Contents

Root numbers
David E. Rohrlich 1

Root numbers 3
Introduction 3

Lecture 1. Trivial central zeros 5
1. Nonexistence of trivial central zeros for Dirichlet L-functions 6
2. Hecke characters and Hecke L-functions 7
3. A family of Hecke L-functions with trivial central zeros 11
4. An open problem 18
5. Evaluation of the quadratic Gauss sum 19
6. Exercises 23

Lecture 2. Local formulas 25
1. The idele class group 25
2. Idele class characters 26
3. The functional equation 30
4. Quadratic root numbers 32
5. Local root numbers 34
6. An open problem 36
7. Epsilon factors 38
8. Exercises 46

Lecture 3. Motivic L-functions 49
1. Artin representations and Artin L-functions 49
2. The functional equation 53
3. Compatible families 55
4. Premotives 61
5. Uniqueness of the functional equation 62
6. An open problem 63
7. Local factors for Artin L-functions 63
8. Exercises 65

Lecture 4. Local formulas in arbitrary dimension 67
1. The local Weil and Weil-Deligne groups 67
2. From Galois representations to Weil-Deligne representations 71
3. An open problem 75
4. Local factors 76
5. Normalizations of the root number in the literature 81
6. Exercises 81

Lecture 5. The minimalist dichotomy 83
1. Elliptic curves 84
2. The minimalist trichotomy 86
3. Elliptic curves revisited 88
4. An open problem 91
5. Exercises 92

Bibliography 93

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 its 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 roughly to four possibilities for the underlying 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 unspecified "L-functions" 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 with its λ-adic topology or the algebraic closure of a finite field with the discrete topology. 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 character 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 often 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": there is an open neighborhood $\mathcal{U}$ of the identity in $\mathrm{GL}_n(\mathbb{C})$ 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). Suppose now that 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.

Although we have made a point of proving this little fact about profinite groups, in the pages that follow results both large and small will usually be stated without proof. In particular we do not reproduce Tate's proof of the functional equation of Hecke L-functions or Deligne's proof of the existence of local epsilon factors. On the other hand, we do include some rather detailed proofs of statements for which a convenient reference to the literature is lacking, and occasionally we also include a proof to emphasize a point (as in the previous paragraph) or to illustrate a technique. In the end, both the omission of most proofs and the inclusion of some reflect our overall aim, which is to complement the literature rather than duplicate it and to emphasize motivation rather than foundations.

It is a pleasure to record my indebtedness to many people: to the organizers of the conference, Cristian Popescu, Karl Rubin, and Alice Silverberg; to the participants in the conference, especially Keith Conrad, Ralph Greenberg, Dick Gross, Chan-Ho Kim, Myoungil Kim, Thomas de La Rochefoucauld, Álvaro Lozano-Robledo, Rachel Newton, Sami Omar, Robert Pollack, and John Tate; and to many other people whose help I solicited along the way, especially Avner Ash, Barbara Beeton, Philippe Cassou-Noguès, Pierre Deligne, John Polking, and Fernando Rodriguez Villegas. To all of them I extend my sincere thanks.

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

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

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

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

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

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

where

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

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 $W(\chi) = 1$.*

In spite of our disclaimer in the introduction, we will actually give a proof of Theorem 1.1 at the end of the lecture. 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 $s = -2, -4, -6, \ldots$ 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

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

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 $\Lambda(s, \chi) = N^{s/2}\,\Gamma_{\mathbb{R}}(s + m)L(s, \chi)$. Here $W(\chi)$ and m 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 [**6**], [**20**], [**46**], [**47**], [**69**], [**72**], and [**90**]), 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 [**9**] 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. This phenomenon will be illustrated here not using elliptic curves with complex multiplication by $\mathbb{Q}(i)$ as in [**9**] but rather with the "$\mathbb{Q}$-curves" of Gross [**38**], for which the field of complex multiplication varies. But first of all we provide 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 consisting of such $\mathfrak{a}$ will be denoted $I(\mathfrak{f})$, and the subgroup $P \cap I(\mathfrak{f})$ of principal fractional ideals in $I(\mathfrak{f})$ will be denoted $P(\mathfrak{f})$. Note by the way 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 $\alpha\mathcal{O} \in P(\mathfrak{f})$, and we write $K(\mathfrak{f})$ for the subgroup of $K^\times$ consisting of all such α. Thus $K(\mathfrak{f})$ is $(S^{-1}\mathcal{O})^\times$, the group of units of the localization of $\mathcal{O}$ at the multiplicative set

$$S = \bigcap_{\mathfrak{p}|\mathfrak{f}} (\mathcal{O} \smallsetminus \mathfrak{p})$$

(with $S = \mathcal{O} \smallsetminus \{0\}$ if $\mathfrak{f} = \mathcal{O}$). Given $\alpha \in K^\times$, we write $\alpha \equiv 1 \bmod^* \mathfrak{f}$ to mean that for every prime ideal $\mathfrak{p}$ dividing $\mathfrak{f}$ we have $v_\mathfrak{p}(\alpha - 1) \geqslant \mathrm{ord}_\mathfrak{p}\mathfrak{f}$, where $v_\mathfrak{p}$ is the valuation associated to $\mathfrak{p}$ and $\mathrm{ord}_\mathfrak{p}\mathfrak{f}$ the multiplicity of $\mathfrak{p}$ in $\mathfrak{f}$. More succinctly, $\alpha \equiv 1 \bmod^* \mathfrak{f}$ means $\alpha \equiv 1 \bmod \mathfrak{f}(S^{-1}\mathcal{O})$. The set of all such α is a subgroup $K_\mathfrak{f}$ of $K(\mathfrak{f})$, and we write $P_\mathfrak{f}$ for the subgroup of $P(\mathfrak{f})$ consisting of all $\alpha\mathcal{O} \in P(\mathfrak{f})$ with $\alpha \in K_\mathfrak{f}$.

A **Hecke character of** K **to the modulus** $\mathfrak{f}$ is a group homomorphism $\chi : I(\mathfrak{f}) \to \mathbb{C}^\times$ with the following property: 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 $\chi(\alpha\mathcal{O}) = \chi_\infty^{-1}(\alpha)$. Here we are identifying $\alpha \in K^\times$ with $1 \otimes \alpha \in (\mathbb{R} \otimes_\mathbb{Q} K)^\times$, as is often convenient. Without this identification the condition on χ reads

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

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

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

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

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

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

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 $\mathfrak{f}'$ the **conductor** of χ and χ' the **primitive Hecke character determined by** χ. 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 $\chi(\alpha\mathcal{O}) = \chi_\infty^{-1}(1 \otimes \alpha)$ for all $\alpha \in K^\times$. Consider for instance the **power-of-the-norm** map $\chi : I \to \mathbb{C}^\times$ given by $\chi(\mathfrak{a}) = (\mathbf{N}\mathfrak{a})^{s_0}$, where $s_0 \in \mathbb{C}$ 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

$$\chi_\infty(u_1, u_2, \ldots, u_{r_1+r_2}) = |u_1 u_2 \cdots u_{r_1}|^{-s_0} \cdot |u_{r_1+1} u_{r_1+2} \cdots u_{r_1+r_2}|^{-2s_0}. \tag{1.13}$$

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 $\chi : I \to \{\pm 1\}$ (the "Liouville function" of K) by specifying that $\chi(\mathfrak{p}) = -1$ for every prime ideal $\mathfrak{p}$. Equivalently,

$$\chi(\mathfrak{a}) = (-1)^{\Omega(\mathfrak{a})},$$

where $\Omega(\mathfrak{a})$ 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 $\Omega(\alpha\mathcal{O})$ is even and the set of α such that $\Omega(\alpha\mathcal{O})$ 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_{unit}, so that $\chi = \chi_{\text{unit}} \cdot |\chi|$.

Proposition 1.1. *If χ is a Hecke character of K then there exists $c \in \mathbb{R}$ such that $|\chi| = \mathbf{N}^c$, whence*

$$\chi = \chi_{\text{unit}} \cdot \mathbf{N}^c.$$

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

Proof. Let $\mathbb{R}_{>0}$ denote the multiplicative group of positive real numbers. The point requiring proof is that a Hecke character with values in $\mathbb{R}_{>0}$ coincides with a real power of the norm. So after changing notation we may suppose that χ is a Hecke character $I(\mathfrak{f}) \to \mathbb{R}_{>0}$, and we must show that $\chi = \mathbf{N}^c$ for some $c \in \mathbb{R}$. It will suffice to see that χ_∞ has the form (1.13) with $s_0 \in \mathbb{R}$, for then we may take $c = s_0$. Indeed if c is so chosen then $\chi \cdot \mathbf{N}^{-c}$ is a character with values in $\mathbb{R}_{>0}$ which factors through the finite group $I(\mathfrak{f})/P_{\mathfrak{f}}$, and consequently $\chi \cdot \mathbf{N}^{-c}$ is trivial.

Put $\mathbf{T} = \{e^{i\theta} : \theta \in \mathbb{R}\}$, so that we have topological group isomorphisms $\mathbb{R}^\times \cong \{\pm 1\} \times \mathbb{R}_{>0}$ and $\mathbb{C}^\times \cong \mathbf{T} \times \mathbb{R}_{>0}$. Any continuous homomorphism $\mathbb{R}_{>0} \to \mathbb{R}_{>0}$ raises the elements of $\mathbb{R}_{>0}$ to some fixed real exponent, which we can of course choose to write as twice some other real exponent. Thus χ_∞ has the form

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

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

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

Hence using the notation of (1.12) we deduce from (1.14) that

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

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

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

vanishes identically on the hyperplane $\sum_{j=1}^{r_1} t_j + \sum_{j=r_1+1}^{r_1+r_2} 2t_j = 0$. It follows that c_j is a constant c independent of j, whence (1.14) is indeed of the form (1.13) with $s_0 = c$, a real number. □

2.5. Hecke L-functions

If χ is a Dirichlet character to the modulus N then one puts $\chi(n) = 0$ 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 $\mathfrak{a}$ is not relatively prime to $\mathfrak{f}$, 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 $\mathfrak{a} \mapsto (\mathbf{N}\mathfrak{a})^{s_0}$ then $L(s, \chi) = \zeta_K(s - s_0)$. 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 of the form $\mathbf{N}^{s_0}$) or holomorphic except for a simple pole at $s = s_0 + 1$ (if $\chi = \mathbf{N}^{s_0}$) and which satisfies a functional equation relative to $s \mapsto 2c + 1 - s$. We will say more about the functional equation in Lecture 2, but returning for now to the right half-plane of absolute convergence, we observe that $L(s, \chi)$ has 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 $\mathfrak{f} = N\mathbb{Z}$ 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 $\chi(\mathfrak{a}) = \chi(a)$. Furthermore, 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 character 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 $\chi : I(\mathfrak{f}) \to \mathbb{C}^\times$ and $\chi_\infty : (\mathbb{R} \otimes_{\mathbb{Q}} K)^\times \to \mathbb{C}^\times$ be respectively a homomorphism and 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 $\varepsilon(\alpha)$. At the same time we see that $\varepsilon : K(\mathfrak{f}) \to \mathbb{C}^\times$ is a homomorphism trivial on $K_{\mathfrak{f}}$ and so may 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. After fixing an embedding of K in $\mathbb{C}$ we can identify $\mathbb{R} \otimes_{\mathbb{Q}} K$ with $\mathbb{C}$ and hence $(\mathbb{R} \otimes_{\mathbb{Q}} K)^\times$ with $\mathbb{C}^\times$. Thus if χ is a Hecke character of K then χ_∞ is a continuous homomorphism from $\mathbb{C}^\times$ to itself, and we can ask whether χ_∞ is the character $z \mapsto z^{-1}$. If it is then 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).

As we have already indicated, our goal is to exhibit the trivial central zeros found by Gross [**38**] in his study of $\mathbb{Q}$-curves. As a first step we exhibit the relevant Hecke characters of K of type $(1,0)$. Let D be the absolute value of the discriminant of K, so that $K = \mathbb{Q}(\sqrt{-D})$. The set of Hecke characters at issue will be denoted $X(D)$. To define $X(D)$ precisely, let κ be the primitive quadratic Dirichlet character of conductor D given by

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

where the Kronecker symbol on the right is understood to equal -1 when $n = -1$ (in other words, the Kronecker symbol is viewed as a Dirichlet character rather than as a norm residue symbol). Then $X(D)$ consists of all primitive Hecke character χ of K of type (1,0) satisfying three conditions:

(a) $\mathfrak{f}(\chi)|D^\infty$. (In other words, $\mathfrak{f}(\chi)$ divides some power of D.)
(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. Consider characters of the form $\varepsilon : (\mathcal{O}/\mathfrak{f})^\times \to \{\pm 1\}$ with $\mathfrak{f}|D^\infty$. We impose two conditions: First, $\varepsilon(n) = \kappa(n)$ for $n \in \mathbb{Z}$ relatively prime to D, and second, ε is primitive in the usual sense that ε does not factor through $(\mathcal{O}/\mathfrak{f}')^\times$ for any ideal $\mathfrak{f}'$ properly dividing $\mathfrak{f}$. The set of such ε will be denoted E. 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 arbitrarily to $I(\mathfrak{f})$ we obtain an element of $X(D)$.

We must now prove (1.21). Given $\varepsilon \in E$, write $\mathfrak{f}(\varepsilon)$ for the ideal $\mathfrak{f}$ such that ε is a primitive character of $(\mathcal{O}/\mathfrak{f})^\times$. Also, if $D||4$ then let $\mathfrak{T}$ denote the prime ideal of $\mathcal{O}$ lying over 2. We claim 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. 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).

At this point we 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 see that

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

for $\chi \in X(D)$, because it follows from (1.22) that $\mathfrak{f}(\chi) = \mathfrak{f}(\varepsilon)$.

Next suppose that $4||D$. Then $D = 4C$ with $C \equiv 1 \bmod 4$. If there exists an $\varepsilon \in E$, then $\sqrt{-C}\mathfrak{T}^3|\mathfrak{f}(\varepsilon)$ by (1.23); we claim that in fact

$$\mathfrak{f}(\varepsilon) = \sqrt{-C}\mathfrak{T}^k \qquad \text{with } k = 3 \text{ or } 4. \tag{1.25}$$

To see this, we first argue as in the case D odd: Since ε is quadratic and primitive, the kernel of the reduction map $(\mathcal{O}/\mathfrak{f}(\varepsilon))^\times \to (\mathcal{O}/\sqrt{-C}\mathfrak{T}^3)^\times$ has 2-power order. As $\mathfrak{f}(\varepsilon)|D^\infty$ this already implies that $\mathfrak{f}(\varepsilon) = \sqrt{-C}\mathfrak{T}^k$ with $k \geqslant 3$. But one checks 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 $k = 3, 4$, 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

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

and $\varepsilon = \varepsilon'\varepsilon''$ with quadratic characters ε' and ε'' of $(\mathcal{O}/\mathfrak{T}^k)^\times$ 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 $(\mathcal{O}/\mathfrak{T}^k)^\times$ for $k = 4$ and *a fortiori* for $k = 3$: indeed $(2 + \sqrt{-C})^2 \equiv -1 \bmod 4\mathcal{O}$.

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

$\mathfrak{f}(\varepsilon) = 2\sqrt{-D}\mathcal{O}$. Now write $D = 8C$, and let $\mathfrak{C}$ be the product of the prime ideals of $\mathcal{O}$ dividing C. We have $(\mathcal{O}/2\sqrt{-D}\mathcal{O})^\times \cong (\mathcal{O}/\mathfrak{T}^5)^\times \times (\mathcal{O}/\mathfrak{C})^\times$ and a corresponding decomposition of characters $\varepsilon = \varepsilon'\varepsilon''$. Also $(\mathbb{Z}/D\mathbb{Z})^\times \cong (Z/8\mathbb{Z})^\times \times (Z/C\mathbb{Z})^\times$ and $\kappa = \kappa'\kappa''$. Using the natural embedding of $(Z/C\mathbb{Z})^\times$ in $(\mathcal{O}/\mathfrak{C})^\times$ 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 $(\mathcal{O}/\mathfrak{T}^5)^\times$ realizes $(\mathbb{Z}/8\mathbb{Z})^\times$ as one summand in a direct sum decomposition of $(\mathcal{O}/\mathfrak{T}^5)^\times$, 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 possibilities for the value of ε' on the coset of $1 + \sqrt{-2C}$, namely ±1. Thus $|E| = 2$. Furthermore, we see that

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

for $\chi \in X(D)$, because if χ and ε are related as in (1.22) then $\mathfrak{f}(\chi) = \mathfrak{f}(\varepsilon)$. □

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 primitive 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 of $L(s, \chi)$. One such 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 ([**38**], 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 $|X(D)| = 2h(D)$. A proof of the following statement (albeit a proof in a more general context) can be found in [**76**], pp. 538 – 541, and a proof in the present setting will be outlined in Exercise 2.4.

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 positive, 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 1.5 and 1.6 imply that $L(s, \chi)$ has a trivial central zero if and only if either $D \equiv 3$ mod 8 or else $8|D$ and $\chi \in X^-(D)$. In the remaining cases, when $D \equiv 7$ mod 8 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.

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

For the proof see Montgomery-Rohrlich [**66**] or Miller-Yang [**65**] according as $W(\chi)$ is 1 or -1. 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 $\mathfrak{a} \in I(\mathfrak{f})$, where $\mathfrak{f} = \mathfrak{f}(\chi)$. As the values of χ on principal ideals 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 $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_t \in I(\mathfrak{f})$ 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 $\chi(\mathfrak{a}_1), \chi(\mathfrak{a}_2), \ldots, \chi(\mathfrak{a}_t)$ 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 [**87**], [**88**] 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 [**39**] 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 $h(D)^{-1}\sum_{\varphi\in\Phi} L(1,\chi\varphi) \neq 0$ or that $h(D)^{-1}\sum_{\varphi\in\Phi} L'(1,\chi\varphi) \neq 0$ according as $W(\chi) = 1$ or $W(\chi) = -1$. The point of this reduction is that as a Dirichlet series, $L(s,\chi)$ 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 only. Analytically the latter sum 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 definition 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 $p \equiv 3$ mod 4 ($p > 3$), by a consideration of minimal discriminants (Gross [**38**], 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 [**78**] of the Coates-Wiles theorem (if $W(\chi) = 1$) or the Gross-Zagier formula [**39**] and the theorem of Kolyvagin-Logachev [**54**] supplemented by either Bump-Friedberg-Hoffstein [**14**] or Murty-Murty [**70**] (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 then 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 $p \equiv 7$ mod 8, the fact that $A(p)(F)$ has rank 0 was proved by Gross [**38**] 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 [**101**] 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 [**38**].) But if $4||D$ then B need not be the restriction of scalars of any elliptic curve over H. Nonetheless, Yang proves analogues for 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. We are primarily concerned with the case where w is odd, but to carry along both cases for one moment longer, 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

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

(see Exercise 2.5). We note in particular that the center of symmetry of the functional equation is $(w + 1)/2$. Thus if w is odd then the center is an integer, and in fact a critical integer in the sense of Deligne [**24**].

Problem 1. *Suppose that w is odd and relatively prime to $h(D)$. Show that*

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

An example of Rodriguez Villegas shows that the assumption $\gcd(w, h(D)) = 1$ cannot be omitted if (1.38) is to hold without exception ([**74**], p. 437, Remark 2), but we would also like a variant of the problem in which the coprimality hypothesis is eliminated at the expense of a weaker conclusion. However to begin with let us consider the problem as stated. A basic result in this domain is the theorem of Liu and Xu [**58**], who have shown that if w is given then there exists a constant $c(w)$ such that (1.38) is satisfied for $D \geqslant c(w)$. As is common in papers of this sort (cf. [**59**], [**60**], [**75**], and [**102**]), the authors actually prove the stronger statement that (1.38) remains valid when $L(s, \chi^w)$ is replaced by $L(s, \chi^w\mu)$ with a primitive quadratic Dirichlet character μ of sufficiently small conductor d relative to D (the precise condition in [**58**] is $d \ll D^{1/12-\varepsilon}$ for any $\varepsilon > 0$; of course D must still be sufficiently large relative to w). On the other hand, if $W(\chi) = 1$ then the constant $c(w)$ implicit in [**58**] is ineffective, so that the validity of (1.38) for all D is not reduced to a finite number of verifications even when w is fixed. However in the case where D is a prime p, necessarily with $p \equiv 3 \bmod 4$, Boxer and Diao [**10**] have recently proved a result which is not only effective but also remarkably tidy: If $W(\chi) = 1$ and $p \geqslant 13(w - 1)^2/8$ then $L((w + 1)/2, \chi^w) \neq 0$. Using Proposition 1.5 and (1.37), one readily verifies that when $D = p$ the condition $W(\chi) = 1$ is equivalent to $w \equiv (-1)^{(p+1)/4} \bmod 4$, so the result of Boxer and Diao is as explicit as can be. Even so, the validity of (1.38) for all D and all odd w prime to $h(D)$ remains an open problem.

If the condition $\gcd(w, h(D)) = 1$ is dropped then the problem is not only open but open-ended in the sense that we lack a conjecture to guide us. The most optimistic conjecture would be that (1.38) holds for all but finitely many triples (w, D, χ) with $\chi \in X(D)$, but the evidence is as yet too weak to support this hope. The underlying problem here is that most attempts to prove (1.38) begin by showing that (1.38) holds for *some* $\chi \in X(D)$, and if the characters $\chi^w\varphi$ with $\varphi \in \Phi$ are all Galois-conjugate (in other words, if χ can be replaced by χ^w in (1.32)) then one deduces that (1.38) holds for *all* $\chi \in X(D)$. The deduction here is based on Shimura [**87**] as before if $W(\chi^w) = 1$ and on Zhang [**105**] rather than Gross-Zagier [**39**] if $W(\chi^w) = -1$ with $w \geqslant 3$. But if $\gcd(w, h(D)) > 1$ then the argument falls apart, because the characters $\chi^w\varphi$ are simply not all Galois-conjugate. Let $h_w(D)$ be the order of the quotient of the ideal class group by its subgroup of elements of order dividing w. Then the size of a Galois orbit of $\{\chi^w\varphi : \varphi \in \Phi\}$ is $h_w(D)$, so the fact that (1.38) holds for one element of $X(D)$ implies only that (1.38) holds for at least $h_w(D)$ elements. By estimating $h_w(D)$ using the recent bounds of Ellenberg and Venkatesh [**28**] on torsion in ideal class groups, Masri [**60**] deduces that the number of characters $\chi \in X(D)$ satisfying (1.38) for fixed w and $D = p$ is $\gg p^\delta$ for some $\delta > 0$ (for instance if $w = 3$ then δ can be any number $< 1/6$). If $w \geqslant 5$ then the results of [**28**] and hence of [**60**] depend on the generalized Riemann hypothesis, but Masri's papers [**59**] and [**60**] also give a second method which is based on the subconvexity results of Duke, Friedlander, and Iwaniec [**27**] and is independent of the generalized Riemann hypothesis. See also Masri-Yang [**61**]. The implicit constant $c(w)$ in [**60**] such that (1.38) holds for at least p^δ characters if $p \geqslant c(w)$ is ineffective, but once again Boxer and Diao [**10**] give an effective result: If $W(\chi^w) = 1$ and $D = p \geqslant 13(w-1)^2/8$ then the number of good characters is at least $h_w(D)$.

All of this meshes well with the example of Rodriguez Villegas [**74**] mentioned above, in which $D = 59$, $w = 3$, and $L(2, \chi^3) = 0$ for some $\chi \in X(D)$, despite the fact that $W(\chi^3) = 1$. The point is that $h(D) = 3$ in this case, in line with the preceding discussion. (Incidentally, Rodriguez Villegas deduces the vanishing of $L(2, \chi^3)$ from a calculation and an *a priori* bound on the denominator of the special value.) One might imagine that in this example there are infinitely many w divisible by 3 such that $W(\chi^w) = 1$ but $L((w+1)/2, \chi^w) = 0$ for some $\chi \in X(D)$. However this possibility is excluded by a general theorem of Greenberg [**36**], valid for any imaginary quadratic field K and any primitive Hecke character of K of type $(w, 0)$. In our setting, the theorem asserts that if we fix $\chi \in X(D)$ then there are only finitely many odd positive integers w such that $W(\chi^w) = 1$ but $L((w+1)/2, \chi^w) = 0$. Pondering this statement, we realize that Problem 1 is subsumed in a larger problem, still to be formulated, in which the hypothesis $\gcd(w, h(D)) = 1$ is omitted but the conclusion (1.38) is asserted to hold for as large a set of characters as possible. An optimal description of this set is the point that remains open-ended.

5. Evaluation of the quadratic Gauss sum

For the sake of contrasting two different techniques, we give a self-contained proof of Theorem 1.1 here and a proof of a more general statement in the next lecture. To get started we record a few facts about the "Fourier transform" on $\mathbb{Z}/N\mathbb{Z}$.

Let V be the complex vector space consisting of $\mathbb{C}$-valued functions on $\mathbb{Z}/N\mathbb{Z}$. The Fourier transform on $\mathbb{Z}/N\mathbb{Z}$ is the linear automorphism $f \mapsto \hat{f}$ of V, where

$$\hat{f}(x) = \sum_{y \in \mathbb{Z}/N\mathbb{Z}} f(y) e^{2\pi i xy/N}.$$

Sometimes we write $\hat{f}$ as $f\hat{\ }$. That $f \mapsto \hat{f}$ is an automorphism follows from the identity $(f\hat{\ })\hat{\ }(x) = Nf(-x)$, which in turn is a consequence of the calculation

$$(f\hat{\ })\hat{\ }(x) = \sum_{y \in \mathbb{Z}/N\mathbb{Z}} \hat{f}(y) e^{2\pi i xy/N} = \sum_{z \in \mathbb{Z}/N\mathbb{Z}} f(z) \sum_{y \in \mathbb{Z}/N\mathbb{Z}} e^{2\pi i (x+z)y/N}$$

(observe that the inner sum is N or 0 according as z is or is not $-x$). The main fact about the Fourier transform which is needed for the proof of Theorem 1.1 is a formula for $\widehat{\chi}$, where χ is a primitive Dirichlet character of conductor N. Here we are viewing χ as a character of $(\mathbb{Z}/N\mathbb{Z})^\times$ and hence as a function on $\mathbb{Z}/N\mathbb{Z}$ via the usual convention that $\chi(x) = 0$ if the residue class $x \in \mathbb{Z}/N\mathbb{Z}$ is not invertible.

The formula that we need is

$$\widehat{\chi} = \tau(\chi)\overline{\chi}. \tag{1.39}$$

To verify (1.39), we take $x \in \mathbb{Z}/N\mathbb{Z}$ and compute $\widehat{\chi}(x)$ from the definition:

$$\widehat{\chi}(x) = \sum_{y \in (\mathbb{Z}/N\mathbb{Z})^\times} \chi(y) e^{2\pi i xy/N}. \tag{1.40}$$

There are two cases to consider, according as x is a nonunit or a unit.

Suppose first that $x \in M\mathbb{Z}/N\mathbb{Z}$, where M is a divisor of N and $M > 1$. To prove (1.39) in this case we must see that the right-hand side of (1.40) is 0. Put $G = (\mathbb{Z}/N\mathbb{Z})^\times$ and let H be the kernel of the map from $(\mathbb{Z}/N\mathbb{Z})^\times$ to $(\mathbb{Z}/(N/M)\mathbb{Z})^\times$ given by reduction modulo N/M. Write $y = gh$, where $h \in H$ and g runs over a set of coset representatives for H in G. Then $\chi(y) = \chi(g)\chi(h)$, and since χ is primitive $\chi|H$ is nontrivial. If we write the right-hand side of (1.40) as a double sum consisting of an inner sum over h and an outer sum over g, then the inner sum is 0 for each g, because $\chi|H$ is nontrivial and $e^{2\pi i xgh/N}$ is independent of h.

Next suppose that $x \in (\mathbb{Z}/N\mathbb{Z})^\times$. Then in the sum over y we can replace y by yx^{-1}, and referring to the definition (1.2) we see that $\widehat{\chi}(x) = \tau(\chi)\overline{\chi}(x)$. This completes the proof of (1.39).

An immediate corollary of (1.39), given the relation $(f\hat{\ })\hat{\ }(x) = Nf(-x)$, is that

$$\tau(\chi)\tau(\overline{\chi}) = \chi(-1)N. \tag{1.41}$$

It follows in particular that if χ is quadratic then $\tau(\chi)^2 = \chi(-1)N$. Thus the validity of (1.1) up to sign is easy, as already mentioned. Returning to the case of an arbitrary primitive χ, and observing that (1.39) and (1.40) together give $\overline{\tau(\chi)} = \chi(-1)\tau(\overline{\chi})$, we deduce from (1.41) that

$$|\tau(\chi)| = \sqrt{N}. \tag{1.42}$$

Of course both (1.41) and (1.42) can be reformulated in terms of root numbers: Applying the definition (1.3), we obtain

$$W(\chi)W(\overline{\chi}) = 1 \tag{1.43}$$

and

$$|W(\chi)| = 1 \tag{1.44}$$

respectively.

So much for general orientation. We turn now to the proof of Theorem 1.1 itself. The key step is the special case (1.1), for which we use an argument of Schur.

5.1. Schur's proof

Now take $N = p$ and write $\mathcal{F}$ for the Fourier transform $f \mapsto \hat{f}$ on V. To prove (1.1) we put

$$Q = \frac{\det \mathcal{F}}{|\det \mathcal{F}|}. \tag{1.45}$$

and 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 $e^{2\pi ijk/p}$ as its (j,k) entry, and consequently $\det \mathcal{F}$ is a Vandermonde determinant:

$$\det \mathcal{F} = \prod_{0 \leqslant j < k \leqslant p-1} (e^{2\pi ik/p} - e^{2\pi ij/p}). \tag{1.46}$$

To compute Q we can replace $\det \mathcal{F}$ in (1.45) by any positive scalar multiple of $\det \mathcal{F}$. In particular, the factors in (1.46) with $j = 0$ can be removed from (1.46), because the factors corresponding to $(0,k)$ and $(0, p-k)$ are complex conjugates, hence their product is positive. Now the remaining factors correspond to pairs (j,k) with $1 \leqslant j < k \leqslant p-1$, and the map $(j,k) \mapsto (p-k, p-j)$ is an involution on the set of such pairs. Furthermore the fixed points are precisely the pairs $(j, p-j)$ with $1 \leqslant j \leqslant (p-1)/2$, and if (j,k) is not a fixed point then the factor corresponding to $(p-k, p-j)$ is the negative of the complex conjugate of the factor corresponding to (j,k). The upshot of these remarks is that $Q = R/|R|$ with

$$R = (-1)^{(p-1)(p-3)/4} \prod_{1 \leqslant j \leqslant (p-1)/2} (e^{-2\pi ij/p} - e^{2\pi ij/p}).$$

But $(p-1)(p-3)/4$ is even, so the factor $(-1)^{(p-1)(p-3)/4}$ can be removed. Then

$$Q = (-i)^{(p-1)/2}, \tag{1.47}$$

because $e^{-2\pi ij/p} - e^{2\pi ij/p} = -2i \sin(2\pi j/p)$ 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 $\mathbb{F}_p^\times$. In conformity with a convention established earlier, 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

$$\chi_1, \overline{\chi}_1, \chi_2, \overline{\chi}_2, \ldots, \chi_{(p-3)/2}, \overline{\chi}_{(p-3)/2} \tag{1.48}$$

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

$$\lambda, \delta_0, \chi_0, \chi_1, \overline{\chi}_1, \chi_2, \overline{\chi}_2, \ldots, \chi_{(p-3)/2}, \overline{\chi}_{(p-3)/2} \tag{1.49}$$

is an ordered basis for V. Let us compute the matrix of $\mathcal{F}$ relative to this basis.

