

# $L$ -functions

Davide Lombardo

*The Zeta function knows everything about algebraic number fields,  
the only problem is to make it speak – G. Harder (?)*

## Contents

<b>Contents</b>	<b>1</b>
<b>Introduction</b>	<b>3</b>
<b>1 Classical <math>L</math>-functions and applications</b>	<b>6</b>
1.1 What is an $L$ -function, anyway? . . . . .	6
1.1.1 The Riemann $\zeta$ function . . . . .	6
1.1.2 The Selberg class . . . . .	9
1.1.3 Dedekind $\zeta$ functions . . . . .	9
1.1.4 Dirichlet $L$ -functions . . . . .	10
1.2 The prime number theorem . . . . .	13
1.2.1 The Riemann–von Mangoldt exact formula . . . . .	20
1.3 Review of algebraic number theory . . . . .	21
1.3.1 Structure of the ring of integers . . . . .	22
1.3.2 Unique factorisation of ideals . . . . .	22
1.3.3 Splitting of primes . . . . .	22
1.3.4 Galois action on the primes . . . . .	24
1.3.5 Frobenius elements . . . . .	25
1.3.6 Dirichlet’s unit theorem and the regulator . . . . .	27
1.3.7 The class group . . . . .	29
1.3.8 Completed $\zeta$ functions: the local factors at infinity . . . . .	30
1.4 The $L$ -function of a (complex) Galois representation . . . . .	30
1.4.1 Independence of the choice of $\mathfrak{P}$ . . . . .	31
1.4.2 Convergence of the Euler product . . . . .	33

1.4.3	The Riemann and Dedekind $\zeta$ functions, and Dirichlet's $L$ -functions, are Artin $L$ -functions . . . . .	33
1.4.4	The formalism of Artin $L$ -functions . . . . .	36
1.4.5	Artin's conjecture on analytic continuation . . . . .	41
1.4.6	Factorisation of the Dedekind $\zeta$ -function . . . . .	42
1.5	Dirichlet's theorem on arithmetic progressions . . . . .	43
1.5.1	Pontryagin duality: finite case . . . . .	43
1.5.2	Densities . . . . .	47
1.5.3	Factorisation of the cyclotomic Dedekind $\zeta$ function, reprise . . . . .	49
1.5.4	Infinitely many primes in arithmetic progressions . . . . .	50
1.5.5	The philosophy of special values . . . . .	52
1.6	Chebotarev's density theorem . . . . .	54
1.6.1	Analytic proof . . . . .	56
1.6.2	Algebraic (well, mostly algebraic) proof . . . . .	59
1.6.3	Exercises . . . . .	66
<b>2</b>	<b>Prerequisites for Tate's thesis</b>	<b>68</b>
2.1	The Haar measure . . . . .	68
2.1.1	Preliminaries . . . . .	68
2.1.2	Haar measure: existence . . . . .	70
2.1.3	Haar measure: uniqueness (up to constants) . . . . .	76
2.2	Abstract Fourier analysis . . . . .	78
2.2.1	Pontryagin duality: general case . . . . .	78
2.2.2	The abstract Fourier transform . . . . .	80
2.3	Review of local fields . . . . .	82
2.4	Restricted direct products . . . . .	86
2.4.1	Abstract group theory . . . . .	87
2.4.2	Topological groups . . . . .	88
2.4.3	(Quasi-)Characters of a restricted product . . . . .	89
2.4.4	Measure theory . . . . .	91
2.4.5	Fourier analysis . . . . .	94
<b>3</b>	<b>Tate's thesis</b>	<b>98</b>
3.1	The local theory . . . . .	98
3.1.1	The additive group . . . . .	98
3.1.2	The multiplicative group . . . . .	103
3.1.3	Local zeta functions I: the general functional equation . . . . .	107
3.1.4	Local zeta functions II: computation of the local factors . . . . .	111
3.2	The global theory . . . . .	120
3.2.1	The additive group: the adèles . . . . .	120
3.2.2	The multiplicative group: the idèles . . . . .	133
3.2.3	Global zeta functions . . . . .	140
3.3	Hecke $L$ -functions, reprise . . . . .	145
3.4	Characters of the idèles . . . . .	146
3.5	Recovering the classical theory . . . . .	150
3.5.1	The Riemann zeta function . . . . .	150
3.5.2	Dedekind $\zeta$ functions . . . . .	150

3.5.3	The general case: $L$ -functions of characters . . . . .	152
<b>4</b>	<b>Exam questions</b>	<b>160</b>
	<b>Bibliography</b>	<b>162</b>

## Introduction

$L$ -functions are an essential topic in modern number theory, playing a fundamental role in the study of various arithmetic phenomena. There are ways to attach an  $L$ -function to almost any mathematical object, and certainly to all the main objects of interest in number theory, such as algebraic number fields, Dirichlet characters, and elliptic curves.  $L$ -functions encode a wealth of information about these objects, allowing us to analyse their properties and make deep connections between seemingly unrelated areas of mathematics. One of the most significant applications of  $L$ -functions, and historically the first, is their use in understanding the distribution of prime numbers, both as a subset of all natural numbers (the Prime Number Theorem of Hadamard and de la Vallée–Poussin) and in arithmetic progressions (Dirichlet’s theorem).

These course notes focus on two main topics related to  $L$ -functions: their classical applications in number theory and their analytic properties. The first part of the course covers results such as the prime number theorem and Dirichlet’s theorem on arithmetic progressions, as well as the more sophisticated theorem of Chebotarev concerning the distribution of Frobenius automorphisms in Galois groups. I focus on the derivation of the number-theoretic results from the analytic properties of  $L$ -functions, that I mostly take for granted, postponing their discussion to the last chapter of these notes (where they are eventually proved in full). I try to give a unifying framework to understand many different constructions by discussing Artin’s general definition of  $L$ -functions, but I focus mostly on the so-called *abelian*  $L$ -functions (namely, in the language of Artin, those that correspond to abelian extensions of number fields). This already covers a huge class of  $L$ -functions, including all zeta functions of number fields, as well as the classical functions studied by Dirichlet to prove his theorem.

The second part of the course focuses on the proof of the main analytic properties of abelian  $L$ -functions, such as functional equations, analytic continuation, and the analytic class number formula. I follow closely the presentation of Tate’s doctoral thesis, providing additional details with respect to the original material.

These notes are the result of a course for master’s and PhD students given at the University of Pisa in the spring of 2023. They contain essentially no original material, with the possible exception of Section 1.6.1, which gives a streamlined analytic proof of the Chebotarev density theorem. In preparing these notes I have drawn heavily from various sources, most of which are cited in the text, but which I repeat here.

- The proof of the Prime Number Theorem I give is taken from Zagier’s famous short note [Zag97]. I also sketch a second proof, closer in spirit to the original point of view of Riemann on his zeta function, that is heavily inspired by Tao’s blog post [Tao21].
- For the treatment of Artin’s  $L$ -functions I have borrowed mainly from Chapter V of Neukirch’s book on algebraic number theory [Neu99].

- I have written the proof of Dirichlet’s theorem on primes in arithmetic progressions without referring to any particular book, but my understanding of the topic is certainly influenced by Serre’s *Cours d’arithmétique* [Ser77]. For this proof in particular, I have tried to stress how the deduction of the number-theoretic consequences from the analytic properties of  $L$ -functions is comparatively easy, and can be placed in a general framework that gives us the first hints of the abstract Fourier analysis which is used systematically in Tate’s thesis.
- The two arguments for Chebotarev’s theorem, which I call the ‘analytic’ and ‘algebraic’ proofs (and which are secretly the same proof in disguise), come respectively from [LO77], which I have tried to strip of as much of the heavy analytic machinery as possible, and from chapter 15 of Schoof’s delightful book on Catalan’s conjecture [Sch08].
- The second chapter of these notes, which deals with some preliminaries necessary for understanding Tate’s thesis, is mainly inspired by [RV99]. Since the emphasis of the course was on number theory, I have decided to cover the construction of the Haar measure in detail, but to leave out the proofs of the main theorems in the abstract theory of Fourier inversion.
- Finally, Chapter 3 is simply my retelling of Tate’s thesis itself [Tat67]. Although the original is an unsurpassed masterpiece, I still hope that my humble, low-brow version of the story can be of help to someone.

Of course, many important topics are not even touched upon: I haven’t discussed Hasse-Weil  $L$ -functions and, more generally,  $L$ -functions of geometric origin; I haven’t ventured into the problem of modularity of  $L$ -functions; I haven’t described Weil’s reinterpretation of Tate’s thesis in terms of distributions; and I haven’t even dared to hint at the whole Langlands programme, of which, unfortunately, I know too little. Nevertheless, I hope that what *is* there can be useful to people interested in number theory, providing a slightly different take on the very classical and important topic of  $L$ -functions.

## Acknowledgments

I thank Lucrezia Bertolotti, Sebastiano Boscardin, Davide Colpo, Lorenzo Furio, Andrea Gallese, Giulio Grammatica, Francesco Moroniti, Luca Speciale, Mirko Torresani and Cristofer Villani for pointing out mistakes in a preliminary version of these notes. I am grateful to Alberto Perelli for an interesting discussion about functional equations, for some insightful comments on the definition of the Selberg class, and for sharing with me the notes of one of his courses.

## Symbols for exercises

♠ denotes an exercise requiring some input from basic algebraic number theory (at the level of an introductory course, e.g., ‘Teoria Algebrica dei Numeri 1’).

★ denotes a harder exercise.

# Chapter 1

## Classical $L$ -functions and applications

## 1.1 What is an $L$ -function, anyway?

To paraphrase the physicists' definition of a *vector*<sup>1</sup>, an  $L$ -function is anything that behaves like an  $L$ -function. More seriously, while it is possible to conjecturally describe the class of  $L$ -functions by means of the so-called *axioms of the Selberg class* (see below), I feel it is more natural to form one's idea of  $L$ -functions by looking at examples. We will later give a (still partial) definition of  $L$ -function that at the very least encompasses all the main examples we will meet in this course.

We start by introducing the notion of *Dirichlet series*:

**Definition 1.1.1** (Dirichlet series). Let  $(a_n)_{n \geq 1}$  be a sequence of complex numbers. The associated **Dirichlet series** is

$$\sum_{n \geq 1} \frac{a_n}{n^s},$$

seen as a function of the complex variable  $s$  (if the sum converges). The **abscissa of absolute convergence** is

$$\sigma_0 := \inf \left\{ \sigma \in \mathbb{R} : \Re s > \sigma \Rightarrow \sum_{n \geq 1} \frac{a_n}{n^s} \text{ converges absolutely} \right\}.$$

The function  $s \mapsto \sum_{n \geq 1} \frac{a_n}{n^s}$  is holomorphic for  $s \in \{\Re s > \sigma_0\}$ .

### 1.1.1 The Riemann $\zeta$ function

The single most important example of  $L$ -function is given by Riemann's  $\zeta$  function.

**Definition 1.1.2** (Riemann  $\zeta$  function). The **Riemann  $\zeta$  function** is given by

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}$$

for all  $s \in \mathbb{C}$  with  $\Re s > 1$ .

By standard results,  $\zeta(s)$  is well-defined (since  $\sum_{n \geq 1} n^{-s}$  converges for all real numbers  $s > 1$ ) and defines a holomorphic function on  $\{\Re s > 1\}$ . We will later show:

**Theorem 1.1.3.** *The function  $\zeta(s)$  extends to a meromorphic function on the whole of  $\mathbb{C}$ , with a single simple pole at  $s = 1$  with residue 1. In particular,  $\zeta(s) = \frac{1}{s-1} + O(1)$  as  $s \rightarrow 1$ .*

This is a consequence of the famous *functional equation* for  $\zeta(s)$ . In order to discuss it, we need to recall Euler's  $\Gamma$  function:

**Definition 1.1.4.** We define

$$\Gamma(s) = \int_0^{\infty} t^s e^{-t} \frac{dt}{t}$$

for  $\Re s > 0$ .

---

<sup>1</sup>our definition of a vector is that a vector is anything that transforms like a vector, see [https://phys.libretexts.org/Bookshelves/Relativity/Book%3A\\_Special\\_Relativity\\_\(Crowell\)/07%3A\\_Coordinates/7.02%3A\\_Transformation\\_of\\_Vectors](https://phys.libretexts.org/Bookshelves/Relativity/Book%3A_Special_Relativity_(Crowell)/07%3A_Coordinates/7.02%3A_Transformation_of_Vectors)

**Remark 1.1.5.** One way to remember the definition of  $\Gamma(s)$  (and the reason I write it in this way, instead of the more usual  $\int_0^\infty t^{s-1}e^{-t} dt$ ) is to notice that it is the Mellin transform (=abstract Fourier transform for the group  $(\mathbb{R}_{>0}, \cdot)$ ) of the function  $e^{-t}$ , see Remark 3.1.38.

**Exercise 1.1.6.** Check the following properties of  $\Gamma(s)$ :

1.  $\Gamma(s)$  is a holomorphic function of  $s$  in the right half-plane  $\{\Re s > 0\}$ ;
2.  $\Gamma(s+1) = s\Gamma(s)$  for all  $s \in \mathbb{C}$  with  $\Re s > 0$ ;
3.  $\Gamma(s)$  extends to a meromorphic function on  $\mathbb{C}$ , with poles only at the non-positive integers;
4.  $\Gamma(\frac{1}{2}) = \sqrt{\pi}$ ;
5.  $(\star)$  Legendre's duplication formula:

$$\frac{\Gamma(s)\Gamma(s + \frac{1}{2})}{\Gamma(2s)} = \frac{\Gamma(\frac{1}{2})}{2^{2s-1}} = \frac{\sqrt{\pi}}{2^{2s-1}}.$$

*Hint.* This is much harder than the other parts of the exercise. Here is a possible strategy.

- a) Introduce the Beta function

$$B(m, n) = \int_0^1 u^{m-1}(1-u)^{n-1} du$$

and prove that  $B(m, n) = \frac{\Gamma(m)\Gamma(n)}{\Gamma(m+n)}$ .

- b) Replacing  $m = n = z$  and then  $u = \frac{1+x}{2}$ , obtain

$$\frac{\Gamma(z)^2}{\Gamma(2z)} = 2^{1-2z} \left( 2 \int_0^1 (1-x^2)^{z-1} dx \right).$$

- c) Prove the following identity for the Beta function:

$$B(m, n) = 2 \int_0^1 x^{2m-1}(1-x^2)^{n-1} dx.$$

- d) Obtain the equality

$$\frac{\Gamma(z)^2}{\Gamma(2z)} = 2^{1-2z} B(1/2, z) = 2^{1-2z} \frac{\Gamma(1/2)\Gamma(z)}{\Gamma(z+1/2)}$$

and conclude.

6.  $(\star\star)$  It is useful to also mention **Euler's reflection formula**,

$$\Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin(\pi z)},$$

which you don't need to prove unless you really want to.

7.  $\Gamma(s)$  has no zeroes in  $\mathbb{C}$  (even though it is not necessary, you might want to use Euler's formula to prove this).

Having introduced the  $\Gamma$  function, we can define a further auxiliary function (which will eventually turn out to be somewhat more natural than  $\zeta(s)$ ):

**Definition 1.1.7** (Landau's  $\xi$  function). We set  $\xi(s) = \frac{1}{2}s(s-1)\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s)$ .

In terms of  $\xi(s)$ , one has:

**Theorem 1.1.8** (Functional equation for  $\xi(s)$ ). *The  $\xi$  function is holomorphic on the whole complex plane and satisfies*

$$\xi(s) = \xi(1-s).$$

**Exercise 1.1.9.** Assuming the functional equation  $\xi(s) = \xi(1-s)$  in Theorem 1.1.8, prove that  $\xi(s)$  is everywhere holomorphic.

**Remark 1.1.10.** The factor  $s(s-1)$  in the definition of  $\xi(s)$  is invariant under the transformation  $s \mapsto 1-s$ . It follows from the functional equation that the simple function  $f(s) = \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s)$  satisfies the functional equation  $f(s) = f(1-s)$ . From the point of view we will later take, this function  $f$  is probably the 'most natural version' of the Riemann  $\zeta$  function.

The last basic property of  $\zeta(s)$  we want to recall is its representation as an Euler product. More generally, we recall the following result:

**Theorem 1.1.11** (Euler product). *Let  $f : \mathbb{N} \rightarrow \mathbb{C}$  be a multiplicative<sup>2</sup> function and let  $F(s) = \sum_{n \geq 1} \frac{f(n)}{n^s}$  be the associated Dirichlet series. Denote by  $\sigma_0$  the abscissa of absolute convergence. There is an equality of holomorphic functions*

$$F(s) := \sum_{n \geq 1} \frac{f(n)}{n^s} = \prod_{p \text{ prime}} \left( \sum_{n \geq 0} \frac{f(p^n)}{p^{ns}} \right),$$

valid over  $\{\Re s > \sigma_0\}$ . If furthermore  $f$  is completely multiplicative<sup>3</sup>, one has  $\sum_{n \geq 0} \frac{f(p^n)}{p^{ns}} = \sum_{n \geq 0} \left( \frac{f(p)}{p^s} \right)^n = \frac{1}{1-f(p)p^{-s}}$ , and hence

$$\sum_{n \geq 1} \frac{f(n)}{n^s} = \prod_{p \text{ prime}} (1 - f(p)p^{-s})^{-1}.$$

In particular, taking  $f(n) = 1$  for all  $n \geq 1$  we get

$$\zeta(s) = \prod_{p \text{ prime}} (1 - p^{-s})^{-1}.$$

**Remark 1.1.12.** One of the objectives of this course will be to give an interpretation of the function  $\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\prod_{p \text{ prime}}(1 - p^{-s})^{-1}$  from Remark 1.1.10 as an 'extended Euler product', where the additional factor  $\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)$  'comes from the infinite place of  $\mathbb{Q}$ ' (cf. Definition 2.3.1 for the notion of *place*).

<sup>2</sup>that is,  $(m, n) = 1$  implies  $f(mn) = f(m)f(n)$

<sup>3</sup>that is,  $f(mn) = f(m)f(n)$  for all positive integers  $m, n$



### 1.1.2 The Selberg class

This section is taken almost verbatim from Wikipedia [Wik23b]. The idea is to define axiomatically a class of functions that (conjecturally) consists precisely of those we want to call ‘ $L$ -functions’. However, at present, we are unable to prove that many functions we *do* want to call  $L$ -functions actually belong to this class. For this reason, we will make no use of the notion of the Selberg class.

The formal definition of the class  $S$  is the set of all Dirichlet series

$$F(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

absolutely convergent for  $\Re s > 1$  that satisfy the following four conditions:

1. Analyticity:  $F(s)$  has a meromorphic continuation to the entire complex plane, with the only possible pole (if any) when  $s$  equals 1. More precisely, there exists an integer  $m \geq 0$  such that  $(s-1)^m F(s)$  has analytic continuation to an entire function of finite order<sup>4</sup>;
2. Ramanujan conjecture:  $a_1 = 1$  and  $a_n \ll_{\varepsilon} n^{\varepsilon}$  for any  $\varepsilon > 0$ ;
3. Functional equation: there is a gamma factor of the form

$$\gamma(s) = Q^s \prod_{i=1}^k \Gamma(\omega_i s + \mu_i)$$

where  $Q$  is real and positive, the  $\omega_i$  are real and positive, and the  $\mu_i$  are complex with non-negative real part, as well as a so-called root number  $\alpha \in \mathbb{C}$ ,  $|\alpha| = 1$ , such that the function

$$\Phi(s) = \gamma(s)F(s)$$

satisfies

$$\Phi(s) = \alpha \overline{\Phi(1-\bar{s})};$$

4. Euler product: for  $\Re s > 1$ ,  $F(s)$  can be written as a product over primes,

$$F(s) = \prod_p F_p(s)$$

with  $F_p(s) = \exp\left(\sum_{n=1}^{\infty} \frac{b_p^n}{p^{ns}}\right)$  and, for some  $\vartheta < \frac{1}{2}$ ,  $b_p^n = O(p^{n\vartheta})$ .

### 1.1.3 Dedekind $\zeta$ functions

Our next family of  $L$ -functions is given by the so-called (Dedekind)  $\zeta$  functions of number fields. Before defining them, we quickly recall the notion of *ring of integers* of a number field:

---

<sup>4</sup>I am grateful to Alberto Perelli for pointing out the importance of this condition, which plays a fundamental role in the proof of many results concerning the Selberg class. At the present state of knowledge it is not clear whether it can be removed, nor whether it follows from the other axioms.

**Definition 1.1.13** (Ring of integers). Let  $K$  be a number field, that is, a finite extension of  $\mathbb{Q}$ . The **ring of integers of  $K$** , denoted by  $\mathcal{O}_K$ , is the subring

$$\{\alpha \in K : \mu_\alpha(x) \in \mathbb{Q}[x] \text{ has integral coefficients}\}$$

of  $K$ . Here  $\mu_\alpha(x)$  is the unique monic minimal polynomial of  $\alpha$  over  $\mathbb{Q}$ .

We will also need the notion of *norm* of an ideal:

**Definition 1.1.14.** The **norm** of an ideal  $I \triangleleft \mathcal{O}_K$  is the cardinality of the quotient  $\mathcal{O}_K/I$ . We will denote it by  $N(I)$ .

**Exercise 1.1.15** (♠).

1. Show that  $N(I)$  is finite if and only if  $I \neq (0)$ .
2. (★) Show that for every positive integer  $m$  the set  $\{I \triangleleft \mathcal{O}_K : N(I) = m\}$  is finite.

Exercise 1.1.15 shows that the following definition makes sense:

**Definition 1.1.16** (Dedekind  $\zeta$  function). Let  $K$  be a number field. The **Dedekind  $\zeta$  function of  $K$**  is

$$\zeta_K(s) = \sum_{\substack{I \triangleleft \mathcal{O}_K \\ I \neq (0)}} \frac{1}{N(I)^s} := \sum_{n \geq 1} \frac{\#\{I \triangleleft \mathcal{O}_K : N(I) = n\}}{n^s}.$$

**Exercise 1.1.17** (♠).

1. Prove the second equality appearing in Definition 1.1.16.
2. Show that there is an ‘Euler product’ representation of the form

$$\zeta_K(s) = \prod_{P \text{ non-zero prime ideal of } \mathcal{O}_K} (1 - N(P)^{-s})^{-1}.$$

3. (★) Show that  $\zeta_K(s)$  converges for  $\Re s > 1$ .

These functions satisfy properties similar to those of the Riemann  $\zeta$  function. In particular, we will later establish the following:

**Theorem 1.1.18** (Analytic continuation of  $\zeta_K(s)$ ). *The function  $\zeta_K(s)$  extends to a meromorphic function on the entire complex plane, with a single simple pole at  $s = 1$ .*

## 1.1.4 Dirichlet $L$ -functions

The very name ‘ $L$ -function’ comes from a class of functions introduced by Dirichlet in his study of primes in arithmetic progressions. In order to define them, we need to first introduce the notion of *Dirichlet character*.

**Definition 1.1.19** (Dirichlet characters). Let  $m$  be a positive integer. The **group of characters modulo  $m$** , denoted by  $\mathbb{D}_m$ , is the group  $\text{Hom}((\mathbb{Z}/m\mathbb{Z})^\times, \mathbb{S}^1)$ , where  $\mathbb{S}^1$  is the multiplicative group of complex numbers of norm 1. Given an element  $\chi \in \mathbb{D}_m$ , we extend  $\chi$  to a function (again denoted by  $\chi$ )

$$\chi : \mathbb{Z} \rightarrow \mathbb{C}$$

by setting

$$\chi(n) = \begin{cases} \chi(n \bmod m), & \text{if } (m, n) = 1; \\ 0, & \text{if } (m, n) > 1. \end{cases}$$

This extended function is called a **Dirichlet character modulo  $m$** .

**Remark 1.1.20.** Let  $m \geq 2$  be an integer and let  $\chi \in \mathbb{D}_m$  be the trivial element (that is, the homomorphism sending every element of  $(\mathbb{Z}/m\mathbb{Z})^\times$  to 1. The corresponding Dirichlet character  $\chi : \mathbb{Z} \rightarrow \mathbb{C}$  depends on  $m$ , because

$$\chi(n) = \begin{cases} 1, & \text{if } (m, n) = 1 \\ 0, & \text{if } (m, n) > 1. \end{cases}$$

All such characters are called the **trivial** (or **principal**) **character** (or more precisely, the **trivial character mod  $m$** ), and one should be aware that there are infinitely many of them!

**Exercise 1.1.21.** Check the following statements:

1.  $\mathbb{D}_m$  is isomorphic to  $(\mathbb{Z}/m\mathbb{Z})^\times$ ;
2. any Dirichlet character  $\chi : \mathbb{Z} \rightarrow \mathbb{C}$  is a completely multiplicative function.

**Remark 1.1.22.** The isomorphism of the previous exercise is not canonical, and as such, it is better to distinguish the groups  $(\mathbb{Z}/m\mathbb{Z})^\times$  and  $\mathbb{D}_m$ . We will later call these two groups ‘dual to each other in the sense of Pontryagin’, see Proposition 1.5.8, Remark 1.5.5 and Theorem 2.2.2.

To each Dirichlet character we now attach a corresponding  $L$ -function:

**Definition 1.1.23** (Dirichlet  $L$ -functions). Let  $\chi$  be a Dirichlet character modulo  $m$ . We set

$$L(s, \chi) := \sum_{n \geq 1} \frac{\chi(n)}{n^s}.$$

**Exercise 1.1.24.** Show that the abscissa of absolute convergence for these Dirichlet series is  $\sigma_0 = 1$ .

From Exercises 1.1.24 and 1.1.21 and Theorem 1.1.11 it follows that for  $s \in \{\Re s > 1\}$  one has

$$L(s, \chi) = \prod_{p \text{ prime}} (1 - \chi(p)p^{-s})^{-1}. \quad (1.1)$$

**Exercise 1.1.25.** Let  $\chi$  be the trivial character modulo  $m$ . Is  $L(s, \chi)$  the same as the Riemann  $\zeta$  function? Express  $L(s, \chi)$  in terms of  $\zeta(s)$  and simple holomorphic functions.

