mathfrak{f}(\chi))$*.*

Proof. Put $n = \mathbf{N}\mathfrak{a}$, so that $\mathfrak{a}\overline{\mathfrak{a}} = n\mathcal{O}$. Then

$$\chi(\mathfrak{a})\chi(\overline{\mathfrak{a}}) = \chi(n\mathcal{O}) = \kappa(n)n = n,$$

because the Kronecker symbol κ is trivial on norms from K. Thus $\chi(\mathfrak{a})\chi(\overline{\mathfrak{a}}) = \mathbf{N}\mathfrak{a}$, and it suffices to see that $\chi(\mathfrak{a})\overline{\chi(\mathfrak{a})} = \mathbf{N}\mathfrak{a}$ or in other words that

$$|\chi(\mathfrak{a})| = \sqrt{\mathbf{N}\mathfrak{a}}. \tag{1.30}$$

Now in contrast to the identity $\chi(\mathfrak{a})\chi(\overline{\mathfrak{a}}) = \mathbf{N}\mathfrak{a}$, which depended on the relation $\varepsilon(n) = \kappa(n)$, (1.30) is a general property of Hecke characters of type (1,0). In fact since both sides of (1.30) are postive, it suffices to verify that equality holds after both sides are raised to the power $h(D)|K(\mathfrak{f})/K_{\mathfrak{f}}|$, where $\mathfrak{f} = \mathfrak{f}(\chi)$. Thus we may assume that $\mathfrak{a} = \alpha\mathcal{O}$ with $\alpha \in K_{\mathfrak{f}}$. But then $\chi(\mathfrak{a}) = \alpha$ and (1.30) is immediate. □

Thus if $\chi \in X(D)$ then the functional equation (1.27) becomes

$$\Lambda(s, \chi) = W(\chi)\Lambda(2 - s, \chi) \tag{1.31}$$

and we can talk about trivial central zeros. (Note by the way that quite apart from Propositions (1.5) and (1.6), the fact that $W(\chi) = \pm 1$ is clear *a priori* from (1.31).) Now $-D$ is a discriminant, so if D is odd then D is 3 mod 4 and in particular either 3 or 7 mod 8. Hence Propositions Propositions (1.5) and (1.6) imply that $L(s, \chi)$ has a trivial central zero if and only if either $D \equiv 3 \bmod 8$ or else $8|D$ and $\chi \in X^{-}(D)$. In the remaining cases, when $D \equiv 7 \bmod 4$ or $8|D$ and $\chi \in X^{+}(D)$, there is no trivial reason for $L(s, \chi)$ to vanish at $s = 1$, and we can ask the same question as with Dirichlet L-functions: Is $L(1, \chi)$ in fact nonzero? Actually, even if $W(\chi) = -1$ we can ask the analogous question about $L'(1, \chi)$, for while $L(s, \chi)$ vanishes to odd order at $s = 1$, there is no trivial reason for the order of vanishing to be > 1.

Theorem 1.2.

$$\mathrm{ord}_{s=1}L(s, \chi) = \begin{cases} 0 & \text{if } W(\chi) = 1 \\ 1 & \text{if } W(\chi) = -1. \end{cases}$$

Proof. For the case $W(\chi) = 1$ see Montgomery and Rohrlich [**45**], and for the case $W(\chi) = -1$ see Miller and Yang [**44**]. We mention just one aspect of these proofs and of others like them, namely the key role played by the fact that

$$\{\chi^{\sigma} : \sigma \in \mathrm{Aut}(\mathbb{C}/K)\} = \{\chi\varphi : \varphi \in \Phi\} \tag{1.32}$$

for $\chi \in X(D)$. Here χ^σ is the character defined by $\chi^\sigma(\mathfrak{a}) = \chi(\mathfrak{a})^\sigma$ for $\mathfrak{a} \in I(\mathfrak{f})$ with $\mathfrak{f} = \mathfrak{f}(\chi)$. As the values of χ on principal ideals takes lie in K, it follows that χ and χ^σ coincide on principal ideals, and consequently the left-hand side of (1.32) is contained in the right-hand side. Thus to prove that equality holds it suffices to see that the cardinality of the left-hand side of (1.32) is $\geqslant h(D)$. Given $\mathfrak{a} \in I(\mathfrak{f})$, let n be its order in the ideal class group $I(\mathfrak{f})/P(\mathfrak{f})$; then $\mathfrak{a}^n = \alpha\mathcal{O}$ for some $\alpha \in K(\mathfrak{f})$, and consequently $\chi(\mathfrak{a})^n = \pm\alpha$. One readily deduces that $\chi(\mathfrak{a})$ generates an extension of K of degree n. Now choose ideals $\mathfrak{a}_1, \mathfrak{a}_2, \dots, \mathfrak{a}_t \in I(\mathfrak{f})$ such that I/P is the direct sum of the cyclic subgroups generated by the classes of the ideals $\mathfrak{a}_i$. Then $h(D) = n_1 n_2 \cdots n_t$, where n_i is the order of the class of $\mathfrak{a}_i$. Given these observations, it is not hard to believe or to prove that the extension of K generated by $\chi(\mathfrak{a}_1), \chi(\mathfrak{a}_2), \dots, \chi(\mathfrak{a}_t)$ has degree $h(D)$ over K. It follows that the left-hand side of (1.32) has cardinality $\geqslant h(D)$, whence equality holds and (1.32) follows.

The significance of (1.32) is that it meshes well with algebraicity results for special values of L-functions. In the case case $W(\chi) = 1$, results of Shimura [**57**], [**58**] imply that if $L(1, \chi) = 0$ then $L(1, \chi^\sigma) = 0$ for all $\sigma \in \mathrm{Aut}(\mathbb{C})$, whence $h(D)^{-1} \sum_{\varphi \in \Phi} L(1, \chi\varphi) = 0$ by (1.32). Similarly, in the case $W(\chi) = -1$ the Gross-Zagier formula [**27**] implies that if $L'(1, \chi) = 0$ then $h(D)^{-1} \sum_{\varphi \in \Phi} L'(1, \chi\varphi) = 0$. Thus to prove the theorem it suffices to show that $h(D)^{-1} \sum_{\varphi \in \Phi} L(1, \chi\varphi) \neq 0$ if $W(\chi) = 1$ and $h(D)^{-1} \sum_{\varphi \in \Phi} L'(1, \chi\varphi) \neq 0$ if $W(\chi) = -1$. The point of this reduction is that part of the analytic complexity of $L(s, \chi)$ is that as a Dirichlet series it is the sum $\sum \chi(\mathfrak{a})(\mathbf{N}\mathfrak{a})^{-s}$ over all nonzero ideals of $\mathcal{O}$, and in particular over ideals belonging to all ideal classes. By contrast, $h(D)^{-1} \sum_{\varphi \in \Phi} L(s, \chi\varphi)$ is the sum $\sum \chi(\mathfrak{a})(\mathbf{N}\mathfrak{a})^{-s}$ taken over the *principal* ideals, which analytically is a much more tractable object. □

3.2. Gross's $\mathbb{Q}$-curves

The significance of Hecke characters of type $(1, 0)$ is that they correspond to elliptic curves with complex multiplication, and the significance of the Hecke characters $\chi \in X(D)$ is that the corresponding elliptic curves are the canonical examples of Gross's "$\mathbb{Q}$-curves." To make this precise, recall that the modular invariant j can be evaluated not only on elliptic curves but also on lattices in $\mathbb{C}$: in fact if A is an elliptic curve over $\mathbb{C}$ and $\mathcal{L}$ its period lattice relative to a nonzero regular differential then $j(A) = j(\mathcal{L})$. In particular, since we are viewing K as a subfield of $\mathbb{C}$ we may take $\mathcal{L}$ to be $\mathcal{O}$, and then an elliptic curve with invariant $j(\mathcal{O})$ has complex multiplication by $\mathcal{O}$. Putting $F = \mathbb{Q}(j(\mathcal{O}))$ and $H = K(j(\mathcal{O}))$, we see that F is the minimal field of definition for an elliptic curve with invariant $j(\mathcal{O})$ and H the minimal field of defintion for its complex multiplication.

Now if D is odd then the set $X(D)$ picks out a canonical isogeny class of elliptic curves over F with invariant $j(\mathcal{O})$, any member of which will be denoted $A(D)$. Similarly, if $8|D$ then the sets $X^+(D)$ and $X^-(D)$ each pick out such isogeny classes, say with members $A^+(D)$ and $A^-(D)$ respectively. We then have

$$L(s, A(D)) = \prod_{\chi \in X(D)} L(s, \chi) \qquad (D \text{ odd}) \tag{1.33}$$

and

$$L(s, A^\pm(D)) = \prod_{\chi \in X^\pm(D)} L(s, \chi) \qquad (8|D). \tag{1.34}$$

We emphasize that the isogeny classes at issue all contain more than one isomorphism class over F, so that $A(D)$, $A^+(D)$, and $A^-(D)$ have not been specified up to isomorphism. It is possible to do so, at least in the case of $A(p)$ with a prime $p \equiv 3 \bmod 4$ ($p > 3$), by a consideration of minimal discriminants (cf. [**26**], p. 35), but for the validity of (1.33) and (1.34) this refinement is unnecessary: the L-function of an elliptic curve depends only on its isogeny class. Incidentally, if A is any one of $A(D)$, $A^+(D)$, and $A^-(D)$ then the isogeny class of A over H is defined over $\mathbb{Q}$ in the sense that A is isogenous over H to all of its Galois conjugates. This is the reason for the term "$\mathbb{Q}$-curve."

Combining Proposition 1.7 and Theorem 1.2 with (1.33) and (1.34), and applying either Rubin's generalization [**50**] of the Coates-Wiles theorem (if $W(\chi) = 1$) or the Gross-Zagier formula [**27**] and the theorem of Kolyvagin and Logachev [**36**] (if $W(\chi) = -1$), we obtain:

Theorem 1.3. *If D is odd then the rank of $A(D)(F)$ is 0 or $h(D)$ according as D is 7 or 3 modulo 8. If D is divisible by 8 the the rank of $A^+(D)$ over F is 0 and the rank of $A^-(D)$ over F is $h(D)$.*

In the case of a prime $p \equiv 7 \bmod 8$, the fact that $A(p)(F)$ has rank 0 was proved by Gross [**26**] several years before Theorem 1.2 using descent.

3.3. Yang's simplest abelian varieties

While we have seen that $X(D) = \emptyset$ if $4||D$, the exclusion of this case was nonetheless a peculiar anomaly for several years. However Yang [**66**] has shown that the case $4||D$ can be incorporated into the theory if on the geometric side elliptic curves are replaced by abelian varieties and on the arithmetic side the requirement that the values of χ on principal ideals lie in K – condition (c) in the original definition of $X(D)$ – is replaced by conditions (c) and (d) below. Let K be an imaginary quadratic field and D the absolute value of its discriminant. We consider the set $Y(D)$ of primitive Hecke characters υ of K of type (1,0) satisfying the following conditions:

(a) $\mathfrak{f}(\upsilon)|D^\infty$.
(b) $\upsilon(n\mathcal{O}) = \kappa(n)n$ for $n \in \mathbb{Z}$ prime to D.
(c) Let T be the extension of K generated by the values of υ. Then $[T : K]$ is minimal subject to (a) and (b).
(d) Also $\mathbf{N}\mathfrak{f}(\upsilon)$ is minimal subject to (a) and (b).

Suppose once again that $D \neq 3, 4$. Yang associates an isogeny class of abelian varieties over K with complex multiplication by T to the Galois orbit of an element $\upsilon \in Y(D)$, and he shows that these abelian varieties are in a natural sense the "simplest" among all abelian varieties over K with complex multiplication by T. If D is odd or divisible by 8 then $Y(D) = X(D)$, and if we fix a Galois orbit of elements of this set then Yang's abelian variety B is related to Gross's $\mathbb{Q}$-curve A via Weil's restriction-of-scalars functor: $B = \mathrm{res}_{H/K}A$. (In the case where D is a prime congruent to 3 mod 4 this restriction of scalars figured prominently already in [**26**].) But if $4||D$ then B need not be the restriction of scalars of any elliptic curve over H. Nonetheless, Yang proves analogues for of all of the results already mentioned for $X(D)$. The proof of Yang's analogue of Theorem 1.2 is particularly daunting, because one no longer has (1.32): the Galois conjugates of χ are not all of the form $\chi\varphi$ with $\varphi \in \Phi$.

4. An open problem

In a nutshell, the problem is to prove an analogue of Theorem 1.2 with χ replaced by a power of χ. Let w be a positive integer and take χ in $X(D)$. If w is odd then χ^w is still primitive of conductor $\mathfrak{f}(\chi)$, but if w is even then χ^w extends to a Hecke character to the modulus $\mathcal{O}$ and so is no longer primitive. To handle the two cases simultaneously, write χ_w to mean χ^w if w is odd and the primitive Hecke character determined by χ^w if w is even. Then Hecke's functional equation for $L(s, \chi_w)$ is

$$\Lambda(s, \chi_w) = W(\chi_w)\Lambda(w + 1 - s, \chi_w) \tag{1.35}$$

with

$$\Lambda(s, \chi_w) = \begin{cases} (D\mathbf{N}\mathfrak{f}(\chi))^{s/2}\Gamma_{\mathbb{C}}(s)L(s, \chi_w) & \text{if } w \text{ is odd} \\ D^{s/2}\Gamma_{\mathbb{C}}(s)L(s, \chi_w) & \text{if } w \text{ is even.} \end{cases} \tag{1.36}$$

and

$$W(\chi_w) = \begin{cases} (-1)^{(w-1)/2}W(\chi) & \text{if } w \text{ is odd} \\ 1 & \text{if } w \text{ is even.} \end{cases} \tag{1.37}$$

In particular, the center of the critical strip is $(w+1)/2$ and the functional equation relates $L(s, \chi_w)$ to itself. Here is a precise formulation of the problem:

Suppose that w is odd and relatively prime to $h(D)$. Show that

$$\mathrm{ord}_{s=(w+1)/2}L(s, \chi^w) = \begin{cases} 0 & \text{if } W(\chi) = 1, \\ 1 & \text{if } W(\chi) = -1. \end{cases} \tag{1.38}$$

One reason for drawing attention to this problem is that it seems quite accessible. In fact from one point of view the problem is nearly solved: Liu and Xu [**39**] have shown that if one fixes w then (1.38) holds for all but finitely many D. Their result is actually stronger than that, because as in other papers of this sort ([**40**], [**41**],[**47**], and [**67**], for example), the authors prove that (1.38) still holds when $L(s, \chi^w)$ is replaced by $L(s, \chi^w\mu)$ for a primitive quadratic Dirichlet character μ of sufficiently small conductor d relative to D (the precise condition in [**39**] is $d \ll D^{1/12-\varepsilon}$ for any $\varepsilon > 0$; of course D must be sufficiently large). Even granting this refinement, however, the fact remains that (1.38) does not yet seem to be known for *all* D.

It is natural to ask why we have placed restrictions on w and $h(D)$. One possible response is that unless w is assumed odd, the condition on $h(D)$ (about which more in a moment) is satisfied only when D is a prime or $D = 8$. A better response is that if w is odd then the central point $(w + 1)/2$ is an integer, and in fact a critical integer in Deligne's sense. That said, I do not know of any reason to believe that (1.38) is false when w is even.

The condition on $h(D)$, on the other hand, seems to be necessary, because a calculation of Rodriguez Villegas (actually a theorem, given the precision of the calculation and an *a priori* bound on the denominator of the special value) indicates that if $D = 59$ and $w = 3$ then there exists a $\chi \in X(D)$ such that $L(2, \chi^3) = 0$, despite the fact that $W(\chi^3) = 1$ (see [**46**], p. 437, Remark 2). Note that $h(D) = 3$ in this case. Perhaps we should not be surprised, because the fact that the characters $\chi^w\varphi$ with $\varphi \in \Phi$ form a single orbit under $\mathrm{Aut}(\mathbb{C}/K)$ – in other words, equation (1.32) with χ replaced by χ^w – has been a critical ingredient of most work in this area, and if $\gcd(w, h(D)) > 1$ then the characters $\chi^w\varphi$ simply are not all Galois-conjugate. Even so, it would be interesting to relax the condition $\gcd(w, h(D)) > 1$

to the extent possible. A step in this direction has been taken by Masri [**40**], [**41**], who uses the recent bounds of Ellenberg and Venkatesh [**18**] on torsion in ideal class groups to give upper bounds on the number of Galois orbits in $\{\chi^w : \chi \in X(D)\}$. As a result he is able to prove the first nontrivial upper bounds for the number of characters $\chi \in X(D)$ violating (1.38).

5. Evaluation of the quadratic Gauss sum

Although we shall prove more general statements later on, we nonetheless give a self-contained proof of Theorem 1.1. The key is to prove the special case (1.1), for which we use an argument of Schur.

5.1. Schur's proof

Let V be the complex vector space consisting of functions $f : \mathbb{F}_p \to \mathbb{C}$. We define a linear automorphism $f \mapsto \hat{f}$ of V by setting

$$\hat{f}(x) = \sum_{y \in \mathbb{F}_p} f(y) e^{2\pi i x y/p}.$$

That this "Fourier transform" is actually an automorphism of V follows from the identity $\hat{\hat{f}}(x) = pf(-x)$, which in turn is a consequence of the calculation

$$\hat{\hat{f}}(x) = \sum_{y \in \mathbb{F}_p} \hat{f}(y) e^{2\pi i x y/p} = \sum_{z \in \mathbb{F}_p} f(z) \sum_{y \in \mathbb{F}_p} e^{2\pi i (x+z) y/p}$$

(observe that the inner sum is p or 0 according as $z = -x$ or $z \neq x$). Denote the linear automorphism $f \mapsto \hat{f}$ by $\mathcal{F}$ and put $Q = \det \mathcal{F} / |\det \mathcal{F}|$. We shall compute Q in two different ways.

The first way is to use the ordered basis $\delta_0, \delta_1, \ldots, \delta_{p-1}$ for V, where $\delta_j(y) = 1$ if y is j mod p and $\delta_j(y) = 0$ otherwise. The matrix of $\mathcal{F}$ relative to this basis has $e^{2\pi i j k/p}$ as its (j,k) entry, and consequently the determinant of $\mathcal{F}$ is a Vandermonde determinant:

$$\det \mathcal{F} = \prod_{1 \leqslant j < k \leqslant p-1} (e^{2\pi i k/p} - e^{2\pi i j/p}). \tag{1.39}$$

Now the map $(j,k) \mapsto (p-k, p-j)$ is an involution on the set of pairs (j,k) with $1 \leqslant j < k \leqslant p-1$, and the fixed points are precisely the pairs $(j, p-j)$ with $1 \leqslant j \leqslant (p-1)/2$. Furthermore, if (j,k) is not a fixed point then precisely one member of the set $\{(j,k), (p-k, p-j)\}$ has the property that its first coordinate is $< (p-1)/2$. Hence we can rewrite (1.39) in the form

$$\det \mathcal{F} = \prod_{1 \leqslant j < (p-1)/2} \prod_{j < k \leqslant p-1} |e^{2\pi i k/p} - e^{2\pi i j/p}|^2 \cdot \prod_{1 \leqslant j \leqslant (p-1)/2} (e^{-2\pi i j/p} - e^{2\pi i j/p}).$$

It follows that

$$Q = (-i)^{(p-1)/2} \tag{1.40}$$

because $e^{-2\pi i j/p} - e^{2\pi i j/p} = -2i \sin(2\pi j/p)$ and $\sin(2\pi j/p) > 0$ for $1 \leqslant j < p/2$.

On the other hand, we obtain most of a second basis for V from the characters $\chi : \mathbb{F}_p^\times \to \mathbb{C}^\times$ of $\mathbb{F}_p^\times$. If χ is nontrivial then we extend it to a function on $\mathbb{F}_p$ by

setting $\chi(0) = 0$. We also extend the trivial character χ_0 by setting $\chi_0(0) = 1$. Now let

$$\chi_1, \overline{\chi}_1, \chi_2, \overline{\chi}_2, \dots, \chi_{(p-3)/2}, \overline{\chi}_{(p-3)/2} \tag{1.41}$$

be an enumeration of the conjugate pairs of nontrivial nonquadratic characters of $\mathbb{F}_p^\times$. Then

$$\lambda, \delta_0, \chi_0, \chi_1, \overline{\chi}_1, \chi_2, \overline{\chi}_2, \dots, \chi_{(p-3)/2}, \overline{\chi}_{(p-3)/2} \tag{1.42}$$

is an ordered basis for V, and we shall now consider the matrix of $\mathcal{F}$ relative to this basis.

To do so, we first observe that if χ is any nontrivial character of $\mathbb{F}_p^\times$ then

$$\widehat{\chi} = \tau(\chi)\overline{\chi}, \tag{1.43}$$

where $\tau(\chi) = \sum_{x \in \mathbb{F}_p} \chi(x) e^{2\pi i x/p}$ is again the associated Gauss sum. To verify (1.43), we take $x \in \mathbb{F}_p$ and compute $\widehat{\chi}(x)$ from the definition:

$$\widehat{\chi}(x) = \sum_{y \in \mathbb{F}_p} \chi(y) e^{2\pi i x y/p}.$$

If $x = 0$ then the right-hand side is the sum over $y \in \mathbb{F}_p^\times$ of the values $\chi(y)$ of the nontrivial character χ, whence $\hat{\chi}(0) = 0$. Thus $\widehat{\chi}(x) = \tau(\chi)\overline{\chi}(x)$ for $x = 0$. On the other hand, if $x \neq 0$ then in the sum over y we can replace y by yx^{-1}, and we see that $\hat{\chi}(x) = \tau(\chi)\overline{\chi}(x)$ also for $x \neq 0$. This proves (1.43). Since $\hat{\hat{f}}(x) = pf(-x)$ the relation

$$\tau(\chi)\tau(\overline{\chi}) = \chi(-1)p \tag{1.44}$$

is an immediate corollary. We note in passing that if $\chi = \lambda$ then we obtain $\tau(\lambda)^2 = \lambda(-1)p$. Hence as already remarked, the fact that (1.1) holds up to sign is easy.

As a special case of (1.43) we have $\mathcal{F}\lambda = \tau(\lambda)\lambda$, because λ is quadratic. Furthermore $\mathcal{F}\delta_0 = \chi_0$, whence $\mathcal{F}\chi_0 = p\delta_0$ by the relation $\hat{\hat{f}}(x) = pf(-x)$. Thus the matrix of $\mathcal{F}$ relative to the basis (1.42) is block-diagonal: The entry $\tau(\lambda)$ in the upper left-hand corner is followed by the 2×2 block

$$B_0 = \begin{pmatrix} 0 & p \\ 1 & 0 \end{pmatrix}$$

and then by the 2×2 blocks

$$B_j = \begin{pmatrix} 0 & \tau(\chi_j) \\ \tau(\overline{\chi_j}) & 0 \end{pmatrix}$$

for $1 \leqslant j \leqslant (p-3)/2$. Now $\det B_0 = -p$ by inspection while $\det B_j = -\chi_j(-1)p$ for $1 \leqslant j \leqslant (p-3)/2$ by (1.44). As $Q = \det\{/|\det \mathcal{F}|$ we deduce that

$$Q = \frac{\tau(\lambda)}{\sqrt{p}}(-1)^{(p-1)/2} \prod_{j=1}^{(p-3)/2} \chi_j(-1),$$

and comparing this result with (1.40) we obtain

$$\frac{\tau(\lambda)}{\sqrt{p}} = i^{(p-1)/2} \prod_{j=1}^{(p-3)/2} \chi_j(-1).$$

Equivalently,

$$\frac{\tau(\lambda)}{\sqrt{p}} = i^{(p-1)/2}(-1)^{\nu}, \tag{1.45}$$

where ν is the number of odd characters among the χ_j $(1 \leqslant j \leqslant (p-3)/2)$. Since χ is odd if and only if $\overline{\chi}$ is odd, we can also say that ν is half the number of odd characters among the characters listed in (1.41).

If $p \equiv 1 \bmod 4$ then all $(p-1)/2$ odd characters of $\mathbb{F}_p^\times$ occur in (1.41), because neither χ_0 nor λ is odd. Hence $\nu = (p-1)/4$ and the right-hand side of (1.45) is 1. If $p \equiv 3 \bmod 4$ then λ is odd, and consequently only $(p-3)/2$ of the odd characters of $\mathbb{F}_p^\times$ occur in (1.41). Hence $\nu = (p-3)/4$ and the right-hand side of (1.45) is i. This completes Schur's proof of (1.1).

5.2. The general case

Now suppoose that χ is an arbitrary primitive quadratic Dirichlet character, and let N be the conductor of χ. If N is an odd prime then Theorem 1.1 has just been proved, and if $N = 4$ or $N = 8$ then the theorem is easily verified by explicit calculation. Putting these cases aside, and keeping in mind that N is the conductor of a *primitive quadratic* Dirichlet character, we can write $N = N_1N_2$ with coprime integers N_1 and N_2 *which are again the conductors of primitive quadratic Dirichlet characters,* say χ_1 and χ_2 respectively. Note that $\chi = \chi_1\chi_2$. By the Chinese Remainder Theorem, the numbers

$$j = j_1N_2 + j_2N_1 \qquad (0 \leqslant j_1 \leqslant N_1 - 1, \quad 0 \leqslant j_2 \leqslant N_2 - 1) \tag{1.46}$$

represent the distinct residue classes modulo N, and when j is written in this way we have $e^{j/N} = e^{j_1/N_1}e^{j_2/N_2}$, $\chi_1(j) = \chi_1(j_1)\chi_1(N_2)$, and $\chi_2(j) = \chi_2(j_2)\chi_2(N_1)$ Hence inserting (1.46) in (1.2), we obtain

$$\tau(\chi) = \chi_1(N_2)\chi_2(N_1) \cdot \tau(\chi_1)\tau(\chi_2). \tag{1.47}$$

Now divide both sides of (1.47) by $\sqrt{N}\, i^{m(\chi)}$. On applying the law of quadratic reciprocity in the form

$$\chi_1(N_2)\chi_2(N_1) = i^{m(\chi_1\chi_2)-m(\chi_1)-m(\chi_2)}$$

we obtain $W(\chi) = W(\chi_1)W(\chi_2)$. Hence Theorem 1.1 follows by induction on the number of distinct prime factors of N.

6. Exercises

Exercise 1.1. We have observed that the negative even integers are trivial zeros of $\zeta(s)$. Generalize this remark in two directions:

- Determine the trivial zeros of the Dedekind zeta function $\zeta_K(s)$. Your answer will depend on the number of real and complex embeddings of the number field K. (See Theorem 2.1 for the functional equation of $\zeta_K(s)$.)
- Determine the trivial zeros of $L(s, \chi)$ for an arbitrary primitive Dirichlet character χ. Your answer will depend on the parity of χ.

The assumption that χ is primitive is natural when one talks about trivial zeros of $L(s, \chi)$, because imprimitivity perturbs the functional equation. Note however that trivial *central* zeros are unaffected: If χ is an imprimitive Dirichlet character and χ' is the primitive Dirichlet character determined by χ then $L(s, \chi)$ differs from

$L(s, \chi')$ by a factor which does not vanish at $s = 1/2$. On the other hand, what happens at $s = 0$?

Exercise 1.2. Let χ be a primitive Dirichlet character of order $\geqslant 3$. To see that $L(s, \chi)$ does not have a trivial central zero, we argued that the functional equation could have no bearing on $\mathrm{ord}_{s=1/2} L(s, \chi)$ because $\chi \neq \overline{\chi}$ and hence $L(s, \chi) \neq L(s, \overline{\chi})$. Implicit in this argument is a basic analytic fact:

> *If two Dirichlet series $\sum_{n \geqslant 1} a(n) n^{-s}$ and $\sum_{n \geqslant 1} b(n) n^{-s}$ coincide as holomorphic functions in some right half-plane in which they both converge absolutely then $a(n) = b(n)$ for all $n \geqslant 1$.*

Verify this assertion by proving an equivalent statement:

> *If a Dirichlet series $\sum_{n \geqslant 1} a(n) n^{-s}$ is identically 0 in some right half-plane in which the series is absolutely convergent then $a(n) = 0$ for all $n \geqslant 1$.*

Then explain why Proposition 1.7 does imply that $L(s, \chi) = L(s, \overline{\chi})$ for $\chi \in X(D)$, even though in this case $\chi \neq \overline{\chi}$.

Exercise 1.3. Apart from the identities $W(\chi) W(\overline{\chi}) = 1$ and $|W(\chi)| = 1$, which are easily deduced from the basic definitions, we have said nothing at all about $W(\chi)$ when χ is a primitive Dirichlet character of order $\geqslant 3$. The present exercise supplies a few bits of information about this case.

(a) Look up the statement of Stickelberger's theorem (see e. g. [**37**]), which gives a factorization of a Gauss sum of prime conductor as a product of prime ideals in an appropriate cyclotomic field. Deduce that if χ has prime conductor and order $\geqslant 3$ then $W(\chi)$ is not an algebraic integer, and in particular not a root of unity, despite the fact that $|W(\chi^\sigma)| = 1$ for every automorphism σ of $\mathbb{C}$.

(b) On the other hand, suppose that χ is primitive of conductor p^ν with $\nu \geqslant 2$. Prove that in this case $W(\chi)$ is in fact a root of unity. (Hint: Let $n = [(\nu + 1)/2]$. Then $\chi(1 + p^n(x + y)) = \chi(1 + p^n x)\chi(1 + p^n y)$ for $x, y \in \mathbb{Z}/p^{\nu - n}\mathbb{Z}$. Put $G = (\mathbb{Z}/p^\nu \mathbb{Z})^\times$ and let H be the kernel of $(\mathbb{Z}/p^\nu\mathbb{Z})^\times \to (\mathbb{Z}/p^n\mathbb{Z})^\times$. Write (1.2) as a sum over $j \in (\mathbb{Z}/p^\nu\mathbb{Z})^\times$ and then write $j = gh$, where $h \in H$ and g runs over a set of coset representatives for H in G. Then the sum over j becomes a double sum, where the outer sum runs over g and the inner sum over h. Show that the inner sum is 0 for all but one value of g.)

(c) (*Literature search.*) In the case where χ has order 3 or 4, Matthews [**42**], [**43**] expresses $\tau(\chi)$ in terms of values of the Weierstrass $\wp$-function at imaginary quadratic arguments. Furthermore, Heath-Brown and Patterson [**29**] prove the equidistribution (relative to Lebesgue measure on the unit circle) of the numbers $W(\chi)$ as χ runs over primitive Dirichlet characters of order 3 and prime conductor. What is known about possible generalizations of the results of Matthews and of Heath-Brown and Patterson to Dirichlet characters of orders greater than 3 or 4?

Exercise 1.4. (*Literature search.*) While it is widely expected that Dirichlet L-functions do not vanish at $s = 1/2$, the history of this conjecture deserves to be elucidated. Is it correct to say that the first mention of the conjecture (at least in the quadratic case) is in Chowla [**12**]? Soundarajan [**60**] notes that the nonvanishing of $L(1/2, \chi)$ would follow from the conjectured $\mathbb{Q}$-linear independence of the set

$$\{\gamma : L(1/2 + i\gamma, \chi) = 0, \ \ \gamma \geqslant 0\},$$

but what is the history of the latter conjecture?

LECTURE 2

Local formulas

In principle, we could derive the explicit formula for $W(\chi)$ in Proposition 1.5 by calculating directly from formula (45) of Hecke's original paper [**30**]. However Hecke's formula is expressed in terms of "ideal numbers," an extrinsic construction long superseded by the intrinsically defined "ideles" of Chevalley and Weil. Rather than rescue ideal numbers from desuetude, we prefer to emphasize the correspondence between Hecke characters and idele class characters and the use of Tate's local formulas.

1. The idele class group

Let K be a number field. The **ring of adeles** of K is the restricted direct product

$$\mathbb{A} = \prod_v{}' K_v, \tag{2.1}$$

where v runs over the standard set of places of K and K_v is the completion of K at v. If we wish to indicate the dependence of $\mathbb{A}$ on K then we write $\mathbb{A}_K$. The restriction (indicated by the prime) is that an element $x = (x_v)_v$ of the usual direct product belongs to $\mathbb{A}_K$ if and only if $x_v \in \mathcal{O}_v$ for all but finitely many finite v, where $\mathcal{O}_v$ is the ring of integers of K_v. Since K is naturally embedded in each of its completions, we may view it as a subring of $\mathbb{A}$ via the diagonal embedding. In other words, we identify $x \in K$ with the adele $(x_v)_v$ such that $x_v = x$ for all v.

If v in (2.1) runs over the finite places only then the resulting ring $\mathbb{A}_{\text{fin}}$ is called the **ring of finite adeles** of K. Putting $\mathbb{A}_\infty = \prod_{v|\infty} K_v$, we may write the full adele ring $\mathbb{A}$ as the ordinary direct product of its finite and infinite components:

$$\mathbb{A} = \mathbb{A}_{\text{fin}} \times \mathbb{A}_\infty. \tag{2.2}$$

Of course $\mathbb{A}_\infty = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R} \otimes_{\mathbb{Q}} K$, where r_1 and r_2 have their usual meaning.

Next consider the **ring of adelic integers of** K, defined as the direct product

$$\widehat{\mathcal{O}} = \prod_{v \nmid \infty} \mathcal{O}_v \tag{2.3}$$

and viewed as a subring of $\mathbb{A}_{\text{fin}}$. We topologize $\mathbb{A}_{\text{fin}}$ by imposing two requirements:

- $\widehat{\mathcal{O}}$ is open in $\mathbb{A}_{\text{fin}}$, and the relative topology on $\widehat{\mathcal{O}}$ induced by $\mathbb{A}_{\text{fin}}$ is the usual product topology coming from (2.3).
- For each $a \in \mathbb{A}_{\text{fin}}$, the map $x \mapsto a + x$ is a homeomorphism from $\mathbb{A}_{\text{fin}}$ to itself.

One can check that there is a unique topology on $\mathbb{A}_{\text{fin}}$ satisfying these conditions and that with this topology $\mathbb{A}_{\text{fin}}$ becomes a topological ring. The topology on $\mathbb{A}$ is then the direct product topology afforded by (2.2), where $\mathbb{A}_\infty$ has its standard topology as the finite-dimensional real vector space $\mathbb{R} \otimes_{\mathbb{Q}} K$.