Since λ is quadratic we have $\mathcal{F}\lambda = \tau(\lambda)\lambda$ by (1.39). Furthermore $\mathcal{F}\delta_0 = \chi_0$, whence $\mathcal{F}\chi_0 = p\delta_0$ by the relation $(\mathcal{F}^2 f)(x) = pf(-x)$. Thus the matrix of $\mathcal{F}$

relative to the basis (1.49) is block-diagonal: The entry $\tau(\lambda)$ in the upper left-hand corner is followed by the 2×2 block

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

which is followed in turn by the 2×2 blocks – here we are using (1.39) again –

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

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 (1.41). Computing modulo positive real numbers, 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 (1.47) we obtain

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

Equivalently,

$$\frac{\tau(\lambda)}{\sqrt{p}} = i^{(p-1)/2}(-1)^{\nu}, \tag{1.50}$$

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 (1.48).

If $p \equiv 1 \bmod 4$ then all $(p-1)/2$ odd characters of $\mathbb{F}_p^\times$ occur in (1.48), because neither χ_0 nor λ is odd. Hence $\nu = (p-1)/4$ and the right-hand side of (1.50) 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 (1.48). Hence $\nu = (p-3)/4$ and the right-hand side of (1.50) is i. This completes Schur's proof of (1.1).

5.2. The general case

Now suppose 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 $N = N_1N_2$ and $\chi = \chi_1\chi_2$ with coprime integers N_1 and N_2 and primitive quadratic Dirichlet characters χ_1 and χ_2 of conductors N_1 and N_2 respectively. The numbers

$$j = j_1N_2 + j_2N_1 \qquad (0 \leqslant j_1 \leqslant N_1 - 1, \quad 0 \leqslant j_2 \leqslant N_2 - 1) \tag{1.51}$$

represent the distinct residue classes modulo N, and when j is written in this way we have $j/N = (j_1/N_1) + (j_2/N_2)$, $\chi_1(j) = \chi_1(j_1)\chi_1(N_2)$, and $\chi_2(j) = \chi_2(j_2)\chi_2(N_1)$. Hence inserting (1.51) in (1.2), we obtain

$$\tau(\chi) = \chi_1(N_2)\chi_2(N_1) \cdot \tau(\chi_1)\tau(\chi_2). \tag{1.52}$$

At this point it is convenient to write the integer m of (1.4) as $m(\chi)$ to indicate its dependence on χ. Dividing both sides of (1.52) by $\sqrt{N}\, i^{m(\chi)}$ and 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 appeared as equations (1.43) and (1.44) in the prolegomena to the proof of Theorem 1.1, we have said nothing at all about $W(\chi)$ when χ is a primitive Dirichlet character of order $\geqslant 3$. In this problem we assume that χ is not only primitive of order $\geqslant 3$ but also of prime conductor p. The easier case (easier in the sense that more complete results can be given) is actually the case of prime-power conductor p^ν with $\nu \geqslant 2$, for which see Exercises 1.4, 1.5, and 1.6 below.

(a) Stickelberger's theorem (see for example [**55**], p. 97, Theorem 10) gives a factorization of $\tau(\chi)^{p-1}$ as a product of prime ideals in the cyclotomic field $\mathbb{Q}(e^{2\pi i/(p-1)})$. Using this factorization, show that $W(\chi)$ is not an algebraic integer, and in particular not a root of unity, in spite of the fact that $|W(\chi^\sigma)| = 1$ for every automorphism σ of $\mathbb{C}$.

(b) (*Literature search.*) In the case where χ has order 3 or 4, Matthews [**62**], [**63**] expresses $\tau(\chi)$ in terms of values of the Weierstrass $\wp$-function at quadratic imaginary arguments. Furthermore, Heath-Brown and Patterson [**41**] 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. The purpose of this exercise and the two that follow is to show that if χ is a primitive Dirichlet character of conductor p^ν with $\nu \geqslant 2$ then $W(\chi)$ is a root of unity (in contrast to part (a) of Exercise 1.3).

(a) Suppose that χ is of p-power order (and hence of order dividing $p^{\nu-1}$). Using the defining formula (1.2) and (1.42), show that $\tau(\chi)$ is an element of $\mathbb{Z}[e^{2\pi i/p^\nu}]$ of absolute value $p^{\nu/2}$ in every complex embedding of $\mathbb{Q}(e^{2\pi i/p^\nu})$. Deduce that $\tau(\chi)^2$ is a root of unity times p^ν, and conclude that $W(\chi)$ is a root of unity.

(b) Deduce that if χ is primitive of conductor 2^ν then $W(\chi)$ is a root of unity.

Exercise 1.5. With notation as in Exercise 1.4, suppose that ν is even, and put $n = \nu/2$. Observe that $\chi(1+p^n(x+y)) = \chi(1+p^n x)\chi(1+p^n y)$ for $x, y \in \mathbb{Z}/p^n\mathbb{Z}$, and deduce that $W(\chi)$ is a root of unity. (Hint: Put $G = (\mathbb{Z}/p^\nu\mathbb{Z})^\times$ and let H be the kernel of $(\mathbb{Z}/p^\nu\mathbb{Z})^\times \to (\mathbb{Z}/p^n\mathbb{Z})^\times$. Express (1.2) as a sum over $j = gh$, where $h \in H$ and g runs over a set of coset representatives for H in G. Then write the sum over j as a double sum over g and h, and show that the inner sum over h is 0 for all but one value of g.)

Exercise 1.6. With notation as in Exercise 1.4, suppose that ν is odd and hence $\geqslant 3$, and put $m = (\nu-1)/2$. Since the case $p = 2$ has already been dealt with in part (b) of Exercise 1.4, we may assume that p is odd.

(a) Using the binomial theorem, show that $(1+p^m x)^p \equiv 1 + p^{m+1}x \bmod p^\nu$ for arbitrary $x \in \mathbb{Z}$.

(b) Using the hint for Exercise 1.5 with $n = m+1$, show that there is a unique element $c \in \mathbb{Z}/\mathbb{Z}p^m$ such that $\chi(1+p^n x) = e^{2\pi i c x/p^m}$ for $x \in \mathbb{Z}/p^m\mathbb{Z}$. Deduce that $\tau(\chi)$ is a root of unity times $p^m S$, where S is the sum

$$S = \sum_{x \in \mathbb{F}_p} \chi(1+p^m x) e^{2\pi i g_0 x/p^n}$$

and $g_0 \in \mathbb{Z}/\mathbb{Z}p^n$ is any element which reduces mod p^m to $-c$.

(c) Using (a), show that $\chi(1+p^m x)e^{2\pi i g_0 x/p^n}$ is a pth root of unity, whence $S \in \mathbb{Z}[e^{2\pi i/p}]$. Show that S has absolute value $p^{1/2}$ in every complex embedding of $\mathbb{Q}(e^{2\pi i/p})$, and conclude as in Exercise 1.4 that $W(\chi)$ is a root of unity.

Exercise 1.7. (*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 [**18**]? Soundararajan [**90**] 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 [**42**]. 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 $x = (x_v)$ of the usual direct product belongs to $\mathbb{A}$ 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) 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 $\mathbb{A}_\infty \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R} \otimes_{\mathbb{Q}} K$, 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:

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

but this time the restriction is that an element $x = (x_v)$ 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 $\mathbb{A}_{\text{fin}}$ is characterized by two properties:

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

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

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

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 $x = (x_v)$ such that $x_v = 1$ for $v \nmid \infty$. If $\mathbb{A}_{\text{fin}}^\times$ is similarly identified with the subgroup of $\mathbb{A}^\times$ consisting of ideles $x = (x_v)$ 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 $x \mapsto x_{\text{fin}}$ and $x \mapsto x_\infty$ respectively, so that $x = x_{\text{fin}} x_\infty$.

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) 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 v. 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 nontrivial or trivial. Now $\mathcal{O}_v^\times$ is precisely the set $\{x \in K_v^\times : |x|_v = 1\}$, and if we temporarily denote this set by $\mathcal{O}_v^\times$ even when v is an infinite place then 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.

The "seamless extension" just described is often useful, particularly when one wants to distinguish between "narrow ray class characters" and "wide ray class characters" in class field theory. But this distinction is tangential to the matter at hand, and henceforth we will speak of ramified and unramified characters only at the finite places, reserving the notation $\mathcal{O}_v^\times$ for the finite places also.

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,

$$\chi = \prod_v{}' \chi_v, \tag{2.8}$$

where the prime indicates that χ_v is unramified for all but finitely many finite v. It is only by virtue of this last property that (2.8) has a meaning, for we interpret (2.8) to mean that if $x = (x_v) \in \mathbb{A}^\times$ 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 also 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.* In fact one often identifies 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:

$$||x|| = \prod_v ||x_v||_v \qquad (x = (x_v) \in \mathbb{A}_K^\times). \tag{2.9}$$

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

$$L(s,\chi) = \prod_{\substack{v\nmid\infty \\ \chi_v \text{ unram}}} (1 - \chi_v(\pi_v) q_v^{-s})^{-1}, \tag{2.10}$$

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 (2.10) 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 $x = (x_v) \in \mathbb{A}_{\text{fin}}^\times$ 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

$$\mathbb{A}^\times = K^\times \cdot \mathbb{A}_{\mathfrak{f}} \cdot (\mathbb{R} \otimes_{\mathbb{Q}} K)^\times \tag{2.11}$$

with

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

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 (2.11) to write

$$x = \alpha \cdot y \cdot r \tag{2.13}$$

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

$$\chi_{\mathbb{A}}(x) = \chi(\mathfrak{a}_y)\chi_\infty(r), \tag{2.14}$$

where

$$\mathfrak{a}_y = \prod_{v \nmid \infty} \mathfrak{p}_v^{\mathrm{ord}_v y_v} \tag{2.15}$$

and $\mathfrak{p}_v$ is the prime ideal of $\mathcal{O}$ 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 (2.15) 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 (2.12), the definition (2.14) is unambiguous provided the right-hand side is trivial whenever $x = 1$, $y = \alpha_{\mathrm{fin}}^{-1}$, and $r = \alpha_\infty^{-1}$ with $\alpha \in K_{\mathfrak{f}}$. 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

$$\widehat{\mathcal{O}}_{\mathfrak{f}} = \mathbb{A}_{\mathfrak{f}} \cap \widehat{\mathcal{O}}^\times. \tag{2.16}$$

If y in (2.13) belongs to $\widehat{\mathcal{O}}_{\mathfrak{f}}$ then $\mathfrak{a}_y = \mathcal{O}$, whence (2.14) becomes $\chi_{\mathbb{A}}(x) = \chi_\infty(r)$. Furthermore, if x belongs to the open subgroup $\widehat{\mathcal{O}}_{\mathfrak{f}} \times (\mathbb{R} \otimes_{\mathbb{Q}} K)^\times$ of $\mathbb{A}^\times$ then we can take $y = x_{\mathrm{fin}}$ and $r = x_\infty$ in (2.13), 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, once one has the notion of a "conductor" (still to come), 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, (2.14) 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 (2.8). 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

$$\chi(\alpha\mathcal{O}) = \varepsilon(\alpha)\chi_\infty^{-1}(1 \otimes \alpha) \tag{2.17}$$

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

$$(\mathcal{O}/\mathfrak{f})^\times = \prod_{\mathfrak{p}|\mathfrak{f}} (\mathcal{O}/\mathfrak{p}^{n(\mathfrak{p})})^\times, \tag{2.18}$$

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

$$\varepsilon = \prod_{\mathfrak{p}|\mathfrak{f}} \varepsilon_{\mathfrak{p}}, \tag{2.19}$$

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.*

(a) *If $\mathfrak{p} \nmid \mathfrak{f}$ then χ_v is unramified and $\chi_v(\pi_v) = \chi(\mathfrak{p})$.*

(b) *If $\mathfrak{p}|\mathfrak{f}$ then $\chi_v|\mathcal{O}_v^\times = \varepsilon_v^{-1}$, whence χ_v is in particular ramified. Furthermore, suppose that for some $\beta \in \mathcal{O}$ the principal ideal $\beta\mathcal{O}$ is a power of $\mathfrak{p}$. Then*

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

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.

(a) Given $z \in \mathcal{O}_v^\times$, take $x = (x_w)$ 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 (2.13), whence $\mathfrak{a}_y = \mathcal{O}$. So (2.14) and (2.8) give $\chi_v(z) = \chi(x) = 1$, and we conclude that χ_v is unramified. On the other hand, choosing $x = (x_w)$ 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 (2.13), but this time we get $\mathfrak{a}_y = \mathfrak{p}$ and consequently $\chi_v(\pi_v) = \chi(\mathfrak{p})$.

(b) Given $z \in \mathcal{O}_v^\times$, take $x = (x_w)$ 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 (2.18), 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 $\alpha_{\text{fin}}^{-1}x \in \mathbb{A}_{\mathfrak{f}}$, so we may take $y = \alpha_{\text{fin}}^{-1}x$ and $r = \alpha_\infty^{-1}$ in (2.13). Then $\mathfrak{a}_y = \alpha^{-1}\mathcal{O}$, and consequently (2.14) gives $\chi(x) = \chi(\alpha^{-1}\mathcal{O})\chi_\infty(1 \otimes \alpha^{-1})$. Replacing α by α^{-1} in (2.17), 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 (2.8) and (2.19). Thus $\chi_v|\mathcal{O}_v^\times = \varepsilon_v^{-1}$.

Now suppose that $\beta\mathcal{O}$ is a power of $\mathfrak{p}$. Evaluating both sides of (2.8) at β gives

$$1 = \prod_{w|\mathfrak{f}\infty} \chi_w(\beta), \tag{2.20}$$

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 (2.20), we obtain the claimed formula for $\chi_v(\beta)$. $\square$

2.3. An example

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 (2.9). 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. In other words, if v is an infinite place then $\chi_v = || * ||_v^{-1}$. To see that the same is true at the finite places, let $\mathfrak{p}$ be a prime ideal of K and v the corresponding finite place. By part (a) of Proposition 2.1, χ_v is the unramified character of $K_v^\times$ taking the value $\mathbf{N}\mathfrak{p}$ on any uniformizer 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 again $\chi_v = || * ||_v^{-1}$, and we conclude that $\chi_{\mathbb{A}} = || * ||^{-1}$, as claimed.

2.4. The conductor

As pointed out 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 as in (2.8), 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 $\widehat{\mathcal{O}} = \varprojlim_{\mathfrak{f}} \mathcal{O}/\mathfrak{f}$ and $\widehat{\mathcal{O}}^\times = \varprojlim_{\mathfrak{f}} (\mathcal{O}/\mathfrak{f})^\times$, where $\mathfrak{f}$ runs over the nonzero integral ideals of K ordered by divisibility. In particular, the expression for $\widehat{\mathcal{O}}^\times$ as an inverse limit shows that the restriction of an idele class character to $\widehat{\mathcal{O}}^\times$ is trivial on $\widehat{\mathcal{O}}_{\mathfrak{f}}$ for some $\mathfrak{f}$, where $\widehat{\mathcal{O}}_{\mathfrak{f}}$ is as in (2.16).

The same remark holds locally at every finite place v: If $v = v_{\mathfrak{p}}$ then we have $\mathcal{O}_v = \varprojlim_n \mathcal{O}/\mathfrak{p}^n$ and $\mathcal{O}_v^\times = \varprojlim_n (\mathcal{O}/\mathfrak{p}^n)^\times$, and we deduce that any 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 $a(\chi_v)$ defined as follows: If χ_v is unramified then $a(\chi_v) = 0$, and if χ_v is ramified then $a(\chi_v)$ is the smallest integer $n \geqslant 1$ such that χ_v is trivial on $1 + \pi_v^n \mathcal{O}_v$. 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 integral ideals $\mathfrak{f}$ of K such that χ is trivial on $\widehat{\mathcal{O}}_{\mathfrak{f}}$, defining $\mathfrak{f}(\chi)$ to be the smallest such $\mathfrak{f}$ in terms of divisibility, or else we set

$$\mathfrak{f}(\chi) = \prod_{v \nmid \infty} \mathfrak{p}_v^{a(\chi_v)}, \tag{2.21}$$

where $\mathfrak{p}_v$ 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 adelic 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 (2.8) 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 (2.21), 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 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

$$L(s,\chi_v) = \begin{cases} (1-\chi_v(\pi_v)q_v^{-s})^{-1} & \text{if } \chi_v \text{ is unramified} \\ 1 & \text{if } \chi_v \text{ is ramified,} \end{cases} \tag{2.22}$$

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 (2.10) and (2.22) shows that the global L-function $L(s,\chi)$ is the product of the local L-factors:

$$L(s,\chi) = \prod_{v\nmid\infty} L(s,\chi_v). \tag{2.23}$$

Furthermore, if one thinks of χ as a primitive Hecke character then one can verify that the original definition (1.18) of $L(s,\chi)$ is equivalent to (2.10) and (2.23). (The key point is that if v is a finite place where χ is unramified and x in (2.13) 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," $L_{\text{fin}}(s,\chi)$, and the notation $L(s,\chi)$ would be reserved for the "completed L-function" $L_\infty(s,\chi)L_{\text{fin}}(s,\chi)$, where $L_\infty(s,\chi)$ is the product of the L-factors at the infinite places:

$$L_\infty(s,\chi) = \prod_{v\mid\infty} L(s,\chi_v). \tag{2.24}$$

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

In practice we will continue to write $L(s,\chi)$ for the traditional L-function $L_{\text{fin}}(s,\chi)$, but the factorization (2.24) will be used in the statement of the functional equation of $L(s,\chi)$. Hence we need to make the local factors in (2.24) explicit.

Suppose first that v is a real place. Then $K_v = \mathbb{R}$, 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

$$L(s,\chi_v) = \Gamma_\mathbb{R}(s+s_0+m), \tag{2.25}$$

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

$$L(s, \chi_v) = \Gamma_{\mathbb{C}}(s + s_0 + |m|/2). \tag{2.26}$$

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 (2.26) stays the same. Thus $L(s, \chi_v)$ is well defined.

3.2. Hecke's theorem

Given an idele class character χ of K, put

$$\Lambda(s, \chi) = (D\mathbf{N}\mathfrak{f}(\chi))^{s/2} L_\infty(s, \chi) L(s, \chi), \tag{2.27}$$

where D is the absolute value of the discriminant of K and $L_\infty(s, \chi)$ and $L(s, \chi)$ are as in (2.24) and (2.23) respectively. Let c be as in Proposition 1.1, and put

$$\begin{cases} w = 2c \\ k = w + 1, \end{cases} \tag{2.28}$$

so that $k = 2c + 1$.

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

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

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 $\Lambda(s, \chi)$ is often written 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 $W(\chi) = 1$.*

Proof. If χ is the trivial character then Theorem 2.2 is already contained in Theorem 2.1, so we may assume that χ is quadratic. We will use the identity

$$\zeta_L(s) = \zeta_K(s) L(s, \mathrm{sign}_{L/K}), \tag{2.29}$$

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

$$\mathrm{sign}_{L/K}(\mathfrak{p}) = \begin{cases} 1 & \text{if } \mathfrak{p} \text{ splits in } L \\ -1 & \text{if } \mathfrak{p} \text{ remains prime in } L \end{cases} \tag{2.30}$$

for prime ideals $\mathfrak{p}$ of K unramified in L. The fact that the homomorphism defined by (2.30) is actually a Hecke character of K (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 [**43**], p. 246. In any case, to prove the theorem we combine (2.29) 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 χ we can write

$$\zeta_L(s) = \zeta_K(s)L(s,\chi), \tag{2.31}$$

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

We claim that (2.31) remains valid when $\zeta_L(s)$, $\zeta_K(s)$, and $L(s,\chi)$ are replaced by their normalized versions:

$$Z_L(s) = Z_K(s)\Lambda(s,\chi). \tag{2.32}$$

To verify (2.32), 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

$$r_1(K) = r_{1/1}(L/K) + r_{2/1}(L/K). \tag{2.33}$$

Also

$$\begin{cases} r_1(L) = 2r_{1/1}(L/K) \\ r_2(L) = 2r_2(K) + r_{2/1}(L/K), \end{cases} \tag{2.34}$$

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 (2.24) and (2.27) we take $s_0 = m = 0$ in (2.25) and (2.26), obtaining

$$Z_L(s) = D_L^{s/2}\Gamma_{\mathbb{R}}(s)^{r_1(L)}\Gamma_{\mathbb{C}}(s)^{r_2(L)}\zeta_L(s) \tag{2.35}$$

and

$$Z_K(s) = D_K^{s/2}\Gamma_{\mathbb{R}}(s)^{r_1(K)}\Gamma_{\mathbb{C}}(s)^{r_2(K)}\zeta_K(s). \tag{2.36}$$

As for $\Lambda(s,\chi)$, the relation $\chi = \mathrm{sign}_{L/K}$ has the following consequences: If v is a complex place of K then $(s_0, m) = (0,0)$ in (2.26), while if v is a real place then $(s_0, m) = (0,0)$ or $(s_0, m) = (0,1)$ in (2.25) according as v splits or ramifies in L. As $\mathfrak{f}(\chi) = \mathfrak{d}_{L/K}$, we see that (2.27) gives

(2.37)
$$\Lambda(s,\chi) = (D_{L/K}D_K)^{s/2}\Gamma_{\mathbb{R}}(s)^{r_{1/1}(L/K)}\Gamma_{\mathbb{R}}(s+1)^{r_{2/1}(L/K)}\Gamma_{\mathbb{C}}(s)^{r_2(K)}L(s,\chi),$$

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 of (2.36) and (2.37) with (2.35). Taking account of (2.33) and (2.34) as well as the duplication formula (1.9) and the standard relation $D_L = D_{L/K}D_K^2$, we obtain (2.32).

To deduce the theorem we apply Theorem 2.1 on both sides of (2.32), obtaining

$$Z_L(1-s) = Z_K(1-s)W(\chi)\Lambda(1-s,\chi). \tag{2.38}$$

Replacing s by $1-s$ in (2.32) and comparing the result with (2.38), we conclude that $W(\chi) = 1$. $\square$

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

$$W(\chi) = \prod_v W(\chi_v), \tag{2.39}$$

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 we treat these formulas as a black box, ignoring their provenance. Afterwards we 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 $K^\times$; a notation like $||*||$, for example, now refers to the *local* norm on $K^\times$. An important point about root numbers is that they see only the unitary part of a character. In other words, if we put $\chi_{\text{unit}} = \chi/|\chi|$ as before then

$$W(\chi) = W(\chi_{\text{unit}}). \tag{2.40}$$

Hence if it is convenient to do so one may assume that χ is unitary.

If K is archimedean then there is no need to do so. Indeed if K is archimedean then χ has the form $x \mapsto ||x||^{s_0}(x/|x|)^m$ with unique elements $s_0 \in \mathbb{C}$ and either $m \in \{0,1\}$ or $m \in \mathbb{Z}$ according as $K = \mathbb{R}$ or $K \cong \mathbb{C}$. The character χ is unitary if and only if $s_0 \in i\mathbb{R}$, but $W(\chi)$ depends only on m, not on s_0:

$$W(\chi) = i^{-|m|}. \tag{2.41}$$

In other words, if $K = \mathbb{R}$ and $\chi(t) = |t|^{s_0}(t/|t|)^m$ then $W(\chi) = i^{-m}$, and if $K \cong \mathbb{C}$ and $\chi(z) = |z|^{2s_0}(z/|z|)^m$ then (2.41) holds and is independent of the identification $K \cong \mathbb{C}$ chosen: the alternative identification merely replaces m by $-m$.

Now take $p < \infty$. In the nonarchimedean setting it would be a slight convenience to assume that χ is unitary, but instead we shall replace χ by χ_{unit} 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 d for the **exponent of the different ideal** of K. Thus if π is a uniformizer of K then $\pi^d\mathcal{O}$ is the different ideal of K over $\mathbb{Q}_p$. Now put $\mathfrak{f}(\chi) = \pi^{a(\chi)}\mathcal{O}$ and choose an element $\gamma \in \pi^{a(\chi)+d}\mathcal{O}^\times$. It follows from the definitions that the functions $x \mapsto \chi(x)$ and $x \mapsto e^{2\pi i \operatorname{tr}_{K/\mathbb{Q}_p}(x/\gamma)}$ on $\mathcal{O}^\times$ depend only on the residue class of x in $(\mathcal{O}/\mathfrak{f}(\chi))^\times$. Writing q for the order of the residue class field of K, we have

$$W(\chi) = \chi_{\text{unit}}(\gamma) \cdot q^{-a(\chi)/2} \sum_{x \in (\mathcal{O}/\mathfrak{f}(\chi))^\times} \chi^{-1}(x) e^{2\pi i \operatorname{tr}_{K/\mathbb{Q}_p}(x/\gamma)}. \tag{2.42}$$

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

It is somewhat unconventional to express the nonarchimedean local root number by a single formula, as in (2.42). Normally something like (2.42) would be stated for ramified characters only, and for unramified characters one would give the separate formula

$$W(\chi) = \chi_{\text{unit}}(\gamma) \qquad (a(\chi) = 0). \tag{2.43}$$

However (2.42) actually reduces to (2.43) in the unramified case provided we agree that if $a(\chi) = 0$ and hence $\mathfrak{f}(\chi) = \mathcal{O}$ then $(\mathcal{O}/\mathfrak{f}(\chi))^\times$ has just one element, namely the coset of 1.

Having stated the local formulas, we return to the global setting and write K for a number field, χ for an idele class character of K, and $\mathfrak{f}(\chi)$ for the conductor of χ. Let $\mathfrak{D}$ denote the different ideal of K. It follows from (2.43) that if v is the finite place of K corresponding to a prime ideal $\mathfrak{p}$ of K not dividing $\mathfrak{D}\mathfrak{f}(\chi)$ then $W(\chi_v) = 1$. In particular, since $\mathfrak{p} \nmid \mathfrak{D}\mathfrak{f}(\chi)$ for all but finitely many $\mathfrak{p}$ we conclude that the product in (2.39) has only finitely many factors different from 1, as claimed.

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 (2.43) gives $W(\chi_v) = 1$ for all finite places $v \nmid \mathfrak{D}$. And since $\chi_\infty(z) = z^{-1}$ we have $W(\chi_\infty) = i^{-1}$ (take $s_0 = -1/2$ and $m = -1$ in (2.41)). Thus (2.39) gives

$$W(\chi) = i^{-1} \prod_{v|\mathfrak{D}} W(\chi_v), \tag{2.44}$$

and it remains to evaluate $W(\chi_v)$ at the places v above the prime divisors p of D.

Suppose then that $p|D$ and that $v = v_\mathfrak{p}$, where $\mathfrak{p}$ is the prime ideal above p. Then χ_v is ramified, so the appropriate local formula is (2.42). Since $a(\chi_v) = d_v = 1$ (d_v being the exponent of the local different at v) we may take the quantity γ in (2.42) to be p. Furthermore, since the natural map $(\mathbb{Z}/p\mathbb{Z})^\times \to (\mathcal{O}/\mathfrak{p})^\times$ is an isomorphism, the coset representatives x in (2.42) may be taken to be rational integers. So (2.42) becomes

$$W(\chi_v) = (\chi_v)_{\text{unit}}(p) \cdot p^{-1/2} \sum_{n \in (\mathbb{Z}/p\mathbb{Z})^\times} \chi_v^{-1}(n) e^{2\pi i (2n/p)}. \tag{2.45}$$

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 (2.45), 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

$$W(\chi_v) = \lambda(\overline{2})(\chi_v)_{\text{unit}}(p) \cdot p^{-1/2} \sum_{n \in (\mathbb{Z}/p\mathbb{Z})^\times} \lambda(n) e^{2\pi i (n/p)}. \tag{2.46}$$

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

$$\chi_v(p) = p \prod_{\substack{q|D \\ q \neq p}} \left(\frac{p}{q}\right), \tag{2.47}$$

and the factor of p on the right-hand side disappears when χ_v is replaced by $(\chi_v)_{\text{unit}}$ on the left-hand side. Finally, the sum in (2.46) is evaluated by Gauss's formula (1.1). Thus (2.46) becomes

$$W(\chi_v) = i^\delta \left(\frac{2}{p}\right) \prod_{\substack{q|D \\ q\neq p}} \left(\frac{p}{q}\right) \tag{2.48}$$

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 (2.48) in (2.44), we get

$$W(\chi) = i^{t-1} \left(\frac{2}{D}\right) \prod_{p\neq q} \left(\frac{p}{q}\right), \tag{2.49}$$

where the product on the right-hand side of (2.49) 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 (2.49) does give Gross's result, Proposition 1.5.

6. An open problem

The preceding example illustrates a simple point: Armed with the formulas (2.39) through (2.43), we can in principle detect trivial central zeros of Hecke L-functions whenever they exist. But do we always care? Does a trivial central zero of a Hecke L-function, or indeed of any L-function, always have arithmetic significance? Consider for example the L-functions associated to Maass forms for $\mathrm{SL}(2, \mathbb{Z})$. A theorem of Venkov [**98**] 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 a primitive equivariant Hecke character of K of finite order and $\chi_0 : I \to \mathbb{C}^\times$ is the Hecke character of K defined in two steps as follows. First we define χ_0 on P by the formula

$$\chi_0(\alpha\mathcal{O}) = |\alpha/\alpha'|^{\pi i/\log\varepsilon_0} \qquad (\alpha \in K^\times), \tag{2.50}$$

where ε_0 is the fundamental unit of K. Then we extend χ_0 to a character of I arbitrarily. In Exercise 2.6 the reader is invited to verify that (2.50) gives a well-defined function on principal ideals and that any extension of (2.50) to I is an equivariant Hecke character. Now put $\chi = \eta\chi_0$, and let D be the discriminant of K. Applying Theorem 2.1, we find that the functional equation of $L(s, \chi)$ can be written $\Lambda(s, \chi) = W(\chi)\Lambda(1 - s, \chi)$ with

$$\Lambda(s, \chi) = (D\mathbf{N}\mathfrak{f}(\eta))^{s/2}\Gamma_\mathbb{R}(s + \pi i/\log\varepsilon_0)\Gamma_\mathbb{R}(s - \pi i/\log\varepsilon_0)L(s, \chi). \tag{2.51}$$

However if we make the additional assumption that the conductor of η has the form $\mathfrak{f}(\eta) = N\sqrt{D}\mathcal{O}$ for some rational integer $N \geqslant 1$ then $W(\chi) = W(\eta)$, and consequently the functional equation becomes

$$\Lambda(s,\chi) = W(\eta)\Lambda(1-s,\chi). \tag{2.52}$$

Incidentally, the equivariance of η already ensures that $\mathfrak{f}(\eta)' = \mathfrak{f}(\eta)$ and hence that $\mathfrak{f}(\eta)$ has the form $N\mathfrak{C}$ for some ideal $\mathfrak{C}$ of $\mathcal{O}$ dividing $\sqrt{D}\mathcal{O}$, so the condition $\mathfrak{f}(\eta) = N\sqrt{D}\mathcal{O}$ is relatively mild. In any case, assume that the condition is satisfied. Then (2.52) suggests the following question:

Problem 2. *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 of a Hecke character η of finite order for which $L(s,\eta) = L(s,\overline{\eta})$ and $W(\eta) = -1$ were given by Armitage [**3**] and Serre 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 [**31**] found a connection with Galois module structure: The quartic characters η considered by Fröhlich correspond to certain 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 [**15**], [**16**], [**17**], [**21**], [**32**], and [**95**]. This snippet of history should caution us against dismissing Problem 2 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 $W(\eta) = -1$ and $\mathfrak{f}(\eta)$ of the required form. Take $K = \mathbb{Q}(\sqrt{r(r+4)})$ with a prime $r > 5$ congruent to 1 mod 4. Then the discriminant of K has the form $D = rs$, where $r + 4 = sm^2$ with s square-free and $m \in \mathbb{Z}$. Let κ be the primitive quadratic Dirichlet character of conductor D given by

$$\kappa(n) = \left(\frac{n}{D}\right), \tag{2.53}$$

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 (2.53) we have at least $\varepsilon(-1) = \kappa(-1) = 1$. On the other hand, put $u = ((r+2) + \sqrt{r(r+4)})/2$. According to Katayama [**48**], u is the fundamental unit of K, so we must verify that $\varepsilon(u) = 1$ also.