Exercise 1.1.25 and the properties of the Riemann  $\zeta$  function take care of the principal character. For all other characters, we will later show the following:

**Theorem 1.1.26** (Analyticity of Dirichlet  $L$ -functions of non-trivial characters). *Let  $\chi$  be a non-principal character modulo  $m$ . The function  $L(s, \chi)$  extends to an entire function (that is, a holomorphic function on the whole complex plane).*

For later use, we also quickly review the notion of **primitivity** for Dirichlet characters.

**Definition 1.1.27** (Primitive character, conductor). Let  $m$  be a positive integer. A character  $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \rightarrow \mathbb{S}^1$  is said to be **imprimitive** if there exist a divisor  $d$  of  $m$ , with  $d < m$ , and a character  $\tilde{\chi} : (\mathbb{Z}/d\mathbb{Z})^\times \rightarrow \mathbb{S}^1$  such that  $\chi = \tilde{\chi} \circ \pi$ , where  $\pi : (\mathbb{Z}/m\mathbb{Z})^\times \rightarrow (\mathbb{Z}/d\mathbb{Z})^\times$  is the canonical projection. A character is **primitive** if it is not imprimitive.

Any  $d$  such that  $\chi$  factors as above is called a **modulus** for the character  $\chi$ , while the *minimal* such  $d$  is called the **conductor**. The character  $\tilde{\chi} : (\mathbb{Z}/d\mathbb{Z})^\times \rightarrow \mathbb{S}^1$  which induces  $\chi$  (where  $d$  is the conductor) is called the **primitive character inducing**  $\chi$ .

Finally, a Dirichlet character is called primitive if its modulus coincides with the conductor of the multiplicative character that induces it.

**Example 1.1.28.** *Let  $\chi : \mathbb{Z} \rightarrow \{0, \pm 1\}$  be the function given by*

$$\chi(n) = \begin{cases} 0, & \text{if } (6, n) > 1 \\ 1, & \text{if } (6, n) = 1 \text{ and } n \equiv \pm 1 \pmod{8} \\ -1, & \text{if } (6, n) = 1 \text{ and } n \equiv \pm 3 \pmod{8} \end{cases}$$

*We also identify  $\chi$  to the character  $\chi : (\mathbb{Z}/24\mathbb{Z})^\times \rightarrow \{\pm 1\}$  given essentially by the same rule. It is clear that  $\chi$  is not primitive, since it is induced by the homomorphism  $\tilde{\chi} : (\mathbb{Z}/8\mathbb{Z})^\times \rightarrow \{\pm 1\}$  given by*

$$\tilde{\chi}(n) = \begin{cases} 1, & \text{if } n \equiv \pm 1 \pmod{8} \\ -1, & \text{if } n \equiv \pm 3 \pmod{8}. \end{cases}$$

*One can check easily that  $\tilde{\chi}$  is primitive, so that the conductor of  $\chi$  is 8. Finally, letting  $K = \mathbb{Q}(\sqrt{2})$ , it is not hard to show that  $\zeta_K(s) = \zeta(s)L(s, \tilde{\chi})$ .*

**Exercise 1.1.29.** Prove the last statement in the previous example:  $\zeta_{\mathbb{Q}(\sqrt{2})}(s) = \zeta(s)L(s, \tilde{\chi})$ . *Hint.* You can (and should) do this in at least two ways, which are equivalent but offer slightly different points of view:

1. using the development of  $\zeta(s), \zeta_{\mathbb{Q}(\sqrt{2})}(s)$  as Euler products;
2. writing  $\mathbb{Q}(\sqrt{2}) = \mathbb{Q} \oplus \mathbb{Q} \cdot \sqrt{2}$  as a sum of irreducible representations of  $\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$  and using Theorem 1.4.12.

**Exercise 1.1.30** (Characters vs Dirichlet characters). There are some subtleties concerning the distinction between characters considered as homomorphisms  $(\mathbb{Z}/m\mathbb{Z})^\times \rightarrow \mathbb{S}^1$  or as Dirichlet characters  $\mathbb{Z} \rightarrow \mathbb{C}$ . The best you can do is think about this yourself; if you want a specific exercise, here is a (hopefully) instructive one.

Let  $\tilde{\chi} : (\mathbb{Z}/d\mathbb{Z})^\times \rightarrow \mathbb{S}^1$  be a primitive character modulo  $d$ , let  $m$  be a multiple of  $d$ , and let  $\chi = \tilde{\chi} \circ \pi$  be the character modulo  $m$  that is induced by  $\tilde{\chi}$ . Finally, let  $\chi_{\text{Dirichlet}}$  be the Dirichlet character corresponding to  $\chi$ .

1. Show that the non-zero values of  $\chi_{\text{Dirichlet}}$  are periodic of minimal period  $d$ .

2. Show that  $\chi_{\text{Dirichlet}}$  is periodic of period  $m$ .
3. Show that the minimal period of  $\chi_{\text{Dirichlet}}$  can be equal to  $m > d$ .
4. Show that the minimal period of  $\chi_{\text{Dirichlet}}$  can be equal to  $d$  even when  $m > d$ .

We have now met the main characters of this course. We will later introduce the Hecke  $L$ -functions, which generalise Dirichlet  $L$ -functions to arbitrary number fields, but the examples we have seen so far are already enough to discuss two important theorems in analytic number theory: the prime number theorem and Dirichlet's theorem on arithmetic progressions.

## 1.2 The prime number theorem

The purpose of this essentially self-contained section is to prove the Prime Number Theorem, namely, to show the following:

**Theorem 1.2.1** (Prime Number Theorem). *Let  $\pi(x) = \#\{p \text{ prime} : p \leq x\}$  be the prime-counting function. As  $x \rightarrow \infty$ , we have the asymptotic relation*

$$\pi(x) \sim \frac{x}{\log x}.$$

We will follow the strategy of Newman [New80], as streamlined by Zagier [Zag97]. We introduce the auxiliary functions

$$\Phi(s) = \sum_p \frac{\log p}{p^s}, \quad \vartheta(x) = \sum_{p \leq x} \log p,$$

where every sum indexed by  $p$  (here and below) ranges over the prime numbers.

**Proposition 1.2.2.**  $\vartheta(x) = O(x)$ .

*Proof.* Let  $N$  be a positive integer. Notice that every prime  $p$  with  $N < p \leq 2N$  divides  $\binom{2N}{N}$ , so

$$\vartheta(2N) - \vartheta(N) = \sum_{N < p \leq 2N} \log p \leq \log \binom{2N}{N} \leq \log 2^{2N} = 2N \log 2.$$

In particular,  $\vartheta(2^{k+1}) - \vartheta(2^k) \leq 2^{k+1} \log 2$ . Summing over  $k = 0, \dots, n$  we get

$$\vartheta(2^{n+1}) = \vartheta(2^{n+1}) - \vartheta(1) \leq \log 2 (2 + 2^2 + 2^3 + \dots + 2^{n+1}) < 2^{n+2} \log 2.$$

For generic  $x \geq 1$ , we have  $2^n \leq x < 2^{n+1}$  for some  $n \in \mathbb{N}$ , hence

$$\vartheta(x) \leq \vartheta(2^{n+1}) \leq 2^{n+2} \log 2 \leq (4 \log 2)x.$$

□

The key point in the proof of the Prime Number Theorem is the following non-vanishing result:

**Theorem 1.2.3** (Non-vanishing of  $\zeta$  along  $\Re s = 1$ ). *The function  $\zeta(s)$  does not have any zeroes along the line  $\Re s = 1$ , and the function  $\Phi(s) - \frac{1}{s-1}$  extends to a holomorphic function on the closed<sup>5</sup> right half-plane  $\{\Re s \geq 1\}$ .*

*Proof.* We start by noticing the following formal identity, valid for  $\Re s > 1$ :

$$\log \zeta(s) = \log \prod_p (1 - p^{-s})^{-1} = - \sum_p \log(1 - p^{-s}).$$

Taking the derivative of both sides,

$$\begin{aligned} \frac{\zeta'(s)}{\zeta(s)} &= - \sum_p \frac{\log p \cdot p^{-s}}{1 - p^{-s}} = - \sum_p \frac{\log p}{p^s(1 - p^{-s})} \\ &= - \sum_p \frac{\log p}{p^s} \sum_{k \geq 0} p^{-ks} = - \sum_p \sum_{k \geq 1} \frac{\log p}{p^{ks}} \\ &= - \sum_{n \geq 1} \frac{\Lambda(n)}{n^s}, \end{aligned} \tag{1.2}$$

where  $\Lambda(n)$  is the **von Mangoldt function**,

$$\Lambda(n) = \begin{cases} \log p, & \text{if } n = p^k \text{ for a prime } p \\ 0, & \text{otherwise.} \end{cases}$$

Essentially the same calculation shows

$$\begin{aligned} - \frac{\zeta'(s)}{\zeta(s)} &= \sum_p \frac{\log p}{p^s(1 - p^{-s})} = \sum_p \frac{\log p(1 - p^{-s} + p^{-s})}{p^s(1 - p^{-s})} \\ &= \sum_p \frac{\log p}{p^s} + \sum_p \frac{\log p}{p^s(p^s - 1)} = \Phi(s) + \sum_p \frac{\log p}{p^s(p^s - 1)}, \end{aligned} \tag{1.3}$$

where the sum  $\sum_p \frac{\log p}{p^s(p^s - 1)}$  converges (to a holomorphic function) for  $\Re s > \frac{1}{2}$ . Hence,  $\Phi(s) = - \frac{\zeta'(s)}{\zeta(s)} - \sum_p \frac{\log p}{p^s(p^s - 1)}$  is holomorphic over  $\{\Re s > \frac{1}{2}\}$ , except for the poles of  $\frac{\zeta'(s)}{\zeta(s)}$ , which are  $s = 1$  and the zeros of  $\zeta(s)$ . Indeed, recall that the logarithmic derivative  $f'(s)/f(s)$  of an analytic function  $f(s)$  is analytic except at the zeroes and poles of  $f$ . At each zero (of multiplicity  $m > 0$ ) or pole (of multiplicity  $-m > 0$ ) of  $f(s)$ , the logarithmic derivative has a simple pole with residue  $m$ . Finally, we already know (Theorem 1.1.8) that  $\zeta(s)$  doesn't have any poles apart from  $s = 1$ , hence that  $-\frac{\zeta'(s)}{\zeta(s)} = \frac{1}{s-1} + O(1)$  for  $s$  near 1. We then obtain that  $\Phi(s) - \frac{1}{s-1}$  extends holomorphically to  $\{\Re s \geq 1\}$  if and only if  $\zeta(s)$  does not have any zeroes on the line  $\{\Re s = 1\}$ . We now prove this crucial statement.

Using again the properties of the logarithmic derivative, we obtain that the order of vanishing of  $\zeta(s)$  at  $1 + it$  is given by

$$\text{ord}_{1+it} \zeta = \lim_{\varepsilon \rightarrow 0^+} \varepsilon \frac{\zeta'(1 + it + \varepsilon)}{\zeta(1 + it + \varepsilon)}. \tag{1.4}$$

---

<sup>5</sup>this means that every point in this set has an open neighbourhood on which the function in question is holomorphic. These open neighbourhoods will necessarily contain complex numbers with real part strictly less than 1

Notice furthermore that  $\overline{\zeta(s)} = \zeta(\bar{s})$  since the coefficients of the Dirichlet series defining  $\zeta$  are real. Let  $\alpha$  be a positive real number and denote by  $\mu \geq 0, \nu \geq 0$  the orders of vanishing of  $\zeta$  at  $1 + i\alpha$  and  $1 + 2i\alpha$ . Combining Equations (1.4) and (1.3), and recalling that  $\sum_p \frac{\log p}{p^s(p^s-1)}$  is holomorphic along  $\{\Re s = 1\}$ , we obtain

$$\lim_{\varepsilon \rightarrow 0^+} \varepsilon \Phi(1 + \varepsilon) = 1, \quad \lim_{\varepsilon \rightarrow 0^+} \varepsilon \Phi(1 + \varepsilon \pm i\alpha) = -\mu, \quad \lim_{\varepsilon \rightarrow 0^+} \varepsilon \Phi(1 + \varepsilon \pm 2i\alpha) = -\nu. \quad (1.5)$$

On the other hand, we have the following inequality,

$$\sum_{r=-2}^2 \binom{4}{r+2} \Phi(1 + \varepsilon + ri\alpha) = \sum_p \frac{\log p}{p^{1+\varepsilon}} (p^{i\alpha/2} + p^{-i\alpha/2})^4 \geq 0$$

which follows directly from the definitions, the binomial expansion, and the positivity of squares. Multiplying by  $\varepsilon > 0$ , passing to the limit  $\varepsilon \rightarrow 0^+$  and replacing the values given by (1.5) we finally get

$$-2\nu - 8\mu + 6 \geq 0,$$

which clearly gives  $\mu < 1$ , hence  $\mu = 0$ . By definition of  $\mu$ , this means  $\zeta(1 + i\alpha) \neq 0$ , as desired.  $\square$

**Theorem 1.2.4** (Tauberian theorem). *Let  $f(t) : \mathbb{R}_{\geq 0} \rightarrow \mathbb{C}$  be a bounded, locally integrable function. Suppose that the function  $g(z) = \int_0^\infty f(t)e^{-zt} dt$ , which is defined and holomorphic for  $\Re z > 0$ , extends holomorphically to  $\Re z \geq 0$ . The integral  $\int_0^\infty f(t) dt$  exists and equals  $g(0)$ .*

*Proof.* For  $T > 0$  set  $g_T(z) = \int_0^T f(t)e^{-zt} dt$ . This function is holomorphic on the whole complex plane. We will show that  $\lim_{T \rightarrow \infty} g_T(0) = g(0)$ . Let  $R$  be large and let  $C$  be the boundary of the region  $D = \{z \in \mathbb{C} : |z| \leq R, \Re z \geq -\delta\}$  (see Figure 1.1). Here  $\delta > 0$  is chosen as a function of  $R$  in such a way that  $g_T - g$  is holomorphic inside and on  $C$ .

To show that such a  $\delta$  exists, notice that  $g_T$  is everywhere holomorphic, whereas, by assumption, the function  $g(z)$  is holomorphic along the segment  $I = \{it : -R \leq t \leq R\}$ . Since being holomorphic is an open property, for every point  $z$  of  $I$  there is a small disc centred at  $z$  in which  $g(z)$  is holomorphic. By compactness of  $I$ , a finite union of such discs covers it. We can then take  $\delta$  to be the minimum of the radii of these finitely many discs.

Let  $h_T(z) = (g(z) - g_T(z))e^{zT} \left(1 + \frac{z^2}{R^2}\right)$ . Cauchy's integral formula gives

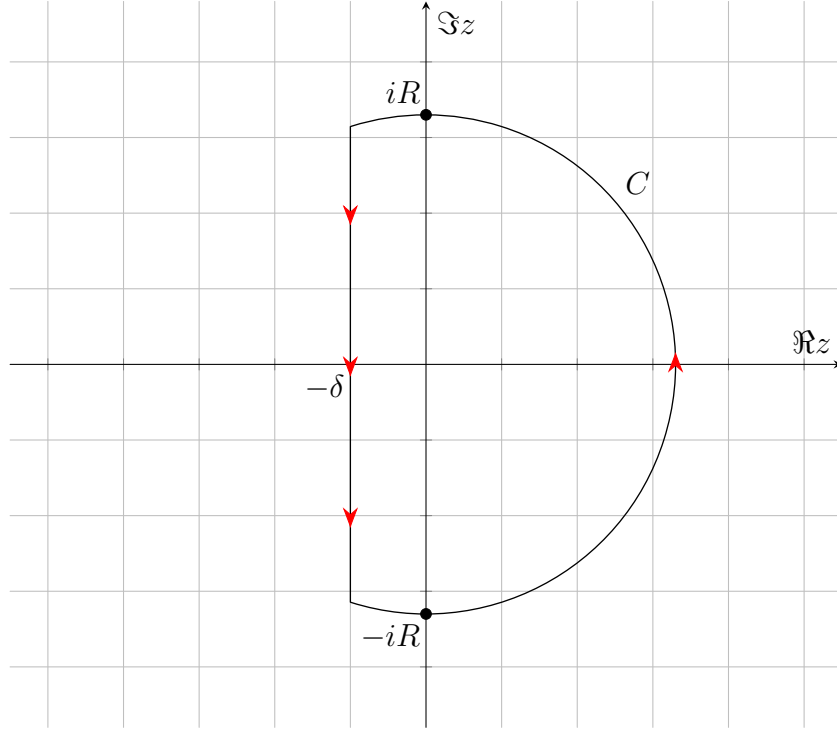
$$h_T(0) = g(0) - g_T(0) = \frac{1}{2\pi i} \int_C (g(z) - g_T(z)) e^{zT} \left(1 + \frac{z^2}{R^2}\right) \frac{dz}{z}.$$

Our aim is to show that  $\lim_{T \rightarrow \infty} h_T(0) = 0$ . We study Cauchy's integral separately along the arcs

$$C_+ := C \cap \{\Re z > 0\} \quad \text{and} \quad C_- := C \cap \{\Re z < 0\}.$$

Along  $C_+$  we have

$$\begin{aligned} |g(z) - g_T(z)| &= \left| \int_T^\infty f(t)e^{-zt} dt \right| \leq \int_T^\infty |f(t)| |e^{-zt}| dt = \\ &\leq \|f\|_\infty \int_T^\infty |e^{-zt}| dt = \frac{\|f\|_\infty e^{-\Re z T}}{\Re z}. \end{aligned} \quad (1.6)$$

Figure 1.1: The contour  $C$ 

Note also that (by essentially the same calculation as in Equation (1.6)) when  $\Re z$  is negative we have  $|g_T(z)| \leq \frac{\|f\|_\infty e^{-\Re(z)T}}{|\Re z|}$ . Furthermore, all along the circle  $|z| = R$  we can estimate

$$\begin{aligned} \left| e^{zT} \left( 1 + \frac{z^2}{R^2} \right) \frac{1}{z} \right| &= e^{\Re(z)T} \left| \left( \frac{|z|^2}{z} + z \right) \frac{1}{R^2} \right| \\ &= \frac{e^{\Re(z)T}}{R^2} |\bar{z} + z| = \frac{2|\Re z|}{R^2} e^{\Re(z)T}. \end{aligned} \quad (1.7)$$

Hence, the integral of  $h_T(z)$  along  $C_+$  is bounded in absolute value by

$$\|f\|_\infty \cdot \frac{2}{R^2} \cdot (\pi R) = \frac{2\pi\|f\|_\infty}{R}.$$

In particular, we see that the contribution from the integral along  $C_+$  vanishes in the limit  $R \rightarrow \infty$ .

We now consider the integral along  $C_-$ , separating the contributions from  $g(z)$  and  $g_T(z)$ . As for  $g_T(z)$ , which is entire, we can deform the integration contour to the semi-circle  $D_- := \{|z| = R, \Re z < 0\}$ . Along this semi-circle we can use the estimates  $|g_T(z)| \leq \frac{\|f\|_\infty e^{-\Re(z)T}}{|\Re z|}$  and (1.7) to obtain as above

$$\left| \int_{D_-} g_T(z) e^{zT} \left( 1 + \frac{z^2}{R^2} \right) \frac{1}{z} dz \right| \leq \frac{2\pi\|f\|_\infty}{R}.$$

This quantity also vanishes in the limit  $R \rightarrow \infty$ , so we are left with considering the integral  $\int_{C_-} g(z) e^{zT} \left( 1 + \frac{z^2}{R^2} \right) \frac{dz}{z}$ . We will show that this integral vanishes in the limit  $T \rightarrow \infty$  (note



that here we take the limit in  $T$ , not in  $R$ : this contribution vanishes also for fixed, finite values of  $R$ , provided that  $T$  is taken large enough). To handle this integral, note that the function  $T \mapsto |g(z)e^{zT} \left(1 + \frac{z^2}{R^2}\right) \frac{1}{z}|$  is decreasing (since  $|e^{zT}| = e^{-|\Re(z)T|}$ ), and it is integrable (even holomorphic) for any fixed value of  $T$ . By the dominated convergence theorem, we obtain

$$\lim_{T \rightarrow \infty} \int_{C_-} g(z)e^{zT} \left(1 + \frac{z^2}{R^2}\right) \frac{dz}{z} = \int_{C_-} \lim_{T \rightarrow \infty} g(z)e^{zT} \left(1 + \frac{z^2}{R^2}\right) \frac{dz}{z} = \int_{C_-} 0 \, dz = 0,$$

where we have used the pointwise convergence of  $g(z)e^{zT} \left(1 + \frac{z^2}{R^2}\right) \frac{1}{z}$  to 0 (which again follows from  $\Re z < 0$  along  $C_-$ ). We have thus proved that  $\lim_{T \rightarrow \infty} |h_T(0)| \leq \frac{4\pi}{R} \|f\|_\infty$ . As  $R$  is arbitrary, this shows  $\lim_{T \rightarrow \infty} h_T(0) = 0$ , as desired.  $\square$

To prove our next result we will need Abel's summation by parts formula:

**Theorem 1.2.5** (Abel's summation by parts). *Let  $(a_n)_{n \geq 1}$  be a sequence of complex numbers and let  $\varphi : [1, \infty) \rightarrow \mathbb{R}$  be a  $C^1$  function. For all  $x > 1$  we have*

$$\sum_{n \leq x} a_n \varphi(n) = \left( \sum_{n \leq x} a_n \right) \varphi(x) - \int_1^x \left( \sum_{n \leq t} a_n \right) \varphi'(t) \, dt.$$

*Proof.* This is elementary, but we give an unforgettable (!) proof using distributions, which shows that this is *exactly* (and not just philosophically) the integration-by-parts formula. Consider the function  $A(x) = \sum_{n \leq x} a_n$ . This function is constant on all intervals of the form  $[n, n+1)$ . Its derivative (in the distributional sense) is concentrated on the integers, and it is easy to see that it is  $\sum_n a_n \delta(x-n)$ , where  $\delta$  is Dirac's delta. Since integration by parts works for distributions, we get (for any  $\varepsilon \in (0, 1)$ )

$$\begin{aligned} \sum_{n \leq x} a_n \varphi(n) &= \sum_n a_n \int_{1-\varepsilon}^x \delta(t-n) \varphi(t) \, dt = \int_{1-\varepsilon}^x \sum_n a_n \delta(t-n) \varphi(t) \, dt \\ &= \int_{1-\varepsilon}^x A'(t) \varphi(t) \, dt = [A(t) \varphi(t)]_{1-\varepsilon}^x - \int_{1-\varepsilon}^x A(t) \varphi'(t) \, dt \\ &= \left( \sum_{n \leq x} a_n \right) \varphi(x) - \int_1^x A(t) \varphi'(t) \, dt, \end{aligned}$$

where we have used  $A(1-\varepsilon) = 0$  for any  $\varepsilon > 0$ . Passing to the limit  $\varepsilon \rightarrow 0^+$  yields the result.  $\square$

**Proposition 1.2.6.** *The integral*

$$\int_1^\infty \frac{\vartheta(t) - t}{t^2} \, dt$$

*converges.*

*Proof.* We fix  $s > 1$  and apply Theorem 1.2.5 to the sequence

$$a_n = \begin{cases} \log n, & \text{if } n \text{ is a prime number;} \\ 0, & \text{otherwise} \end{cases}$$

and to the function  $\varphi(x) = x^{-s}$ . By definition, the function  $\sum_{n \leq x} a_n$  coincides with  $\vartheta(x)$ . Abel's formula yields

$$\sum_{p \leq x} \frac{\log p}{p^s} = \frac{1}{x^s} \sum_{p \leq x} \log p + s \int_1^x \frac{\vartheta(t)}{t^{s+1}} dt.$$

Letting  $x \rightarrow \infty$  we obtain

$$\Phi(s) = \lim_{x \rightarrow \infty} \frac{1}{x^s} \vartheta(x) + s \int_1^\infty \frac{\vartheta(t)}{t^{s+1}} dt,$$

and by Proposition 1.2.2 we have  $\lim_{x \rightarrow \infty} \frac{1}{x^s} \vartheta(x) = 0$  since  $s > 1$ . Thus, we have

$$\Phi(s) = s \int_1^\infty \frac{\vartheta(t)}{t^{s+1}} dt.$$

The exponential change of variables  $t = e^u$  allows us to rewrite this as

$$\Phi(s) = s \int_0^\infty \vartheta(e^u) e^{-us} du. \quad (1.8)$$

Note that we have proved this for  $s \in \mathbb{R}_{>1}$ , but by analytic continuation the two sides of this equation coincide wherever both are defined and analytic.

We now apply Theorem 1.2.4 to the functions

$$f(t) = \vartheta(e^t) e^{-t} - 1, \quad g(z) = \frac{\Phi(z+1)}{z+1} - \frac{1}{z}.$$

We check the assumptions:

1.  $f(t)$  is bounded and locally integrable: we know that  $\vartheta(e^t) = O(e^t)$  by Proposition 1.2.2, which shows that  $f(t)$  is bounded, and  $\vartheta(e^t), e^{-t}$  are certainly locally integrable.
2. Next we need to check that  $\int_0^\infty f(t) e^{-zt} dt = g(z)$  in  $\{\Re z > 0\}$ , and that  $g(z)$  extends holomorphically to  $\{\Re z \geq 0\}$ . We have

$$\int_0^\infty f(t) e^{-zt} dt = \int_0^\infty (\vartheta(e^t) e^{-t} - 1) e^{-zt} dt = \int_0^\infty \vartheta(e^t) e^{-(z+1)t} dt - \int_0^\infty e^{-zt} dt.$$

From Equation (1.8) we know that  $\int_0^\infty \vartheta(e^t) e^{-(z+1)t} dt = \frac{\Phi(z+1)}{z+1}$  whenever  $\Re(z+1) > 1$ , that is,  $\Re z > 0$ . The integral  $\int_0^\infty e^{-zt} dt$  is immediate to compute, and evaluates to  $\left[ \frac{e^{-zt}}{-z} \right]_0^\infty = \frac{1}{z}$ . Thus, the functions  $\int_0^\infty f(t) e^{-zt} dt$  and  $g(z)$  coincide for all  $z$  with  $\Re z > 0$ . On the other hand, the crucial Theorem 1.2.3 implies that  $g(z)$  has analytic continuation to  $\{\Re z \geq 0\}$ : indeed, we know that  $\Phi(z) - \frac{1}{z-1}$  is analytic in  $\{\Re z \geq 1\}$ , hence  $\Phi(z+1) - \frac{1}{z}$  is analytic in  $\{\Re z \geq 0\}$ . Multiplying by  $\frac{1}{z+1}$ , which is analytic in  $\{\Re z \geq 0\}$ , we obtain that

$$\frac{\Phi(z+1)}{z+1} - \frac{1}{z(z+1)}$$

is also analytic on the same set. The difference between this function and  $\frac{\Phi(z+1)}{z+1} - \frac{1}{z}$  is

$$\frac{1}{z} - \frac{1}{z(z+1)} = \frac{1}{z+1},$$

which is also analytic in  $\{\Re z \geq 0\}$ .