The multiplicative group $\mathbb{A}^\times$ of $\mathbb{A}$ is known as the **group of ideles** of K. It too is a restricted direct product:

$$\mathbb{A}^\times = \prod_v{}' K_v, \tag{2.4}$$

but this time the restriction is that an element $x = (x_v)_v$ of the unrestricted direct product belongs to $\mathbb{A}^\times$ if and only if $x_v \in \mathcal{O}_v^\times$ for all but finitely many finite v. The topology on $\mathbb{A}^\times$ is *not* the relative topology from $\mathbb{A}$, but it can nonetheless be defined in a similar way. Indeed consider the multiplicative group of $\widehat{\mathcal{O}}$:

$$\widehat{\mathcal{O}}^\times = \prod_{v\nmid\infty} \mathcal{O}_v^\times. \tag{2.5}$$

The topology on $\mathbb{A}_{\mathrm{fin}}$ is characterized by two properties:

- $\widehat{\mathcal{O}}^\times$ is open in $\mathbb{A}_{\mathrm{fin}}^\times$, and the relative topology on $\widehat{\mathcal{O}}^\times$ induced by $\mathbb{A}_{\mathrm{fin}}^\times$ is the usual product topology coming from (2.5).
- For each $a \in \mathbb{A}_{\mathrm{fin}}^\times$, the map $x \mapsto ax$ is a homeomorphism from $\mathbb{A}_{\mathrm{fin}}^\times$ to itself.

Once again, there is a unique topology on $\mathbb{A}_{\mathrm{fin}}^\times$ satisfying these conditions, and with this topology $\mathbb{A}_{\mathrm{fin}}^\times$ becomes a topological group. To topologize $\mathbb{A}^\times$ we use (2.2) to write

$$\mathbb{A}^\times = \mathbb{A}_{\mathrm{fin}}^\times \times \mathbb{A}_\infty^\times, \tag{2.6}$$

and then we give $\mathbb{A}^\times$ the direct product topology corresponding to (2.6).

While $\mathbb{A}_\infty^\times$ can be identified either with $(\mathbb{R}\otimes_{\mathbb{Q}} K)^\times$ or with $\prod_{v|\infty} K_v^\times$, it will frequently be viewed as the subgroup of $\mathbb{A}^\times$ consisting of ideles $x = (x_v)_v$ such that $x_v = 1$ for $v \nmid \infty$. If $\mathbb{A}_{\mathrm{fin}}^\times$ is similarly identified with the subgroup of $\mathbb{A}^\times$ consisting of ideles $x = (x_v)_v$ such that $x_v = 1$ for $v|\infty$ then (2.6) expresses $\mathbb{A}^\times$ as a direct product of two subgroups. The associated projection functions will be written $x \mapsto x_{\mathrm{fin}}$ and $x \mapsto x_\infty$ respectively, so that $x = x_{\mathrm{fin}}x_\infty$.

Since $K^\times$ is naturally embedded in each of its completions, we may view it as a subgroup of $\mathbb{A}^\times$ via the diagonal embedding, just as K was viewed as a subring of $\mathbb{A}$. Thus an element $x \in K^\times$ is identified with the idele $(x_v)_v$ such that $x_v = x$ for all v. The quotient group $\mathbb{A}^\times/K^\times$ is called the **idele class group** of K.

2. Idele class characters

Let v be a place of K, finite or infinite, and let $p \leqslant \infty$ be the place of $\mathbb{Q}$ below p. We write $|*|_v$ for the absolute value on K_v which extends the standard absolute value $|*|_p$ on $\mathbb{Q}_p$, and we define the **local norm** $||*||_v$ on $K_v^\times$ by setting

$$||*||_v = |*|_v^{[K_v:\mathbb{Q}_p]}. \tag{2.7}$$

For example, if $K_v \cong \mathbb{C}$ then $p = \infty$ and $||*||_v = |*|_v^2$.

If v is finite then a character $\chi_v : K_v^\times \to \mathbb{C}^\times$ is **ramified** or **unramified** according as the restriction $\chi_v|\mathcal{O}_v^\times$ is trivial or nontrivial. Now

$$\mathcal{O}_v^\times = \{x \in K_v : |x|_v = 1\}, \tag{2.8}$$

and while it is unconventional to do so, we can take the right-hand side of (2.8) as the *definition* of the left-hand side even when v is an infinite prime. The point of doing so is that we obtain a seamless extension of the notions *ramified* and

unramified to the infinite places: In all cases, $\mathcal{O}_v^\times$ is a subgroup of $K_v^\times$ (coinciding with $\{\pm 1\}$ if v is real and with the circle group if v is complex), and in all cases we call χ_v ramified or unramified according as $\chi_v|\mathcal{O}_v^\times$ is nontrivial or trivial.

By an **idele class character** of K we mean a continuous homomorphism $\chi : \mathbb{A}^\times \to \mathbb{C}^\times$ which is trivial on the diagonally embedded subgroup $K^\times$. Such a character necessarily factors as a product of local characters,

$$\chi = \prod_v{}' \chi_v, \tag{2.9}$$

and the continuity of χ ensures that χ_v is unramified for all but finitely many v. It is only by virtue of this last property that (2.9) has a meaning, for we interpret (2.9) to mean that if $x = (x_v)_v \in \mathbb{A}^\times$ then $\chi(x) = \prod_v \chi_v(x_v)$, and the product is finite precisely because for all but finitely many finite v we have $x_v \in \mathcal{O}_v^\times$ and $\chi_v|\mathcal{O}_v^\times = 1$. When χ_v is unramified we say that χ is unramified at v.

By definition, an idele class character of K factors through the idele class group $\mathbb{A}^\times/K^\times$, whence the term *idele class character.* We shall often identify idele class characters with characters of $\mathbb{A}^\times/K^\times$.

As an example of an idele class character, consider the **idelic norm**, defined as the product of the local norms:

$$||x|| = \prod_v ||x_v||_v \qquad\qquad (x = (x_v)_v \in \mathbb{A}_K^\times). \tag{2.10}$$

This product is meaningful, because for all but finitely many finite v we have $x_v \in \mathcal{O}_v^\times$ and hence $||x_v||_v = 1$. It is immediately verified that the idelic norm is a continuous character of $\mathbb{A}^\times$, and by the so-called "Product Formula" it is trivial on $K^\times$, hence an idele class character.

2.1. Hecke characters as idele class characters

The L-function of an idele class character χ of K is defined by the formula

$$L(s,\chi) = \prod_{\substack{v \nmid \infty \\ \chi_v \text{ unram}}} (1 - \chi_v(\pi_v) q_v^{-s})^{-1}, \tag{2.11}$$

where the Euler product on the right-hand side runs over the finite places of K at which χ is unramified, q_v being the order of the residue class field of $\mathcal{O}_v$ and $\pi_v \in \mathcal{O}_v$ a uniformizer. The fact that χ_v is unramified means precisely that $\chi_v(\pi_v)$ is independent of the choice of π_v, so the right-hand side of (2.11) is well defined at least as a formal product. But in fact the product converges in some right half-plane and hence defines a holomorphic function there.

This last assertion may sound familiar, because the very same claim was made in connection with the L-function of a Hecke character. This is no coincidence: an idele class character is essentially the same thing as a primitive Hecke character. More precisely, there is a map $\chi \mapsto \chi_{\mathbb{A}}$ from Hecke characters of K to idele class characters of K which is a bijection when restricted to primitive Hecke characters. The map $\chi \mapsto \chi_{\mathbb{A}}$ comes about as follows.

Given a nonzero integral ideal $\mathfrak{f}$ of $\mathcal{O}$, let $\mathbb{A}_\mathfrak{f} \subset \mathbb{A}_{\text{fin}}^\times$ be the subgroup consisting of all elements $x = (x_v)_v \in \mathbb{A}_{\text{fin}}^\times$ such that $x_v \in 1 + \mathfrak{f}\mathcal{O}_v$ whenever $v = v_\mathfrak{p}$ with $\mathfrak{p}|\mathfrak{f}$. By the Artin-Whaples approximation theorem (or simply the Chinese remainder

theorem), we can write

$$\mathbb{A}^\times = K^\times \cdot \mathbb{A}_\mathfrak{f} \cdot (\mathbb{R} \otimes_\mathbb{Q} K)^\times \tag{2.12}$$

with

$$K^\times \cap (\mathbb{A}_\mathfrak{f}(\mathbb{R} \otimes_\mathbb{Q} K)^\times) = K_\mathfrak{f}. \tag{2.13}$$

Suppose now that χ is a Hecke character of K to the modulus $\mathfrak{f}$ and with infinity type χ_∞. Given $x \in \mathbb{A}^\times$, we use (2.12) to write

$$x = \alpha \cdot y \cdot r \tag{2.14}$$

with $\alpha \in K^\times$, $y \in \mathbb{A}_\mathfrak{f}$, and $r \in (\mathbb{R} \otimes_\mathbb{Q} K)^\times$, and we set

$$\chi_\mathbb{A}(x) = \chi(\mathfrak{a}_y)\chi_\infty(r), \tag{2.15}$$

where

$$\mathfrak{a}_y = \prod_{v \nmid \infty} \mathfrak{p}_v^{\mathrm{ord}_v y_v} \tag{2.16}$$

and $\mathfrak{p}_v$ is the prime ideal of $\mathcal{O}_K$ underlying v. The definition of $\mathbb{A}^\times$ as a restricted direct product ensures that $\mathrm{ord}_v y_v = 0$ for all but finitely many v, whence (2.16) is meaningful. As $y \in \mathbb{A}_\mathfrak{f}$ we have $\mathfrak{a}_y \in I(\mathfrak{f})$, and therefore $\chi(\mathfrak{a}_y)$ is defined.

By (2.13), the definition (2.15) is unambiguous provided the right-hand side is trivial whenever $y = \alpha_\mathrm{fin}$ and $r = \alpha_\infty$ for some $\alpha \in K_\mathfrak{f}$. In other words if $\alpha \in K_\mathfrak{f}$ then we must have $\chi(\alpha\mathcal{O}) = \chi_\infty(1 \otimes \alpha)^{-1}$. This is precisely the defining property (1.10) of a Hecke character.

By construction, $\chi_\mathbb{A}$ is trivial on $K^\times$. To see that it is continuous, put

$$\mathcal{O}_\mathfrak{f} = \mathbb{A}_\mathfrak{f} \cap \widehat{\mathcal{O}}^\times. \tag{2.17}$$

If y in (2.14) belongs to $\mathcal{O}_\mathfrak{f}$ then $\mathfrak{a}_y = \mathcal{O}$, whence (2.15) becomes $\chi_\mathbb{A}(x) = \chi_\infty(r)$. Furthermore if x belongs to the open subgroup $\mathcal{O}_\mathfrak{f} \times (\mathbb{R} \otimes_\mathbb{Q} K)^\times$ of $\mathbb{A}^\times$ then necessarily $y = x_\mathrm{fin}$ and $r = x_\infty$ in (2.14), whence the restriction of $\chi_\mathbb{A}$ to this open subgroup is the function $x \mapsto \chi_\infty(x_\infty)$. As χ_∞ is continuous by assumption, the continuity of $\chi_\mathbb{A}$ on all of $\mathbb{A}^\times$ follows from the fact that a group homomorphism is continuous if and only if its restriction to some open subgroup is.

Thus $\chi_\mathbb{A}$ is an idele class character. A review of the construction shows that if $\mathfrak{f}$ had been replaced by an ideal divisible by $\mathfrak{f}$ then $\chi_\mathbb{A}$ would have been unchanged. It follows that $\chi_\mathbb{A}$ depends only on the primitive Hecke character determined by χ. Furthermore, using the notion of "conductor" introduced below, one can verify that every idele class character has the form $\chi_\mathbb{A}$ for a unique primitive χ.

In practice, since χ and $\chi_\mathbb{A}$ can be distinguished by their arguments – ideals and ideles respectively – the subscript on $\chi_\mathbb{A}$ will usually be omitted. For example, (2.15) can be written $\chi(x) = \chi(\mathfrak{a}_y)\chi_\infty(r)$.

2.2. Local components of idele class characters

For some calculations it is useful to be able to go directly from a Hecke character χ written as in Proposition 1.2 to the local components χ_v in (2.9). The following proposition helps us to do so. Let χ be a primitive Hecke character of K of conductor $\mathfrak{f}$ and infinity type χ_∞, and let ε be the character of $(\mathcal{O}/\mathfrak{f})^\times$ such that

$$\chi(\alpha\mathcal{O}) = \varepsilon(\alpha)\chi_\infty^{-1}(1 \otimes \alpha) \tag{2.18}$$

for $\alpha \in K(\mathfrak{f})$. (As in Proposition 1.2, we are viewing ε as a character of $K(\mathfrak{f})$ via the identification $K(\mathfrak{f})/K_{\mathfrak{f}} \cong (\mathcal{O}/\mathfrak{f})^\times$.) By the Chinese remainder theorem we can write

$$(\mathcal{O}/\mathfrak{f})^\times = \prod_{\mathfrak{p}|\mathfrak{f}} (\mathcal{O}/\mathfrak{p}^{n(\mathfrak{p})})^\times, \tag{2.19}$$

where the product runs over the distinct prime ideals dividing $\mathfrak{f}$ and $n(\mathfrak{p})$ is the multiplicity of $\mathfrak{p}$ in $\mathfrak{f}$. There is a corresponding decomposition

$$\varepsilon = \prod_{\mathfrak{p}|\mathfrak{f}} \varepsilon_{\mathfrak{p}}, \tag{2.20}$$

where $\varepsilon_{\mathfrak{p}}$ is a character of $(\mathcal{O}/\mathfrak{p}^{n(\mathfrak{p})})^\times$. If $v = v_{\mathfrak{p}}$ is the place of K corresponding to $\mathfrak{p}$ then we write ε_v for the character of $\mathcal{O}_v^\times$ obtained by composing $\varepsilon_{\mathfrak{p}}$ with the natural map of $\mathcal{O}_v^\times$ onto $(\mathcal{O}/\mathfrak{p}^{n(\mathfrak{p})})^\times$.

Proposition 2.1. *Let $\mathfrak{p}$ be a prime ideal of K and $v = v_{\mathfrak{p}}$ the corresponding finite place. Let $\pi_v \in \mathcal{O}_v$ be a uniformizer.*

- *If $\mathfrak{p} \nmid \mathfrak{f}$ then χ_v is unramified and $\chi_v(\pi_v) = \chi(\mathfrak{p})$.*
- *If $\mathfrak{p}|\mathfrak{f}$ then $\chi_v|\mathcal{O}_v^\times = \varepsilon_v^{-1}$. In particular, χ_v is ramified.*

Furthermore, if $\beta \in \mathcal{O}$ and $\beta\mathcal{O}$ is a power of some prime ideal $\mathfrak{p}$ dividing $\mathfrak{f}$, then

$$\chi_v(\beta) = \chi_\infty^{-1}(\beta) \cdot \prod_{\substack{\mathfrak{q}|\mathfrak{p} \\ \mathfrak{q}\neq\mathfrak{p}}} \varepsilon_{\mathfrak{q}}(\beta),$$

where $\mathfrak{q}$ runs over prime ideals dividing $\mathfrak{f}$ but different from $\mathfrak{p}$.

Proof. Throughout the proof, w denotes an arbitrary place of K. Suppose first that $\mathfrak{p} \nmid \mathfrak{f}$. Given $z \in \mathcal{O}_v^\times$, take $x = (x_w)_w$ to be the idele with $x_v = z$ and $x_w = 1$ for $w \neq v$. Then we may take $\alpha = r = 1$ and $y = x$ in (2.14), whence $\mathfrak{a}_y = \mathcal{O}$. So (2.15) and (2.9) give $\chi_v(z) = \chi(x) = 1$, and we conclude that χ_v is unramified. On the other hand, choosing $x = (x_w)_w$ to be the idele with $x_v = \pi_v$ and $x_w = 1$ for $w \neq v$, we may again take $\alpha = r = 1$ and $y = x$ in (2.14), but this time we get $\mathfrak{a}_y = \mathfrak{p}$ and consequently $\chi_v(\pi_v) = \chi(\mathfrak{p})$.

Next suppose that $\mathfrak{p}|\mathfrak{f}$. Given $z \in \mathcal{O}_v^\times$, take $x = (x_w)_w$ to be the idele with $x_v = z$ and $x_w = 1$ for $w \neq v$. Applying the Chinese remainder theorem and the notation of (2.19), we choose $\alpha \in \mathcal{O}$ so that $\alpha \equiv z \bmod \mathfrak{p}^{n(\mathfrak{p})}\mathcal{O}_v$ and also $\alpha \equiv 1 \bmod \mathfrak{q}^{n(\mathfrak{q})}$, for all prime ideals $\mathfrak{q}$ dividing $\mathfrak{f}$ but different from $\mathfrak{p}$. Then $\alpha_{\mathrm{fin}}^{-1} x \in \mathbb{A}_{\mathfrak{f}}$, so we may take $y = \alpha_{\mathrm{fin}}^{-1} x$ and $r = \alpha_\infty^{-1}$ in (2.14). Then $\mathfrak{a}_y = \alpha^{-1}\mathcal{O}$, and consequently (2.15) gives $\chi(x) = \chi(\alpha^{-1}\mathcal{O})\chi_\infty(1 \otimes \alpha^{-1})$. Replacing α by α^{-1} in (2.18), we deduce that $\chi(x) = \varepsilon^{-1}(\alpha)$. In view of the choice of x and α, we obtain $\chi_v(z) = \varepsilon_v^{-1}(z)$ by (2.9) and (2.20). Thus $\chi_v|\mathcal{O}_v^\times = \varepsilon_v^{-1}$.

Finally, if $\beta\mathcal{O}$ is a power of $\mathfrak{p}$ for some prime ideal $\mathfrak{p}$ dividing $\mathfrak{f}$ then (2.9) gives

$$1 = \prod_{w|\mathfrak{f}\infty} \chi_w(\beta), \tag{2.21}$$

because $\chi|K^\times$ is trivial and χ_w is unramified for $w \nmid \mathfrak{f}\infty$. Now if $\mathfrak{q}$ is a prime ideal dividing $\mathfrak{f}$ and $\mathfrak{q} \neq \mathfrak{p}$ then $\beta \in \mathcal{O}_w^\times$, where w is the place corresponding to $\mathfrak{q}$. Hence we can apply the result of the previous paragraph with $\mathfrak{p}$ replaced by $\mathfrak{q}$, obtaining $\chi_w(\beta) = \varepsilon_{\mathfrak{q}}^{-1}(\beta)$. Inserting this information in (2.21), we obtain the claimed formula for $\chi_v(\beta)$. □

To illustrate both the map $\chi \mapsto \chi_{\mathbb{A}}$ and the use of Proposition 2.1, consider the case where χ is the absolute norm, $\chi(\mathfrak{a}) = \mathbf{N}\mathfrak{a}$. We claim that $\chi_{\mathbb{A}}$ is $||*||^{-1}$, the reciprocal of the idelic norm defined by (2.10). Indeed in the notation of Proposition 1.2 we have $\mathfrak{f} = \mathcal{O}$ and $\varepsilon = 1$, and by taking $s_0 = 1$ in (1.13) we see that χ_∞ is the product of the reciprocals of the local norms at infinity:

$$\chi_\infty(x_v)_{v|\infty} = \prod_{v|\infty} ||*||_v^{-1}. \tag{2.22}$$

On the other hand, if $\mathfrak{p}$ is a prime ideal of K and v the corresponding finite place, then according to Proposition 2.1, χ_v is the unramified character of $K_v^\times$ taking the value $\mathbf{N}\mathfrak{p}$ on any uniforizer π_v. But the local norm is also unramified, and $\mathbf{N}\mathfrak{p} = q_v = ||\pi_v||_v^{-1}$, where q_v is the order of the residue class field of K. Hence $\chi_v = ||*||_v^{-1}$. Taking the product over all finite places and then multiplying by (2.22), we obtain (2.10), whence $\chi_{\mathbb{A}}$ is indeed $||*||^{-1}$.

2.3. The conductor

As pointed out already in the introduction, a complex representation of a profinite group is trivial on an open subgroup. The one-dimensional case of this remark underlies some verifications that have already been passed over without comment, for example the fact that every idele class character is a restricted direct product of local characters (formula (2.9)), or the fact that the map $\chi \mapsto \chi_{\mathbb{A}}$ from Hecke characters to idele class characters is surjective. The relevant profinite groups are $\widehat{\mathcal{O}}$ and $\widehat{\mathcal{O}}^\times$; instead of (2.3) and (2.5) we write

$$\widehat{\mathcal{O}} = \varprojlim_{\mathfrak{f}} \mathcal{O}/\mathfrak{f} \tag{2.23}$$

and

$$\widehat{\mathcal{O}}^\times = \varprojlim_{\mathfrak{f}} (\mathcal{O}/\mathfrak{f})^\times, \tag{2.24}$$

where $\mathfrak{f}$ runs over the nonzero integral ideals of K ordered by divisibility. In particular, we see from (2.24) that the restriction of an idele class character to $\widehat{\mathcal{O}}^\times$ is trivial on $\mathcal{O}_\mathfrak{f}$ for some $\mathfrak{f}$.

The same remark holds locally at every finite place v: If $v = v_\mathfrak{p}$ then

$$\mathcal{O}_v = \varprojlim_n \mathcal{O}/\mathfrak{p}^n \tag{2.25}$$

and

$$\mathcal{O}^\times = \varprojlim_n (\mathcal{O}/\mathfrak{p}^n)^\times, \tag{2.26}$$

and the latter equation shows that a character of $K_v^\times$ is trivial on $1 + \pi_v^n \mathcal{O}_v$ for some $n \geqslant 1$.

These remarks permit us to define the **conductor** of a character both locally and globally. Consider first the local case: If v is a finite place of K and χ_v a character of $K_v^\times$ then the **exponent of the conductor** of χ_v is the integer

$$a(\chi_v) = \begin{cases} 0 & \text{if } \chi_v \text{ is unramified,} \\ \min\{n \geqslant 1 : \chi_v \text{ trivial on } 1 + \pi_v^n \mathcal{O}_v\} & \text{if } \chi_v \text{ is ramified,} \end{cases} \tag{2.27}$$

and the conductor of χ_v is the ideal $\pi_v^{a(\chi_v)}\mathcal{O}_v$ of $\mathcal{O}_v$. Turning now to the global setting, we have two ways of defining the conductor $\mathfrak{f}(\chi)$ of an idele class character χ of K: Either we consider nonzero integral ideals $\mathfrak{f}$ of K such that χ is trivial on

$\mathcal{O}_{\mathfrak{f}}$, and we define $\mathfrak{f}(\chi)$ to be the smallest such $\mathfrak{f}$ (in terms of divisibility), or else we set

$$\mathfrak{f}(\chi) = \prod_{v \nmid \infty} \mathfrak{p}_v^{a(\chi_v)} \tag{2.28}$$

(recall that $\mathfrak{p}_v$ is the prime ideal determined by v). One verifies that these two definitions are equivalent to each other and also to our original definition of the conductor of a primitive Hecke character when χ is viewed as such.

3. The functional equation

Our goal now is to see how the idelic viewpoint facilitates the statement of the functional equation for Hecke L-functions. The key point is that once we think of an idele class character χ as a product of local characters using (2.9) we can define the objects appearing in the functional equation of $L(s,\chi)$ as products of local objects also. In the case of the conductor $\mathfrak{f}(\chi)$ we have already taken this step in (2.27) and (2.28), although the benefit gained may not yet be apparent. The real prize we anticipate is a factorization of the root number $W(\chi)$. But first we consider the factorization of $L(s,\chi)$ itself as a product of local L-factors.

3.1. L-factors

It may appear appear at first that there is nothing new here. Given a finite place v of K and a character χ_v of $K_v^\times$, we set

$$L(s,\chi_v) = \begin{cases} (1-\chi_v(\pi_v)q_v^{-s})^{-1} & \text{if } \chi_v \text{ is unramified} \\ 1 & \text{if } \chi_v \text{ is ramified,} \end{cases} \tag{2.29}$$

where as before, π_v is a uniformizer and q_v the order of the residue class field of $\mathcal{O}_v$. As we have already noted, the fact that χ_v is unramified means precisely that χ_v is independent of the choice of π_v. Now if χ is an idele class character of K then a comparison of (2.11) and (2.29) shows that the global L-function $L(s,\chi)$ is the product of the local L-factors:

$$L(s,\chi) = \prod_{v \nmid \infty} L(s,\chi_v). \tag{2.30}$$

Furthermore, if we think of χ as a primitive Hecke character then one can verify that the original definition (1.18) of $L(s,\chi)$ is equivalent to (2.11) and (2.30). (The key point is that if v is a finite place where χ is unramified and x in (2.14) is the idele with π_v at the place v and 1 at all other places then we can take $\alpha = r = 1$ and $y = x$, whence $\mathfrak{a}_y = \mathfrak{p}_v$.) So our definitions are compatible, but the introduction of local L-factors appears to add nothing new.

However from the adelic point of view it is natural to associate L-factors not only to the finite places of K but also to the infinite places, where the "L-factors" turn out to be the gamma factors in the functional equation. In fact what we have been calling $L(s,\chi)$ would in some contexts be regarded as merely "the finite part of the L-function," $L_{\mathrm{fin}}(s,\chi)$, and the notation $L(s,\chi)$ would be reserved for the "completed L-function" $L_\infty(s,\chi)L_{\mathrm{fin}}(s,\chi)$, where $L_\infty(s,\chi)$ is the product of the L-factors at the infinite places:

$$L_\infty(s,\chi) = \prod_{v \mid \infty} L(s,\chi_v). \tag{2.31}$$

Hence the completed L-function $L_\infty(s,\chi)L_{\mathrm{fin}}(s,\chi)$ is the product of the L-factors $L(s,\chi_v)$ over *all* the places of K and includes both the traditional L-function $L_{\mathrm{fin}}(s,\chi)$ and its gamma factors.

In practice we will continue to write $L(s,\chi)$ for the traditional L-function $L_{\mathrm{fin}}(s,\chi)$, but the factorization (2.31) will be used in the statement of the functional equation of $L(s,\chi)$. Hence we need to make the local factors in (2.31) explicit.

Suppose first that v is a real place. Then $K_v \cong \mathbb{R}$, and the identification is unique because $\mathbb{R}$ has no nontrivial automorphisms (even as an abstract field). Thus a character χ_v of $K_v^\times$ can be identified with a character of $\mathbb{R}^\times$. But a character of $\mathbb{R}^\times$ is necessarily of the form $t \mapsto |t|^{s_0}(t/|t|)^m$ with unique numbers $s_0 \in \mathbb{C}$ and $m \in \{0,1\}$. We set

$$L(s,\chi_v) = \Gamma_{\mathbb{R}}(s+s_0+m), \tag{2.32}$$

where we recall that the real gamma factor $\Gamma_{\mathbb{R}}(s)$ is defined by (1.7).

Next suppose that v is complex. Then there are two possible identifications $K_v \cong \mathbb{C}$. Choosing one of them, we may view a character χ_v of $K_v^\times$ as a character of $\mathbb{C}^\times$. Then χ_v is necessarily of the form $z \mapsto |z|^{2s_0}(z/|z|)^m$ with unique numbers $s_0 \in \mathbb{C}$ and $m \in \mathbb{Z}$. We set

$$L(s,\chi_v) = \Gamma_{\mathbb{C}}(s+s_0+|m|/2), \tag{2.33}$$

If we replace our chosen identification of K_v with $\mathbb{C}$ with the complex-conjugate identification then $\chi_v(z)$ is replaced by $\chi_v(\overline{z})$ and hence m by $-m$; but (2.33) stays the same. Thus $L(s,\chi_v)$ is well defined.

3.2. Statement of the functional equation

Given an idele class character χ of K, put

$$\Lambda(s,\chi) = D_K^{s/2}(\mathbf{N}\mathfrak{f}(\chi))^{s/2}L_\infty(s,\chi)L(s,\chi), \tag{2.34}$$

where D_K is the absolute value of the discriminant of K and $L_\infty(s,\chi)$ and $L(s,\chi)$ are as in (2.31) and (2.30) respectively. Let c be as in Proposition 1.1, and put

$$\begin{cases} w = 2c \\ k = 2c+1, \end{cases} \tag{2.35}$$

so that $k = w+1$.

Theorem 2.1. *There is a constant $W(\chi) \in \mathbb{C}$ with $|W(\chi)| = 1$ such that*

$$\Lambda(s,\chi) = W(\chi)\Lambda(k-s,\overline{\chi}). \tag{2.36}$$

Furthermore, if χ is the trivial character then $W(\chi) = 1$.

Of course if χ is the trivial character then $L(s,\chi)$ is just the Dedekind zeta function $\zeta_K(s)$ of K, and we will usually write $\Lambda(s,\chi)$ as $Z_K(s)$ in this case. If $K = \mathbb{Q}$ then we will continue to write $\zeta_{\mathbb{Q}}(s)$ and $Z_{\mathbb{Q}}(s)$ simply as $\zeta(s)$ and $Z(s)$, as we did in Lecture 1.

4. Quadratic root numbers

Before saying even one word about local root numbers, we can deduce from Theorem 2.1 that root numbers of quadratic idele class characters are trivial:

Theorem 2.2. *Suppose that χ is an idele class character of K such that χ^2 is trivial. Then $W(\chi) = 1$.*

When χ is the trivial character Theorem 2.2 is already contained in Theorem 2.1, so we may assume that χ is in fact quadratic. Under this assumption the main input beyond Theorem 2.1 that is needed for the proof of Theorem 2.2 is the identity

$$\zeta_L(s) = \zeta_K(s)L(s, \mathrm{sign}_{L/K}), \tag{2.37}$$

where L/K is a quadratic extension of number fields and $\mathrm{sign}_{L/K}$ is **the quadratic Hecke character associated to** L/K. The meaning of this last phrase is as follows. Let $\mathfrak{d}_{L/K}$ be the relative discriminant ideal of L/K. Then $\mathrm{sign}_{L/K} : I(\mathfrak{d}_{L/K}) \to \{\pm 1\}$ is the unique homomorphism satisfying

$$\mathrm{sign}_{L/K}(\mathfrak{p}) = \begin{cases} 1 & \text{if } \mathfrak{p} \text{ splits in } L \\ -1 & \text{if } \mathfrak{p} \text{ remains prime in } L \end{cases} \tag{2.38}$$

for prime ideals $\mathfrak{p}$ of K unramified in L. The fact that the homomomorphism defined by (2.38) is actually a Hecke character (indeed a primitive Hecke character of conductor $\mathfrak{d}_{L/K}$) is essentially quadratic reciprocity over number fields, although a little bit of work is required to go back and forth between this statement and the classical version found for example in [**31**], p. 246. In any case, to prove Theorem 2.2 we combine (2.37) with the fact that any quadratic idele class character χ of K has the form $\chi = \mathrm{sign}_{L/K}$ for some quadratic extension L of K. In other words, given a nontrivial χ as in Theorem 2.2 we use (2.37) by writing

$$\zeta_L(s) = \zeta_K(s)L(s, \chi), \tag{2.39}$$

where the quadratic extension L of K being determined by χ.

We claim that (2.39) remains valid when $\zeta_L(s)$, $\zeta_K(s)$, and $L(s, \chi)$ are replaced by their normalized versions:

$$Z_L(s) = Z_K(s)\Lambda(s, \chi). \tag{2.40}$$

To verify (2.40), write $r_{1/1}(L/K)$ for the number of real places of K which split into two real places of L and $r_{2/1}(L/K)$ for the number of real places of K which ramify into a complex place of L. Since every real place of K either splits or ramifies, the number of such places satisfies

$$r_1(K) = r_{1/1}(L/K) + r_{2/1}(L/K). \tag{2.41}$$

Also

$$\begin{cases} r_1(L) = 2r_{1/1}(L/K) \\ r_2(Y) = 2r_2(K) + r_{2/1}(L/K), \end{cases} \tag{2.42}$$

because every place of L is an extension of a unique place of K. Now $\zeta_L(s)$ and $\zeta_K(s)$ are the L-functions of the trivial idele class character of L and K respectively. Hence in applying (2.31) and (2.34) we take $s_0 = m = 0$ in (2.32) and (2.33), obtaining

$$Z_L(s) = D_L^{s/2}\Gamma_{\mathbb{R}}(s)^{r_1(L)}\Gamma_{\mathbb{C}}(s)^{r_2(L)}\zeta_L(s). \tag{2.43}$$

and

$$Z_K(s) = D_K^{s/2}\Gamma_{\mathbb{R}}(s)^{r_1(K)}\Gamma_{\mathbb{C}}(s)^{r_2(K)}\zeta_K(s). \tag{2.44}$$

As for $\Lambda(s, \chi)$, the relation $\chi = (\mathrm{sign}_{L/K})_{\mathbb{A}}$ has the following consequences: If v is a complex place of K then $(s_0, \nu) = (0, 0)$ in (2.33), while if v is a real place then

$(s_0, \nu) = (0, 0)$ or $(s_0, \nu) = (0, 1)$ in (2.32) according as v splits or ramifies in K. As $\mathfrak{f}(\chi) = \mathfrak{d}_{L/K}$, we see that (2.34) gives

$$\Lambda(s, \chi) = (D_{L/K} D_K)^{s/2} \Gamma_{\mathbb{R}}(s)^{r_{1/1}(F)} \Gamma_{\mathbb{R}}(s+1)^{r_{2/1}(F)} \Gamma_{\mathbb{C}}(s)^{r_2(F)} L(s, \chi), \tag{2.45}$$

where $D_{L/K}$ is the absolute norm of the relative different ideal of L/K and hence also the absolute norm of $\mathfrak{d}_{L/K}$. Now compare the product (2.44) and (2.45) with (2.44). Taking account of (2.41) and (2.42) as well as the duplication formula (1.9) and the standard relation $D_L = D_{L/K} D_K^2$, we obtain (2.40).

To deduce Theorem 2.2,we simply insert Theorem 2.1 in (2.40), obtaining

$$Z_K(1-s) = Z_F(1-s) W(\chi) \Lambda(1-s, \chi). \tag{2.46}$$

Replacing s by $1 - s$ in (2.40) and comparing the result with (2.46), we conclude that $W(\chi) = 1$.