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

$$\eta(\alpha\mathcal{O}) = \varepsilon(\alpha) \qquad (\alpha \in K(\mathfrak{f})), \tag{2.54}$$

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

$$W(\eta) = \left(\frac{2}{D}\right) \tag{2.55}$$

(Exercise 2.7). But $D = r(r+4)/m^2$ 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." In rectifying these omissions we shall also add a few words about Tate's global and local functional equations [**92**], which are the source of the formulas for $W(\chi)$ stated earlier. For a more thorough treatment see [**92**] or Chapter XIV of [**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 $\psi : K \to \mathbb{C}^\times$. There is a canonical choice of ψ which we denote ψ^{can}. If $p = \infty$ then

$$\psi^{\text{can}}(x) = e^{-2\pi i \operatorname{tr}_{K/\mathbb{R}}(x)}, \tag{2.56}$$

and if $p < \infty$ then

$$\psi^{\text{can}}(x) = e^{2\pi i \{\operatorname{tr}_{K/\mathbb{Q}_p}(x)\}_p}. \tag{2.57}$$

Here $\{z\}_p$ is the p-adic principal part of a number $z \in \mathbb{Q}_p$: thus if $z = \sum_{n\in\mathbb{Z}} a_n p^n$ with $a_n \in \{0, 1, \ldots, p-1\}$ for all n and $a_n = 0$ for $n \ll 0$ then $\{z\}_p = \sum_{n<0} a_n p^n$. Note that (2.56) can also be written

$$\psi^{\text{can}}(x) = e^{-2\pi i \{\operatorname{tr}_{K/\mathbb{R}}(x)\}_\infty}, \tag{2.58}$$

where $\{t\}_\infty$ is the fractional part of a real number t, defined by the requirements $0 \leqslant \{t\}_\infty < 1$ and $t \equiv \{t\} \bmod \mathbb{Z}$. Normally $\{t\}_\infty$ is written simply as $\{t\}$, but we have included the subscript to emphasize the analogy with (2.57).

Let χ be a character of $K^\times$. Associated to χ and to an arbitrary additive character ψ of K is a **local root number** $W(\chi, \psi)$. The definition of $W(\chi, \psi)$ will be given later, and it will turn out that our $W(\chi)$ coincides with $W(\chi, \psi^{\text{can}})$. Furthermore, any ψ has the form $\psi(x) = \psi^{\text{can}}(ax)$ for some $a \in K^\times$, and we shall see that $W(\chi, \psi) = \chi_{\text{unit}}(a) W(\chi)$. It follows that

$$W(\chi, \psi_b) = \chi_{\text{unit}}(b) W(\chi, \psi) \tag{2.59}$$

for any $b \in K^\times$, where $\psi_b(x) = \psi(bx)$.

We now switch to the global setting and change notation accordingly. 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. Again there is a canonical choice ψ^{can}. It is simply the product of the local canonical choices:

$$\psi^{\mathrm{can}}(x) = \prod_v \psi_v^{\mathrm{can}}(x_v) \qquad (x = (x_v) \in \mathbb{A}). \tag{2.60}$$

Of course to make sense of (2.60) we must verify that $\psi_v^{\mathrm{can}}(x_v) = 1$ for all but finitely many v. Certainly $x_v \in \mathcal{O}_v$ for all but finitely many finite v, and if $x_v \in \mathcal{O}_v$ then $\mathrm{tr}_{K_v/\mathbb{Q}_p}(x_v) \in \mathbb{Z}_p$, where p is the residue characteristic of v. Then $\psi_v^{\mathrm{can}}(x_v) = 1$. Hence (2.60) is indeed meaningful.

To see that ψ^{can} is a global additive character of K we must still check that it is trivial on K. So suppose that $\alpha \in K$. Referring to (2.57) and (2.58), we find that the identity to be verified is

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

The sum of the local traces at the places of K 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

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

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. We define the global root number $W(\chi, \psi)$ to be the product of the local root numbers:

$$W(\chi, \psi) = \prod_v W(\chi_v, \psi_v). \tag{2.61}$$

However the dependence of $W(\chi, \psi)$ on ψ is illusory: We can write $\psi(x) = \psi^{\mathrm{can}}(\alpha x)$ for some $\alpha \in K^\times$, and then the right-hand side of (2.61) becomes

$$\prod_v W(\chi_v, (\psi_v^{\mathrm{can}})_\alpha) = \prod_v (\chi_v)_{\mathrm{unit}}(\alpha) W(\chi_v, \psi_v^{\mathrm{can}}) \tag{2.62}$$

by virtue of (2.59). Note that $(\chi_v)_{\mathrm{unit}} = (\chi_{\mathrm{unit}})_v$. Since χ_{unit} is an idele class character and $\alpha \in K^\times$, the right-hand side of (2.62) is simply $\prod_v W(\chi_v, \psi_v^{\mathrm{can}})$ or in other words our previous $\prod_v W(\chi_v)$. Hence we recover the definition (2.39) of the global root number which 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 reason 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 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 which forces one to consider arbitrary additive characters. Indeed for the prime field $\mathbb{Q}$ there is a canonical choice of additive character, whence for any number field there is a canonical choice via composition with trace. But a function field is of infinite degree over its prime field, and consequently a preferred additive character is lacking. In the absence of a preferred choice one is forced to consider all choices.

7.2. The global epsilon factor and the global functional equation

The fact that there is no trace from a function field to its prime field has other consequences as well. The framework within which we have been working – ideles, idele class characters, L-functions – carries over without change to function fields, and Hecke's functional equation

$$\Lambda(s,\chi) = W(\chi)\Lambda(k-s,\overline{\chi}) \tag{2.63}$$

(Theorem 2.1, with k as in (2.28)) is subsumed in Tate's functional equation

$$L(s,\chi) = \varepsilon(s,\chi)L(1-s,\chi^{-1}) \tag{2.64}$$

for the L-function associated to an idele class character χ of an arbitrary global field. Here $L(s,\chi)$ is the completed L-function associated to χ and $\varepsilon(s,\chi)$ is the **global epsilon factor**, an elementary factor of the form $a\cdot b^s$ with $a \in \mathbb{C}^\times$ and $b > 0$. We define $\varepsilon(s,\chi)$ more precisely below, but right now the key point is that in Tate's more general setting, (2.63) has to be replaced by (2.64), because $\Lambda(s,\chi)$ no longer has a meaning: The definition of $\Lambda(s,\chi)$ involves the absolute discriminant, and function fields do not have absolute discriminants. Such an invariant exists for a number field K only because one can take the trace down to the prime field and obtain the canonical pairing $\langle x,y\rangle = \mathrm{tr}_{K/\mathbb{Q}}(xy)$.

Before explaining how (2.64) reduces to (2.63) in the case of number fields, we repeat that the L-function $L(s,\chi)$ in (2.64) is the *completed* L-function associated to χ. In other words, $L(s,\chi) = L_\infty(s)L_{\mathrm{fin}}(s,\chi)$, where $L_{\mathrm{fin}}(s,\chi)$ is the Euler product (2.10). Normally it is this Euler product itself which we denote $L(s,\chi)$, but *for the remainder of the present lecture only,* we shall use $L(s,\chi)$ to mean the completed L-function, reverting in subsequent lectures to the more traditional usage in force until now. Note that it is only in the number field case that this distinction is even an issue: If there are no infinite places then $L_\infty(s,\chi) = 1$, whence $L(s,\chi)$ coincides with (2.10) by either convention.

To make a connection between (2.63) and (2.64) we must say a word about $\varepsilon(s,\chi)$, although we postpone the formal definition a little longer. Roughly speaking, epsilon factors are Gauss sums, or a generalization and renormalization of Gauss sums. For example if χ is a primitive Dirichlet character of conductor N, simultaneously viewed as the corresponding idele class character $\chi_{\mathbb{A}}$, then

$$\varepsilon(s,\chi) = \tau(\chi)/(i^m N^s) = W(\chi)N^{1/2-s}, \tag{2.65}$$

where $\tau(\chi)$ is the Gauss sum (1.2) and m is as in (1.4). The second equality in (2.65) is a consequence of (1.3). As this example illustrates, the epsilon factor of an idele class character of a number field binds the root number to the the product of the conductor and the absolute value of the discriminant, although the latter factor is of course 1 in the case of $\mathbb{Q}$. In general, if K is an arbitrary number field and χ an idele class character of K then

$$\varepsilon(s,\chi) = W(\chi)(D\mathbf{N}\mathfrak{f}(\chi))^{k/2-s} \tag{2.66}$$

(see Exercise 2.9). Granting (2.66), let us verify that (2.64) does reduce to (2.63) when K is a number field. In addition to (2.66), we will need the formula

$$L(s,\chi\cdot||*||^{s_0}) = L(s+s_0,\chi), \tag{2.67}$$

where $||*||$ is as usual the idelic norm. The validity of (2.67) follows by inspection from formulas (2.22) through (2.26).

To deduce (2.63) from (2.64), we recall first of all that when the absolute norm is viewed as an idele class character it coincides with the *reciprocal* of the idelic norm. Thus the idelic version of Proposition 1.1, given (2.28), is

$$\chi = \chi_{\text{unit}} \cdot ||*||^{-(k-1)/2}. \tag{2.68}$$

Consequently $\chi^{-1} = \overline{\chi}_{\text{unit}} \cdot ||*||^{(k-1)/2}$, whence

$$L(1-s, \chi^{-1}) = L(1-s+(k-1)/2, \overline{\chi}_{\text{unit}})$$

by (2.67). Another appeal to (2.67) now gives

$$L(1-s, \chi^{-1}) = L(k-s, \overline{\chi}_{\text{unit}} \cdot ||*||^{-(k-1)/2}) = L(k-s, \overline{\chi}), \tag{2.69}$$

where the second equality follows from (2.68). On substituting (2.66) and (2.69) in (2.64) and then multiplying through by $(D\mathbf{N}\mathfrak{f}(\chi))^{s/2}$, we do indeed recover (2.63).

We come finally to the definition of $\varepsilon(s, \chi)$, where χ is now an idele class character of a global field K. Choose a global additive character ψ of K – recall this means that ψ is a nontrivial unitary character of the adele ring $\mathbb{A}$ of K, trivial on K – and let dx be the Haar measure on $\mathbb{A}$ giving the quotient $\mathbb{A}/K$ measure 1. As with any Haar measure on $\mathbb{A}$, we can write dx as a restricted direct product measure, $dx = \otimes_v dx_v$, where dx_v is a Haar measure on K_v and dx_v gives $\mathcal{O}_v$ measure 1 for all but finitely many finite v. If $\{c_v\}$ is a family of positive real numbers such that $c_v = 1$ for all but finitely many v and $\prod_v c_v = 1$, then we also have $dx = \otimes_v c_v dx_v$, so the decomposition $dx = \otimes_v dx_v$ is not unique. Neither is ψ, of course. Nonetheless, we obtain a global factor $\varepsilon(s, \chi)$ independent of any choices by setting

$$\varepsilon(s, \chi) = \prod_v \varepsilon(s, \chi_v, \psi_v, dx_v), \tag{2.70}$$

where the **local epsilon factor** $\varepsilon(s, \chi_v, \psi_v, dx_v)$ must now be defined.

7.3. The local epsilon factor and the local functional equation

Since the issue is now local, we drop the subscript v and switch to a local setting. Thus K is a local field, χ a character of $K^\times$, ψ an additive character of K, and dx a Haar measure on K. We must define $\varepsilon(s, \chi, \psi, dx)$. Once we have done so we will put

$$\varepsilon(\chi, \psi, dx) = \varepsilon(s, \chi, \psi, dx)|_{s=0} \tag{2.71}$$

and define the local root number $W(\chi, \psi)$ by the formula

$$W(\chi, \psi) = \frac{\varepsilon(\chi, \psi, dx)}{|\varepsilon(\chi, \psi, dx)|}. \tag{2.72}$$

As the notation suggests, the right-hand side of (2.72) turns out to be independent of the choice of dx.

One point to understand at the outset is that the definition of $\varepsilon(s, \chi, \psi, dx)$ involves integrals which may converge only for $\Re(s) \gg 0$. However $\varepsilon(s, \chi, \psi, dx)$ extends to an entire function of s, so that (2.71) defines $\varepsilon(\chi, \psi, dx)$ by analytic continuation. Going in the other direction, we will see that

$$\varepsilon(s, \chi, \psi, dx) = \varepsilon(\chi \cdot ||*||^s, \psi, dx); \tag{2.73}$$

of course $||*||$ now denotes the local norm (2.7), given that we are dropping the subscript v.

The integrals just mentioned appear along with $\varepsilon(s,\chi,\psi,dx)$ in Tate's local functional equation. Quite apart from the fact that Tate's method is applicable to function fields as well as number fields, the local functional equation is from the perspective of Hecke's method something completely new. The setting for the innovation is the **Schwartz space** $\mathcal{S}(K)$ of K. 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 $K \cong \mathbb{C}$) are of rapid decay. In all cases we define the **Fourier transform** $\hat{f}$ of a function $f \in \mathcal{S}(K)$ by

$$\hat{f}(x) = \int_K f(y)\psi(xy)\, dy. \tag{2.74}$$

The definition depends on the choice of ψ, but for any choice, $\hat{f}$ is again in $\mathcal{S}(K)$.

To state the local functional equation, take $f \in \mathcal{S}(K)$ and set

$$I(s,\chi,\psi,dx,f) = \int_{K^\times} f(x)\chi(x)||x||^s\,\frac{dx}{||x||}. \tag{2.75}$$

Even though $I(s,\chi,\psi,dx,f)$ does not actually depend on ψ, we retain it in the notation to remind ourselves that $\hat{f}$ depends on ψ. As for the right-hand side of (2.75), 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 $K^\times$. By a consideration of cases one can show that the integral converges for $\Re(s) \gg 0$ and extends to a meromorphic function on $\mathbb{C}$. Tate's local functional equation is the statement that

$$\frac{I(1-s,\chi^{-1},\psi,dx,\hat{f})}{L(1-s,\chi^{-1})} = \varepsilon(s,\chi,\psi,dx)\frac{I(s,\chi,\psi,dx,f)}{L(s,\chi)}, \tag{2.76}$$

where the local L-factors are as in (2.22), (2.25), and (2.26) and $\varepsilon(s,\chi,\psi,dx)$ is an entire nowhere vanishing function independent of f.

Formula (2.76) is the *definition* of $\varepsilon(\chi,\psi,dx,s)$. More precisely, one first proves that for arbitrary $f, g \in \mathcal{S}(K)$ the identity

$$I(s,\chi,\psi,dx,f)I(1-s,\chi^{-1},\psi,dx,\hat{g}) = I(s,\chi,\psi,dx,g)I(1-s,\chi^{-1},\psi,dx,\hat{f})$$

holds, and then for each χ one exhibits a choice of g such that $I(s,\chi,\psi,dx,g)$ and $I(1-s,\chi^{-1},\psi,dx,\hat{g})$ are nonzero as meromorphic functions. Finally, given such a g one defines $\varepsilon(s,\chi,\psi,dx)$ by putting

$$\varepsilon(s,\chi,\psi,dx) = \frac{L(s,\chi)I(1-s,\chi^{-1},\psi,dx,\hat{g})}{L(1-s,\chi^{-1})I(s,\chi,\psi,dx,g)}. \tag{2.77}$$

Then $\varepsilon(s,\chi,\psi,dx)$ is independent of the choice of g and (2.76) follows.

We will not delve into the details of these calculations, nor into the passage from (2.76) to (2.64), which is based on an adelic version of the Poisson summation formula. For all of this see [**92**]. However we will illustrate the use of (2.76) by determining the dependence of $\varepsilon(s,\chi,\psi,dx)$ on the parameters ψ, dx, and s, and by proving a duality relation. We will also record some formulas for $\varepsilon(s,\chi,\psi,dx)$ which arise as a by-product of the proof of (2.76) and which in the number field case are the source of the local formulas for $W(\chi)$ stated earlier.

7.4. Dependence on the parameters

To determine how $\varepsilon(s,\chi,\psi,dx)$ depends on ψ, we return to the spot where ψ entered the picture, namely the definition (2.74) of the Fourier transform. If we temporarily write $(\psi,\hat{f})$ and $(\psi_b,\hat{f})$ for the Fourier transform of f taken relative to ψ and ψ_b respectively, then (2.74) gives $(\psi_b,\hat{f})(x) = (\psi,\hat{f})(bx)$. Hence by using the invariance of $dx/||x||$ under $x \mapsto b^{-1}x$ in the integral for $I(1-s,\chi^{-1},\psi_b,dx,\hat{f})$, we see that

$$I(1-s,\chi^{-1},\psi_b,dx,\hat{f}) = \chi(b)||b||^{s-1}I(1-s,\chi^{-1},\psi,dx,\hat{f}).$$

Since the L-factors and $I(s,\chi,\psi,dx,f)$ are unaffected by the switch from ψ to ψ_b, the formula

$$\varepsilon(s,\chi,\psi_b,dx) = \chi(b)||b||^{s-1}\varepsilon(s,\chi,\psi,dx) \tag{2.78}$$

now follows from (2.76). In particular, taking $s=0$, we obtain

$$\varepsilon(\chi,\psi_b,dx) = \chi(b)||b||^{-1}\varepsilon(\chi,\psi,dx), \tag{2.79}$$

and inserting this information in (2.72), we recover the claimed formula (2.59) for the dependence of $W(\chi,\psi)$ on ψ. Furthermore, if we redo the calculation (2.62) with (2.61) replaced by (2.70) and (2.59) by (2.78) then we find that the global epsilon factor in (2.70) is indeed independent of the global additive character.

Next we determine the dependence of $\varepsilon(s,\chi,\psi,dx)$ on dx. Any other Haar measure on K has the form $c\,dx$ with $c>0$, and from (2.74) and (2.75) we deduce that $I(1-s,\chi^{-1},c\,dx,\hat{f}) = c^2\,I(1-s,\chi^{-1},dx,\hat{f})$ and $I(s,\chi,c\,dx,f) = c\,I(s,\chi,dx,f)$. The formula

$$\varepsilon(s,\chi,\psi,c\,dx) = c\,\varepsilon(s,\chi,\psi,dx) \tag{2.80}$$

now follows from (2.76). Taking $s=0$, we find that

$$\varepsilon(\chi,\psi,c\,dx) = c\,\varepsilon(\chi,\psi,dx). \tag{2.81}$$

Thus the definition (2.72) of $W(\chi,\psi)$ is independent of dx, as claimed. Another claim also follows, namely that the global epsilon factor does not depend on the decomposition of the global Haar measure as a restricted direct product of local Haar measures.

Finally, let us verify the relation (2.73), the dependence of $\varepsilon(s,\chi,\psi,dx)$ on s. This is easy. First of all, it is immediate from the definition of $I(s,\chi,\psi,dx,f)$ that if s' is a second complex variable then

$$I(s+s',\chi,\psi,dx,f) = I(s',\chi\cdot||*||^s,\psi,dx,f).$$

It is likewise immediate from the definition of $L(s,\chi)$ given in formulas (2.22), (2.25), and (2.26) that $L(s+s',\chi) = L(s',\chi\cdot||*||^s)$. Hence (2.76) gives

$$\varepsilon(s+s',\chi,\psi,dx) = \varepsilon(s',\chi\cdot||*||^s,\psi,dx).$$

Setting $s'=0$, we obtain (2.73).

7.5. A duality relation

Given $f \in \mathcal{S}(K)$, define $f^- \in \mathcal{S}(K)$ by $f^-(x) = f(-x)$. If we fix ψ and use it to define the Fourier transform $f \mapsto \hat{f}$ on $\mathcal{S}(K)$, then the **self-dual Haar measure** dx_ψ relative to ψ is the unique Haar measure on K such that $(f\hat{\ })\hat{\ } = f^-$. Taking $dx = dx_\psi$ and applying (2.76) a second time, we find that

$$I(s,\chi,\psi,dx_\psi,f^-) = \varepsilon(s,\chi,\psi,dx_\psi)\varepsilon(1-s,\chi^{-1},\psi,dx_\psi)I(s,\chi,\psi,dx_\psi,f).$$

The substitution $x \mapsto -x$ in the integral $I(s, \chi, \psi, dx_\psi, f^-)$ now gives

$$\varepsilon(s, \chi, \psi, dx_\psi)\varepsilon(1 - s, \chi^{-1}, \psi, dx_\psi) = \chi(-1). \tag{2.82}$$

This is the duality relation at issue.

A less transparent version of (2.82) will actually be more useful to us. We claim first of all that a local analogue of Proposition 1.1 holds:

$$\chi = \chi_{\text{unit}} \cdot || * ||^{-c} \tag{2.83}$$

with $c \in \mathbb{R}$. The assertion in (2.83) is that $|\chi| = || * ||^{-c}$ and indeed that any character of $K^\times$ with values in $\mathbb{R}_{>0}$ is a real power of $|| * ||$. If K is $\mathbb{R}$ or $\mathbb{C}$ this fact has already been noted, and if K is nonarchimedean then it suffices to observe that a character of $K^\times$ with values in $\mathbb{R}_{>0}$ is trivial on $\mathcal{O}^\times$ and thus determined by its value on a uniformizer, hence equal to $|| * ||^{-c}$ for some c. Now (2.83) implies that $\chi^{-1} = \overline{\chi} \cdot || * ||^{2c}$, whence substitution in (2.82) gives

$$\varepsilon(\chi, \psi, dx_\psi)\varepsilon(1 + 2c, \overline{\chi}, \psi, dx_\psi) = \chi(-1) \tag{2.84}$$

when we take $s = 0$ and use (2.73).

On the other hand, applying complex conjugation to both sides of (2.76) gives $\overline{\varepsilon(s, \chi, \psi, dx_\psi)} = \varepsilon(\overline{s}, \overline{\chi}, \psi_{-1}, dx_\psi)$, because $\overline{\psi} = \psi^{-1} = \psi_{-1}$. Thus

$$\overline{\varepsilon(s, \chi, \psi, dx_\psi)} = \chi(-1)\varepsilon(\overline{s}, \overline{\chi}, \psi, dx_\psi)$$

by (2.78). Taking $s = 1 + 2c$ and substituting the result in (2.84), we obtain

$$\varepsilon(\chi, \psi, dx_\psi)\overline{\varepsilon(\chi \cdot || * ||^{1+2c}, \psi, dx_\psi)} = 1 \tag{2.85}$$

after canceling $\chi(-1)$ on both sides and once again using (2.73). In spite of its apparent awkwardness, (2.85) will lead to a formula for the absolute value of $\varepsilon(\chi, \psi, dx_\psi)$.

7.6. Explicit formulas

As we have already indicated, an essential part of the proof of (2.76) is to exhibit a Schwartz function g for which $I(s, \chi, \psi, dx, g) \neq 0$. In the process one obtains the following useful information about $\varepsilon(s, \chi, \psi, dx)$.

First, if K is archimedean and dx^{can} is the self-dual measure relative to ψ^{can} then

$$\varepsilon(s, \chi, \psi^{\text{can}}, dx^{\text{can}}) = \varepsilon(\chi, \psi^{\text{can}}, dx^{\text{can}}) = W(\chi) \tag{2.86}$$

with $W(\chi)$ as in (2.41). Standard formulas for the Fourier transform on euclidean space show that dx^{can} is Lebesgue measure or twice Lebesgue measure according as $K = \mathbb{R}$ or $K \cong \mathbb{C}$. In the latter case we can also say that dx^{can} is $|dz \wedge d\overline{z}|$.

Next suppose that K is nonarchimedean. Let $\mathcal{O}$ be its ring of integers, π a uniformizer, $a(\chi)$ the exponent of the conductor of χ, and $n(\psi)$ the largest integer n such that $\psi|\pi^{-n}\mathcal{O}$ is trivial. Choose $\gamma \in \pi^{a(\chi)+n(\psi)}\mathcal{O}^\times$. If χ is unramified then

$$||\gamma||\, \varepsilon(\chi, \psi, dx) = \chi(\gamma) \int_{\mathcal{O}} dx, \tag{2.87}$$

and if χ is ramified then

$$||\gamma||\, \varepsilon(\chi, \psi, dx) = \int_{\mathcal{O}^\times} \chi^{-1}(x/\gamma)\psi(x/\gamma)dx. \tag{2.88}$$

Of course the integral in (2.87) is just $\text{meas}(\mathcal{O})$, the measure of $\mathcal{O}$ relative to dx.

We note two consequences of (2.87) and (2.88). First, an inspection of these formulas shows that the effect of replacing χ by $\chi\cdot||*||^s$ is to multiply the right-hand side of the formulas by $||\gamma||^s$. In other words

$$\varepsilon(\chi\cdot||*||^s,\psi,dx) = q^{-(a(\chi)+n(\psi))s}\varepsilon(\chi,\psi,dx) \tag{2.89}$$

with $q = |\mathcal{O}/\pi\mathcal{O}|$. In particular, take $s = 2c+1$, where c is as in (2.83). Inserting (2.89) in (2.85), we obtain

$$|\varepsilon(\chi,\psi,dx_\psi)|^2 = q^{(a(\chi)+n(\psi))k} \tag{2.90}$$

with $k = 2c+1$.

The second consequence is particularly simple and depends only on (2.87): If $a(\chi) = n(\psi) = 0$ and $\text{meas}(\mathcal{O}) = 1$ then $\varepsilon(\chi,\psi,dx) = 1$. On replacing χ by $\chi\cdot||*||^s$ and applying (2.73) we find more generally that if $a(\chi) = n(\psi) = 0$ and $\text{meas}(\mathcal{O}) = 1$ then $\varepsilon(s,\chi,\psi,dx) = 1$. If we switch to the global setting, so that K is now a global field, χ an idele class character, ψ a global additive character, and dx the Haar measure on $\mathbb{A}$ giving $\mathbb{A}/K$ measure 1, then for all but finitely many finite places v we have $a(\chi_v) = n(\psi_v) = 0$ and $\text{meas}(\mathcal{O}_v) = 1$, and thus $\varepsilon(s,\chi_v,\psi_v,dx_v) = 1$. Hence the product (2.70) defining the global epsilon factor is indeed meaningful.

7.7. The number field case

It remains to check that we do recover the formulas for $W(\chi)$ stated earlier – namely (2.41), (2.42), and (2.43) – when we take K to be a finite extension of $\mathbb{Q}_p$ ($p \leqslant \infty$) and ψ to be ψ^{can}. That (2.86) and (2.72) imply (2.41) is a tautology, so we may assume that $p < \infty$.

If χ is unramified then γ in (2.87) is just an element of valuation $n(\psi)$. Furthermore $n(\psi)$ is d, the exponent of the different ideal, because $\psi = \psi^{\text{can}}$. Hence dividing the two sides of (2.87) by their absolute values, we obtain (2.43).

To derive (2.42), let dx^{can} denote the self-dual measure on K relative to ψ^{can}. We claim first of all that dx^{can} coincides with the measure dx on K for which $\text{meas}(\mathcal{O}) = q^{-d/2}$. To justify the claim it suffices to exhibit a single nonzero element $f \in \mathcal{S}(K)$ such that $(f\hat{\ })\hat{\ } = f^-$ when the Fourier transform is computed using ψ^{can} and dx. Let f and g be the characteristic functions of $\mathcal{O}$ and $\pi^{-d}\mathcal{O}$ respectively. A straightforward calculation shows that $\hat{f} = q^{-d/2}g$ and that $\hat{g} = q^{d/2}f$, whence $(f\hat{\ })\hat{\ } = f = f^-$ and $dx^{\text{can}} = dx$, as claimed. Thus $\mathcal{O}$ has measure $q^{-d/2}$ relative to dx^{can}. It follows that each coset of $\pi^{a(\chi)}\mathcal{O}$ in $\mathcal{O}$ has measure $q^{-d/2-a(\chi)}$. But the value at $x \in \mathcal{O}^\times$ of $\chi^{-1}(x/\gamma)\psi(x/\gamma)$ depends only on the coset of x modulo $\pi^{a(\chi)}\mathcal{O}$, so we can replace the integral in (2.88) by a sum:

$$q^{-a(\chi)-d}\,\varepsilon(\chi,\psi^{\text{can}},dx^{\text{can}}) = q^{-a(\chi)-d/2}\sum_{x\in(\mathcal{O}/\pi^{a(\chi)}\mathcal{O})^\times}\chi^{-1}(x/\gamma)\psi^{\text{can}}(x/\gamma). \tag{2.91}$$

Furthermore, we know from (2.90) that the absolute value of $\varepsilon(\chi^{\text{can}},\psi,dx^{\text{can}})$ is $q^{(a(\chi)+d)k/2}$, where $k = 2c+1$ and $|\chi(\pi)| = q^c$. It follows that the absolute value of the two sides of (2.91) is $q^{(a(\chi)+d)(c-1/2)}$. Dividing both sides of (2.91) by this quantity while substituting

$$\chi(\gamma) = \chi_{\text{unit}}(\gamma)q^{(a(\chi)+d)c},$$

we obtain (2.42).

8. Exercises

Exercise 2.1. Let $\mathbb{A}$ be the adele ring of a number field K. We have characterized the topology on $\mathbb{A}$ by two properties. Verify that there does in fact exist a unique topology on $\mathbb{A}$ with these properties and that a basis for the topology is given by 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. Similarly, verify that there is a unique topology on $\mathbb{A}^\times$ 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, C its ideal class group, and $c(\mathfrak{D}) \in C$ the class of the different ideal $\mathfrak{D}$. 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, Hecke's proof on p. 261 of [**43**] is quite different. The proof outlined in the hint follows an argument of Armitage [**2**] suggested by Serre.