The conclusion of the theorem is that  $\int_0^\infty f(t) dt$  exists, that is, the integral

$$\int_0^\infty (\vartheta(e^t)e^{-t} - 1) dt$$

is convergent. Substituting back  $t = \log u$ , we obtain that

$$\int_1^\infty \left( \frac{\vartheta(u)}{u} - 1 \right) \frac{du}{u}$$

converges, which (up to renaming  $u$  to  $t$ ) is exactly the statement of the proposition.  $\square$

**Proposition 1.2.7.** *The function  $\vartheta(x)$  is asymptotic to  $x$  as  $x \rightarrow \infty$ .*

*Proof.* This follows from Proposition 1.2.6. More precisely, suppose by contradiction that there exists  $\lambda > 1$  such that  $\frac{\vartheta(x_n)}{x_n} > \lambda$  for a sequence  $x_n$  going to infinity. Since  $\vartheta(x)$  is clearly monotonically increasing, we obtain

$$\begin{aligned} \int_{x_n}^{\lambda x_n} \frac{\vartheta(t) - t}{t^2} dt &\geq \int_{x_n}^{\lambda x_n} \frac{\vartheta(x_n) - t}{t^2} dt \geq \int_{x_n}^{\lambda x_n} \frac{\lambda x_n - t}{t^2} dt \\ &\stackrel{t=yx_n}{=} \int_1^\lambda \frac{\lambda x_n - yx_n}{(yx_n)^2} x_n dy = \int_1^\lambda \frac{\lambda - y}{y^2} dy. \end{aligned}$$

This is a contradiction: convergence of the integral  $\int_1^\infty \frac{\vartheta(t)-t}{t^2} dt$  implies that the ‘partial tail’  $\int_x^{\lambda x} \frac{\vartheta(t)-t}{t^2} dx$  can be made arbitrarily small by choosing  $x$  large enough.

Conversely, suppose that for some  $\lambda < 1$  there is an unbounded sequence  $x_n$  such that  $\frac{\vartheta(x_n)}{x_n} < \lambda$ . Reasoning as above, we obtain

$$\int_{x_n}^{\lambda x_n} \frac{\vartheta(t) - t}{t^2} dt \leq \int_1^\lambda \frac{\lambda - y}{y^2} dy < 0,$$

which is again a contradiction.  $\square$

*Proof of Theorem 1.2.1.* On the one hand, we have

$$\vartheta(x) = \sum_{p \leq x} \log p \leq \sum_{p \leq x} \log x = \pi(x) \log(x),$$

while on the other we also have

$$\begin{aligned} \vartheta(x) &\geq \sum_{x^{1-\varepsilon} \leq p \leq x} \log p \geq \sum_{x^{1-\varepsilon} \leq p \leq x} (1 - \varepsilon) \log x \\ &= (1 - \varepsilon) \log x \left( \sum_{x^{1-\varepsilon} \leq p \leq x} 1 \right) = (1 - \varepsilon) \log x (\pi(x) - \pi(x^{1-\varepsilon})). \end{aligned}$$

Since clearly  $\pi(x^{1-\varepsilon}) \leq x^{1-\varepsilon} = O(x^{1-\varepsilon})$ , we have obtained

$$(1 - \varepsilon) \log(x) (\pi(x) + O(x^{1-\varepsilon})) \leq \vartheta(x) \leq \pi(x) \log(x).$$

Dividing through by  $x$  and using Proposition 1.2.7 we get

$$(1 - \varepsilon) \left( \frac{\pi(x)}{x/\log x} + o(1) \right) \leq 1 + o(1) \leq \frac{\pi(x)}{x/\log x} \quad \text{as } x \rightarrow \infty,$$

which (since  $\varepsilon$  is arbitrary) implies the theorem.  $\square$

### 1.2.1 The Riemann–von Mangoldt exact formula

Even though this is not strictly speaking a course in analytic number theory, I would be remiss if I did not (try to) explain more carefully the role of the zeros of the  $\zeta$  function in controlling the distribution of primes. We will not give full proofs, but hopefully the content of this section will be enough to convince you that information on the distribution of the zeros of  $\zeta$  translates fairly directly into information on the distribution of the prime numbers. To make this concrete, we state and sketch a proof of an exact formula for a close relative of the function  $\vartheta$ :

**Theorem 1.2.8** (Riemann–von Mangoldt exact formula). *For every non-integer  $x$  we have*

$$\sum_{n \leq x} \Lambda(n) = x - \lim_{T \rightarrow \infty} \sum_{\rho: |\operatorname{Im}(\rho)| \leq T} \frac{x^\rho}{\rho} - \log(2\pi) - \frac{1}{2} \log(1 - x^{-2}),$$

where the sum ranges over the zeroes of  $\zeta$  in the critical strip  $\Re s \in [0, 1]$ .

**Remark 1.2.9.** Let  $\Theta(x) := \sum_{n \leq x} \Lambda(n)$ . The difference  $\Theta(x) - \vartheta(x)$  is given by

$$\sum_{p \leq x} \sum_{\substack{n \geq 2 \text{ such} \\ \text{that } p^n \leq x}} \log(p) = \sum_{n=2}^{\log_2(x)} \sum_{p \leq x^{1/n}} \log p = \sum_{n=2}^{\log_2(x)} \vartheta(x^{1/n}) \ll x^{1/2} \log(x),$$

where we have used Proposition 1.2.2. Thus, precise estimates on  $\Theta(x)$  lead to precise estimates on the function  $\vartheta(x)$ , which – as we have seen – is intimately tied to the actual distribution of prime numbers.

The following sketch is very rough (we ignore a number of problems related to the convergence and well-posedness of integrals and sums), but I hope it gives an idea of the inextricably close connection between the distribution of prime numbers (in the form of  $\Lambda(n)$ ) and  $\zeta(s)$ .

*Sketch of proof of Theorem 1.2.8.* Setting aside the analytic difficulties, the key point lies in an application of Perron’s formula (see Exercise 1.2.10 below). In particular, we start from the equality

$$\sum_{n \geq 1} \frac{\Lambda(n)}{n^s} = -\frac{\zeta'(s)}{\zeta(s)}$$

that we obtained in Equation (1.2). Setting  $g(s) = -\frac{\zeta'(s)}{\zeta(s)}$  in Perron’s formula, we get

$$\Theta(x) = \sum_{n \leq x} \Lambda(n) = - \int_{c-i\infty}^{c+i\infty} \frac{\zeta'(z)}{\zeta(z)} \frac{x^z}{z} dz.$$

Now, using the residue theorem, shift the integration contour from  $c + i\mathbb{R}$  (where  $c$ , in order to use Perron’s formula, is taken to be  $> 1$ ) to  $-R + i\mathbb{R}$  (and then take the limit  $R \rightarrow \infty$ ). In so doing, by the residue theorem, we pick up a correction term every time we cross a pole  $\rho$  of  $\frac{\zeta'}{\zeta}$ ; these corrections are of the form  $-2\pi i \operatorname{Res}_{z=\rho} \left( \frac{\zeta'(z)}{\zeta(z)} \frac{x^z}{z} \right)$ , contribution which then gets divided by the factor  $2\pi i$  in Perron’s formula.

The poles of  $\zeta'/\zeta$  are precisely the poles of  $\zeta$  (of which there is one, at  $z = 1$ ) and its zeroes (of which there are many...). The term corresponding to the pole gives a residue of 1 for  $-\zeta'/\zeta$ ,

which – multiplied by  $x^z/z$  at  $z = 1 -$  gives a contribution of  $x$ . Each zero  $\rho$ , on the other hand, gives a residue of  $-1$  for  $\zeta'/\zeta$ , which – when multiplied by  $\frac{x^z}{z}|_{z=\rho} = \frac{x^\rho}{\rho}$  – gives the contribution  $x^\rho/\rho$  in the Riemann-von Mangoldt exact formula.

If you want to understand the (bounded) terms  $\log(2\pi)$  and  $\frac{1}{2}\log(1-x^{-2})$  you should read a complete proof of the theorem, for example at Terence Tao's blog [Tao21]. I will simply point out that these additional contributions come from working with the completed  $\zeta$  function of Definition 1.1.7 instead of  $\zeta$  itself.  $\square$

**Exercise 1.2.10** (Perron's formula). Let

$$g(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

be a Dirichlet series. Assume that it converges uniformly for  $\Re(s) > \sigma$ , and let  $x > 0$  be a real number which is *not* an integer. Also fix  $c > \max\{0, \sigma\}$ . We have

$$\sum_{n \leq x} a_n = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} g(z) \frac{x^z}{z} dz.$$

**Remark 1.2.11** (Prime Number Theorem under the Riemann Hypothesis). This remark is even less precise than the proof sketch given above, but my conscience doesn't let me *not* mention the Riemann hypothesis. As just about everyone knows, this is the statement that all the zeroes of  $\zeta(s)$  in the 'critical strip'  $\{0 < \Re(s) < 1\}$  have real part equal to  $\frac{1}{2}$ . In particular, for every zero  $\rho$  of  $\zeta$  in this strip we have  $|x^\rho| = x^{1/2}$ . Assuming that the Riemann hypothesis holds, and ignoring again all sorts of analytic difficulties, we then see from Theorem 1.2.8 that

$$\sum_{n \leq x} \Lambda(n) = x + O\left(\sum_{\rho} \frac{x^{1/2}}{|\rho|}\right).$$

Since one can show that there aren't too many zeroes of  $\zeta$  in the critical strip, this leads to

$$\sum_{n \leq x} \Lambda(n) = x + O(x^{1/2+\varepsilon}).$$

Recalling Remark 1.2.9 we then get  $\vartheta(x) = x + O(x^{1/2+\varepsilon})$ , which in turn leads to a strong form of Theorem 1.2.1, namely,  $\pi(x) = \frac{x}{\log x} + O_\varepsilon(x^{1/2+\varepsilon})$  for every  $\varepsilon > 0$ .

## 1.3 Review of algebraic number theory

Our next main objective is to prove Dirichlet's theorem on primes in arithmetic progressions. Before doing this, however, we want to give a unified interpretation of all the  $L$ -functions we have seen this far in terms of Galois representations. This requires a fair amount of basic algebraic number theory, which we now review. All results in this section are standard, so we will not provide proofs (for which the reader can refer to [Mar18]). The reader familiar with the basics of algebraic number theory can safely skip to Section 1.4.

### 1.3.1 Structure of the ring of integers

We have already met the notion of *ring of integers* of a number field, see Definition 1.1.13. It is useful to recall that, if  $K$  is a number field of degree  $n = [K : \mathbb{Q}]$ , the ring  $\mathcal{O}_K$  is isomorphic as an additive group to the free group  $\mathbb{Z}^n$ . Thus, one can fix a  $\mathbb{Z}$ -basis  $\alpha_1, \dots, \alpha_n$  of  $\mathcal{O}_K$ ; any two  $\mathbb{Z}$ -basis are related by a base-change matrix in  $\mathrm{GL}_n(\mathbb{Z})$ . We denote by  $\sigma_1, \dots, \sigma_n$  the embeddings of  $K$  into  $\mathbb{C}$ .

**Definition 1.3.1** (Discriminant). The **discriminant** of  $K$  is

$$d_K := \det(\sigma_i(\alpha_j))^2.$$

It is an integer independent of the choice of the basis  $\alpha_1, \dots, \alpha_n$ .

**Example 1.3.2.** For  $K = \mathbb{Q}(\sqrt{2})$  one has  $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$ , hence we can take  $\alpha_1 = 1$  and  $\alpha_2 = \sqrt{2}$ . The discriminant is therefore

$$d_K = \det \begin{pmatrix} 1 & \sqrt{2} \\ 1 & -\sqrt{2} \end{pmatrix}^2 = (-2\sqrt{2})^2 = 8.$$

### 1.3.2 Unique factorisation of ideals

The ring  $\mathcal{O}_K$  enjoys the following properties:

**Theorem 1.3.3.**

1. If  $I$  is any non-zero ideal of  $\mathcal{O}_K$ , the quotient  $\mathcal{O}_K/I$  is finite. The cardinality of  $\mathcal{O}_K/I$  is called the **norm** of  $I$ , see Definition 1.1.14. The ideal norm is multiplicative: if  $I = I_1 I_2$ , then  $N(I) = N(I_1)N(I_2)$ .
2. Non-zero prime ideals of  $\mathcal{O}_K$  are maximal. Every primary ideal of  $\mathcal{O}_K$  is the power of a prime ideal. The norm of a prime ideal is of the form  $p^f$ , where  $p \in \mathbb{Z}$  is prime and  $f$  is a positive integer.
3. Every non-zero ideal  $I$  of  $\mathcal{O}_K$  factors uniquely (up to reordering the factors) as a product  $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$  of prime ideals  $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ .
4. In particular, if  $I = \prod_i \mathfrak{p}_i^{e_i}$  and  $N(\mathfrak{p}_i) = p_i^{f_i}$  for every  $i$ , then

$$N(I) = N \left( \prod_i \mathfrak{p}_i^{e_i} \right) = \prod_i p_i^{e_i f_i}.$$

### 1.3.3 Splitting of primes

Let  $\mathfrak{p}$  be a non-zero prime ideal of  $\mathcal{O}_K$ . The contraction  $\mathfrak{p} \cap \mathbb{Z}$  is a non-zero prime ideal of  $\mathbb{Z}$ , so it is of the form  $(p)$ . We say that  $\mathfrak{p}$  lies over  $p$ , or equivalently, that  $p$  lies under  $\mathfrak{p}$  (the terminology is justified, at least *a posteriori*, by the scheme-theoretic interpretation: there is a natural map  $\mathrm{Spec} \mathcal{O}_K \rightarrow \mathrm{Spec} \mathbb{Z}$ , which we can think of as a ramified cover, and the point  $(p)$  is the image of the point  $\mathfrak{p}$  for this topological map, which is usually drawn with  $\mathrm{Spec} \mathcal{O}_K$  lying above  $\mathrm{Spec} \mathbb{Z}$ ).

Conversely, starting from a non-zero prime  $(p)$  of  $\mathbb{Z}$ , one can factor the ideal  $(p)\mathcal{O}_K$  using Theorem 1.3.3 to obtain an expression of the form

$$(p)\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

We say that  $\mathfrak{p}_1, \dots, \mathfrak{p}_r$  are the **primes of  $\mathcal{O}_K$  lying over  $(p)$** , that  $e_i$  is the **ramification index of  $\mathfrak{p}_i$  over  $p$** , and that the exponent  $f_i$  defined by  $N(\mathfrak{p}_i) = p^{f_i}$  is the **inertia degree of  $\mathfrak{p}_i$  over  $p$** . One can easily show that  $f_i$  is also the degree of the field extension  $\frac{\mathcal{O}_K}{\mathfrak{p}_i} / \mathbb{F}_p$ . The field  $\frac{\mathcal{O}_K}{\mathfrak{p}_i}$  is called the **residue field of (or at)  $\mathfrak{p}_i$** . Borrowing the standard notation from scheme theory, we will denote it by  $\kappa(\mathfrak{p}_i)$ .

There is also a fundamental formula, which is ultimately a consequence of the flatness<sup>6</sup> of  $\mathcal{O}_K$  over  $\mathbb{Z}$ , relating the invariants  $e_i, f_i$  with the degree  $[K : \mathbb{Q}]$ .

**Theorem 1.3.4.** *Let  $p$  be a prime of  $\mathbb{Z}$  and write  $p = \prod_{i=1}^r \mathfrak{p}_i^{e_i}$  for the factorisation of  $p$  in  $\mathcal{O}_K$ . Letting  $f_i$  be the inertia degree of  $\mathfrak{p}_i$  over  $p$ , we have*

$$\sum_{i=1}^r e_i f_i = [K : \mathbb{Q}].$$

Consider now the relative setting of an extension  $L/K$ , and let  $\mathfrak{p}$  be a prime of  $\mathcal{O}_K$ . As above, one may factor  $\mathfrak{p}\mathcal{O}_L$  as  $\prod_{i=1}^r \mathfrak{P}_i^{e_i}$ , and we say that the  $\mathfrak{P}_i$  are the primes of  $\mathcal{O}_L$  (or, more informally, of  $L$ ) lying over  $\mathfrak{p}$ . We call  $e_i$  the **ramification index of  $\mathfrak{P}_i$  over  $\mathfrak{p}$** , and define  $f_i$  as

$$f_i = [\kappa(\mathfrak{P}_i) : \kappa(\mathfrak{p})], \quad (1.9)$$

that is, the degree of the extension between the residue fields at  $\mathfrak{P}_i$  and at  $\mathfrak{p}$ . The analogue of Theorem 1.3.4 in this setting is as follows.

**Theorem 1.3.5.** *With the above notation we have*

$$\sum_{i=1}^r e_i f_i = [L : K].$$

We say that a prime ideal  $\mathfrak{p}$  of  $\mathcal{O}_K$  **ramifies** in  $L$  if in the factorisation  $\mathfrak{p}\mathcal{O}_L = \prod_i \mathfrak{P}_i^{e_i}$  at least one exponent  $e_i$  is strictly greater than 1. When this is the case, we say more precisely that the prime  $\mathfrak{P}_i$  is ramified in the extension  $L/K$ .

**Remark 1.3.6.** It would be more precise to always speak of the extension  $\mathcal{O}_L/\mathcal{O}_K$ . However, it is both traditional and quite practical to talk about the extension  $L/K$  (secretly meaning the corresponding extension of rings of integers), just like it is common use to write *primes of  $L$*  instead of *primes of  $\mathcal{O}_L$* .

Finally, a fundamental fact is that only finitely many primes ramify in any given (finite) extension  $L/K$ :

**Theorem 1.3.7.** *Let  $L/K$  be an extension of number fields<sup>7</sup>. The set of primes  $\mathfrak{p}$  of  $\mathcal{O}_L$  that are ramified in  $L/K$  is finite.*

<sup>6</sup>since the local rings of  $\mathbb{Z}$  are all PIDs, flatness is equivalent to torsion-freeness, which is obvious

<sup>7</sup>by definition, a number field is a finite extension of  $\mathbb{Q}$ . As a consequence, any extension of number fields is automatically finite.

The following theorem is also often useful:

**Theorem 1.3.8** (Minkowski). *The only number field  $K$  such that no prime of  $\mathbb{Q}$  ramifies in  $K$  is  $K = \mathbb{Q}$  itself.*

### 1.3.4 Galois action on the primes

We now specialise to the case of  $L/K$  being Galois, with group  $G$ . In this case, there is an obvious action of  $G$  on  $\mathcal{O}_L$ : indeed, it is clear from the definition that if  $\alpha \in L$  is an algebraic integer and  $\sigma$  is any element of  $G$ , then  $\sigma(\alpha)$  is still an algebraic integer.

Let  $\mathfrak{p}$  be a prime of  $\mathcal{O}_K$  and let  $\mathfrak{P}$  be a prime of  $\mathcal{O}_L$  lying over  $\mathfrak{p}$ . For every  $\sigma \in G$  we have

$$\sigma(\mathfrak{P}) \cap \mathcal{O}_K = \sigma(\mathfrak{P} \cap \mathcal{O}_K) = \sigma(\mathfrak{p}) = \mathfrak{p},$$

so  $\sigma(\mathfrak{P})$  is another prime ideal of  $\mathcal{O}_L$  lying over  $\mathfrak{p}$ : the Galois action permutes the primes of  $L$  over  $\mathfrak{p}$ . This action has many nice properties:

**Theorem 1.3.9** (Galois action on the primes). *Let  $\mathfrak{p}$  be a prime of  $\mathcal{O}_K$  and denote by  $X = \{\mathfrak{P}_1, \dots, \mathfrak{P}_r\}$  the set of primes of  $\mathcal{O}_L$  lying over  $\mathfrak{p}$ .*

1.  $G$  acts transitively on  $X$ .
2. Let  $D_i = D(\mathfrak{P}_i | \mathfrak{p})$  be the stabiliser of  $\mathfrak{P}_i$  for this action. The groups  $D_i$  are all conjugate to each other, and  $r = [G : D_i]$  for every  $i$ . We call  $D_i$  the **decomposition group** of  $\mathfrak{P}_i$  over  $\mathfrak{p}$ .
3. Let  $I_i = \{\sigma \in G : \sigma(x) \equiv x \pmod{\mathfrak{P}_i} \forall x \in \mathcal{O}_L\}$ . The group  $I_i$ , called the **inertia group** of  $\mathfrak{P}_i$ , is normal in  $D_i$ , and there is a canonical isomorphism

$$\frac{D_i}{I_i} \cong \text{Gal}(\kappa(\mathfrak{P}_i) / \kappa(\mathfrak{p})).$$

We will denote  $I_i$  by  $I(\mathfrak{P}_i | \mathfrak{p})$ .

4. The group  $I_i$  is trivial whenever  $\mathfrak{P}_i$  is unramified over  $\mathfrak{p}$ .

**Remark 1.3.10.** Even though we will not prove this, note that part (2) is an obvious consequence of (1) and standard facts about group actions.

It is not hard to see that the transitivity of the action (Theorem 1.3.9 (1)) implies that all the ramification indices  $e_i$  are equal to each other and all the inertia degrees  $f_i$  are equal to each other. Writing  $e, f$  for their common values, the formula of Theorem 1.3.5 takes the simple form

$$[L : K] = r \cdot e \cdot f. \tag{1.10}$$



### 1.3.5 Frobenius elements

We now come to the real protagonists of this section, namely, Frobenius elements in Galois groups. We keep the setup of the previous section, namely, we let  $L/K$  be a Galois extension with group  $G$ . Let  $\mathfrak{p}$  be a prime of  $K$  that is unramified in  $L$  and let  $\mathfrak{P}$  be a prime of  $L$  lying over it. Let  $f$  be the inertia degree of  $\mathfrak{P}$  over  $\mathfrak{p}$  (note that  $e = 1$  since  $\mathfrak{P}$  is unramified).

The group  $\text{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$  is cyclic of order  $f$ , generated by the Frobenius automorphism  $\text{Frob} : x \mapsto x^{N(\mathfrak{p})}$ . Using the assumption  $e = 1$  and Theorem 1.3.9 (4), we see that the inertia group  $I := I(\mathfrak{P} | \mathfrak{p})$  is trivial. The isomorphism of Theorem 1.3.9 (3) then shows that  $\text{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$  is canonically isomorphic to the decomposition group  $D := D(\mathfrak{P} | \mathfrak{p})$ . In particular,  $\text{Frob} \in \text{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$  corresponds to a unique element  $\text{Frob}_{\mathfrak{P}} \in D \subseteq G$ . The following all-important definition will be crucial for us.

**Definition 1.3.11** (Artin symbol). Let  $\mathfrak{p}$  be a prime of  $\mathcal{O}_K$  and let  $\mathfrak{P}$  be a prime of  $\mathcal{O}_L$  lying over it. Suppose that  $\mathfrak{P}$  is unramified over  $\mathfrak{p}$ . We let

$$\left( \frac{L/K}{\mathfrak{P}} \right)$$

denote the element  $\text{Frob}_{\mathfrak{P}} \in G$  constructed above. The element  $\left( \frac{L/K}{\mathfrak{P}} \right)$  is called the **Artin symbol** of  $\mathfrak{P}$  in the extension  $L/K$ , and is often also called the **Frobenius (element) at  $\mathfrak{P}$** . More generally, when  $\mathfrak{p}$  is ramified and  $\mathfrak{P}$  is a prime lying over  $\mathfrak{p}$ , we say that  $g \in G$  is a **Frobenius element at  $\mathfrak{P}$**  if it lies in  $D$  and its image in  $D/I \cong \text{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$  is the Frobenius automorphism of the residue field. We will also denote by  $\left( \frac{L/K}{\mathfrak{P}} \right)$  any such Frobenius element.

**Remark 1.3.12.** Unwinding the definitions, we see that  $\left( \frac{L/K}{\mathfrak{P}} \right)$  is the unique element  $\sigma \in G$  that satisfies

$$\sigma(x) \equiv x^{N(\mathfrak{p})} \pmod{\mathfrak{P}} \quad (1.11)$$

for all  $x \in \mathcal{O}_L$ .

**Remark 1.3.13.** When  $\mathfrak{P}$  is ramified over  $\mathfrak{p}$ , there are several choices for a Frobenius element at  $\mathfrak{P}$ . However, by definition, they all lie in  $D$  and they all have the same image in  $D/I$ , and therefore, given any two choices  $g, g'$  of elements of  $G$  that are Frobenii at  $\mathfrak{P}$  there exists an  $h \in I$  such that  $g = g'h$ .

**Remark 1.3.14.** Suppose  $\mathfrak{P}'$  is a different prime of  $\mathcal{O}_L$  lying over  $\mathfrak{p}$ . By Theorem 1.3.9 (1), there is an element  $\sigma \in G$  such that  $\mathfrak{P}' = \sigma\mathfrak{P}$ . It is then easy to check that

$$\left( \frac{L/K}{\mathfrak{P}'} \right) = \sigma \left( \frac{L/K}{\mathfrak{P}} \right) \sigma^{-1} :$$

indeed, this follows easily from the characterisation given in Equation (1.11).