5. Local root numbers

Let K be a number field and χ an idele class character of K. As we have already hinted, the root number $W(\chi)$ defined by Theorem 2.1 has a factorization

$$W(\chi) = \prod_v W(\chi_v), \tag{2.47}$$

where $W(\chi_v)$ is the **local root number** attached to χ_v and is equal to 1 for all but finitely many places v. We shall give formulas for $W(\chi_v)$ and then illustrate their use by verifying Proposition 1.5. Initially our approach is that of a cookbook rather than a mathematical treatise. Afterwards we shall fill in a number of points: the implicit dependence of the local root number on a choice of additive character, the connection with epsilon factors, and so on.

5.1. Formulas for local root numbers

We change notation, writing K_v and χ_v simply as K and χ respectively. Thus K is a finite extension of $\mathbb{Q}_p$ for some fixed $p \leqslant \infty$ and χ is a character of $K^\times$. An important point about root numbers is that they see only the unitary part of a character. In other words, if we put $\chi_{\mathrm{u}} = \chi/|\chi|$ as before then

$$W(\chi) = W(\chi_{\mathrm{u}}). \tag{2.48}$$

Hence when it is convenient to do so we may assume that χ is unitary.

If K is archimedean then there is no need to do so. Indeed if $K = \mathbb{R}$ and χ is the map $t \mapsto |t|^{s_0}(t/|t|)^m$ with $s_0 \in \mathbb{C}$ and $m \in \{0, 1\}$ then

$$W(\chi) = i^{-m}. \tag{2.49}$$

If χ is unitary then $s_0 \in i\mathbb{R}$, but formula (2.49) is valid for any s_0. Similarly, if $K \cong \mathbb{C}$ and χ is the map $z \mapsto |z|^{2s_0}(z/|z|)^m$ with $s_0 \in \mathbb{C}$ and $m \in \mathbb{Z}$ then

$$W(\chi) = i^{-|m|}. \tag{2.50}$$

As with (2.33), this formula is independent of the identification $K \cong \mathbb{C}$, and while $s_0 \in i\mathbb{R}$ if χ is unitary, formula (2.50) is valid for any s_0.

We turn now to the nonarchimedean case. Here it would be a slight convenience to assume that χ is unitary, but instead we shall replace χ by χ_{u} in the formulas themselves, so that the formulas are universally valid. As before, we write $a(\chi)$ for the exponent of the conductor of χ. Furthermore, we write n for the **exponent of**

the different ideal of K over $\mathbb{Q}_p$. Thus if π is a uniformizer of K then $\pi^n\mathcal{O}$ is the different ideal of K over $\mathbb{Q}_p$.

When χ is unramified we have

$$W(\chi) = \chi_{\mathrm{u}}(\pi^n). \tag{2.51}$$

In particular, if K is unramified over $\mathbb{Q}_p$ and χ is an unramified character then (2.51) gives

$$W(\chi) = 1. \tag{2.52}$$

To appreciate (2.52), let us return for a moment to the global setting and write K for a number field and K_v for its completion at the finite place v corresponding to a prime ideal $\mathfrak{p}$ of K. In this notation (2.52) asserts that if $\mathfrak{D}$ is the different ideal of K and $\mathfrak{p} \nmid \mathfrak{D}\mathfrak{f}(\chi)$ then

$$W(\chi_v) = 1. \tag{2.53}$$

Since the condition $\mathfrak{p} \nmid \mathfrak{D}\mathfrak{f}(\chi)$ is satisfied by all but finitely many $\mathfrak{p}$, we conclude that the product in (2.47) has only finitely many factors different from 1, as claimed.

Finally, if χ is ramified choose $\beta \in K^\times$ so that

$$v(\beta) = a(\chi) + n, \tag{2.54}$$

where v is the valuation on K. Then

$$W(\chi) = q^{-a(\chi)/2} \sum_{x \in (\mathcal{O}/\mathfrak{f}(\chi))^\times} \chi_{\mathrm{u}}^{-1}(x/\beta) e^{2\pi i \,\mathrm{tr}_{K/\mathbb{Q}_p}(x/\beta)}, \tag{2.55}$$

with $\mathfrak{f}(\chi) = \pi^{a(\chi)}\mathcal{O}$ and q the order of the residue class field of K. Although the appearance of the expression x/β inside both χ_{u}^{-1} and the exponential is a good mnemonic device, it is sometimes more practical to separate these two terms:

$$W(\chi) = \chi_{\mathrm{u}}(\beta) \cdot q^{-a(\chi)/2} \sum_{x \in (\mathcal{O}/\mathfrak{f}(\chi))^\times} \chi^{-1}(x) e^{2\pi i \,\mathrm{tr}_{K/\mathbb{Q}_p}(x/\beta)}, \tag{2.56}$$

Note that we have not bothered to write $\chi^{-1}(x)$ as $\chi_{\mathrm{u}}^{-1}(x)$, because the restriction of any character of $K_v^\times$ to $\mathcal{O}_v^\times$ has finite order and is therefore automatically unitary.

5.2. An example

We illustrate these formulas by proving Proposition 1.5, or in other words by computing $W(\chi)$ for $\chi \in X(D)$ with D odd. Thus K is now $\mathbb{Q}(\sqrt{-D})$. By Proposition 1.4, the different ideal $\mathfrak{D} = \sqrt{-D}\mathcal{O}$ coincides with the conductor $\mathfrak{f}(\chi)$, whence (2.53) gives $W(\chi_v) = 1$ for all finite places $v \nmid D$. And since $\chi_\infty(z) = z^{-1}$ we have $W(\chi_\infty) = i^{-1}$ (take $s_0 = -1/2$ and $m = -1$ in (2.50)). Thus (2.47) gives

$$W(\chi) = i^{-1} \prod_{v|D} W(\chi_v), \tag{2.57}$$

and it remains to evaluate $W(\chi_v)$ for $v|D$.

Suppose then that $v = v_{\mathfrak{p}}$ for a prime ideal $\mathfrak{p}$ dividing D. Then χ_v is ramified, so the appropriate local formula is (2.55). Since $n_v = a(\chi_v) = 1$ we may take the quantity β in (2.55) to be the rational prime p below $\mathfrak{p}$. Note also that since the natural map $(\mathbb{Z}/D\mathbb{Z})^\times \to (\mathcal{O}/\sqrt{-D}\mathcal{O})^\times$ is an isomorphism, the coset representatives

x in (2.55) may be taken to be rational integers. So (2.55) becomes

$$W(\chi_v) = (\chi_v)_{\mathrm{u}}(p) \cdot p^{-1/2} \sum_{n \in (\mathbb{Z}/p\mathbb{Z})^\times} \chi_v^{-1}(n) e^{2\pi i (2n/p)}. \tag{2.58}$$

Now recall condition (b) in the original definition of $X(D)$: $\chi(n\mathcal{O}) = \kappa(n)n$ for $n \in \mathbb{Z}$ prime to D. Here κ is the Kronecker symbol with numerator $-D$, as before. It follows that if $\chi | P(\mathfrak{f}(\chi))$ is written as in Proposition 1.2 then $\varepsilon(n) = \kappa(n)$. Thus in the notation of Proposition 2.1, we have $\varepsilon_v(n) = \lambda(n)$ for n prime to p, where λ is the Legendre symbol at p. Consequently the proposition just cited gives $\chi_v^{-1}(n) = \lambda(n)$ for such n. Making this substitution in (2.58), and replacing the summation over n by a summation over $\overline{2}n$, where $\overline{2}$ is a representative for the multiplicative inverse of 2 in $(\mathbb{Z}/p\mathbb{Z})^\times$, we find

$$W(\chi_v) = \lambda(\overline{2})(\chi_v)_{\mathrm{u}}(p) \cdot p^{-1/2} \sum_{n \in (\mathbb{Z}/p\mathbb{Z})^\times} \lambda(n) e^{2\pi i (2n/p)}. \tag{2.59}$$

Of course $\lambda(\overline{2}) = \lambda(2)$ since λ is quadratic. Furthermore, by taking $\beta = p$ in Proposition 2.1 we obtain

$$\chi_v(p) = p \prod_{\substack{q | D \\ q \neq p}} \left(\frac{p}{q} \right), \tag{2.60}$$

and the factor of p on the right-hand side disappears when χ_v is replaced by $(\chi_v)_{\mathrm{u}}$ on the left-hand side. Finally, the sum in (2.59) is evaluated by Gauss's formula (1.1). Thus (2.59) becomes

$$W(\chi_v) = i^\delta \left(\frac{2}{p} \right) \prod_{\substack{q | D \\ q \neq p}} \left(\frac{p}{q} \right) \tag{2.61}$$

with δ equal to 0 or 1 according as p is 1 mod 4 or 3 mod 4.

The rest is bookkeeping. Let t be the number of prime divisors of D which are congruent to 3 mod 4. Substituting (2.61) in (2.57), we get

$$W(\chi) = i^{t-1} \left(\frac{2}{D} \right) \prod_{p \neq q} \left(\frac{p}{q} \right), \tag{2.62}$$

where the product on the right-hand side of (2.62) runs over pairs (p, q) of distinct prime divisors of D. By quadratic reciprocity, this product is $(-1)^{t(t-1)/2}$. On the other hand, the odd integer $-D$ is a discriminant, hence congruent to 1 mod 4. Therefore t is odd, and we can write $i^{t-1} = (-1)^{(t-1)/2}$. Multiplying this factor by the factor $(-1)^{t(t-1)/2}$ coming from quadratic reciprocity, we obtain $(-1)^{(t^2-1)/2}$, which is 1. Thus (2.62) gives the result stated in Proposition 1.5.

6. An open problem

The preceding example illustrates a simple point: Armed with the formulas (2.47) through (2.55), we can in principle detect trivial central zeros of Hecke L-functions whenever they exist. But do we always care? Does the vanishing at the center of a Hecke L-function, or indeed of any L-function, always have arithmetic significance? Certainly the conjecture of Birch and Swinnerton-Dyer attaches a meaning to examples like the one just considered, but consider instead the L-functions associated to Maass forms for $\mathrm{SL}(2, \mathbb{Z})$. A theorem of Venkov [**64**] implies that half of these

L-functions have a trivial central zero. What is the arithmetic significance of this fact, if any?

The L-functions associated to Maass forms for $\mathrm{SL}(2,\mathbb{Z})$ lie outside the scope of these lectures, but a satisfactory substitute is available, namely Hecke L-functions which are of "Maass type" in the sense that they coincide with the L-functions associated to certain Maass forms for congruence subgroups of $\mathrm{SL}(2,\mathbb{Z})$. Let K be a real quadratic field, viewed as a subfield of $\mathbb{R}$, and write $\alpha \mapsto \alpha'$ for the nonidentity embedding of K in $\mathbb{R}$. We will call a primitive Hecke character χ of K **equivariant** if $\chi(\mathfrak{a}') = \overline{\chi(\mathfrak{a})}$ for $\mathfrak{a} \in I(\mathfrak{f}(\chi))$. The Hecke characters of Maass type to be considered here have the form $\chi = \eta\chi_0$, where η is an equivariant primitive Hecke character of K of finite order and $\chi_0 : I \to \mathbb{C}^\times$ is a fixed Hecke character of K constructed as follows: Writing ε_0 for the fundamental unit of K, we define χ_0 on P by the formula

$$\chi_0(\alpha\mathcal{O}) = |\alpha/\alpha'|^{\pi i/\log\varepsilon_0} \qquad (\alpha \in K^\times), \tag{2.63}$$

and then we extend χ_0 arbitrarily to I. It is not hard to verify that (2.63) gives a well-defined function of principal ideals, that any extension of (2.63) to I is an equivariant Hecke character, and finally (using Theorem 2.1) that the L-function of the resulting equivariant Hecke character $\chi = \eta\chi_0$ satisfies the functional equation

$$\Lambda(s,\chi) = W(\eta)\Lambda(1-s,\chi) \tag{2.64}$$

with

$$\Lambda(s,\chi) = (D\mathbf{N}\mathfrak{f}(\eta))^{s/2}\Gamma_{\mathbb{R}}(s+\pi i/\log\varepsilon_0)\Gamma_{\mathbb{R}}(s-\pi i/\log\varepsilon_0)L(s,\chi), \tag{2.65}$$

where D is the discriminant of K. The appearance of $W(\eta)$ in place of $W(\chi)$ in (2.64) is not a misprint: one can show that $W(\chi) = W(\eta)$. In view of (2.64), we can ask the following question:

> *Suppose that $W(\eta) = -1$. Does the resulting trivial central zero of $L(s,\chi)$ have any arithmetic significance?*

An example where the hypothesis $W(\eta) = -1$ is satisfied will be given below. Historically, the first examples over any number field of a Hecke character η for which $L(s,\eta) = L(s,\overline{\eta})$ and $W(\eta) = -1$ were given by Armitage [**2**] and Serre (unpublished) around 1972. At the time there was no arithmetic interpretation for such trivial central zeros, but in the case of certain quartic Hecke characters of real quadratic fields, Fröhlich [**21**] found a connection with Galois module structure: The quartic charcters η considered by Fröhlich correspond to Galois extensions N of $\mathbb{Q}$ with Galois group the quaternion group of order 8, and Fröhlich proved that $W(\eta)$ is 1 or -1 according as $\mathcal{O}_N$ is or is not a free $\mathbb{Z}[\mathrm{Gal}(N/\mathbb{Q})]$-module. Since then a vast literature has developed relating root numbers to Galois module structure; see for example [**9**], [**10**], [**11**], and [**63**]. This snippet of history should caution us against dismissing the above question too cavalierly.

Returning to the matter at hand, we need an example of a real quadratic field K and an equivariant Hecke character η of K with $W(\eta) = -1$. Take $K = \mathbb{Q}(\sqrt{p(p+4)})$ with a prime $p > 5$ satisfying $p \equiv 1 \bmod 4$, and let D be the discriminant of K. Then $D = pr$, where $p+4 = rm^2$ with r square-free and $m \in \mathbb{Z}$. Let κ be the primitive quadratic Dirichlet character of conductor D given by

$$\kappa(n) = \left(\frac{n}{D}\right), \tag{2.66}$$

and define $\varepsilon : (\mathcal{O}/\sqrt{D}\mathcal{O})^\times \to \{\pm 1\}$ by composing κ (viewed as a character of $(\mathbb{Z}/D\mathbb{Z})^\times$) with the canonical identification $(\mathcal{O}/\sqrt{D}\mathcal{O})^\times \cong (\mathbb{Z}/D\mathbb{Z})^\times$. We claim that ε is trivial on the image of $\mathcal{O}^\times$ in $(\mathcal{O}/\sqrt{D}\mathcal{O})^\times$. In view of (2.66) we have at least $\varepsilon(-1) = \kappa(-1) = 1$, because $D = p(p+4)/m^2$ and so $D \equiv 1 \bmod 4$. On the other hand, put $u = ((p+2) + \sqrt{p(p+4)})/2$. According to Katayama [**35**], u is the fundamental unit of K, so we must verify that $\varepsilon(u) = 1$ also.

To see this, write $(\mathbb{Z}/D\mathbb{Z})^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/r\mathbb{Z})^\times$, and let $\kappa = \kappa'\kappa''$ be the corresponding decomposition of κ into primitive quadratic characters of conductors p and r respectively. Also put $\mathfrak{f} = \sqrt{D}\mathcal{O}$ and let $\mathfrak{p}$ and $\mathfrak{r}$ be respectively the prime ideal of K over p and the product of the prime ideals dividing r. Then $(\mathcal{O}/\mathfrak{f})^\times \cong (\mathcal{O}/\mathfrak{p})^\times \times (\mathcal{O}/\mathfrak{r})^\times$ and we have a corresponding decomposition of characters $\varepsilon = \varepsilon'\varepsilon''$. Recalling that $u = ((p+2) + \sqrt{p(p+4)})/2$ and $p + 4 = rm^2$, we see that $u \equiv 1 \bmod \mathfrak{p}$ and $u \equiv -1 \bmod \mathfrak{r}$, whence $\varepsilon(u) = \varepsilon'(1)\varepsilon''(-1) = \kappa''(-1)$. But $\kappa''(-1) = 1$ because $r \equiv 1 \bmod 4$, so ε is trivial on $\mathcal{O}^\times$, as claimed.

It follows that we obtain a well-defined character η of $P(\mathfrak{f})$ by setting

$$\eta(\alpha\mathcal{O}) = \varepsilon(\alpha) \qquad (\alpha \in K(\mathfrak{f})), \tag{2.67}$$

where α is viewed as a character of $K(\mathfrak{f})$ as in Proposition 1.2. Extending η arbitrarily to $I(\mathfrak{f})$ we obtain a primitive Hecke character which we also denote η and which is readily verified to be equivariant. A calculation shows that

$$W(\eta) = \left(\frac{2}{D}\right). \tag{2.68}$$

But $D = p(p+4)/m^2$ and in particular $D \equiv 5 \bmod 8$, so $W(\eta) = -1$.

7. Epsilon factors

Even a brief perusal of the literature on root numbers will reveal that our discussion has so far neglected two basic issues: the dependence of the local root number on an "additive character" and the relation between root numbers and "epsilon factors." Rectifying these omissions is a first step toward proving Theorem 2.1 with $W(\chi)$ given by formulas (2.47) through (2.55).

7.1. Additive characters

Let K be a finite extension of $\mathbb{Q}_p$ with $p \leqslant \infty$. By an **additive character** of K we mean a nontrivial unitary character $\psi : K \to \mathbb{C}^\times$. A canonical choice, call it ψ^{can}, is possible here. If $p = \infty$ then

$$\psi^{\mathrm{can}}(x) = e^{-2\pi i \operatorname{tr}_{K/\mathbb{R}}(x)}. \tag{2.69}$$

If $p < \infty$ then

$$\psi^{\mathrm{can}}(x) = e^{2\pi i \{\operatorname{tr}_{K/\mathbb{Q}_p}(x)\}_p}, \tag{2.70}$$

where $\{z\}_p$ is the p-adic principal part of a number $z \in \mathbb{Q}_p$ (in other words, if $z = \sum_{n\in\mathbb{Z}} a_n p^n$ with $a_n \in \{0, 1, \dots, p-1\}$ for all n and $a_n = 0$ for $n \ll 0$ then $\{z\}_p = \sum_{n<0} a_n p^n$). Note that (2.69) can also be written

$$\psi^{\mathrm{can}}(x) = e^{-2\pi i \{\operatorname{tr}_{K/\mathbb{R}}(x)\}_\infty}, \tag{2.71}$$

where $\{t\}_\infty$ is the fractional part of a real number t (thus $0 \leqslant \{t\}_\infty < 1$ and $t \equiv \{t\} \bmod \mathbb{Z}$).

Next let χ be a chharacter of $K^\times$. Our $W(\chi)$ coincides with the $W(\chi, \psi^{\mathrm{can}})$ found in the literature. In general, for any additive character ψ of K there is an intrinsically defined local root number $W(\chi, \psi)$, but it is also easily expressed in terms of $W(\chi)$. In fact any such ψ has the form $\psi(x) = \psi(ax)$ for some $a \in K^\times$, and then $W(\chi, \psi) = \chi(a)W(\psi)$. It follows that

$$W(\chi, \psi_b) = \frac{\chi(b)}{|\chi(b)|} W(\chi, \psi) \tag{2.72}$$

for any $b \in K^\times$, where the additive character ψ_b is defined by $\psi_b(x) = \psi(bx)$.

Now we change notation. Let K be a number field and $\mathbb{A}$ its ring of adeles. A **global additive character** of K is a nontrivial unitary character ψ of $\mathbb{A}$ which is trivial on K. Such a character has the form

$$\psi(x) = \prod_v \psi_v(x_v) \qquad\qquad (x = (x_v)_v \in \mathbb{A}), \tag{2.73}$$

where v runs over the places of K and ψ_v is an additive character of K_v. Of course to make sense of (2.73) one needs to know that $\psi_v(x_v) = 1$ for all but finitely v. This condition is satisfied if we take $\psi_v = \psi_v^{\mathrm{can}}$ for all v, because for all but finitely many finite v we have both $x_v \in \mathcal{O}_v$ and $\mathcal{O}_v = \mathfrak{D}_v$, where $\mathfrak{D}_v$ is the local different of K_v over $\mathbb{Q}_p$ and $v|p$. Thus for all but finitely many finite v we have $\mathrm{tr}_{K_v/\mathbb{Q}_p}(x_v) \in \mathbb{Z}_p$, as required.

Going a step further, we claim that if we take $\psi_v = \psi_v^{\mathrm{can}}$ on the right-hand side of (2.73) then the left-hand side becomes a global additive character ψ^{can} of K. The point to be checked is that ψ^{can} is trivial on K. So suppose that $\alpha \in K$. Referring to (2.70) and (2.71), we see that the identity to be verified is

$$\sum_{p<\infty} \sum_{v|p} \{\mathrm{tr}_{K_v/\mathbb{Q}_p}(\alpha)\}_p \equiv \sum_{v|\infty} \{\mathrm{tr}_{K_v/\mathbb{R}}(\alpha)\}_\infty \pmod{\mathbb{Z}}.$$

Now the sum of the local traces at the places lying over a given place of $\mathbb{Q}$ is equal to the global trace, so putting $\beta = \mathrm{tr}_{K/\mathbb{Q}}(\alpha)$, we must show that

$$\sum_{p<\infty} \{\beta\}_p \equiv \sum_{v|\infty} \{\beta\}_\infty \pmod{\mathbb{Z}}.$$

But this is a familiar fact: The principal part of a rational number differs from its fractional part by an integer.

Now let χ be an idele class character of K and ψ a global additive character of K. The global root number is the product of the local root numbers:

$$W(\chi, \psi) = \prod_v W(\chi_v, \psi_v). \tag{2.74}$$

But the left-hand side of (2.74) can simply be denoted $W(\chi)$, because the dependence on ψ is illusory: For any global additive character ψ of K there exists $\alpha \in K^\times$ such that $\psi(x) = \psi^{\mathrm{can}}(\alpha x)$, and thus the right-hand side of (2.74) becomes

$$\prod_v W(\chi_v, (\psi_v)_\alpha) = \prod_v (\chi_v(\alpha)/|\chi_v(\alpha)|) W(\chi_v, \psi_v^{\mathrm{can}}) \tag{2.75}$$

by virtue of (2.72). Since χ is an idele class character and $\alpha \in K$, the right-hand side of (2.75) is simply $\prod_v W(\chi_v, \psi_v^{\mathrm{can}})$ or in other words our previous $\prod_v W(\chi_v)$, and we recover the definition (2.47) of the global root number that we had before the introduction of additive characters.

If we are back where we started, then what was the point of introducing additive characters in the first place? One answer is that additive characters provide a flexibility which is useful theoretically, but a more compelling answer is that one wants a theory which is applicable to function fields in one variable over finite fields, not just to number fields. Usually the difference between number fields and function fields is thought to be the presence or absence of archimedean places, but another important difference is that the prime field of a number field is another number field, whereas the prime field of a function field is not a global field at all. It is the latter difference that makes it necessary to introduce additive characters. Sure, any function field K contains a subfield of the form $\mathbb{F}_q(t)$, and perhaps one can make a canonical choice of an additive character of $\mathbb{F}_q(t)$ and its completions and then compose with trace. But the problem is that K contains infinitely many subfields of the form $\mathbb{F}_q(t)$, and in general one is no more canonical than the others.

7.2. The local epsilon factor and local functional equation

Roughly speaking, epsilon factors are Gauss sums, or factors of Gauss sums, or a generalization of Gauss sums. For example the Gauss sum $\tau(\chi)$ (1.2) introduced at the beginning of Lecture 1 is the product over the finite primes of $\mathbb{Q}$ of the local epsilon factors associated to $\chi_{\mathbb{A}}$, and $\tau(\chi)/i^{a_\infty(\infty)}$ is the global epsilon factor of $\chi_{\mathbb{A}}$. As this example illustrates, the epsilon factor binds the root number to the square root of the conductor – in fact to the square root of the product of the conductor and the absolute value of the discriminant, although the latter factor is of course 1 in the case of $\mathbb{Q}$. Actually the discriminant will have to be replaced by some quantity dependent on the choice of an additive character, for we would like to define the epsilon factor in a way that makes sense for function fields as well as number fields. Given the broader framework, we should revisit the definitions already made – adeles, ideles, idele class characters, and so on – so as to include the function field case, but the necessary adjustments are minimal and will be left as an exercise.

Suppose then that K is a local field, χ a character of $K^\times$, ψ an additive character of K, and dx a Haar measure on K. Let s denote a complex variable. The epsilon factor $\varepsilon(\chi, \psi, dx)$ is the value at $s = 0$ of an entire function denoted $\varepsilon(\chi, \psi, dx, s)$:

$$\varepsilon(\chi, \psi, dx) = \varepsilon(\chi, \psi, dx, s)|_{s=0}. \tag{2.76}$$

If this looks circuitous, the point us that the definition of $\varepsilon(\chi, \psi, dx, s)$ involves integrals which may converge only for $\Re(s) \gg 0$, but (2.76) defines $\varepsilon(\chi, \psi, dx)$ by analytic continuation.

The integrals just mentioned appear together with $\varepsilon(\chi, \psi, dx, s)$ in Tate's local functional equation. Quite apart from the fact that Tate's method applies to function fields as well as number fields, the local functional equation is a major innovation in its own right. To state it, let $\mathcal{S}(K)$ denote the **Schwartz space** of K. Thus if K is nonarchimedean then $\mathcal{S}(K)$ consists of locally constant functions on K of compact support, while if K is $\mathbb{R}$ or $\mathbb{C}$ then $\mathcal{S}(K)$ consists of C^∞ functions f on K such that the derivatives of f of all orders (mixed partial derivatives of all orders if $K \cong \mathbb{C}$) have rapid decay. To spell out the archimedean case in more detail, if $K = \mathbb{R}$ then given $n, N \geqslant 0$ there exists $C = C(n, N, f)$ such that $|f^{(n)}(x)| \leqslant C/(1 + |x|)^N$, and if $K \cong C$ then given $m, n, N \geqslant 0$ there exists $C = C(m, n, N, f)$ such that $|\partial^{m+n} f/\partial^m x \partial^n y| \leqslant C/((1 + |x|)(1 + |y|))^N$. In all

cases, archimedean or not, we define the Fourier transform $\hat{f}$ of a function $f \in \mathcal{S}(K)$ by

$$\hat{f}(y) = \int_K f(x)\psi(xy)\ dx. \tag{2.77}$$

Then $\hat{f}$ is again in $\mathcal{S}(K)$.

Now given $f \in \mathcal{S}(K)$, set

$$I(\chi, dx, s, f) = \int_{K^\times} f(x)\chi(x)||x||^s\ \frac{dx}{||x||}, \tag{2.78}$$

where $||*||$ is the local norm (2.7). (The reason for writing the integrand as $f(x)\chi(x)||x||^s\,dx/||x||$ rather than simply as $f(x)\chi(x)||x||^{s-1}\,dx$ is that $dx/||x||$ is a Haar measure on $K^\times$, a fact that will be used in a moment.) Tate's local functional equation states that

$$\frac{I(\chi^{-1}, dx, 1-s, \hat{f})}{L(1-s, \chi^{-1})} = \varepsilon(\chi, \psi, dx, s)\frac{I(\chi, dx, s, f)}{L(s, \chi)}, \tag{2.79}$$

where the local L-factors are as in (2.29), (2.32), and (2.33). Formula (2.79) is the definition of $\varepsilon(\chi, \psi, dx, s)$.

It is not be hard to verify that the integral defining $I(\chi, dx, f, s)$ converges for $\Re(s) \gg 0$ and extends to a meromorphic function of s, and it is immediate from the definitions (2.29), (2.32), and (2.33) that $L(s, \chi)$ is a meromorphic function on $\mathbb{C}$. Thus the main content of (2.79) is that the function

$$\varepsilon(\chi, \psi, dx, s, f) = \frac{L(s, \chi)I(\chi^{-1}, dx, 1-s, \hat{f})}{L(1-s, \chi^{-1})I(\chi, dx, s, f)} \tag{2.80}$$

is entire and independent of f.

Granting (2.79), let us examine the dependence of $\varepsilon(\chi, \psi, dx, s)$ on ψ. Write the integrand of (2.78) as $\hat{f}(x)\chi(x)||x||^s\,d\mu(x)$, where $d\mu(x)$ is the Haar measure $dx/||x||$ on $K^\times$, and take $a \in K^\times$. If ψ is replaced by ψ_a in (2.77) then $\hat{f}(y)$ is replaced by $\hat{f}(ay)$, and consequently the integrand $\hat{f}(x)\chi^{-1}(x)||x||^{1-s}\,d\mu(x)$ of $I(\chi^{-1}, dx, 1-s, \hat{f})$ is replaced by $\hat{f}(ax)\chi^{-1}(x)||x||^{1-s}\,d\mu(x)$. Using the invariance of $d\mu$ under $x \mapsto a^{-1}x$, we see that the new $I(\chi^{-1}, dx, 1-s, \hat{f})$ is $\chi(a)||a||^{s-1}$ times the old one. Since the L-factors and $I(\chi, dx, s, f)$ are unaffected by the switch from ψ to ψ_a, we conclude from (2.79) that

$$\varepsilon(\chi, \psi_a, dx, s) = \chi(a)||a||^{s-1}\varepsilon(\chi, \psi, dx, s). \tag{2.81}$$

In particular, we have

$$\varepsilon(\chi, \psi_a, dx) = \chi(a)||a||^{-1}\varepsilon(\chi, \psi, dx) \tag{2.82}$$

by taking $s = 0$ in (2.81).

The dependence of $\varepsilon(\chi, \psi, dx, s)$ on dx is also easy to determine. Any other Haar measure on K has the form $c\,dx$ with a real number $c > 0$, and (2.78) gives $I(\chi, c\,dx, s, f) = c\,I(\chi, dx, s, f)$ while (2.78) and (2.77) together give $I(\chi^{-1}, c\,dx, 1-s, \hat{f}) = c^2\,I(\chi^{-1}, dx, 1-s, \hat{f})$. From (2.79) we conclude that

$$\varepsilon(\chi, \psi, c\,dx, s) = c\,\varepsilon(\chi, \psi, dx, s). \tag{2.83}$$

In particular,

$$\varepsilon(\chi, \psi, c\,dx) = c\,\varepsilon(\chi, \psi, dx) \tag{2.84}$$

on taking $s = 0$.

Given $f \in \mathcal{S}(K)$, define $f^- \in \mathcal{S}(K)$ by $f^-(x) = f(-x)$. To make one further deduction from (2.79) , we apply (2.79) a second time and use the fact that $\hat{\hat{f}} = f^-$ if dx is equal to dx_{sd}, the **self-dual Haar measure** relative to ψ. (The identity $\hat{\hat{f}} = f^-$ can be taken as the defining property of a self-dual Haar measure.) Making the substitution $x \mapsto -x$ in $I(\chi, dx_{\mathrm{sd}}, f^-, s)$, we find that

$$\varepsilon(\chi, \psi, dx_{\mathrm{sd}}, s)\varepsilon(\chi^{-1}, \psi, dx_{\mathrm{sd}}, 1-s) = \chi(-1). \tag{2.85}$$

There is also a version of (2.85) for $\epsilon(\chi, \psi, dx_{\mathrm{sd}})$, but it is not obvious from the formulas that have been mentioned so far, and we state only the case where K is nonarchimedean:

$$\varepsilon(\chi, \psi, dx_{\mathrm{sd}})\varepsilon(\chi^{-1}, \psi, dx_{\mathrm{sd}}) = \chi(-1)q^{n(\psi)+a(\chi)}, \tag{2.86}$$

where $a(\chi)$ is the exponent of the conductor of χ as before and $n(\psi)$ is the largest integer ν such that ψ is trivial on $\pi^{-\nu}\mathcal{O}$.

7.3. Epsilon factors and root numbers

It should be apparent that our point of view has changed: The primary object is now the local epsilon factor, not the local root number. However the latter can be defined in terms of the former by setting

$$W(\chi, \psi) = \frac{\varepsilon(\chi, \psi, dx)}{|\varepsilon(\chi, \psi, dx)|}. \tag{2.87}$$

It follows from (2.84) that the left-hand side of (2.87) is indeed independent of the choice of dx. Furthermore (2.72) is now a consequence of (2.82), and (2.86) gives the new relation

$$W(\chi, \psi)W(\chi^{-1}, \psi) = \chi(-1), \tag{2.88}$$

which in this form is actually valid for all K, archimedean or nonarchimedean. The explicit formulas (2.48) through (2.56) follow from (2.87) and the explicit calculation of $\varepsilon(\chi, \psi, dx)$ which are part of Tate's proof of the local and global functional equations.

8. Exercises

Exercise 2.1. We have characterized the topology on $\mathbb{A}_K$ by two properties. Verify that there does in fact exist a unique topology $\mathcal{T}$ on $\mathbb{A}_K$ with these properties and that the sets $\prod_v \mathcal{U}_v$ with $\mathcal{U}_v$ open in K_v for all v and $\mathcal{U}_v = \mathcal{O}_v$ for all but finitely many finite v form a basis for $\mathcal{T}$. Similarly, verify that there is a unique topology on $\mathbb{A}_K^\times$ with the two properties claimed for it, and show that a basis for this topology is given by the sets $\prod_v \mathcal{U}_v$ with $\mathcal{U}_v$ open in $K_v^\times$ for all v and $\mathcal{U}_v = \mathcal{O}_v^\times$ for all but finitely many finite v.

Exercise 2.2. Let K be a number field, let C be its ideal class group, and let $c(\mathfrak{D}) \in C$ be the class of the different ideal $\mathfrak{D}$ of K. Prove that $c(\mathfrak{D}) \in C^2$. (Hint: If this is not the case then there is a quadratic ideal class character χ of K such that $\chi(\mathfrak{D}) = -1$. Compute $W(\chi)$ and obtain a contradiction to Theorem 2.2.) Although the theorem that $c(\mathfrak{D}) \in C^2$ is due to Hecke, the proof given by Hecke ([**31**], p. 261) is quite different. The proof outlined in the hint follows an argument of Armitage [**1**] suggested by Serre.

Exercise 2.3. The purpose of this exercise is to complete the proof of Proposition 1.7 in the case $D|8$ by showing that a decomposition $X(D) = X^+(D) \cup X^-(D)$ with the stated properties exists.

(a) Show that that $W(\chi\varphi) = W(\chi)$ for $\chi \in X(D)$ and $\varphi \in \Phi$. (Hint: If $\mathfrak{p}$ is a prime ideal dividing $\mathfrak{f}(\chi)$ and v is the corresponding place of K then $\mathfrak{p}^{a(\chi_v)+n_v}$ is principal.)