Exercise 2.3. Given an idele class character χ of a number field K, write $W(\chi_{\text{fin}})$ and $W(\chi_\infty)$ for the product of the local root numbers $W(\chi_v)$ taken over $v \nmid \infty$ and over $v|\infty$ respectively. Using (2.42), show that if χ' is an idele class character of K with $\mathfrak{f}(\chi') = \mathcal{O}$ then

$$W((\chi\chi')_{\text{fin}}) = \chi'_{\text{unit}}(\mathfrak{f}(\chi)\mathfrak{D})W(\chi_{\text{fin}}),$$

where $\mathfrak{D}$ is the different ideal of K. (Of course in writing $\chi'_{\text{unit}}(\mathfrak{f}(\chi)\mathfrak{D})$ we are thinking of χ'_{unit} as a Hecke character.) It follows that

$$W(\chi\chi') = \omega \cdot \chi'_{\text{unit}}(\mathfrak{f}(\chi)\mathfrak{D})W(\chi) \tag{2.92}$$

with $\omega = W((\chi\chi')_\infty)/W(\chi_\infty)$.

Exercise 2.4. This exercise outlines a proof of Proposition 1.6. Notation is as in that proposition and as in the last paragraph of the proof of Proposition 1.3.

(a) Show that that $W(\chi\varphi) = W(\chi)$ for $\chi \in X(D)$ and $\varphi \in \Phi$. (Hint: Use (2.92) with $\chi' = \varphi$.)

(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

$$(\mathcal{O}/\mathfrak{T}^5)^\times \cong (\mathbb{Z}/8\mathbb{Z})^\times \times \langle (1 + \sqrt{-2C}) + \mathfrak{T}^5 \rangle, \tag{2.93}$$

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 $\mathfrak{T}^3\mathfrak{C}$ and $16\mathcal{O} = \mathfrak{T}^8$.)

(c) Deduce that $\sum_{\chi \in X(D)} W(\chi) = 0$, and conclude that the sets $X^\pm(D)$ are both nonempty, whence both are of cardinality $h(D)$ by (a) and Proposition 1.3.

Exercise 2.5. Given $\chi \in X(D)$ and a positive integer w, use the local formulas and Theorem 2.1 to verify that (1.35) holds with $\Lambda(s, \chi_w)$ as in (1.36) and $W(\chi_w)$ as in (1.37). (Hint: If w is odd then (2.92) can be applied with $\chi' = \chi^{w-1}$.)

Exercise 2.6. This exercise pertains to our example of a Hecke L-function of "Maass type." Let K be a real quadratic field of discriminant D.

(a) Show that (2.50) gives a well-defined equivariant character χ_0 of P and that any extension of this character to I is an equivariant Hecke character. (Hint: To check the equivariance, observe that if $\mathfrak{a}$ is any ideal of $\mathcal{O}$ then $\mathfrak{a}\mathfrak{a}'$ is the principal ideal generated by a rational integer, namely $\mathbf{N}\mathfrak{a}$.)

(b) Let η be a primitive equivariant Hecke character of K of finite order, and assume that $\mathfrak{f}(\eta) = N\sqrt{D}\mathcal{O}$ for some integer $N \geqslant 1$. Put $\chi = \eta\chi_0$, where χ_0 is now any extension of (2.50) to I. Show that $W(\chi) = W(\eta)$. (Hint: Use (2.92) with χ and χ' replaced by η and χ_0.)

Exercise 2.7. This exercise leads to a proof of (2.55). Fix a prime $r > 5$ congruent to 1 mod 4, put $K = \mathbb{Q}(\sqrt{r(r+4)})$, and let $\mathfrak{f} = \sqrt{D}\mathcal{O}$, where D as before is the discriminant of K. Also let η be any extension of (2.54) to $I(\mathfrak{f})$.

(a) Verify that η is an equivariant Hecke character of conductor $\mathfrak{f}$ and trivial infinity type.

(b) Deduce that $W(\eta_v) = 1$ if v is a place of K not dividing $\mathfrak{f}$.

(c) Now consider the place v of K corresponding to a given prime ideal $\mathfrak{p}$ dividing $\mathfrak{f}$, and let p be the prime number below $\mathfrak{p}$. Show that

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

with δ equal to 0 or 1 according as p is 1 mod 4 or 3 mod 4. (Note the similarity to (2.48).)

(d) Finally, use quadratic reciprocity to complete the proof of (2.55).

(e) Deduce from Theorem 2.2 that the class number of K is even.

Exercise 2.8. Let K be a number field, and let χ and χ' be idele class characters of K of relatively prime conductors.

(a) Show that the following formula of Langlands is a generalization of (2.92):

$$W(\chi\chi') = \omega \cdot \chi_{\text{unit}}(\mathfrak{f}(\chi'))\chi'_{\text{unit}}(\mathfrak{f}(\chi))W(\chi)W(\chi'), \tag{2.94}$$

where $\omega = W((\chi\chi')_\infty)/(W(\chi_\infty)W(\chi'_\infty))$.

(b) Prove (2.94).

(c) By taking $K = \mathbb{Q}$ and choosing χ and χ' appropriately, derive quadratic reciprocity from (2.94).

Exercise 2.9. Let χ be an idele class character of a number field K, and define k as in (2.28). Using (2.86), (2.89), and (2.90), derive (2.66).

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 representations and 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. The requirement that a representation of a topological group be continuous is very restrictive in the case of Artin representations, because $\mathrm{Gal}(\overline{K}/K)$ with its Krull topology is the profinite group $\varprojlim_L \mathrm{Gal}(L/K)$, where L runs over finite Galois extensions of K inside $\overline{K}$, and a complex representation of a profinite group is trivial on an open subgroup. It follows that an Artin representation of K can be regarded as a 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 **Artin L-function** $L(s, \rho)$ is defined by an Euler product:

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

where $\mathfrak{p}$ runs over nonzero prime ideals of K and $B_{\mathfrak{p}}(x)$ is the polynomial with constant term 1 defined as follows.

Given $\mathfrak{p}$, 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 on l induces an isomorphism of D/I onto $\mathrm{Gal}(l/k)$, and the latter group has a canonical generator, the Frobenius automorphism. If $\sigma \in D$ is a preimage of the Frobenius automorphism under the composition of maps $D \to D/I \to \mathrm{Gal}(l/k)$ then σ is called a **Frobenius element** at $\mathfrak{P}$. While it is only σI and not σ which is uniquely determined by $\mathfrak{P}$, if we restrict attention to the **subspace of inertial invariants**

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

then the resulting linear automorphism $\rho(\sigma)|V^I$ of V^I is well defined. We set $B_{\mathfrak{p}}(x) = x^d P(x^{-1})$, where $P(x)$ is the characteristic polynomial of $\rho(\sigma)|V^I$ and d is the dimension of V^I. Thus

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

Of course I is trivial unless $\mathfrak{p}$ is ramified in L, and when I is trivial, $V^I = V$. 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 $\mathfrak{p}$. Furthermore, since ρ is a representation of the finite group $\mathrm{Gal}(L/K)$, the eigenvalues of $\rho(\sigma)|V^I$ are roots of unity, and consequently the Euler product in (3.1) converges for $\Re(s) > 1$.

The definition (3.3) of $B_{\mathfrak{p}}(x)$ may appear to depend on our choice of a prime ideal $\mathfrak{P}$ over $\mathfrak{p}$, but if $\mathfrak{P}'$ is another choice 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 replaced by gDg^{-1}, gIg^{-1}, $g\sigma g^{-1}$, and $\rho(g)(V^I)$ respectively. Since characteristic polynomials are similarity invariants, (3.3) is unchanged. We also see that we can define ρ to be **unramified at $\mathfrak{p}$** (or at the corresponding place of K) if ρ is trivial on I, for then it is trivial on gIg^{-1} for all $g \in \mathrm{Gal}(L/K)$. If $\rho|I$ is nontrivial then ρ is **ramified at $\mathfrak{p}$**.

One can also define a notion of ramification at the infinite places. Let v be an infinite place of K and w a place of L over v. If v is real and w is complex then we let $I \subset \mathrm{Gal}(L/K)$ be the subgroup of order two generated by the complex conjugation corresponding to w. If v is complex or w is real then we take I to be the trivial subgroup of $\mathrm{Gal}(L/K)$. We say that ρ is **ramified** or **unramified** at v according as ρ is nontrivial or trivial on I. Note once again that ramification at v is a meaningful concept even though I may depend on w.

If S is a 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 Artin representations

The phrase *finite order* is crucial here. Idele class characters of infinite order do not correspond to Artin representations. However we do have a canonical bijection $\xi \mapsto \chi_\xi$ from one-dimensional Artin representations to idele class characters of finite order. The mechanism underlying this bijection is the Artin symbol. Since it will be convenient to think of χ_ξ as a primitive Hecke character we shall describe the Artin symbol at the level of ideals rather than at the level of ideles.

Let K be a number field and L a finite abelian extension of K, and let $\mathfrak{f}$ be a nonzero integral ideal of K which is divisible by every prime ideal of K ramified in L. 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 write $\sigma_{\mathfrak{P}}$ as $\sigma_{\mathfrak{p}}$, because $\sigma_{\mathfrak{P}}$ is independent of the choice of prime ideal $\mathfrak{P}$ over $\mathfrak{p}$: Since $\mathrm{Gal}(L/K)$ is abelian we have $g\sigma_{\mathfrak{P}}g^{-1} = \sigma_{\mathfrak{P}}$ for all $g \in \mathrm{Gal}(L/K)$. We define the Artin symbol $(*, L/K)$ on prime ideals by setting

$$(\mathfrak{p}, L/K) = \sigma_{\mathfrak{p}}. \tag{3.4}$$

Since $I(\mathfrak{f})$ is the free abelian group on the prime ideals not dividing $\mathfrak{f}$, the map $\mathfrak{p} \mapsto \sigma_{\mathfrak{p}}$ extends uniquely to a homomorphism $I(\mathfrak{f}) \to \mathrm{Gal}(L/K)$, the **Artin map** or **reciprocity law map**. We write this map as $\mathfrak{a} \mapsto (\mathfrak{a}, L/K)$, where $\mathfrak{a}$ denotes an arbitrary element of $I(\mathfrak{f})$.

The Artin map is surjective, and hence it gives rise to the **Artin isomorphism** from an appropriate quotient of $I(\mathfrak{f})$ onto $\mathrm{Gal}(L/K)$. But an even deeper fact of class field theory is embedded in the next statement: If ξ is a one-dimensional character of $\mathrm{Gal}(L/K)$ and we pull it back to $I(\mathfrak{f})$ via the Artin map then the resulting character of $I(\mathfrak{f})$ is a Hecke character, necessarily of finite order. Since we have not been careful about the choice of $\mathfrak{f}$ we cannot claim that the Hecke character in question is primitive, but it certainly determines a primitive Hecke character, and it is this primitive character that we denote χ_ξ. The relation between ξ and χ_ξ is summarized in the formula

$$\chi_\xi(\mathfrak{a}) = \xi((\mathfrak{a}, L/K)) \qquad (\mathfrak{a} \in I(\mathfrak{f})). \tag{3.5}$$

If we start with a character ξ of $\mathrm{Gal}(\overline{K}/K)$ then there are many choices of a finite abelian extension L of K such that ξ factors through $\mathrm{Gal}(L/K)$, but the primitive Hecke character χ_ξ obtained is independent of the choice. This follows from the "consistency property" of the Artin symbol: the fact that if M is an intermediate field of the extension L/K then the restriction of $(\mathfrak{a}, L/K)$ to M is $(\mathfrak{a}, M/K)$. The upshot is that we may think of $\xi \mapsto \chi_\xi$ as a map from one-dimensional Artin representations of K to primitive Hecke characters of K of finite order.

This map is a bijection. The injectivity is clear from the definition, and the surjectivity is essentially one version of the "existence theorem" of class field theory. To elaborate on this point very briefly, we introduce the **narrow ray class group** $I(\mathfrak{f})/P_{\mathfrak{f},>0}$ to the modulus $\mathfrak{f}$. Here $\mathfrak{f}$ is an integral ideal of K, and $P_{\mathfrak{f},>0}$ is the subgroup of $P_\mathfrak{f}$ consisting of principal fractional ideals generated by a *totally positive* element of $K_\mathfrak{f}$ (an element which is sent to a positive number by every real embedding of K). Of course if K is totally complex then $P_{\mathfrak{f},>0} = P_\mathfrak{f}$. Now when we combine the defining property (1.10) of Hecke characters with the fact that a finite-order character of $\mathbb{C}^\times$ or $R_{>0}$ is trivial, we see that if χ is a primitive Hecke character of K of finite order with $\mathfrak{f} = \mathfrak{f}(\chi)$ then χ factors through $I(\mathfrak{f})/P_{\mathfrak{f},>0}$. On the other hand, the existence theorem of class field theory assures us that there is an abelian extension $K^\mathfrak{f}$ of K, unramified outside the infinite places of K and the places dividing $\mathfrak{f}$, such that the kernel of the Artin symbol $(*, K^\mathfrak{f}/K)$ on $I(\mathfrak{f})$ is precisely $P_{\mathfrak{f},>0}$. The field $K^\mathfrak{f}$ is uniquely determined by these conditions and is called the **narrow ray class field** of K to the modulus $\mathfrak{f}$. If K is totally complex then we can omit the word *narrow*. In any case, the Artin map gives an isomorphism

$$I(\mathfrak{f})/P_{\mathfrak{f},>0} \cong \mathrm{Gal}(K^\mathfrak{f}/K). \tag{3.6}$$

Thus every primitive Hecke character χ of K of finite order with $\mathfrak{f} = \mathfrak{f}(\chi)$ has the form χ_ξ for some character ξ of $\mathrm{Gal}(K^\mathfrak{f}/K)$.

1.2. The arithmetic versus the geometric convention

The definitions (3.3) and (3.5) follow what we will call the **arithmetic convention** for Frobenius elements. The arithmetic convention is the traditional convention, and it seems like the appropriate convention to follow in the context of Artin L-functions. However there is a more recent convention, the **geometric convention**, and if we were to follow that convention then (3.5) would be replaced by

$$\chi_\xi(\mathfrak{a}) = \xi((\mathfrak{a}, L/K)^{-1}) \qquad (\mathfrak{a} \in I(\mathfrak{f})) \tag{3.7}$$

and (3.3) would be replaced by

$$B_\mathfrak{p}(x) = \det(1 - x\rho(\Phi)|V^I), \tag{3.8}$$

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.

1.3. The Artin formalism

Almost anything one does with Artin L-functions depends on three basic properties. These properties are collectively known as the **Artin formalism.**

The first is **additivity**: If ρ and ρ' are representations of $\mathrm{Gal}(L/K)$ then

$$L(s,\rho\oplus\rho')=L(s,\rho)L(s,\rho'). \tag{3.9}$$

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 ρ is a representation of $\mathrm{Gal}(L/M)$, let $\mathrm{ind}_{M/K}\rho$ denote the representation of $\mathrm{Gal}(L/K)$ induced by ρ. Then

$$L(s,\mathrm{ind}_{M/K}\rho)=L(s,\rho). \tag{3.10}$$

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**. Let ξ be a one-dimensional Artin representation and and χ_ξ the primitive Hecke character of finite order which corresponds to ξ under the identification (3.5). Then

$$L(s,\xi)=L(s,\chi_\xi). \tag{3.11}$$

This is a straightforward consequence of (1.18) (3.3), and (3.4).

There is actually a fourth property which can be considered part of the Artin formalism, namely **invariance under inflation**, although the invariance of $L(s,\rho)$ under inflation is more a property of Frobenius elements than of L-functions. 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

$$L(s,\mathrm{infl}_{L/M}\rho)=L(s,\rho). \tag{3.12}$$

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 $\mathfrak{P}$. The consistency property of the Artin symbol mentioned earlier is just an abelian consequence of this fact. In any case, the significance of (3.12) 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 the basic properties constituting the Artin formalism. We can now see that we encountered the first nontrivial instance of the Artin formalism in the previous lecture, when we looked at quadratic root numbers (Theorem 2.2). Given 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 ξ denote respectively the trivial and the nontrivial one-dimensional characters of $\mathrm{Gal}(L/K)$. Then $\mathrm{ind}_{L/K}1_L=1_K\oplus\xi$, so (3.9) and (3.10) give

$$L(s,1_L)=L(s,1_K)L(s,\xi). \tag{3.13}$$

Now it is immediate from the definitions that $L(s,1_L)=\zeta_L(s)$ and $L(s,1_K)=\zeta_K(s)$. Furthermore, on combining (3.4) with (3.5) we find that χ_ξ is the quadratic Hecke character $\mathrm{sign}_{L/K}$ defined in (2.30). It follows that (3.13) is simply the relation (2.29).

2. The functional equation

The example (3.13) 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

Let G be a finite group. We recall that $\mathrm{Groth}(G)$, the **Grothendieck group of virtual representations of G over** $\mathbb{C}$, can be viewed as the free abelian group on the isomorphism classes of the irreducible complex representations of G, whence a **virtual representation** of G is just an integral linear combination of such isomorphism classes. Also, a representation of G is **monomial** if it is induced by a one-dimensional character of G. Given a representation ρ of G over $\mathbb{C}$, write $[\rho]$ for its class in $\mathrm{Groth}(G)$. For our purposes, the essential content of Brauer's theorem is that the classes $[\rho]$ with ρ monomial span $\mathrm{Groth}(G)$ over $\mathbb{Z}$.

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

$$[\rho] = \sum_{(M,\xi)} n_{M,\xi}\,[\mathrm{ind}_{M/K}\xi] \tag{3.14}$$

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 (3.9) we can view $L(s,*)$ as 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 (3.14), we obtain

$$L(s,\rho) = \prod_{(M,\xi)} L(s, \mathrm{ind}_{M/K}\xi)^{n_{M,\xi}}, \tag{3.15}$$

and then the inductivity and compatibility properties (3.10) and (3.11) give

$$L(s,\rho) = \prod_{(M,\xi)} L(s,\chi_\xi)^{n_{M,\xi}}. \tag{3.16}$$

Each $L(s,\chi_\xi)$ is a Hecke L-function and so extends to a meromorphic function on $\mathbb{C}$. Thus (3.16) 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 (3.14), put

$$A_{M,\xi} = D_M \mathbf{N}\mathfrak{f}(\chi_\xi), \tag{3.17}$$

where D_M is the absolute value of the discriminant of M. We set

$$A(\rho) = \prod_{(M,\xi)} A_{M,\xi}^{n_{M,\xi}}, \tag{3.18}$$

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

$$W(\rho) = \prod_{(M,\xi)} W(\chi_\xi)^{n_{M,\xi}}, \tag{3.20}$$

and

$$\Lambda(s,\rho) = A(\rho)^{s/2} L_\infty(s,\rho) L(s,\rho). \tag{3.21}$$

Then

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

with $\Lambda(s,\chi_\xi)$ as in (2.27). Now dualization is a well-defined operation on Groth(G) and commutes with induction, so (3.14) also gives

$$[\rho^\vee] = \sum_{(M,\xi)} n_{M,\xi}[\mathrm{ind}_{M/K}\overline{\xi}]. \tag{3.23}$$

Furthermore $\chi_{\overline{\xi}} = \overline{\chi_\xi}$. Hence the counterpart to (3.16) is

$$L(s,\rho^\vee) = \prod_{(M,\xi)} L(s,\overline{\chi_\xi})^{n_{M,\xi}}. \tag{3.24}$$

Similarly, to define $A(\rho^\vee)$ and $L_\infty(s,\rho^\vee)$ we replace $A_{M,\xi}$ by $A_{M,\overline{\xi}}$ in (3.18) and $L_\infty(s,\chi_\xi)$ by $L_\infty(s,\overline{\chi_\xi})$ in (3.19) (neither replacement actually changes anything). Finally, to define $\Lambda(s,\rho^\vee)$ we replace ρ by $\rho^\vee$ on the right-hand side of (3.21), or simply in $L(s,\rho)$. Then

$$\Lambda(s,\rho^\vee) = \prod_{(M,\xi)} \Lambda(s,\overline{\chi_\xi})^{n_{M,\xi}}, \tag{3.25}$$

whence (3.20), (3.22), (3.25), and Hecke's functional equation (Theorem 2.1) give

$$\Lambda(s,\rho) = W(\rho)\Lambda(1-s,\rho^\vee). \tag{3.26}$$

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

2.2. Dependence on Brauer's theorem

With the functional equation (3.26) now established, let us review the definition of the four types of quantities which appear in it: the L-function $L(s,\rho)$, the gamma factor $L_\infty(s,\rho)$, the exponential factor $A(\rho)$, and the root number $W(\rho)$. Our goal in reviewing the definitions is to distinguish between those that are "Brauer-dependent" – in other words, dependent on an expression for $[\rho]$ like (3.14) – and those that are not. The definition of $L(s,\rho)$ 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 $L_\infty(s,\rho)$, for the Brauer-dependent global definitions (3.18) and (3.19) will eventually be replaced by the Brauer-independent local definitions (3.50) and (3.51) below. However in the case of $W(\rho)$ a Brauer-independent definition is simply not known. By itself this is not problematic: while the decomposition (3.14) of $[\rho]$ is not unique, the resulting quantity (3.20) has to be independent of the decomposition because the functional equation (3.26) can't hold with two different values of $W(\rho)$. What is problematic, however, is that the definition (3.20) is not local. True, each factor $W(\chi_\xi)$ in (3.20) can be written as a product of local root numbers, but no analogue of Tate's local functional equation is known in dimension > 1, so even if one decomposes each $W(\chi_\xi)$ into local factors and reassembles the local factors corresponding to a given place v it is not obvious that the resulting local root number $W(\rho_v)$ is independent of the decomposition of $[\rho]$. That there is in fact a well-defined purely local root number is a theorem of Langlands and Deligne [**23**], about which we will have a little more to say in Lecture 4. For now we continue with the global theory but develop it in a more general context.

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 L-functions of Hecke characters of type (1,0) of imaginary quadratic fields and the L-functions of Hecke characters of finite order. However they do not include all Hecke L-functions: the L-functions of "nonalgebraic" Hecke characters like (2.50) will now fall by the wayside.

3.1. ℓ-adic representations

Up to this point, all representations have been defined 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.**

A key difference between complex and ℓ-adic Galois representations is that the latter need not factor through the Galois group of a finite Galois extension. Nonetheless, given a number field K and a prime ideal $\mathfrak{p}$ of K we can choose a prime ideal $\mathfrak{P}$ of $\overline{K}$ over $\mathfrak{p}$ and consider the associated inertia subgroup $I \subset \mathrm{Gal}(\overline{K}/K)$ and Frobenius coset $\sigma I = I\sigma$, where $\sigma \in \mathrm{Gal}(\overline{K}/K)$ is any Frobenius element at $\mathfrak{P}$. 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 σI to $\sigma' I'$. This was the property justifying certain definitions which we made for Artin representations and which therefore now go through for ℓ-adic representations as well. In particular, ρ_ℓ is **ramified** or **unramified** at $\mathfrak{p}$ according as $\rho_\ell|I$ is nontrivial or trivial, and if $\mathfrak{p} \nmid \ell$ then $B_\mathfrak{p}(x)$ is defined by analogy with (3.8):

$$B_\mathfrak{p}(x) = \det(1 - x\rho_\ell(\Phi)|V_\ell^I), \tag{3.27}$$

where $\Phi = \sigma^{-1}$ and V_ℓ is the space of ρ_ℓ. The subspace V_ℓ^I is defined as in (3.2) but with V and ρ replaced by V_ℓ and ρ_ℓ.

Note that in (3.27) we are following the geometric convention, as we shall do consistently from now on. The arithmetic convention would dictate that

$$B_\mathfrak{p}(x) = \det(1 - x\rho_\ell(\sigma)|(V_\ell)_I), \tag{3.28}$$

where $(V_\ell)_I$ is the space of **inertial coinvariants**, the quotient of V_ℓ by the subspace spanned by all expressions of the form $v - \rho_\ell(i)v$ with $v \in V_\ell$ and $i \in I$. The relation between the two conventions is that if $V_\ell^\vee$ is the dual space of V_ℓ then

$$\det(1 - x\rho_\ell^\vee(\Phi)|(V_\ell^\vee)^I) = \det(1 - x\rho_\ell(\sigma)|(V_\ell)_I). \tag{3.29}$$

To see that (3.28) generalizes Artin's original arithmetic definition (3.3), observe that V^I can be replaced by V_I in (3.3): Artin representations are complex representations of a finite group, hence semisimple.

3.2. Full compatibility

Since the coefficients of $B_\mathfrak{p}(x)$ lie in $\mathbb{Q}_\ell$ rather than in $\mathbb{C}$, it is not *a priori* meaningful to substitute $x = (\mathbf{N}\mathfrak{p})^{-s}$. But suppose that for each prime number ℓ we have an ℓ-adic representation ρ_ℓ of $\mathrm{Gal}(\overline{K}/K)$. The resulting collection $\{\rho_\ell\}$ is called a **family of ℓ-adic representations of** $\mathrm{Gal}(\overline{K}/K)$, and we say that the family is **fully compatible** if the following conditions are satisfied:

(i) There is a finite set S of prime ideals of K, independent of ℓ, such that if $\mathfrak{p} \notin S$ and $\mathfrak{p} \nmid \ell$ then ρ_ℓ is unramified at $\mathfrak{p}$.
(ii) The polynomial $B_\mathfrak{p}(x)$ in (3.27), which *a priori* has coefficients in $\mathbb{Q}_\ell$, actually has coefficients in $\mathbb{Q}$ and is independent of ℓ in the sense that $B_\mathfrak{p}(x)$ is unchanged if ℓ in (3.27) 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 $B_\mathfrak{p}(x)$ is required to be independent of ℓ *only for* $\mathfrak{p}$ *not in* S. There is also mere *compatibility*, an even weaker concept; see Serre [**82**], 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 [**26**], [**80**], and [**81**]. Fortunately, standard terms do exist for two other concepts: The fully compatible family $\{\rho_\ell\}$ 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.

3.3. Examples

The prototypical example of a fully compatible family of integral ℓ-adic representations of $\mathrm{Gal}(\overline{K}/K)$ is the one-dimensional family $\{\omega_\ell^{-1}\}$ consisting of the duals of the ℓ-adic cyclotomic characters

$$\omega_\ell : \mathrm{Gal}(\overline{K}/K) \to \mathbb{Z}_\ell^\times .$$

Let σ denote an arbitrary element of $\mathrm{Gal}(\overline{K}/K)$ and ζ an arbitrary root of unity of ℓ-power order. Then ω_ℓ is defined by the condition

$$\sigma(\zeta) = \zeta^{\omega_\ell(\sigma)}.$$

In particular, if σ is a Frobenius element at a prime ideal $\mathfrak{p}$ of K not dividing ℓ then $\omega_\ell(\sigma) = \mathbf{N}\mathfrak{p}$. Equivalently, if Φ is an inverse Frobenius at $\mathfrak{p}$ then $\omega_\ell^{-1}(\Phi) = \mathbf{N}\mathfrak{p}$, and consequently $B_\mathfrak{p}(x) = x - \mathbf{N}\mathfrak{p}$ by (3.27). Thus because we are following the geometric convention the family $\{\omega_\ell^{-1}\}$ is integral, but not the family $\{\omega_\ell\}$. The exceptional set of both families is the empty set.

Another example is provided by any elliptic curve E over K. Let $T_\ell(E)$ be the ℓ-adic Tate module of E, and let $\rho_{E,\ell}$ be the associated representation of $\mathrm{Gal}(\overline{K}/K)$ on the space $V_\ell(E) = \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_\ell(E)$. Then the family $\{\rho_{E,\ell}\}$ is fully compatible, and the dual family $\{\rho_{E,\ell}^\vee\}$ is fully compatible and integral. We remark that the ℓ-adic cohomology groups $H_\ell^1(E)$ are dual to the spaces $V_\ell(E)$, so that $\rho_{E,\ell}^\vee$ is the representation of $\mathrm{Gal}(\overline{K}/K)$ on $H_\ell^1(E)$. The exceptional set S of $\{\rho_{E,\ell}^\vee\}$ consists of the places where E has bad reduction.

The preceding example serves as a useful mnemonic device. The spaces $V_\ell(E)$ yield integral families relative to the arithmetic convention (3.28), while the spaces $H_\ell^1(E)$ yield integral families relative to the geometric convention (3.27). Since ℓ-adic cohomology is expected to be the primary source of fully compatible families, the geometric convention has been adopted as the standard.

3.4. λ-adic representations

If χ is a Dirichlet 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.

Let $\mathbb{E}$ be a number field and λ a finite place of $\mathbb{E}$ of residue characteristic ℓ. A representation with field of scalars $\mathbb{E}_\lambda$ is called a **λ-adic representation**. If $\mathbb{E} = \mathbb{Q}$ then we recover the notion of an ℓ-adic representation. Now let K be a number field and ρ_λ a λ-adic representation of $\mathrm{Gal}(\overline{K}/K)$. If $\mathfrak{p}$ is a prime ideal of K and I the inertia subgroup of $\mathrm{Gal}(\overline{K}/K)$ at some prime ideal of $\overline{K}$ over $\mathfrak{p}$ then we say that ρ_λ is **ramified** or **unramified** at $\mathfrak{p}$ according as $\rho_\lambda|I$ is nontrivial or trivial. And if $\mathfrak{p} \nmid \ell$ then we set

$$B_\mathfrak{p}(x) = \det(1 - x\rho_\lambda(\Phi)|V_\lambda^I), \tag{3.30}$$

where V_λ is the space of ρ_λ.

By a **family of λ-adic representations of** $\mathrm{Gal}(\overline{K}/K)$ we mean a collection $\{\rho_\lambda\}$, where λ runs over the finite places of $\mathbb{E}$ and ρ_λ is a λ-adic representation of $\mathrm{Gal}(\overline{K}/K)$. The family $\{\rho_\lambda\}$ is **fully compatible** if two conditions hold:

(i) There is a finite set S of prime ideals of K, independent of λ, such that if $\mathfrak{p} \notin S$ and $\mathfrak{p} \nmid \ell$ (ℓ being the residue characteristic of λ) then ρ_λ is unramified at $\mathfrak{p}$.

(ii) The polynomial $B_\mathfrak{p}(x)$ in (3.30) has coefficients in $\mathbb{E}$ and is unchanged if λ in (3.30) is replaced by λ', where λ' is another finite place of $\mathbb{E}$ of residue characteristic not divisible by $\mathfrak{p}$.

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

3.5. Compatible families of Artin and Hecke type

Let ρ be an Artin representation of K. Since any complex representation of a finite group is realizable over a number field, there is a representation of $\mathrm{Gal}(\overline{K}/K)$ on a vector space V over a number field $\mathbb{E} \subset \mathbb{C}$ such that ρ is the representation on $\mathbb{C} \otimes_\mathbb{E} V$ afforded by extension of scalars. But extension of scalars also gives 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.