Remark 1.3.14 allows us to define an ‘Artin symbol’ that only depends on  $\mathfrak{p}$  and not on  $\mathfrak{P}$ :

**Definition 1.3.15** (Conjugacy class of Frobenius). Let  $L/K$  be a Galois extension of number fields with group  $G$ . Let  $\mathfrak{p}$  be a prime of  $\mathcal{O}_K$  unramified in  $L$ . We define

$$\left( \frac{L/K}{\mathfrak{p}} \right)$$

as the *conjugacy class* in  $G$  of the Artin symbol  $\left( \frac{L/K}{\mathfrak{P}} \right)$ , where  $\mathfrak{P}$  is any prime of  $L$  lying over  $\mathfrak{p}$ . We will often write  $\text{Frob}_{\mathfrak{p}}$  for this conjugacy class, or for any element of it if the choice of the element does not make any difference.

**Remark 1.3.16.** The following special case is particularly interesting: if  $L/K$  is an *abelian* extension, that is, it is a Galois extension whose group is commutative, then conjugacy classes consist of a single element. *In this special case*, the Artin symbol of Definition 1.3.15 can be identified to a specific element of the Galois group.

**Example 1.3.17** (Frobenius elements for the cyclotomic extensions). *Consider the Galois extension  $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ , with group  $G \cong (\mathbb{Z}/n\mathbb{Z})^\times$ . Recall that, under this isomorphism, the residue class  $a \in (\mathbb{Z}/n\mathbb{Z})^\times$  corresponds to the unique automorphism  $\sigma_a$  of  $\mathbb{Q}(\zeta_n)$  that sends  $\zeta_n$  to  $\zeta_n^a$ .*

*The primes that ramify in  $\mathbb{Q}(\zeta_n)$  are precisely those that divide  $n$ . Let  $p$  be any other prime, and let  $\mathfrak{p}$  be a prime of  $\mathbb{Q}(\zeta_n)$  lying over  $p$ . By Equation (1.11), the Artin symbol  $\left( \frac{\mathbb{Q}(\zeta_n)/\mathbb{Q}}{\mathfrak{p}} \right)$  is the unique  $\sigma \in G$  such that*

$$\sigma(x) \equiv x^p \pmod{\mathfrak{p}}$$

for all  $x \in \mathcal{O}_{\mathbb{Q}(\zeta_n)}$ . It is well-known that  $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$ , so we require

$$\sigma \left( \sum c_i \zeta_n^i \right) \equiv \left( \sum c_i \zeta_n^i \right)^p \equiv \sum c_i^p \zeta_n^{pi} \equiv \sum c_i \zeta_n^{pi} \pmod{\mathfrak{p}},$$

where we have used the fact that in the residue field  $\kappa(\mathfrak{p})$  (of characteristic  $p$ ) we have  $(x+y)^p = x^p + y^p$  (freshman's dream) and  $c_i^p = c_i$  since  $c_i \in \mathbb{Z}$ . Now, the  $\sigma$  we are looking for must be of the form  $\sigma_a$  for some  $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ , and it is clear that taking  $a = p \pmod{n}$  works. Since there exists at most one element in the Galois group that satisfies (1.11) (this follows from Theorem 1.3.9 (3)), we conclude that

$$\left( \frac{\mathbb{Q}(\zeta_n)/\mathbb{Q}}{\mathfrak{p}} \right) = \sigma_p,$$

and that, moreover, the conjugacy class  $\left( \frac{\mathbb{Q}(\zeta_n)/\mathbb{Q}}{\mathfrak{p}} \right)$  consists of the single element  $\sigma_p$ .

We conclude this section by mentioning a fundamental theorem (which we will prove in a few lectures' time!) that gives some motivation as to why Frobenius elements/Artin symbols are so important:

**Theorem 1.3.18** (Chebotarev, first approximate form). *Let  $L/K$  be a Galois extension of number fields with group  $G$ . For every element  $\sigma$  of  $G$ , there exist infinitely many primes  $\mathfrak{P}$  of  $\mathcal{O}_L$  such that  $\left( \frac{L/K}{\mathfrak{P}} \right) = \sigma$  and  $N(\mathfrak{P})$  is a prime number.*

While this may not look like much, we point out right away that Theorem 1.3.18 contains Dirichlet's theorem on primes in arithmetic progressions as a(n extremely) special case.

**Theorem 1.3.19** (Dirichlet's theorem on primes in arithmetic progressions). *Let  $a, m$  be integers with  $(a, m) = 1$ . There exist infinitely many primes  $p$  that satisfy  $p \equiv a \pmod{m}$ .*

*Proof of Theorem 1.3.19 assuming Theorem 1.3.18.* Apply Theorem 1.3.18 to the Galois extension  $\mathbb{Q}(\zeta_m)/\mathbb{Q}$  and to the element  $\sigma_a$  of the Galois group  $(\mathbb{Z}/m\mathbb{Z})^\times$ . It yields infinitely many primes  $\mathfrak{p}$  of  $\mathbb{Q}(\zeta_m)$  such that  $\left(\frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{\mathfrak{p}}\right) = \sigma_a$  and  $N(\mathfrak{p})$  is a prime number  $p$ . We have shown in Example 1.3.17 that  $\left(\frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{\mathfrak{p}}\right) = \sigma_{N(\mathfrak{p})} = \sigma_p$ , so we obtain  $\sigma_p = \sigma_a$ , that is,  $p \equiv a \pmod{m}$ . Since Chebotarev's theorem guarantees the existence of infinitely many such  $p$ , we are done.  $\square$

### 1.3.6 Dirichlet's unit theorem and the regulator

Before returning to our main topic of  $L$ -functions we review two more facts from algebraic number theory: the structure of the group of units of a number ring and the finiteness of the class group.

**Definition 1.3.20.** The **signature** of a number field  $K$  of degree  $n$  is the pair  $(r_1, r_2)$ , where  $r_1$  is the number of distinct embeddings of  $K$  into  $\mathbb{R}$ , and  $r_2$  is the number of pairs of complex conjugate embeddings of  $K$  into  $\mathbb{C}$  whose image is not contained in  $\mathbb{R}$ . One has  $r_1 + 2r_2 = n$ .

**Theorem 1.3.21** (Dirichlet's unit theorem). *Let  $K$  be a number field of signature  $(r_1, r_2)$ . The group  $\mathcal{O}_K^\times$  is isomorphic to  $T \times \mathbb{Z}^{r_1+r_2-1}$ , where  $T$  – the torsion subgroup – is precisely given by the set of roots of unity in  $K^\times$ .*

The 'standard' proof of Theorem 1.3.21 uses in a fundamental way the so-called **logarithmic embedding**. We now recall this map.

Let  $\sigma_1, \dots, \sigma_{r_1}, \tau_1, \overline{\tau_1}, \dots, \tau_{r_2}, \overline{\tau_{r_2}}$  be the set of embeddings  $K \hookrightarrow \mathbb{C}$ , where  $\sigma_1, \dots, \sigma_{r_1}$  are the embeddings with image in  $\mathbb{R}$  and  $\tau_1, \overline{\tau_1}, \dots, \tau_{r_2}, \overline{\tau_{r_2}}$  are the  $r_2$  pairs of complex embeddings.

It is also useful to set

$$\rho_1 = \sigma_1, \dots, \rho_{r_1} = \sigma_{r_1}, \quad \rho_{r_1+1} = \tau_1, \dots, \rho_{r_1+r_2} = \tau_{r_2}$$

and

$$N_1 = \dots = N_{r_1} = 1, \quad N_{r_1+1} = \dots = N_{r_1+r_2} = 2.$$

This will allow for more uniform formulas below.

**Definition 1.3.22** (Logarithmic embedding). The map

$$\begin{aligned} L: \mathcal{O}_K \setminus \{0\} &\rightarrow \mathbb{R}^{r_1} \times \mathbb{R}^{r_2} = \mathbb{R}^{r_1+r_2} \\ x &\mapsto (\log(|\sigma_i(x)|))_{i=1, \dots, r_1}, (\log |\tau_j(x)|^2)_{j=1, \dots, r_2} \end{aligned}$$

is called the **logarithmic embedding**. It can equivalently be defined as

$$\begin{aligned} L: \mathcal{O}_K \setminus \{0\} &\rightarrow \mathbb{R}^{r_1+r_2} \\ x &\mapsto (N_i \log(|\rho_i(x)|))_{i=1, \dots, r_1+r_2}. \end{aligned}$$

Now recall that every element  $\alpha$  in  $\mathcal{O}_K^\times$  satisfies

$$\pm 1 = N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{r_1} \sigma_i(\alpha) \cdot \prod_{j=1}^{r_2} \tau_j(\alpha) \overline{\tau_j(\alpha)},$$

which implies

$$0 = \log |\pm 1| = \sum_{i=1}^{r_1} \log |\sigma_i(\alpha)| + \sum_{j=1}^{r_2} \log (|\tau_j(\alpha)|^2).$$

This shows that  $L(\mathcal{O}_K^\times)$  is contained in the hyperplane  $\Pi$  of  $\mathbb{R}^{r_1+r_2}$  given by the condition that the sum of the coordinates vanishes. A more precise version of Dirichlet's unit theorem shows that  $L(\mathcal{O}_K^\times)$  is a *lattice* in  $\Pi$ , that is, it is a discrete subgroup such that  $\Pi/L(\mathcal{O}_K^\times)$  is a compact topological space. (Equivalently,  $L(\mathcal{O}_K^\times)$  is discrete in  $\Pi$  and spans it).

**Definition 1.3.23** (Regulator of a number field). The **regulator** of  $K$  is by definition

$$\text{Reg}_K = \frac{1}{\sqrt{r_1 + r_2}} \text{vol}(\Pi/L(\mathcal{O}_K^\times)).$$

Equivalently, and more practically, it can be obtained as follows. Let  $u_1, \dots, u_{r_1+r_2-1} \in \mathcal{O}_K^\times$  generate a subgroup  $U$  such that  $\mathcal{O}_K^\times/U$  is a finite group (in other words,  $u_1, \dots, u_{r_1+r_2-1}$  is a lift of a basis of the free group  $\mathcal{O}_K^\times/\text{torsion}$ ). Consider the matrix

$$M := (N_i \log |\rho_i(u_j)|)_{\substack{i=1, \dots, r_1+r_2 \\ j=1, \dots, r_1+r_2-1}}.$$

The matrix  $M$  has size  $(r_1 + r_2) \times (r_1 + r_2 - 1)$ , and every line sums to zero. This implies that any minor of size  $(r_1 + r_2 - 1) \times (r_1 + r_2 - 1)$  gives the same determinant, up to sign. This common value is the regulator of  $K$ .

**Example 1.3.24.** We compute the regulator of  $K = \mathbb{Q}(\sqrt{2})$ . Notice that  $K$  has 2 real embeddings, so  $r_1 = 2, r_2 = 0$ , and Dirichlet's unit theorem gives  $\mathcal{O}_K^\times \cong \langle -1 \rangle \times \mathbb{Z}$ .

One has  $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$ . Units of  $\mathcal{O}_K$  are numbers of the form  $x + y\sqrt{2} \in \mathcal{O}_K$  with  $x, y \in \mathbb{Z}$  and  $x^2 - 2y^2 = \pm 1$ . The theory of Pell equations shows that all solutions to this equation are given by  $x + y\sqrt{2} = \pm(1 + \sqrt{2})^n$  for  $n \in \mathbb{Z}$ . Hence, a generator of the free part of the group of units can be taken to be  $1 + \sqrt{2}$ . Now consider the matrix  $M$  from Definition 1.3.23. The two embeddings of  $K$  into  $\mathbb{C}$  send  $\sqrt{2}$  to  $\pm\sqrt{2}$ , and we have  $N_1 = N_2 = 1$ , so the matrix  $M$  is given by

$$(\log |1 + \sqrt{2}| \quad \log |1 - \sqrt{2}|) = \left( \log(1 + \sqrt{2}) \quad \log \left| \frac{-1}{1 + \sqrt{2}} \right| \right) = (\log(1 + \sqrt{2}) \quad -\log(1 + \sqrt{2})).$$

As already observed, every line of  $M$  sums to zero. The regulator is simply the absolute value of any of the two coefficients of  $M$ :

$$\text{Reg}_{\mathbb{Q}(\sqrt{2})} = \log(1 + \sqrt{2}).$$

Finally, we discuss more generally the structure of the so-called group of **S-units**.

**Theorem 1.3.25.** Let  $K$  be a number field and let  $S$  be a finite set of primes of  $\mathcal{O}_K$ . The group

$$\mathcal{O}_{K,S}^\times = \{x \in K^\times : \mathfrak{p} \text{ does not appear in the factorisation of the principal ideal } (x) \quad \forall \mathfrak{p} \notin S\}$$

is a finitely generated abelian group of rank  $|S| + (r_1 + r_2 - 1)$ . Its torsion part is given by the set of roots of unity in  $K$ .

**Remark 1.3.26.** This can be stated more elegantly in the following form, by using the notion of *place* (see Definition 2.3.1). Let  $S$  be a finite set of places of  $K$ , containing all the infinite ones. Then the ring of  $S$ -integers is

$$\mathcal{O}_{K,S} = \{x \in K : \|x\|_v \leq 1 \quad \forall v \notin S\},$$

and the group of  $S$ -units  $\mathcal{O}_{K,S}^\times$  is simply the multiplicative subgroup of this ring. The previous theorem can then be restated simply as:  $\mathcal{O}_{K,S}^\times$  is a finitely generated abelian group of rank  $|S| - 1$ .

### 1.3.7 The class group

To conclude this review of basic algebraic number theory, we recall the definition of the *class group* of a number field. This group can be considered as a measure of the failure of unique factorisation in  $\mathcal{O}_K$ , but we will not use this interpretation much. In order to define the class group, we begin by introducing the notion of fractional ideal:

**Definition 1.3.27** (Fractional ideal). A **fractional ideal**  $\mathcal{I}$  of  $K$  is a finitely generated  $\mathcal{O}_K$ -submodule of  $K$ . Equivalently, it is a subset of  $K$  of the form  $\mathcal{I} = \frac{1}{d}I = \left\{\frac{i}{d} : i \in I\right\}$ , where  $I$  is a (usual<sup>8</sup>) ideal of  $\mathcal{O}_K$  and  $d \in K^\times$ .

Fractional ideals can be multiplied, as in the next definition:

**Definition 1.3.28** (Product of fractional ideals). Let  $\mathcal{I}_1, \mathcal{I}_2$  be two fractional ideals. The product  $\mathcal{I}_1\mathcal{I}_2$  is the set  $\{\sum x_i y_i \mid x_i \in \mathcal{I}_1, y_i \in \mathcal{I}_2\}$ . Equivalently, if  $\mathcal{I}_1 = \frac{1}{d_1}I_1$  and  $\mathcal{I}_2 = \frac{1}{d_2}I_2$  with  $I_1, I_2$  integral ideals, then

$$\mathcal{I}_1\mathcal{I}_2 = \frac{1}{d_1 d_2} I_1 I_2.$$

The product makes the set of non-zero fractional ideals into a group.

**Theorem 1.3.29** (Group of fractional ideals). *The set  $\mathcal{F}(K)$  of non-zero fractional ideals of  $K$  forms an abelian group with respect to the multiplication of Definition 1.3.28. In particular, let  $\mathcal{I}$  be a non-zero fractional ideal. There exists a fractional ideal  $\mathcal{J}$  such that  $\mathcal{I}\mathcal{J} = \mathcal{O}_K$ .*

We are almost ready to define the class group, but we need one more definition:

**Definition 1.3.30** (Principal fractional ideal). A fractional ideal  $\mathcal{I} = \frac{1}{d}I$  is **principal** if the integral ideal  $I$  is principal in the usual sense. Equivalently,  $\mathcal{I}$  is principal if and only if it is of the form  $\mathcal{O}_K \cdot \alpha$  for some  $\alpha \in K$ .

It is clear that the (non-zero) principal fractional ideals  $\text{Princ}(K)$  form a subgroup of  $\mathcal{F}(K)$ , so we can consider the quotient:

**Definition 1.3.31** (Class group). The quotient  $\frac{\mathcal{F}(K)}{\text{Princ}(K)}$  is the **class group** of  $K$ , usually denoted by  $\text{Cl}(K)$ . The order of  $\text{Cl}(K)$  is called the **class number** and is denoted by  $h_K$ .

The next theorem gives two very important properties of  $\text{Cl}(K)$ .

**Theorem 1.3.32** (Finiteness of the class group). *The group  $\text{Cl}(K)$  is finite for every number field  $K$ . It is trivial if and only if  $\mathcal{O}_K$  is a unique factorisation domain.*

<sup>8</sup>in this context, an ideal of  $\mathcal{O}_K$  is sometimes called an *integral ideal*

### 1.3.8 Completed $\zeta$ functions: the local factors at infinity

The following is a generalisation of Theorem 1.1.8:

**Theorem 1.3.33** (Functional equation for the Dedekind  $\zeta$  function). *Let  $K$  be a number field of signature  $(r_1, r_2)$  and discriminant  $d_K$ . The **completed  $\zeta$  function***

$$\Lambda_K(s) = \left( \frac{|d_K|}{4^{r_2} \pi^n} \right)^{s/2} \Gamma\left(\frac{s}{2}\right)^{r_1} \Gamma(s)^{r_2} \zeta_K(s)$$

*satisfies the functional equation  $\Lambda_K(1-s) = \Lambda_K(s)$ . The function  $\zeta_K(s)$  has meromorphic continuation to  $\mathbb{C}$ , with a simple pole at  $s = 1$ .*

As is the case for the  $\xi$  function (see Theorem 1.1.8), one should consider that

$$\left( \frac{|d_K|}{4^{r_2} \pi^n} \right)^{s/2} \Gamma\left(\frac{s}{2}\right)^{r_1} \Gamma(s)^{r_2}$$

plays the role of a ‘local factor at infinity’. Notice that  $K$  has  $r_1$  places at which the completion is  $\mathbb{R}$ , and  $r_2$  places at which the completion is  $\mathbb{C}$  (see Definition 2.3.1 for the notion of *place* of a number field). Thus, it is very tempting to think that this ‘local factor at infinity’ factors even further, as an actual product over the infinite places of  $K$ . Tate’s approach will make it clear that this is indeed the case.

## 1.4 The $L$ -function of a (complex) Galois representation

We are finally ready to define a large class of  $L$ -functions, that contains all those we have already met. Recall that a **(linear) representation** of a group  $G$  is simply a homomorphism from  $G$  to a group of the form  $\mathrm{GL}(V)$ , where  $V$  is a vector space (in our applications, we will always take  $V$  to be of finite dimension).

**Definition 1.4.1** (Artin  $L$ -function). Let  $L/K$  be a Galois extension of number fields with group  $G$ . Let  $\rho : G \rightarrow \mathrm{GL}(V)$  be a finite-dimensional complex representation of  $\rho$  (that is,  $V$  is a finite-dimensional complex vector space). For every (non-zero) prime  $\mathfrak{p}$  of  $\mathcal{O}_K$ , fix a prime  $\mathfrak{P}$  of  $\mathcal{O}_L$  and let  $I_{\mathfrak{P}} < G$  be the corresponding inertia subgroup. We define the **Artin  $L$ -function** of  $\rho$  to be

$$L(s, \rho) := \prod_{\mathfrak{p} \text{ nonzero prime of } \mathcal{O}_K} \det \left( \mathrm{Id} - \rho \left( \left( \frac{L/K}{\mathfrak{P}} \right) \right) N(\mathfrak{p})^{-s} \mid V^{I_{\mathfrak{P}}} \right)^{-1}, \quad (1.12)$$

where  $V^{I_{\mathfrak{P}}}$  is the subspace of  $V$  on which  $I_{\mathfrak{P}}$  acts trivially via  $\rho$ . Notice that, when  $\mathfrak{P}$  is ramified over  $\mathfrak{p}$ , the Artin symbol  $\left( \frac{L/K}{\mathfrak{P}} \right)$  is not a well-defined element of  $G$  (see Remark 1.3.13). In this case, we simply take an arbitrary choice of Frobenius element at  $\mathfrak{P}$  to represent the Artin symbol: Remark 1.4.2 below shows that the definition is independent of this choice.

The factor  $\det \left( \mathrm{Id} - \rho \left( \left( \frac{L/K}{\mathfrak{P}} \right) \right) N(\mathfrak{p})^{-s} \mid V^{I_{\mathfrak{P}}} \right)$  appearing in the above product is often called the **local factor at  $\mathfrak{p}$**  of the Artin  $L$ -function.

**Remark 1.4.2.** With the notation of the previous definition, we show that

1.  $V^{I_{\mathfrak{P}}}$  is stable under the action of  $\rho\left(\left(\frac{L/K}{\mathfrak{P}}\right)\right)$ ;
2.  $\rho\left(\left(\frac{L/K}{\mathfrak{P}}\right)\right)$  is a well-defined endomorphism of  $V^{I_{\mathfrak{P}}}$  even when  $I_{\mathfrak{P}}$  is non-trivial (recall that in this case we have made an arbitrary choice in the definition of  $\left(\frac{L/K}{\mathfrak{P}}\right)$ , see Definition 1.3.11).

Write for simplicity  $g \in G$  for a fixed choice of Frobenius element at  $\mathfrak{P}$ . Any other choice of Frobenius element at  $\mathfrak{P}$  is of the form  $g \cdot h$  for some  $h \in I_{\mathfrak{P}}$ , see also Remark 1.3.13. Let furthermore  $x \in V$  be a vector fixed by  $\rho(I_{\mathfrak{P}})$ . Since  $I_{\mathfrak{P}}$  is a normal subgroup of the decomposition group of  $\mathfrak{P}$ , for every  $h' \in I_{\mathfrak{P}}$  we have  $h'g = gh''$  for some  $h'' \in I_{\mathfrak{P}}$ , and therefore

$$\rho(h') \cdot (\rho(gh) \cdot v) = \rho(h'gh) \cdot v = \rho(gh''h) \cdot v = \rho(g) \cdot (\rho(h''h) \cdot v) = \rho(g) \cdot v,$$

where we used that  $v$  is left fixed by  $\rho(I_{\mathfrak{P}})$ . The above equality shows that  $\rho(gh)v$  is again in  $V^{I_{\mathfrak{P}}}$ , for any  $v \in I_{\mathfrak{P}}$  and any choice  $gh$  of Frobenius element at  $\mathfrak{P}$ . In particular, it makes sense to consider  $\text{Id} - \rho\left(\left(\frac{L/K}{\mathfrak{P}}\right)\right) N(\mathfrak{p})^{-s}$  as an endomorphism of  $V^{I_{\mathfrak{P}}}$ . The same calculation also shows that  $\text{Id} - \rho\left(\left(\frac{L/K}{\mathfrak{P}}\right)\right) N(\mathfrak{p})^{-s}$  is independent of the choice of the Frobenius element  $\left(\frac{L/K}{\mathfrak{P}}\right)$  at  $\mathfrak{P}$ .

In the rest of the section, we will discuss the following:

1. the definition does not depend on the choice of the prime  $\mathfrak{P}$  of  $\mathcal{O}_L$  lying over  $\mathfrak{p}$ , and the dimension of the subspace  $V^{I_{\mathfrak{P}}}$  itself does not depend on the choice of  $\mathfrak{P}$ ;
2. the Euler product defining  $L(\rho, s)$  converges for all  $s$  with  $\Re s > 1$ ;
3. every  $L$ -function we have met so far is in fact an Artin  $L$ -function;
4. Artin's conjecture on analytic continuation.

### 1.4.1 Independence of the choice of $\mathfrak{P}$

**Proposition 1.4.3.** *Let  $L/K$  be a Galois extension of number fields with group  $G$  and let  $\mathfrak{p}$  be a prime of  $\mathcal{O}_K$ . Let  $\mathfrak{P}, \mathfrak{P}'$  be two primes of  $\mathcal{O}_L$  lying over  $\mathfrak{p}$ , and let  $I_{\mathfrak{P}}, I_{\mathfrak{P}'}$  be the corresponding inertia groups. Finally, let  $\rho : G \rightarrow \text{GL}(V)$  be a finite-dimensional complex representation of  $G$ . The following hold:*

1. the subspaces  $V^{I_{\mathfrak{P}}}$  and  $V^{I_{\mathfrak{P}'}}$  have the same dimension;
2. the complex numbers

$$\det\left(\text{Id} - \rho\left(\left(\frac{L/K}{\mathfrak{P}}\right)\right) N(\mathfrak{p})^{-s} \mid V^{I_{\mathfrak{P}}}\right) \text{ and } \det\left(\text{Id} - \rho\left(\left(\frac{L/K}{\mathfrak{P}'}\right)\right) N(\mathfrak{p})^{-s} \mid V^{I_{\mathfrak{P}'}}\right)$$

are equal.

*Proof.* By Theorem 1.3.9 (1) we know that there exists  $\sigma \in G$  such that  $\sigma(\mathfrak{P}) = \mathfrak{P}'$ . One checks immediately that  $I_{\mathfrak{P}'} = \sigma I_{\mathfrak{P}} \sigma^{-1}$ .

1. By definition,  $v \in V^{I_{\mathfrak{P}'}}$  means

$$\rho(i) \cdot v = v \quad \forall i \in I_{\mathfrak{P}'} = \sigma I_{\mathfrak{P}} \sigma^{-1},$$

which is equivalent to

$$\rho(\sigma i \sigma^{-1}) \cdot v = v \quad \forall i \in I_{\mathfrak{P}},$$

and therefore also to

$$\rho(i) \rho(\sigma)^{-1} \cdot v = \rho(\sigma)^{-1} \cdot v \quad \forall i \in I_{\mathfrak{P}}.$$

Thus,  $v$  is in  $V^{I_{\mathfrak{P}'}}$  if and only if  $\rho(\sigma)^{-1} \cdot v$  is in  $V^{I_{\mathfrak{P}}}$ . It follows that  $V^{I_{\mathfrak{P}'}} = \rho(\sigma) V^{I_{\mathfrak{P}}}$ , and in particular, since  $\rho(\sigma)$  is an invertible linear transformation, these two spaces have the same dimension.