(b) Let $\mathfrak{T}$ be the prime ideal of $\mathcal{O}$ above 2, let E be as in the proof of Proposition 1.3, and write $E = \{\varepsilon, \delta\}$. Also let ε' and δ' be the corresponding quadratic characters of

$$(\mathcal{O}/\mathfrak{T}^5)^\times \cong (\mathbb{Z}/8\mathbb{Z})^\times \times \langle (1+\sqrt{-2C}) + \mathfrak{T}^5 \rangle, \tag{2.89}$$

where the second factor on the right-hand side is the cyclic group of order 4 generated by the coset of $1+\sqrt{-2C}$. Replacing this second factor by its subgroup of order 2, we obtain a subgroup H of index 2 in $(\mathcal{O}/\mathfrak{T}^5)^\times$ such that $\varepsilon' = -\delta'$ on the complement of H and $\varepsilon' = \delta'$ on H. By direct calculation, show that

$$\sum_{h \in H} \varepsilon'(h) e^{2\pi i \operatorname{tr}_{K/\mathbb{Q}}(h/16)} = 0.$$

(To interpret $e^{2\pi i \operatorname{tr}_{K/\mathbb{Q}}(h/16)}$, replace h by any of its coset representatives in $\mathcal{O}$: The value of the exponential is independent of the coset representative because the different ideal of K is $\mathfrak{T}^3$.)

(c) Deduce that $\sum_{\chi \in X(D)} W(\chi) = 0$, and thus complete the proof of Proposition 1.7

Exercise 2.4. Using the local formulas and Theorem 2.1, verify that (1.35) holds with $\Lambda(s, \chi^w)$ as in (1.36) and $W(\chi)$ as in (1.37).

Exercise 2.5. The purpose of this exercise is to fill in some details pertaining to (2.63), (2.67), and (2.68).

(a) Let K be any real quadratic field. Show that (2.63) gives a well-defined equivariant character χ_0 of P and that any extension of this character to I is a primitive Hecke character and still equivariant.

(b) With K and χ_0 as in (a), let η be any equivariant primitive Hecke character of K of finite order. Show that (2.64) holds with $\chi = \eta\chi_0$ and $\Lambda(s, \chi)$ as in (2.65). In particular, show that $W(\chi) = W(\eta)$.

(c) Now take $K = \mathbb{Q}(\sqrt{p(p+4)})$ with a prime $p > 5$ such that $p \equiv 1 \bmod 4$, and let η be as in (2.67). Explain why η is equivariant, and verify (2.68).

LECTURE 3

Motivic L-functions

The discussion now moves to L-functions associated to Galois representations. Within this large framework Artin L-functions form a natural point of departure for one simple reason: All known methods of obtaining an L-function from a Galois representation are variants of Artin's original construction.

1. Artin L-functions

Let K be a number field. A representation of $\mathrm{Gal}(\overline{K}/K)$ over $\mathbb{C}$ is called an **Artin representation** of K. Thus an Artin representation is a continuous homomorphism $\mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}(V)$, where V is a finite-dimensional vector space over $\mathbb{C}$.

The continuity condition is very restrictive here, because the topologies on $\mathrm{GL}(V)$ and $\mathrm{Gal}(\overline{K}/K)$ are utterly disparate. On the one hand, $\mathrm{GL}_n(\mathbb{C})$ has no small subgroups, as previously noted; on the other hand, $\mathrm{Gal}(\overline{K}/K)$ is the profinite group $\varprojlim_L \mathrm{Gal}(L/K)$, where L runs over finite Galois extensions of K inside $\overline{K}$. Since a complex representation of a profinite group is trivial on an open subgroup, we see that an Artin representation of K can be regarded simply as a finite-dimensional complex representation of $\mathrm{Gal}(L/K)$ for some finite Galois extension L of K, and this is the point of view that we shall usually adopt.

Consider then a finite Galois extension L of K, a finite-dimensional complex vector space V, and an Artin representation $\rho : \mathrm{Gal}(L/K) \to \mathrm{GL}(V)$. The associated Artin L-function $L(s, \rho)$ is an Euler product over the nonzero prime ideals $\mathfrak{p}$ of K,

$$L(s, \rho) = \prod_{\mathfrak{p}} B_{\mathfrak{p}}((\mathbf{N}\mathfrak{p})^{-s})^{-1}, \tag{3.1}$$

where $B_{\mathfrak{p}}(x) \in \mathbb{C}[x]$ is a polynomial with constant term 1. It will be clear from the definition of $B_{\mathfrak{p}}(x)$ that the roots of $B_{\mathfrak{p}}(x)$ are roots of unity, and from this it follows that the right-hand side of (3.1) converges for $\Re(s) > 1$.

To define $B_{\mathfrak{p}}(x)$ for a given $\mathfrak{p}$, we fix a prime ideal $\mathfrak{P}$ of L over $\mathfrak{p}$ and let D and I be the corresponding decomposition and inertia subgroups of $\mathrm{Gal}(L/K)$. Also write l and k for the residue class fields of $\mathfrak{P}$ and $\mathfrak{p}$ respectively. The natural action of $D(\mathfrak{P})$ on l induces an isomorphism of D/I onto $\mathrm{Gal}(l/k)$, and the latter group has a canonical generator, the Frobenius automorphism $x \mapsto x^{|k|}$. By a **Frobenius element** at $\mathfrak{P}$ we mean an element $\sigma \in D$ such that the coset σI is mapped to the Frobenius element of $\mathrm{Gal}(l/k)$. While it is only σI and not σ which is uniquely determined by $\mathfrak{P}$, if we restrict attention to the subspace

$$V^I = \{v \in V : \rho(i)(v) = v \text{ for all } i \in I\} \tag{3.2}$$

of inertial invariants then we obtain a well-defined linear automorphism $\rho(\sigma)|V^I$ of V^I. We set $B_{\mathfrak{p}}(x) = x^{\dim V} P(x^{-1})$, where $P(x)$ is the characteristic polynomial of

$\rho(\sigma)|V^I$. In other words,

$$B_{\mathfrak{p}}(x) = \det(1 - x\rho(\sigma)|V^I). \tag{3.3}$$

Of course I is trivial unless $\mathfrak{p}$ is ramified in L, and if I is trivial then $V^I = V$. It follows that the degree of $B_{\mathfrak{p}}(x)$ is $\leqslant \dim V$ for all $\mathfrak{p}$ and is equal to $\dim V$ for all but finitely many $\mathfrak{p}$.

All of this appears to depend on our choice of $\mathfrak{P}$ over $\mathfrak{p}$, but if we make a different choice, say $\mathfrak{P}'$, then there is an element $g \in \mathrm{Gal}(L/K)$ such that $\mathfrak{P}' = g(\mathfrak{P})$, and then D, I, σ, and V^I are replace by gDg^{-1}, gIg^{-1}, $g\sigma g^{-1}$ and gV^Ig^{-1} respectively. Since characteristic polynomials are similarity invariants, (3.3) is unchanged.

For the same reason, it is meaningful to define ρ to be **unramified at** $\mathfrak{p}$ if ρ is trivial on I, for then it is trivial on gIg^{-1} for all $g \in \mathrm{Gal}(L/K)$. If ρ is nontrivial on I then ρ is **ramified at** $\mathfrak{p}$.

So far the discussion has been confined to the finite places of K. We shall discuss the L-factors of ρ at the infinite places in a more general context later on, but the notion of ramification at the infinite places fits well here, because I has a natural analogue, namely the group of order two generated by complex conjugation. More precisely, given a real place v of K such that the places of L over v are complex, we say that ρ is **ramified at** v if ρ is nontrivial on one (hence on any) of the complex conjugations in $\mathrm{Gal}(L/K)$ corresponding to v. If v remains real in L, or if v becomes complex in L but ρ is trivial on the resulting complex conjugations, or if v is a complex place of K to begin with, then ρ is **unramified at** v.

If S is any set of places of K then we say that ρ is **unramified outside** S if ρ is unramified at every place $v \notin S$. For example, if S contains all of the places of K which ramify in L then ρ is unramified outside S. In particular, an Artin representation is always unramified outside a finite set of places.

1.1. Idele class characters of finite order as one-dimensional Artin representations

The phrase *finite order* is crucial here. Idele class characters (or primitive Hecke characters) of infinite order do not give rise to Artin representations. However there is a canonical bijection $\chi \mapsto \chi_{\mathrm{Art}}$ from idele class characters of K of finite order to one-dimensional Artin representations. It arises from the **Artin isomorphism** (or **reciprocity law isomorphism**)

$$(*, K^{\mathrm{ab}}/K)_{\mathbb{A}} : C/D \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K), \tag{3.4}$$

where C is the idele class group of K and D is the closure of the image in C of the subgroup $\mathbb{R}_+^{r_1} \times (\mathbb{C}^\times)^{r_2}$ of $(\mathbb{R} \otimes_{\mathbb{Q}} K)^\times$. A character of $\mathbb{R}_+$ or $\mathbb{C}^\times$ of finite order is trivial, and consequently an idele class character of finite order is trivial on D. Conversely, every character of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ has finite order, so it follows from (3.4) that the idele class characters of K of finite order are *precisely* the characters of C/D. Hence we can define $\chi \mapsto \chi_{\mathrm{Art}}$ by the requirement

$$\chi_{\mathrm{Art}}((x, K^{\mathrm{ab}}/K)_{\mathbb{A}}) = \chi(x) \qquad (x \in \mathbb{A}^\times). \tag{3.5}$$

Actually the convention adopted in the more recent literature is to precompose with $x \mapsto x^{-1}$:

$$\chi_{\mathrm{Art}}((x, K^{\mathrm{ab}}/K)_{\mathbb{A}}) = \chi(x^{-1}) \qquad (x \in \mathbb{A}^\times); \tag{3.6}$$

cf. [**14**], [**62**]. We shall refer to (3.5) and (3.6) as the **arithmetic convention** and the **geometric convention** respectively. As we shall explain later, there are good

reasons for preferring one convention or the other, depending on the context. By defining $B_{\mathfrak{p}}(x)$ as in (3.3) we have implicitly chosen the more traditional arithmetic convention, for otherwise we would have replaced σ by σ^{-1} in (3.3). In other words, the geometric convention for $B_{\mathfrak{p}}(x)$ is

$$B_{\mathfrak{p}}(x) = \det(1 - x\rho(\Phi)|V^I), \tag{3.7}$$

where Φ is an **inverse Frobenius element** at $\mathfrak{p}$, the inverse of a Frobenius element. While we are still on the topic of Artin L-functions we will continue to follow the arithmetic convention, but once we start to look at more general motivic L-functions we will make a permanent switch to the geometric convention, for reasons to be discussed later.

Returning to the theme of idele class characters of finite order as Artin representations, we must confess that what is useful to us right now is not the map $\chi \mapsto \chi_{\mathrm{Art}}$ but rather its inverse. Given a one-dimensional Artin representation ρ, let us write χ_ρ for the idele class χ such that $\rho = \chi_{\mathrm{Art}}$. We would like to describe χ_ρ as a primitive Hecke character. To do so, we first recall how (3.4) is defined on the level of ideals.

Let L be the fixed field of the kernel of ρ, and view ρ as a faithful character of $\mathrm{Gal}(L/K)$. We consider integral ideals $\mathfrak{f}$ of $\mathcal{K}$ with the property that a prime ideal of K divides $\mathfrak{f}$ if and only it ramifies in L. In other words, $\mathfrak{D}_{L/K}|\mathfrak{f}^\infty$ and $\mathfrak{f}\mathfrak{D}_{L/K}^\infty$, where $\mathfrak{D}_{L/K}$ is the relative different ideal of L/K. Given a prime ideal $\mathfrak{p} \in I(\mathfrak{f})$ and a prime ideal $\mathfrak{P}$ of L above $\mathfrak{p}$, we can speak of *the* Frobenius element $\sigma_{\mathfrak{P}} \in \mathrm{Gal}(L/K)$ determined by $\mathfrak{P}$, because the inertia subgroup $I \subset \mathrm{Gal}(L/K)$ corresponding to $\mathfrak{P}$ is trivial. In fact we can speak of *the* Frobenius element $\sigma_{\mathfrak{p}} \in \mathrm{Gal}(L/K)$ determined by $\mathfrak{p}$, because $\mathrm{Gal}(L/K)$ is by assumption abelian, and consequently $g\sigma_{\mathfrak{P}}g^{-1} = \sigma_{\mathfrak{P}}$ for all $g \in \mathrm{Gal}(L/K)$. We can now define the Artin symbol $(*, L/K)$ on prime ideals by setting

$$(\mathfrak{p}, L/K) = \sigma_{\mathfrak{p}}. \tag{3.8}$$

Since $I(\mathfrak{f})$ is the free abelian group on the prime ideals it contains, the map $\mathfrak{p} \mapsto \sigma_{\mathfrak{p}}$ extends uniquely to a homomorphism $(*, L/K) : I(\mathfrak{f}) \to \mathrm{Gal}(L/K)$, the adelized version of which is (3.4).

Coming back to our one-dimensional representation ρ of $\mathrm{Gal}(L/K)$, we set

$$\chi_\rho(\mathfrak{a}) = \rho((\mathfrak{a}, L/K)) \qquad (\mathfrak{a} \in I(\mathfrak{f})). \tag{3.9}$$

The basic theorems of class field theory imply that if $\mathfrak{f}$ is chosen correctly then χ_ρ is a primitive Hecke character of conductor $\mathfrak{f}$ and that the map $\rho \mapsto \chi_\rho$ is a bijection from the set of one-dimensional Artin representations of K to the set of Hecke characters of K of finite order. Furthermore, on comparing the definitions (1.18) and (3.1) of the respective L-functions we see that

$$L(s, \rho) = L(s, \chi_\rho) \tag{3.10}$$

Here we are following the arithmetic convention, but in fact (3.10) holds with the geometric convention as well, because of the double inversion: not only is (3.3) replaced by (3.7) but also (3.9) is replaced by

$$\chi_\rho(\mathfrak{a}) = \rho((\mathfrak{a}, L/K)^{-1}) \qquad (\mathfrak{a} \in I(\mathfrak{f})), \tag{3.11}$$

this being the analogue of (3.6) on the level of ideals.

1.2. Basic properties

Almost anything one does with Artin L-functions depends on three basic properties. The first is **additivity**: If ρ and ρ' are representations of $\mathrm{Gal}(L/K)$ then

$$L(s, \rho \oplus \rho') = L(s, \rho)L(s, \rho'). \tag{3.12}$$

This is immediate from the additivity of the characteristic polynomial and the additivity of the map $V \mapsto V^I$.

The second property, which is trickier to prove, is **inductivity**. If M is an intermediate field of the Galois extension L/K and φ is a representation of $\mathrm{Gal}(L/M)$, let $\mathrm{ind}_{M/K}\varphi$ denote the representation of $\mathrm{Gal}(L/K)$ induced by φ. Then

$$L(s, \mathrm{ind}_{M/K}\varphi) = L(s, \varphi). \tag{3.13}$$

Note that the left-hand side is an Artin L-function of K while the right-hand side is an Artin L-function of M.

The third property is **compatibility in dimension one**: If $\dim\rho = 1$ and χ_ρ is the corresponding Hecke character of finite order then

$$L(s, \rho) = L(s, \chi_\rho). \tag{3.14}$$

This property has already been noted, and it depends on choosing the arithmetic convention (3.9). If instead we choose the geometric convention (3.11) then the right-hand side of (3.14) would be replaced by $L(s, \overline{\chi_\rho})$.

There is actually a fourth property of Artin L-functions which fits here, their **invariance under inflation**, even though it is more a property of the Artin symbol itself than of the L-function. Suppose that M is an intermediate field of the finite Galois extension L/K, and let ρ be a representation of $\mathrm{Gal}(M/K)$. Then ρ can be inflated to a representation of $\mathrm{Gal}(L/K)$ by composition with the canonical map $\mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$, and we write $\mathrm{infl}_{L/M}\rho$ for the representation of $\mathrm{Gal}(L/K)$ so obtained. Then

$$L(s, \mathrm{infl}_{L/M}\rho) = L(s, \rho). \tag{3.15}$$

This follows from the fact that if $\sigma \in \mathrm{Gal}(L/K)$ is a Frobenius element at a prime ideal $\mathfrak{P}$ of L then $\sigma|M$ is a Frobenius element at the prime ideal of M lying below $\mathfrak{P}$. One consequence of (3.15) is that if ρ is presented to us as a representation of $\mathrm{Gal}(\overline{K}/K)$, then $L(s, \rho)$ is independent of the choice of a finite Galois extension L of K such that ρ factors through $\mathrm{Gal}(L/K)$.

This concludes our recitation of basic properties. The first nontrivial illustration of them arises from a quadratic extension of number fields L/K. Let 1_L denote the one-dimensional character of the trivial subgroup $\mathrm{Gal}(L/L)$ of $\mathrm{Gal}(L/K)$, and let 1_K and λ denote respectively the trivial and the nontrivial one-dimensional characters of $\mathrm{Gal}(L/K)$. Then $\mathrm{ind}_{L/K}1_L = 1_K \oplus \lambda$, so (3.13) and (3.12) give

$$L(s, 1_L) = L(s, 1_K)L(s, \lambda). \tag{3.16}$$

Now it is immediate from the definitions that if $\rho = 1_L$ then χ_ρ is the trivial Hecke character of L to the modulus $\mathcal{O}_L$, so that $L(s, 1_L) = \zeta_L(s)$ by (3.14). Similarly $L(s, 1_K) = \zeta_K(s)$. Furthermore, on combining (3.8) with (3.9) we find that χ_λ is the quadratic Hecke character $\mathrm{sign}_{L/K}$ defined in (2.38). It follows that (3.16) is simply the relation (2.37).

2. The functional equation

The preceding example was a warm-up exercise for the task now at hand, which is to deduce a functional equation for Artin L-functions from the properties listed above and the known functional equation of Hecke L-functions. The key ingredient here is Brauer's induction theorem.

2.1. Derivation of the functional equation from Brauer's theorem

Given a finite group G, let $\mathrm{Groth}(G)$ denote the Grothendieck group of virtual representations of G over $\mathbb{C}$, and given a genuine representation ρ of G over $\mathbb{C}$, write $[\rho]$ for its class in $\mathrm{Groth}(G)$. Maschke's theorem implies that the classes $[\rho]$ with ρ irreducible form a basis for $\mathrm{Groth}(G)$ over $\mathbb{Z}$, and Brauer's theorem tells us that the classes $[\rho]$ with ρ monomial form at least a spanning set. In fact Brauer's theorem asserts that we can restrict our attention to monomial representations which are induced by one-dimensional characters of *elementary* subgroups of G, but this more precise assertion will not be needed in the sequel.

Now take $G = \mathrm{Gal}(L/K)$, where L/K is a Galois extension of number fields. If ρ is any representation of G then by Brauer's theorem we can write

$$[\rho] = \sum_{(M,\xi)} n_{M,\xi}[\mathrm{ind}_{M/K}\xi] \tag{3.17}$$

with $n_{M,\xi} \in \mathbb{Z}$, where (M,ξ) runs over pairs consisting of an intermediate field M and a one-dimensional character ξ of $\mathrm{Gal}(L/M)$. On the other hand, by virtue of the additivity property (3.12) we can view $L(s,*)$ as defining a homomorphism from $\mathrm{Groth}(G)$ to the multiplicative group of nonzero meromorphic functions on the right half-plane $\Re(s) > 1$. Applying this homomorphism to both sides of (3.17), we obtain

$$L(s,\rho) = \prod_{(M,\xi)} L(s,\mathrm{ind}_{M/K}\xi)^{n_{M,\xi}}, \tag{3.18}$$

and then the inductivity and compatibility properties (3.13) and (3.14) give

$$L(s,\rho) = \prod_{(M,\xi)} L(s,\chi_\xi)^{n_{M,\xi}}. \tag{3.19}$$

Each $L(s,\chi_\xi)$ is a Hecke L-function and so extends to a meromorphic function on $\mathbb{C}$. Thus (3.19) gives the continuation of $L(s,\rho)$ to a meromorphic function on $\mathbb{C}$.

But we want more: a functional equation. For each pair (M,ξ) in (3.17), put

$$A_{M,\xi} = D_M \mathbf{N}\mathfrak{f}(\chi_\xi), \tag{3.20}$$

and set

$$A(\rho) = \prod_{(M,\xi)} A_{M,\xi}^{n_{M,\xi}}. \tag{3.21}$$

Also set

$$L_\infty(s,\rho) = \prod_{(M,\xi)} L_\infty(s,\chi_\xi)^{n_{M,\xi}}, \tag{3.22}$$

$$W(\rho) = \prod_{(M,\xi)} W(\chi_\xi)^{n_{M,\xi}}, \tag{3.23}$$

and

$$\Lambda(s,\rho) = A^{s/2}L_\infty(s,\rho)L(s,\rho). \tag{3.24}$$

We claim that

$$\Lambda(s,\rho) = W(\rho)\Lambda(1-s,\rho^\vee). \tag{3.25}$$

This is the desired functional equation of $L(s,\rho)$.

To verify (3.25), one additional remark is needed. Of course to define $\Lambda(s,\rho^\vee)$ we simply apply the same procedure to ρ^{vee} as we applied to ρ, starting with the decomposition (3.17) in Groth(G). The remark is that dualization is a well-defined operation on Groth(G) and commutes with induction, so that taking duals of both sides of (3.17) gives

$$[\rho^\vee] = \sum_{(M,\xi)} n_{M,\xi}[\mathrm{ind}_{M/K}\overline{\xi}] \tag{3.26}$$

Also $\chi_{\overline{\xi}} = \overline{\chi_\xi}$. Hence formulas (3.18) through (3.24) give not only

$$\Lambda(s,\rho) = \prod_{(M,\xi)} \Lambda(s,\chi_\xi)^{n_{M,\xi}}, \tag{3.27}$$

but also, after the appropriate substitutions,

$$\Lambda(s,\rho^\vee) = \prod_{(M,\xi)} \Lambda(s,\overline{\chi_\xi})^{n_{M,\xi}}. \tag{3.28}$$

In view of (3.27), (3.28), and (3.23), we obtain the functional equation (3.25) by applying Hecke's functional equation (Theorem 2.1) to the individual factors $\Lambda(s,\chi_\xi)$.

2.2. Dependence on Brauer's theorem

The functional equation (3.25) is a relation between the four quantities $L(s,\rho)$, $L_\infty(s,\rho)$, $A(\rho)$, and $W(\rho)$. It is time to look more closely at the definitions of these quantities and to distinguish between those that are "Brauer-dependent" – in other words, dependent on an expression for $[\rho]$ like (3.17) – and those that are not. The definition of $L(s,\rho)$ itself is of the latter type: It is both Brauer-independent and local in the sense that (3.1) makes no reference to Brauer's theorem and expresses $L(s,\rho)$ as a product of local factors (3.3) defined in an intrinsic way. The same is true of $A(\rho)$ and $L_\infty(\rho)$, although so far we have given only the Brauer-dependent global definitions (3.21) and (3.22) . However in the case of $W(\rho)$ no Brauer-independent definition is known. At first this may not appear to be problematic. After all, even though the decomposition (3.17) of $[\rho]$ is not unique, the resulting expression (3.23) for $W(\rho)$ has to be independent of the decomposition because the functional equation (3.25) can't hold with two different values of $W(\rho)$. But the problem is that the Brauer-dependent definition is not local. Sure, each factor $W(\chi_\xi)$ in (3.23) can be written as a product of local root numbers, but in dimension > 1 there is no known analogue of Tate's local functional equation (at least none on the Galois as opposed to automorphic side), so even if one decomposes each $W(\chi_\xi)$ in (3.23) into local factors and reassembles the local factors corresponding to a given place v it is not *a priori* clear that the resulting local root number $W(\rho_v)$ is independent of the decomposition of $[\rho]$. That it is in fact possible to define root numbers purely locally is a theorem of Langlands and Deligne [**14**], a full appreciation of which depends on passing to a more general framework.

3. Compatible families

The L-function of an elliptic curve without complex multiplication is neither a Hecke L-function nor an Artin L-function, and for this reason alone we need to broaden the discussion. The L-functions associated to the "compatible families" to be discussed next include all L-functions of elliptic curves, all Artin L-functions, and much else. In particular, since they include all L-functions of elliptic curves and all Artin L-functions they also include the Hecke L-functions attached to Hecke characters of type (1,0) of imaginary quadratic fields as well as all Hecke characters of finite order. However they do not include all Hecke L-functions: the L-functions of "nonalgebraic" Hecke characters like (2.63) will now fall by the wayside.

3.1. ℓ-adic representations

Until now, all representations have been representations over $\mathbb{C}$. Now we consider representations with field of scalars $\mathbb{Q}_\ell$, where ℓ is a prime number. Such a representation is called an **ℓ-adic representation.**

Let K be a number field. A key difference between a complex representation of $\mathrm{Gal}(\overline{K}/K)$ and an ℓ-adic representation of $\mathrm{Gal}(\overline{K}/K)$ is that the latter need no longer factor through the Galois group of a finite Galois extension of K. In particular, if ρ_ℓ is an ℓ-adic representation of $\mathrm{Gal}(\overline{K}/K)$ then it is *a priori* possible that infinitely many prime ideals of K ramify in the fixed field of the kernel of ρ_ℓ. Nonetheless, given a prime ideal $\mathfrak{p}$ of K we can choose a prime ideal $\mathfrak{P}$ of $\overline{K}$ over $\mathfrak{p}$ and speak of the associated the inertia subgroup $I \subset \mathrm{Gal}(\overline{K}/K)$ and the associated set σI of Frobenius elements, where $\sigma \in \mathrm{Gal}(\overline{K}/K)$ is any individual Frobenius element. If $\mathfrak{P}'$ is another prime ideal of K over $\mathfrak{p}$ and I' and σ' are the analogues of I and σ then there is an element of $\mathrm{Gal}(\overline{K}/K)$ which conjugates $\mathfrak{P}$ to $\mathfrak{P}'$, I to I', and σ to σ'. Thus a number of definitions previously made for Artin representations go through without change: The representation ρ_ℓ is **unramified at $\mathfrak{p}$**, or at the corresponding finite place, if $\rho_\ell(I) = \{1\}$, and if S is a finite set of places of K then χ is **unramified outside** S if it is unramified at each finite place of K not in S. One slight divergence from the analogy with Artin representations is that one does not usually refer to an ℓ-adic representation as being ramified or unramifed at an infinite place. However if $\mathfrak{p}$ is any prime ideal of K not dividing ℓ then by analogy with (3.7) we set

$$B_\mathfrak{p}(x) = \det(1 - x\rho_\ell(\Phi)|V_\ell^I) \qquad (\mathfrak{p} \nmid \ell), \tag{3.29}$$

where Φ is an inverse Frobenius element at $\mathfrak{p}$, V_ℓ is the space of ρ_ℓ, and V_ℓ^I is the subspace of inertial invariants (defined as in (3.2) but with V and ρ replaced by V_ℓ and ρ_ℓ). Note that we are following the geometric convention here, as we shall do consistently from now on. If we were to follow the arithmetic convention then the formula would be

$$B_\mathfrak{p}(x) = \det(1 - x\rho_\ell(\sigma)|(V_\ell)_I) \qquad (\mathfrak{p} \nmid \ell), \tag{3.30}$$

where $(V_\ell)_I$ is the space of **inertial coinvariants**, the quotient of V by the subspace spanned by all expressions of the form $v - \rho_\ell(i)v$ with $v \in V$ and $i \in I$. The point here is that the arithmetic and geometric conventions are in some sense dual to each other, so that V_ℓ^I in (3.29) must be replaced by its dual. The reason that the distinction between V^I and V_I did not show up already in (3.3) and (3.7) is that Artin representations are complex representations of a compact group, hence semisimple, so that V^I and V_I are isomorphic. In any case the real issue for us is

that regardless of the convention followed, the coefficients of $B_{\mathfrak{p}}(x)$ lie in $\mathbb{Q}_\ell$ rather than $\mathbb{C}$, so that the substitution $x = (\mathbf{N}\mathfrak{p})^{-s}$ is not *a priori* meaningful.

Now consider a map which assigns to each rational prime ℓ an ℓ-adic representation ρ_ℓ of $\mathrm{Gal}(\overline{K}/K)$. The resulting collection $\{\rho_\ell\}_\ell$ will usually be denoted simply $\{\rho_\ell\}$ and called a **family of ℓ-adic representations of** $\mathrm{Gal}(\overline{K}/K)$. We say that the family is **fully compatible** if the following conditions are satisfied:

(i) There is a finite set S of places of K, independent of ℓ, such that ρ_ℓ is unramified outside the set $S \cup \{\mathfrak{l} : \mathfrak{l}|\ell\}$ consisting of the places in S and the places of K dividing ℓ.

(ii) The polynomial $B_{\mathfrak{p}}(x)$ in (3.30), which *a priori* has coefficients in $\mathbb{Q}_\ell$ and thus depends on the prime ℓ used to define it, actually has coefficients in $\mathbb{Q}$ and is independent of ℓ in the sense that $B_{\mathfrak{p}}(x)$ is unchanged if ℓ in (3.30) is replaced by some other rational prime ℓ' with $\mathfrak{p} \nmid \ell'$.

Although we have not made it part of the definition, it follows from (i) and (ii) that the dimension of ρ_ℓ is independent of ℓ. Indeed, given a second rational prime ℓ', we can choose a prime ideal $\mathfrak{p}$ of K such that $\mathfrak{p} \notin S$ and $\mathfrak{p} \nmid \ell\ell'$. Then $V_\ell^I = V_\ell$ and $V_{\ell'}^I = V_{\ell'}$, whence the degree of $B_{\mathfrak{p}}(x)$ coincides both with $\dim(V_\ell)$ and $\dim(V_{\ell'})$.

A warning is in order here: The term *fully compatible* is not a standard term, and no standard term for the concept just defined seems to exist in the literature. The usual term is **strictly compatible**, but this is a slightly weaker notion: For strict compatibility the $B_{\mathfrak{p}}(x)$ is required to be independent of ℓ *only for* $\mathfrak{p}$ *not in* S. There is also mere *compatiblity*, an even weaker concept; see Serre [**54**], pp. I-10 – I-11. While the concept that we have dubbed *full compatibility* may lack a widely accepted name, the concept itself is all over the literature; see for example [**17**], [**52**], and [**53**]. Fortunately, standard terms do exist for two other concepts needed here: The representation ρ_ℓ is **integral** if the coefficients of $B_{\mathfrak{p}}(x)$ are rational integers, and the minimal set S satisfying (i) is the **exceptional set** of the family.

The simplest example of a fully compatible family of ℓ-adic representations of $\mathrm{Gal}(\overline{K}/K)$ is the one-dimensional family $\{\omega_\ell\}$ of ℓ-adic cyclotomic characters. Here $\omega_\ell : \mathrm{Gal}(\overline{K}/K) \to \mathbb{Z}_\ell^\times$ is defined by the condition

$$\sigma(\zeta) = \zeta^{\omega_\ell(\sigma)}, \tag{3.31}$$

where σ denotes an arbitrary element of $\mathrm{Gal}(\overline{K}/K)$ and ζ an arbitrary root of unity of ℓ-power order. The exceptional set S is the empty set.

Another example is afforded by the Tate modules of any elliptic curve E over K. The natural action of $\mathrm{Gal}(\overline{K}/K)$ on $T_\ell(E)$ extends to a representation $\rho_{E,\ell}$ of $\mathrm{Gal}(\overline{K}/K)$ on the space $V_\ell = \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_\ell(E)$, and the resulting family $\{\rho_{E,\ell}\}$ is fully compatible. In this case S consists of the places of K where E has bad reduction.

We remark that because we are following the geometric convention (3.29), neither the family $\{\omega_\ell\}$ nor the family $\{\rho_{E,\ell}\}$ is integral. In general, the main source of strictly compatible families of integral ℓ-adic representations of $\mathrm{Gal}(\overline{K}/K)$ is the ℓ-adic cohomology of smooth projective varieties over K, but while it is conjectured that these families are always fully compatible, this is not known.

3.2. λ-adic representations

If χ is a Dirchlet character of order $\geqslant 3$ then there are infinitely many ℓ such that the values of χ do not lie in $\mathbb{Q}_\ell$, but we would nonetheless like to associate a compatible family to χ and indeed to any Artin representation. A similar comment

applies to Hecke characters of imaginary quadratic fields. Thus we need to expand our notion of a compatible family slightly.

Let $\mathbb{E}$ be a number field and λ a finite place of $\mathbb{E}$. A representation with field of scalars $\mathbb{E}_\lambda$ is called a **λ-adic representation**. Thus a **family of λ-adic representations of** $\mathrm{Gal}(\overline{K}/K)$ is a collection $\{\rho_\lambda\}_\lambda$ indexed by the finite places of $\mathbb{E}$, where ρ_λ is a λ-adic representation of $\mathrm{Gal}(\overline{K}/K)$. We usually drop the external index and write simply $\{\rho_\lambda\}$. If $\mathfrak{p}$ is a prime ideal of K which does not divide the residue characteristic of $\mathbb{E}_\lambda$ then by analogy with formula (3.29) we set

$$B_\mathfrak{p}(x) = \det(1 - x\rho_\lambda(\Phi)|V_\lambda^I) \qquad (\mathfrak{p} \nmid \ell), \tag{3.32}$$

where V_λ is the space of ρ_λ. Of course if we were following the arithmetic convention then we would put

$$B_\mathfrak{p}(x) = \det(1 - x\rho_\lambda(\sigma)|(V_\lambda)_I) \qquad (\mathfrak{p} \nmid \ell). \tag{3.33}$$

We say that the family $\{\rho_\lambda\}$ is **fully compatible** if two conditions hold:

(i) There is a finite set S of places of K, independent of λ, such that ρ_λ is unramified outside the set $S \cup \{\mathfrak{l} : \mathfrak{l}|\ell\}$, where ℓ is the residue characteristic of $\mathbb{E}_\lambda$.

(ii) The polynomial $B_\mathfrak{p}(x)$ in (3.33) has coefficients in $\mathbb{E}$ and is unchanged if λ in (3.33) is replaced by λ', where λ' is another finite place of $\mathbb{E}$ of residue characteristic not divisible by $\mathfrak{p}$.