Next let K be an imaginary quadratic field and χ a primitive Hecke character of K of type (1,0) and conductor $\mathfrak{f}$. Let $\mathbb{E}$ be the finite extension of K generated by the values of χ. Given a prime number ℓ and a prime ideal $\mathfrak{l}$ of $\mathbb{E}$ dividing ℓ, we consider the map

$$I(\mathfrak{f}\ell^n)/P_{\mathfrak{f}\ell^n} \to \mathbb{E}(\mathfrak{l}^n)/\mathbb{E}_{\mathfrak{l}^n}$$

given by

$$\mathfrak{a}P_{\mathfrak{f}\ell^n} \mapsto \chi(\mathfrak{a})^{-1}\mathbb{E}_{\mathfrak{l}^n} \tag{3.31}$$

for $\mathfrak{a} \in I(\mathfrak{f}\ell^n)$. This map is well defined by (1.10) (note in particular that $\chi(\mathfrak{a})$ is relatively prime to ℓ because $\chi(\mathfrak{a})^r$ is relatively prime to ℓ, where $r = |I(\mathfrak{f})/P_\mathfrak{f}|$).

Making our usual identification of $\mathbb{E}(\mathfrak{l}^n)/\mathbb{E}_{\mathfrak{l}^n}$ with $(\mathcal{O}_{\mathbb{E}}/\mathfrak{l}^n)^\times$ and then taking inverse limits, we obtain a one-dimensional λ-adic representation

$$\varprojlim{}_n I(\mathfrak{f}\ell^n)/P_{\mathfrak{f}\ell^n} \to \mathcal{O}_\lambda^\times, \tag{3.32}$$

where λ is the place of $\mathbb{E}$ corresponding to $\mathfrak{l}$. To get a λ-adic *Galois* representation χ_λ from (3.32), we identify the left-hand side of (3.32) with a quotient of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ by using the Artin isomorphism (3.6). The resulting family $\{\chi_\lambda\}$ is fully compatible and integral, and the exceptional set consists of the places of K dividing $\mathfrak{f}$.

3.6. 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 $\mathbb{C}$, we can define the L-function of M by analogy with (3.1):

$$L(s, M) = \prod_{\mathfrak{p}} B_{\mathfrak{p}}((\mathbf{N}\mathfrak{p})^{-s})^{-1}, \tag{3.33}$$

where $\mathfrak{p}$ runs over the prime ideals of K and $B_{\mathfrak{p}}(x)$ is as in (3.30).

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

$$L(s, M \oplus M') = L(s, M)L(s, M'). \tag{3.34}$$

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 $\mathrm{Gal}(\overline{K}/L)$. Then the family $\{\mathrm{ind}_{L/K}\rho_\lambda\}$ is also fully compatible, and its isomorphism class, which we will denote $\mathrm{ind}_{L/K}M$, satisfies

$$L(s, \mathrm{ind}_{L/K}M) = L(s, M). \tag{3.35}$$

As in the case of Artin L-functions, (3.34) is immediate from the definitions, (3.35) less straightforward.

By way of illustration, if ρ is an Artin representation and M is the isomorphism class of $\{\rho_\lambda\}$ then $L(s, M) = L(s, \rho^\vee)$, because we followed the arithmetic convention when defining Artin L-functions. On the other hand, if χ is a Hecke character of type $(1, 0)$ of an imaginary quadratic field and M is the isomorphism class of $\{\chi_\lambda\}$ then the net effect of the replacement of $\chi(\mathfrak{a})$ by $\chi(\mathfrak{a})^{-1}$ in (3.31) and the replacement of σ by Φ in (3.27) is to leave the L-function unchanged: $L(s, M) = L(s, \chi)$. Finally, if E is an elliptic curve and M is the isomorphism class of $\{\rho^\vee_{E,\ell}\}$ then $L(s, M) = L(s, E)$ by virtue of (3.29) with $V_\ell = V_\ell(E)$.

3.7. 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 $\operatorname{tr}\rho_\lambda(\Phi_\mathfrak{p}) = \operatorname{tr}\rho_{\lambda'}(\Phi_\mathfrak{p})$, because both traces coincide with the coefficient of $-x$ in $B_\mathfrak{p}(x)$. Thus $\operatorname{tr}\rho_\lambda$ and $\operatorname{tr}\rho_{\lambda'}$ coincide on a dense subset of $\mathrm{Gal}(\overline{K}/K)$. Since both are continuous each determines the other. $\square$

Without the semisimplicity assumption the assertion is false. For example, fix a finite place λ_0 of $\mathbb{E}$, 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.

3.8. 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 need to impose a condition on the **reciprocal roots** of $B_\mathfrak{p}(x)$, in other words the numbers $\alpha \in \mathbb{C}^\times$ 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 $\mathfrak{p} \notin S$ and one for $\mathfrak{p} \in S$. Fix $w \in \mathbb{Z}$ and let τ run over arbitrary field automorphisms of $\mathbb{C}$. The conditions are

$$|\tau(\alpha)| = (\mathbf{N}\mathfrak{p})^{w/2} \qquad (\mathfrak{p} \notin S) \tag{3.36}$$

and

$$|\tau(\alpha)| \leqslant (\mathbf{N}\mathfrak{p})^{w/2} \qquad (\mathfrak{p} \in S) \tag{3.37}$$

respectively. If M satisfies (3.36) and (3.37) then we say that M has **weight** w.

The point of this definition is that 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 (3.36) and (3.37) only for τ equal to the identity automorphism, but by allowing $\tau \in \mathrm{Aut}(\mathbb{C})$ to be arbitrary, we compensate for the fact that we have fixed an embedding of $\mathbb{E}$ in $\mathbb{C}$. Fixing such an embedding is convenient, but we do not want our definition of *weight* to depend on the choice of embedding.

Next we want an analytic continuation and functional equation. To begin to formulate the latter, we introduce the notion of a **gamma factor of weight** w over K. This term will refer to any product of the form

$$\gamma(s) = \prod_{v|\infty} \gamma_v(s), \tag{3.38}$$

where $\gamma_v(s)$ is a a gamma factor of weight w over K_v in the following sense.

If w is odd, or if w is even and $K_v \cong \mathbb{C}$, then $\gamma_v(s)$ is a product of the form

$$\gamma_v(s) = \prod_{\substack{p+q=w \\ q\geqslant p\geqslant 0}} \Gamma_{\mathbb{C}}(s-p)^{h^{pq}}, \tag{3.39}$$

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 $\gamma_v(s)$ is a product of the form

$$\gamma_v(s) = \Gamma_{\mathbb{R}}(s-w/2)^{h^{w/2+}} \cdot \Gamma_{\mathbb{R}}(s-w/2+1)^{h^{w/2-}} \cdot \prod_{\substack{p+q=w \\ q>p\geqslant 0}} \Gamma_{\mathbb{C}}(s-p)^{h^{pq}}, \tag{3.40}$$

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.

3.9. 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

$$\overline{M} = M^\vee(-w) \tag{3.41}$$

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 to $B_{\mathfrak{p}}(x)$ 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 (3.36), at least if $\mathfrak{p} \notin S$, so

$$\alpha_j^{-1} \cdot (\mathbf{N}\mathfrak{p})^w = \overline{\alpha_j} \qquad (\mathfrak{p} \notin S). \tag{3.42}$$

The notation for the left-hand side of (3.41) is meant to remind us of (3.42).

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

$$M(\chi) = \mathrm{ind}_{K/\mathbb{Q}} M'(\chi). \tag{3.43}$$

If χ is equivariant in the sense that it satisfies the identity $\chi(\overline{\mathfrak{a}}) = \overline{\chi}(\mathfrak{a})$ 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 (3.35) with $L(s, M'(\chi))$ and hence with $L(s,\chi)$, Theorem 1.2 remains valid with $L(s,\chi)$ replaced by $L(s, M(\chi))$.

3.10. An algebraic desideratum

There is one further requirement that we would like to impose on M. Let $\{\rho_\lambda\}$ be a 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 $\overline{K}$ above $\mathfrak{p}$. 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 the characteristic polynomial of $\rho_\lambda(g)$ to have coefficients in $\mathbb{E}$ and to be independent of λ for all finite places λ of $\mathbb{E}$ such that $\mathfrak{p}$ and λ are of distinct residue characteristics. The reason for referring to this property as "Condition C_8" is that it is so labeled in Serre [**81**]. We could also have referred to Problem 2 on p. 514 of Serre-Tate [**86**]. 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 $s = w/2 + 1$ 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 $\gamma(s) = L_\infty(s, M)$ 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 $k = w + 1$.

The **rank** of M is the dimension of ρ_λ for $\{\rho_\lambda\} \in M$, and if we can choose $\{\rho_\lambda\}$ to have a given number field $\mathbb{E}$ as coefficient field then we say that M **admits** $\mathbb{E}$ **as coefficient field**.

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 and 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.

What is more problematic about the definition is that by requiring (ii) and (iii) we have limited our stock of examples. Not that we are entirely without examples: The isomorphism class of $\{\omega_\ell^{-w/2}\}$ is a premotive of weight w for any even integer $w \geqslant 0$, and if K is an imaginary quadratic field, χ a Hecke character of K of type $(1, 0)$, and $M(\chi)$ and $M(\chi')$ as in (3.43), then $M(\chi)$ and $M(\chi')$ are premotives of weight 1 over K and $\mathbb{Q}$ respectively by virtue of the analytic properties of Hecke L-functions, in particular Theorem 2.1. But we cannot make the analogous claim for an arbitrary Artin representation ρ of a number field K because (ii) is unknown in general: The statement that $L(s, \rho)$ is holomorphic everywhere except possibly at $s = 1$ is the Artin conjecture. (More precisely, the Artin conjecture asserts that if ρ is irreducible and nontrivial then $L(s,\rho)$ is entire. But if ρ is irreducible and trivial then $L(s,\rho)=\zeta_K(s)$. Hence by additivity the Artin conjecture implies that for any ρ, irreducible or not, $L(s,\rho)$ is holomorphic except possibly at $s=1$.) While the Artin conjecture is known in certain cases – including for example the case of monomial representations, where it follows by inductivity from the analytic properties of Hecke L-functions, and many two-dimensional cases (Langlands [**57**], Tunnell [**97**], and Khare and Wintenberger [**50**], [**51**] with Kisin [**52**]) – the fact remains that Artin representations do not automatically provide examples of premotives. Similarly, if E is an elliptic curve over $\mathbb{Q}$ then the isomorphism class of $\{\rho^\vee_{E,\ell}\}$ is a premotive of weight 1 by virtue of the modularity of E (Wiles [**100**], Taylor and Wiles [**96**], and Breuil, Conrad, Diamond, and Taylor [**11**]), but if $\mathbb{Q}$ is replaced by an arbitrary number field then the assertion remains conjectural.

In spite of this objection, we have included (ii) and (iii) in the definition so as to be able to refer to the order of vanishing of $L(s,M)$ at $s=(w+1)/2$ without using the word *conjectural* at every turn. But when we are not talking about trivial central zeros (ii) and (iii) will play no role.

5. Uniqueness of the functional equation

Given that we do include the functional equation in the definition, it may seem strange that the factors $A(M)$, $W(M)$, and $L_\infty(s,M)$ are not defined more precisely. However the following proposition shows that they are in fact uniquely determined by the functional equation. Both the proposition and its proof were suggested by Théorème 4.6 on p. 514 of Deligne-Serre [**25**].

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

$$(A(M)/\widetilde{A}(M))^{s/2}\frac{\gamma(s)}{\tilde\gamma(s)}=(W(M)/\widetilde{W}(M))(A(M)/\widetilde{A}(M))^{(k-s)/2}\frac{\gamma(k-s)}{\tilde\gamma(k-s)}. \tag{3.44}$$

Now it follows from the formulas (3.39) and (3.40) that the left-hand side of (3.44) 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 (3.44) 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 w 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 $\widetilde{W}(M)=W(M)$. □

6. An open problem

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

Problem 3. *Does every premotive come from a motive?*

This is not a new question. In fact a stronger version appears as Question 2 on p. I-12 of Serre [**82**], and while the Fontaine-Mazur conjecture [**30**] is concerned with other issues, it too implies a statement about the provenance of fully compatible families which is in most respects much stronger than what we are asking for here (see [**30**], pp. 196 – 197). Furthermore, the converse of Problem 3 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, not only because the analytic continuation and functional equation of $L(s, M)$ are not known, but also because the full compatibility of the family of λ-adic representations attached to M is not known either, nor the semisimplicity of the representations ρ_λ, nor Condition C_8.

Since Problem 3 and its converse are already well-known open problems, the only reason for drawing attention to them here is 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 (3.39) and (3.40), because if M does come from a motive then the gamma factor $L_\infty(s, M)$ that one associates to M is given by (3.38) with h^{pq} and $h^{p\pm}$ equal to the usual Hodge numbers; cf. [**24**], 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, Problem 3 has little bearing on our present train of thought. We would like to define $A(M)$ and $W(M)$ as products of local factors rather than via the abstract uniqueness of a conjectural functional equation. While the quest for such a self-contained local definition will encounter a difficulty, the difficulty would not disappear if we knew that our premotive came from a motive.

7. Local factors for Artin L-functions

Earlier we mentioned that if ρ is an Artin representation of K then the factors $A(\rho)$ and $L_\infty(s, \rho)$ defined by (3.18) and (3.19) respectively could also be defined in a Brauer-independent and local way. We now record these local definitions, thereby demonstrating that in the case of Artin representations, the theory to be described in the next lecture is needed only for the sake of $W(\rho)$.

7.1. The exponential factor

Given a finite place v of K, we identify $\mathrm{Gal}(\overline{K_v}/K_v)$ with the decomposition subgroup of $\mathrm{Gal}(\overline{K}/K)$ at some place of $\overline{K}$ above v, and we put $\rho_v = \rho|\mathrm{Gal}(\overline{K_v}/K_v)$. The **conductor** of ρ is the integral ideal

$$\mathfrak{f}(\rho) = \prod_{v \nmid \infty} \mathfrak{p}_v^{a(\rho_v)} \tag{3.45}$$

of K, where $\mathfrak{p}_v$ is the prime ideal corresponding to v and $a(\rho_v)$ is the **exponent of the local conductor**, a nonnegative integer still to be defined. The definition will show that $a(\rho_v) > 0$ if and only if ρ is ramified at $\mathfrak{p}_v$. Since ρ is unramified outside a finite set it follows that the product on the right-hand side of (3.45) is finite.

The definition of $a(\rho_v)$ is a purely local matter, and thus we change our notation by dropping the subscript v: K is now a finite extension of $\mathbb{Q}_p$ with $p < \infty$, and ρ is a representation of $\mathrm{Gal}(\overline{K}/K)$. We choose a finite Galois extension L of K such that ρ factors through $\mathrm{Gal}(L/K)$, and we view ρ as a representation of $\mathrm{Gal}(L/K)$.

The definition of $a(\rho)$ involves the higher ramification subgroups I_n $(n \geqslant 0)$ of $\mathrm{Gal}(L/K)$. If $n = 0$ then $I_n = I$, the inertia subgroup of $\mathrm{Gal}(L/K)$, and in general

$$I_n = \{\sigma \in I : \sigma(x) \equiv x \pmod{\mathfrak{p}_L^{n+1}} \text{ for all } x \in \mathcal{O}_L\},$$

where $\mathcal{O}_L$ is the ring of integers of L and $\mathfrak{p}_L$ its maximal ideal. Let V be the space of ρ and V^{I_n} the subspace of vectors fixed by $\rho(I_n)$. Then

$$a(\rho) = \sum_{n \geqslant 0} (e_n/e) \dim(V/V^{I_n}), \tag{3.46}$$

where $e_n = |I_n|$ and $e\ (= e_0)$ is the ramification index of L over K. If n is sufficiently large then I_n is the trivial subgroup of $\mathrm{Gal}(L/K)$, so the sum is finite. Also $V^I = V$ if and only if $\rho(I)$ is the trivial subgroup of $\mathrm{GL}(V)$, so $a(\rho) = 0$ if and only if ρ is unramified, as already mentioned. That $a(\rho)$ is integral and independent of the choice of L follows from an alternative expression for $a(\rho)$ as an inner product of the character of ρ with the "Artin character" (see Chapter VI of Serre [**83**], especially Theorem 1' on p. 99 and the Corollary to Proposition 3 on p. 101).

The conductor-exponents $a(\rho)$ satisfy a modified Artin formalism, and consequently so does the global conductor (3.45). We will go directly to the global version, and thus we take K to be a number field again. The additivity of the conductor is immediate from the definitions: If ρ and ρ' are Artin representations of K then

$$\mathfrak{f}(\rho \oplus \rho') = \mathfrak{f}(\rho)\mathfrak{f}(\rho'). \tag{3.47}$$

Next let M be a finite extension of K and ρ an Artin representation of M. The counterpart to inductivity is not quite invariance under induction but rather

$$\mathfrak{f}(\mathrm{ind}_{M/K}\rho) = \mathfrak{d}_{M/K}^{\dim\rho} N_{M/K}(\mathfrak{f}(\rho)), \tag{3.48}$$

where $\mathfrak{d}_{M/K}$ is the relative discriminant ideal of the extension M/K. Finally, if ξ is a one-dimensional Artin representation and χ_ξ the corresponding idele class character of finite order, then

$$\mathfrak{f}(\xi) = \mathfrak{f}(\chi_\xi), \tag{3.49}$$

where the right-hand side is the usual conductor of an idele class character, defined as in (2.21).

Now let D be the absolute value of the discriminant of K. Given an Artin representation ρ of K, we define its **exponential factor** to be the positive integer

$$A(\rho) = D^{\dim\rho}\mathbf{N}\mathfrak{f}(\rho). \tag{3.50}$$

From (3.47), (3.48), and (3.49) we deduce the Artin formalism for the exponential factor: $A(\rho\oplus\rho') = A(\rho)A(\rho')$, $A(\inf_{M/K}\rho) = A(\rho)$, and $A(\xi) = A(\chi_\xi)$. Using these identities, one can verify that the exponential factor defined by (3.50) coincides with the Brauer-dependent quantity defined by (3.18).

7.2. The gamma factor

Given an infinite place v of K we identify the decomposition subgroup of $\mathrm{Gal}(\overline{K}/K)$ at some place above v with $\mathrm{Gal}(\overline{K_v}/K_v)$, just as in the archimedean case. Of course in the archimedean case there is no distinction between the decomposition and inertia groups: Either both are trivial or both are the group of order two generated by the relevant complex conjugation. If ρ is an Artin representation of K then we put $\rho_v = \rho|\mathrm{Gal}(\overline{K_v}/K_v)$ and define the gamma factor of ρ to be the product

$$L_\infty(s,\rho) = \prod_{v|\infty} L(s,\rho_v), \tag{3.51}$$

where the individual factors $L(s,\rho_v)$ must still be defined. Since the issue is now local, we fix v and drop the subscript on ρ_v and K_v. Thus ρ is a representation of $\mathrm{Gal}(\overline{K}/K)$ with $K = \mathbb{R}$ or $K \cong \mathbb{C}$.

The first step is to declare that $L(s,\rho\oplus\rho') = L(s,\rho)L(s,\rho')$ and thus to reduce the definition of $L(s,\rho)$ to the case where ρ is one-dimensional. Next, to a one-dimensional ρ we associate a character χ of $K^\times$ as follows: If ρ is trivial then χ is trivial, and if $K = \mathbb{R}$ and ρ is the nontrivial character of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ then χ is the sign character of $\mathbb{R}^\times$. We put

$$L(s,\rho) = L(s,\chi). \tag{3.52}$$

Referring to (2.25) and (2.26), we see that the definition (3.52) amounts to saying that if $K \cong \mathbb{C}$ then $L(s,\rho) = \Gamma_{\mathbb{C}}(s)$ and if $K = \mathbb{R}$ then $L(s,\rho)$ is either $\Gamma_{\mathbb{R}}(s)$ or $\Gamma_{\mathbb{R}}(s+1)$ according as ρ is trivial or nontrivial.

8. Exercises

Exercise 3.1. Give examples of a one-dimensional Artin representation and a two-dimensional irreducible Artin representation such that the associated Artin L-function has a trivial central zero. (Hint: Exercise 2.7 with (3.5) and induction.)

Exercise 3.2. Let K be a number field and L a Galois extension of K with $\mathrm{Gal}(L/K)$ isomorphic to A_4, the alternating group on 4 letters. Let ρ be the irreducible complex representation of $\mathrm{Gal}(L/K)$ of dimension 3, unique up to isomorphism. Show that $W(\rho) = 1$. (Hint: Write ρ as a monomial representation and apply Theorem 2.2, or else use Theorem 2.2 in conjunction with (3.53) below.) Incidentally, both this exercise and Theorem 2.2 are instances of a result of Fröhlich and Queyrut [**33**] asserting that $W(\rho) = 1$ if ρ is orthogonal.

Exercise 3.3. Let K be a number field and L a finite Galois extension of K. Using the fact that $\mathrm{ind}_{L/K} 1_L$ is the regular representation of $\mathrm{Gal}(L/K)$, show that

$$\zeta_L(s) = \prod_{\rho} L(s,\rho)^{\dim\rho}, \tag{3.53}$$

where ρ runs over the distinct isomorphism classes of irreducible complex representations of $\mathrm{Gal}(L/K)$. In particular, if one of the L-functions in (3.53) has a trivial central zero (as Exercise 3.1 shows can happen) and the others are holomorphic at $s = 1/2$ (as the Artin conjecture says they must be) then $\zeta_L(1/2) = 0$. But the zero of $\zeta_L(s)$ at $s = 1/2$ is not a trivial central zero as we have defined the term, because the functional equation of $\zeta_L(s)$ is $Z_L(s) = Z_L(1-s)$. This is arguably a reason to revise our notion of a trivial zero to take account not only of the functional equation of the given L-function but also of the functional equation of its factors.

Exercise 3.4. Let $\mathbb{E}_\lambda$ be a finite extension of $\mathbb{Q}_\ell$ and ρ_λ a λ-adic representation of a compact group G. Put $d = \dim \rho_\lambda$. Prove that ρ_λ is equivalent to a representation into $\mathrm{GL}_d(\mathcal{O}_\lambda)$, where $\mathcal{O}_\lambda$ is the ring of integers of $\mathbb{E}_\lambda$. (Hint: View ρ_λ as a continuous homomorphism $G \to \mathrm{GL}_d(\mathbb{E}_\lambda)$, and let H be the inverse image of $\mathrm{GL}_d(\mathcal{O}_\lambda)$. Then H is an open subgroup of G, hence of finite index. Let $\mathcal{L}$ be the sum of the $\mathcal{O}_\lambda$-submodules $\rho_\lambda(g)(\mathcal{O}_\lambda^d)$ of $\mathbb{E}_\lambda^d$, 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 $\mathbb{E}_\lambda^d$.)

Exercise 3.5. Let $\{\rho_\ell\}$ be a fully compatible family of one-dimensional ℓ-adic representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with exceptional set $S = \emptyset$. Prove that $\rho_\ell = \omega_\ell^n$ for some $n \in \mathbb{Z}$.

Exercise 3.6. Let K be a number field, and consider the map $\rho \mapsto \{\rho_\lambda\}$ 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 a family $\{\rho_\lambda\}$ then the key point is to show that the image of ρ_λ is finite. By Exercise 3.4, ρ_λ may be viewed as a continuous homomorphism $\mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_d(\mathcal{O}_\lambda)$. Let $\mathbb{F}_\lambda$ be the residue class field of $\mathcal{O}_\lambda$ and ℓ the residue characteristic. Show that the reduction map $\mathrm{GL}_d(\mathcal{O}_\lambda) \to \mathrm{GL}_d(\mathbb{F}_\lambda)$ is injective on elements of order prime to ℓ.)

Exercise 3.7. (*Reading.*) Let K and $\mathbb{E}$ be number fields. Given a fully compatible family $\{\rho_\lambda\}$ over K with coefficient field $\mathbb{E}$, consider the extension F of $\mathbb{E}$ generated by all the roots of the equations $B_\mathfrak{p}(x) = 0$ as $\mathfrak{p}$ varies over prime ideals of K. A necessary and condition for F to be of finite degree over $\mathbb{E}$ is given by Khare [**49**]. By examining some special cases (e. g. elliptic curves, Artin representations) and perhaps glancing at the title of Khare's paper, try to guess what Khare's necessary and sufficient condition is. Then compare your answer to [**49**].

LECTURE 4

Local formulas in arbitrary dimension

To associate a local factor to an Artin representation one starts by restricting the Artin representation to a decomposition subgroup, but to deal with more general premotives one is forced to replace the decomposition subgroup by its close relative, the local Weil or Weil-Deligne group.

1. The local Weil and Weil-Deligne groups

Until further notice, K denotes a finite extension of $\mathbb{Q}_p$ with $p < \infty$. As usual, $\mathcal{O}$ is the ring of integers of K and π a uniformizer of $\mathcal{O}$, and we put $q = ||\pi||^{-1} = |\mathcal{O}/\pi\mathcal{O}|$. The maximal unramified extension of K inside $\overline{K}$ will be denoted K_{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 $\mathrm{Gal}(\overline{K}/K_{\mathrm{unr}})$.

1.1. The Weil group

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

$$\mathrm{W}(\overline{K}/K) = \bigcup_{n\in\mathbb{Z}} \sigma^n I. \tag{4.1}$$

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 (4.1) 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 $\mathrm{W}(\overline{K}/K)$ and make $\mathrm{W}(\overline{K}/K)$ 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

$$\mathrm{W}(\overline{K}/K)/\mathrm{W}(\overline{K}/L) \cong \mathrm{Gal}(\overline{K}/K)/\mathrm{Gal}(\overline{K}/L) \cong \mathrm{Gal}(L/K). \tag{4.2}$$

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, and it is then determined by its value on σ. In particular, there is a unique 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 the intersection $\mathrm{Gal}(\overline{K}/K^{\mathrm{ab}}) \cap \mathrm{W}(\overline{K}/K)$. 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 Artin 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. Thus a one-dimensional representation ρ of $\mathrm{W}(\overline{K}/K)$ is the same thing as a character χ of $K^\times$. In making the identification we follow the geometric convention:

$$\rho((x, K^{\mathrm{ab}}/K)) = \chi(x^{-1}) \qquad (x \in K^\times). \tag{4.3}$$

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 $K^\times$.

1.2. The Weil-Deligne group

With regard to the **Weil-Deligne group** $\mathrm{WD}(\overline{K}/K)$ our point of view will be tannakian: Instead of defining $\mathrm{WD}(\overline{K}/K)$ itself we define its representations. 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 a nilpotent endomorphism of the space of ρ satisfying

$$\rho(g)N\rho(g)^{-1} = \omega(g)N \tag{4.4}$$

for $g \in \mathrm{W}(\overline{K}/K)$. Henceforth representations of $\mathrm{W}(\overline{K}/K)$ will be viewed as the special case $N = 0$ of representations of $\mathrm{WD}(\overline{K}/K)$. 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 following proposition will be needed later and for the moment can serve to illustrate the definitions just made. Let us 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 4.1. *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. The proof is like the standard argument that commuting matrices over an algebraically closed field are simultaneously triangularizable. The only reason for reviewing the details is to illustrate the use of (4.4). In fact consider endomorphisms A and N of a finite-dimensional complex vector space V such that N is nilpotent and $AN = cNA$ with a nonzero scalar c. Write V_N for the kernel of N. We will 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 $v_2 + W, v_3 + W, \ldots, v_n + W$ for V/W relative to which these endomorphisms are upper-triangular. Then A and N are upper-triangular relative to the basis for V consisting of $v_1, v_2, \ldots, v_n$. □

1.3. Operations on representations of the Weil-Deligne group

A representation of $\mathrm{WD}(\overline{K}/K)$ as defined above is not quite a group representation in the usual sense, so the standard operations of representation theory may require some explication. In the following definitions the field of scalars is taken to be $\mathbb{C}$, but $\mathbb{C}$ could be replaced by any field of characteristic zero.

If $\boldsymbol{\rho} = (\rho, N)$ and $\boldsymbol{\rho}' = (\rho', N')$ are representations of $\mathrm{WD}(\overline{K}/K)$ then we define their **direct sum** by

$$\boldsymbol{\rho} \oplus \boldsymbol{\rho}' = (\rho \oplus \rho', N \oplus N') \tag{4.5}$$

and their **tensor product** by

$$\boldsymbol{\rho} \otimes \boldsymbol{\rho}' = (\rho \otimes \rho', N \otimes 1' + 1 \otimes N'), \tag{4.6}$$

where 1 and $1'$ denote the identity automorphism of the space of $\boldsymbol{\rho}$ and $\boldsymbol{\rho}'$ respectively. In particular, for $s_0 \in \mathbb{C}$ we have

$$\boldsymbol{\rho} \otimes \omega^{s_0} = (\rho \otimes \omega^{s_0}, N). \tag{4.7}$$

This follows from (4.6) 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': Thus $T\rho(g) = \rho'(g)T$ for $g \in \mathrm{WD}(\overline{K}/K)$ and $TN = N'T$. An intertwining map which is a linear isomorphism is an **isomorphism of representations**.

Given a representation $\boldsymbol{\rho}$ of $\mathrm{WD}(\overline{K}/K)$, we define its **dual** $\boldsymbol{\rho}^\vee$ by

$$\boldsymbol{\rho}^\vee = (\rho^\vee, -N^\vee). \tag{4.8}$$

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

Given a finite extension L of K inside $\overline{K}$, put $\mathrm{res}_{L/K}\rho = \rho|\mathrm{WD}(\overline{K}/L)$. Then

$$\mathrm{res}_{L/K}\boldsymbol{\rho} = (\mathrm{res}_{L/K}\rho, N) \tag{4.9}$$

is the **restriction** of $\boldsymbol{\rho}$ to $\mathrm{WD}(\overline{K}/L)$.

Finally, with L still a finite extension of K, take $\boldsymbol{\rho}$ to be a representation of $\mathrm{WD}(\overline{K}/L)$. To define the **induced representation** $\mathrm{ind}_{L/K}\boldsymbol{\rho}$ of $\mathrm{WD}(\overline{K}/K)$, let V be the space of $\boldsymbol{\rho}$ and put $G = \mathrm{W}(\overline{K}/K)$ and $H = \mathrm{W}(\overline{K}/L)$. Then ρ makes V into an H-module, and we can take the space of $\mathrm{ind}_{L/K}\rho$ to be $\mathbb{C}[G] \otimes_{\mathbb{C}[H]} V$. We set

$$\mathrm{ind}_{L/K}\boldsymbol{\rho} = (\mathrm{ind}_{L/K}\rho, \omega^{-1} \cdot (1 \otimes N)), \tag{4.10}$$

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

$$\omega^{-1} \cdot (1 \otimes N)(g \otimes v) = \omega^{-1}(g)(g \otimes Nv) \tag{4.11}$$

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

Let us verify that (4.11) gives a well-defined endomorphism of $\mathbb{C}[G] \otimes_{\mathbb{C}[H]} V$ and that the resulting pair (4.10) satisfies (4.4). To facilitate the verifications, we 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. Then $\omega_K|\mathrm{W}(\overline{K}/L) = \omega_L$. Now to see that $\omega^{-1} \cdot (1 \otimes N)$ is well defined, we must examine (4.11) when $g \otimes v$ is rewritten as $gh \otimes \rho(h)^{-1}v$ with $h \in H$. According to (4.11), we get

$$\omega^{-1} \cdot (1 \otimes N)(gh \otimes \rho(h)^{-1}v) = \omega_K^{-1}(gh)(gh \otimes N\rho(h)^{-1}v). \tag{4.12}$$

As $N\rho(h)^{-1} = \omega_L(h)\rho(h)^{-1}N$, we see that (4.11) and (4.12) are consistent.