2. It is useful to interpret the factor  $\det \left( \text{Id} - \rho \left( \left( \frac{L/K}{\mathfrak{P}} \right) \right) N(\mathfrak{p})^{-s} \mid V^{I_{\mathfrak{P}}} \right)$  as the evaluation at  $t = N(\mathfrak{p})^{-s}$  of the (inverse) characteristic polynomial

$$f_{\mathfrak{P}}(t) := \det \left( \text{Id} - t \rho \left( \left( \frac{L/K}{\mathfrak{P}} \right) \right) \mid V^{I_{\mathfrak{P}}} \right)$$

of  $\left( \frac{L/K}{\mathfrak{P}} \right)$  acting on  $V^{I_{\mathfrak{P}}}$ , and similarly for the factor corresponding to  $\mathfrak{P}'$ . The claim now follows from the fact that  $\rho(\sigma)$  acts as a change of basis between  $\rho \left( \left( \frac{L/K}{\mathfrak{P}} \right) \right)$  and  $\rho \left( \left( \frac{L/K}{\mathfrak{P}'} \right) \right)$ . □

**Remark 1.4.4** (Local factors at the unramified places). Suppose that  $\mathfrak{p}$  is unramified in  $L$ . In this case,  $V^{I_{\mathfrak{P}}}$  is simply  $V$ , and the interpretation of the local factor at  $\mathfrak{p}$  as a characteristic polynomial shows that it is independent of the choice of the Frobenius element in the conjugacy class  $\left( \frac{L/K}{\mathfrak{p}} \right)$ . We may therefore write the local factor without any reference to the choice of  $\mathfrak{P}$  as

$$\det(\text{Id} - t \rho(\text{Frob}_{\mathfrak{p}}));$$

see Definition 1.3.15 for the notation  $\text{Frob}_{\mathfrak{p}}$  (any element in the conjugacy class  $\left( \frac{L/K}{\mathfrak{p}} \right)$ ).

Finally, we introduce what is probably a more common notation for the local factors of Artin  $L$ -functions: for a prime  $\mathfrak{p}$  of  $\mathcal{O}_K$ , choose a prime  $\mathfrak{P}$  of  $\mathcal{O}_L$  lying over it and define

$$L_{\mathfrak{p}}(t) := \det \left( \text{Id} - t \rho \left( \left( \frac{L/K}{\mathfrak{P}} \right) \right) \mid V^{I_{\mathfrak{P}}} \right).$$

We then have

$$L(s, \rho) = \prod_{\mathfrak{p}} \frac{1}{L_{\mathfrak{p}}(N(\mathfrak{p})^{-s})},$$

which, in my experience, is the way Artin  $L$ -functions are most commonly written.



### 1.4.2 Convergence of the Euler product

**Proposition 1.4.5.** *The Euler product in Equation (1.12) converges absolutely for all  $s$  with  $\Re s > 1$ .*

*Proof.* Notice that, since  $G := \text{Gal}(L/K)$  is a finite group, for every  $g \in G$  (hence in particular for every Artin symbol  $\left(\frac{L/K}{\mathfrak{P}}\right) \in G$ ), the element  $\rho(g)$  has finite order, hence all its eigenvalues are roots of unity. Hence, for each prime  $\mathfrak{P}$  of  $\mathcal{O}_L$  lying over the prime  $\mathfrak{p}$  of  $\mathcal{O}_K$ , we have

$$\det \left( \text{Id} - t \rho \left( \left( \frac{L/K}{\mathfrak{P}} \right) \right) \mid V^{I_{\mathfrak{P}}} \right) = \prod_{j=1}^{\dim V^{I_{\mathfrak{P}}}} (1 - t \zeta_j),$$

where the  $\zeta_j$ , for  $j = 1, \dots, \dim V^{I_{\mathfrak{P}}}$ , are the eigenvalues of  $\rho \left( \left( \frac{L/K}{\mathfrak{P}} \right) \right)$  acting on  $V^{I_{\mathfrak{P}}}$ . Thus, in particular,

$$\begin{aligned} \prod_{\mathfrak{p}} \left| \det \left( \text{Id} - N(\mathfrak{p})^{-s} \rho \left( \left( \frac{L/K}{\mathfrak{P}} \right) \right) \mid V^{I_{\mathfrak{P}}} \right) \right|^{-1} &= \prod_{\mathfrak{p}} \prod_{j=1}^{\dim V^{I_{\mathfrak{P}}}} |1 - N(\mathfrak{p})^{-s} \zeta_{\mathfrak{p},j}|^{-1} \\ &\leq \prod_{\mathfrak{p}} \prod_{j=1}^{\dim V^{I_{\mathfrak{P}}}} (1 - |p^{-s}|)^{-1} \leq \prod_{j=1}^{\dim V} \prod_{\mathfrak{p}} (1 - p^{-\Re(s)})^{-1} \\ &= \prod_{j=1}^{\dim V} \prod_p \prod_{\mathfrak{p}|\mathfrak{p}} (1 - p^{-\Re(s)})^{-1} \leq \zeta(\Re(s))^{\dim V \cdot [K:\mathbb{Q}]}, \end{aligned}$$

which converges for all  $s$  with  $\Re s > 1$  as claimed. (In the last step we used that there are  $\dim V$  factors in the product over  $j$ , and at most  $[K:\mathbb{Q}]$  in the product over  $\mathfrak{p}$ , since each rational prime factors into at most  $[K:\mathbb{Q}]$  primes in  $\mathcal{O}_K$ .)  $\square$

### 1.4.3 The Riemann and Dedekind $\zeta$ functions, and Dirichlet's $L$ -functions, are Artin $L$ -functions

**Proposition 1.4.6.**

1. *The Riemann  $\zeta$  function is an Artin  $L$ -function.*
2. *Let  $K$  be a number field. The Dedekind  $\zeta$  function of  $K$  is an Artin  $L$ -function.*
3. *Let  $\chi$  be a **primitive** Dirichlet character modulo  $m$ . The Dirichlet  $L$ -function  $L(s, \chi)$  is an Artin  $L$ -function.*
4. *Let  $\chi$  be an arbitrary Dirichlet character modulo  $m$ . There exists an Artin  $L$ -function  $L_{\text{Artin}}(s, \rho)$  such that  $L_{\text{Dirichlet}}(s, \chi) = f(s) L_{\text{Artin}}(s, \rho)$ , where the factor  $f(s)$  is a holomorphic function of  $s$  which is nonvanishing on  $\{\Re s > 0\}$ .*

*Proof.* 1. Clearly, Riemann's  $\zeta$  function is the Dedekind  $\zeta$  function of  $\mathbb{Q}$ , so it suffices to prove 2.

2. In Definition 1.4.1 we take  $L = K$  and  $\rho$  to be the unique 1-dimensional trivial representation of  $G = \text{Gal}(L/K)$ . With reference to Equation (1.12), the inertia groups  $I_{\mathfrak{p}}$  are all trivial, so  $V^{I_{\mathfrak{p}}} = V$  for all  $\mathfrak{p}$ , while  $\rho\left(\left(\frac{L/K}{\mathfrak{p}}\right)\right) = 1$ . Thus, Equation (1.12) reads simply

$$L(\rho, s) = \prod_{\mathfrak{p}} \det(1 - N(\mathfrak{p})^{-s})^{-1} = \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1} = \zeta_K(s),$$

where the last equality follows from Exercise 1.1.17.

3. In Definition 1.4.1 we take  $K = \mathbb{Q}$ ,  $L = \mathbb{Q}(\zeta_m)$  and define a Galois representation of  $G = \text{Gal}(L/K) \cong (\mathbb{Z}/m\mathbb{Z})^\times$  by setting

$$\rho(\sigma_a) = \chi(a) \text{Id} \in \text{GL}(V),$$

where  $V = \mathbb{C}$  and  $\sigma_a \in G$  is the automorphism  $\zeta_m \mapsto \zeta_m^a$ , corresponding to  $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ . On the one hand, since  $\chi$  is a completely multiplicative function, by Theorem 1.1.11 we have

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

On the other hand, the definition of  $L(s, \rho)$  gives

$$L(s, \rho) = \prod_{\mathfrak{p}} \det \left( 1 - \rho \left( \left( \frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{\mathfrak{p}} \right) \right) N(p)^{-s} \mid V^{I_{\mathfrak{p}}} \right)^{-1}.$$

We now prove equality by matching up the local factors. Let  $p$  be a rational prime and let  $\mathfrak{p}$  be a prime of  $\mathbb{Q}(\zeta_m)$  lying over  $p$ .

- a) Suppose that  $p \nmid m$ . Then  $p$  is unramified in  $\mathbb{Q}(\zeta_m)$ , so  $I_{\mathfrak{p}}$  is trivial, while  $\left(\frac{\mathbb{Q}(\zeta_m)/\mathbb{Q}}{\mathfrak{p}}\right) \in G$  is given by  $\sigma_p$ , see Example 1.3.17. It follows that the local factor of  $L(s, \rho)$  at  $p$  is  $\det(1 - \rho(\sigma_p)p^{-s} \mid \mathbb{C})^{-1} = (1 - \chi(p)p^{-s})^{-1}$ , which precisely matches the local factor of  $L(s, \chi)$  at  $p$ .
- b) Suppose now that  $p \mid m$ . The local factor at  $p$  of  $L(s, \chi)$  is trivially 1. To conclude the proof, it suffices to show that  $V^{I_{\mathfrak{p}}}$  is trivial, that is, that  $\rho(I_{\mathfrak{p}})$  is not the trivial group. If this were the case,  $\chi$  would be trivial on the (nontrivial) subgroup  $J_p$  of  $(\mathbb{Z}/m\mathbb{Z})^\times$  corresponding to  $I_{\mathfrak{p}}$  under the canonical isomorphism  $G \cong (\mathbb{Z}/m\mathbb{Z})^\times$ . Writing  $m = p^s m'$  with  $(p, m') = 1$ , we claim that  $J_p$  is precisely the kernel of the canonical projection  $(\mathbb{Z}/m\mathbb{Z})^\times \rightarrow (\mathbb{Z}/m'\mathbb{Z})^\times$ . Assuming the claim, we obtain that if  $\rho(I_{\mathfrak{p}})$  is trivial, then  $\chi$  factors via  $(\mathbb{Z}/m\mathbb{Z})^\times / J_p \cong (\mathbb{Z}/m'\mathbb{Z})^\times$ , contradicting the fact that  $\chi$  is primitive. The claim is an exercise in algebraic number theory, and is left to the reader (see Exercise 1.4.8 below).
4. Construct  $L_{\text{Artin}}(s, \rho)$  as in part 3. For all primes  $p \nmid m$ , the local factors at  $p$  of  $L_{\text{Dirichlet}}(s, \chi)$  and  $L_{\text{Artin}}(s, \rho)$  match, so their ratio

$$f(s) = \frac{L_{\text{Dirichlet}}(s, \chi)}{L_{\text{Artin}}(s, \rho)}$$

is a finite product of factors of the form  $1 - \chi(p)p^{-s}$  for (certain) primes dividing  $m$ . These functions are clearly holomorphic on all of  $\mathbb{C}$ , and their zeroes arise for  $1 - \chi(p)p^{-s} = 0$ . Taking absolute values we get  $|p^{-s}| = 1$ , that is,  $\Re s = 0$ . It follows that  $f(s)$  is nonvanishing in  $\{\Re s > 0\}$ . □

**Remark 1.4.7.** Let  $\chi$  be a Dirichlet character modulo  $m$ , induced from the primitive Dirichlet character  $\tilde{\chi}$  modulo the conductor  $d$  of  $\chi$ . The proof of Proposition 1.4.6 shows that  $L_{\text{Dirichlet}}(s, \tilde{\chi})$  is the Artin  $L$ -function attached to the representation

$$\text{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q}) \cong (\mathbb{Z}/d\mathbb{Z})^\times \xrightarrow{\tilde{\chi}} \mathbb{C}^\times.$$

By Theorem 1.4.12 (2) below, this implies that  $L_{\text{Dirichlet}}(s, \tilde{\chi})$  is also the Artin  $L$ -function of the representation

$$\text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \twoheadrightarrow \text{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q}) \cong (\mathbb{Z}/d\mathbb{Z})^\times \xrightarrow{\tilde{\chi}} \mathbb{C}^\times.$$

**Exercise 1.4.8 (♠).** Let  $p$  be a prime number,  $s$  be a positive integer, and  $m'$  be a positive integer prime to  $p$ . Set  $m = p^s m'$ . Let  $G = \text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ , let  $\mathfrak{p}$  be a prime of  $\mathbb{Q}(\zeta_m)$  lying over  $p$ , and let  $I_{\mathfrak{p}}$  be the corresponding inertia subgroup.

1. Show that  $I_{\mathfrak{p}}$  depends only on  $p$  and not on the choice of the prime  $\mathfrak{p}$  lying over it. We will therefore denote the group  $I_{\mathfrak{p}}$  simply by  $I_p$ .
2. Prove (or recall) that  $\mathbb{Q}(\zeta_{m'})/\mathbb{Q}$  is unramified at  $p$ .
3. Deduce that  $I_p$  is contained in the kernel of the canonical map

$$\text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \rightarrow \text{Gal}(\mathbb{Q}(\zeta_{m'})/\mathbb{Q}).$$

4. Conclude that  $I_p$  is in fact *equal* to the kernel of  $\text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \rightarrow \text{Gal}(\mathbb{Q}(\zeta_{m'})/\mathbb{Q})$  (one way to do this is to argue by cardinality, showing that  $\#I_p = \varphi(p^s)$ ).

This is also a good time to informally introduce our last family of (abelian)  $L$ -functions, namely, **Hecke  $L$ -functions**:

**Definition 1.4.9** (Hecke  $L$ -functions, **wrong** definition). Let  $K$  be a number field, let  $L/K$  be a finite Galois extension with group  $G$ , and let  $\chi : G \rightarrow \mathbb{S}^1$  be a character (equivalently, a representation of dimension 1) of  $G$ . The **Hecke  $L$ -function** attached to this data is the Artin  $L$ -function  $L(s, \chi)$ .

**Remark 1.4.10.** Hecke did not introduce his  $L$ -functions in this way at all. His definition was

$$L(s, \chi) = \sum_{I \triangleleft \mathcal{O}_K} \frac{\chi(I)}{N(I)^s},$$

where  $\chi$  is a map from the ideals of  $\mathcal{O}_K$  to  $\mathbb{C}$  satisfying a complicated set of properties that generalise those of Dirichlet characters. The fact that (many) Hecke  $L$ -functions can be expressed as Artin  $L$ -functions as in Definition 1.4.9 is related to the fact that the abelian extensions of a number field are well-understood in terms of class field theory. We will come back to this point towards the end of this document, in Section 3.3.

At this point, the reader will not be surprised by the following result:

**Theorem 1.4.11** (Analytic continuation for the Hecke  $L$ -functions). *Let  $L/K$  be a finite abelian extension with group  $G$  and let  $\chi : G \rightarrow \mathbb{S}^1$  be a nontrivial character. The Hecke  $L$ -function  $L(s, \chi)$  admits analytic continuation to the full complex plane.*

Artin  $L$ -functions also satisfy a (fairly complicated) functional equation relating  $s$  to  $1 - s$  and  $\rho$  to its dual representation, but we will not need its precise form, so we omit the exact statement. The interested reader can refer to [Neu99, Theorem 12.6 in Chapter VII].

#### 1.4.4 The formalism of Artin $L$ -functions

The following result collects some formal properties of Artin  $L$ -functions that are not too hard to prove.

**Theorem 1.4.12** (Functoriality of Artin  $L$ -functions). *Let  $L/F/K$  be a tower of extensions of number fields, with  $L/K$  Galois. Let  $G = \text{Gal}(L/K)$ ,  $N = \text{Gal}(L/F)$ , and (when  $F/K$  is Galois)  $H = \text{Gal}(F/K)$ . Let  $\rho_1, \rho_2$  be representations of  $G$ , let  $\sigma$  be a representation of  $H$ , and let  $\tau$  be a representation of  $N$ . The following hold:*

1.  $L(s, \rho_1 \oplus \rho_2) = L(s, \rho_1)L(s, \rho_2)$ .
2. If  $F/K$  is Galois, then  $L(s, \text{Inf}_H^G(\sigma)) = L(s, \sigma)$ , where the **inflation** of  $\sigma$  from  $H$  to  $G$ , denoted by  $\text{Inf}_H^G(\sigma)$ , is the composition of the natural map  $G \rightarrow H$  with the representation  $\sigma : H \rightarrow \text{GL}(V)$ .
3.  $L(s, \text{Ind}_N^G(\tau)) = L(s, \tau)$ , where  $\text{Ind}_N^G(\tau)$  is the representation of  $G$  induced by the representation  $\tau$  of  $N$ . Notice that if  $\tau$  takes values in  $\text{GL}_d(\mathbb{C})$ , then  $\text{Ind}_N^G(\tau)$  takes values in  $\text{GL}_{d[G:N]}(\mathbb{C})$ .

*Proof.* 1. Recall the following elementary fact from linear algebra: if  $M_1, M_2$  are matrices in  $\text{GL}_{d_1}(\mathbb{C}), \text{GL}_{d_2}(\mathbb{C})$  respectively, and if  $M_1 \oplus M_2$  denotes their block-sum in  $\text{GL}_{d_1+d_2}(\mathbb{C})$ , then the characteristic polynomial of  $M_1 \oplus M_2$  is the product of the characteristic polynomials of  $M_1, M_2$ . This allows one to identify the local factors of  $L(s, \rho_1 \oplus \rho_2)$  with the product of the corresponding local factors of  $L(s, \rho_1), L(s, \rho_2)$ .

2. It suffices to prove that  $L(s, \text{Inf}_H^G(\sigma))$  and  $L(s, \sigma)$  have the same local factors at each prime. Fix a place  $\mathfrak{P}$  of  $F$  lying over  $\mathfrak{p}$  and a place  $\mathfrak{Q}$  of  $L$  lying over  $\mathfrak{P}$ .

We denote by  $D, I$  (respectively  $D', I'$ ) the decomposition and inertia group of  $\mathfrak{P}$  over  $\mathfrak{p}$  (respectively, of  $\mathfrak{Q}$  over  $\mathfrak{p}$ ). Let  $\pi : G \rightarrow H$  be the canonical projection. It is a standard (but surprisingly tricky) fact in algebraic number theory that  $I = \pi(I')$ , see Exercise 1.4.13. We now compare (representatives of) the Artin symbols

$$\left( \frac{F/K}{\mathfrak{p}} \right) \quad \text{and} \quad \left( \frac{L/K}{\mathfrak{p}} \right).$$

Fix an element  $\varphi \in D' \subseteq G$  that represents a Frobenius at  $\mathfrak{Q}$ . This means that the congruence

$$\varphi(x) \equiv x^{N\mathfrak{p}} \pmod{\mathfrak{Q}} \iff \varphi(x) - x^{N\mathfrak{p}} \in \mathfrak{Q}$$

holds for all  $x \in \mathcal{O}_L$ , hence, in particular, for every  $x \in \mathcal{O}_F$  we have

$$\varphi(x) - x^{N\mathfrak{p}} \in \mathfrak{Q} \cap \mathcal{O}_F$$

since  $F/K$  is Galois (and therefore  $\varphi(F) = F, \varphi(\mathcal{O}_F) = \mathcal{O}_F$ ). The previous equation can be rewritten as

$$\varphi|_F(x) - x^{N\mathfrak{p}} \in \mathfrak{P} \quad \forall x \in \mathcal{O}_F \iff \varphi|_F(x) \equiv x^{N\mathfrak{p}} \pmod{\mathfrak{P}} \quad \forall x \in \mathcal{O}_F,$$

which shows that  $\varphi|_F = \pi(\varphi)$  is a representative for the Frobenius at  $\mathfrak{P}$ .

We are finally ready to prove the statement. Since  $\pi(\varphi)$  gives a Frobenius at  $\mathfrak{P}$ , the local factor at  $\mathfrak{p}$  of the  $L$ -function  $L(s, \sigma)$  is given by

$$\det \left( 1 - N(\mathfrak{p})^{-s} \sigma(\pi(\varphi)) \mid V_\sigma^{\sigma(I)} \right)^{-1},$$

where  $V_\sigma$  is the underlying vector space of the representation  $\sigma$ .

On the other hand, the local factor of  $L(s, \text{Inf}_H^G(\sigma))$  at the same place  $\mathfrak{p}$  is given by

$$\det \left( 1 - N(\mathfrak{p})^{-s} \text{Inf}_H^G(\sigma)(\varphi) \mid V_\sigma^{\text{Inf}_H^G(\sigma)(I')} \right)^{-1}.$$

Since  $\text{Inf}_H^G(\sigma)(\varphi) = \sigma(\pi(\varphi))$  and  $\text{Inf}_H^G(\sigma)(I') = \sigma(\pi(I')) = \sigma(I)$ , the claim follows.

3. Again we try to match local factors, but more complications arise in this case. Let  $\mathfrak{p}$  be a place of  $K$ , let  $\mathfrak{P}_1, \dots, \mathfrak{P}_r$  be the primes of  $F$  lying over  $\mathfrak{p}$ , and let for each  $i = 1, \dots, r$  let  $\mathfrak{Q}_i$  be a prime of  $L$  lying over  $\mathfrak{P}_i$  (see Figure 1.2). Further denote by

$$D_i = D(\mathfrak{Q}_i \mid \mathfrak{p}), \quad I_i = I(\mathfrak{Q}_i \mid \mathfrak{p})$$

the decomposition and inertia groups of the  $\mathfrak{Q}_i$  over  $\mathfrak{p}$ . From the definitions one easily obtains that

$$D'_i := D(\mathfrak{Q}_i \mid \mathfrak{P}_i) = N \cap D_i, \quad I'_i := I(\mathfrak{Q}_i \mid \mathfrak{P}_i) = N \cap I_i.$$

The inertia degree  $f_i$  of  $\mathfrak{P}_i$  over  $\mathfrak{p}$  is

$$f(\mathfrak{P}_i \mid \mathfrak{p}) = \# \text{Gal}(\kappa(\mathfrak{P}_i) \mid \kappa(\mathfrak{p})) = \# \frac{D_i/I_i}{D'_i/I'_i} = \# \frac{D_i}{D'_i I_i}.$$

Note that by definition we have  $N(\mathfrak{P}_i) = N(\mathfrak{p})^{f_i}$ . We now set some further notation for Frobenius elements. For simplicity, we choose elements  $\tau_i \in G$  such that  $\tau_i^{-1}(\mathfrak{Q}_1) = \mathfrak{Q}_i$ , and choose  $\varphi_1 \in D_1$  that represents the Frobenius of  $\mathfrak{Q}_1$  over  $\mathfrak{p}$ . We then have the relations

$$D_i = \tau_i^{-1} D_1 \tau_i, \quad I_i = \tau_i^{-1} I_1 \tau_i,$$

and the element

$$\varphi_i := \tau_i^{-1} \varphi_1 \tau_i$$

represents a Frobenius of  $\mathfrak{Q}_i$  over  $\mathfrak{p}$ . Moreover,  $\varphi_i^{f_i}$  represents a Frobenius of  $\mathfrak{Q}_i$  over  $\mathfrak{P}_i$ .

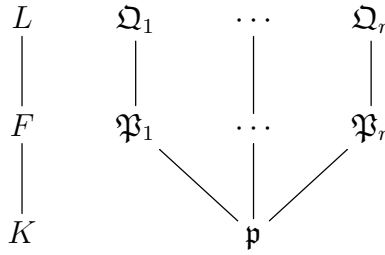


Figure 1.2: Fields and primes in the proof of Theorem 1.4.12 (3)

Let  $W$  be the underlying vector space of the representation  $\tau$ , and let

$$V = \text{Ind}_N^G(W) = \{f : G \rightarrow W \mid f(\tau g) = \tau f(g) \quad \forall \tau \in N\}$$

the vector space underlying  $\text{Ind}_N^G(\tau)$ . For ease of notation, denote by  $\psi : G \rightarrow \text{GL}(V)$  the map giving the induced representation of  $G$ . In order to establish the theorem, it is enough to prove that

$$\det(1 - N(\mathfrak{p})^{-s} \psi(\varphi_1) \mid V^{I_1}) = \prod_{i=1}^r \det(1 - N(\mathfrak{P}_i)^{-s} \tau(\varphi_i^{f_i}) \mid W^{I'_i}).$$

In fact, since  $N(\mathfrak{P}_i) = N(\mathfrak{p})^{f_i}$ , it suffices to prove the polynomial identity

$$\det(1 - t\psi(\varphi_1) \mid V^{I_1}) = \prod_{i=1}^r \det(1 - t^{f_i} \tau(\varphi_i^{f_i}) \mid W^{I'_i}).$$

We now observe that, under the action of  $N$ , the induced representation  $V$  splits as the direct sum of copies of  $W$ , and we may regard  $\tau$  as a subrepresentation of  $V$ . In particular, in  $V$  it makes sense to conjugate using  $\psi(\tau_i)$ , and we obtain (omitting  $\psi$  for simplicity)

$$\begin{aligned} \det(1 - t^{f_i} \tau(\varphi_i^{f_i}) \mid W^{I'_i}) &= \det(1 - t^{f_i} \tau_i \tau(\varphi_i^{f_i}) \tau_i^{-1} \mid \tau_i(W^{I'_i})) \\ &= \det(1 - t^{f_i} \tau(\tau_i \varphi_i^{f_i} \tau_i^{-1}) \mid \tau_i(W^{I'_i})) \\ &= \det(1 - t^{f_i} \tau(\varphi_1^{f_i}) \mid (\tau_i W)^{\tau_i I'_i \tau_i^{-1}}) \\ &= \det(1 - t^{f_i} \tau(\varphi_1^{f_i}) \mid (\tau_i W)^{\tau_i (N \cap I_i) \tau_i^{-1}}) \\ &= \det(1 - t^{f_i} \tau(\varphi_1^{f_i}) \mid (\tau_i W)^{\tau_i N \tau_i^{-1} \cap I_1}). \end{aligned}$$

Similarly,

$$f_i = [D_i : D'_i I_i] = [\tau_i^{-1} D_1 \tau_i : (N \cap \tau_i^{-1} D_1 \tau_i) \tau_i^{-1} I_1 \tau_i] = [D_1 : (\tau_i N \tau_i^{-1} \cap D_1) I_1].$$

For every  $i$  we now choose a system of representatives  $\sigma_{i,j}$  for the left<sup>9</sup> cosets of  $\tau_i N \tau_i^{-1} \cap D_1$  in  $D_1$ . Since the  $\tau_i$  are representatives for the cosets of  $D_1$  in  $G$ , we obtain (Exercise 1.4.15) that  $\{\sigma_{i,j} \tau_i\}$  represent the left cosets of  $N$  in  $G$ . Hence,

$$V = \bigoplus_{i,j} \sigma_{i,j} \tau_i W,$$

<sup>9</sup>the left cosets of a subgroup  $B$  of a group  $A$  are those of the form  $aB$ .

and each  $V_i = \bigoplus_j \sigma_{i,j} \tau_i W$  is a  $D_1$ -submodule of  $V$ , with  $V \cong \bigoplus_{i=1}^r V_i$  as  $D_1$ -modules. Thus, since  $\varphi_1$  is in  $D_1$ , we obtain

$$\det(1 - t\psi(\varphi_1) | V^{I_1}) = \prod_{i=1}^r \det(1 - t\psi(\varphi_1) | V_i^{I_1}),$$

and it suffices to show that

$$\det(1 - t\psi(\varphi_1) | V_i^{I_1}) = \det \left( 1 - t^{f_i} \tau(\varphi_1^{f_i}) | (\tau_i W)^{\tau_i N \tau_i^{-1} \cap I_1} \right).$$

Notice that  $V_i$  is the induced representation of  $W$  from  $D_1 \cap \tau_i N \tau_i^{-1}$  to  $D_1$  (indeed,  $V_i$  is obtained by summing over representatives for the cosets of  $D_1 \cap \tau_i N \tau_i^{-1}$  in  $D_1$ ). Thus, renaming

$$G := D_1, I := I_1, N := D_1 \cap \tau_i N \tau_i^{-1}, f := f_i, V := V_i, W := \tau_i W, \varphi := \varphi_1,$$

the desired equality can be rewritten as

$$\det(1 - t\psi(\varphi) | V^I) = \det \left( 1 - t^f \tau(\varphi^f) | W^{N \cap I} \right),$$

so that we are essentially reduced to the case  $r = 1$  and  $D_1 = G$ . The next and final reduction is to the case  $I = \{1\}$ . We claim that

$$V^I = \text{Ind}_{N/I \cap H}^{G/I} (W^{N \cap I}).$$

We show this from the definition. An element of  $V^I$  is by definition a function  $f : G \rightarrow W$  that satisfies

- a)  $f(g) = f(gi)$  for every  $g \in G, i \in I$  (this is the condition  $i \cdot f = f$  that ensures  $f \in V^I$ ). Notice that, since  $I$  is normal in  $G$ , right-invariance and left-invariance are equivalent, and therefore we also have  $f(ig) = f(g)$  for all  $g \in G, i \in I$
- b)  $h \cdot f(g) = f(hg)$  for every  $g \in G, h \in N$  (this is the condition that ensures that  $f$  is in  $\text{Ind}_N^G(W)$ ).