The representation ρ_λ is **integral** if the coefficients of $B_\mathfrak{p}(x)$ lie in $\mathcal{O}_\mathbb{E}$, and the **exceptional set** of a fully compatible family is the minimal set S satisfying (i). We refer to the field $\mathbb{E}$ as the **coefficient field** of the compatible family.

Now suppose that ρ is an Artin representation of $\mathrm{Gal}(\overline{K}/K)$. Then ρ is realizable over a number field $\mathbb{E}$. (In fact by a theorem of Brauer ρ is realizable over the field generated by the mth roots of unity, where m is any exponent for the image of ρ.) Hence we may take the space of ρ to be a vector space V over $\mathbb{E}$, and by extension of scalars we get a representation ρ_λ on $\mathbb{E}_\lambda \otimes_\mathbb{E} V$ for each finite place λ of $\mathbb{E}$. The resulting family $\{\rho_\lambda\}$ is fully compatible and integral, and its exceptional set is the set of places where ρ is ramified.

Finally, let K be an imaginary quadratic field, and χ a primitive Hecke character of K of type (1,0). Let $\mathbb{E}$ be the finite extension of K generated by the values of χ. To obtain a fully compatible family $\{\chi_\lambda\}$ of integral λ-adic representations of $\mathrm{Gal}(\overline{K}/K)$, think of χ as an idele class character. It follows from (2.15) that the character of $\mathbb{A}^\times$ sending $x = (x_v)_v$ to $\chi(x)\chi_\infty^{-1}(x_\infty)$ takes values in $\mathbb{E}$. Indeed write $x = \alpha \cdot y \cdot r$ as in (2.14); then $\chi(x)\chi_\infty^{-1}(x_\infty) = \chi(\mathfrak{a}_y)\alpha^{-1}$. Now let λ be a finite place of $\mathbb{E}$. The place of K below λ will be denoted λ also. Then the formula

$$\chi_\lambda(x) = \chi(x)\chi_\infty^{-1}(x_\infty)x_\lambda^{-1} \tag{3.34}$$

defines a character of $\mathbb{A}^\times$ with values in $\mathbb{E}_\lambda$. Furthermore, if $\alpha \in K^\times$ then $\chi(\alpha) = 1$ and $\chi_\infty^{-1}(\alpha_\infty) = \alpha = \alpha_\lambda$, so that the character defined by (3.34) is trivial on $K^\times$. Thus we may view χ_λ as a continuous homomorphism $C \to \mathbb{E}_\lambda^\times$, where C is the idele class group of K. Since $\mathbb{E}_\lambda$ is totally disconnected, χ_λ is trivial on D, the closure of the image in C of $\mathbb{R}_+^{r_1} \times \mathbb{C}^{\times r_2}$, and consequently we may view χ_λ as a λ-adic character of C/D. Composing with the inverse of the reciprocity law isomorphism (3.4) and identifying $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ with $\mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}}$, we obtain finally a one-dimensional λ-adic representation $\chi_\lambda : \mathrm{Gal}(\overline{K}/K) \to \mathbb{E}_\lambda^\times$. The exceptional set of the fully compatible family $\{\chi_\lambda\}$ consists of the places dividing $\mathfrak{f}(\chi)$.

3.3. The L-function of a fully compatible family

Henceforth it will be convenient to view all coefficient fields as subfields of $\mathbb{C}$. Notationally it is more convenient to associate an L-function to the *isomorphism class* of a fully compatible family rather than to the family itself, so a definition is in order. Let $\{\rho_\lambda\}$ and $\{\rho'_{\lambda'}\}$ be fully compatible families of representations of $\mathrm{Gal}(\overline{K}/K)$ with coefficient fields $\mathbb{E}$ and $\mathbb{E}'$ respectively. We say that these two families are **isomorphic** if there exists a number field $\mathbb{E}''$ containing $\mathbb{E}$ and $\mathbb{E}'$ such that for every finite place λ'' of $\mathbb{E}''$, the representations $\rho_{\lambda''}$ and $\rho'_{\lambda''}$ are isomorphic over $\mathbb{E}''_{\lambda''}$. Here $\rho_{\lambda''}$ and $\rho'_{\lambda''}$ are the representations over $\mathbb{E}''_{\lambda''}$ obtained by extension of scalars from ρ_λ and $\rho'_{\lambda'}$ respectively, where λ and λ' lie below λ''.

Now let M be the isomorphism class of a fully compatible family of λ-adic representations of $\mathrm{Gal}(\overline{K}/K)$ with coefficient field $\mathbb{E}$. Since we are viewing $\mathbb{E}$ as a subfield of $\mathbb{C}$, it is clear how to define the L-function of M: By analogy with (3.1), we put

$$L(s, M) = \prod_{\mathfrak{p}} B_{\mathfrak{p}}((\mathbf{N}\mathfrak{p})^{-s})^{-1}, \tag{3.35}$$

where $\mathfrak{p}$ runs over the prime ideals of K and $B_{\mathfrak{p}}(x)$ is as in (3.33).

The analogy with Artin L-functions extends beyond the definition to include also the properties of additivity and inductivity. Let M and M' be the isomorphism classes of two fully compatible families $\{\rho_\lambda\}$ and $\{\rho'_\lambda\}$, which by extension of scalars may be assumed to have the same coefficient field. Then $M \oplus M'$ denotes the isomorphism class of the family $\{\rho_\lambda \oplus \rho'_\lambda\}$, and

$$L(s, M \oplus M') = L(s, M)L(s, M'). \tag{3.36}$$

On the other hand, let L be a finite extension of K and let M be the isomorphism class of a fully compatible family $\{\rho_\lambda\}$ of λ-adic representations of $\mathrm{Gal}(\overline{K}/L)$. One can show that the family $\{\mathrm{ind}_{L/K}\rho_\lambda\}$ is also fully compatible and that its isomorphism class, which we will denote $\mathrm{ind}_{L/K}M$, satisfies

$$L(s, \mathrm{ind}_{L/K}M) = L(s, M). \tag{3.37}$$

As in the case of Artin L-functions, (3.36) is immediate from the definitions while the proof of (3.37) is a bit trickier.

3.4. Examples

We see at once that if M is the isomorphism class of the family $\{\rho_\lambda\}$ coming from an Artin representation ρ then $L(s, M) = L(s, \rho^\vee)$, because we followed the arithmetic convention when defining Artin L-functions. On the other hand, if K is an imaginary quadratic field and M is the isomorphism class of $\{\chi_\lambda\}$ for some Hecke character χ of K of type $(1, 0)$ then $L(s, M) = L(s, \chi)$, because now (3.6) comes into play as well as the appearance of Φ in place of σ in (3.29).

Now if we start with an elliptic curve E, then there are two families of fully compatible ℓ-adic representations to consider: the family $\{\rho_{E,\ell}\}$ afforded by the Tate modules of E and the family $\{\rho^\vee_{E,\ell}\}$ afforded by the ℓ-adic cohomology groups $H^1_\ell(E)$, which are dual to the modules $V_\ell(E)$. Denoting the isomorphism classes of these two families by M and $M^\vee$ respectively, we have $L(s, M) = L(s, E)$ if we follow the arithmetic convention (3.30) and $L(s, M^\vee) = L(s, E)$ if we follow the geometric convention (3.29). The point is that $\rho^\vee(\Phi)|V_\lambda^I$ is the transpose of $\rho(\sigma)|(V_\lambda)_I$ and so has the same characteristic polynomial. But if we follow the

arithmetic convention then $L(s, M^\vee) = L(s+1, E)$. The upshot is that if an ℓ-adic representation comes from ℓ-adic cohomology then the geometric convention is the natural one. Since ℓ-adic cohomology appears to be the primary source of ℓ-adic representations, and since the geometric convention predominates in the current literature anyway, we follow it here.

3.5. Semisimplicity

Let M be the isomorphism class of a fully compatible family $\{\rho_\lambda\}$. Since characteristic polynomials are insensitive to semisimplification, $L(s, M)$ is unchanged if the representations ρ_λ are replaced by their semisimiplifications. So from this point of view there is no loss in assuming that the ρ_λ are semisimple to being with, and in fact there is something to be gained:

Proposition 3.1. *Let $\{\rho_\lambda\}$ be a fully compatible family of semisimple λ-adic representations of $\mathrm{Gal}(\overline{K}/K)$, and let M be its isomorphism class. Then M is uniquely determined by the isomorphism class of any one of the representations ρ_λ.*

Proof. This is a simple consequence of the fact that a semisimple representation over a field of characteristic 0 is determined up to isomorphism by its character. Indeed fix places λ and λ' of the coefficient field $\mathbb{E}$ of the family, and given a prime ideal $\mathfrak{p}$ of K let $\Phi_\mathfrak{p} \in \mathrm{Gal}(\overline{K}/K)$ be an inverse Frobenius element at $\mathfrak{p}$. For all but finitely many $\mathfrak{p}$ we have

$$\mathrm{tr}\,\rho_\lambda(\Phi_\mathfrak{p}) = \mathrm{tr}\,\rho_{\lambda'}(\Phi_\mathfrak{p}), \tag{3.38}$$

because both sides coincide with the coefficient of $-x$ in $B_\mathfrak{p}(x)$. By (3.38), $\mathrm{tr}\,\rho_\lambda$ and $\mathrm{tr}\,\rho_{\lambda'}$ coincide on a dense subset of $\mathrm{Gal}(\overline{K}/K)$. Since both are continuous each determines the other. □

Without the semisimplicity assumption the assertion is false. For example, fix a finite place λ_0 of E, and for $\lambda \neq \lambda_0$ set $\rho_\lambda = 1_K \oplus 1_K$. We can complete $\{\rho_\lambda\}_{\lambda\neq\lambda_0}$ to a fully compatible family $\{\rho_\lambda\}$ by setting $\rho_{\lambda_0} = 1_K \oplus 1_K$ but also by setting

$$\rho_{\lambda_0}(g) = \begin{pmatrix} 1 & \log\omega_{\ell_0}(g) \\ 0 & 1 \end{pmatrix} \qquad (g \in \mathrm{Gal}(\overline{K}/K)),$$

where ℓ_0 is the residue characteristic of λ_0 and log is the ℓ_0-adic logarithm on $\mathbb{Z}_{\ell_0}$. Of course the associated L-function is $\zeta_K(s)^2$ in both cases.

3.6. Analytic desiderata

Let M be the isomorphism class of a fully compatible family of λ-adic representations of $\mathrm{Gal}(\overline{K}/K)$ with coefficient field $\mathbb{E}$ and exceptional set S. It is not at all clear that the Euler product defining $L(s, M)$ converges in some right half-plane, and without this property $L(s, M)$ is of no use to us. Hence we consider a condition on the **reciprocal roots** of $B_\mathfrak{p}(x)$, in other words the numbers $\alpha \in \mathbb{C}$ such that $B_\mathfrak{p}(\alpha^{-1}) = 0$ (recall that $B_\mathfrak{p}(x)$ has constant term 1, so that 0 is not a root). Actually we consider two conditions: one for $\mathfrak{p}$ not belonging to the exceptional set S of M, and an auxiliary condition for $\mathfrak{p} \in S$. Fix $w \in \mathbb{Z}$. The respective conditions are

$$|\iota(\alpha)| = (\mathbf{N}\mathfrak{p})^{w/2} \qquad (\mathfrak{p} \notin S) \tag{3.39}$$

for all field automorphisms ι of $\mathbb{C}$, and

$$|\iota(\alpha)| = |\iota'(\alpha')| \leqslant (\mathbf{N}\mathfrak{p})^{w/2} \qquad (\mathfrak{p} \in S) \tag{3.40}$$

for any two reciprocal roots α and α' of $B_{\mathfrak{p}}(x)$ and any two field automorphisms ι and ι' of $\mathbb{C}$. Thus if $\mathfrak{p} \in S$ then we specify only an upper bound for $|\iota(\alpha)|$, not the exact value, but we require that the exact value be the same for all reciprocal roots and all field automorphisms. If M satisfies both (3.39)and (3.40) then we say that M has **weight** w.

If M has weight w then the Euler product defining $L(s, M)$ converges for $\Re(s) > w/2+1$. Of course this would be true even if we required (3.39) and (3.40) only for ι equal to the identity automorphism, but by allowing $\iota \in \mathrm{Aut}(\mathbb{C})$ to be arbitrary, we compensate for the fact that we have fixed an embedding of $\mathbb{E}$ in $\mathbb{C}$. It is convenient to do so, but we do not want our definition of "weight" to depend on the choice of embedding.

To recapitulate, if M has a weight then the Euler product for $L(s, M)$ does converge in some right half-plane. But we also want an analytic continuation and functional equation, and to formulate the latter we need some terminology for gamma factors. By a **gamma factor of weight** w over K we mean a product

$$\gamma(s) = \prod_{v|\infty} \gamma_v(s), \tag{3.41}$$

where $\gamma_v(s)$ is a gamma factor of weight w over K_v. The latter concept is defined as follows.

If w is odd, or if w is even and $K_v \cong \mathbb{C}$, then a gamma factor of weight w over K_v is a product of the form

$$\gamma_v(s) = \prod_{\substack{p+q=w \\ q \geqslant p \geqslant 0}} \Gamma_{\mathbb{C}}(s-p)^{h^{pq}}, \tag{3.42}$$

where p and q are nonnegative integers satisfying the stated conditions and the exponents h^{pq} are nonnegative integers. Of course if w is odd then the condition $q \geqslant p \geqslant 0$ can be replaced by $q > p \geqslant 0$.

If w is even and $K_v = \mathbb{R}$ then a gamma factor of weight w over K_v is a product of the form

$$\gamma_v(s) = \Gamma_{\mathbb{R}}(s-w/2)^{h^{w/2+}} \cdot \Gamma_{\mathbb{R}}(s-w/2+1)^{h^{w/2-}} \cdot \prod_{\substack{p+q=w \\ q>p\geqslant 0}} \Gamma_{\mathbb{C}}(s-p)^{h^{pq}}, \tag{3.43}$$

where as before, p and q are nonnegative integers satisfying the stated conditions and the exponents $h^{w/2+}$, $h^{w/2-}$, and h^{pq} are all nonnegative integers.

3.7. Duality

To state a functional equation we need not only gamma factors but also a notion of duality. This is straightforward: If M is the isomorphism class of $\{\rho_\lambda\}$ then the **dual** $M^\vee$ of M is the isomorphism class of $\{\rho_\lambda^\vee\}$. Given $r \in \mathbb{Z}$, we define the **r-fold Tate twist** $M(r)$ of M to be the isomorphism class of $\{\rho_\lambda \otimes \omega_\ell^r\}$, where the tensor product of ρ_λ with the ℓ-adic cyclotomic character ω_ℓ is formed by viewing the latter as a representation over $\mathbb{E}_\lambda$. Now if M has weight w then we put

$$\overline{M} = M^\vee(-w) \tag{3.44}$$

and call M **essentially self-dual** if $\overline{M} \cong M$. The notation $\overline{M}$ seems reasonable, because if $\alpha_1, \alpha_2, \ldots, \alpha_n$ are the reciprocal roots of $B_{\mathfrak{p}}(x)$ in $\mathbb{C}$, listed with their multiplicities, then the reciprocal roots of the counterpart of $B_{\mathfrak{p}}(x)$ for $M^\vee(-w)$

are the numbers $\alpha_j^{-1} \cdot (\mathbf{N}\mathfrak{p})^w$ with $1 \leqslant j \leqslant n$. But $\alpha_j^{-1} = \overline{\alpha_j}/|\alpha_j|^2 = \overline{\alpha_j}/(\mathbf{N}\mathfrak{p})^w$ by (3.39), at least if $\mathfrak{p} \notin S$, so

$$\alpha_j^{-1} \cdot (\mathbf{N}\mathfrak{p})^w = \overline{\alpha_j} \qquad (\mathfrak{p} \notin S). \tag{3.45}$$

The notation for the left-hand side of (3.44) is meant to remind us of (3.45).

To illustrate the definitions, let K be an imaginary quadratic field and consider a primitive Hecke character χ of K of type (1,0). Let $M'(\chi)$ be the isomorphism class of the associated one-dimensional family $\{\chi_\lambda\}$. Then $M'(\chi)$ is of weight one by (1.30), but $\chi \neq \overline{\chi}$ and consequently $M'(\chi)$ is not essentially self-dual. But put

$$M(\chi) = \mathrm{ind}_{K/\mathbb{Q}} M'(\chi). \tag{3.46}$$

If χ is equivariant in the sense that it satisfies the identity $\chi(\mathfrak{a}) = \overline{\chi}(\mathfrak{a})$ then one readily verifies that $M(\chi)$ is essentially self-dual of weight 1. In particular this is the case if $\chi \in X(D)$, by Proposition 1.7. And since $L(s, M(\chi))$ coincides by (3.37) with $L(s, M'(\chi))$ and hence with $L(s, \chi)$, Theorem 1.2 remains valid with $L(s, \chi)$ replaced by $L(s, M(\chi))$.

3.8. An algebraic desideratum

The property that we have called "full compatibility" makes it possible to define $L(s, M)$ but not to give a purely algebraic definition of the associated root number $W(M)$. To rectify this shortcoming, let $\{\rho_\lambda\}$ be any representative of M and $\mathbb{E}$ its coefficient field. We will say that M satisfies **Condition $\mathbf{C_8}$** if the following property holds. Let $\mathfrak{p}$ be a prime ideal of K, and D and I the decomposition and inertia subgroups of $\mathrm{Gal}(\overline{K}/K)$ associated to a prime ideal $\mathfrak{P}$ of $\overline{K}$ over $\mathfrak{p}$. Suppose that $g \in D$ is an element such that the coset of g in D/I coincides with the coset of σ^n for some Frobenius element σ at $\mathfrak{P}$ and some $n \in \mathbb{Z}$. Then we require that the characteristic polynomial of $\rho_\lambda(g)$ have coefficients in $\mathbb{E}$ and be independent of λ for all finite places λ of $\mathbb{E}$ such that $\mathfrak{p} \nmid \ell$, where ℓ is the residue characteristic of λ. The reason for referring to this property as "Condition C_8" is that it is so labeled in Serre [**53**]. We could also have referred to Problem 2 on p. 514 of Serre and Tate [**55**]. Note that Condition C_8 neither supersedes nor is superseded by full compatibility, because if $\mathfrak{p}$ belongs to the exceptional set S then Condition C_8 pertains to $\rho_\lambda(g)$ itself whereas full compatibility pertains to the restriction of $\rho_\lambda(g)$ to the space of inertial invariants.

4. Premotives

We come now to the main point. Let M be the isomorphism class of a fully compatible family of semisimple integral λ-adic representations of $\mathrm{Gal}(\overline{K}/K)$. We call M a **premotive of weight** w over K if three conditions are satisfied:

(i) M has weight w and satisfies condition C_8.

(ii) $L(s, M)$ extends to a meromorphic function on $\mathbb{C}$ which is entire if w is odd and holomorphic everywhere except possibly at $s \neq w/2 + 1$ if w is even.

(iii) There is a positive integer $A(M)$, a constant $W(M) \in \mathbb{C}$ of absolute value 1, and a gamma factor $\gamma(s)$ of weight w over K such that

$$\Lambda(s, M) = W(M)\Lambda(k - s, \overline{M})$$

with $\Lambda(s, M) = A(M)^{s/2}\gamma(s)L(s, M)$, $\Lambda(s, \overline{M}) = A(M)^{s/2}\gamma(s)L(s, \overline{M})$, and $k = w + 1$.

If M is a premotive of weight w then the integrality of the underlying representations ρ_λ implies that $w \geqslant 0$. We could broaden the definition to allow premotives of negative weight by declaring that $M((r-w)/2)$ has weight $w < 0$ if M is a premotive of weight $r \geqslant 0$ with $r \equiv w \bmod 2$. However premotives of negative weight will play no role in what follows.

The definition of "premotive" given above does not make the quantities $A(M)$, $W(M)$, and $\gamma(s)$ explicit. Nonetheless, they are uniquely determined by the definition in the following sense:

Proposition 3.2. *If $\widetilde{A(M)}$ is a positive integer, $\widetilde{W}(M) \in \mathbb{C}$ a constant of absolute value 1, and $\tilde{\gamma}(s)$ a gamma factor of weight w over K such that*

$$\widetilde{\Lambda}(s, M) = \widetilde{W}(M)\widetilde{\Lambda}(k-s, \overline{M})$$

with $\widetilde{\Lambda}(s, M) = \widetilde{A}(M)^{s/2} \cdot \tilde{\gamma}(s) \cdot L(s, M)$ *and* $\widetilde{\Lambda}(s, \overline{M}) = \widetilde{A}(M)^{s/2} \cdot \tilde{\gamma}(s) \cdot L(s, \overline{M})$, *then* $\widetilde{A}(M) = A(M)$, $\widetilde{W}(M) = W(M)$, *and* $\tilde{\gamma}(s) = \gamma(s)$.

Proof. Taking the ratio of the two functional equations, we obtain

$$(A(M)/\widetilde{A}(M))^{s/2} \frac{\gamma(s)}{\tilde{\gamma}(s)} = (W(M)/\widetilde{W}(M))(A(M)/\widetilde{A}(M))^{(k-s)/2} \frac{\gamma(k-s)}{\tilde{\gamma}(k-s)}. \tag{3.47}$$

Now it follows from the formulas (3.42) and (3.43) that the left-hand side of (3.47) is holomorphic and nonvanishing for $\Re(s) > [w/2]$ and the right-hand side for $\Re(s) < k - [w/2]$. Since $k = w+1$ we have $[w/2] < k - [w/2]$ and consequently both sides of (3.47) are entire and nonvanishing. Thus $\gamma(s)/\tilde{\gamma}(s)$ is entire and nonvanishing. If w is odd then $\gamma(s)/\tilde{\gamma}(s)$ has the form $\prod_{p=0}^{(w-1)/2} \Gamma_{\mathbb{C}}(s-p)^{n_p}$ with $n_p \in \mathbb{Z}$, and the fact that $\gamma(s)/\tilde{\gamma}(s)$ is holomorphic and nonzero at $s = (w-1)/2$ shows that $n_p = 0$ for $p = (w-1)/2$. Applying this argument inductively we find that $n_p = 0$ for $0 \leqslant p \leqslant (w-1)/2$, whence $\tilde{\gamma}(s) = \gamma(s)$. If n is even we use the duplication formula to write $\gamma(s)/\tilde{\gamma}(s)$ in the form $\prod_{p=-1}^{w/2} \Gamma_{\mathbb{R}}(s-p)^{n_p}$, and a similar argument again gives $\tilde{\gamma}(s) = \gamma(s)$. Thus in both cases we conclude that $(A(M)/\widetilde{A}(M))^s = (W(M)/\widetilde{W}(M))(A(M)/\widetilde{A}(M))^{k/2}$ for all s, whence $\widetilde{A}(M) = A(M)$ and $\widetilde{W}(M) = W(M)$. □

5. An open problem

The term *premotive* was just an expository device enabling us to talk about motivic L-functions without first talking about motives, but the choice of terminology suggests a question:

Does every premotive come from a motive?

This is not a new question. In fact a stronger version of it appears as Question 2 on p. I-12 of Serre [**54**], and the Fontaine-Mazur conjecture [**20**], while concerned with different issues, also implies a statement about the provenance of fully compatible families which is in most respects much stronger than what we are asking for (see the discussion on pp. 196 – 197 of [**20**]). Furthermore, the converse of the open problem is also a well-known open problem. In other words, if we start with a pure motive M of weight w then it is not known in general that M is a premotive of weight w in our sense, because the analytic continuation and functional equation of $L(s, M)$ are not known. For that matter the full compatibility (as opposed to

the strict compatibility) of the family of λ-adic representations attached to M is not known in general either, nor is the semisimplicity of the representations ρ_λ.

Thus the purpose of raising the above question is not so much to draw attention to a problem that is already well known, but rather to justify the coinage "premotive" and the use of the term *motivic L-function* for the L-function associated to a premotive. By postulating a connection with motives we also justify the notations h^{pq} and $h^{p\pm}$ in (3.42) and (3.43), because if M does come from a motive then the gamma factor $L_\infty(s, M)$ of $L(s, M)$ is given by (3.41) with h^{pq} and $h^{p\pm}$ equal to the usual Hodge numbers; cf. [**16**], p. 329. More precisely, h^{pq} is the usual Hodge number and $h^{p\pm}$ is the multiplicity of the eigenvalue $(-1)^p(\pm 1)$ of the "Frobenius at infinity" – in other words, of complex conjugation – on H^{pp}.

That said, we will continue to try to get as much information as possible from the family of λ-adic representations itself without reference to a possible underlying motive. In particular, we would like to write $A(M)$ and $W(M)$ as products of local factors. The first step is to introduce the local Weil and Weil-Deligne groups and show how a premotive M gives rise to a local representation over $\mathbb{C}$ at every finite place.

6. The local Weil and Weil-Deligne groups

We switch temporarily from a global setting to a local nonarchimedean setting. Thus K is now a finite extension of $\mathbb{Q}_p$ with $p < \infty$. We write $\mathcal{O}$ for the ring of integers of K and π for a uniformizer of $\mathcal{O}$, and we put $q = |\mathcal{O}/\mathfrak{p}\mathcal{O}|$. The maximal unramified extension of K inside $\overline{K}$ will be denoted $K_{\rm unr}$, and any element $\sigma \in \mathrm{Gal}(\overline{K}/K)$ which reduces to the map $x \mapsto x^q$ on $\mathcal{O}/\pi\mathcal{O}$ will be called a Frobenius element of $\mathrm{Gal}(\overline{K}/K)$. The symbol Φ denotes the inverse of a Frobenius element, and I is the inertia group $\mathrm{Gal}(\overline{K}/K_{\rm unr})$.

6.1. The Weil group

As an abstract group, the **Weil group** $\mathrm{W}(\overline{K}/K)$ of K is the union of the cosets of I represented by powers of a Frobenius element:

$$\mathrm{W}(\overline{K}/K) = \bigcup_{n\in\mathbb{Z}} \sigma^n I. \tag{3.48}$$

Since I is normal in $\mathrm{Gal}(\overline{K}/K)$, the union is a subgroup of $\mathrm{Gal}(\overline{K}/K)$, and since any two Frobenius elements differ by an element of I the definition (3.48) is independent of the choice of σ. We topologize $\mathrm{W}(\overline{K}/K)$ by imposing two requirements:

- I is open in $\mathrm{W}(\overline{K}/K)$, and the relative topology on I from $\mathrm{W}(\overline{K}/K)$ coincides with its relative topology from $\mathrm{Gal}(\overline{K}/K)$.
- For every $g \in \mathrm{W}(\overline{K}/K)$, the map $x \mapsto gx$ is a homeomorphism from $\mathrm{W}(\overline{K}/K)$ to itself.

These conditions determine a unique topology on $\mathrm{W}(\overline{K}/K)$ making $\mathrm{W}(\overline{K}/K)$ into a topological group. The most important property of this topology, immediate from its definition, is that *an abstract group homomorphism from* $\mathrm{W}(\overline{K}/K)$ *into another topological group is continuous if and only its restriction to* I *is continuous.* We also note that if L is a finite extension of K inside $\overline{K}$ then $\mathrm{W}(\overline{K}/L)$ is an open subgroup of $\mathrm{W}(\overline{K}/K)$ just as $\mathrm{Gal}(\overline{K}/L)$ is an open subgroup of $\mathrm{Gal}(\overline{K}/K)$, and if

L is Galois over K then there are identifications

$$\mathrm{W}(\overline{K}/K)/\mathrm{W}(\overline{K}/L) \cong \mathrm{Gal}(\overline{K}/K)/\mathrm{Gal}(\overline{K}/L) \cong \mathrm{Gal}(L/K). \tag{3.49}$$

However the open subgroups of $\mathrm{Gal}(\overline{K}/K)$ are *precisely* the subgroups $\mathrm{Gal}(\overline{K}/L)$ with L finite over K, whereas the subgroups $\mathrm{W}(\overline{K}/L)$ of $\mathrm{W}(\overline{K}/K)$ are merely the open subgroups *of finite index*.

A character of $\mathrm{W}(\overline{K}/K)$ is **unramified** if its restriction to I is trivial. Of particular importance is the unramified character ω of $\mathrm{W}(\overline{K}/K)$ such that $\omega(\sigma) = q$. The similarity to the notation ω_ℓ for the ℓ-adic cyclotomic character is not coincidental. We introduced ω_ℓ as a character of a global Galois group, but if we restrict to a decomposition group then we obtain a character of our local Galois group $\mathrm{Gal}(\overline{K}/K)$. Restricting further to $\mathrm{W}(\overline{K}/K)$, and making the assumption $\ell \neq p$, we get our present ω, because both ω and $\omega_\ell|\mathrm{W}(\overline{K}/K)$ are unramified characters taking the value q on Frobenius elements. We may think of ω as the **prime-to-p cyclotomic character.**

We write $\mathrm{W}(\overline{K}/K)^{\mathrm{ab}}$ for the quotient of $\mathrm{W}(\overline{K}/K)$ by the closure of its commutator subgroup, or equivalently for the quotient of $\mathrm{W}(\overline{K}/K)$ by $\mathrm{Gal}(\overline{K}/K^{\mathrm{ab}}) \cap \mathrm{W}(\overline{K}/K)$. The latter description realizes $\mathrm{W}(\overline{K}/K)^{\mathrm{ab}}$ as a subgroup of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$, and we shall denote this subgroup $\mathrm{W}(K^{\mathrm{ab}}/K)$. One pleasant feature of $\mathrm{W}(\overline{K}/K)$ that distinguishes it from $\mathrm{Gal}(\overline{K}/K)$ is that the **local reciprocity law homomorphism** $x \mapsto (x, K^{\mathrm{ab}}/K)$ from $K^\times$ to $\mathrm{W}(K^{\mathrm{ab}}/K)$ is an isomorphism rather than merely an injective homomorphism with dense image. This means in particular that the one-dimensional characters of $K^\times$ can be identified with those of $\mathrm{W}(\overline{K}/K)$. Since we are now following the "geometric convention," the identification takes the form

$$\chi((x, K^{\mathrm{ab}}/K)) = \chi(x^{-1}) \qquad (x \in K^\times). \tag{3.50}$$

For example, when the prime-to-p cyclotomic character ω of $\mathrm{W}(\overline{K}/K)$ is viewed as a character of $K^\times$ it coincides with $||*||$, the local norm on $K^\times$.

6.2. The Weil-Deligne group

Our point of view with regard to the **Weil-Deligne group** $\mathrm{WD}(\overline{K}/K)$ of K will in the first instance be tannakian: Instead of defining $\mathrm{WD}(\overline{K}/K)$ itself we define its representations. By definition, a **representation of** $\mathrm{WD}(\overline{K}/K)$ is a pair $\boldsymbol{\rho} = (\rho, N)$, where ρ is a representation of $\mathrm{W}(\overline{K}/K)$ and N is a nilpotent endomorphism of the space of ρ satisfying the relation

$$\rho(g) N \rho(g)^{-1} = \omega(g) N \tag{3.51}$$

for $g \in \mathrm{W}(\overline{K}/K)$. Henceforth representations of $\mathrm{W}(\overline{K}/K)$ are to be viewed as a special case of representations of $\mathrm{WD}(\overline{K}/K)$, namely the case $N = 0$. In other words, we identify a representation ρ of $\mathrm{W}(\overline{K}/K)$ with the representation $\boldsymbol{\rho} = (\rho, 0)$ of $\mathrm{WD}(\overline{K}/K)$.

The L-factor of a representation of $\mathrm{WD}(\overline{K}/K)$ over $\mathbb{C}$ is defined as follows. Let $\boldsymbol{\rho} = (\rho, N)$ be the representation, V its space,and V_N the kernel of N, and put

$$V_N^I = V^I \cap V_N. \tag{3.52}$$

The relation $\rho(g)N = \omega(g)N\rho(g)$ for $g \in \mathrm{W}(\overline{K}/K)$ shows that V_N^I is stable under ρ, and the **L-factor** associated to $\boldsymbol{\rho}$ is the meromorphic function

$$L(s, \boldsymbol{\rho}) = \det(1 - q^{-s}\rho(\Phi)|V_N^I), \tag{3.53}$$

where $\Phi \in \mathrm{W}(\overline{K}/K)$ is an inverse Frobenius element. Since V_N^I is a subspace of the space of inertial invariants of ρ, the definition of $L(s, \boldsymbol{\rho})$ is independent of the choice of Φ.

The following simple remark will be needed later and for the moment can serve to illustrate the definitions. We say that two endomorphisms of a finite-dimensional vector space V are **simultaneously triangularizable** if there is a basis for V relative to which both endomorphisms are represented by upper triangular matrices.

Proposition 3.3. *Let $\boldsymbol{\rho} = (\rho, N)$ be a representation of $\mathrm{WD}(\overline{K}/K)$ over $\mathbb{C}$ and g any element of $\mathrm{W}(\overline{K}/K)$. Then $\rho(g)$ and N are simultaneously triangularizable.*

Proof. This is a straightforward generalization of the standard proof that commuting matrices are simultaneously triangularizable. In fact let V be a finite-dimensional vector space over an algebraically closed field, and let A and N be endomorphisms of V satisfying $AN = cNA$ with a nonzero scalar c. Suppose N is nilpotent and let V_N denote its kernel. We prove that A and N are simultaneously triangularizable by induction on the dimension of V. If $\dim V = 1$ there is nothing to prove. If $\dim V = n \geqslant 2$ then we use the identity $AN = cNA$, which shows that V_N is stable under A. Furthermore $V_N \neq \{0\}$ because N is nilpotent. Let $v_1 \in V_N$ be a nonzero eigenvector of A and W its span. Applying the inductive hypothesis to the endomorphisms of V/W determined by A and N, we obtain a basis $v_2+W, v_3+W, \dots, v_n+W$ for V/W relative to which the latter endomorphisms are upper-triangular, and then $v_1, v_2, \dots, v_n$ do the same for A and N. □

6.3. The Weil-Deligne group and the standard operations of representation theory

Since a representation of $\mathrm{WD}(\overline{K}/K)$ as defined above is not quite a group representation in the usual sense, we should be clear on how the standard operations of representation theory work for representations of $\mathrm{WD}(\overline{K}/K)$.