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 $\varphi(g)^{-1}(g' \otimes v) = g^{-1}g' \otimes v$, (4.11) 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. It is instructive to drop the tannakian perspective for a moment and let the cat out of the bag: As an actual group, $\mathrm{WD}(\overline{K}/K)$ is just the semidirect product $\mathbb{C} \rtimes \mathrm{W}(\overline{K}/K)$ with $gzg^{-1} = \omega(g)z$ for $g \in \mathrm{W}(\overline{K}/K)$ and $z \in \mathbb{C}$. One is supposed to view the factor $\mathbb{C}$ as the set of complex points of the algebraic group $\mathbb{G}_{\mathrm{a}}$, so 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 preceding definitions for $\oplus$, $\otimes$, and so on are just the standard operations of representation theory applied to the group $\mathbb{C} \rtimes \mathrm{W}(\overline{K}/K)$.

1.4. The archimedean Weil group

Now suppose that $K = \mathbb{R}$ or $K \cong \mathbb{C}$. In the archimedean case there is no distinction between $\mathrm{W}(\overline{K}/K)$ and $\mathrm{WD}(\overline{K}/K)$; the notations $\mathrm{W}(\overline{K}/K)$ and $\mathrm{WD}(\overline{K}/K)$ are interchangeable. The definition is as follows. If $K \cong \mathbb{C}$ then

$$\mathrm{W}(\overline{K}/K) = \mathrm{W}(\overline{K}/\overline{K}) = K^\times \cong \mathbb{C}^\times,$$

and if $K = \mathbb{R}$ then

$$\mathrm{W}(\overline{K}/K) = \overline{K}^\times \cup J\overline{K}^\times \cong \mathbb{C}^\times \cup J\mathbb{C}^\times,$$

where $J^2 = -1$ and $JzJ^{-1} = \overline{z}$ for $z \in \overline{K}^\times \cong \mathbb{C}^\times$. In the case $K = \mathbb{R}$ we identify the subgroup $\overline{K}^\times$ of $\mathrm{W}(\overline{K}/K)$ with $\mathrm{W}(\overline{K}/\overline{K})$, which thus becomes a subgroup of index 2 in $\mathrm{W}(\overline{K}/K)$. The nontrivial coset is represented by J.

The reason that we have been so pedantic about distinguishing $\mathrm{W}(\overline{K}/K)$ from $\mathbb{C}^\times$ (when $K \cong \mathbb{C}$) or from $\mathbb{C}^\times \cup J\mathbb{C}^\times$ (when $K = \mathbb{R}$) is that we would like to identify $\mathrm{W}(\overline{K}/K)^{\mathrm{ab}}$ with $K^\times$, just as in the nonarchimedean case. Let $\pi : \mathrm{W}(\overline{K}/K) \to K^\times$ be the identity map if $K \cong \mathbb{C}$ and the map sending J to -1 and z to $|z|^2$ if $K = \mathbb{R}$. Then π factors through a map $\mathrm{W}(\overline{K}/K)^{\mathrm{ab}} \to K^\times$, and we claim that the latter map is an isomorphism. This is obvious if $K \cong \mathbb{C}$, so suppose that $K = \mathbb{R}$. One readily verifies that the commutator subgroup of $\mathrm{W}(\overline{K}/K)$ consists of all elements of the form $JzJ^{-1}z^{-1}$ with $z \in \overline{K}$. Furthermore, let $\mathbf{T}$ be the subgroup of $\overline{K}^\times$ consisting of numbers of absolute value 1. Since $JzJ^{-1}z^{-1} = \overline{z}/z$ it follows that the commutator subgroup of $\mathrm{W}(\overline{K}/K)$ is $\mathbf{T}$, and it is also easy to see that $\mathbf{T}$ is the kernel of π and that π is surjective. Thus $\mathrm{W}(\overline{K}/K)^{\mathrm{ab}} \cong K^\times$ as claimed.

Henceforth we shall identify the one-dimensional characters of $\mathrm{W}(\overline{K}/K)$ with those of $K^\times$ by putting

$$\chi(g) = \chi(\pi(g)) \qquad (g \in \mathrm{W}(\overline{K}/K)). \tag{4.13}$$

This is the archimedean analogue of (4.3). Given that we know the characters of $\mathbb{C}^\times$ and $\mathbb{R}^\times$ explicitly, we can regard (4.13) as an explicit description of the characters of $\mathrm{W}(\overline{K}/K)$. In fact we can describe not just the one-dimensional representations but all the irreducible complex representations of $\mathrm{W}(\overline{K}/K)$. If $K \cong \mathbb{C}$ then $\mathrm{W}(\overline{K}/K)$ is abelian and there are no irreducible representations of dimension > 1, and if $K = \mathbb{R}$ then $\mathrm{W}(\overline{K}/K)$ has an abelian subgroup of index 2, namely $\mathrm{W}(\overline{K}/\overline{K})$, whence any irreducible representation of $\mathrm{W}(\overline{K}/K)$ of dimension > 1 is two-dimensional, induced by a character of $\mathrm{W}(\overline{K}/\overline{K})$. Let χ be a character of $\mathrm{W}(\overline{K}/\overline{K})$ and let $\rho = \mathrm{ind}_{\overline{K}/K}\chi$ be the representation of $\mathrm{W}(\overline{K}/K)$ it induces. Identifying $\mathrm{W}(\overline{K}/\overline{K})$ with $\mathbb{C}^\times$ and writing $\chi(z) = |z|^{2s_0}(z/|z|)^m$ with $s_0 \in \mathbb{C}$ and $m \in \mathbb{Z}$, one checks that ρ is irreducible if and only if $m \neq 0$.

2. From Galois representations to Weil-Deligne representations

Let K be a number field. We seek an analogue for premotives of the map $\rho \mapsto \rho_v$ sending an Artin representation of K to its restriction to a decomposition subgroup of $\mathrm{Gal}(\overline{K}/K)$ at a given place v of K. The analogue should be a map $M \mapsto \boldsymbol{\rho}_{M,v}$, where M is a premotive over K and $\boldsymbol{\rho}_{M,v}$ a complex representation of $\mathrm{WD}(\overline{K}_v/K_v)$. What the theory of Grothendieck and Deligne provides in the first instance, however, is a purely local correspondence from λ-adic representations of $\mathrm{Gal}(\overline{K}_v/K_v)$ to λ-adic representations of $\mathrm{WD}(\overline{K}_v/K_v)$. To describe this local correspondence we make two preliminary remarks about profinite groups.

Given a prime ℓ, we say that a profinite group has order prime to ℓ if it is an inverse limit of finite groups of order prime to ℓ. The first remark is that every homomorphism (of topological groups) from a profinite group of order prime to ℓ to a pro-ℓ-group is trivial. This follows from the corresponding fact about finite groups.

Let Γ be a pro-ℓ-group and $\varphi : \mathbb{Z}_\ell \to \Gamma$ a homomorphism. The second remark is that if $\gamma = \varphi(1)$ then for arbitrary $z \in \mathbb{Z}_\ell$ we have $\varphi(z) = \gamma^z$, the point being that γ^z is meaningful as a limit even if $z \notin \mathbb{Z}$. More generally, suppose that I is a profinite group with the following property: There is a closed normal subgroup Q of I, of profinite order prime to ℓ, such that $I/Q \cong \mathbb{Z}_\ell$. If $t : I \to \mathbb{Z}_\ell$ is an epimorphism and $\varphi : I \to \Gamma$ an arbitrary homomorphism then

$$\varphi(i) = \gamma^{t(i)} \tag{4.14}$$

for $i \in I$, where $\gamma \in \Gamma$ is the image under φ of any preimage of $1 \in \mathbb{Z}_\ell$ under t.

2.1. The local correspondence

Now let K be a finite extension of $\mathbb{Q}_p$ with $p < \infty$, and write K_{tame} for the maximal tamely ramified extension of K inside $\overline{K}$. 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 gives an identification of $\mathrm{Gal}(K_{\mathrm{unr}}(\varpi^{1/n})/K_{\mathrm{unr}})$ with $\mathbb{Z}/n\mathbb{Z}$ and hence an identification

$$I/P \cong \prod_{\ell \neq p} \mathbb{Z}_\ell \tag{4.15}$$

after taking inverse limits. Since P is a pro-p-group, it follows that if $\ell \neq p$ then there is a closed normal subgroup Q of I, profinite of order prime to ℓ, such that $I/Q \cong \mathbb{Z}_\ell$. In particular, the space of homomorphisms $I \to \mathbb{Q}_\ell$ is one-dimensional over $\mathbb{Q}_\ell$. Furthermore (4.15) and our deductions from it hold with I replaced by any open subgroup I' of I and P by $P \cap I'$, because any open subgroup of the right-hand side of (4.15) is again isomorphic to the right-hand side of (4.15).

The theorem to be stated next combines results of Grothendieck and Deligne, and the proof follows the exposition of Serre-Tate ([**86**], pp. 515 – 516) and Deligne ([**23**], pp. 566 – 571). 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 $\boldsymbol{\rho}$ constructed in the theorem below is independent of the choice of t_ℓ and σ (cf. [**23**], p. 569). However we do not bother to prove this remark, because the local issue presented by the choice of t_ℓ and σ will be overshadowed by a far more problematic global pair of choices later on. In any case, once a choice of t_ℓ has been fixed, the following identity holds for arbitrary elements g and i of $\mathrm{W}(\overline{K}/K)$ and I respectively:

$$t_\ell(gig^{-1}) = \omega(g)t_\ell(i). \tag{4.16}$$

This is proved by applying the usual Galois equivariance of the Kummer pairing to the extension $K_{\mathrm{unr}}(\varpi^{1/n})/K_{\mathrm{unr}}$ and then taking inverse limits. Note the formal resemblance of (4.16) to (4.4)!

Theorem 4.1. *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 3.4, we may think of ρ_λ as a map $\mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_d(\mathcal{O}_\lambda)$. Let Γ be the open pro-ℓ-subgroup of $\mathrm{GL}_d(\mathcal{O}_\lambda)$ consisting of matrices congruent to 1 mod ℓ^2, and put $I' = I \cap \rho_\lambda^{-1}(\Gamma)$. Then I' is an open subgroup of I and $\rho_\lambda|I'$ is a homomorphism of I' into a pro-ℓ-group. Choose $c \in \mathbb{Q}_\ell$ such that $ct_\ell|I'$ is a surjection of I' onto $\mathbb{Z}_\ell$. Applying (4.14) with $\varphi = \rho_\lambda|I'$ and $t = ct_\ell$, we see that $\rho_\lambda(i) = \gamma^{ct_\ell(i)}$ for some $\gamma \in \Gamma$ and all $i \in I'$. Let $\mathrm{M}_{d\times d}(\mathcal{O}_\lambda)$ be the set of $d \times d$ matrices with coefficients in $\mathcal{O}_\lambda$, and write

$\gamma = \exp(N)$ with $N \in \ell^2 \mathrm{M}_{d\times d}(\mathcal{O}_\lambda)$. Then $\rho_\lambda(i) = \exp(ct_\ell(i)N)$ for $i \in I'$, and it follows from (4.16) that for $g \in \mathrm{W}(\overline{K}/K)$ we have $\rho_\lambda(gig^{-1}) = \exp(c\omega(g)t_\ell(i)N)$. But if we simply conjugate the equation $\rho_\lambda(i) = \exp(ct_\ell(i)N)$ by $\rho_\lambda(g)$ then we get a second expression for $\rho_\lambda(gig^{-1})$, namely $\exp(ct_\ell(i)\rho_\lambda(g)N\rho_\lambda(g)^{-1})$. Applying the ℓ-adic logarithm to both expressions, we find 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 had a nonzero eigenvalue r then N would have infinitely many eigenvalues, namely the numbers rq^ν. Replacing N by cN we preserve the nilpotence of N and the relation $\rho(g)N\rho(g)^{-1} = \omega(g)N$ and we gain the simplified formula $\rho_\lambda(i) = \exp(t_\ell(i)N)$ for $i \in I'$. This equation determines N uniquely, because the exponential is a bijection from nilpotent matrices to unipotent matrices.

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 (4.16) gives

$$\rho(gg') = \exp((-t_\ell(i) - q^n t_\ell(h))N)\rho_\lambda(gg') \tag{4.17}$$

while

$$\rho(g)\rho(g') = \exp(-t_\ell(i)N)\rho_\lambda(g)\exp(-t_\ell(h)N)\rho_\lambda(g'). \tag{4.18}$$

The identity $\rho_\lambda(g)N\rho_\lambda(g)^{-1} = \omega(g)N$ shows that the right-hand sides of (4.17) and (4.18) 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. In addition, J is open in I, because it is the subgroup of I on which ρ_λ coincides with the map $i \mapsto \exp(t_\ell(i)N)$, and this subgroup is open by (a). 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 $l \geqslant 1$ such that σ^l acts trivially on I/J. Since ρ factors through $\mathrm{W}(\overline{K}/K)/J$, we deduce that $\rho(\sigma^l)$ centralizes $\rho(I)$. But $\rho(\sigma^l)$ certainly commutes with $\rho(\sigma)$, so $\rho(\sigma^l)$ centralizes the image of ρ.

Now let u be the unipotent Jordan component of $\rho(\sigma)$. Then u^l is the unipotent Jordan component of $\rho(\sigma^l)$. But the semisimple and unipotent components of an invertible matrix are polynomials in the matrix. Since $\rho(\sigma^l)$ centralizes the image of ρ it follows that u^l does too. Using the binomial series for $(1+x)^{1/l}$, we see that u is a polynomial in u^l, 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 $\rho^{\mathrm{u}}(g^l) = \rho^{\mathrm{u}}(g)^l$ and unipotent automorphisms have unique unipotent lth roots, it suffices to see that $\rho^{\mathrm{u}}(g^l) = u^{nl}$. But $\rho(g^l) = \rho(i')\rho(\sigma^{nl})$ for some $i' \in I$ and $\rho(\sigma^{nl}) = \rho^{\mathrm{ss}}(\sigma^{nl})u^{nl}$, so

$$\rho(g^l) = (\rho(i')\rho^{\mathrm{ss}}(\sigma^{nl}))\cdot u^{nl}. \tag{4.19}$$

We contend that (4.19) is the multiplicative Jordan decomposition of $\rho(g^l)$, whence $\rho^{\mathrm{u}}(g^l) = u^{nl}$, as desired. As u^{nl} is unipotent and commutes with $\rho(i')\rho^{\mathrm{ss}}(\sigma^{nl})$ it suffices to see that $\rho(i')\rho^{\mathrm{ss}}(\sigma^{nl})$ is semisimple. But $\rho(i')$ is semisimple because $\rho|I$ factors through the finite group I/J, and $\rho^{\mathrm{ss}}(\sigma^{nl})$ is semisimple and commutes with $\rho(i')$. Hence $\rho(i')\rho^{\mathrm{ss}}(\sigma^{nl})$ 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 $g, g' \in \mathrm{W}(\overline{K}/K)$, 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 $\mathrm{GL}_d(\mathbb{E}_\lambda)$ on $\mathrm{M}_{d\times d}(\mathbb{E}_\lambda)$ by Ad, so that

$$\mathrm{Ad}(x)(y) = xyx^{-1}$$

for $x \in \mathrm{GL}_d(\mathbb{E}_\lambda)$ and $y \in \mathrm{M}_{d\times d}(\mathbb{E}_\lambda)$. 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. □

2.2. Characteristic polynomials

Next we examine the effect of the maps $\rho_\lambda \mapsto \boldsymbol{\rho}$ and $\boldsymbol{\rho} \mapsto \boldsymbol{\rho}^{\mathrm{ss}}$ of Theorem 4.1 on the space of inertial invariants. Let V_λ denote the space of ρ_λ and V the space of $\boldsymbol{\rho}$. While V_λ and V are equal as abstract vector spaces, by using different notations we can distinguish between the subspaces V_λ^I and V^I, which need not be equal: one consists of vectors fixed by $\rho_\lambda(I)$, the other of vectors fixed by $\rho(I)$. We claim that the relation between them is

$$V_\lambda^I = V_N^I, \tag{4.20}$$

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

To verify (4.20), we return to the relation $\rho_\lambda(i) = \exp(t_\ell(i)N)\rho(i)$ for $i \in I$. The inclusion $V_N^I \subset V_\lambda^I$ is an immediate consequence. For the reverse inclusion, recall that $\rho_\lambda(j) = \exp(t_\ell(j)N)$ for all j in some open subgroup J of I. Any element of V_λ^I is in particular fixed by J and hence by $\exp(t_\ell(j)N)$ for $j \in J$. By writing $t_\ell(j)N$ as $-\sum_{\nu\geqslant 1}(1-x)^\nu/\nu$ with $x = \exp(t_\ell(j)N)$, we see that a vector fixed by $\exp(t_\ell(j)N)$ is in the kernel of N, whence $V_\lambda^I \subset V_N$. Now the relation $\rho(g)N = \omega(g)N\rho(g)$ for $g \in \mathrm{W}(\overline{K}/K)$ shows that V_N is stable under ρ, so the inclusion $V_\lambda^I \subset V_N$ and the relation $\rho_\lambda(i) = \exp(t_\ell(i)N)\rho(i)$ for $i \in I$ together imply that $\rho_\lambda(i) = \rho(i)$ on V_λ^I. Hence $V_\lambda^I \subset V_N^I$, and (4.20) follows.

Put $\Phi = \sigma^{-1}$. Then the definition of ρ in part (a) of Theorem 4.1 gives $\rho(\Phi) = \rho_\lambda(\Phi)$, whence in particular $\rho_\lambda(\Phi)|V_\lambda^I = \rho(\Phi)|V_N^I$ by (4.20). Since characteristic polynomials are insensitive to semisimplification, we obtain:

Proposition 4.2. $\det(1 - x\rho_\lambda(\Phi)|V_\lambda^I) = \det(1 - x\rho^{\mathrm{ss}}(\Phi)|V_N^I)$.

3. An open problem

Let K be a number field again and M a premotive over K. Fix a finite place v of K and write p for its residue characteristic. We would like to claim that M determines a complex representation $\boldsymbol{\rho}_{M,v}$ of $\mathrm{WD}(\overline{K}_v/K_v)$ up to isomorphism.

There is an obvious candidate for $\boldsymbol{\rho}_{M,v}$. Let $\{\rho_\lambda\} \in M$ be a fully compatible family and $\mathbb{E}$ its coefficient field, and choose a place λ of $\mathbb{E}$ of residue characteristic $\ell \neq p$. As usual, we identify $\mathrm{Gal}(\overline{K_v}/K_v)$ with the decomposition subgroup of $\mathrm{Gal}(\overline{K}/K)$ at a place of $\overline{K}$ above v, so it is meaningful to consider the restriction $\rho_{\lambda,v} = \rho_\lambda|\mathrm{Gal}(\overline{K_v}/K_v)$. This is a λ-adic representation of $\mathrm{Gal}(\overline{K_v}/K_v)$ to which we may apply Theorem 4.1. The result is a representation $\boldsymbol{\rho}_v^{\mathrm{ss}} = (\rho_v^{\mathrm{ss}}, N_v)$ 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

$$\boldsymbol{\rho}_{M,v} = ((\rho_v^{\mathrm{ss}})^\iota, (N_v)^\iota) \tag{4.21}$$

of $\mathrm{WD}(\overline{K_v}/K_v)$ over $\mathbb{C}$.

Problem 4. *Up to isomorphism, is $\boldsymbol{\rho}_{M,v}$ independent of the choice of λ and ι?*

If M comes from an Artin representation or a Hecke character of type $(1,0)$ then an affirmative answer follows tautologically from the definitions, and an affirmative answer is also known if M comes from an elliptic curve or more generally from an abelian variety, cf. [**23**], p. 571. Admittedly, an Artin representation for which we do not know the Artin conjecture cannot be offered as an example of a premotive according to our definition of the term, nor can an elliptic curve over an arbitrary number field. But the analytic conditions that we have imposed on a premotive could be omitted from the definition and Problem 4 would still make prefect sense. The real issue is that an affirmative answer to Problem 4 is unknown in general even if one assumes that M comes from a motive. It should be added, however, that if we write $\boldsymbol{\rho}_{M,v} = (\rho_{M,v}, N_{M,v})$ then it is only $N_{M,v}$ which is problematic. Indeed the theory of Grothendieck and Deligne does yield the following.

Theorem 4.2. *Up to isomorphism, $\rho_{M,v}$ is independent of the choice of λ and ι.*

Proof. Let $\boldsymbol{\rho}_v = (\rho_v, N_v)$ be the representation of $\mathrm{WD}(\overline{K_v}/K_v)$ resulting from $\rho_{\lambda,v}$ as in part (a) of Theorem 4.1, and let g denote an arbitrary element of $\mathrm{W}(\overline{K_v}/K_v)$, written as in the theorem. By Proposition 4.1 , there is a basis for the space of ρ_v relative to which the matrices of $\rho_v(g)$ and N_v are both upper triangular. Then $\exp(t_\ell(i)N_v)$ is upper triangular with all diagonal entries equal to 1, and as $\rho_{\lambda,v}(g) = \exp(t_\ell(i)N_v)\rho_v(g)$ we deduce that the characteristic polynomials of $\rho_{\lambda,v}(g)$ and $\rho_v(g)$ are equal. On the other hand, the characteristic polynomials of $\rho_v(g)$ and $\rho_v^{\mathrm{ss}}(g)$ are equal because $\rho_v^{\mathrm{ss}}(g)$ is the semisimple Jordan component of $\rho_v(g)$. By Condition C_8, the characteristic polynomial of $\rho_{\lambda,v}(g)$ has coefficients in $\mathbb{E}$ and is independent of λ, so the same is true for the characteristic polynomial of $\rho_v^{\mathrm{ss}}(g)$. Furthermore this characteristic polynomial is unchanged when ι is used to extend the field of scalars of $\rho_v^{\mathrm{ss}}(g)$ from $\mathbb{E}_\lambda$ to $\mathbb{C}$, because ι is the identity on $\mathbb{E}$. We conclude that the characteristic polynomial of $(\rho_v^{\mathrm{ss}})^\iota(g)$ is independent of the choice of λ and ι. In particular the trace of $(\rho_v^{\mathrm{ss}})^\iota$ is independent of the choice of λ and ι, and since $(\rho_v^{\mathrm{ss}})^\iota$ is semisimple we conclude that the isomorphism class of $(\rho_v^{\mathrm{ss}})^\iota$ is independent of the choices as well. $\square$

As stated, Problem 4 pertains only to the finite places of K, because it is only for finite v that we have presented a candidate for $\boldsymbol{\rho}_{M,v}$. However the Fontaine-Mazur conjectures provide a candidate for $\boldsymbol{\rho}_{M,v}$ when v is an infinite place as well, at least if $K = \mathbb{Q}$ ([**30**], p. 197, Conjecture 3a). The definition of $\boldsymbol{\rho}_{M,v}$ depends on the standing assumption in [**30**], namely potential semistability, and in this sense it does not mesh too well with the present framework. However if we simply impose potential semistability as an additional requirement on M then in principle we can take v in Problem 4 to be any place of K, finite or infinite. The choice of λ and ι remains very much an issue at the infinite places, because for us there is no distinguished prime p and of course no distinguished embedding of $\overline{\mathbb{Q}_p}$ into $\mathbb{C}$.

In the remainder of this lecture we define the local factors – the L-factor, the conductor, the root number – associated to a complex representation of the Weil-Deligne group of a finite extension of $\mathbb{Q}_p$ for $p \leqslant \infty$. If Problem 4 has an affirmative answer, then once we have made the local definitions we can put

$$L_\infty(s, M) = \prod_{v \mid \infty} L(s, \boldsymbol{\rho}_{M,v}), \tag{4.22}$$

$$W(M) = \prod_{v} W(\boldsymbol{\rho}_{M,v}), \tag{4.23}$$

$$\mathfrak{f}(M) = \prod_{v \nmid \infty} \mathfrak{p}_v^{a(\boldsymbol{\rho}_{M,v})}, \tag{4.24}$$

and

$$A(M) = D^{\mathrm{rk}(M)} \mathbf{N}\mathfrak{f}(M), \tag{4.25}$$

where D is the absolute value of the discriminant of K and $\mathrm{rk}(M)$ is the rank of M (recall that this is $\dim \rho_\lambda$ for $\{\rho_\lambda\} \in M$). Thus if we grant an affirmative answer to Problem 4 then $L_\infty(s, M)$, $A(M)$, and $W(M)$ will finally have an intrinsic definition, one that does not depend on the uniqueness of a conjectural functional equation (Proposition 3.2). For the sake of the overall coherence of the discussion we will also check that

$$L(s, M) = \prod_{v \nmid \infty} L(s, \boldsymbol{\rho}_{M,v}), \tag{4.26}$$

even though we already have the intrinsic definition (3.33) of $L(s, M)$. In fact by virtue of this intrinsic definition, verifying (4.26) will amount to checking that

$$B_{\mathfrak{p}}((\mathbf{N}\mathfrak{p})^{-s}) = L(s, \boldsymbol{\rho}_{M,v}), \tag{4.27}$$

where $\mathfrak{p}$ is an arbitrary prime ideal of K and $v = v_{\mathfrak{p}}$.

4. Local factors

Henceforth K is a finite extension of $\mathbb{Q}_p$ ($p \leqslant \infty$) and $\boldsymbol{\rho}$ a representation of $\mathrm{WD}(\overline{K}/K)$ over $\mathbb{C}$. We will define the local factors associated to $\boldsymbol{\rho}$.

4.1. L-factors

Suppose first that $p < \infty$, and write $\boldsymbol{\rho} = (\rho, N)$. Let V be the space of ρ and V_N the kernel of N, and put $V_N^I = V^I \cap V_N$ as before. Recall also that by virtue of (4.4), V_N^I is stable under ρ. We put

$$L(s, \boldsymbol{\rho}) = \det(1 - q^{-s}\rho(\Phi)|V_N^I)^{-1}, \tag{4.28}$$

where $\Phi \in \mathrm{W}(\overline{K}/K)$ is an inverse Frobenius element and q is the order of the residue class field of K. Since $V_N^I \subset V^I$ the definition of $L(s, \boldsymbol{\rho})$ is as usual independent of the choice of Φ. Furthermore, (4.27) is an immediate consequence of Proposition 4.2 given the definitions (3.30), (4.21), and (4.28).

Suppose next that $p = \infty$. Then there is no distinction between $\boldsymbol{\rho} = (\rho, 0)$ and ρ, and the definition of the L-factor $L(s, \boldsymbol{\rho}) = L(s, \rho)$ is a straightforward generalization of our earlier discussion of gamma factors for Artin L-functions. In fact the only new issue is that the L-factor of ρ is by definition the L-factor of the semisimplification of ρ. (Of course in the context of Artin representations, ρ is automatically semisimple.) If ρ is a semisimple representation of $\mathrm{W}(\overline{K}/K)$ then we define $L(s, \rho)$ by imposing the Artin formalism. In particular, additivity holds by fiat: in other words we declare that $L(s, \rho \oplus \rho') = L(s, \rho)L(s, \rho')$, whence it suffices to define $L(s, \rho)$ for ρ irreducible.

So suppose that ρ is irreducible. If ρ is one-dimensional then we use (4.13) to identify ρ with a character χ of $K^\times$, and we set $L(s, \rho) = L(s, \chi)$, thus defining $L(s, \rho)$ by (2.25) and (2.26). If $K = \mathbb{R}$ and ρ is two-dimensional then $\rho = \mathrm{ind}_{\overline{K}/K}\chi$ for some character χ of $\mathrm{W}(\overline{K}/\overline{K})$, and again we set $L(s, \rho) = L(s, \chi)$, as required by inductivity. Incidentally, the fact that inductivity holds even for reducible inductions follows from the duplication formula (1.9).

4.2. The exponent of the conductor

We return to the case $p < \infty$ and write $\boldsymbol{\rho} = (\rho, N)$ as before. The exponent $a(\boldsymbol{\rho})$ of the conductor $\pi^{a(\boldsymbol{\rho})}\mathcal{O}$ of $\boldsymbol{\rho}$ is a sum of two terms,

$$a(\boldsymbol{\rho}) = a(\rho) + b(\boldsymbol{\rho}), \tag{4.29}$$

and only the second term depends on N. In fact

$$b(\boldsymbol{\rho}) = \dim(V^I/V_N^I). \tag{4.30}$$

It follows in particular that if $N = 0$ then $b(\boldsymbol{\rho}) = 0$, so that (4.29) is consistent with our identification of ρ with $(\rho, 0)$. Turning to the first term, we declare first of all that $a(\rho)$ depends only on the semisimplification of ρ. We also impose additivity – in other words, we take the identity $a(\rho \oplus \rho') = a(\rho) + a(\rho')$ to be part of the definition of $a(*)$ – and so reduce the problem of defining $a(\rho)$ to the case where ρ is irreducible.

To handle this case we need the notion of a representation **of Galois type**. This term refers to any representation of $\mathrm{W}(\overline{K}/K)$ over $\mathbb{C}$ which 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 from (4.2) that a representation of Galois type is simply a representation of $\mathrm{Gal}(L/K)$ for some L. The following proposition is drawn from Deligne [**23**], p. 542. The proof (also drawn from [**23**]) recalls the first step in the proof of part (b) of Theorem 4.1.

Proposition 4.3. *Let ρ be a representation of* $\mathrm{W}(\overline{K}/K)$ *over* $\mathbb{C}$. *If ρ is irreducible then there exists $s_0 \in \mathbb{C}$ such that $\rho \otimes \omega^{s_0}$ 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 that the coset $\sigma^n J$ 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 if $s_0 = -s/n$ then $\rho \otimes \omega^{s_0}$ 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 the proposition for us is that if ρ is a representation of Galois type and hence a representation of $\mathrm{Gal}(L/K)$ for some finite Galois extension L of K then we have already seen a definition of $a(\rho)$ in the context of Artin representations: $a(\rho)$ is defined by (3.46). Hence given an arbitrary *irreducible* representation ρ of $\mathrm{W}(\overline{K}/K)$ we can put

$$a(\rho) = a(\rho \otimes \omega^{s_0}), \tag{4.31}$$

where the right-hand side is defined by (3.46) with s_0 chosen so that $\rho \otimes \omega^{s_0}$ is of Galois type. While such an s_0 is not unique (for it can be replaced by $s_0 + 2\pi i r/\log q$ with $r \in \mathbb{Q}$), an inspection of (3.46) shows that $a(\rho \otimes \omega^{s_0})$ depends only on $(\rho \otimes \omega^{s_0})|I$ and hence only on $\rho|I$. Thus Proposition 4.3 and (4.31) together assign a meaning to $a(\rho)$ for irreducible ρ and hence by semisimplification and additivity for all ρ.