Now, the first condition is equivalent to  $f$  factoring via  $G/I$ . Moreover, any such function takes values in  $W^{N \cap I}$ , because

$$i \cdot f(g) = f(ig) = f(g)$$

for all  $i \in N \cap I$ . The claim follows. So, replacing  $G$  by  $G/I$ ,  $I$  by  $\{1\}$ , and  $W$  by  $W^{N \cap I}$ , we are reduced<sup>10</sup> to proving

$$\det(1 - t\psi(\varphi) | \text{Ind}_1^G(W)) = \det \left( 1 - t^f \tau(\varphi^f) | W \right).$$

In this case  $G$  is cyclic, generated by  $\varphi$ , and  $V = \bigoplus_{i=0}^{f-1} \varphi^i W$ . If  $A$  is the matrix of  $\tau(\varphi)$  (with respect to any basis  $w_1, \dots, w_d$  of  $W$ ), then the matrix of  $\psi(\varphi)$  with respect to the

<sup>10</sup>this essentially amounts to replacing  $L$  by  $L^I$ , which is normal over  $F$  since we are now assuming  $G = D$ .

basis  $\{\varphi^i w_j\}$  is

$$M := \begin{pmatrix} & & & & \boxed{A} \\ \boxed{\text{Id}_d} & & & & \\ & \boxed{\text{Id}_d} & & & \\ & & \ddots & & \\ & & & \boxed{\text{Id}_d} & \end{pmatrix},$$

a block matrix with  $f$  blocks on each row/column. An easy exercise in linear algebra (Exercise 1.4.14) now shows that

$$\det(1 - tM) = \det(1 - t^f \det A^f), \quad (1.13)$$

which finishes the proof. □

**Exercise 1.4.13.** Let  $L/F/K$  be extensions of number fields, with  $L/K$  and  $F/K$  both Galois. Let  $\mathfrak{Q}$  be a place of  $L$ , and let  $\mathfrak{P}, \mathfrak{p}$  be the places of  $F$  and  $K$  lying under  $\mathfrak{Q}$ . Let  $G = \text{Gal}(L/K)$ ,  $H = \text{Gal}(F/K)$ , and  $\pi : G \rightarrow H$  be the projection map. Show that  $\pi(I(\mathfrak{Q} | \mathfrak{p})) = I(\mathfrak{P} | \mathfrak{p})$ .

*Hint.* It is easy to show that  $\pi$  sends  $I(\mathfrak{Q} | \mathfrak{p})$  into  $I(\mathfrak{P} | \mathfrak{p})$ . For the surjectivity, take a pre-image in  $G$ , then try to modify it using elements in  $\ker(G \rightarrow H)$ .

**Exercise 1.4.14.** Prove the formula in Equation (1.13).

**Exercise 1.4.15.** With notation as in the proof of Theorem 1.4.12(3), prove that  $\{\sigma_{i,j}\tau_i\}$  is a set of representatives for the left cosets of  $N$  in  $G$ .

*Hint.* To show that they are the correct number, observe that

$$\begin{aligned} \sum_i \left| \frac{D_1}{\tau_i N \tau_i^{-1} \cap D_1} \right| &= \sum_i \left| \frac{\tau_i^{-1} D_1 \tau_i}{N \cap \tau_i^{-1} D_1 \tau_i} \right| = \sum_i \left| \frac{D_i}{N \cap D_i} \right| \\ &= \sum_i \left| \frac{D_i}{D'_i} \right| = \sum_i \frac{e(\mathfrak{Q}_i | \mathfrak{p}) f(\mathfrak{Q}_i | \mathfrak{p})}{e(\mathfrak{Q}_i | \mathfrak{P}_i) f(\mathfrak{Q}_i | \mathfrak{P}_i)} \\ &= \sum_i e(\mathfrak{P}_i | \mathfrak{p}) f(\mathfrak{P}_i | \mathfrak{p}) = [F : K] = [G : N]. \end{aligned}$$

To show that they represent distinct cosets, assume

$$\sigma_{i,j}\tau_i N = \sigma_{i',j'}\tau_{i'} N.$$

Prove that  $\tau_{i'}^{-1} \sigma_{i',j'}^{-1} \sigma_{i,j} \tau_i$  sends  $\mathfrak{Q}_i$  to  $\mathfrak{Q}_{i'}$  and  $\mathfrak{P}_i$  to  $\mathfrak{P}_{i'}$ . Conclude that  $i = i'$  and then that  $j = j'$ .

**Exercise 1.4.16.** Let  $L/K$  be a Galois extension of number fields with group  $G$  and let  $\rho$  be a finite-dimensional Galois representation of  $G$ . Set  $\chi(g) = \text{tr } \rho(g)$ . Prove the following formula for the logarithm of  $L(s, \rho)$ :

$$\log L(s, \rho) = \sum_{\mathfrak{p}} \sum_{m \geq 1} \frac{\chi(\mathfrak{p}^m)}{m(N\mathfrak{p})^{ms}},$$



where  $\chi(\mathfrak{p}^m)$  is defined as follows: let  $\mathfrak{P}$  be a prime of  $L$  lying over  $\mathfrak{p}$  and let  $e = e(\mathfrak{P} | \mathfrak{p})$ . Fix a representative  $\sigma \in G$  for the Artin symbol  $\left(\frac{L/K}{\mathfrak{p}}\right)$ . We set

$$\chi(\mathfrak{p}^m) := \frac{1}{e} \sum_{\tau \in I(\mathfrak{P} | \mathfrak{p})} \chi(\sigma^m \tau).$$

*Hint.* It can be useful to write the determinant of a linear map as the product of its eigenvalues. This leads to the identity

$$\begin{aligned} \log \det(1 - tA) &= \log \prod_i (1 - \lambda_i t) = \sum_i \log(1 - \lambda_i t) \\ &= - \sum_i \sum_{m \geq 1} \frac{(\lambda_i t)^m}{m} = - \sum_{m \geq 1} \frac{t^m}{m} \left( \sum_i \lambda_i^m \right) \\ &= - \sum_{m \geq 1} \operatorname{tr}(A^m) \frac{t^m}{m}. \end{aligned}$$

Up to some fiddling at the ramified places, this gives the required formula.

### 1.4.5 Artin's conjecture on analytic continuation

The following is one of the most important conjectures related to Artin's  $L$ -functions:

**Conjecture 1.4.17** (Artin). *Let  $L/K$  be a Galois extension of number fields with group  $G$ . If  $\rho$  is a non-trivial irreducible representation of  $G$ , then  $L(s, \rho)$  has analytic continuation to the whole complex plane.*

While Conjecture 1.4.17 is wide open, we sketch a proof of the fact that  $L(s, \rho)$  admits meromorphic continuation to the full complex plane.

**Theorem 1.4.18** (Meromorphic continuation for Artin  $L$ -functions). *For any Galois extension  $L/K$  with group  $G$  and every complex representation  $\rho$  of  $G$ , the  $L$ -function  $L(s, \rho)$  has meromorphic extension to the complex plane.*

For the proof, we will assume the following result in representation theory:

**Theorem 1.4.19** (Brauer's induction theorem). *Let  $G$  be a finite group and let  $\rho : G \rightarrow \operatorname{GL}_n(\mathbb{C})$  be a finite-dimensional complex representation. There exists finitely many subgroups  $H_1, \dots, H_r$  of  $G$ , characters  $\lambda_i : H_i \rightarrow \mathbb{S}^1$  for  $i = 1, \dots, r$ , and integers  $n_1, \dots, n_r$  such that*

$$\operatorname{tr}(\rho(g)) = \sum_{i=1}^r n_i \operatorname{tr}(\operatorname{Ind}_{H_i}^G(\lambda_i))(g).$$

*Sketch of proof of Theorem 1.4.18.* Let  $\chi = \operatorname{tr}(\rho)$  be the character of the representation  $\rho$ . Write  $\chi = \sum n_i \operatorname{tr} \operatorname{Ind}_{H_i}^G(\lambda_i)$  as in Brauer's theorem. Rearranging this equation, we get an equality of the form

$$\chi + \sum n_i \operatorname{tr} \operatorname{Ind}_{H_i}^G(\lambda_i) = \sum n'_j \operatorname{tr} \operatorname{Ind}_{H'_j}^G(\lambda'_j),$$

where the integers  $n_i, n'_j$  are now all strictly positive. Since the character of a complex representation of a finite group determines the representation itself, we obtain

$$\rho \oplus \bigoplus (\text{Ind}_{H_i}^G(\lambda_i))^{\oplus n_i} \cong \bigoplus \left( \text{Ind}_{H'_j}^G(\lambda'_j) \right)^{\oplus n'_j}.$$

In particular, we have

$$L\left(s, \rho \oplus \bigoplus (\text{Ind}_{H_i}^G(\lambda_i))^{\oplus n_i}\right) = L\left(s, \bigoplus \left( \text{Ind}_{H'_j}^G(\lambda'_j) \right)^{\oplus n'_j}\right)$$

The general formalism of Artin  $L$ -functions (Theorem 1.4.12) implies first

$$L(s, \rho) \cdot \prod_i L\left(s, \text{Ind}_{H_i}^G(\lambda_i)\right)^{n_i} = \prod_j L\left(s, \text{Ind}_{H'_j}^G(\lambda'_j)\right)^{n'_j}$$

and then

$$L(s, \rho) \cdot \prod_i L(s, \lambda_i)^{n_i} = \prod_j L(s, \lambda'_j)^{n'_j}.$$

Since the  $\lambda_i, \lambda'_j$  are characters with values in  $\mathbb{S}^1$ , they factor via some abelian (Galois) group, hence they are Hecke  $L$ -functions. Thus, each  $L(s, \lambda_i)$  and  $L(s, \lambda'_j)$  admits meromorphic continuation by Theorem 1.4.11. Since the above formula expresses  $L(s, \rho)$  as a ratio of (products of) such Hecke  $L$ -functions,  $L(s, \rho)$  also has meromorphic continuation to the complex plane.  $\square$

**Remark 1.4.20.** This theorem is perhaps part of the motivation for Artin's conviction that *abelian  $L$ -functions should be sufficient to understand arbitrary extensions of number fields*. In other words, class field theory (the description of *abelian* extensions of a number field) should contain in itself all the necessary ingredients to describe arbitrary (Galois) extensions of number fields. No one has (yet) been able to fully realise Artin's dream (and extending class field theory to arbitrary non-abelian extensions remains a central problem in number theory), but since Artin had enormous insight in the theory of  $L$ -functions, I wouldn't be too quick to dismiss his intuition!

### 1.4.6 Factorisation of the Dedekind $\zeta$ -function

**Theorem 1.4.21** (Factorisation of the Dedekind  $\zeta$  function in terms of Artin  $L$ -functions). *Let  $L/K$  be a Galois extension of number fields with group  $G$ . The function  $\zeta_L(s)$  factors as*

$$\zeta_L(s) = \zeta_K(s) \prod_{\rho \neq 1} L(s, \rho)^{\dim \rho},$$

where the product runs over the non-trivial irreducible complex representations<sup>11</sup> of  $G$ .

*Proof.* This is a special case of Theorem 1.4.12. Specifically, in the setting of that theorem, take  $F = L$  (so that  $N = \{1\}$ ) and  $\sigma$  to be the trivial representation of the trivial group.

<sup>11</sup>let me take another page from the physicists' books and write *irrep* for *irreducible complex representation*.

Then  $\text{Ind}_N^G(\sigma)$  is the regular representation of  $G$ , which – as it is well-known – decomposes as  $\bigoplus_{\rho \text{ irrep of } G} \rho^{\oplus \dim \rho}$ . Hence, applying properties (3) and (1) in Theorem 1.4.12 we get

$$L(s, 1) = L(s, \text{Ind}_N^G(1)) = L\left(s, \bigoplus_{\rho \text{ irrep of } G} \rho^{\oplus \dim \rho}\right) = \prod_{\rho \text{ irrep of } G} L(s, \rho)^{\dim \rho}.$$

Finally, the trivial representation 1 of  $N$  gives the Dedekind  $\zeta$  function of  $L$ , while the trivial representation 1 of  $G$  gives  $\zeta_K$ . Thus, the previous equation can be rewritten as

$$\zeta_L(s) = \zeta_K(s) \prod_{\substack{\rho \text{ irrep of } G \\ \rho \neq 1}} L(s, \rho)^{\dim \rho},$$

as desired. □

**Corollary 1.4.22.** *For every integer  $n \geq 2$  we have the factorisation*

$$\zeta_{\mathbb{Q}(\zeta_n)} = \zeta(s) \prod_{\substack{\chi \text{ non-trivial Dirichlet} \\ \text{character modulo } n}} L(s, \tilde{\chi}),$$

where  $\tilde{\chi}$  is the primitive character corresponding to  $\chi$ .

*Proof.* Follows from Theorem 1.4.21 together with our identification of Dirichlet's  $L$ -functions as special Artin  $L$ -functions (see Proposition 1.4.6 and Remark 1.4.7). Also note that every complex representation of the abelian group  $G = \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$  is 1-dimensional, hence a character. □

In the interest of keeping these notes more accessible, we will give below in Proposition 1.5.30 an independent proof of (a slightly weaker version of) Corollary 1.4.22 that avoids all the machinery of representation theory and Artin  $L$ -functions. This weaker version will be sufficient for the proof of Dirichlet's theorem on arithmetic progressions.

## 1.5 Dirichlet's theorem on arithmetic progressions

In this section we will *assume* Theorems 1.1.18 and 1.1.26 and show that these analytic results have deep arithmetic consequences. In particular, we will show that they imply rather easily Dirichlet's famous theorem on primes in arithmetic progressions, namely, Theorem 1.3.19. We start by discussing a notion of duality for (finite) abelian groups.

### 1.5.1 Pontryagin duality: finite case

The central notion in this section is that of *dual* group.

**Definition 1.5.1** (Dual group, finite case). Let  $G$  be a finite abelian group. The **dual group** (or **group of characters**) of  $G$  is the set

$$\hat{G} := \text{Hom}(G, \mathbb{C}^\times),$$

equipped with the operation of pointwise product (that is,  $(\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g)$ ). The elements of  $\hat{G}$  are called the **characters** of  $G$ .

**Remark 1.5.2** (Connection to representation theory). Recall that every irreducible complex representation of an abelian group  $G$  is 1-dimensional. The elements of  $\hat{G}$  are in bijection with the 1-dimensional complex representations of  $G$ : a 1-dimensional representation coincides with its character, which justifies the name.

As  $G$  is finite, the image of any character  $\chi : G \rightarrow \mathbb{C}^\times$  has order dividing  $|G|$ , which implies that  $\chi(G) \subseteq \mu_{|G|}$ , where  $\mu_{|G|}$  is the set of roots of unity of order dividing  $|G|$ . Hence, we can identify  $\hat{G}$  with  $\text{Hom}(G, \mu_{|G|})$ . With this observation in hand, and using the structure theorem for finite abelian groups, the following result becomes an easy exercise:

**Exercise 1.5.3.** The groups  $G$  and  $\hat{G}$  are isomorphic.

**Remark 1.5.4.** Let  $\chi \in \hat{G}$  be a character. We have already observed that  $\chi(g)$  is a root of unity for every  $g \in G$ . The inverse and the complex conjugate of any root of unity coincide, hence we obtain

$$\overline{\chi(g)} = \chi(g)^{-1} = \chi(g^{-1}).$$

**Remark 1.5.5.** The group  $\hat{G}$  should be compared with the dual of a vector space. As in the linear-algebraic setting,  $\hat{G}$  and  $G$  are isomorphic, but only non-canonically. On the other hand, we will prove below that  $\hat{\hat{G}} \cong G$  canonically, see Proposition 1.5.8

**Remark 1.5.6.** There is a pairing  $\langle \cdot, \cdot \rangle : G \times \hat{G} \rightarrow \mathbb{C}$  given by  $\langle g, \chi \rangle = \chi(g)$ . This pairing is perfect: the only element  $g \in G$  such that  $\langle g, \chi \rangle = 1$  for all  $\chi \in \hat{G}$  is the identity of  $G$ , and the only character  $\chi$  such that  $\langle g, \chi \rangle = 1$  for all  $g \in G$  is the trivial character (the identity element of  $\hat{G}$ , that is, the homomorphism that sends every element of  $G$  to 1).

**Exercise 1.5.7.** Prove the claims made in Remark 1.5.6.

**Proposition 1.5.8** (Canonical isomorphism of  $G$  with  $\hat{\hat{G}}$ ). *The map*

$$\begin{aligned} \Psi : G &\rightarrow \hat{\hat{G}} \\ g &\mapsto \psi_g, \end{aligned}$$

where the homomorphism  $\psi_g : \hat{G} \rightarrow \mathbb{C}^\times$  (which is an element of  $\hat{\hat{G}}$ ) is defined by

$$\begin{aligned} \psi_g : \hat{G} &\rightarrow \mathbb{C}^\times \\ \chi &\mapsto \chi(g), \end{aligned}$$

gives an isomorphism  $G \cong \hat{\hat{G}}$ .

*Proof.* The homomorphism  $\Psi$  is injective by Remark 1.5.6. By Exercise 1.5.3, one has  $|G| = |\hat{G}| = |\hat{\hat{G}}|$ , so  $\Psi$  is also surjective, hence an isomorphism.  $\square$

**Remark 1.5.9.** Proposition 1.5.8, which is almost trivial when  $G$  is finite, can be generalised to a suitable class of infinite abelian groups  $G$ . This more general statement often goes under the name of Pontryagin duality, see Theorem 2.2.2.

To finish our introduction to the dual group, we remark on its functorial properties.

**Proposition 1.5.10** (Functoriality of  $G \mapsto \hat{G}$ ). *The following hold:*

1. *The association  $G \mapsto \hat{G}$  can be extended to a contravariant functor from the category of finite abelian groups to itself by letting it act on arrows as follows: if  $f : G \rightarrow H$  is a group homomorphism, we define*

$$\begin{aligned} \hat{f} : \hat{H} &\rightarrow \hat{G} \\ \chi &\mapsto \chi \circ f. \end{aligned}$$

2. *This functor is exact: for every short exact sequence*

$$0 \rightarrow H \xrightarrow{\iota} G \xrightarrow{\pi} G/H \rightarrow 0,$$

*the dual sequence*

$$0 \rightarrow \widehat{G/H} \xrightarrow{\hat{\pi}} \hat{G} \xrightarrow{\hat{\iota}} \hat{H} \rightarrow 0$$

*is also exact. Note that  $\hat{\iota}$  is simply the restriction map: given an element  $\chi \in \hat{G}$ , that is, a homomorphism  $\chi : G \rightarrow \mathbb{C}^\times$ , the character  $\hat{\iota}(\chi) \in \hat{H}$  is simply  $\chi|_H$ .*

**Exercise 1.5.11.** Prove Proposition 1.5.10.

After these formal preliminaries, we are ready to state and prove the orthogonality relations, which we will then use to prove a Fourier inversion theorem for functions on abelian groups.

**Proposition 1.5.12** (Orthogonality relations I). *Fix  $g_0 \in G$  and  $\chi_0 \in \hat{G}$ . We have*

$$\sum_{\chi \in \hat{G}} \chi(g_0) = \begin{cases} 0, & \text{if } g_0 \neq \text{id}_G \\ |G|, & \text{otherwise} \end{cases}$$

and

$$\sum_{g \in G} \chi_0(g) = \begin{cases} 0, & \text{if } \chi_0 \neq \text{id}_{\hat{G}} \\ |G|, & \text{otherwise.} \end{cases}$$

*Proof.* We begin with the second statement. If  $\chi_0$  is the identity of  $\hat{G}$ , the statement is trivial. Otherwise, let  $a \in G$  be an element such that  $\chi_0(a) \neq 1$ . Setting  $S := \sum_{g \in G} \chi_0(g)$ , we obtain

$$\chi_0(a)S = \sum_{g \in G} \chi_0(a)\chi_0(g) = \sum_{g \in G} \chi_0(ag) = \sum_{g \in G} \chi_0(g) = S,$$

hence  $(\chi_0(a) - 1)S = 0$ . Since  $\chi_0(a) \neq 1$ , this implies  $S = 0$ .

The first statement follows upon applying the first to  $\hat{G}$  and using the identification  $\hat{\hat{G}} \cong G$  provided by Proposition 1.5.8.  $\square$

**Corollary 1.5.13** (Orthogonality relations II).

1. *Let  $\chi_1, \chi_2$  be elements of  $\hat{G}$ . We have*

$$\sum_{g \in G} \chi_1(g) \overline{\chi_2(g)} = \begin{cases} 0, & \text{if } \chi_1 \neq \chi_2 \\ |G|, & \text{otherwise.} \end{cases}$$

2. Let  $g, h$  be elements of  $G$ . We have

$$\sum_{\chi \in \hat{G}} \chi(g) \overline{\chi(h)} = \begin{cases} 0, & \text{if } g \neq h \\ |G|, & \text{otherwise.} \end{cases}$$

*Proof.* For the first statement, observe that  $\chi_1(g) \overline{\chi_2(g)} = \chi_1(g) \chi_2(g)^{-1} = (\chi_1 \chi_2^{-1})(g)$  by Remark 1.5.4 and apply Proposition 1.5.12 to the character  $\chi_1 \chi_2^{-1}$ .

Similarly, for the second statement observe that  $\chi(g) \overline{\chi(h)} = \chi(gh^{-1})$  and apply Proposition 1.5.12 to the element  $gh^{-1}$ .  $\square$

For later use, we introduce the following handy notation:

**Definition 1.5.14.** Let  $G$  be a group. The function  $\delta : G^2 \rightarrow \{0, 1\}$  is defined by

$$\delta(g, h) = \begin{cases} 1, & \text{if } g = h \\ 0, & \text{otherwise.} \end{cases}$$

We will usually write  $\delta_{g,h}$  instead of  $\delta(g, h)$ .

**Definition 1.5.15** (Abstract Fourier transform, finite case). Let  $f$  be any function  $G \rightarrow \mathbb{C}$ . The **Fourier transform** of  $f$ , denoted by  $\hat{f}$ , is the function

$$\begin{aligned} \hat{f} : \hat{G} &\rightarrow \mathbb{C} \\ \chi &\mapsto \frac{1}{|G|} \sum_{g \in G} f(g) \overline{\chi(g)}. \end{aligned}$$

**Remark 1.5.16.** Exactly as in the real case, there are several natural normalisations for the Fourier transform. The abstract theory we will discuss in Section 2.2 helps clarify the nature of these normalisations.