If $\boldsymbol{\rho}' = (\rho', N')$ is another representation of $\mathrm{WD}(\overline{K}/K)$ then we define the **direct sum** of $\boldsymbol{\rho}$ and $\boldsymbol{\rho}'$ by

$$\boldsymbol{\rho} \oplus \boldsymbol{\rho}' = (\rho \oplus \rho', N \oplus N') \tag{3.54}$$

and their **tensor product** by

$$\boldsymbol{\rho} \otimes \boldsymbol{\rho}' = (\rho \otimes \rho', N \otimes 1' + 1 \otimes N'), \tag{3.55}$$

where 1 and $1'$ denote the identity automorphism of the space of $\boldsymbol{\rho}$ and $\boldsymbol{\rho}'$ respectively.

In particular, if ρ is a representation over $\mathbb{C}$ then for $c \in \mathbb{C}$ we have

$$\boldsymbol{\rho} \otimes \omega^c = (\rho \otimes \omega^c, N). \tag{3.56}$$

This follows from (3.55) in view of our identification of ω with $\boldsymbol{\omega} = (\omega, 0)$.

Let $\boldsymbol{\rho}$ and $\boldsymbol{\rho}'$ be arbitrary representations of $\mathrm{WD}(\overline{K}/K)$ again. We define an **intertwining map** or **homomorphism of representations** from $\boldsymbol{\rho}$ to $\boldsymbol{\rho}'$ to be a linear map T from the space of $\boldsymbol{\rho}$ to the space of $\boldsymbol{\rho}'$ which intertwines ρ with ρ' and N with N': In other words, $T \circ \rho = \rho' \circ T$ and $TN = NT'$. An intertwining map which is a linear isomorphism is an **isomorphism of representations**.

Next we consider operations on a single representation $\boldsymbol{\rho}$. The **dual** $\boldsymbol{\rho}^\vee$ of $\boldsymbol{\rho}$ is defined by

$$\boldsymbol{\rho}^\vee = (\rho^\vee, -N^\vee), \tag{3.57}$$

where $N^\vee$ is the transpose of N: If V is the space of $\boldsymbol{\rho}$ and $V^\vee$ the space of linear forms on V then $N^\vee(f) = f \circ N$ for $f \in V^\vee$.

If L is a finite extension of K inside $\overline{K}$ then we define the **restriction** of $\boldsymbol{\rho}$ to $\mathrm{WD}(\overline{K}/L)$ by

$$\mathrm{res}_{L/K}\boldsymbol{\rho} = (\mathrm{res}_{L/K}\rho, N), \tag{3.58}$$

where $\mathrm{res}_{L/K}\rho = \rho|\mathrm{WD}(\overline{K}/L)$.

Finally, let us change notation slightly and take $\boldsymbol{\rho}$ to be a represe ntation of $\mathrm{WD}(\overline{K}/L)$, where L is a finite extension of K as before. We would like to define the **induced representation** $\mathrm{ind}_{L/K}\boldsymbol{\rho}$ of $\mathrm{WD}(\overline{K}/K)$. To do so, let V be the space of $\boldsymbol{\rho}$ and put $G = \mathrm{WD}(\overline{K}/K)$ and $H = \mathrm{WD}(\overline{K}/L)$. Then ρ makes V into an H-module, and the space $\mathbb{C}[G] \otimes_{\mathbb{C}[H]} V$ (or the analogous space with $\mathbb{C}$ replaced by the appropriate field of scalars) is a standard model for the space of $\mathrm{ind}_{L/K}\rho$. We set

$$\mathrm{ind}_{L/K}\boldsymbol{\rho} = (\mathrm{ind}_{L/K}\rho, \omega^{-1} \cdot (1 \otimes N)), \tag{3.59}$$

where the endomorphism $\omega^{-1} \cdot (1 \otimes N)$ of $\mathbb{C}[G] \otimes_{\mathbb{C}[H]} V$ is defined by its effect on pure tensors:

$$\omega^{-1} \cdot (1 \otimes N)(g \otimes v) = \omega^{-1}(g)(g \otimes Nv) \tag{3.60}$$

for $g \in G$ and $v \in V$.

To carry out the verifications associated with (3.59) and (3.60), it is helpful to put a subscript on ω: Our current ω is ω_K, and the prime-to-p cyclotomic character of $\mathrm{W}(\overline{K}/L)$ will be denoted ω_L. The relationship between them is that $\omega_K|\mathrm{W}(\overline{K}/L) = \omega_L$. To see that $\omega^{-1} \cdot (1 \otimes N)$ is well defined, we must examine (3.60) when $g \otimes v$ is rewritten as $gh \otimes \rho(h)^{-1}g$ with $h \in H$. According to (3.60), we get

$$\omega^{-1} \cdot (1 \otimes N)(gh \otimes \rho(h)^{-1}g) = \omega_K^{-1}(gh)(gh \otimes N\rho(h)^{-1}). \tag{3.61}$$

Since $gh \otimes N\rho(h)^{-1} = g \otimes \omega_L(h)N$ we see that (3.61) does give the same result as (3.60).

Now put $\boldsymbol{\varphi} = \mathrm{ind}_{L/K}\boldsymbol{\rho}$, $\varphi = \mathrm{ind}_{L/K}\rho$, and $M = \omega^{-1} \cdot (1 \otimes N)$. To verify that $\boldsymbol{\varphi}$ satisfies the required identity $\varphi(g)M\varphi(g)^{-1} = \omega_K(g)M$ for $g \in G$, we compare the effect of both sides on pure tensors. Since $\varphi(g)^{-1}(g' \otimes v) = (g^{-1}g' \otimes v)$, (3.60) gives $M\varphi(g)^{-1}(g' \otimes v) = \omega_K(g')^{-1}\omega_K(g)(g^{-1}g' \otimes Nv)$, whence $\varphi(g)M\varphi(g)^{-1}(g' \otimes v)$ is indeed $\omega_K(g)M(g' \otimes v)$.

This completes our discussion of the standard operations. We'll let the cat out of the bag now and define $\mathrm{WD}(\overline{K}/K)$ itself: $\mathrm{WD}(\overline{K}/K) = \mathbb{C} \rtimes \mathrm{W}(\overline{K}/K)$, where $gzg^{-1} = \omega(g)z$ for $g \in \mathrm{W}(\overline{K}/K)$ and $z \in \mathbb{C}$. However one is supposed to think of the factor $\mathbb{C}$ of $\mathbb{C} \rtimes \mathrm{W}(\overline{K}/K)$ as the set of points over $\mathbb{C}$ of the algebraic group $\mathbb{G}_\mathrm{a}$, the additive group. Hence a representation of $\mathbb{C} \rtimes \mathrm{W}(\overline{K}/K)$ should be algebraic and in particular holomorphic when restricted to the factor $\mathbb{C}$. Using this fact, one can show that a representation $\boldsymbol{\rho}$ of $\mathrm{WD}(\overline{K}/K)$ has the form $zg \mapsto \exp(zN)\rho(g)$, where ρ is a representation of $\mathrm{W}(\overline{K}/K)$ and N a nilpotent endomorphism of the space of ρ. This not only explains the identification of $\boldsymbol{\rho}$ with the pair (ρ, N) but also shows

(after some calculation) that the definitions given above for $\oplus$, $\otimes$, and so on are just the standard operations of representation theory applied to representations of $\mathbb{C} \rtimes \mathrm{W}(\overline{K}/K)$.

6.4. Tame inertia

Two remarks about profinite groups and homomorphisms between profinite groups are useful at this juncture. As always with topological groups, a homomorphism of profinite groups is understood to be continuous.

The first remark is that if q and ℓ are distinct prime numbers then every homomorphism from a pro-q-group to a pro-ℓ-group is trivial. Given the definition of the profinite topology, this is a straightforward consequence of the fact that a homomorphism from a finite q-group to a finite ℓ-group is trivial.

The second remark is that if g is an element of a pro-ℓ-group G and z is any element of $\mathbb{Z}_\ell$ then g^z is a well-defined element of G: the obvious element if $z \in \mathbb{Z}$, and the limit of a convergent sequence in general. In particular, suppose that G is a procyclic pro-ℓ-group, so that there is an isomorphism $t : G \to \mathbb{Z}_\ell$. If G is written multiplicatively and $g_0 = t^{-1}(1)$ then $g = g_0^{t(g)}$ for all $g \in G$. One consequence is that if Γ is an arbitrary pro-ℓ-group written multiplicatively then a homomorphism $f : G \to \Gamma$ is necessarily of the form $f(g) = \gamma^{t(g)}$, where $\gamma = f(g_0)$. This last consequence is of particular use to us when combined with the observation that the vector space of homomorphisms $G \to \mathbb{Q}_\ell$ has dimension one over $\mathbb{Q}_\ell$. Thus any nonzero homomorphism $t' : G \to \mathbb{Q}_\ell$ is a scalar multiple of t, and therefore f also has the form $f(g) = \gamma^{ct'(g)}$ with $c \in \mathbb{Q}_\ell$.

Let us now return to K, a finite extension of $\mathbb{Q}_p$ with $p < \infty$. We write K_{tame} for the maximal tamely ramified extension of K inside $\overline{K}$, and we put $P = \mathrm{Gal}(\overline{K}/K_{\mathrm{tame}})$. If we fix a uniformizer ϖ of K_{unr} then K_{tame} can be described as the compositum of all extensions of K_{unr} of the form $K_{\mathrm{unr}}(\varpi^{1/n})$ with positive integers n prime to p. Kummer theory then an identification of $\mathrm{Gal}(K_{\mathrm{unr}}(\varpi^{1/n})/K_{\mathrm{unr}})$ with $\mathbb{Z}/n\mathbb{Z}$ and hence an identification

$$I/P \cong \prod_{\ell \neq p} \mathbb{Z}_\ell \tag{3.62}$$

after taking inverse limits. Since P is a pro-p-group it follows that if $\ell \neq p$ then the space of homomorphisms $I \to \mathbb{Q}_\ell$ has dimension one over $\mathbb{Q}_\ell$. In fact this conclusion holds with I replaced by an arbitrary open subgroup J of I, because any open subgroup of the right-hand side of (3.62) is again isomorphic to the right-hand side of (3.62).

The theorem below combines results of Grothendieck and Deligne. To state it, we fix a nonzero homomorphism $t_\ell : I \to \mathbb{Q}_\ell$ and a Frobenius element $\sigma \in \mathrm{W}(\overline{K}/K)$. Since t_ℓ is unique only up to a scalar multiple and σ only up to multiplication by an element of I, it is important to remark that the isomorphism class of the representation $\boldsymbol{\rho}$ of $\mathrm{W}(\overline{K}/K)$ in the theorem is independent of the choice of t_ℓ and σ. However we shall not prove this remark, because we will prove a much stronger type of independence assertion when we return to the global setting later on. However, by way of motivation we point out that a connection between t_ℓ and $\mathrm{WD}(\overline{K}/K)$ is suggested already by the identity

$$t_\ell(gig^{-1}) = \omega(g)t_\ell(i), \tag{3.63}$$

where g and i denote arbitrary elements of $\mathrm{W}(\overline{K}/K)$ and I respectively (use the Kummer pairing for the extension $K_{\mathrm{unr}}(\varpi^{1/n})/K_{\mathrm{unr}}$ and take inverse limits). The precise connection is as follows:

Theorem 3.1. *Let $\mathbb{E}_\lambda$ be a finite extension of $\mathbb{Q}_\ell$ with $\ell \neq p$, and let ρ_λ be a representation of $\mathrm{Gal}(\overline{K}/K)$ over $\mathbb{E}_\lambda$.*

(a) There is a unique nilpotent endomorphism N of the space of ρ_λ such that

$$\rho_\lambda(i) = \exp(t_\ell(i)N)$$

for all i in some open subgroup of I. Furthermore, consider the function ρ on $\mathrm{W}(\overline{K}/K)$ defined by setting

$$\rho(g) = \exp(-t_\ell(i)N)\rho_\lambda(g)$$

for $g = i\sigma^n$ with $i \in I$ and $n \in \mathbb{Z}$. This function is a representation of $\mathrm{W}(\overline{K}/K)$ on the space of ρ_λ, and the pair $\boldsymbol{\rho} = (\rho, N)$ is a representation of $\mathrm{WD}(\overline{K}/K)$.

(b) Let ρ and N be as in (a), and for each $g \in \mathrm{W}(\overline{K}/K)$ let $\rho^{\mathrm{ss}}(g)$ be the semisimple component of $\rho(g)$ in a multiplicative Jordan decomposition of $\rho(g)$. Then the map $g \mapsto \rho^{\mathrm{ss}}(g)$ is a semisimple representation of $\mathrm{W}(\overline{K}/K)$ trivial on an open subgroup of I, and the pair $\boldsymbol{\rho}^{\mathrm{ss}} = (\rho^{\mathrm{ss}}, N)$ is a representation of $\mathrm{WD}(\overline{K}/K)$.

Proof. (a) Let $\mathcal{O}_\lambda$ be the ring of integers of $\mathbb{E}_\lambda$. By Exercise 3.3, we may think of ρ_λ as a map $\mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_d(\mathcal{O}_\lambda)$. Let $\Gamma \subset \mathrm{GL}_d(\mathcal{O}_\lambda)$ be the subgroup consisting of matrices congruent to 1 mod ℓ^2. Then Γ is a pro-ℓ-group and an open normal subgroup of $\mathrm{GL}_d(\mathcal{O}_\lambda)$. Consequently the subgroup $J = I \cap \rho_\lambda^{-1}(\Gamma)$ is an open normal subgroup of I and $\rho_\lambda|J$ is a homomorphism of J into a pro-ℓ-group. Choose $c \in \mathbb{Q}_\ell$ such that $ct_\ell|J$ is a surjection of J onto $\mathbb{Z}_\ell$. Then there exists $\gamma \in \Gamma$ and such that $\rho_\lambda(j) = \gamma^{ct_\ell(j)}$ for $j \in J$. As γ is congruent to 1 mod ℓ^2, it is in the image of the ℓ-adic exponential map on $d \times d$ matrices with coefficients in $\ell^2\mathcal{O}_\lambda$. In fact on this domain the exponential is a bijection onto Γ. Thus we can write $\rho_\lambda(j) = \exp(t_\ell(j)N)$ for a unique $d \times d$ matrix N over $\mathbb{E}_\lambda$, and it follows from (3.63) that if $g \in \mathrm{W}(\overline{K}/K)$ then $\rho_\lambda(gjg^{-1}) = \exp(\omega(g)t_\ell(j)N)$. But if we simply conjugate the equation $\rho_\lambda(j) = \exp(t_\ell(j)N)$ by $\rho_\lambda(g)$ then we get a second expression for $\rho_\lambda(gjg^{-1})$, namely $\exp(t_\ell(j)\rho_\lambda(g)N\rho_\lambda(g)^{-1})$, so the uniqueness of N implies that $\rho_\lambda(g)N\rho_\lambda(g)^{-1} = \omega(g)N$. This identity immediately carries over to the identity $\rho(g)N\rho(g)^{-1} = \omega(g)N$ if we define ρ as in the statement of the theorem. And by taking $g = \sigma^\nu$ with $\nu \in \mathbb{Z}$ we deduce that N is nilpotent, for if N has a nonzero eigenvalue r then N has infinitely many eigenvalues, namely the numbers rq^ν.

To complete the proof of (a) we must check that ρ is a homomorphism. So suppose that $g = i\sigma^n$ and $g' = h\sigma^m$ with $m, n \in \mathbb{Z}$ and $h, i \in I$. Then

$$\rho(gg') = \exp(-t_\ell(i) - q^n t_\ell(h))\rho_\lambda(gg') \tag{3.64}$$

while

$$\rho(g)\rho(g') = \exp(-t_\ell(i)N)\rho_\lambda(g)\exp(-t_\ell(h)N)\rho_\lambda(g'). \tag{3.65}$$

The identity $\rho_\lambda(g)N\rho_\lambda(g_)^{-1} = \omega(g)N$ shows that the right-hand sides of (3.64) and (3.65) are equal, whence $\rho(gg') = \rho(g)\rho(g')$.

(b) Let J be the kernel of $\rho|I$. Since I is normal in $\mathrm{W}(\overline{K}/K)$ so is J. Furthermore J is open in I, because it is the subgroup of I on which ρ_λ coincides with the map $i \mapsto \exp(t_\ell(i)N)$. It follows that I/J is a finite normal subgroup of

$\mathrm{W}(\overline{K}/K)/J$, and consequently the action of $\mathrm{W}(\overline{K}/K)/J$ on I/J by conjugation gives a map from $\mathrm{W}(\overline{K}/K)$ to the finite group $\mathrm{Aut}(I/J)$. Hence the kernel of this map has finite index in $\mathrm{W}(\overline{K}/K)$, and there is an integer $d \geqslant 1$ such that σ^d acts trivially on I/J. Since ρ factors through $\mathrm{W}(\overline{K}/K)/J$, we deduce that $\rho(\sigma^d)$ centralizes $\rho(I)$. But $\rho(\sigma^d)$ certainly commutes with $\rho(\sigma)$, so $\rho(\sigma^d)$ centralizes the image of ρ.

Now let u be the unipotent Jordan component of $\rho(\sigma)$. Then u^d is the unipotent Jordan component of $\rho(\sigma^d)$. Thus $u^d = \rho(\sigma^d)\rho^{\mathrm{ss}}(\sigma^d)^{-1}$; but $\rho^{\mathrm{ss}}(\sigma^d)$ is a polynomial in $\rho(\sigma^d)$, and since $\rho(\sigma^d)$ centralizes the image of ρ it follows that $\rho^{\mathrm{ss}}(\sigma^d)$ does too, hence also u^d. Using the binomial series for $(1+x)^{1/d}$, we see that u is a polyomial in u^d, so we conclude that u centralizes the image of ρ.

Next consider an arbitrary element $g \in \mathrm{W}(\overline{K}/K)$, and write $g = i\sigma^n$ with $i \in I$ and $n \in \mathbb{Z}$. Let $\rho^{\mathrm{u}}(g)$ denote the unipotent Jordan component of $\rho(g)$; we claim that $\rho^{\mathrm{u}}(g) = u^n$. Since $\rho^{\mathrm{u}}(g^d) = \rho^{\mathrm{u}}(g)^d$ and unipotent automorphisms have unique unipotent dth roots, it suffices to see that $\rho^{\mathrm{u}}(g^d) = u^{nd}$. But $\rho(g^d) = \rho(i')\rho(\sigma^{nd})$ for some $i' \in I$ and $\rho(\sigma^{nd}) = \rho^{\mathrm{ss}}(\sigma^{nd})u^{nd}$, so

$$\rho(g^d) = (\rho(i')\rho^{\mathrm{ss}}(\sigma^{nd})) \cdot u^{nd}. \tag{3.66}$$

We contend that (3.66) is the multiplicative Jordan decomposition of $\rho(g^d)$, whence $\rho^{\mathrm{u}}(g^d) = u^{nd}$, as desired. As u^{nd} is unipotent and commutes with $\rho(i')\rho^{\mathrm{ss}}(\sigma^{nd})$ it suffices to see that $\rho(i')\rho^{\mathrm{ss}}(\sigma^{nd})$ is semisimple. But $\rho(i')$ is semisimple because $\rho|I$ factors through the finite group I/J, and $\rho^{\mathrm{ss}}(\sigma^{nd})$ is semisimple and commutes with $\rho(i')$. Hence $\rho(i')\rho^{\mathrm{ss}}(\sigma^{nd})$ is indeed semisimple, and we conclude that $\rho^{\mathrm{u}}(g) = u^n$.

We can now show that ρ^{ss} is a representation (necessarily trivial on J because ρ is). Given $g, h \in \mathrm{W}(\overline{K}/K)$, write $g = i\sigma^n$ and $g' = h\sigma^m$ with $m, n \in \mathbb{Z}$ and $h, i \in I$. Then $\rho^{\mathrm{ss}}(g)\rho^{\mathrm{ss}}(g') = \rho(g)u^{-n}\rho(g')u^{-m} = \rho(gg')u^{-(n+m)} = \rho^{\mathrm{ss}}(gg')$, where the last equality follows from the fact that $gg' = i'\sigma^{n+m}$ for some $i' \in I$, whence $u^{n+m} = \rho^{\mathrm{u}}(gg')$.

To see that ρ^{ss} is semisimple we quote a general fact: A representation of a group over a field of characteristic 0 is semisimple if and only if its restriction to a subgroup of finite index is semisimple. In the case at hand, the infinite cyclic group $\langle\sigma\rangle$ generated by σ is of finite index in $\mathrm{W}(\overline{K}/K)/J$, and $\rho^{\mathrm{ss}}|\langle\sigma\rangle$ is semisimple by the very definition of ρ^{ss}.

Finally, we must check the identity $\rho^{\mathrm{ss}}(g)N\rho^{\mathrm{ss}}(g)^{-1} = \omega(g)N$. Since we already know that $\rho(g)N\rho(g)^{-1} = \omega(g)N$, it will suffice to see that u commutes with N. Denote the adjoint representation of $\mathrm{GL}(U)$ on $\mathrm{End}(U)$ by Ad, so that $\mathrm{Ad}(x)(y) = xyx^{-1}$ for $x \in \mathrm{GL}(U)$ and $y \in \mathrm{End}(U)$. It is readily verified that $\mathrm{Ad}(x)^{\mathrm{ss}} = \mathrm{Ad}(x^{\mathrm{ss}})$ and $\mathrm{Ad}(x)^{\mathrm{u}} = \mathrm{Ad}(x^{\mathrm{u}})$. In particular, since $\mathrm{Ad}(x)^{\mathrm{u}}$ is a polynomial in $\mathrm{Ad}(x)$, we see that any eigenvector of $\mathrm{Ad}(x)$ is also an eigenvector of $\mathrm{Ad}(x^{\mathrm{u}})$. Apply the preceding remark with $x = \rho(\sigma)$ and $x^{\mathrm{u}} = u$. The relation $\rho(\sigma)N\rho(\sigma)^{-1} = qN$ shows that N is an eigenvector of $\mathrm{Ad}(\rho(\sigma))$ and hence of $\mathrm{Ad}(u)$. But $\mathrm{Ad}(u)$ is $\mathrm{Ad}(\rho(\sigma))^{\mathrm{u}}$ and therefore unipotent; its eigenvalues equal 1. Thus N is an eigenvector of $\mathrm{Ad}(u)$ with eigenvalue 1; in other words, u commutes with N. □

7. From compatible families to local representations

We return to the global setting. Thus K is a number field again and M a premotive over K. Fix a finite place v of K. Our goal is to see how M determines the isomorphism class of a representation $\boldsymbol{\rho}_{M,v}$ of $\mathrm{WD}(\overline{K}_v/K_v)$ over $\mathbb{C}$.

Write p for the residue characteristic of v. We fix a place of $\overline{K}$ over v and identify the corresponding decomposition subgroup of $\mathrm{Gal}(\overline{K}/K)$ with $\mathrm{Gal}(\overline{K_v}/K_v)$. By restriction to the decomposition subgroup, any representation of $\mathrm{Gal}(\overline{K}/K)$ gives rise to a representation of $\mathrm{Gal}(\overline{K_v}/K_v)$, and the isomorphism class of the latter representation is independent of the choice of place of $\overline{K}$ over v.

We apply the preceding remark to the members of a fully compatible family $\{\rho_\lambda\} \in M$. Write $\mathbb{E}$ for the coefficient field of this family. If the residue characteristic of λ is a prime $\ell \neq p$ then the restriction $\rho_{\lambda,v} = \rho_\lambda|\mathrm{Gal}(\overline{K_v}/K_v)$ is a representation to which we may apply Theorem 3.1. The result is a representation $\boldsymbol{\rho}^{\mathrm{ss}} = (\rho^{\mathrm{ss}}, N)$ of $\mathrm{WD}(\overline{K_v}/K_v)$. over $\mathbb{E}_\lambda$. To obtain a representation over $\mathbb{C}$, fix an abstract field embedding ι of $\mathbb{E}_\lambda$ in $\mathbb{C}$. Since we regard $\mathbb{E}$ as a subfield both of $\mathbb{E}_\lambda$ and of $\mathbb{C}$, we can require ι to be the identity on $\mathbb{E}$. Extending scalars from $\mathbb{E}_\lambda$ to $\mathbb{C}$ via ι, we obtain a representation $((\rho^{\mathrm{ss}})^\iota, N^\iota)$ of $\mathrm{WD}(\overline{K_v}/K_v)$ over $\mathbb{C}$. At first glance this seems like the obvious candidate for $\boldsymbol{\rho}_{M,v}$. However when $\boldsymbol{\rho}_{M,v}$ is defined in this way then I do not know how to show that its isomorphism class is independent of the choice of λ and ι. I also do not know of any place in the literature where it is claimed that the desired independence holds. Fortunately, there is a way of modifying N so that we do get a representation $\boldsymbol{\rho}_{M,v}$ of $\mathrm{WD}(\overline{K_v}/K_v)$ over $\mathbb{C}$ which up to isomorphism is independent of the choice of λ and ι. Furthermore, the modification is innocuous in the sense that it does not affect the local conductor and local root number which we ultimately wish to extract from $\boldsymbol{\rho}_{M,v}$.

To describe the modification, let V be the space of ρ^{ss} and observe that since ρ^{ss} is semisimple, the sum of any collection of its isotypic components has a unique invariant complement. In particular, since V^I is the sum of the isotypic components of the *unramified* irreducible representations of $\mathrm{W}(\overline{K_v}/K_v)$ over $\mathbb{E}_\lambda$, there is a unique invariant subspace W of V such that $V = V^I \oplus W$. Of course W is just the sum of the isotypic components of the ramified irreducible representations. In any case, the desired modification of N is the nilpotent endomorphism N^* of V which coincides with N on V^I and with 0 on W. The pair $(\rho^{\mathrm{ss}}, N^*)$ is still a representation of $\mathrm{WD}(\overline{K_v}/K_v)$ over $\mathbb{E}_\lambda$, because on V^I the relation $\rho^{\mathrm{ss}}(g)N^*\rho^{\mathrm{ss}}(g)^{-1} = \omega(g)N$ for $g \in \mathrm{W}(\overline{K_v}/K_v)$ is satisfied as before, and on W the relation is trivial. Let $\boldsymbol{\rho}_{M,v} = ((\rho^{\mathrm{ss}})^\iota, (N^*)^\iota)$ be the representation of $\mathrm{WD}(\overline{K_v}/K_v)$ over $\mathbb{C}$ obtained by applying ι to the matrix coefficients of ρ^{ss} and N^*.

Theorem 3.2. *Up to isomorphism, $\boldsymbol{\rho}_{M,v}$ is independent of the choice of λ and ι.*

Proof. Let $\boldsymbol{\rho} = (\rho, N)$ be the representation of $\mathrm{WD}(\overline{K}/K)$ resulting from $\rho_{\lambda,v}$ as in part (a) of Theorem 3.1, and let g denote an arbitrary element of $\mathrm{W}(\overline{K_v}/K_v)$, written as in the theorem. By Proposition 3.3 , there is a basis for the space of ρ relative to which the matrices of $\rho(g)$ and N are both upper triangular. Then $\exp(t_\ell(i)N)$ is also upper triangular and has all diagonal entries equal to 1. Thus it follows from the relation $\rho_{\lambda,v}(g) = \exp(t_\ell(i)N)\rho(g)$ that the characteristic polynomials of $\rho_{\lambda,v}(g)$ and $\rho(g)$ are equal. On the other hand, the characteristic polynomials of $\rho(g)$ and $\rho^{\mathrm{ss}}(g)$ are equal because $\rho^{\mathrm{ss}}(g)$ is the semisimple Jordan component of $\rho(g)$. Now as M satisfies condition C_8, the characteristic polynomial of $\rho_{\lambda,v}(g)$ has coefficients in $\mathbb{E}$ and is independent of λ, and consequently the same is true for the characteristic polynomial of $\rho^{\mathrm{ss}}(g)$. Furthermore this characteristic polynomial is unchanged when ι is used to extend the field of scalars of $\rho(g)$ from $\mathbb{E}_\lambda$ to $\mathbb{C}$, because ι is the identity on $\mathbb{E}$. We conclude that the characteristic polynomial of

$(\rho^{\mathrm{ss}})^\iota(g)$ is independent of the choice of λ and ι. In particular $\operatorname{tr}(\rho^{\mathrm{ss}})^\iota$ is independent of the choice of λ and ι, and since $(\rho^{\mathrm{ss}})^\iota$ is semisimple we conclude that the isomorphism class of $(\rho^{\mathrm{ss}})^\iota$ is independent of the choices as well.

To complete the proof of the theorem we will show that $(N^*)^\iota$ can be described without reference to λ or ι. In fact we shall reconstruct $(N^*)^\iota$ from $(\rho^{\mathrm{ss}})^\iota$ and the polynomial $B_{\mathfrak{p}}(x)$ (3.32), where $\mathfrak{p}$ is the prime ideal corresponding to v. It suffices to reconstruct $(N^*)^\iota$ on V^I, because on the unique complement of V^I in V we have defined N^* to be 0.

To avoid confusion, let us denote the space of $\rho_{\lambda,v}$ by V_λ and the space of $\boldsymbol{\rho} = (\rho, N)$ by V. Then V_λ and V are equal as abstract vector spaces, but by making the distinction notationally we can distinguish between V_λ^I and V^I, which are *not* equal. Indeed V_λ^I is the subspace of V_λ consisting of vectors fixed by $\rho_{\lambda,v}(I)$, whereas V^I is the subspace of V consisting of vectors fixed by $\rho(I)$. We claim that the relation between them is

$$V_\lambda^I = V_N^I, \tag{3.67}$$

where as before, V_N is the kernel of N and $V_N^I = V_N \cap V^I$.

To verify (3.67), we return to part (a) of Theorem 3.1, according to which $\rho_{\lambda,v}(i) = \exp(t_\ell(i)N)\rho(i)$ for $i \in I$. The inclusion $V_N^I \subset V_\lambda^I$ is an immediate consequence. For the opposite inclusion, recall from Theorem 3.1 that $\rho_{\lambda,v}(i) = \exp(t_\ell(i)N)$ for all i in some open subgroup of I. Consequently $V_\lambda^I \subset V_N$, whence the inclusion $V_\lambda^I \subset V_N^I$ follows again from the relation $\rho_{\lambda,v}(i) = \exp(t_\ell(i)N)\rho(i)$.

The significance of (3.67) is that by assumption, the coefficients of the characteristic polynomial of $\rho_\lambda(\Phi)|V_\lambda^I$ lie in $\mathbb{E}$ and are independent of λ, because this characteristic polynomial is just $x^n B_{\mathfrak{p}}(x^{-1})$, where $n = \dim V_\lambda^I$. Thus (3.67) tells us that the coefficients of the characteristic polynomial of $\rho(\Phi)|V_N^I$ likewise lie in $\mathbb{E}$ and are independent of λ. Furthermore, this assertion remains true when $\rho(\Phi)|V_N^I$ is replaced by $\rho^{\mathrm{ss}}(\Phi)|V_{N^*}^I$, because $\rho^{\mathrm{ss}}(\Phi)$ and $\rho(\Phi)$ have the same characteristic polynomial and N^* and N coincide on V^I.

Put $U = (\mathbb{C} \otimes_{\mathbb{E}_\lambda} V)^I$, $A = (\rho^{\mathrm{ss}})^\iota(\Phi)|U$ and $J = (N^*)^\iota|U$. We have just seen that the eigenvalues of A on $\ker J$ are independent of the choice of λ and ι. It is also the case that the eigenvalues of A on all of U are independent of λ and ι, because the isomorphism class of $(\rho^{\mathrm{ss}})^\iota$ is independent of these choices and U is an intrinsically defined subspace of the space of $(\rho^{\mathrm{ss}})^\iota$.

Let $d \geqslant 1$ be the size of a Jordan block of maximal size in the Jordan normal form of J, so that $J^d = 0$ and d is minimal with this property. The content of the preceding paragraph is that the eigenvalues of A on $\ker J^i$ are independent of the choice of λ and ι for $i = 1$ and $i = d$. Now by using the relation $AJ = q^{-1}JA$ and induction, we see that $\ker J^i$ is stable under A for any $i \geqslant 1$. As A is semisimple it follows that there is an A-stable complement U_i to $\ker J^{i-1}$ inside $\ker J^i$. Furthermore, for $2 \leqslant i \leqslant d$ the map $u \mapsto Ju$ is an isomorphism of U_i onto its image in $\ker J^{i-1}$, and the image $J(U_i)$ is again stable under A. Since A is semisimple it follows that there is a basis for $J(U_i)$ consisting of eigenvectors of A. Now suppose that $u \in J(U_i)$ is a nonzero eigenvector of A with eigenvalue c, and let u' be its preimage under $J|U_i$. Then the relation $AJ = q^{-1}JA$ shows that u' is also an eigenvector of A, but with eigenvalue qc. By induction, we see in particular that the eigenvalues of $A|U_i$ all have absolute value $q^{i-1}r$, where r is the absolute value of the eigenvalues of $A|\ker J$: these eigenvalues all have the same absolute

value by (3.39) and (3.40). Since

$$U = (\ker J) \oplus U_2 \oplus U_3 \oplus \cdots \oplus U_d \tag{3.68}$$

and the eigenvalues (listed with their multiplicities) of A on $\ker J$ and on all of U are known to be independent of λ and ι, we deduce from (3.68) that the eigenvalues of A on U_i are independent of λ and ι as well, because they are characterized as precisely the eigenvalues of A which are of absolute value $q^{i-1}r$. In particular we have determined the Jordan normal form of J, because the number of Jordan blocks of J of size i is precisely $\dim U_i$, which is also the number of eigenvalues of A of absolute value $q^{i-1}r$. At the same time we have obtained a basis for U relative to which J is in Jordan normal form and A is diagonal. □

8. Exercises

Exercise 3.1. Let L be a finite Galois extension of $\mathbb{Q}$.

(a) Show that $\zeta_L(s) = \prod_\rho L(s,\rho)^{\dim\rho}$, where ρ runs over the distinct isomorphism classes of irreducible complex representations of $\mathrm{Gal}(L/\mathbb{Q})$. (Hint: Let 1_L be the trivial character of $\mathrm{Gal}(L/L)$. Then $\mathrm{ind}_{L/\mathbb{Q}} 1_L$ is the regular representation of $\mathrm{Gal}(L/\mathbb{Q})$.)

(b) Let K be a real quadratic field and η a primitive equivariant Hecke character of K of finite order such that $W(\eta) = -1$. For example, η could be the character in (2.67). Put $\rho = \eta_{\mathrm{Art}}$ and let L be the fixed field of the kernel of ρ. Show that $\zeta_L(s)$ has a zero of order at least 2 at $s = 1/2$.