4.3. Root numbers

To start with take $p < \infty$ and $\boldsymbol{\rho} = (\rho, N)$. Just as $a(\boldsymbol{\rho})$ is the sum of the two terms $a(\rho)$ and $b(\boldsymbol{\rho})$, with $a(\rho)$ independent of N, the root number $W(\boldsymbol{\rho})$ is similarly the product of two factors, the first of which is independent of N:

$$W(\boldsymbol{\rho}) = W(\rho)\Delta(\boldsymbol{\rho}). \tag{4.32}$$

Furthermore the definition of $\Delta(\boldsymbol{\rho})$, like the definition of $b(\boldsymbol{\rho})$, is straightforward: Writing V for the space of ρ and the same letter ρ for the quotient representation on V^I/V_N^I determined by ρ, we put

$$\delta(\boldsymbol{\rho}) = \det(-\rho(\Phi)|V^I/V_N^I) \tag{4.33}$$

and

$$\Delta(\boldsymbol{\rho}) = \frac{\delta(\boldsymbol{\rho})}{|\delta(\boldsymbol{\rho})|}. \tag{4.34}$$

Note that the identification of ρ with $(\rho, 0)$ is once again respected here, because if $N = 0$ then $\delta(\boldsymbol{\rho})$ is the determinant of a linear automorphism of the trivial vector space, whence $\Delta(\boldsymbol{\rho}) = \delta(\boldsymbol{\rho}) = 1$ and $W(\boldsymbol{\rho}) = W(\rho)$.

If $p = \infty$ then (4.32) is still valid provided we understand that $N = 0$. Thus $\Delta = 1$ and $W(\boldsymbol{\rho}) = W(\rho)$. Furthermore the definition of $W(\rho)$ is straightforward in the archimedean case, but the archimedean case will not be treated separately because it is included in the general case to be discussed now.

While the definition of $W(\rho)$ is indirect, the underlying strategy is simple: Define $W(\rho)$ by imposing a modified Artin formalism. This means first of all that $W(\rho)$ depends only on the semisimplification of ρ, and secondly that additivity holds – in other words that $W(\rho \oplus \rho') = W(\rho)W(\rho')$. We also impose compatibility in dimension one: If ρ is one-dimensional and we identify it with a character χ of $K^\times$ via (4.3) and (4.13), then $W(\rho) = W(\chi)$. So far this is just the standard Artin formalism. But as soon as we impose additivity and compatibility in dimension one there are simple counterexamples to inductivity. For instance take the case of the unramified quadratic extension L of a finite extension K of $\mathbb{Q}_p$, where $p < \infty$. Write $\mathrm{sign}_{L/K}$ for the nontrivial character of $\mathrm{Gal}(L/K)$. Then $\mathrm{ind}_{L/K} 1_L = 1_K \oplus \mathrm{sign}_{L/K}$, while (2.43) gives $W(1_L) = W(1_K) = 1$ and $W(\mathrm{sign}_{L/K}) = (-1)^d$ with d equal to the exponent of the different ideal of K. If the root number were to satisfy inductivity we would have $1 = (-1)^d$, a contradiction if d is odd (as it is for example if $K = \mathbb{Q}_p(\sqrt{p})$).

Thus inductivity must be modified. The modification is a weaker condition called **inductivity in dimension zero** (or "in degree zero"). Fix a finite extension K of $\mathbb{Q}_p$ with $p \leqslant \infty$, and consider the Grothendieck group $\mathrm{Groth}(\mathrm{W}(\overline{K}/K))$ of virtual representations of $\mathrm{W}(\overline{K}/K)$. If we want the root number to depend only on the semisimplification of its argument and to satisfy additivity then it becomes a function on $\mathrm{Groth}(\mathrm{W}(\overline{K}/K))$, so that $W(\rho)$ acquires a meaning even for virtual representations of $\mathrm{W}(\overline{K}/K)$. Now a virtual representation has a virtual dimension, and to impose inductivity in dimension zero is to demand that

$$W(\mathrm{ind}_{L/K}\rho) = W(\rho) \tag{4.35}$$

whenever L is a finite extension of K and ρ a virtual representation of $\mathrm{W}(\overline{K}/L)$ of dimension zero.

With this modification, the Artin formalism can be realized: By the theorem of Langlands and Deligne ([**23**], p. 535; see also Tate [**93**], [**94**]), there is a unique map $\rho \mapsto W(\rho)$ from virtual representations of $\mathrm{W}(\overline{K}/K)$ to complex numbers of absolute value 1 which satisfies additivity, compatibility in dimension one, and inductivity in dimension zero. The uniqueness of $\rho \mapsto W(\rho)$ is the easy part of the assertion, but it is worth verifying here, for the argument shows how $W(\rho)$ can be computed in practice.

What is needed for the verification is a "dimension-zero" variant of Brauer's theorem (cf. [**23**], p. 510, Proposition 1.5). Let us say that a virtual representation of a finite group G is **monomial of dimension zero** if it is induced by the difference of two one-dimensional representations of a subgroup of G. The dimension-zero version of Brauer's theorem states that in $\mathrm{Groth}(G)$ any virtual representation of G of dimension zero is an integral linear combination of monomial representations of dimension zero. Suppose now that ρ is an irreducible representation of $\mathrm{W}(\overline{K}/K)$ over $\mathbb{C}$. By Proposition 4.3 there exists $s_0 \in \mathbb{C}$ such that $\rho \otimes \omega^{s_0}$ factors through $\mathrm{Gal}(L/K)$ for some finite Galois extension L of K. Hence taking $G = \mathrm{Gal}(L/K)$ we can write

$$[\rho \otimes \omega^{s_0}] - (\dim\rho)[1_K] = \sum_{(M,\xi,\xi')} n_{M,\xi,\xi'} \mathrm{ind}_{M/K}([\xi] - [\xi']) \tag{4.36}$$

with integers $n_{M,\xi,\xi'}$, subfields M of L containing K, and one-dimensional characters ξ and ξ' of $\mathrm{Gal}(L/M)$. Tensoring both sides of (4.36) with $[\omega^{-s_0}]$, we obtain

$$[\rho] = (\dim\rho)[\omega^{-s_0}] + \sum_{(M,\xi,\xi')} n_{M,\xi,\xi'} \mathrm{ind}_{M/K}([\xi_0] - [\xi_0']) \tag{4.37}$$

in Groth(W($\overline{K}/K$)), where $\xi_0 = \xi\omega_M^{-s_0}$ and $\xi'_0 = \xi'\omega_M^{-s_0}$. Here we are using the fact that our ω is really ω_K and satisfies $\omega|\mathrm{W}(\overline{K}/M) = \omega_M$. The modified Artin formalism now implies that

$$W(\rho) = W(||*||^{-s_0})^{\dim\rho} \prod_{(M,\xi,\xi')} (W(\chi_{\xi_0})/W(\chi_{\xi'_0}))^{n_{M,\xi,\xi'}}, \tag{4.38}$$

where χ_{ξ_0} and $\chi_{\xi'_0}$ are the characters of $M^\times$ corresponding to ξ_0 and ξ'_0 respectively under (4.3) and (4.13). It follows from (4.38) that the modified Artin formalism does indeed determine $W(\rho)$ uniquely for irreducible ρ, and consequently, by semisimplification and additivity, for all ρ.

4.4. Epsilon factors

Just as in the one-dimensional case, the local root number is subsumed in a broader concept, the epsilon factor. Given a local field K, a complex representation $\boldsymbol{\rho}$ of WD($\overline{K}/K$), an additive character ψ of K, and a Haar measure dx on K, one puts

$$\varepsilon(\boldsymbol{\rho}, \psi, dx) = \varepsilon(\rho, \psi, dx)\delta(\boldsymbol{\rho}), \tag{4.39}$$

where $\delta(\boldsymbol{\rho})$ is as in (4.33) – note that the definition is indeed independent of ψ and dx – and $\varepsilon(\rho, \psi, dx)$ is defined by the theorem of Langlands and Deligne. In the context of epsilon factors their theorem states that the modified Artin formalism can be imposed on $\varepsilon(\rho, \psi, dx)$ and then defines $\varepsilon(\rho, \psi, dx)$ uniquely. Inductivity in dimension zero now takes account of the additive character: the requirement is that

$$\varepsilon(\mathrm{ind}_{L/K}\rho, \psi \circ \mathrm{tr}_{L/K}, d_L x) = \varepsilon(\rho, \psi, d_K x) \tag{4.40}$$

for every finite extension L of K, virtual representation ρ of W($\overline{K}/L$) of dimension zero, additive character ψ of K, and Haar measures $d_L x$ and $d_K x$ on L and K respectively. Additivity means as usual that

$$\varepsilon(\rho \oplus \rho', \psi, dx) = \varepsilon(\rho, \psi, dx)\varepsilon(\rho', \psi, dx),$$

and compatibility in dimension one means that if ρ is one-dimensional then

$$\varepsilon(\rho, \psi, dx) = \varepsilon(\chi, \psi, dx),$$

where χ is the character of $K^\times$ corresponding to ρ under (4.3) and (4.13).

Although a local functional equation is lacking in dimension > 1, one can still introduce a complex parameter s by putting

$$\varepsilon(s, \boldsymbol{\rho}, \psi, dx) = \varepsilon(\boldsymbol{\rho} \otimes \omega^s, \psi, dx) \tag{4.41}$$

and thus generalizing (2.73). One can also define $W(\boldsymbol{\rho}, \psi)$ by a straightforward generalization of (2.72):

$$W(\boldsymbol{\rho}, \psi) = \frac{\varepsilon(\boldsymbol{\rho}, \psi, dx)}{|\varepsilon(\boldsymbol{\rho}, \psi, dx)|}. \tag{4.42}$$

If K has characteristic zero then we recover $W(\boldsymbol{\rho})$ by taking $\psi = \psi^{\mathrm{can}}$. Indeed if L is a finite extension of K and ψ_L^{can} and ψ_K^{can} denote the respective canonical additive characters then $\psi_L^{\mathrm{can}} = \psi_K^{\mathrm{can}} \circ \mathrm{tr}_{L/K}$, so (4.40) and (4.42) do give (4.35). Thus the theorem of Langlands and Deligne does imply that $W(\rho)$ can be defined by imposing the modified Artin formalism.

5. Normalizations of the root number in the literature

We conclude this lecture with a brief but important caveat: In (2.72), (4.32), and (4.42) we have normalized the local and hence also the global root number to have absolute value 1, but this is far from being a standard convention. In fact what is more commonly found in the literature (see for example [**93**], p. 105) is the normalization

$$W(\rho,\psi)=\epsilon(1/2,\rho,\psi,dx_\psi), \tag{4.43}$$

which does not always give $W(\rho,\psi)$ absolute value 1. Suppose for instance that K is nonarchimedean, with residue class field of order q. Take ρ to be one-dimensional and view it as a character χ of $K^\times$ via (4.3). Applying (2.89) and (2.90), we see that if the root number is defined by (4.43) then $|W(\chi,\psi)|=q^{(a(\chi)+n(\psi))c}$, where c is as in (2.83). Hence $|W(\chi,\psi)|\neq 1$ unless χ is unitary or $a(\chi)+n(\psi)=0$.

On the other hand, while our convention that root numbers have absolute value 1 may not be widely supported in the literature, it seems to be standard in the mathematical vernacular. For example, have you ever heard anybody say that the root number of the elliptic curve $X_0(11)$ is $+\sqrt{11}$?

6. Exercises

Exercise 4.1. 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 $\overline{K}$.

Exercise 4.2. Let E be an elliptic curve over a finite extension K of $\mathbb{Q}_p$, and let $\rho_{E,\ell}$ be the representation of $\mathrm{Gal}(\overline{K}/K)$ on $V_\ell(E)$ for some prime $\ell\neq p$. Let $\boldsymbol{\rho}=(\rho,N)$ be the representation of $\mathrm{WD}(\overline{K}/K)$ obtained from $\rho_{E,\ell}^\vee$ by applying part (a) of Theorem 4.1. Show that if E has (i) good reduction then ρ is unramified and $N=0$, (ii) bad but potentially good reduction then ρ is ramified but $N=0$, and (iii) potentially multiplicative reduction then $N\neq 0$ and $\rho\cong\chi\oplus\chi\omega$, where χ is the unique quadratic or trivial character of $\mathrm{W}(\overline{K}/K)$ such that the twist of E by χ is a Tate curve over K. Furthermore, show that $W(\boldsymbol{\rho})=1$ in case (i) and that

$$W(\boldsymbol{\rho})=\begin{cases}-1 & \text{if } \chi=1\\ 1 & \text{if } \chi \text{ is the unique unramified quadratic character of } \mathrm{W}(\overline{K}/K)\\ \chi(-1) & \text{if } \chi \text{ is ramified}\end{cases}$$

in case (iii).

Exercise 4.3. 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. Put $W(E)=W(M)$, where M is the isomorphism class of $\{\rho_{E,\ell}^\vee\}$. Using Exercise 4.2, derive the classic formula $W(E)=(-1)^{r_1+r_2+s}$. (Essential information: The representation ρ_v of $\mathrm{W}(\overline{K}_v/K_v)$ associated to E at an infinite place v is as follows. Let $\chi:\mathbb{C}^\times\to\mathbb{C}^\times$ be the character $z\mapsto z^{-1}$. If v is complex and we identify $\mathrm{W}(\overline{K}_v/K_v)$ with $\mathbb{C}^\times$ then $\rho_v=\chi\oplus\overline{\chi}$. If v is real and we identify the subgroup $\mathrm{W}(\overline{K}_v/\overline{K}_v)$ of $\mathrm{W}(\overline{K}_v/K_v)$ with $\mathbb{C}^\times$ then $\rho_v=\mathrm{ind}_{\overline{K}_v/K_v}\chi$.)

Exercise 4.4. 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 if χ is as in (2.50) then $L(s,\chi)$ is not motivic – let alone the L-functions of arbitrary automorphic forms. Nonetheless, at the *local* level, representations of the Weil-Deligne group still serve as parameters for local components of automorphic representations. To illustrate this point, let f be a Maass form for $\mathrm{SL}(2,\mathbb{Z})$. Then the representation of $\mathrm{W}(\mathbb{C}/\mathbb{R})$ 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. (Hint: Given that f is a Maass form for $\mathrm{SL}(2,\mathbb{Z})$ rather than for one of its congruence subgroups, what can you infer about the conductor of the representation of $\mathrm{WD}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ associated to f at primes $p < \infty$?)

Exercise 4.5. (*Reading.*) Let G be a finite group and ρ a representation of G. There are theorems of Snaith [**89**] 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?

Exercise 4.6. Let $\boldsymbol{\rho}^{\mathrm{ss}} = (\rho^{\mathrm{ss}}, N)$ be as in part (b) of Theorem 4.1, and let V be the space of $\boldsymbol{\rho}^{\mathrm{ss}}$.

(a) Show that there is a unique invariant subspace W of V such that $V = V^I \oplus W$. Here "invariant" means "stable under ρ^{ss}."

(b) Let N^* be the nilpotent endomorphism of V which coincides with N on V^I and with 0 on W. Show that the pair $\boldsymbol{\rho}^{\mathrm{ss}*} = (\rho^{\mathrm{ss}}, N^*)$ is a representation of $\mathrm{WD}(\overline{K_v}/K_v)$ and that $L(s,\boldsymbol{\rho}^{\mathrm{ss}*}) = L(s,\boldsymbol{\rho}^{\mathrm{ss}})$, $a(\boldsymbol{\rho}^{\mathrm{ss}*}) = a(\boldsymbol{\rho}^{ss})$, and $W(\boldsymbol{\rho}^{\mathrm{ss}*}) = W(\boldsymbol{\rho}^{ss})$.

Exercise 4.7. With notation as in (4.21), put

$$\boldsymbol{\rho}^*_{M,v} = ((\rho_v^{\mathrm{ss}})^\iota, (N_v^*)^\iota), \tag{4.44}$$

where N_v^* is defined as in Exercise 4.6. (Note that there is an implicit choice of λ in (4.44) as well as of ι.) Assume that a condition stronger than (3.37) holds, namely that for every prime ideal $\mathfrak{p}$ in the exceptional set S of M, for every pair of reciprocal roots α and α' of $B_{\mathfrak{p}}(x)$, and for every pair of field automorphisms τ and τ' of $\mathbb{C}$, we have

$$|\tau(\alpha)| = |\tau'(\alpha')| \leqslant (\mathbf{N}\mathfrak{p})^{w/2}. \tag{4.45}$$

Prove that the isomorphism class of $\boldsymbol{\rho}^*_{M,v}$ is independent of the choice of λ and ι.

Exercise 4.8. The preceding two exercises may appear to be a partial solution to Problem 4, or at least a successful circumvention of it: If we simply replace N by N^* then the local L-factor, conductor, and root number are unaffected (Exercise 4.6) but the isomorphism class of $\boldsymbol{\rho}^*_{M,v}$ is now independent of all choices provided (4.45) holds (Exercise 4.7). The purpose of the present exercise is to show that this "solution" to Problem 4 is completely unsatisfactory.

(a) Give an example showing that (4.45) need not be satisfied even in the simple case of the motive associated to H^1 of the product of two elliptic curves.

(b) Give an example of representations $\boldsymbol{\rho} = (\rho, N)$ and $\boldsymbol{\rho}' = (\rho', N')$ for which $(N \otimes 1' + 1 \otimes N')^* \neq N^* \otimes 1' + 1 \otimes N'^*$, in contrast to (4.6).

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 $L(s,M)$ has the form $\Lambda(s,M) = W(M)\Lambda(k-s,M)$ 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 [**8**], 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 M, or for the associated L-function $L(s,M)$, if (5.1) is satisfied.

We have already encountered an infinite family of self-dual premotives in which the minimalist dichotomy holds for every member: the premotives $M(\chi)$ associated by (3.43) to the "canonical" characters χ. Indeed we have $L(s,M(\chi)) = L(s,\chi)$ and $W(M(\chi)) = W(\chi)$, so that (5.1) holds with $M = M(\chi)$ by Theorem 1.3. On the other hand, as a universal statement about L-functions of essentially self-dual premotives, (5.1) is simply false. In the case of elliptic curves this point is perhaps so familiar as to require no comment, but for the record, if one takes the base field to be $\mathbb{Q}$ and orders elliptic curves by their conductor then the first counterexample to (5.1) is the curve 389A1 in Cremona's tables ([**22**], p. 306). Of course the fact that one can be so precise depends on the confluence of several breakthroughs of the past quarter-century: first of all the modularity of elliptic curves over $\mathbb{Q}$ proved by Wiles [**100**], Taylor and Wiles [**96**], and Breuil, Conrad, Diamond, and Taylor [**11**], and secondly the theorems of Kolyvagin [**53**] (supplemented by Bump-Friedberg-Hoffstein [**14**] or Murty-Murty [**70**]) and Gross-Zagier [**39**], which together imply 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 $\leqslant 1$. For curves of conductor $\leqslant 999$ an inspection of Cremona's tables ([**22**], pp. 293 – 340) reveals that the converse also holds, and consequently the first curve in the tables of rank > 1 – namely the curve 389A1, which has rank 2 – it is also the first elliptic curve over $\mathbb{Q}$ for which the minimalist dichotomy fails. Using results like those in [**79**] one can produce as many other counterexamples as one likes.

Nonetheless, we can ask as in [**8**] 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: for example the absolute value of the minimal discriminant $\Delta(E)$, the Arakelov height of 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 [**13**]) and in the case $\nu(E) = N(E)$ (Watkins [**99**]), although the constant c may depend on ν. Next consider Conjecture 3.4 on p. 244 of [**8**] (based on the heuristics of Watkins [**99**]), 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 [**8**] is on the first line of (5.1), so that the roles of $\mathcal{E}$ and $\mathcal{D}$ are actually played by the set $\mathcal{E}^+$ of isomorphism classes with $W(E) = 1$ and the subset $\mathcal{D}^+$ of isomorphism classes 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 [**8**] 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 [**13**] with elliptic curves of prime conductor $< 10^8$, the calculations of Stein and Watkins [**91**] 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} can be regarded as 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 [**34**] for quadratic twists of a fixed elliptic curve, the average rank conjecture is here understood to apply to all isomorphism classes of elliptic curves over $\mathbb{Q}$ simultaneously. It asserts that if ν is any of the counting functions $\mathcal{E} \to \mathbb{Z}_{\geqslant 0}$ mentioned above then 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. In principle the choice of ν favored in the literature is the coarse height (5.2), but even when ν is so chosen, the "average rank" r that one is likely to encounter in research papers 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 [**12**]), $r \leqslant 2$ (Heath-Brown [**40**]), $r \leqslant 25/14$ (Young [**103**], cf. also [**104**]), and $r \leqslant 27/14$ (Baier and Zhao [**5**]). The two more recent works draw inspiration from random matrix theory (cf. Iwaniec, Luo, and Sarnak [**45**]), 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 [**5**]. See also Exercise 5.4. 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 (see Exercise 5.1) that an estimate of the form

$$\sum_{N(E)\leqslant x} \mathrm{ord}_{s=1} L(s,E) = \frac{1}{2}\vartheta_{\mathcal{E}}(x) + O(x^{\gamma'}) \tag{5.7}$$

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 the assertion that $r_N(\mathcal{E}) = 1/2$ in (5.5), while (5.8) is weaker than (5.4). But if we grant (5.3) then (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 its center of symmetry is the minimum compatible with its functional equation." This notion may simply be wrong, but without a precise formulation there is nothing to refute.

Fix a number field K and an integer $w \geqslant 0$, and put $k = w+1$, so that if M is a premotive of weight w over K then the functional equation of $L(s,M)$ is $\Lambda(s,M) = W(M)\Lambda(k-s,\overline{M})$. Since we are not restricting ourselves to essentially self-dual premotives, it is not necessarily the case that $W(M) = \pm 1$. Hence the dichotomy (5.1) should now be replaced by

$$\mathrm{ord}_{s=k/2} L(s,M) = \begin{cases} 0 & \text{if } M \ncong \overline{M}, \\ 0 & \text{if } M \cong \overline{M} \text{ and } W(M) = 1, \\ 1 & \text{if } M \cong \overline{M} \text{ and } W(M) = -1. \end{cases} \tag{5.9}$$

Of course an equivalent but more succinct formulation would be

$$\mathrm{ord}_{s=k/2} L(s,M) = \begin{cases} 1 & \text{if } M \cong \overline{M} \text{ and } W(M) = -1, \\ 0 & \text{otherwise,} \end{cases} \tag{5.10}$$

but perhaps (5.9) is more illuminating than (5.10). We shall refer to (5.9) as the **minimalist trichotomy**.

Now fix an integer $n \geqslant 1$ and let $\mathcal{S}_{K,w,n}$ be the set of premotives over K of weight w and rank n. Let $\mathcal{T}_{K,w,n} \subset \mathcal{S}_{K,w,n}$ be the subset of elements satisfying the minimalist trichotomy, and put $\mathcal{S} = \mathcal{S}_{K,w,n}$ and $\mathcal{T} = \mathcal{T}_{K,w,n}$ for simplicity. We also take $\nu(M) = \mathbf{N}\mathfrak{f}(M)$ and omit the subscript ν on $\vartheta_{\mathcal{S},\nu}$ and $\vartheta_{\mathcal{T},\nu}$. A naïve attempt at a **minimalist conjecture for premotives** would assert that

$$\lim_{x\to\infty} \vartheta_{\mathcal{T}}(x)/\vartheta_{\mathcal{S}}(x) = 1. \tag{5.11}$$

This blunt formulation implies in particular that factorizations like (1.33) and (1.34) are relatively rare: the resulting central zeros of high multiplicity occur with density zero. Conceivably this is a reason to reject (5.11). But a more fundamental problem is that we do not know that ν is a counting function on $\mathcal{S}_{K,w,n}$. In other words, to formulate the minimalist conjecture as in (5.11) we need:

Hypothesis 1. *Given $x > 0$, there are only finitely many premotives M over K of weight w and rank n such that $\mathbf{N}\mathfrak{f}(M) \leqslant x$.*

It might be possible to reduce this statement to the following assertion about Galois representations over finite fields (cf. [**67**]), which however is also unknown:

Hypothesis 2. *Fix a prime number ℓ. If $x > 0$ is given, then there are only finitely many isomorphism classes of semisimple representations $\rho : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_n(\overline{\mathbb{F}}_\ell)$ with $\mathbf{N}\mathfrak{f}(\rho) \leqslant x$. Here $\mathfrak{f}(\rho)$ is defined exactly as in* (3.45)*, except that the product runs only over the prime ideals of K which do not divide ℓ.*

The evidence in favor of these hypotheses includes the following points:

- Hypothesis 2 is known to hold if the image of ρ is solvable (Moon and Taguchi [**68**], p. 2530, Theorem 2), and for Hypothesis 2 to hold in general it suffices that it hold when the image of ρ is a finite simple group of Lie type in characteristic ℓ ([**68**], p. 2531, Proposition 3).
- The analogue of Hypothesis 2 over $\mathbb{C}$ – in other words, the statement that there are only finitely many isomorphism classes of n-dimensional Artin representations of K with conductor below a given bound – was proved by Ralph Greenberg (unpublished) and by Anderson, Blasius, Coleman, and Zettler [**1**]. Thus Hypothesis 1 holds for $w = 0$.
- Hypothesis 2 would follow from a suitable generalization of Serre's conjecture [**85**], as in Ash, Doud, and Pollack [**4**].

Nonetheless, if we want to formulate the minimalist conjecture without relying on unproven hypotheses then a slight modification is needed.

With K, w, and n as before, fix a number field $\mathbb{E}$ and let $\mathcal{S}_{K,\mathbb{E},w,n} \subset \mathcal{S}_{K,w,n}$ be the subset of elements which admit $\mathbb{E}$ as coefficient field. Let $\mathcal{T}_{K,\mathbb{E},w,n} \subset \mathcal{S}_{K,\mathbb{E},w,n}$ be the subset of elements satisfying the minimalist trichotomy. If we take the sets $\mathcal{S}$ and $\mathcal{T}$ in (5.11) to be $\mathcal{S}_{K,\mathbb{E},w,n}$ and $\mathcal{T}_{K,\mathbb{E},w,n}$ rather than $\mathcal{S}_{K,w,n}$ and $\mathcal{T}_{K,w,n}$ then we obtain a variant of the minimalist conjecture which is meaningful unconditionally:

Proposition 5.1. *The map $M \mapsto \mathbf{N}\mathfrak{f}(M)$ is a counting function on $\mathcal{S}_{K,\mathbb{E},w,n}$.*

To prove Proposition 5.1 we use the following result, which restates a well-known lemma of Faltings ([**29**], pp. 362 – 363, or see [**44**], p. 285). The lemma was embedded in the proof of Satz 5 of [**29**] and used there only in the case $\mathbb{E}_\lambda = \mathbb{Q}_\ell$, but the argument works for any finite extension of $\mathbb{Q}_\ell$.

Proposition 5.2. *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 semisimple representation of $\mathrm{Gal}(\overline{K}/K)$ over $\mathbb{E}_\lambda$ which is unramified outside S then ρ_λ is determined up to isomorphism by the $|T|$ values $\mathrm{tr}\,\rho_\lambda(\Phi_\mathfrak{p})$ for $\mathfrak{p} \in T$, where $\Phi_\mathfrak{p}$ denotes an inverse Frobenius element at $\mathfrak{p}$.*

Given an integer $n \geqslant 2$, let $p_{\max}(n)$ be the largest prime number dividing n. We also put $p_{\max}(1) = 1$, so that $p_{\max}(n)$ is defined for every positive integer n. Since $p_{\max}(n) \leqslant n$ for every positive integer n, Proposition 5.1 is an immediate corollary of the following statement:

Proposition 5.3. *The map $M \mapsto p_{\max}(\mathbf{N}\mathfrak{f}(M))$ 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 $x > \ell_0$ be given. Let S be the set of prime ideals of K which lie over a rational prime $\leqslant x$. We apply Proposition 5.2 with ℓ and λ replaced by ℓ_0 and λ_0. Given $M \in \mathcal{S}_{K,\mathbb{E},w,n}$, with $p_{\max}(\mathbf{N}\mathfrak{f}(M)) \leqslant x$, choose $\{\rho_\lambda\} \in M$ with coefficient field $\mathbb{E}$; then M is determined by the isomorphism class of ρ_{λ_0} (Proposition 3.1), and ρ_{λ_0} is unramified outside S. Thus it suffices to see that there are only finitely many possibilities for the numbers $\operatorname{tr}\rho_{\lambda_0}(\Phi_\mathfrak{p})$ with $\mathfrak{p} \in T$. Now $\operatorname{tr}\rho_{\lambda_0}(\Phi_\mathfrak{p})$ is the sum of the reciprocal roots of $B_\mathfrak{p}(x)$ and is therefore an element of $\mathcal{O}_\mathbb{E}$ having absolute value $\leqslant n(\mathbf{N}\mathfrak{p})^{w/2}$ in every archimedean embedding of $\mathbb{E}$. But $\mathcal{O}_E$ has only finitely many such elements. □

3. Elliptic curves revisited

A reasonable expectation of any "minimalist conjecture for premotives" is that it should imply the minimalist conjecture for elliptic curves over $\mathbb{Q}$. However the latter conjecture will need to be reformulated if we are to make a connection. The problem 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. Isomorphism classes are the right objects to consider if ν is taken to be $|\Delta|$, but now that we have settled on $\nu = N$ it is natural to take the domain of ν to be the set of isogeny classes. In fact by the isogeny theorem [**29**] we may identify the isogeny class of an elliptic curve E over $\mathbb{Q}$ with the premotive determined by the fully compatible family $\{\rho^\vee_{E,\ell}\}$. Writing $\mathcal{I}$ for the set of all such premotives, we will henceforth take the minimalist conjecture for elliptic curves over $\mathbb{Q}$ to be the assertion that

$$\lim_{x\to\infty} \vartheta_\mathcal{J}(x)/\vartheta_\mathcal{I}(x) = 1, \tag{5.12}$$

where $\mathcal{J} \subset \mathcal{I}$ is the subset of elements satisfying the minimalist dichotomy.