**Theorem 1.5.17** (Fourier inversion, finite case). Let  $f : G \rightarrow \mathbb{C}$  be any function and let  $\hat{f} : \hat{G} \rightarrow \mathbb{C}$  be its Fourier transform. We have

$$f(g) = \sum_{\chi \in \hat{G}} \hat{f}(\chi) \chi(g).$$

*Proof.* Replacing the definition of  $\hat{f}$  we obtain

$$\begin{aligned} \sum_{\chi \in \hat{G}} \hat{f}(\chi) \chi(g) &= \sum_{\chi \in \hat{G}} \left( \frac{1}{|G|} \sum_{h \in G} f(h) \overline{\chi(h)} \right) \chi(g) \\ &= \frac{1}{|G|} \sum_{h \in G} f(h) \left( \sum_{\chi \in \hat{G}} \overline{\chi(h)} \chi(g) \right) \end{aligned}$$

We can now use Corollary 1.5.13 to rewrite the inner sum as  $|G| \delta_{g,h}$ , obtaining

$$\sum_{\chi \in \hat{G}} \hat{f}(\chi) \chi(g) = \frac{1}{|G|} \sum_{h \in G} f(h) |G| \delta_{g,h} = \sum_{h \in G} f(h) \delta_{g,h} = f(g).$$

$\square$

**Example 1.5.18** (Fourier transform of the characteristic function of a singleton). Let  $G$  be a finite abelian group, let  $a \in G$  be a fixed element, and let  $f := \mathbf{1}_a$  be the function  $\mathbf{1}_a(g) = \delta_{a,g}$ . Its Fourier transform is given by

$$\hat{f}(\chi) = \frac{1}{|G|} \sum_{g \in G} \mathbf{1}_a(g) \overline{\chi(g)} = \frac{1}{|G|} \overline{\chi(a)} = \frac{1}{|G|} \chi(a)^{-1}.$$

Applying Theorem 1.5.17 we obtain the following representation for the function  $\mathbf{1}_a$ :

$$\mathbf{1}_a(g) = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \chi(a)^{-1} \chi(g),$$

which recovers part of Corollary 1.5.13.

**Exercise 1.5.19** (Squaring the Fourier transform). Let  $G$  be a finite abelian group and let  $f : G \rightarrow \mathbb{C}$  be a function. The Fourier transform  $\hat{f}$  is a function  $\hat{G} \rightarrow \mathbb{C}$ , so we can take its Fourier transform, obtaining  $\hat{\hat{f}} : \hat{G} \rightarrow \mathbb{C}$ . Using Proposition 1.5.8 we may identify  $\hat{\hat{f}}$  to a function  $\hat{\hat{f}} : G \rightarrow \mathbb{C}$ . Prove that  $\hat{\hat{f}}(g) = \frac{1}{|G|} f(g^{-1})$  for all  $g \in G$ .

## 1.5.2 Densities

We now define two notions of *density* for sets of prime numbers (or, more generally, prime ideals in a number field): the *natural density* and *Dirichlet density*. Even though the natural density is (as the name suggests) more ‘natural’, we will mostly focus on the notion of Dirichlet density, which is easier to treat from an analytic point of view.

**Definition 1.5.20.** Let  $K$  be a number field and let  $S$  be a set of (non-zero) prime ideals of  $\mathcal{O}_K$ . We define the **natural density** of  $S$  as

$$\lim_{T \rightarrow \infty} \frac{\#\{\mathfrak{p} \in S : N(\mathfrak{p}) \leq T\}}{\#\{\mathfrak{p} \text{ non-zero prime of } \mathcal{O}_K : N(\mathfrak{p}) \leq T\}},$$

provided that the limit exists.

**Definition 1.5.21** (Dirichlet density). Let  $K$  be a number field and let  $S$  be a subset of the set of nonzero prime ideals of  $\mathcal{O}_K$ . We define the **Dirichlet density** of  $S$  as

$$\text{Dens}_K(S) = \lim_{s \rightarrow 1^+} \frac{\sum_{\mathfrak{p} \in S} N(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p} \text{ nonzero prime of } \mathcal{O}_K} N(\mathfrak{p})^{-s}}, \quad (1.14)$$

provided that the limit exists. We will omit the subscript  $K$  if it is clear from context.

**Remark 1.5.22.** There is at least another variant of the definition of Dirichlet density in the literature. For the sake of simplicity, we define it only in the case of the number field  $K$  being  $\mathbb{Q}$ : if  $S$  is a set of prime numbers, the **logarithmic density** of  $S$  is

$$\lim_{x \rightarrow \infty} \frac{\sum_{p \in S, p \leq x} \frac{1}{p}}{\sum_{p \leq x} \frac{1}{p}},$$

if the limit exists.

The following exercise shows that the notion of Dirichlet density is a genuine extension of the notion of natural density:

**Exercise 1.5.23.** Let  $K$  be a number field and let  $S$  be a set of non-zero prime ideals. Prove that, if  $S$  admits natural density, then it also admits Dirichlet density, and the two coincide.

On the other hand, it is a non-trivial exercise in analytic number theory to show that the Dirichlet and logarithmic densities of any set of primes coincide:

**Exercise 1.5.24** ( $\star$ ). Show that, for  $K = \mathbb{Q}$ , a set of primes admits Dirichlet density if and only if it admits logarithmic density, and the two coincide.

*Hint.* Here is a possible strategy.

1. Define

$$a_n = \begin{cases} 1/n, & \text{if } n \in S \\ 0, & \text{otherwise} \end{cases}$$

and  $A(u) = \sum_{n \leq u} a_n$ ,  $\varphi(u) = u^{1-s}$ . Show that  $S$  admits logarithmic density  $\delta_S$  if and only if  $A(u) = (\delta_S + o(1)) \log \log u$ .

2. Assume that  $S$  does admit logarithmic density. By a suitable summation by parts, show that

$$\sum_{p \in S} \frac{1}{p^s} = (s-1) \int_1^\infty A(u) u^{-s} du.$$

3. Prove that

$$(s-1) \int_1^\infty u^{-s} \log \log u du \sim \log \left( \frac{1}{s-1} \right) \text{ as } s \rightarrow 1^+.$$

Deduce that, if  $S$  admits logarithmic density, then it admits Dirichlet density and the two coincide.

4. Show the following general estimate on primes: one has  $\sum_{p \leq t} \left( \frac{1}{p} - \frac{1}{p^{1+1/\log t}} \right) = O(1)$ , and in particular the sum is  $o(\log \log t)$ .

5. Show that  $\sum_{p > t} p^{-1-1/\log t} = O(1) = o(\log \log t)$ . (You may need some weak version of the prime number theorem.)

6. Suppose now that  $S$  admits Dirichlet density  $\delta$ . Introduce  $N(s) = \frac{\sum_{p \in S} p^{-s}}{\sum_p p^{-s}}$  and observe that  $N(s) \sim (\delta + o(1)) \log(1/(s-1))$  for  $s \rightarrow 1^+$ . Prove that  $\sum_{p \in S, p \leq t} \frac{1}{p} = N(1+1/\log t) + o(\log \log t)$  and deduce that  $S$  admits logarithmic density equal to  $\delta$ .

**Remark 1.5.25.** Exercise 1.5.24 is certainly very well-known, but I've never been able to find this statement in the literature. Andrea Tedesco gave a detailed solution in his bachelor's dissertation (Università di Pisa, 2021-2022).

**Remark 1.5.26.** The Dirichlet density satisfies the following basic properties:

1.  $\text{Dens}(S) \in [0, 1]$  for every set  $S$  of primes admitting Dirichlet density.
2. Let  $S$  be the set of all prime numbers: then it follows immediately from the definition that  $\text{Dens}(S) = 1$ .



3. Let  $S$  be a finite set: again, it follows immediately from the definition that  $\text{Dens}(S) = 0$ . In particular, if  $\text{Dens}(S)$  exists and is positive, then  $S$  is infinite.
4. Let  $S_1, S_2$  be sets of primes, each admitting Dirichlet density, and suppose that  $S_1 \cup S_2$  admits density. Then,

$$\text{Dens}(S_1 \cup S_2) \leq \text{Dens}(S_1) + \text{Dens}(S_2).$$

A sufficient condition for equality to hold is  $S_1 \cap S_2 = \emptyset$ .

Furthermore, we will show below that  $\sum_{\mathfrak{p} \text{ nonzero prime of } \mathcal{O}_K} N(\mathfrak{p})^{-s}$  is asymptotic to  $\log\left(\frac{1}{s-1}\right)$  as  $s \rightarrow 1^+$  (see Proposition 1.5.34 and Exercise 1.5.28), so that the denominator in Equation (1.14) can be replaced by  $\log\left(\frac{1}{s-1}\right)$ .

Even though the density doesn't necessarily exist for an arbitrary set of primes, the following variants certainly do:

**Definition 1.5.27** (Upper and lower density). Let  $K$  be a number field and let  $S$  be a subset of the set of prime ideals of  $\mathcal{O}_K$ . We define the **upper and lower density** of  $S$  as

$$\text{Dens}_K^+(S) = \limsup_{s \rightarrow 1^+} \frac{\sum_{\mathfrak{p} \in S} N(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p} \text{ nonzero prime of } \mathcal{O}_K} N(\mathfrak{p})^{-s}}$$

and

$$\text{Dens}_K^-(S) = \liminf_{s \rightarrow 1^+} \frac{\sum_{\mathfrak{p} \in S} N(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p} \text{ nonzero prime of } \mathcal{O}_K} N(\mathfrak{p})^{-s}},$$

respectively. We will omit the subscript  $K$  if it is clear from the context.

**Exercise 1.5.28.** Prove that the denominator  $\sum_{\mathfrak{p} \text{ nonzero prime of } \mathcal{O}_K} N(\mathfrak{p})^{-s}$  appearing in (1.14) is asymptotic to  $\log\left(\frac{1}{s-1}\right)$  as  $s \rightarrow 1^+$ . (You can start by looking at Proposition 1.5.34).

We also recall another general fact in the form of the following exercise.

**Exercise 1.5.29.** Let  $K$  be a number field and  $S$  be a set of primes of  $K$ . Denote by  $S^{(1)}$  the subset of  $S$  consisting of those prime ideals  $\mathfrak{p}$  for which the size of  $\mathcal{O}_K/\mathfrak{p}$  is a prime number. Prove that  $\text{Dens}^+(S^{(1)}) = \text{Dens}^+(S)$  and  $\text{Dens}^-(S^{(1)}) = \text{Dens}^-(S)$ . In particular, if  $S$  admits density, then so does  $S^{(1)}$ , and the densities coincide.

### 1.5.3 Factorisation of the cyclotomic Dedekind $\zeta$ function, reprise

As promised, we give an essentially self-contained proof of (a version of) Corollary 1.4.22.

**Proposition 1.5.30** (Slightly weaker version of Corollary 1.4.22). *For every integer  $n \geq 2$  we have a factorisation*

$$\zeta_{\mathbb{Q}(\zeta_n)} = f(s)\zeta(s) \prod_{\substack{\chi \text{ Dirichlet character} \\ \text{modulo } n}} L(s, \chi),$$

where  $f(s)$  is holomorphic and nonvanishing in  $\{\Re s > 0\}$ .

*Proof.* Both sides are given by suitable Euler products. If  $p$  is a fixed prime, the local contributions at  $p$  to both sides of the desired equality are of the form  $(1 - \zeta_n^j p^{-s})^{\pm 1}$ . Each such function is meromorphic on all of  $\mathbb{C}$ , and all of its zeroes and poles lie on the line  $\Re(s) = 0$ , where  $|\zeta_n^j p^{-s}| = 1$ . Thus, ignoring the finitely many ramified primes (which contribute to the function  $f(s)$ ), it suffices to prove that

$$\prod_{\mathfrak{p}|p} (1 - N(\mathfrak{p})^{-s})^{-1} = \prod_{\chi} (1 - \chi(p)p^{-s})^{-1}, \quad (1.15)$$

where  $\mathfrak{p}$  ranges over the prime divisors of  $p$  in  $\mathbb{Z}[\zeta_n]$  (the ring of integers of  $\mathbb{Q}(\zeta_n)$ ) and  $\chi$  ranges over *all* Dirichlet characters modulo  $n$ , including the principal one. Suppose that the multiplicative order of  $p$  modulo  $n$  is equal to  $f$ : then, the Frobenius at  $p$  is an element of  $G := \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$  of order  $f$ , and by definition this means that the finite field  $\mathbb{F}_{\mathfrak{p}}$  is isomorphic to  $\mathbb{F}_{p^f}$  (since  $\text{Gal}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p)$  is isomorphic to the subgroup of  $G$  generated by the Frobenius at  $p$ ). It follows from Equation (1.10) that there are precisely  $r = \varphi(n)/f$  primes  $\mathfrak{p}$  of  $\mathbb{Q}(\zeta_n)$  lying over  $p$ , and for each of them one has  $N(\mathfrak{p}) = p^f$ . Thus, the left-hand side of (1.15) can be rewritten as  $(1 - p^{-fs})^{-\varphi(n)/f}$ .

We now turn to the right-hand side of (1.15). Let  $H$  be the cyclic subgroup of  $(\mathbb{Z}/n\mathbb{Z})^\times$  generated by the class of  $p$ . By definition,  $|H| = f$ . In (1.15),  $\chi$  ranges over the dual group  $\hat{G}$ , but clearly only the image of  $\chi$  in  $\hat{H}$  is important. Since  $\hat{G} \rightarrow \hat{H}$  is surjective with kernel given by  $\widehat{G/H}$  (Proposition 1.5.10), every character of  $H$  appears  $|\widehat{G/H}| = |G/H| = \varphi(n)/f$  times in this product. Moreover, since  $\hat{H}$  is also cyclic, generated by the character that sends  $p$  to a primitive  $f$ -th root of unity, we obtain that the right-hand side of (1.15) can be written as

$$\prod_{j=1}^f (1 - \zeta_f^j p^{-s})^{-\varphi(n)/f}.$$

The claim now follows from the elementary identity  $\prod_{j=1}^f (1 - \zeta_f^j T) = 1 - T^f$ .  $\square$

### 1.5.4 Infinitely many primes in arithmetic progressions

The tools we have developed (or assumed) now allow us to give a quick proof of Dirichlet's theorem (Theorem 1.3.19), which we can now restate in a stronger form:

**Theorem 1.5.31** (Dirichlet's theorem, quantitative form). *Let  $a, m$  be positive integers with  $(a, m) = 1$ . The set*

$$\{p \text{ prime} : p \equiv a \pmod{m}\}$$

*has Dirichlet density  $\frac{1}{\varphi(m)}$ .*

Note that this form clearly implies Theorem 1.3.19 by Remark 1.5.26. Theorem 1.5.31 is also true with 'Dirichlet density' replaced by 'natural density', but the proof is harder (it involves essentially the same difficulties that one faces when proving the Prime Number Theorem). By Exercise 1.5.23, the version for natural density implies the version given above.

The crux of the proof lies in the following fact:

**Theorem 1.5.32** (Dirichlet). *Let  $m \geq 1$  be an integer and  $\chi$  be a non-principal character of  $(\mathbb{Z}/m\mathbb{Z})^\times$ . The 'special value'  $L(1, \chi)$  is finite and nonzero.*

*Proof.* By Theorem 1.1.26,  $L(1, \chi)$  is well-defined. Consider the formula of Corollary 1.4.22,

$$\zeta_{\mathbb{Q}(\zeta_m)}(s) = \zeta(s) \prod_{\substack{\chi \text{ non-principal Dirichlet} \\ \text{character modulo } m}} L(s, \tilde{\chi}).$$

Since both  $\zeta_{\mathbb{Q}(\zeta_m)}$  and  $\zeta(s)$  have a simple pole at  $s = 1$  (Theorem 1.1.18), this shows that  $\prod_{\substack{\chi \text{ non-principal Dirichlet} \\ \text{character modulo } m}} L(s, \tilde{\chi})$  is bounded and nonzero around  $s = 1$ . Since each  $L(s, \tilde{\chi})$  is holomorphic around  $s = 1$  (Theorem 1.1.26), this implies that each  $L(1, \chi)$  is nonzero.

Note that the same argument also goes through if one uses Proposition 1.5.30 instead of Corollary 1.4.22.  $\square$

**Lemma 1.5.33.** *The sum  $\sum_{p,k \geq 2} p^{-ks}$  remains bounded as  $s \rightarrow 1^+$ .*

*Proof.* This is easy:

$$\sum_{p,k \geq 2} \frac{1}{p^{ks}} = \sum_p \frac{1}{p^s(p^s - 1)} \leq \sum_p \frac{1}{p(p-1)} \leq \sum_{n \geq 2} \frac{1}{n(n-1)} = 1.$$

$\square$

**Proposition 1.5.34.** *Let  $m$  be a positive integer and let  $\chi$  be a character of  $(\mathbb{Z}/m\mathbb{Z})^\times$ . We consider the function  $\sum_p \chi(p) \frac{1}{p^s}$ .*

1. *If  $\chi$  is the trivial character,  $\sum_p \frac{1}{p^s}$  is asymptotic to  $\log\left(\frac{1}{s-1}\right)$  as  $s \rightarrow 1^+$ .*
2. *If  $\chi$  is non-trivial,  $\sum_p \chi(p) \frac{1}{p^s}$  stays bounded as  $s \rightarrow 1$ .*

*Proof.* 1. We have

$$\begin{aligned} \log \zeta(s) &= \log \prod_p (1 - p^{-s})^{-1} = - \sum_p \log(1 - p^{-s}) \\ &= \sum_p \sum_k \frac{1}{kp^{ks}} = \sum_p p^{-s} + \sum_{p,k \geq 2} \frac{1}{kp^{ks}}. \end{aligned}$$

Since  $\zeta(s) \sim \frac{1}{s-1}$  as  $s \rightarrow 1^+$  (Theorem 1.1.3), the first claim follows from the fact that  $\sum_{p,k \geq 2} \frac{1}{kp^{ks}}$  stays bounded as  $s \rightarrow 1$ . Since  $\sum_{p,k \geq 2} \frac{1}{kp^{ks}} \leq \sum_{p,k \geq 2} \frac{1}{p^{ks}}$ , this is true by Lemma 1.5.33.

2. We proceed in a similar fashion. We have

$$\log L(s, \chi) = \log \prod_p (1 - \chi(p)p^{-s})^{-1} = - \sum_p \log(1 - \chi(p)p^{-s}) = \sum_p \sum_{k \geq 1} \frac{\chi(p)^k}{kp^{ks}},$$

and this time we know (from Theorems 1.1.26 and 1.5.32) that  $L(s, \chi)$  is holomorphic **and nonzero** in a neighbourhood of  $s = 1$ , so that  $\log L(s, \chi)$  is also holomorphic at  $s = 1$ .

In the above expression, the sum for  $k \geq 2$  stays bounded as  $s \rightarrow 1^+$  (take absolute values and apply Lemma 1.5.33), so we obtain as desired that  $\sum_p \frac{\chi(p)}{p^s}$  is bounded as  $s \rightarrow 1^+$ .  $\square$

*Proof of Theorem 1.5.31.* Fix  $s > 1$  and consider the sum

$$\sum_{\substack{p \leq x \\ p \equiv a \pmod{m}}} \frac{1}{p^s} = \sum_{p \leq x} \mathbf{1}_a(p) \frac{1}{p^s},$$

where  $\mathbf{1}_a(x)$  is the characteristic function of the subset  $\{n \in \mathbb{Z} : n \equiv a \pmod{m}\}$  of  $\mathbb{Z}$ . Clearly,  $\mathbf{1}_a(x)$  factors via  $\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$ . By Example 1.5.18, we can then rewrite the above sum as

$$\frac{1}{\varphi(m)} \sum_{p \leq x} \sum_{\chi \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(a)^{-1} \chi(p) \frac{1}{p^s} = \frac{1}{\varphi(m)} \sum_{\chi \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(a)^{-1} \sum_{p \leq x} \chi(p) \frac{1}{p^s}.$$

Passing to the limit for  $x \rightarrow \infty$  and applying Proposition 1.5.34 we obtain

$$\sum_{\substack{p \equiv a \\ \pmod{m}}} \frac{1}{p^s} = \frac{1}{\varphi(m)} \log \left( \frac{1}{s-1} \right) (1 + o(1)) + \sum_{\substack{\chi \in (\mathbb{Z}/m\mathbb{Z})^\times \\ \chi \neq 1}} O(1) \quad \text{as } s \rightarrow 1^+,$$

which, dividing by  $-\log(s-1)$  and passing to the limit  $s \rightarrow 1$ , yields that the Dirichlet density of  $\{p \text{ prime} \mid p \equiv a \pmod{m}\}$  is equal to  $\frac{1}{\varphi(m)}$ , as claimed.  $\square$

### 1.5.5 The philosophy of special values

Dirichlet's original proof of Theorem 1.5.31 follows<sup>12</sup> basically the approach outlined above, with the main difference being in the proof of Theorem 1.5.32. In this section, we sketch briefly the main idea, which helps demonstrate one of the key features of  $L$ -functions: values of  $L$ -functions (especially at points where they are not naturally defined) encode arithmetic information.

*Sketch of proof of Theorem 1.5.32.* Consider the factorisation in Theorem 1.4.21,

$$\zeta_{\mathbb{Q}(\zeta_m)}(s) = \zeta(s) \prod_{\chi \neq 1} L(s, \tilde{\chi}). \quad (1.16)$$

Since  $L(s, \tilde{\chi}) = f(s)L(s, \chi)$  for some function  $f(s)$  which is holomorphic and nonvanishing near  $s = 1$  (see Proposition 1.4.6 (4)), the quantity  $L(1, \tilde{\chi})$  is nonzero if and only if  $L(s, \chi)$  is. Suppose that for some  $\chi$  with  $\bar{\chi} \neq \chi$  we had  $L(1, \chi) = 0$ . Then it is immediate to see that also  $\overline{L(1, \chi)} = L(1, \bar{\chi}) = 0$ , hence the right-hand side of (1.16) vanishes at  $s = 1$  (since the *simple* pole of  $\zeta(s)$  cancels out with the zero of  $L(s, \chi)$ , and then  $L(1, \bar{\chi}) = 0$  implies the vanishing). This is clearly a contradiction, because

$$\lim_{s \rightarrow 1^+} \zeta_{\mathbb{Q}(\zeta_m)}(s) \geq \lim_{s \rightarrow 1^+} \sum_{I \triangleleft \mathbb{Z}[\zeta_m]} N(I)^{-s} \geq \lim_{s \rightarrow 1^+} 1 = 1.$$

Hence, it only remains to show that  $L(1, \chi) \neq 0$  when  $\chi = \bar{\chi}$ , that is, when  $\chi$  takes values in  $\{\pm 1\}$ . Now, such a character (seen as a character  $(\mathbb{Z}/m\mathbb{Z})^\times \rightarrow \{\pm 1\}$ ) defines – via taking the

<sup>12</sup>I am not a historian of mathematics, so take this statement with a pinch of salt.

fixed field of the kernel – a quadratic extension  $\mathbb{Q}(\sqrt{a})$  of  $\mathbb{Q}$ . Using Theorem 1.4.21 again (in a very simple case), one obtains

$$\zeta_{\mathbb{Q}(\sqrt{a})}(s) = \zeta(s)L(s, \tilde{\chi}).$$

The claim now follows from Theorem 1.5.35 below, where the crucial point is that the *arithmetic* interpretation of the limit immediately implies its non-vanishing.  $\square$

The following is another famous theorem of Dirichlet (at least in the case  $K$  is a quadratic number field; I'm not sure who the general form is due to).

**Theorem 1.5.35** (Analytic class number formula). *Let  $K$  be a number field, with standard invariants  $d_K$  (discriminant),  $h_K$  (class number),  $(r_1, r_2)$  (signature), and  $R_K$  (regulator). Let  $w_K$  be the number of roots of unity in  $K$ . We have*

$$\lim_{s \rightarrow 1} (s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}h_K R_K}{\sqrt{|d_K|}w_K}.$$

**Remark 1.5.36** (Philosophical principle: analytic information versus arithmetic information). Analytic objects can encode arithmetic information! Theorem 1.5.35 is extremely remarkable, in that it relates something which is purely analytic (the residue of a holomorphic function) to something arithmetic (information about unique factorisation, roots of unity, etc.)

There is also another (surprising) point of view on Theorem 1.5.35:

**Remark 1.5.37** (Philosophical principle: local-global principles). One can also reformulate Theorem 1.5.35 as

$$\operatorname{Res}_{s=1} \prod_{\mathfrak{p}} (1 - N\mathfrak{p}^{-s})^{-1} = \frac{2^{r_1}(2\pi)^{r_2}h_K R_K}{\sqrt{|d_K|}w_K}.$$

This shows that we can get 'global' information on the arithmetic of  $K$  from the knowledge of (an infinite amount of) 'local' data, namely, the sizes of the residue fields of  $\mathcal{O}_K$ .

### Further special values

The functional equation (Theorem 1.3.33) and the analytic class number formula (Theorem 1.5.35) imply that  $\zeta_K(s)$  has a zero of order  $r = \operatorname{rk} \mathcal{O}_K^\times = r_1 + r_2 - 1$  at  $s = 0$ , and one has

$$\lim_{s \rightarrow 0} s^{-r} \zeta_K(s) = -\frac{h_K R_K}{w_K}.$$

Conjecturally, the values (or more precisely, the first non-zero terms in the local series development) of  $\zeta_K$  at all integers should have an arithmetic interpretation. Discussing this in detail would take us quite far afield, so we limit ourselves to recalling a striking formula due to Euler and its connection with the arithmetic of cyclotomic extensions.

**Theorem 1.5.38** (Euler). *Let  $n$  be a positive integer. We have*

$$\zeta(2n) = (-1)^{n+1} \frac{B_{2n}(2\pi)^{2n}}{2(2n)!},$$

where  $B_{2n}$  are the **Bernoulli numbers**, defined by the power series development

$$\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}.$$

Even though this result does not seem to have much arithmetic content (after all, the numbers  $B_k$  seem to have nothing to do with arithmetic!), Kummer, Herbrand and Ribet have found a remarkable interpretation for these numbers:

**Theorem 1.5.39** (Kummer; Herbrand [Her32], Ribet [Rib76]). *A prime  $p$  divides the class number of  $\mathbb{Q}(\zeta_p)$  if and only if  $p$  divides the numerator of some Bernoulli number  $B_n$  for some even  $n$  with  $0 < n < p - 1$ .*

The question of special values of  $L$ -functions is a *deep* rabbit hole! To get a sense of just *how deep*, the reader can have a look at Question 4.2 in [Lic73], and then start learning about  $K$ -theory, higher regulators, and a number of topics I know nothing about.

## 1.6 Chebotarev's density theorem

In this section we (re)state and prove Chebotarev's theorem.