Remark. The zero of $\zeta_L(s)$ at $s = 1/2$ is not a trivial zero as we have defined the term, because it is not apparent from the functional equation of $\zeta_L(s)$. However the zero at $s = 1/2$ *is* a trivial zero of $L(s,\eta)$. In light of this example one might want to redefine the term *trivial zero* to take account not only of the functional equation of the given L-function but also of the functional equations of factors of the given L-function.

Exercise 3.2. The fact (Theorem 2.2) that $W(\rho) = 1$ if ρ is one-dimensional and either trivial or quadratic is a special case of a theorem of Fröhlich and Queyrut [**22**] asserting that if ρ is any orthogonal Artin representation then $W(\rho) = 1$.

(a) Take $\rho = \mathrm{ind}_{K/\mathbb{Q}}\eta$, where K is a real quadratic field and η a primitive equivariant Hecke character of K of finite order $\geqslant 3$ (η is viewed as a one-dimensional Artin representation of K using (3.5)). Show that ρ is irreducible and self-dual, and deduce from the Fröhlich-Queyrut theorem that if $W(\eta) = -1$ then ρ is symplectic.

(b) (*Pure group theory.*) Show that if G is a group, H a subgroup of index 2, and η a one-dimensional character of H then the determinant of the representation $\rho = \mathrm{ind}_H^G \eta$ is given by

$$\det\rho(g) = \mathrm{sign}_H^G(g)\eta(\mathrm{trans}_H^G(g)) \qquad\qquad (g \in G),$$

where sign_H^G is the nontrivial one-dimensional character of G with kernel H and $\mathrm{trans} : G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ is the transfer (note that η factors throug H^{ab}). For a slightly more general identity see [**14**], p. 508, or [**23**].

(c) With notation as in (a), take η to be the character constructed in (2.67). Show directly – i. e. without applying the Fröhlich-Queyrut theorem – that ρ is symplectic. (Hint: Combine (b) with the fact that a two-dimensional representation is symplectic if and only its determinant is trivial. You will also need to use the fact that under the identification (3.4), the transfer from $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^{\mathrm{ab}}$ to $\mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}}$

corresponds to the natural embedding of $\mathbb{A}_{\mathbb{Q}}^{\times}$ into $\mathbb{A}_K^{\times}$, or rather to the associated map from $C_{\mathbb{Q}}/D_{\mathbb{Q}}$ to C_K/D_K.)

Exercise 3.3. Let $\mathbb{E}$ be a number field, λ a finite place of $\mathbb{E}$, and ρ_λ a λ-adic representation of a compact group G, viewed as a continuous homomorphism $G \to \mathrm{GL}_n(\mathbb{E}_\lambda)$. Prove that ρ_λ is equivalent to a representation into $\mathrm{GL}_n(\mathcal{O}_\lambda)$, where $\mathcal{O}_\lambda$ is the ring of integers of $\mathbb{E}_\lambda$. In other words, show that there exists $u \in \mathrm{GL}_n(\mathbb{E}_\lambda)$ such that $u\rho_\lambda(g)u^{-1} \in \mathrm{GL}_n(\mathcal{O}_\lambda$ for all $g \in G$. (Hint: Let H be the inverse image under ρ_λ of $\mathrm{GL}_n(\mathcal{O}_\lambda)$. Then H is an open subgroup of G and hence of finite index. Viewing $\mathrm{GL}_n(\mathbb{E}_\lambda)$ as the group of linear automorphisms of $\mathbb{E}_\lambda^n$, let $\mathcal{L}$ be the sum of the $\mathcal{O}_\lambda$-submodules $\rho_\lambda(g)(\mathcal{O}_\lambda^n)$ of $\mathbb{Q}_\ell^n$, where g runs over a set of coset representatives for H in G. Show that $\mathcal{L}$ is a G-stable $\mathcal{O}_\lambda$-lattice in $\mathbb{E}_\lambda^n$.)

Exercise 3.4. Let K be a number field, and consider the map $\rho \mapsto \{\rho_\lambda\}_\lambda$ which sends an Artin representation ρ of $\mathrm{Gal}(\overline{K}/K)$ to a fully compatible family of integral λ-adic representations of $\mathrm{Gal}(\overline{K}/K)$. Show that every premotive M of weight 0 over K arises from some Artin representation ρ in this way. (Hint: If M is the isomorphism class of $\{\rho_\lambda\}_\lambda$, then the key point is to show that the image of ρ_λ is finite. By the previous problem, ρ_λ may be viewed as a continuous homomorphism $\mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_n(\mathcal{O}_\lambda)$. Let $\mathbb{F}_\lambda$ be the residue class field of $\mathcal{O}_\lambda$ and ℓ the residue characteristic. Show that the reduction map $\mathrm{GL}_n(\mathcal{O}_\lambda) \to \mathrm{GL}_n(\mathbb{F}_\lambda)$ is injective on elements of order prime to ℓ.)

Exercise 3.5. Let K be a finite extension of $\mathbb{Q}_p$ with $p < \infty$. Show that the open subgroups of infinite index in $\mathrm{W}(\overline{K}/K)$ are precisely the subgroups of the form $\mathrm{Gal}(\overline{K}/R)$ with R a finite extension of K_{unr} inside $\overline{K}$.

LECTURE 4

Local formulas in arbitrary dimension

Let M be a premotive over a number field K. Now that we have defined a representation $\boldsymbol{\rho}_{M,v}$ of $\mathrm{WD}(\overline{K_v}/K_v)$ at every finite place v of K, we can hope to make the factors $A(M)$ and $W(M)$ more explicit by defining them as products over the places of K of local factors associated to representations of $\mathrm{WD}(\overline{K_v}/K)$. In fact this process has already begun: In (3.53) we associated an L-factor $L(s, \boldsymbol{\rho})$ to a representation $\boldsymbol{\rho}$ of $\mathrm{WD}(\overline{K_v}/K)$, and we should now check that

$$L(s, M) = \prod_v L(s, \boldsymbol{\rho}_{M,v}). \tag{4.1}$$

Admittedly, in the case of $L(s, M)$ there is no *need* for the local representations $\boldsymbol{\rho}_{M,v}$ in the sense that the original definition of $L(s, M)$ is as explicit as one might wish. But we certainly wouldn't want to proceed with the program just proposed if (4.1) did *not* hold! Fortunately, a proof of (4.1) is provided by (3.53), (3.67), and the two paragraphs immediately following (3.67).

Our "premotivic" approach to motivic L-functions runs into problems when we attempt to associate an L-factor at infinity to M. If M actually came from a motive then we would could derive $L_\infty(s, M)$ directly from the Hodge realization of M, but as matters stand, we can do no better than the implicit definition of $L_\infty(s, M)$ implicit in Proposition 3.2. For the same reason we cannot give a complete formula for $W(M)$.

1. Local epsilon factors

Let K be a finite extension of $\mathbb{Q}_p$ with $p < \infty$, ψ an additive character of K, dx a Haar measure on K, and $\boldsymbol{\rho} = (\rho, N)$ a representation of $\mathrm{WD}(\overline{K}/K)$. The theory of Langlands and Deligne assigns a nonzero constant $\varepsilon(\boldsymbol{\rho}, \psi, dx)$ to these data. In some treatments $\varepsilon(\boldsymbol{\rho}, \psi, dx)$ is replaced in the first instance by $\varepsilon(\boldsymbol{\rho}, \psi, dx, s)$, a holomorphic function of a complex variable s, and one recovers $\varepsilon(\boldsymbol{\rho}, \psi, dx)$ as in (2.76):

$$\varepsilon(\boldsymbol{\rho}, \psi, dx) = \varepsilon(\boldsymbol{\rho}, \psi, dx, s)|_{s=0}. \tag{4.2}$$

To go in the other direction, one twists by the unramified character $g \mapsto \omega(g)^s$:

$$\varepsilon(\boldsymbol{\rho}, \psi, dx, s) = \varepsilon(\boldsymbol{\rho} \otimes \omega^s, \psi, dx). \tag{4.3}$$

In view of (4.3), there will be no loss of information if we confine our attention to $\varepsilon(\boldsymbol{\rho}, \psi, dx)$. Besides, the current setting is really not analogous to Tate's: In the latter case s was essential, because $\varepsilon(\chi, \psi, dx, s)$ was defined by the local functional equation (2.79), which depends on analytic continuation. In the present context there is no local functional equation.

The first point about $\varepsilon(\boldsymbol{\rho}, \psi, dx)$ is that it is a product of two factors, the first of which depends only on the representation ρ of $\mathrm{W}(\overline{K}/K)$:

$$\varepsilon(\boldsymbol{\rho}, \psi, dx) = \varepsilon(\rho, \psi, dx)\delta(\boldsymbol{\rho}). \tag{4.4}$$

The definition of $\delta(\boldsymbol{\rho})$ is straightforward, so we will mention it first:

$$\delta(\boldsymbol{\rho}) = \det(-\rho(\Phi)|V^I/V_N^I). \tag{4.5}$$

We see that $\delta(\boldsymbol{\rho})$ is indeed independent of ψ and dx, as the notation indicates. If $N = 0$ then $\delta(\boldsymbol{\rho}) = 1$ and therefore $\varepsilon(\boldsymbol{\rho}, \psi, dx) = \varepsilon(\rho, \psi, dx)$.

The definition of $\varepsilon(\rho, \psi, dx)$ is not so straightforward. Before delving into it let us address two points: What will be the dependence of $\varepsilon(\rho, \psi, dx)$ on ψ and dx? And what information does $\varepsilon(\boldsymbol{\rho}, \psi, dx)$ contain?

The dependence of $\varepsilon(\rho, \psi, dx)$ on ψ and dx is summarized in the following formulas, where for $b \in K^\times$ we put $\psi_b(x) = \psi(bx)$ as before:

$$\varepsilon(\rho, \psi_b, dx) = \det \rho(b)||b||^{-\dim\rho}\varepsilon(\psi, dx) \tag{4.6}$$

and

$$\varepsilon(\rho, \psi, c\,dx) = c^{\dim\rho}\varepsilon(\rho, \psi, dx). \tag{4.7}$$

Note that these formulas generalize the case of dimension one (cf. (2.82), (2.84)).

As for the information that $\varepsilon(\boldsymbol{\rho}, \psi, dx)$ contains, we have first of all

$$\varepsilon(\boldsymbol{\rho}, \psi, dx_{\mathrm{sd}})\varepsilon(\boldsymbol{\rho}^\vee, \psi, dx_{\mathrm{sd}}) = \det \rho(-1)q^{n(\psi)\dim\rho + a(\boldsymbol{\rho})}, \tag{4.8}$$

where the notation on the right is as follows: First of all, dx_{sd} is the self-dual Haar measure relative to ψ and $\det\rho$ is viewed as a character of $\mathrm{W}(\overline{K}/K)^{\mathrm{ab}}$ and hence of $K^\times$. The integer $a(\boldsymbol{\rho})$ can be taken as the definition of the exponent of the conductor or ρ, and $n(\psi)$ is the largest integer ν such that ψ is trivial on $\pi^{-\nu}\mathcal{O}$. In particular, if we take $\psi = \psi^{\mathrm{can}}$, the canonical choice made in (2.70), then $n(\psi)$ is the exponent of the different ideal of K over $\mathbb{Q}_p$.

The other bit of information contained in the epsilon factor is the root number:

$$W(\boldsymbol{\rho}, \psi) = \frac{\varepsilon(\boldsymbol{\rho}, \psi, dx)}{|\varepsilon(\boldsymbol{\rho}, \psi, dx)|}. \tag{4.9}$$

The omission of dx from the argument on the left-hand side is justified by (4.7). Furthermore, (4.6) gives

$$W(\boldsymbol{\rho}, \psi_b) = \det\rho(b)W(\boldsymbol{\rho}, \psi), \tag{4.10}$$

so that if $\det\rho$ is trivial then $W(\boldsymbol{\rho}, \psi)$ is independent of ψ as well. In any case, we can set

$$W(\boldsymbol{\rho}) = W(\boldsymbol{\rho}, \psi^{\mathrm{can}}), \tag{4.11}$$

taking advantage of the canonical choice.

Let us temporarily return to the global setting: K is a number field and M is a premotive over K. Using (4.8), we can define the conductor $\mathfrak{f}(M)$ of M:

$$\mathfrak{f}(M) = \prod_{v\nmid\infty} \mathfrak{p}_v^{a(\boldsymbol{\rho}_{M,v})}, \tag{4.12}$$

And thus we can also define the exponential factor in the functional equation of $L(s, M)$:

$$A(M) = D^{\dim M}\mathbf{N}\mathfrak{f}(M), \tag{4.13}$$

this being the global version of (4.8) when we take the canonical additive character at every finite place.

For the root number $W(M)$ we cannot give a complete formula without some implicit assumption that M comes from a motive and therefore has a Hodge realization. Then in principle one could use Deligne's formulas ([**16**], p. 329) to augment (4.11) and set

$$W(M)_= \prod_{v\nmid\infty} W(\boldsymbol{\rho}_{M,\iota})\cdot(*), \tag{4.14}$$

where $(*)$ denotes the local root numbers at infinity associated to the Hodge structure.

2. The theorem of Langlands and Deligne

We return to the local setting; K is again a finite extension of $\mathbb{Q}_p$ with $p<\infty$. The definition of $\varepsilon(\rho,\psi,dx)$ should satisfy certain requirements. Certainly we want a definition which is **compatible in degree one** in the sense that it agrees with Tate's definition of $\varepsilon(\rho,\psi,dx)$ when $\dim\rho = 1$. In addition, like the L-factor $L(\rho,s)$, it should be **additive** in the sense that $\varepsilon(*,\psi,dx)$ extends to a function on the Grothendieck group of virtual representations of $\mathrm{W}(\overline{K}/K)$. In other words, $\varepsilon(\rho,\psi,dx)$ should depend only on the semisimplification of ρ and should satisfy $\varepsilon(\rho\oplus\rho',\psi,dx) = \varepsilon(\rho,psi,dx)\varepsilon(\rho',psi,dx)$. Ideally one might wish for ε) to share another property of $L(s,\rho)$, namely invariance under induction, but this turns out to be impossible, and instead one requires the epsilon factor to be **inductive in degree zero**. This means that if L is a finite extension of K and φ is a virtual representation of $\mathrm{W}(\overline{K}/K)$ of dimension zero then for any additive character ψ of K and any choice of Haar measures dx and dx_L on K and L respectively we have

$$\varepsilon(\mathrm{ind}_{L/K}\varphi,\psi,dx) = \varepsilon(\varphi,\psi\circ\mathrm{tr}_{L/K},dx_L). \tag{4.15}$$

The theorem of Langlands and Deligne is that such a definition is possible [**14**], p. 535:

Theorem 4.1. *Consider the set S with elements (K,ρ,ψ,dx), where K is a finite extension of $\mathbb{Q}_p$ inside $\overline{\mathbb{Q}}_p$, ρ an isomorphism class of complex representations of $\mathrm{W}(\overline{\mathbb{Q}}_p/K)$, ψ an additive character of K, and dx a Haar measure on K. There exists a unique function $(K,\rho,\psi,dx)\mapsto\varepsilon(\rho,psi,dx)$ from S to $\mathbb{C}^\times$ which is compatible in degree one, additive, and inductive in degree zero.*

To see that Theorem 4.1 gives a practical method of computing $\varepsilon(\rho,\psi,dx)$ we need two more results from [**14**]. A representation ρ of $\mathrm{W}(\overline{K}/K)$ over $\mathbb{C}$ is said to be **of Galois type** if there exists $s\in\mathbb{C}$ such that $\rho\otimes\omega^s$ is trivial on an open subgroup of finite index in $\mathrm{W}(\overline{K}/K)$, hence on an open normal subgroup of finite index. Since the open normal subgroups of finite index are precisely the subgroups of the form $\mathrm{W}(\overline{K}/L)$ with L a finite Galois extension of K we see that $\rho\otimes\omega^s$ factors through a finite group of the form $\mathrm{Gal}(L/K)$ (cf. (3.49)).

Proposition 4.1. *Let ρ be a representation of $\mathrm{W}(\overline{K}/K)$ over $\mathbb{C}$. If ρ is irreducible then ρ is of Galois type.*

Proof. Let J be the kernel of $\rho|I$. Then J is normal in $\mathrm{W}(\overline{K}/K)$, and the action of $\mathrm{W}(\overline{K}/K)$ on I by conjugation defines a map $\mathrm{W}(\overline{K}/K)\to\mathrm{Aut}(I/J)$. But

I/J is a finite group, so we deduce that if $\sigma \in \mathrm{W}(\overline{K}/K)$ is a given Frobenius element then there is a positive integer n such that σ^n acts trivially on I/J. It follows by (3.48) that the coset of σ^n is in the center of $\mathrm{W}(\overline{K}/K)/J$, and since ρ can be viewed as an irreducible representation of $\mathrm{W}(\overline{K}/K)/J$ we conclude that $\rho(\sigma^n)$ is scalar. Choose $s \in \mathbb{C}$ such that $\rho(\sigma^n)$ is multiplication by q^s, where $q = \omega(\sigma)$ as usual. Then $(\rho \otimes \omega^{s/n})(\sigma^n)$ is trivial. Hence $\rho \otimes \omega^{s/n}$ is trivial on the open subgroup of $\mathrm{W}(\overline{K}/K)$ generated by J and σ^n, which is of finite index. □

The significance of Proposition (4.1) is that it enables us to apply Brauer's theorem. More precisely, what is needed here is a variant of Brauer's theorem proved by Deligne ([**14**], p. 510, Proposition 1.5). Let us say that a virtual representation of a finite group G is **monomial of degree zero** if it is induced by the difference of two one-dimensional representations of a subgroup of G. Then Deligne's version of Brauer's theorem states that a virtual representation of G of degree zero is an integral linear combination of monomial representations of degree zero.

Proposition 4.2. *Let ρ be an irreducible representation of $\mathrm{W}(\overline{K}/K)$ over $\mathbb{C}$. Then for some $s \in \mathbb{C}$ we can write*

$$[\rho] = (\dim\rho)[\omega^s] + \sum_{(M,\xi,\xi')} n_{M,\xi,\xi'} \mathrm{ind}_{M/K}([\xi] - [\xi'])$$

in the Grothendieck group of virtual representations of $\mathrm{W}(\overline{K}/K)$, where the $n_{M,\xi,\xi'}$ are integers, M runs over finite extensions of K inside $\overline{K}$, and ξ and ξ' denote one-dimensional repesentations of $\mathrm{W}(\overline{K}/M)$.

Proof. By Proposition 4.1, we can choose $s \in \mathbb{C}$ so that $\rho \otimes \omega^s$ is trivial on an open subgroup of finite index in $\mathrm{W}(\overline{K}/K)$. Then $\rho \otimes \omega^s$ becomes a representation of $\mathrm{Gal}(L/K)$ for some finite Galois extension of K, and consequently we can write

$$[\rho \otimes \omega^s] - (\dim\rho)[1_K] = \sum_{(M,\xi,\xi')} n_{M,\xi,\xi'} \mathrm{ind}_{M/K}([\xi] - [\xi']) \tag{4.16}$$

with integers $n_{M,\xi,xi'}$, subfields M of L containing K, and one-dimensional characters ξ and ξ' of $\mathrm{W}(\overline{K}/M)$. Tensoring both sides of (4.16) with $[\omega^{-s}]$ and writing $(\mathrm{ind}_{M/K}\xi) \otimes (\omega^{-s}) = \mathrm{ind}_{M/K}(\xi \otimes (\mathrm{res}_{M/K}\omega^{-s}))$, we obtain the stated decomposition with ξ and ξ' replaced by $\xi \otimes (\mathrm{res}_{M/K}\omega^{-s})$ and $\xi' \otimes (\mathrm{res}_{M/K}\omega^{-s})$. □

Let us now explain why Theorem 4.1 does reduce the evaluation of epsilon factors to the case of dimension one. Since the epsilon factor is additive, it suffices to consider irreducible ρ. Write ρ as in Proposition 4.2. By the additivity and inductivity in degree zero,

$$\varepsilon(\rho,\psi,dx) = \varepsilon(\omega^s,\psi,dx)^{\dim\rho} \prod_{(M,\xi,\xi')} \left(\frac{\varepsilon(\xi, \psi_\circ \mathrm{tr}_{M/K}, dx_M)}{\varepsilon(\xi', \psi \circ \mathrm{tr}_{M/K}, dx_M)} \right)^{n_{M,\xi,\xi'}} \tag{4.17}$$

for any choice of additive character ψ and Haar measure dx for K and any choice of Haar measures dx_M on the fields M. All of the epsilon factors on the right-hand side of (4.2) are for representations of dimension one.

3. The archimedean local Weil group and gamma factors

For the record, let us also say a word about the cases $K = \mathbb{R}$ or $K = \mathbb{C}$. The first point is that in the archimedean case there is no distinction between $\mathrm{W}(\overline{K}/K)$ and $\mathrm{WD}(\overline{K}/K)$. We have $\mathrm{W}(\overline{K}/K) = \mathrm{WD}(\overline{K}/K)$ and $\boldsymbol{\rho} = (\rho, 0) = \rho$. Thus the notations $\mathrm{W}(\overline{K}/K)$ and ρ can be used interchangeably with $\mathrm{WD}(\overline{K}/K)$ and $\boldsymbol{\rho}$.

The definition of $\mathrm{W}(\overline{K}/K)$ is as follows. If $K = \mathbb{R}$ then $\mathrm{W}(\overline{K}/K) = \mathrm{W}(\mathbb{C}/\mathbb{R}) = \mathbb{C}^\times \cup J\mathbb{C}^\times$, where $J^2 = -1$ and $JzJ^{-1} = \overline{z}$ for $z \in \mathbb{C}^\times$. If $K \cong \mathbb{C}$ then $\mathrm{W}(\overline{K}/K) = \mathrm{W}(\mathbb{C}/\mathbb{C}) = \mathbb{C}^\times$. We regard $\mathrm{W}(\mathbb{C}/\mathbb{C})$ as a subgroup of index 2 in $\mathrm{W}(\mathbb{C}/\mathbb{R})$, the nontrivial coset being represented by J.

In the nonarchimedean case we assigned an L-factor to a representation $\boldsymbol{\rho}$ of $\mathrm{WD}(\overline{K}/K)$, and we want to do the same in the archimedean case. In other words, we want an archimedean analogue of (3.53). To define one, we declare first of all that the L-factor $L(s, \rho)$ assigned to a representation ρ of $\mathrm{W}(\mathbb{C}/\mathbb{R})$ or $\mathrm{W}(\mathbb{C}/\mathbb{C})$ depends only on the semisimplification of ρ and is multiplicative across direct sums in the sense that $L(s, \rho \oplus \rho') = L(s, \rho)L(s, \rho')$. Thus it suffices to define $L(s, \rho)$ when ρ is irreducible.

The easier case is $K = \mathbb{C}$. Any irreducible representation of $\mathrm{W}(\mathbb{C}/\mathbb{C})$ is one-dimensional, of the form $\rho(z) = |z|^{2s_0}(z/|z|)^m$ with $s_0 \in \mathbb{C}$ and $m \in \mathbb{Z}$. We define $L(s, \rho)$ to be the right-hand side of (2.33).

When $K = \mathbb{R}$ there are two cases: An irreducible representation of $\mathrm{W}(\mathbb{C}/\mathbb{R})$ is either one-dimensional or two-dimensional. That these are the only two possibilities follows from the fact that $\mathrm{W}(\mathbb{C}/\mathbb{R})$ has an abelian normal subgroup of index 2, namely $\mathrm{W}(\mathbb{C}/\mathbb{C})$. For the same reason, any irreducible two-dimensional representation of $\mathrm{W}(\mathbb{C}/\mathbb{R})$ is induced by a one-dimensional character of $\mathrm{W}(\mathbb{C}/\mathbb{C})$.

Let us identify the one-dimensional characters of $\mathrm{W}(\mathbb{C}/\mathbb{R})$. It is clear that the commutator subgroup of $\mathrm{W}(\mathbb{C}/\mathbb{R})$ consists of all elements of the form $JzJ^{-1}z^{-1}$ with $z \in \mathbb{C}$, and since $JzJ^{-1}z^{-1} = \overline{z}/z$ we see that the commutator subgroup is the group $\mathbf{T}$ of complex numbers of absolute value 1. The map $\pi : \mathrm{W}(\mathbb{C}/\mathbb{R}) \to \mathbb{R}^\times$ sending J to -1 and z to $|z|^2$ is readily verified to be a surjective homomorphism with kernel $\mathbf{T}$, so we conclude that the one-dimensional representations of $\mathrm{W}(\mathbb{C}/\mathbb{R})$ are precisely the representations $\rho = \chi \circ \pi$ with χ a character of $\mathbb{R}^\times$. If $\chi(t) = |t|^{s_0}(t/|t|)^m$ with $s_0 \in \mathbb{C}$ and $m \in \{0, 1\}$ then $L(s, \rho)$ is defined to be the right-hand side of (2.32).

Finally, write $\mathrm{ind}_{\mathbb{C}/\mathbb{R}}\chi$ for the two-dimensional representation ρ of $\mathrm{W}(\mathbb{C}/\mathbb{R})$ induced by a character χ of $\mathrm{W}(\mathbb{C}/\mathbb{C})$. Then $\chi(z) = |z|^{2s_0}(z/|z|)^m$ for some $s_0 \in \mathbb{C}$ and some $m \in \mathbb{Z}$, and ρ is irreducible if and only if $m \neq 0$. If the latter condition is satisfied then we define $L(s, \rho)$ to be the right-hand side of (2.33).

4. An open problem

A survey of the formulas for local L-factors, conductors, and root numbers confirms our remark in the previous lecture that whenever the nilpotent endomorphism N appears in a local formula it appears by way of its restriction to V^I. This was the rationale for replacing N by N^* in Theorem (3.2). Nonetheless, one can ask whether this replacement is really necessary:

> *Let M be a premotive over a number field K and $\{\rho_\lambda\}$ a representative of M. Fix a finite place v of K and consider the representation $\boldsymbol{\rho}^\iota$ obtained*

from ρ_λ as in Theorem 3.1. Is the isomorphism class of $\boldsymbol{\rho}^\iota$ independent of the choice of λ and ι?

It may be that this question is answered in the literature. I can't find anything precise, but perhaps I have looked in the wrong places or have misunderstood what I read.

5. Exercises

Exercise 4.1. Let K be a finite extension of $\mathbb{Q}_p$, let E be an elliptic curve over K, and let ρ_ℓ be the representation of $\mathrm{Gal}(\overline{K}/K)$ on the *dual* of $V_\ell(E)$, with $\ell \neq p$. Let $\boldsymbol{\rho} = (\rho, N)$ be the representation of $\mathrm{WD}(\overline{K}/K)$ obtained from ρ_λ by applying part (a) of Theorem 3.1. Show that (i) if E has good reduction at v then ρ is unramified and $N = 0$, (ii) if E has bad but potentially good reduction then ρ is ramified and $N = 0$, and (iii) if E has potentially multiplicative reduction then $N \neq 0$ (and therefore N has the only Jordan normal form possible for a 2×2 nilpotent matrix $\neq 0$) while $\rho \cong \chi \oplus \chi\omega$, where χ is the unique character of $\mathrm{W}(\overline{K}/K)$ with $\chi^2 = 1$ such that the twist of E by χ is a Tate curve over K. Furthermore, show that $W(E) = 1$ in case (i) and that

$$W(E) = \begin{cases} -1 & \text{if } \chi = 1 \\ 1 & \text{if } \chi \text{ is the unique unramified quadratic character of } \mathrm{W}(\overline{K}/K) \\ \chi(-1) & \text{if } \chi \text{ is ramified} \end{cases}$$

in case (iii).

Exercise 4.2. Let K be a number field with r_1 real embeddings and r_2 pairs of complex conjugate embeddings, and suppose that E is a semistable elliptic curve over K which has split multiplicative reduction at exactly s finite places of K. Using the previous problem, derive the classic formula $W(E) = (-1)^{r_1+r_2+s}$.

Exercise 4.3. As we have already mentioned, the class of motivic L-functions, while very broad, does not include even all Hecke L-functions of number fields – for example the L-function $L(s, \chi)$ with χ as in (2.63) is not included – let alone the L-functions of arbitrary automorphic forms. Nonetheless, the wonderful thing is that at the *local* level, the Weil-Deligne group and its representations cover everything, including (conjecturally) the parameters for the local components of arbitrary automorphic forms. To illustrate this point, let f be a Maass form for $\mathrm{SL}(2, \mathbb{Z})$. Then the representation of $\mathrm{WD}(\mathbb{C}/\mathbb{R})$ associated to f at the infinite place of $\mathbb{Q}$ is $\chi \oplus \overline{\chi}$, where χ has the form $\chi(t) = |t|^{ir}(t/|t|)^m$ with $r \in \mathbb{R}$ and $m \in \{0, 1\}$. Show that the root number $W(f)$ in the functional equation of $L(s, f)$ is 1 or -1 according as $m = 0$ or 1. You do not need to know anything about Maass forms to do this problem! Just use some common sense. (Here's an example of common sense: Given that f is a Maass form for $\mathrm{SL}(2, \mathbb{Z})$, what can you guess about the conductors of the local representations associated to f at the finite places?)

Exercise 4.4. (*Reading.*) Let G be a finite group and ρ a representation of G. There are theorems of Snaith [**59**] and others which express $[\rho]$ in $\mathrm{Groth}(G)$ as an integral linear combination of classes of monomial representations in a *canonical* way. Theorems of this type are call **canonical Brauer induction** theorems. Can they be used to prove the existence of local root numbers?

LECTURE 5

The minimalist dichotomy

In this final lecture we would like to reflect on the following question: To what extent, or under what circumstances, should we expect the order of vanishing of a motivic L-function at the center of its critical strip to be the minimum compatible with its functional equation? To begin with we restrict our attention to essentially self-dual premotives M, so that the functional equation of $L(s, M)$ is $\Lambda(s, M) = W(M)\Lambda(k - s, M)$ with $k = w + 1$, where $w \geqslant 0$ is the weight of M. We are then asking how likely it is that

$$\text{ord}_{s=k/2} L(s, M) = \begin{cases} 0 & \text{if } W(M) = 1, \\ 1 & \text{if } W(M) = -1. \end{cases} \tag{5.1}$$

In the case of elliptic curves E over $\mathbb{Q}$ with $W(E) = 1$ this question is discussed at length in the paper of Bektemirov, Mazur, Stein, and Watkins [**5**], who refer to the conjecture that $L(1, E) \neq 0$ with probability one as the "minimalist conjecture" for such E. Adopting their language, we shall say that the **minimalist dichotomy** holds for $L(s, M)$ if (5.1) is satisfied.

We have seen (Theorem 1.3) that the minimalist dichotomy holds for the premotives $M(\chi)$ associated by (3.46) to the characters $\chi \in X(D)$. On the other hand, as a universal statement about L-functions of elliptic curves, (5.1) is simply false. This point is perhaps so familiar as to require no comment, but for the record, if we take the base field to be $\mathbb{Q}$ and order elliptic curves by their conductor then the first counterexample to (5.1) is the curve 389A1 in Cremona's tables ([**13**], p. 306). Indeed Kolyvagin's theorem implies that if E is an elliptic curve over $\mathbb{Q}$ with $\text{ord}_{s=1} L(s, E) \leqslant 1$ then the rank of E is $\leqslant 1$, and an inspection of Cremona's tables shows that the converse is valid at least for curves of conductor $\leqslant 999$ (see [**13**], pp. 293 – 340). As 389A1 is the first curve in the tables of rank > 1 (its rank is 2) it is also the first for which (5.1) fails. Using results like [**51**] one can produce as many other counterexamples as one likes.

Nonetheless, we can ask as in [**5**] whether the minimalist dichotomy holds for a dense set of elliptic curves over $\mathbb{Q}$. After briefly surveying what is known or conjectured about this question, we shall broaden the discussion to include more general motivic L-functions.

1. Elliptic curves

Let $\mathcal{E}$ be the set of isomorphism classes of elliptic curves E over $\mathbb{Q}$ and $\mathcal{D}$ the subset of isomorphism classes for which $L(s, E)$ satisfies the minimalist dichotomy. Write $\vartheta_{\mathcal{E}}(x)$ and $\vartheta_{\mathcal{D}}(x)$ for the number of isomorphism classes in $\mathcal{E}$ and $\mathcal{D}$ respectively which have conductor $\leqslant x$. By the **minimalist conjecture for elliptic curves over Q** we mean the hypothesis that $\lim_{x\to\infty} \vartheta_{\mathcal{D}}(x)/\vartheta_{\mathcal{E}}(x)$ exists and equals 1.

Before committing ourselves too firmly to this formulation of the problem, we should note that the answer could depend on the fact that we are counting elliptic curves using the conductor rather than some other natural invariant. Quite generally, consider a set $\mathcal{S}$ and a function $\nu : \mathcal{S} \to \mathbb{Z}_{\geqslant 0}$ such that for every $x > 0$ there are only finitely many $s \in \mathcal{S}$ with $\nu(s) \leqslant x$. We will call ν a **counting function** on $\mathcal{S}$. Writing $\vartheta_{\mathcal{S},\nu}(x)$ for the number of such s, one can consider the limit $\lim_{x\to\infty} \vartheta_{\mathcal{T},\nu}(x)/\vartheta_{\mathcal{S},\nu}(x)$ for a given subset $\mathcal{T}$ of $\mathcal{S}$, but even if this limit exists, its value may depend on ν. For example, fix an integer $n \geqslant 3$, let $\mathcal{P}$ be the set of primes, and let $\mathcal{Q}$ the subset of primes $p \equiv -1$ modulo n. If we take $\nu(p) = p$ then $\lim_{x\to\infty} \vartheta_{\mathcal{Q},\nu}(x)/\vartheta_{\mathcal{P},\nu}(x) = 1/\varphi(n)$, but if instead $\nu(p) = p^{\langle p\rangle}$, where $\langle p\rangle$ is the least positive residue of p modulo n, then $\lim_{x\to\infty} \vartheta_{\mathcal{Q},\nu}(x)/\vartheta_{\mathcal{P},\nu}(x) = 0$.