It follows from the definitions that $\mathcal{I} \subset \mathcal{S}_{K,\mathbb{E},w,n}$ with $K = \mathbb{E} = \mathbb{Q}$, $w = 1$, and $n = 2$, and the question at hand is whether the preceding inclusion is actually an equality: if so, then (5.12) is simply (5.11) with $\mathcal{S} = \mathcal{S}_{\mathbb{Q},\mathbb{Q},1,2}$ and $\mathcal{T} = \mathcal{T}_{\mathbb{Q},\mathbb{Q},1,2}$. However the desired equality $\mathcal{I} = \mathcal{S}_{\mathbb{Q},\mathbb{Q},1,2}$ is at present unknown. In fact even a slightly weaker question posed by Lang and Trotter ([**56**], pp. 5 and 19) more than thirty years ago remains open. On the positive side, the Fontaine-Mazur conjecture [**30**] combined with a certain "ordinariness conjecture" (about which more in a moment) does imply that $\mathcal{I} = \mathcal{S}_{\mathbb{Q},\mathbb{Q},1,2}$. An implication in this spirit but oriented more toward the Lang-Trotter question is proved in [**77**], and for the sake of completeness we shall now give a proof of the implication as stated here. The reader is cautioned that the arguments involved – mostly variants of the arguments in [**77**], which are elementary, but also some arguments based on modular forms – temporarily lead us outside the prerequisites for the lectures. This deviation is inevitable, because the Fontaine-Mazur conjecture itself lies outside our self-imposed perimeter. Hence we simply refer the reader to pp. 190 – 191 of [**30**] for the precise statement to be used here. Similarly, we refer to pp. 97–98 of Greenberg [**37**] for the notion of an **ordinary** prime relative to a strictly compatible family $\{\rho_\ell\}$ of ℓ-adic representations of $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. One feature of Greenberg's definition is that the ordinariness of p is a condition on ρ_p only (and in fact only on the restriction of ρ_p to a decomposition subgroup at p), not on ρ_ℓ for $\ell \neq p$. On the other hand, there is a second notion of ordinariness in the literature which is a condition on ρ_ℓ precisely for $\ell \neq p$. This second notion, like the first, can be elaborated in great generality, but we prefer to present it only for the type of strictly compatible family that is relevant here. Thus we take the dimension of ρ_ℓ to be two, and if $p \notin S$ (the exceptional set of the family) then we assume that $B_p(x)$ has the form $B_p(x) = 1 - a(p)x \pm px^2$ with $a(p) \in \mathbb{Z}$. In this setting we will say that p is **classically ordinary** if $p \nmid a(p)$. The **ordinariness conjecture** mentioned above is the first of the two assumptions in the following proposition:

Proposition 5.4. *Assume that classically ordinary primes are ordinary and that the Fontaine-Mazur conjecture holds. Then* $\mathcal{I} = \mathcal{S}_{\mathbb{Q},\mathbb{Q},1,2}$.

PROOF. Given a premotive $M \in S_{\mathbb{Q},\mathbb{Q},1,2}$ and a fully compatible family $\{\rho_\ell\}$ in M with coefficient field $\mathbb{Q}$, we must show that there is an elliptic curve E over $\mathbb{Q}$ such that $\{\rho_\ell\} \cong \{\rho^\vee_{E,\ell}\}$.

Let S be the exceptional set of M and let p denote an arbitrary prime not in S. The coefficients of $B_p(x)$ lie in $\mathbb{Z}$ by assumption, and the reciprocal roots of $B_p(x) = 0$ have complex absolute value $\sqrt{p}$ by (3.36). Consequently we have:

(i) $B_p(x) = 1 - a(p)x \pm px^2$ with $a(p) \in \mathbb{Z}$.
(ii) $|a(p)| < 2\sqrt{p}$.

If for all $p \notin S$ the sign $\pm$ in (i) is the plus sign then the desired conclusion follows from Theorem 1 of [**77**]. Hence it suffices to see that the occurrence of a minus sign in (i) leads to a contradiction.

Let ℓ and p be prime numbers with $p \notin S \cup \{\ell\}$, and let $\Phi_p \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be an inverse Frobenius element at p. Since $\det \rho_\ell(\Phi_p) = \pm p$ in (i) and $\omega_\ell^{-1}(\Phi_p) = p$, the formula $\eta = (\det \rho_\ell)/\omega_\ell^{-1}$ defines a character $\eta : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \{\pm 1\}$ independent of ℓ. Under the assumption that η is nontrivial the equation $\det \rho_\ell = \eta\omega_\ell^{-1}$ will lead to a contradiction.

View η as a primitive quadratic Dirichlet character, and write P for the set of prime numbers $p \notin S$ such that $\eta(p) = -1$. We claim that if $p \in P$ then $a(p) = 0$. To see this, write $1 - a(p)x - px^2 = (1 - \alpha x)(1 - \alpha' x)$ with $\alpha, \alpha' \in \mathbb{C}$. By (3.36) we can write $\alpha = e^{it}\sqrt{p}$ with $t \in \mathbb{R}$, and then $\alpha' = -e^{-it}\sqrt{p}$. Hence $a(p) = 2i(\sin t)\sqrt{p} \in i\mathbb{R}$. But $a(p) \in \mathbb{Z}$ by assumption, so $a(p) = 0$, as claimed.

Let $\mathcal{L}$ be the set of prime numbers ℓ such that there exist primes $p, q \in P$ with $p, q \neq \ell$ and

$$\left(\frac{p}{\ell}\right) = -\left(\frac{q}{\ell}\right). \tag{5.13}$$

We claim that $\mathcal{L}$ is a set of density 1. It suffices to see that the complement $\mathcal{M}$ of $\mathcal{L}$ has density 0. Now $\mathcal{M} = \mathcal{M}^+ \cup \mathcal{M}^-$, where $\mathcal{M}^\pm$ consists of the prime numbers ℓ such that

$$\left(\frac{p}{\ell}\right) = \pm 1 \tag{5.14}$$

for all $p \in P$ with $p \neq \ell$. But P is an infinite set (in fact a set of density 1/2), so it follows from the Chebotarev density theorem – or simply from Dirichlet's theorem – that $\mathcal{M}^+$ and $\mathcal{M}^-$ are sets of density 0. A small technical point here: In case the infinite set of conditions $\ell \neq p$ $(p \in P)$ appears to be a barrier to the application of the Chebotarev or Dirichlet theorems, choose an infinite subset P_0 of P of density 0, and let $\mathcal{M}_0^\pm$ be the set of primes $\ell \notin P_0$ such that (5.14) holds for all $p \in P_0$. If n is any positive integer and Q is any subset of P_0 of cardinality n then $\mathcal{M}_0^\pm$ is a subset of the set of primes $\ell \notin Q$ such that (5.14) holds for all $p \in Q$. But the latter set has density 2^{-n} and n is arbitrary, so we deduce that $\mathcal{M}_0^\pm$ has density 0.

As $\mathcal{M}^{\pm} \subset \mathcal{M}_0^{\pm} \cup \mathcal{P}_0$ and $\mathcal{M}_0^{\pm}$ and $\mathcal{P}_0$ are both sets of density 0, we do conclude that $\mathcal{M}^{\pm}$ has density 0 as well.

Now choose any odd prime ℓ_0 and view ρ_{ℓ_0} as a representation into $\mathrm{GL}_2(\mathbb{Z}_{\ell_0})$ (cf. Exercise 3.4). Let $\overline{\rho}_{\ell_0}$ denote the representation into $\mathrm{GL}_2(\mathbb{F}_{\ell_0})$ obtained from ρ_{ℓ_0} by reduction modulo ℓ_0. We consider the set Ξ of prime numbers $p \notin S \cup \{\ell_0\}$ such that $\overline{\rho}_{\ell_0}(\Phi_p) = 1$, the identity matrix in $\mathrm{GL}_2(\mathbb{F}_{\ell_0})$. By Chebotarev, Ξ has positive density, whence the same is true of $\Xi \cap \mathcal{L}$ because $\mathcal{L}$ has density one. Thus we can choose a prime $r \in \Xi \cap \mathcal{L}$ with $r \geqslant 5$. We claim that r is ordinary and that ρ_r is absolutely irreducible.

To see that ρ_r is ordinary, observe first of all that by construction, $\overline{\rho}_{\ell_0}(\Phi_r) = 1$, whence $\operatorname{tr}\rho_{\ell_0}(\Phi_r) \equiv 2 \bmod \ell_0$. But $\operatorname{tr}\rho_{\ell_0}(\Phi_r) = a(r)$ and ℓ_0 is odd, so we deduce that $a(r) \not\equiv 0 \bmod \ell_0$ and hence in particular that $a(r) \neq 0$. As $|a(r)| < 2\sqrt{r}$ it follows that $r \nmid a(r)$: in other words, r is classically ordinary and hence, under our hypotheses, ordinary.

To see that ρ_r is absolutely irreducible, we use the fact that $r \in \mathcal{L}$. Choose primes $p, q \in P$ with $p, q \neq r$ such that (5.13) holds with ℓ replaced by r. Then one of p and q is a square in $\mathbb{F}_r$ and the other is not. Also $a(p) = a(q) = 0$ because $p, q \in P$. Let us once again view ρ_r as a representation into $\mathrm{GL}_2(\mathbb{Z}_r)$, writing $\overline{\rho}_r$ for its reduction modulo r. Since the characteristic polynomials of $\rho_r(\Phi_p)$ and $\rho_r(\Phi_q)$ are $x^2B_p(x^{-1})$ and $x^2B_q(x^{-1})$ respectively, those of $\overline{\rho}_r(\Phi_p)$ and $\overline{\rho}_r(\Phi_q)$ are $x^2 - p$ and $x^2 - q$, where p and q are regarded as elements of $\mathbb{F}_r$. It follows that the eigenspaces of $\overline{\rho}_r(\Phi_p)$ and $\overline{\rho}_r(\Phi_q)$ over $\overline{\mathbb{F}}_r$ are pairs of distinct lines, but in one case the lines are rational over $\mathbb{F}_r$ and in the other case irrational. Hence a line in $\overline{\mathbb{F}}_r^2$ which is stable under $\overline{\rho}_r$ is both rational and irrational over $\mathbb{F}_r$ and therefore does not exist. Thus $\overline{\rho}_r$ is absolutely irreducible, and *a fortiori* so is ρ_r.

We are now in a position to apply the Fontaine-Mazur conjecture to ρ_r. Since r is ordinary it follows that ρ_r is semistable, and we have just seen that ρ_r is absolutely irreducible. Furthermore $\det\rho_r = \eta\omega_r^{-1}$, and consequently ρ_r is not a Tate twist of a two-dimensional Artin representation (for then $\det\rho_r$ would be a finite-order character times an *even* power of ω_r). Hence the Fontaine-Mazur conjecture implies that there is a primitive cusp form f of weight 2 and Nebentypus character η such that ρ_r is isomorphic to the semisimple representation $\rho_{f,r} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Q}_r)$ associated to f. But $a(p) = 0$ for $p \in P$, a set of density 1/2. It follows (Serre [**84**], p. 174, Corollaire 2) that f is a form of CM type. Thus the results of Ribet ([**73**], pp. 38 – 39, (4.4) and p. 40, (4.5)) imply that there is an imaginary quadratic field K and a primitive Hecke character χ of K of type $(1, 0)$ such that $L(s, \chi) = L(s, f)$. It follows in particular that if p is a prime which splits in K and is relatively prime to $\mathfrak{f}(\chi)$ then $p \notin S$ and

$$a(p) = \chi(\mathfrak{p}) + \chi(\overline{\mathfrak{p}}), \tag{5.15}$$

where $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ are the prime ideals of K above p.

Now let $\kappa = \mathrm{sign}_{K/\mathbb{Q}}$, viewed as a primitive quadratic Dirichlet character. Since f is a form of weight two we have $\eta(-1) = 1$, whereas $\kappa(-1) = -1$ since K is imaginary. But κ and by assumption also η are nontrivial characters, so if N is a common multiple of the conductors of η and κ then the sums $\sum_j \eta(j)$ and $\sum_j \kappa(j)$ are both 0, where j runs over invertible residue classes modulo N. Since $\eta(-1) = 1$ and $\kappa(-1) = -1$ it follows that there is also an invertible residue class c such that $\eta(c) = -1$ and $\kappa(c) = 1$. Hence by Dirichlet's theorem there are infinitely many prime numbers p relatively prime to $\mathfrak{f}(\chi)$ such that $\eta(p) = -1$ and $\kappa(p) = 1$, or in other words such that $p \in P$ and p splits in K: but these conditions imply respectively that $a(p) = 0$ and that (5.15) holds. Thus

$$\chi(\mathfrak{p}) = -\chi(\overline{\mathfrak{p}}). \tag{5.16}$$

Put $\mathfrak{F} = \mathbf{N}\mathfrak{f}(\chi)$ and choose n so that $\mathfrak{p}^n \in P_{\mathfrak{F}}$; then choose $\alpha \in K_{\mathfrak{F}}$ so that $\mathfrak{p}^n = \alpha\mathcal{O}$. By complex conjugation we also have $\overline{\mathfrak{p}}^n = \overline{\alpha}\mathcal{O}$. Both α and $\overline{\alpha}$ belong to $K_{\mathfrak{f}(\chi)}$, whence on raising both sides of (5.16) to the nth power we obtain $\alpha = (-1)^n\overline{\alpha}$. Passing to ideals we get $\mathfrak{p}^n = \overline{\mathfrak{p}}^n$ and consequently $\mathfrak{p} = \overline{\mathfrak{p}}$. Since p splits in K this is a contradiction. □

4. An open problem

Someday somebody may be able to formulate a conjecture which fully captures the notion that "motivic L-functions usually satisfy the minimalist trichotomy," but the hypotheses proposed in this lecture fall short of the mark, for two reasons.

First of all, no matter how $\mathcal{S}$ is chosen, a conjecture like (5.11) 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, we expect that every Dirichlet L-function satisfies the minimalist trichotomy, and Serre has conjectured more generally that the same is true for the L-function of any irreducible Artin representation of $\mathbb{Q}$ ([**35**], p. 324, Conjecture 8.24.1), but no such consequence can be deduced from (5.11). Neither can results like Theorem 1.2 or like Greenberg's theorem [**36**] on powers of Hecke characters of type $(1, 0)$.

Granting this objection, we come to a second issue, namely the choice of $\mathcal{S}$. We have portrayed $\mathcal{S}_{K,w,n}$ as the desired choice and $\mathcal{S}_{K,\mathbb{E},w,n}$ as the default choice, but neither is likely to be the right choice: A satisfactory conjecture would accommodate a wider variety of sets $\mathcal{S}$, subject only to some condition (still to be formulated) which plausibly ensures that (5.11) holds. The point is illustrated already by the two choices $\mathcal{S}_{K,w,n}$ and $\mathcal{S}_{K,\mathbb{E},w,n}$: The former is more inclusive, but without the latter we have no hope of recovering the minimalist conjecture for elliptic curves over $\mathbb{Q}$, and neither $\mathcal{S}_{K,w,n}$ nor $\mathcal{S}_{K,\mathbb{E},w,n}$ is likely to be suitable if one wants to conjecture that L-functions of essentially self-dual premotives satisfy the minimalist dichotomy with probability one. Underlying this last remark is the expectation that essentially self-dual premotives have density zero among all premotives, so that the validity of the minimalist trichotomy with probability one would say nothing about the minimalist dichotomy.

Unable to propose a compelling conjecture in general, we return to the case of elliptic curves over $\mathbb{Q}$, where we would still like to know that the minimalist conjecture is equivalent to the average rank hypothesis. If we grant (5.3) then the missing link, as already noted, is (5.6), which should hold for any of the counting functions ν mentioned earlier:

Problem 5. *Show that*

$$\vartheta_{\mathcal{E}^{\pm},\nu}(x) = \frac{1}{2}\vartheta_{\mathcal{E},\nu}(x) + O(x^{\gamma})$$

with a constant $\gamma < 5/6$.

5. Exercises

Exercise 5.1. It follows from work of Mestre [**64**] that if E is an elliptic curve over $\mathbb{Q}$ then

$$\mathrm{ord}_{s=1}L(s,E) \ll \log N(E), \tag{5.17}$$

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. The case $w = 0$ of Proposition 5.3 implies that if K and $\mathbb{E}$ are fixed number fields, S a fixed finite set of prime ideals of K, and n a fixed positive integer, then there are only finitely many isomorphism classes of n-dimensional Artin representations of K which are unramified outside S and the infinite places of K and which are realizable over $\mathbb{E}$. Give a direct proof of this assertion.

Exercise 5.3. This problem refers to a conjecture of Serre already mentioned: Artin L-functions associated to irreducible Artin representations of $\mathbb{Q}$ satisfy the minimalist trichotomy.

(a) Why is the conjecture restricted to Artin representations of $\mathbb{Q}$? Why not make the same conjecture for Artin representations of arbitrary number fields? (Hint: Exercise 3.3.)

(b) (*Literature search.*) Some numerical evidence in support of Serre's conjecture can be found in the paper of Omar [**71**], where the Artin representations at issue are two-dimensional with image isomorphic to the quaternion group. Have other irreducible representations of dimension > 1 been investigated numerically?

Exercise 5.4. (*Reading.*) Using a counting function similar to (5.2), Bhargava and Shankar [**7**] have recently shown that the average rank of an elliptic curve over $\mathbb{Q}$ is $\leqslant 7/6$. While this result pertains to the Mordell-Weil rank rather than the "analytic rank" $\mathrm{ord}_{s=1}L(s,E)$, under the conjecture of Birch and Swinnerton-Dyer their work does give an upper bound for the quantity $r_\nu(\mathcal{E})$ in (5.5). What are they able to deduce about analytic ranks unconditionally?

Exercise 5.5. As we have already noted, the elliptic curve 389 A1 of [**22**] violates the minimalist dichotomy. The purpose of this problem is to give an example of a premotive M which is *not* essentially self-dual but which also violates the minimalist trichotomy.

(a) Put $K = \mathbb{Q}(\sqrt{-7})$ and $d = -118-18\sqrt{-7}$, and let η be the quadratic Hecke character of K associated to the extension $K(\sqrt{d})$ of K. View $A(7)$ as an elliptic curve over K and write E for the twist of $A(7)$ by η. Using [**38**], p. 82, verify that $y^2 = x^3 - 35x - 98$ is an equation for $A(7)$ over K, whence $dy^2 = x^3 - 35x - 98$ is an equation for E.

(b) Show that the point with coordinates $(x,y) = ((1+\sqrt{-7})/2, 1)$ relative to the equation $dy^2 = x^3 - 35x - 98$ is a point of infinite order on E.

(c) Let χ be the unique element of $X(7)$, and put $\xi = \chi\eta$ and $M = M(\xi)$, so that $L(s,M) = L(s,\xi)$ and $L(s,E/K) = L(s,\xi)L(s,\overline{\xi})$. Using the Coates-Wiles theorem [**19**], deduce from (b) that $L(1,M) = 0$. But show that $L(s,\xi) \neq L(s,\overline{\xi})$, whence M is not self-dual.

Bibliography

[1] G. Anderson, D. Blasius, R. Coleman, and G. Zettler, *On representations of the Weil group with bounded conductor*, Forum Math. 6 (1994), 537 – 545.

[2] J. Armitage, *On a theorem of Hecke in number fields and function fields*, Invent. Math. 2 (1967), 238 – 246.

[3] J. Armitage, *Zeta functions with a zero at $s = 1/2$*, Invent. Math. 15 (1972), 199 – 205.

[4] A. Ash, D. Doud, and D. Pollack, *Galois representations with conjectural connections to arithmetic cohomology*, Duke Math. J. 112 (2002), 521 – 579.

[5] 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.

[6] R. Balasubramanian and V. K. Murty, *Zeros of Dirichlet L-functions*, Ann. Sci. Ecole Norm. Sup. 25 (1992), 567 – 615.

[7] M. Bhargava and A. Shankar, *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank* 0. Online preprint: `http://arxiv.org/abs/1007.0052`.

[8] 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

[9] B. J. Birch and N. M. Stephens, *The parity of the rank of the Mordell-Weil group*, Topology 5 (1966), 295 – 299.

[10] G. A. Boxer and P. Diao, *Effective nonvanishing of canonical Hecke L-functions*, Proc. Amer. Math. Soc., to appear.

[11] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*, J. Amer. Math. Soc. 14 (2001), 843-939.

[12] A. Brumer, *The average rank of elliptic curves I*, Invent. Math. 109 (1992), 445 – 472.

[13] A. Brumer and O. McGuinness, *The behavior of the Mordell-Weil group of elliptic curves*, Bull. Amer. Math. Soc. 23 (1990), 375 – 382.

[14] D. Bump, S. Friedberg, and J. Hoffstein, *Nonvanishing theorems for L-functions of modular forms and their derivatives*, Invent. Math. 102 (1990), 543 – 618.

[15] Ph. Cassou-Noguès, *Quelques théorèmes de base normale d'entiers*, Ann. Inst. Fourier 28 (1978), 1 – 33.

[16] T. Chinburg, B. Erez, G. Pappas, and M. J. Taylor, *ε-constants and the Galois structure of de Rham cohomology*, Ann. of Math. 146 (1997), 411 – 473.

[17] 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.

[18] S. D. Chowla, *The Riemann Hypothesis and Hilbert's Tenth Problem (Mathematics and its Applications Vol. 4)*, Gordon and Breach Science Publishers (1965).

[19] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. 39 (1977), 223 – 251.

[20] B. Conrey and K. Soundararajan, *Real zeros of quadratic Dirichlet L-functions*, Invent. Math. 150 (2002), 1 – 44.

[21] J. Cougnard, *Les travaux de A. Fröhlich, Ph. Cassou-Noguès et M.J. Taylor sur les bases normales*, Séminaire Bourbaki 25, 1982-1983, Exp. No. 598, 25 – 38.

[22] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge University Press (1980).

[23] 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.

[24] 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

[25] P. Deligne and J.-P. Serre, *Formes modulaires de poids 1*, Ann. Sci. Ec. Norm. Sup. 7 (1974), 507 – 530.

[26] C. Deninger, *L-functions of mixed motives.* In: *Motives*, Proc. Symp. Pure Math. Vol. 55 – Part 1, Amer. Math. Soc. (1994), 517 – 525.

[27] W. Duke, J. Friedlander, and H. Iwaniec, *Bounds for automorphic L-functions. II*, Invent. Math. 115 (1994), 219 – 239.

[28] J. Ellenberg and A. Venkatesh *Reflection principles and bounds for class group torsion*, Int. Math. Res. Not. (2007).

[29] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörper*, Invent. Math. 73 (1983), 349 – 366.

[30] 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.

[31] A. Fröhlich, *Artin root numbers and normal integral bases for quaternion fields*, Invent. Math. 17 (1972), 143 – 166.

[32] A. Fröhlich, *Galois module structure* In: *Algebraic Number Fields*, Proceedings of the Durham Symposium, A. Fröhlich, ed., Academic Press (1977), 133 – 191.

[33] A. Fröhlich and J. Queyrut, *On the functional equation for the Artin L-function for characters of real representations*, Invent. Math. 20 (1973), 125–138.

[34] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields.* In: *Number Theory, Carbondale, 1979*, Springer, Lecture Notes in Math. 751 (1979), 108 – 118.

[35] D. Goss, *Basic Structures of Function Field Arithmetic*, Ergebnisse der Math. 35, Springer (1966).

[36] R. Greenberg, *On the critical values of Hecke L-functions for imaginary quadratic fields*, Invent. Math. 79 (1985), 79 – 94.

[37] 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.

[38] B. H. Gross, *Arithmetic on Elliptic Curves with Complex Multiplication*, SLN 776, Springer-Verlag (1980).

[39] B. H. Gross and D. B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. 84 (1986), 225 – 320.

[40] D. R. Heath-Brown, *The average rank of elliptic curves*, Duke Math. J. 122 (2004), 225 – 320.

[41] D. R. Heath-Brown and S. J. Patterson, *The distribution of Kummer sums at prime arguments*, J. reine angew. Math. 310 (1979), 111 – 130.

[42] E. Hecke, *Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen. Zweite Mitteilung*, Math. Z. 6 (1920), 11 – 51.

[43] E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, Chelsea Publishing Company, 2nd ed. (1970).

[44] D. Husemöller, *Elliptic Curves*, Springer GTM 111 (1987).

[45] H. Iwaniec, W. Luo, and P. Sarnak, *Low lying zeros of families of L-functions*, Publ. Math. Inst. Hautes Études Sci. 91 (2000), 55 – 131.

[46] 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.

[47] M. Jutila, *On the mean value of* $L(1/2,\chi)$ *for real characters*, Analysis 1 (1981), 149 – 161.

[48] S. Katayama, *On fundamental units of real quadratic fields with norm +1*, Proc. Japan Acad. 68 Ser. A (1992), 18 – 20.

[49] C. Khare, *F-split Galois representations are potentially abelian*, Proc. Amer. Math. Soc. 131 (2003), 3021 – 3023.

[50] C. Khare and J.-P. Wintenberger, *Serre's modularity conjecture (I)*, Invent. Math. 178 (2009), 485 – 504.

[51] C. Khare and J.-P. Wintenberger, *Serre's modularity conjecture (II)*, Invent. Math. 178 (2009), 505 – 586.

[52] M. Kisin, *Modularity of 2-adic Barsotti-Tate representations*, Invent. Math. 178 (2009), 587 – 634.

[53] V. A. Kolyvagin, *Finiteness of* $E(\mathbf{Q})$ *and* $\text{Ш}(E,\mathbf{Q})$ *for a subclass of Weil curves*, Izv. Akad. Nauk SSSR Ser. Mat. 52 (1988), 522 – 540; Math. USSR Izv. 32 (1989), 523 – 541.

[54] V. A. Kolyvagin and D. Yu. Logachev, *Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties*; Algebra i Analiz 1 (1989), 171 – 196; Leningrad Math. J. 1 (1990) 1229 – 1253.
[55] S. Lang, *Algebraic Number Theory*, 2nd. ed., Springer GTM 110 (1994).
[56] S. Lang and H. Trotter, *Frobenius Distributions in GL_2-Extensions*, Springer-Verlag, LNM vol. 504 (1976).
[57] R. P. Langlands, *Base Change for* GL(2), Princeton Univ. Press, Ann. of Math. Studies 96 (1980).
[58] 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.
[59] R. Masri, *Quantitative nonvanishing of L-series associated to canonical Hecke characters*, IMRN (2007).
[60] R. Masri, *Asymptotics for sums of central values of canonical Hecke L-series*, IMRN (2007).
[61] R. Masri and T. H. Yang, *Average values of Hecke L-functions via Galois suborbits of Heegner points*.
[62] C. R. Matthews, *Gauss sums and elliptic functions: I. The Kummer sum*, Invent. Math. 52 (1979), 163 – 185.
[63] C. R. Matthews, *Gauss sums and elliptic functions: II. The quartic sum*, Invent. Math. 54 (1979), 23 – 52.
[64] J.-F. Mestre, *Formules explicites et minorations de conducteurs de variétés algébriques*, Compositio Math. 58 (1986), 209 – 232.
[65] 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.
[66] 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.
[67] H. Moon, *Finiteness results on certain mod p Galois representations*, J. Number Theory 84 (2000), 156 – 165.
[68] H. Moon and Y. Taguchi, *Mod p Galois representations of solvable image*, Proc. Amer. Math. Soc. 129 (2001), 2529 – 2534.
[69] M. R. Murty and V. K. Murty, *Non-vanishing of L-functions and applications*. In: Progress in Mathematics 157, Birkhäuser (1997).
[70] M. R. Murty and V. K. Murty, *Mean values of derivatives of modular L-series*, Ann. of Math. 133 (1991), 447 – 475.
[71] S. Omar, *On Artin L-functions for octic quaternion fields*, Experim. Math. 10 (2001), 237 – 245.
[72] S. Omar, *Non-vanishing of Dirichlet L-functions at the central point*. In: *Algorithmic Number Theory, 8th International Symposium, ANTS VIII*, A. J. van der Poorten and A. Stein, eds., Springer LNCS 5011 (2008), 443 – 453.
[73] K. A. Ribet, *Galois representations attached to eigenforms with Nebentypus*. In: *Modular Functions of One Variable, V*, Lect. Notes in Math. 601, Springer-Verlag (1977), 17 – 52.
[74] F. Rodriguez Villegas, *Square root formulas for central values of Hecke L-series. II* Duke Math. J. 72 (1993), 431 – 440.
[75] D. E. Rohrlich, *On the L-functions of canonical Hecke characters of imaginary quadratic fields*, Duke Math. J. 47 (1980), 547 – 557.
[76] D. E. Rohrlich, *Root numbers of Hecke L-functions of CM fields*, Am. J. Math. 104 (1982), 517 – 543.
[77] D. E. Rohrlich, *Compatible families of elliptic type*, Acta Arithmetica, 142 (2010), 1 – 9.
[78] K. Rubin, *Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. 64 (1981), 455 – 470.
[79] K. Rubin and A. Silverberg, *Ranks of elliptic curves*, Bull. Amer. Math. Soc. 39 (2002), 455 – 474.
[80] P. Schneider, *Introduction to the Beilinson conjectures*. In: *Beilinson's Conjectures on Special Values of L-Functions*, Academic Press (1988), 1 – 33.
[81] J.-P. Serre, *Facteurs locaux de fonctions zêta des variétés algébriques (définitions et conjectures)*. In: Séminaire Delange-Poitou-Pisot, 1969/70, no. 19.
[82] J.-P. Serre, *Abelian ℓ-Adic Representations and Elliptic Curves*, W. A. Benjamin, 1968.
[83] J.-P. Serre, *Local Fields*, Springer GTM 67 (1979).

[84] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Publ. Math. IHES 54 (1981), 123 – 201.

[85] J.-P. Serre, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. 54 (1987), 179 – 230.

[86] J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. of Math. 88 (1968), 492 – 517.

[87] G. Shimura, *The special values of the zeta functions associated with cusp forms*, Comm. Pure Appl. Math. 29 (1976), 783 – 804.

[88] G. Shimura, *On the periods of modular forms*, Math. Ann. 229 (1977), 211 – 221.

[89] V. P. Snaith, *Explicit Brauer Induction*, Cambridge Studies in Advanced Math. 40, Cambridge Univ. Press (1994).

[90] K. Soundararajan, *Nonvanishing of quadratic Dirichlet L-functions at* $s = 1/2$, Ann. of Math. 152 (2000), 447 – 488.

[91] 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.

[92] J. Tate, *Fourier analysis in number fields and Hecke's zeta functions*. In: *Algebraic Number Theory*, J. W. S. Cassels and A. Fröhlich, eds., Academic Press (1967), 305 – 347.

[93] J. Tate, *Local constants* (prepared in collaboration with C. J. Bushnell and M. J. Taylor). In: *Algebraic Number Fields*, Proceedings of the Durham Symposium, A. Fröhlich, ed., Academic Press (1977), 89 – 131.

[94] 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.

[95] M. J. Taylor, *On Fröhlich's conjecture for rings of integers of tame extensions*, Invent. Math. 63 (1981), 41 – 79.

[96] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. 141 (1995), 553 – 572.

[97] J. Tunnell, *Artin's conjecture for representations of octahedral type*, Bull. AMS 5 (1981), 173 – 175.

[98] 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* $\mathrm{PSL}(2,\mathbb{Z})$, Math. USSR Izvestija 12 (1978), 448 – 462.

[99] M. Watkins, *Some heuristics about elliptic curves*, Experimental Math. 17 (2008), 105 – 125.

[100] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. 141 (1995), 443 – 551.

[101] T. H. Yang, *On CM abelian varietiers over imaginary quadratic fields*, Math. Ann. 329 (2004), 87 – 117.

[102] T. H. Yang, *Nonvanishing of central Hecke L-values and rank of certain elliptic curves*, Compositio Math. 117 (1999), 337-359.

[103] M. P. Young, *Low-lying zeros of families of elliptic curves*, J. Amer. Math. Soc. 19 (2005), 205 – 250.

[104] 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.

[105] S. W. Zhang, *Heegner cycles and derivatives of L-series*, Invent. Math. 130 (19917), 99 – 152.