Returning to $\mathcal{E}$, and writing $\nu(E)$ for the value of ν on the isomorphism class of E, we can defend the choice $\nu(E) = N(E)$ as the only *analytic* possibility for ν – analytic in the sense that $N(E)$ appears in the functional equation of $L(s, E)$ – but on the arithmetic side there are many other possibilities: the Arakelov height of E, or the height of the modular invariant $j(E)$, or the absolute value of the minimal discriminant $\Delta(E)$, or simply the coarse height

$$\nu(E) = \min_{\substack{4a^3+27b^2\neq 0\\ E\cong E_{a,b}}} \max(|a|^3, |b|^2) \tag{5.2}$$

where the minimum is taken over all pairs of integers (a, b) such that $4a^3+27b^2 \neq 0$ and E is isomorphic to the curve $E_{a,b} : y^2 = x^3+ax+b$. Now one can argue that the arithmetic choices are less natural than $N(E)$, for they depend on the *isomorphism* class of E, whereas the validity of (5.1) depends only on the *isogeny* class. However the arithmetic choices of ν are often easier to work with, so it behooves us to know whether the choice $\nu(E) = |\Delta(E)|$, say, is equivalent to the choice $\nu(E) = N(E)$ for the purpose of evaluating the limit $\lim_{x\to\infty} \vartheta_{\mathcal{D},\nu}(x)/\vartheta_{\mathcal{E},\nu}(x)$. This does not seem like an easy question, particularly since it is not known whether $|\Delta(E)|$ is bounded by a power of $N(E)$ – in a stronger form this is Szpiro's conjecture.

But in fact one hopes for more: not only should $\lim_{x\to\infty} \vartheta_{\mathcal{D},\nu}(x)/\vartheta_{\mathcal{E},\nu}(x)$ be the same for $\nu(E) = |\Delta(E)|$ as for $\nu(E) = N(E)$, but even the shape of the error term should be the same. To spell this out, consider the conjecture

$$\vartheta_{\mathcal{E},\nu}(x) \sim c \cdot x^{5/6}. \tag{5.3}$$

The expectation is that (5.3) holds both in the case $\nu(E) = |\Delta(E)|$ (Brumer and McGuinness [**8**]) and in the case $\nu(E) = N(E)$ (Watkins [**65**]), although the constant c may depend on ν. Next consider Conjecture 3.4 on p. 244 of [**5**] (based on the heuristics of Watkins [**65**]), which in principle gives

$$\vartheta_{\mathcal{E},\nu}(x) - \vartheta_{\mathcal{D},\nu}(x) \sim c' \cdot x^{19/24}(\log x)^{3/8} \tag{5.4}$$

both for $\nu(E) = N(E)$ and $\nu(E) = |\Delta(E)|$, although the constant c' may again depend on the choice of ν. We say "in principle" because the focus in [**5**] is on the first line of (5.1), so that the roles of $\mathcal{E}$ and $\mathcal{D}$ are actually played by the set of isomorphism classes $\mathcal{E}^+$ with $W(E) = 1$ and the subset $\mathcal{D}^+$ with $L(1, E) \neq 0$. In any case, since $19/24 < 5/6$ we obtain from (5.3) and (5.4) that $\lim_{x\to\infty} \vartheta_{\mathcal{D}}(x)/\vartheta_{\mathcal{E}}(x) = 1$, regardless of whether the implicit counting function is $|\Delta|$ or N. Henceforth the omission of the subscript ν on $\vartheta_{\mathcal{D}}(x)$ and $\vartheta_{\mathcal{E}}(x)$ indicates as before that $\nu = N$, but now with the implication that the choice of ν shouldn't matter anyway.

As the authors of [**5**] acknowledge, the numerical evidence for all of this is weak. In fact one can almost say that the minimalist conjecture for elliptic curves over $\mathbb{Q}$ is made in defiance of the available data. These data include the calculations of Brumer and McGuinness [**8**] with elliptic curves of prime conductor $< 10^8$, the calculations of Stein and Watkins [**61**] with elliptic curves of composite conductor $\leqslant 10^8$ or prime conductor $< 10^{10}$, and the calculations of the authors themselves involving selected elliptic curves of prime conductor around 10^{14}. None of these works gives much support for the minimalist dichotomy, although there is some hint that the desired numerical evidence may simply lie outside the range of computation. At least the results for 10^{14} are a bit more supportive than those for 10^8 or 10^{10}.

Turning from the numerical to the theoretical, we find that the known results pertain less to the minimalist conjecture than to a slightly different hypothesis, the **average rank conjecture**. Originally enunciated by Goldfeld [**24**] for quadratic twists of a fixed elliptic curve, the average rank conjecture is here understood to assert that the limit

$$r_\nu(\mathcal{E}) = \lim_{x\to\infty} \frac{\sum_{\nu(E)\leqslant x} \operatorname{ord}_{s=1} L(s,E)}{\vartheta_{\mathcal{E},\nu}(x)} \tag{5.5}$$

exists and equals $1/2$ for any of the counting functions $\nu : \mathcal{E} \to \mathbb{Z}_{\geqslant 0}$ mentioned above. In principle the choice favored in the literature is the coarse height (5.2), but even with this choice of ν, the "average rank" r that one encounters in the literature differs from our r_ν in that both the summation in the numerator on the right-hand side of (5.5) and the implicit summation in the denominator run over *all* elliptic curves $E_{a,b}$ such that $|a|^3, |b|^2 \leqslant x$: in other words, redundancies arising from isomorphisms among the curves $E_{a,b}$ are not eliminated. Granting this point, and assuming the generalized Riemann hypothesis for L-functions of elliptic curves over $\mathbb{Q}$, one can cite the successive upper bounds $r \leqslant 23/10$ (Brumer [**7**]), $r \leqslant 2$ (Heath-Brown [**28**]), $r \leqslant 25/14$ (Young [**68**]), and $r \leqslant 27/14$ (Baier and Zhao [**3**]). The two more recent works draw on random matrix theory (cf. Iwaniec, Luo, and Sarnak [**32**]), and while Young's bound is sharper than that of Baier and Zhao, it depends on the generalized Riemann hypothesis for Dirichlet and symmetric square L-functions, a dependence eliminated in [**3**]. It should be added that the limit defining r is not actually known to exist: the results cited above are to be understood as upper bounds for the corresponding limit superior.

Quite apart from the large gap between the upper bounds for r cited above and the conjectured value $r = 1/2$, the average rank conjecture does not seem to imply anything about the minimalist conjecture unless one knows something about the equidistribution of root numbers. As before, let $\mathcal{E}^\pm \subset \mathcal{E}$ be the subset of isomorphism classes with root number ± 1. It does not appear to be known that $\lim_{x\to\infty} \vartheta_{\mathcal{E}^\pm}(x)/\vartheta_{\mathcal{E}}(x) = 1/2$, let alone that

$$\vartheta_{\mathcal{E}^\pm}(x) = \frac{1}{2}\vartheta_{\mathcal{E}}(x) + O(x^\gamma) \tag{5.6}$$

with a constant $\gamma < 5/6$. However if one grants (5.6) along with (5.3) then one can show that an estimate of the form

$$\sum_{N(E)\leqslant x} \operatorname{ord}_{s=1} L(s,E) = \vartheta_{\mathcal{E}}(x) + O(x^{\gamma'}) \tag{5.7}$$

with $\gamma' < 5/6$ implies an estimate of the form

$$\vartheta_{\mathcal{D}}(x) = \vartheta_{\mathcal{E}}(x) + O(x^{\gamma''}) \tag{5.8}$$

with $\gamma'' < 5/6$, and conversely. Note that (5.7) is stronger than (5.5) while (5.8) is weaker than (5.4). But (5.8) does imply the minimalist conjecture for elliptic curves over $\mathbb{Q}$.

2. The minimalist trichotomy

Let us attempt to formalize the idea that " with probability 1, the order of vanishing of a motivic L-function at the center of its critical strip is the minimum compatible with its functional equation." This notion may simply be wrong, but without a precise formulation there can be no counterexample.

Fix number fields K and $\mathbb{E}$ and integers $w \geqslant 0$ and $n \geqslant 1$, and let $\mathcal{S}_{K,\mathbb{E},w,n}$ be the set of premotives M over K of weight w and dimension n which admit $\mathbb{E}$ as coefficient field. (By the **dimension** of M we mean the dimension of ρ_λ for $\{\rho_\lambda\}_\lambda$ in M; and M **admits** $\mathbb{E}$ **as coefficient field** if we can choose $\{\rho_\lambda\}_\lambda$ to have coefficient field $\mathbb{E}$.) As usual, we put $k = w + 1$, so that the functional equation of $L(s, M)$ is $\Lambda(s, M) = W(M)\Lambda(k - s, \overline{M})$. Since we are no longer restricting ourselves to essentially self-dual motives, it is not necessarily the case that $W(M) = \pm 1$. Hence the dichotomy (5.1) should now be replaced by

$$\operatorname{ord}_{s=k/2} L(s, M) = \begin{cases} 0 & \text{if } M \ncong \overline{M}, \\ 0 & \text{if } M \cong \overline{M} \text{ and } W(M) = 1, \\ 1 & \text{if } M \cong \overline{M} \text{ and } W(M) = -1. \end{cases} \tag{5.9}$$

Of course an equivalent but more succinct formulation would be

$$\operatorname{ord}_{s=k/2} L(s, M) = \begin{cases} 1 & \text{if } M \cong \overline{M} \text{ and } W(M) = -1, \\ 0 & \text{otherwise,} \end{cases} \tag{5.10}$$

but perhaps (5.9) is more illuminating than (5.10). We shall refer to (5.9) as the **minimalist trichotomy** and write $\mathcal{T}_{K,\mathbb{E},w,n}$ for the subset of $\mathcal{S}_{K,\mathbb{E},w,n}$ consisting of the isomorphism classes for which the minimalist trichotomy holds. To formulate a hypothesis about the density of $\mathcal{T}_{K,\mathbb{E},w,n}$ in $\mathcal{S}_{K,\mathbb{E},w,n}$ we need a counting function on $\mathcal{S}_{K,\mathbb{E},w,n}$. We will use a lemma of Faltings [**19**]:

Proposition 5.1. *Fix a number field K, a finite set of prime ideals S of K, a prime number ℓ, a finite extension $\mathbb{E}_\lambda$ of $\mathbb{Q}_\ell$, and an integer $n \geqslant 1$. Then there exists a finite set of prime ideals T of K, disjoint from S, with the following property: If ρ_λ is an n-dimensional semisimiple representation of $\operatorname{Gal}(\overline{K}/K)$ over $\mathbb{E}_\lambda$ which is unramified outside S then ρ_λ is determined up to isomorphism by the $|T|$ values $\operatorname{tr} \rho_\lambda(\sigma_\mathfrak{p})$ for $\mathfrak{p} \in T$, where $\sigma_\mathfrak{p}$ denotes a Frobenius element at $\mathfrak{p}$.*

In [**19**] this proposition is stated with $E_\lambda = \mathbb{Q}_\ell$, but the proof works for any $\mathbb{E}_\lambda$.

Proposition 5.2. *The norm of the conductor $\nu(M) = \mathbf{N}\mathfrak{f}(M)$ is a counting function on $\mathcal{S}_{K,\mathbb{E},w,n}$.*

Proof. Fix a prime number ℓ_0 and a place λ_0 of $\mathbb{E}$ above ℓ_0, and let $x > 0$ be given. Let S be the set of prime ideals $\mathfrak{p}$ of K such that $\mathbf{N}\mathfrak{p} \leqslant x$. We apply Proposition 5.1 with ℓ and λ replaced by ℓ_0 and λ_0. Given $M \in \mathcal{S}$ with $\mathbf{N}\mathfrak{f}(M) \leqslant x$, choose $\{\rho_\lambda\}_\lambda \in M$ with coefficient field $\mathbb{E}$; then M is determined by

the isomorphism class of ρ_{λ_0} (Proposition 3.1). Thus it suffices to see that there are only finitely many possibilities for the numbers $\operatorname{tr}\rho_{\lambda_0}(\sigma_{\mathfrak{p}})$ with $\mathfrak{p} \in T$. Now $\operatorname{tr}\rho_{\lambda_0}(\sigma_{\mathfrak{p}})$ is the sum of the roots of $B_{\mathfrak{p}}(x)$, hence an element of $\mathcal{O}_{\mathbb{E}}$ of absolute value $\leqslant n(\mathbf{N}\mathfrak{p})^{w/2}$ in every archimedean embedding of $\mathbb{E}$. Since there are only finitely many such elements of $\mathcal{O}_E$, the proposition follows. □

Now put $\mathcal{S} = \mathcal{S}_{K,\mathbb{E},w,n}$ and $\mathcal{T} = \mathcal{T}_{K,\mathbb{E},w,n}$. We also set $\nu(M) = \mathbf{N}\mathfrak{f}(M)$ and omit the subscript ν on $\vartheta_{\mathcal{S},\nu}$ and $\vartheta_{\mathcal{T},\nu}$. The assertion that $\lim_{x\to\infty}\vartheta_{\mathcal{T}}(x)/\vartheta_{\mathcal{S}}(x) = 1$ will serve as our **miminalist conjecture for premotives**.

2.1. Connection with elliptic curves

An immediate question is whether the miminalist conjecture for premotives implies the minimalist conjecture for elliptic curves over $\mathbb{Q}$. Two issues arise.

The first is that $\mathcal{E}$ was defined to be the set of isomorphism classes of elliptic curves over $\mathbb{Q}$, not the set of isogeny classes. In order to use the arithmetic counting functions we did need to deal with isomorphism classes, but for present purposes we redefine $\mathcal{E}$ as the set of isogeny classes of elliptic curves over $\mathbb{Q}$. Now by the isogeny theorem [**19**], an isogeny class of elliptic curves over $\mathbb{Q}$ is essentially the same thing as an isomorphism class of families of the form $\{\rho_{E,\ell}\}_\ell$ with E an elliptic curve over $\mathbb{Q}$. Let us make this identification. Then taking $K = \mathbb{E} = \mathbb{Q}$, $w = 1$, and $n = 2$, we have $\mathcal{E} \subset \mathcal{S}$.

The second issue is that we do not know whether the preceding inclusion is actually an equality. In fact this is a question of Lang and Trotter ([**38**], pp. 5 and 19), or at least a slight variant of it [**49**]. However, as explained in [**49**], the equality $\mathcal{E} = \mathcal{S}$ does follow from the Fontaine-Mazur conjecture [**20**] provided "classically ordinary" primes are ordinary (definitions below). So under these hypotheses, the case $K = \mathbb{E} = \mathbb{Q}$, $w = 1$, $n = 2$ of the minimalist conjecture for arbitrary premotives is equivalent to the minimalist conjecture for elliptic curves over $\mathbb{Q}$.

Here are the missing definitions. Let M be the isomorphism class of a strictly compatible family $\{\det\rho_\ell\}_\ell$ of integral ℓ-adic representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with coefficient field $\mathbb{Q}$ and exceptional set S. Suppose also that $\det\rho_\ell = \omega_\ell$. Then $B_p(x)$ has the form $B_p(x) = x^2 - a(p)x + p$ for $p \notin S$, where $a(p) \in \mathbb{Z}$. We say that p is **classically ordinary** relative to M if $p \nmid a(p)$. On the other hand, p is **ordinary** (again, relative to M) if p satisfies the definition on pp. 97–98 of Greenberg [**25**]. This means the following, Let $\mathfrak{p}$ be a prime ideal of $\overline{\mathbb{Q}}$ over p, and identify the corresponding decomposition group D with $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. Then by restriction to D we may view ρ_p as a representation of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. Let I be the inertia subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ and V the space of ρ_p. The prime p is ordinary in Greenberg's sense if there is a filtration

$$\cdots \supset F^iV \supset F^{i+1}V \supset \cdots$$

of V by subspaces F^iV stable under $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ such that $F^iV = \{0\}$ for $i \gg 0$, $F^iV = V$ for $i \ll 0$, and I acts on $F^iV_p/F^{i+1}V_p$ by the character $\omega_p^i|I$.

2.2. A variant of the conjecture

Alternatively, one can attempt to formulate the minimalist conjecture so that not all of the parameters K, $\mathbb{E}$, w, and n are fixed. In particular, let $\mathcal{S}_{K,w,n}$ be the set of premotives M over K of weight w and dimension n, and let $\mathcal{T}_{K,w,n}$ be the subset of elements satisfying the minimalist trichotomy. If the norm of the conductor $\nu(M) = \mathbf{N}\mathfrak{f}(M)$ is a counting function on $\mathcal{S}_{K,w,n}$ then one obtains a variant formulation of

the minimalist conjecture, namely $\lim_{x\to\infty} \vartheta_{\mathcal{S}}(x)/\vartheta_{\mathcal{T}}(x) = 1$, where $\mathcal{S} = \mathcal{S}_{K,w,n}$ and $\mathcal{T} = \mathcal{T}_{K,w,n}$. However I do not know how to prove that the norm of the conductor is a counting function on $\mathcal{S}_{K,w,n}$ except in the case $w = 0$:

Proposition 5.3. *Let $x > 0$ be given. There are only finitely many ismorphism classes of n-dimensional Artin representations ρ of K such that $\mathbf{N}\mathfrak{f}(\rho) \leqslant x$.*

Proof. The proof assumes a familiarity with some of the more technical aspects of local class field theory as in [**56**], Chapter IV. Let L be the fixed field of the kernel of ρ, and view the group $G = \mathrm{Gal}(L/K)$ as a subgroup of $\mathrm{GL}_n(\mathbb{C})$. By a theorem of Jordan, there is a constant c depending only on n such that any finite subgroup G of $\mathrm{GL}_n(\mathbb{C})$ has an abelian normal subgroup A of index $\leqslant c$. Applying this to the group $G = \mathrm{Gal}(L/K)$, we see that the fixed field M of A satsifies $[M : K] \leqslant c$. But according to a theorem of Hermite, a number field K has only finitely many extensions of bounded degree which are unramified outside a given finite set of places of K. It follows that there are only finitely many possibilities for M, and from this we would like to deduce that there are only finitely many possibilities for L.

Now L is abelian over M, and the finiteness of ray class groups implies that if the conductor of L over M is bounded then indeed there are only finitely many possibilities for L. So we must show that the conductor of L over M is bounded. If we fix a prime ideal $\mathfrak{p}$ of M then it suffices to see that the exponent of $\mathfrak{p}$ in the conductor of L/M is bounded.

Put $H = \mathrm{Gal}(L/M)$ and let H_i ($i \geqslant 0$) be the higher ramification subgroups of H relative to $\mathfrak{p}$. Similarly write G_i for the higher ramification groups of G relative to the prime of K below $\mathfrak{p}$. Then the bound for $\mathbf{N}\mathfrak{f}(\rho)$ gives a bound for the largest i such that G_i is nontrivial. And since H_i is a subgroup of G_i it follows that we have a bound for the largest i such that H_i is nontrivial. If $v = v_{\mathfrak{p}}$ is the place of M determined by $\mathfrak{p}$ then a bound for the largest i such that H_i is nontrivial gives a bound for the largest m such that $1 + \mathfrak{p}^m\mathcal{O}_v$ is not in the image of the local units from L ([**56**], p. 93, Corollary 4). If m_0 is such a bound then $m_0 + 1$ is a bound for the exponent of $\mathfrak{p}$ in the conductor of L/M. □

In the end, no matter which parameters one fixes, the minimalist conjecture has the limitations inherent in any probabilistic statement: It cannot account for phenomena which hold for *all* or for *all but finitely many* members of a family. For example it cannot account for Theorem 1.2, the fact that the minimalist trichotomy holds for $L(s, \chi)$ for every $\chi \in X(D)$. This example points to another limitation: many natural families are not dense subsets of any $\mathcal{S}_{K,\mathbb{E},w,n}$ or $\mathcal{S}_{K,w,n}$.

3. An open problem

Write $\mathcal{S}^{\mathrm{esd}}_{K,w,n}$ for the subset of $\mathcal{S}_{K,w,n}$ consisting of essentially self-dual motives. For simplicity, we drop the subscripts on $\mathcal{S}_{K,w,n}$ and $\mathcal{S}^{\mathrm{esd}}_{K,w,n}$ in the statement of the following problem:

Show that $\lim_{x\to\infty} \vartheta_{\mathcal{S}^{\mathrm{esd}}}(x)/\vartheta_{\mathcal{S}}(x) = 0$.

In principle, this problem depends on knowing that the norm of the conductor is a counting function on $\mathcal{S}_{K,w,n}$, but it seems reasonable to agree that the limit is 0 by default whenever the norm of the conductor is a counting function on $\mathcal{S}^{\mathrm{esd}}_{K,w,n}$ but not on $\mathcal{S}_{K,w,n}$. Be that as it may, there is already something to think about in the

case $w = 0$: If $K = \mathbb{Q}$ and $n = 1$ then the problem is easy ("Quadratic primitive Dirichlet characters have density 0 among all primitive Dirichlet characters"), but the case of Artin representations of arbitrary dimension already seems interesting.

4. Exercises

Exercise 5.1. Let E denote an elliptic curve over $\mathbb{Q}$. As pointed out by Serre, a method of Stark gives

$$\mathrm{ord}_{s=1} L(s, E) \ll \log N(E), \tag{5.11}$$

where the implied constant is absolute. Using this estimate, prove that

if one grants (5.3) and (5.6) then (5.7) and (5.8) are equivalent, as claimed.

Exercise 5.2. (*Reading.*) Read the proof of Proposition 5.1 in [**19**] and observe that it gives the following more general statement:

> Fix a number field K, a finite set of prime ideals S of K, a prime number ℓ, and integers $m, n \geqslant 1$. Then there exists a finite set of prime ideals T of K, disjoint from S, with the following property: Let ρ_λ be an n-dimensional semisimiple representation of $\mathrm{Gal}(\overline{K}/K)$ over an extension $\mathbb{E}_\lambda$ of $\mathbb{Q}_\ell$ of residue class degree $\leqslant m$, and suppose that ρ_λ is unramified outside S. Then ρ_λ is determined up to isomorphism by the $|T|$ values $\mathrm{tr}\,\rho_\lambda(\sigma_\mathfrak{p})$ for $\mathfrak{p} \in T$.

In other words, one does not have to fix $\mathbb{E}_\lambda$ in advance, only an upper bound for the degree of its residue class field.

Exercise 5.3. This problem presupposes some familiarity with modular forms.

(a) Fix a prime number ℓ, a finite set of prime numbers S, and an integer $k \geqslant 1$. Let N be a positive integer divisible only by primes in S, let f be a cuspidal Hecke eigenform of weight k for $\Gamma_1(N)$, let $\mathbb{E}$ be the extension of $\mathbb{Q}$ generated by the Fourier coefficients of f, and let λ be any place of $\mathbb{E}$ over ℓ. Write the order of the residue class field of $\mathbb{E}_\lambda$ as ℓ^m. Using the generalization of Proposition 5.1 contained in the previous exercise, prove that given $m_0 \geqslant 1$ there exists $N_0 \geqslant 1$ such that $N \geqslant N_0$ implies $m \geqslant m_0$.

(b) Let $\mathcal{E}$ be the set of isogeny classes of elliptic curves over $\mathbb{Q}$, and put $\mathcal{S} = \mathcal{S}_{K,w,n}$ with $K = \mathbb{Q}$, $w = 1$, $n = 2$. Show that

$$\lim_{x \to \infty} \frac{\vartheta_\mathcal{E}(x)}{\vartheta_\mathcal{S}(x)} = 0. \tag{5.12}$$

The limit is understood to be 0 by default if $\nu(M) = \mathbf{N}(\mathfrak{f}(M))$ is not a counting function on $\mathcal{S}$, so in proving (5.12) you may assume that it is.

Exercise 5.4. Formulate and prove a purely group-theoretic statment to the effect that the self-dual representations of finite groups have density 0 among all representations of finite groups.

Bibliography

[1] J. Armitage, *On a theorem of Hecke in number fields and function fields*, Inventiones Math. 2 (1967), 238 – 246.

[2] J. Armitage, *Zeta functions with a zero at $s = 1/2$*, Inventiones Math. 15 (1972), 199 – 205.

[3] S. Baier and L. Zhao, *On the low-lying zeros of Hasse-Weil L-functions for elliptic curves*, Advances in Math. 219 (2008), 952 – 985.

[4] R. Balasubramanian and V. K. Murty, *Zeros of Dirichlet L-functions*, Ann. Sci. Ecole Norm. Sup. 25 (1992), 567 – 615.

[5] B. Bektemirov, B. Mazur, W. Stein, and M. Watkins, *Average ranks of elliptic curves: tension between data and conjecture*, Bull. Amer. Math. Soc. 44 (2007), 233 – 254

[6] B. J. Birch and N. M. Stephens, *The parity of the rank of the Mordell-Weil group*, Topology 5 (1966) 295 – 299.

[7] A. Brumer, *The average rank of elliptic curves I*, Invent. Math. 109 (1992), 445 – 472.

[8] A. Brumer and O. McGuinness, *The behavior of the Mordell-Weil group of elliptic curves*, Bull. Amer. Math. Soc. 23 (1990), 375 – 382.

[9] Ph. Cassou-Noguès, *Quelques théorèmes de base normale d'entiers*, Ann. Inst. Fourier 28 (1978), 1 – 33.

[10] T. Chinburg, B. Erez, G. Pappas, and M. J. Taylor, *ε-constants and the Galois structure of de Rham cohomology*, Annals of Math. 146 (1997), 411 – 473.

[11] T. Chinburg, G. Pappas, and M. J. Taylor, *ε-constants and the Galois structure of de Rham cohomology II*, Jour. reine angew. Math. 519 (2000), 334 – 365.

[12] S. D. Chowla *The Riemann Hypothesis and Hilbert's Tenth Problem (Mathematics and its Applications Vol. 4)*, Gordon and Breach Science Publishers (1965)

[13] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge University Press (1980).

[14] P. Deligne, *Les constantes des équations fonctionelles des fonctions L*. In: *Modular Functions of One Variable, II*, Lect. Notes in Math. 349, Springer-Verlag (1973), 501–595.

[15] P. Deligne, *Les constantes locales de l'équation fonctionelle de la fonction L d'Artin d'une représentation orthogonale*, Invent. Math. 35 (1976), 299 – 316.

[16] P. Deligne, *Valeurs de fonctions L et périodes d'intégrales*. In: *Automorphic Forms, Representations, and L-Functions*, Proc. Symp. Pure Math. Vol. 33 – Part 2, Amer. Math. Soc. (1979), 313 – 346

[17] C. Deninger, *L-functions of mixed motives*. In: *Motives*, Proc. Symp. Pure Math. Vol. 55 – Part 1, Amer. Math. Soc. (1994), 517 – 525.

[18] J. Ellenberg and A. Venkatesh *Reflection principles and bounds for class group torsion* Int. Math. Res. Not. (2007).

[19] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörper*, Inventiones Math. 73 (1983), 349 – 366.

[20] J.-M. Fontaine and B. Mazur, *Geometric Galois representations*. In: *Elliptic Curves, Modular Forms, & Fermat's Last Theorem*, J. Coates and S.-T. Yau, eds. International Press, Cambridge MA (1997), pp. 190 – 227.

[21] A. Fröhlich, *Artin root numbers and normal integral bases for quaternion fields*, Inventiones Math. 17 (1972), 143 – 166.

[22] A. Fröhlich and J. Queyrut, *On the functional equation for the Artin L-function for characters of real representations*, Inventiones Math. 20 (1973), 125–138.

[23] P. X. Gallagher, *Determinants of representations of finite groups*, Abh. Math. Sem. Univ. Hamburg 28 (1965), 162–167.

[24] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*. In: *Number Theory, Carbondale, 1979*, Springer, Lecture Notes in Math. 751 (1979), 108 – 118.

[25] R. Greenberg, *Iwasawa theory for p-adic representations*. In: *Algebraic Number Theory – in honor of K. Iwasawa*, Advanced Studies in Pure Mathematics 17 (1989), pp. 97 – 137.
[26] B. H. Gross, *Arithmetic on Elliptic Curves with Complex Multiplication*, SLN 776, Springer-Verlag (1980).
[27] B. H. Gross and D. B. Zagier, *Heegner points and derivatives of L-series*, Inventiones Math. 84 (1986), 225 – 320.
[28] D. R. Heath-Brown, *The average rank of elliptic curves*, Duke Math. J. 122 (2004), 225 – 320.
[29] D. R. Heath-Brown and S. J. Patterson, *The distribution of Kummer sums at prime arguments*, J. reine angew. Math. 310 (1979), 111 – 130.
[30] E. Hecke, *Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen. Zweite Mitteilung*, Math. Z. 6 (1920), 11 – 51.
[31] E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, Chelsea Publishing Company, 2nd ed. (1970).
[32] H. Iwaniec, W. Luo, and P. Sarnak, *Low lying zeros of families of L-functions*, Publ. Math. Inst. Hautes Etudes Sci. 91 (2000), 55 – 131.
[33] H. Iwaniec and P. Sarnak, *Dirichlet L-functions at the central point*. In: *Number Theory in Progress* vol. 2, de Gruyter, Berlin (1999), 941 – 952.
[34] M. Jutila, *On the mean value of $L(1/2, \chi)$ for real characters*, Analysis 1 (1981), 149 – 161.
[35] S. Katayama, *On fundamental units of real quadratic fields with norm +1*, Proc. Japan Acad. 68 Ser. A (1992), 18 – 20.
[36] V. A. Kolyvagin and D. Yu. Logachev, *Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties* (Russian), Algebra i Analiz 1 (1989), 171 – 196. Translation: Leningrad Math. J. 1 (1990) 1229 – 1253.
[37] S. Lang *Algebraic Number Theory*, Springer-Verlag.
[38] S. Lang and H. Trotter, *Frobenius Distributions in GL_2-Extensions*, Springer-Verlag, LNM vol. 504 (1976).
[39] Chunlei Liu and Lanju Xu *The vanishing order of certain Hecke L-functions of imaginary quadratic fields*, J. of Number Thy. 108 (2004), 76-89.
[40] R. Masri, *Quantitative nonvanishing of L-series associated to canonical Hecke characters*, IMRN (2007).
[41] R. Masri, *Asymptotics for sums of central values of canonical Hecke L-series*, IMRN (2007).
[42] C. R. Matthews, *Gauss sums and elliptic functions: I. The Kummer sum*, Inventiones math. 52 (1979), 163 – 185.
[43] C. R. Matthews, *Gauss sums and elliptic functions: II. The quartic sum*, Inventiones math. 54 (1979), 23 – 52.
[44] S.D. Miller and T. H. Yang *Non-vanishing of the central derivative of canonical Hecke L-functions*, Math. Res. Lett. 7 (2000), 263 – 277.
[45] H. Montgomery and D. E. Rohrlich *On the L-functions of canonical Hecke characters of imaginary quadratic fields. II* Duke Math. J. 49 (1982), 937-942.
[46] F. Rodriguez-Villegas, *Square root formulas for central values of Hecke L-series. II* Duke Math. J. 72 (1993), 431 – 440.
[47] D. E. Rohrlich, *On the L-functions of canonical Hecke characters of imaginary quadratic fields*, Duke Math. J. 47 (1980), 547 – 557.
[48] D. E. Rohrlich, *Root numbers of Hecke L-functions of CM fields*, Am. J. Math. 104 (1982), 517 – 543.
[49] D. E. Rohrlich, *Compatible families of elliptic type*, to appear.
[50] K. Rubin, *Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer*, Inventiones Math. 64 (1981), 455 – 470.
[51] K. Rubin and A. Silverberg, *Ranks of elliptic curves*, Bull. Amer. Math. Soc. 39 (2002), 455 – 474.
[52] P. Schneider, *Introduction to the Beilinson conjectures*. In: *Beilinson's Conjectures on Special Values of L-Functions*, Academic Press (1988), 1 – 33.
[53] J-P. Serre, *Facteurs locaux de fonctions zêta des variétés algébriques (définitions et conjectures)*. In: Séminaire Delange-Poitou-Pisot, 1969/70, no. 19.
[54] J-P. Serre, *Abelian ℓ-Adic Representations and Elliptic Curves*, W. A. Benjamin, 1968.
[55] J-P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. of Math. 88 (1968), 492 – 517.

[56] J-P. Serre, *Local Fields*, Springer GTM 67 (1979).
[57] G. Shimura, *The special values of the zeta functions associated with cusp forms*, Comm. Pure Appl. Math. 29 (1976), 783 – 804.
[58] G. Shimura, *On the periods of modular forms*, Math. Ann. 229 (1977), 211 – 221.
[59] V. P. Snaith, *Explicit Brauer Induction*, Cambridge Studies in Advanced Math. 40, Cambridge Univ. Press (1994).
[60] K. Soundararajan, *Nonvanishing of quadratic Dirichlet L-functions at* $s = 1/2$, Ann. of Math. 152 (2000), 447 – 488.
[61] W. Stein and M. Watkins, *A database of elliptic curves – first report*. In: *Algorithmic Number Theory (Sydney, 2002)*, Springer Lecture Notes in Comput. Sci. 2369, Springer (2002), 267 – 275.
[62] J. Tate, *Number theoretic background*. In: *Automorphic Forms, Representations, and L-Functions*, Proc. Symp. Pure Math. Vol. 33 – Part 2, Amer. Math. Society (1979), 3 – 26.
[63] M. J. Taylor, *On Fröhlich's conjecture for rings of integers of tame extensions*, Inventiones Math. 63 (1981), 41 – 79.
[64] A. B. Venkov, *Selberg's trace formula for the Hecke operator generated by an involution, and the eigenvalues of the Laplace-Beltrami operator on the fundamental domain of the modular group PSL(*$2, \mathbb{Z}$*)*, Math. USSR Izvestija 12 (1978), 448 – 462.
[65] M. Watkins, *Some heuristics about elliptic curves*, Experimental Math. 17 (2008), 105 – 125.
[66] T. H. Yang, *On CM abelian varietiers over imaginary quadratic fields*, Math. Ann. 329 (2004), 87 – 117.
[67] T. H. Yang, *Nonvanishing of the central value of Hecke characters and the rank of their associated elliptic curves*, Compositio Math. 117 (1999), 337-359.
[68] M. P. Young, *Low-lying zeros of families of elliptic curves*, J. Amer. Math. Soc. 19 (2005), 205 – 250.
[69] M. P. Young, *Analytic number theory and ranks of elliptic curves*. In: *Ranks of Elliptic Curves and Random Matrix Theory*, London Math. Soc. Lecture Note Ser. 341, Cambridge University Press (2007), 71 – 92.