**Theorem 1.6.1** (Chebotarev, quantitative form). *Let  $K/F$  be a Galois extension with group  $G$  and let  $C \subseteq G$  be a union of conjugacy classes. The set*

$$S = \{\mathfrak{p} \text{ prime of } \mathcal{O}_F \mid \left(\frac{K/F}{\mathfrak{p}}\right) \subseteq C\}$$

*admits (Dirichlet) density, given by  $\text{Dens}(S) = \frac{\#C}{\#G}$ .*

**Remark 1.6.2.** Note that  $\left(\frac{K/F}{\mathfrak{p}}\right)$  is a conjugacy class (see Definition 1.3.15). Since  $C$  is a union of conjugacy classes, one may equivalently rephrase the condition in the theorem as  $\left(\frac{K/F}{\mathfrak{p}}\right) \in C$ , where  $\left(\frac{K/F}{\mathfrak{p}}\right)$  now means *any element of the conjugacy class*.

**Remark 1.6.3.** Even though we will not use it much in this course, Chebotarev's theorem really is one of the fundamental tools in modern number theory, and its importance is hard to overstate<sup>13</sup>. To give some context, let me mention a few (and quite disparate) consequences of the theorem:

1. let  $F_1, F_2$  be two finite extensions of the number field  $K$ . Then  $F_1, F_2$  have the same Galois closure if and only if the primes of  $K$  that split completely in  $F_1, F_2$  are the same, or even the same up to a subset of density 0.
2.  $a \in \mathbb{Q}^\times$  is a  $p$ -th power if and only if it is a  $p$ -th power modulo  $\ell$  for almost all primes  $\ell$ . Even more: if  $f(x) \in \mathbb{Z}[x]$  is irreducible and has a root modulo almost every prime  $p$ , then  $\deg f = 1$ .
3. a sufficiently strong version of Chebotarev with error term (unfortunately, one *so strong* that we can only prove it under the assumption of the Generalised Riemann Hypothesis for Dedekind  $\zeta$  functions) implies Artin's conjecture on primitive roots:

---

<sup>13</sup>an analytic number theorist, who will remain anonymous, once asked me: *is Chebotarev the **only** result in analytic number theory that you algebraic people care about?*

**Conjecture 1.6.4** (Artin). *Let  $a$  be an integer which is not a square and is different from  $-1$ . There exist infinitely many primes  $p$  such that  $a$  is a primitive root modulo  $p$ .*

4. Let  $f(x) \in \mathbb{Z}[x]$  be an irreducible polynomial of degree at least 2. There exist infinitely many primes  $p$  such that  $f(x) \pmod p$  has no roots.
5. Conversely, let  $f(x) \in \mathbb{Z}[x]$  be any polynomial. There exist infinitely many primes  $p$  such that  $f(x) \pmod p$  splits completely (this can also be proven elementarily, without Chebotarev).
6. Let  $K$  be a number field. The ‘probability’ that a prime of  $\mathcal{O}_K$  is principal (that is, the density of principal primes) is  $1/h(K)$ . This partially justifies the oft-repeated claim that ‘ $h(K)$  measures the failure of unique factorisation’ – recall that unique factorisation is equivalent to the ring of integers being a PID, which in turn is equivalent to every prime ideal being principal, so  $h(K)$  really is a measure of ‘how much’ unique factorisation fails.
7. The density of primes  $p$  that divide at least one number of the form  $2^n + 1$  (for  $n \geq 0$  an integer) exists and is equal to  $\frac{17}{24}$ .
8. (Elementary reformulation of the theorem) Let  $f(x) \in \mathbb{Z}[x]$ , of degree  $n$ , have Galois group  $G$ . Fix a ‘cycle type’, that is, a conjugacy class of permutations in  $S_n$  (which we think as a tuple  $m_1, \dots, m_n$  with  $1m_1 + 2m_2 + \dots + nm_n = n$  – here  $m_i$  is the number of cycles of length  $i$ ). Let  $d$  be the number of elements of  $G$  with the given cycle type. Then, the set

$$S = \left\{ p \text{ prime} : \begin{array}{l} f(x) \pmod p \text{ factors with } m_1 \text{ factors of degree } 1, \\ m_2 \text{ factors of degree } 2 \dots, m_n \text{ factors of degree } n \end{array} \right\}$$

admits density, and this density is  $\frac{d}{\#G}$ .

9. Let  $a, b, c$  be integers with  $(a, b, c) = 1$  and  $d := b^2 - 4ac < 0$ . As  $x, y$  range over the integers, the positive-definite quadratic form  $ax^2 + bxy + cy^2$  represents infinitely many primes. In fact, the density of the set

$$\{p \text{ prime} : \exists x, y \in \mathbb{Z} \text{ such that } p = ax^2 + bxy + cy^2\}$$

is positive and can be expressed in terms of invariants of the number field  $\mathbb{Q}(\sqrt{-d})$ . (This is related to example 6 in this list, and if I’m not mistaken, the density in question should be  $\frac{1}{2h(\mathbb{Q}(\sqrt{-d}))}$ .)

10. Let  $f(x) \in \mathbb{Z}[x]$  be an irreducible polynomial. The average number of zeroes of  $f$  modulo primes is 1, that is to say,


$$\lim_{T \rightarrow \infty} \frac{\sum_{p \leq T} \#\{a \in \mathbb{F}_p : f(a) = 0 \pmod p\}}{\#\{p \text{ prime} : p \leq T\}} = 1.$$

**Exercise 1.6.5.** Prove as many of these as you can.

*Friendly suggestion.* You should avoid 3 (which is really hard), 7 (which is quite hard), and maybe 9. Everything else you should be able to prove; it is especially important to make sure you understand how 8 follows from Chebotarev.

Having convinced you of the importance of the theorem (hopefully), we now turn to its proof. We give both an algebraic proof and an analytic one, starting with the latter.

### 1.6.1 Analytic proof

 **Warning.** The proof below is inspired by a famous paper by Lagarias and Odlyzko [LO77]. However, the aim of that paper is to give effective estimates, which involves some rather heavy analytic number theory. I have tried to streamline the argument so as to arrive at the result *for the Dirichlet density* in the most efficient way possible (Lagarias and Odlyzko work with the natural density). It seems to me that the resulting proof is fairly straightforward, and very interesting in the way it directly generalises the proof of Theorem 1.5.31. However, I have not found this particular approach written down in the literature<sup>14</sup>, so there is a good chance that it could be wrong. Treat everything in this section with extreme suspicion!

We start with the following lemma:

**Lemma 1.6.6.** *Let  $L(s, \rho)$  be the Artin L-function of some representation  $\rho : \text{Gal}(L/K) \rightarrow \text{GL}(V)$ . We have the asymptotic relation*

$$\log L(s, \rho) = \sum_{\mathfrak{p} \text{ unramified in } L} \text{tr } \rho \left( \left( \frac{L/K}{\mathfrak{p}} \right) \right) N(\mathfrak{p})^{-s} + O(1) \text{ as } s \rightarrow 1^+.$$

*Proof.* Starting from Exercise 1.4.16, we can ignore the finitely many ramified primes (which give a bounded contribution), and bound

$$\left| \sum_{\mathfrak{p}} \sum_{m \geq 2} \frac{\chi(\mathfrak{p}^m)}{m(N\mathfrak{p})^{ms}} \right| \leq \sum_{\mathfrak{p}} \sum_{m \geq 2} \left| \frac{\chi(\mathfrak{p}^m)}{m(N\mathfrak{p})^{ms}} \right| \leq \sum_{\mathfrak{p}} \sum_{m \geq 2} \frac{\dim V}{(N\mathfrak{p})^{m\Re s}} \leq [K : \mathbb{Q}] \sum_{\mathfrak{p}} \sum_{m \geq 2} \frac{\dim V}{p^{m\Re s}} = O(1)$$

by Lemma 1.5.33. □

Next we recall (without proof) the orthogonality relations in the case of non-abelian groups:

**Proposition 1.6.7** (Orthogonality relations, non-abelian case). *Let  $\{\varphi_1, \dots, \varphi_r\}$  be the distinct irreducible characters<sup>15</sup> of a finite group  $G$ . The following hold.*

$$1. \sum_{g \in G} \varphi_i(g) \overline{\varphi_j(g)} = \begin{cases} |G|, & \text{if } i = j \\ 0, & \text{otherwise} \end{cases}$$

2. Fix  $g, h \in G$ . We have

$$\sum_{\chi} \chi(g) \overline{\chi(h)} = \begin{cases} |C_G(g)|, & \text{if } g, h \text{ are in the same conjugacy class} \\ 0, & \text{otherwise} \end{cases}$$

where the sum ranges over all the irreducible characters of  $G$ .

<sup>14</sup>apparently, it appears in unpublished notes of Serre: see <https://mathoverflow.net/questions/131543/effective-chebotarev-without-artins-conjecture>

<sup>15</sup>the **character** of a representation is simply its trace. A finite group has only finite many (finite-dimensional) irreducible representations: here we consider the character of each of those.



Now let  $C$  be a conjugacy class in  $G$ . Define the class function<sup>16</sup>

$$f_C = \frac{|G|}{|C|} \mathbf{1}_C. \quad (1.17)$$

Fix  $g \in C$ . The orthogonality relations (Proposition 1.6.7) easily imply that

$$f_C = \sum_{\varphi} \overline{\varphi(g)} \varphi, \quad (1.18)$$

where the sum is over all the characters of the finite-dimensional irreducible representations of  $G$ . Let furthermore  $H = \langle g \rangle$  and let  $\tau$  be the class function on  $H$  defined by

$$\tau = |H| \cdot \mathbf{1}_{\{g\}},$$

where  $\mathbf{1}_{\{g\}}$  is the characteristic function of the set  $\{g\}$ . By the usual abelian orthogonality relations (Corollary 1.5.13) we have

$$\tau = \sum_{\chi \in \hat{H}} \overline{\chi(g)} \chi.$$

A simple calculation (see Lemma 1.6.8 below) shows that

$$\text{Ind}_H^G(\tau) = |C_G(g)| \cdot \mathbf{1}_C = \frac{|G|}{|C|} \mathbf{1}_C = f_C, \quad (1.19)$$

and therefore

$$\sum_{\varphi} \overline{\varphi(g)} \varphi = f_C = \text{Ind}_H^G(\tau) = \sum_{\chi \in \hat{H}} \overline{\chi(g)} \text{Ind}_H^G(\chi). \quad (1.20)$$

**Lemma 1.6.8.** *Equation (1.19) holds.*

*Proof.* Representation theory tells us that, if  $\tau : H \rightarrow \mathbb{C}$  is a class function, then

$$\text{Ind}_H^G(\tau)(x) = \sum_{s \in S} \tau_0(s^{-1}xs),$$

where

$$\tau_0(g) = \begin{cases} \tau(g), & \text{if } g \in H \\ 0, & \text{otherwise} \end{cases}$$

and  $S$  is a set of representatives for the left cosets  $\{sH\}$ . For our specific function  $\tau$ , we then have

$$\text{Ind}_H^G(\tau)(x) = |H| \cdot \#\{s \in S : s^{-1}xs = g\} = |H| \cdot |\{s \in S : x = sgs^{-1}\}|.$$

We claim that this quantity is 0 if  $g, x$  are in different conjugacy classes in  $G$ , and is  $|C_G(g)|$  otherwise. To see this, simply observe that every element of  $H = \langle g \rangle$  commutes with  $g$ , so (since  $G = SH$ ) we obtain

$$|H| \cdot \#\{s \in S : x = sgs^{-1}\} = |\{(s, h) \in S \times H : x = shgh^{-1}s^{-1}\}| = |\{y \in G : x = ygy^{-1}\}|.$$

The statement is now clear: if  $x, g$  belong to different conjugacy classes no such  $y$  exists, while if  $x, g$  are in the same conjugacy class, the set above is a coset for  $C_G(g)$ .  $\square$

<sup>16</sup>a **class function** is a function  $f : G \rightarrow \mathbb{C}$  such that  $f(hgh^{-1}) = f(g)$  for all  $g, h \in G$ .

We are now ready to prove Theorem 1.6.1.

*Proof of Theorem 1.6.1.* We can assume that  $C$  itself is a conjugacy class. We wish to estimate

$$\sum_{\mathfrak{p} \subset \mathcal{O}_K} \mathbf{1}_C \left( \left( \frac{L/K}{\mathfrak{p}} \right) \right) (N\mathfrak{p})^{-s}$$

as  $s \rightarrow 1$ . For simplicity, if  $\varphi$  is a character of  $G = \text{Gal}(L/K)$  and  $\mathfrak{p}$  is a prime of  $K$  unramified in  $L$ , we denote by  $\varphi(\mathfrak{p})$  the value of  $\varphi$  at  $\left( \frac{L/K}{\mathfrak{p}} \right)$ .

Using (1.17) and (1.18), we write the above as

$$\sum_{\mathfrak{p} \subset \mathcal{O}_K} \mathbf{1}_C \left( \left( \frac{L/K}{\mathfrak{p}} \right) \right) (N\mathfrak{p})^{-s} = \frac{|C|}{|G|} \sum_{\mathfrak{p} \subset \mathcal{O}_K} \sum_{\varphi} \overline{\varphi(g)} \varphi(\mathfrak{p}) (N\mathfrak{p})^{-s},$$

where as before  $\varphi$  ranges over the irreducible characters of  $G$ . We now use (1.20) to arrive at

$$\begin{aligned} \sum_{\mathfrak{p} \subset \mathcal{O}_K} \mathbf{1}_C \left( \left( \frac{L/K}{\mathfrak{p}} \right) \right) (N\mathfrak{p})^{-s} &= \frac{|C|}{|G|} \sum_{\mathfrak{p} \subset \mathcal{O}_K} \sum_{\chi \in \hat{H}} \overline{\chi(g)} \text{Ind}_H^G(\chi)(\mathfrak{p}) (N\mathfrak{p})^{-s} \\ &= \sum_{\chi \in \hat{H}} \overline{\chi(g)} \frac{|C|}{|G|} \sum_{\mathfrak{p} \subset \mathcal{O}_K} \text{Ind}_H^G(\chi)(\mathfrak{p}) (N\mathfrak{p})^{-s}. \end{aligned}$$

Lemma 1.6.6 allows us to recognise the last sum as the series development of  $L(s, \text{Ind}_H^G(\chi))$  around  $s = 1$ , up to a bounded error term:

$$\sum_{\mathfrak{p} \subset \mathcal{O}_K} \mathbf{1}_C \left( \left( \frac{L/K}{\mathfrak{p}} \right) \right) (N\mathfrak{p})^{-s} = \sum_{\chi \in \hat{H}} \overline{\chi(g)} \frac{|C|}{|G|} \log L(s, \text{Ind}_H^G(\chi)) + O(1).$$

Using the formalism of Artin  $L$ -functions (in particular, Theorem 1.4.12(3)) we arrive at

$$\sum_{\mathfrak{p} \subset \mathcal{O}_K} \mathbf{1}_C \left( \left( \frac{L/K}{\mathfrak{p}} \right) \right) (N\mathfrak{p})^{-s} = \sum_{\chi \in \hat{H}} \overline{\chi(g)} \frac{|C|}{|G|} \log L(s, \chi) + O(1) \text{ as } s \rightarrow 1, \quad (1.21)$$

where now all the involved Artin  $L$ -functions are Hecke  $L$ -functions!

Letting  $E = L^H$  be the subfield fixed by  $H = \langle g \rangle$ , Theorem 1.4.21 shows that

$$\zeta_L(S) = \zeta_E(s) \prod_{\chi \neq 1, \chi \in \hat{H}} L(s, \chi).$$

(Recall that  $H$  is a cyclic group, so all its irreducible complex representations are 1-dimensional.) Arguing as in Theorem 1.5.32 (and using Theorem 1.4.11 to ensure analyticity of  $L(s, \chi)$  around  $s = 1$  for  $\chi$  a non-principal character), we obtain that  $L(s, \chi)$  is non-vanishing at  $s = 1$  when  $\chi$  is a non-principal character. Thus,  $\log L(s, \chi)$  is bounded as  $s \rightarrow 1$  for  $\chi \neq 1$ . Using this information in Equation (1.21) we finally obtain

$$\sum_{\mathfrak{p} \subset \mathcal{O}_K} \mathbf{1}_C \left( \left( \frac{L/K}{\mathfrak{p}} \right) \right) (N\mathfrak{p})^{-s} = \sum_{\chi=1} \overline{\chi(g)} \frac{|C|}{|G|} \log L(s, \chi) + O(1) = \frac{|C|}{|G|} \log L(s, 1_H) + O(1) \text{ as } s \rightarrow 1.$$

Notice that in this last formula  $1_H$  is the trivial representation of the Galois group  $H$  of  $L$  over  $E$ , so  $L(s, 1_H)$  is the  $\zeta$ -function of  $E$ . Using Theorem 1.1.18 both for  $E$  and for  $K$ , we obtain that (as  $s \rightarrow 1$ ) we have the asymptotic

$$\log L(s, 1_H) = \log \zeta_E(s) \sim \log \left( \frac{1}{s-1} \right) \sim \log \zeta_K(s).$$

Interpreting  $\zeta_K(s)$  as  $L(s, 1_G)$  for the trivial representation of  $G = \text{Gal}(L/K)$ , Lemma 1.6.6 yields  $\log \zeta_K(s) \sim \sum_{\mathfrak{p} \subset \mathcal{O}_K} (N\mathfrak{p})^{-s}$ , again for  $s \rightarrow 1$ . Combining these relations, we have  $\sum_{\mathfrak{p} \subset \mathcal{O}_K} (N\mathfrak{p})^{-s} \sim L(s, 1_H)$ , and we are done:

$$\lim_{s \rightarrow 1^+} \frac{\sum_{\mathfrak{p} \subset \mathcal{O}_K} \mathbf{1}_C \left( \left( \frac{L/K}{\mathfrak{p}} \right) \right) (N\mathfrak{p})^{-s}}{\sum_{\mathfrak{p} \subset \mathcal{O}_K} (N\mathfrak{p})^{-s}} = \lim_{s \rightarrow 1^+} \frac{\frac{|C|}{|G|} \log L(s, 1_H) + O(1)}{\log L(s, 1_H)} = \frac{|C|}{|G|}.$$

□

### 1.6.2 Algebraic (well, mostly algebraic) proof

We now give a second, (superficially) different proof of Chebotarev's theorem, based on Schoof's version given in [Sch08, Chapter 15].

The first step is to establish an analogue of Dirichlet's theorem for arbitrary number fields. Recall that we have already remarked that Dirichlet's theorem is precisely Chebotarev's theorem for the extensions  $\mathbb{Q}(\zeta_m)/\mathbb{Q}$  (see the proof we gave for Theorem 1.3.19). Our first proposition is then a direct generalisation of Dirichlet's theorem to arbitrary number fields.

**Proposition 1.6.9.** *Let  $F$  be a number field and let  $m \geq 1$  be an integer. Write  $H$  for the group  $\text{Gal}(F(\zeta_m)/F)$ . For every  $h \in H$ , the set*

$$S_h := \left\{ \mathfrak{p} \text{ prime of } \mathcal{O}_F \mid \left( \frac{F(\zeta_m)/F}{\mathfrak{p}} \right) = h \right\}$$

*admits Dirichlet density  $1/|H|$ .*

**Remark 1.6.10.** Since  $H$  is abelian,  $\left( \frac{F(\zeta_m)/F}{\mathfrak{p}} \right)$  is well-defined as an element of  $H$  (it is a conjugacy class consisting of a single element).

*Proof.* This closely parallels the proof of Theorem 1.5.31. By restriction,  $H$  can be identified with a subgroup  $\tilde{H}$  of  $\text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$ . For every character  $\chi : \tilde{H} \rightarrow \mathbb{C}^\times$  (that we interpret as a character on a subset of  $(\mathbb{Z}/m\mathbb{Z})^\times$ ) we introduce the series

$$L(s, \chi) = \prod_{\mathfrak{p} \subset \mathcal{O}_F} \left( 1 - \frac{\chi(N(\mathfrak{p}))}{N(\mathfrak{p})^s} \right)^{-1},$$

with the usual convention that  $\chi(n) = 0$  if  $(n, m) > 1$ . This is not a Dirichlet  $L$ -function, but it is a Hecke  $L$ -function, corresponding to the abelian extension  $F(\zeta_m)/F$  and the representation

$$\text{Gal}(F(\zeta_m)/F) \xrightarrow{\sim} \tilde{H} \xrightarrow{\chi} \mathbb{C}^\times.$$

This is proved exactly as in Proposition 1.4.6(2). We show equality of the local factors at the unramified primes (which is enough for our purposes).

Given a prime  $\mathfrak{p}$  of  $F$  unramified in  $F(\zeta_m)$  and a prime  $\mathfrak{P}$  of  $F(\zeta_m)$  lying over it, we show that the Artin symbol  $\left(\frac{F(\zeta_m)/F}{\mathfrak{P}}\right)$  maps to  $N(\mathfrak{p})$  under the isomorphism  $H \rightarrow \tilde{H} \subseteq \text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$ . To see this, notice that  $\sigma := \left(\frac{F(\zeta_m)/F}{\mathfrak{P}}\right)$  is determined by its restriction to  $\mathbb{Q}(\zeta_m)$ , and that it satisfies

$$\sigma(\zeta_m) \equiv \zeta_m^{N(\mathfrak{p})} \pmod{\mathfrak{P} \cap \mathbb{Z}[\zeta_m]}.$$

By uniqueness of Frobenius elements (in the unramified case), since the automorphism  $\zeta_m \mapsto \zeta_m^{N(\mathfrak{p})}$  satisfies the condition above, we see that  $\left(\frac{F(\zeta_m)/F}{\mathfrak{P}}\right)$  does indeed map to  $\zeta_m \mapsto \zeta_m^{N(\mathfrak{p})}$ , which (under the canonical isomorphism  $\text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$ ) corresponds to  $N(\mathfrak{p})$ , as claimed. Thus, for every non-trivial character  $\chi$ , the function  $L(s, \chi)$  agrees (possibly up to finitely many factors of the form  $(1 - \zeta_m^k/N(\mathfrak{p})^s)$ , which are holomorphic and nonvanishing near  $s = 1$ ) with a Hecke  $L$ -function. Hence, by Theorem 1.4.11, it extends to a holomorphic function near  $s = 1$ . On the other hand,  $L(s, 1)$  is the  $\zeta$  function of  $F$ .

As in Corollary 1.4.22 one then shows  $\zeta_{F(\zeta_m)}(s) = g(s) \prod_{\chi} L(s, \chi)$ , where the product runs over the characters  $\chi$  of  $H$  and  $g(s)$  is holomorphic and nonvanishing around  $s = 1$  (in fact,  $g(s)$  is the constant 1, but we won't need this). We then deduce that  $L(1, \chi) \neq 0$  for every nontrivial character, and the rest of the proof of Theorem 1.5.31 goes through.  $\square$

Next we prove the key case of Chebotarev, namely, that of cyclic extensions. We remark that the argument we give applies without change to any *abelian* extension (but of course this is still not enough, since the full Chebotarev theorem applies to arbitrary, possibly non-abelian, Galois extensions).

**Proposition 1.6.11.** *Let  $F$  be a number field and let  $K/F$  be a cyclic extension with group  $G$ . For every  $\sigma \in G$ , the set*

$$S_{\sigma} := \left\{ \mathfrak{p} \text{ prime of } \mathcal{O}_F \mid \left(\frac{K/F}{\mathfrak{p}}\right) = \sigma \right\}$$

*has density equal to  $\frac{1}{\#G}$ .*

Since the proof is long, we divide it into several lemmas and propositions. In what follows, we will tacitly exclude from any set of primes those that ramify in the relevant extensions: since we are going to argue about densities, and the number of ramified primes is always finite, this does not affect any of our arguments.

We begin with the following general setup. Let  $n = [K : F] = |G|$  and put  $N = n^k$ , where  $k$  is any positive integer (we will eventually take the limit  $k \rightarrow \infty$ ). By Dirichlet's theorem (Theorem 1.5.31), there exist infinitely many primes  $q \equiv 1 \pmod{N}$ . In particular, there exists such a prime  $q$  that is unramified in  $K/\mathbb{Q}$ . We will work with this auxiliary prime  $q$  and consider the extension  $K(\zeta_q)$  (which will be easier to treat, since it is a cyclotomic extension: see Proposition 1.6.9).

**Lemma 1.6.12.** *We have  $K \cap \mathbb{Q}(\zeta_q) = F \cap \mathbb{Q}(\zeta_q) = \mathbb{Q}$ , hence the restriction homomorphisms*

$$\text{res}_K : \text{Gal}(K(\zeta_q)/K) \rightarrow \text{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$$

$$\text{res}_F : \text{Gal}(F(\zeta_q)/F) \rightarrow \text{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$$

are isomorphisms.

*Proof.* No prime ramifies both in  $K$  and in  $\mathbb{Q}(\zeta_q)$ , so  $K \cap \mathbb{Q}(\zeta_q)$  is everywhere unramified. By Minkowski's theorem (Theorem 1.3.8), this implies  $K \cap \mathbb{Q}(\zeta_q) = \mathbb{Q}$ . As a consequence, also  $F \cap \mathbb{Q}(\zeta_q) \subseteq K \cap \mathbb{Q}(\zeta_q)$  coincides with  $\mathbb{Q}$ . The last statement follows from basic Galois theory.  $\square$

Let  $H = \text{Gal}(F(\zeta_q)/F)$  and consider the following diagram of field extensions:

$$\begin{array}{ccccc}
 & & K(\zeta_q) & & \\
 & \swarrow & | & \searrow & \\
 K & & & & F(\zeta_q) \\
 & \swarrow & | & \searrow & \\
 & G & K \cap F(\zeta_q) & H & \\
 & \swarrow & | & \searrow & \\
 & & F & & 
 \end{array} \tag{1.22}$$

The restriction homomorphism

$$\text{Gal}(K(\zeta_q)/K) \rightarrow \text{Gal}(F(\zeta_q)/(K \cap F(\zeta_q)))$$

is injective (Galois theory), so

$$\begin{aligned}
 [F(\zeta_q) : K \cap F(\zeta_q)] &\geq [K(\zeta_q) : K] = \# \text{Gal}(K(\zeta_q)/K) \\
 &= \# \text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = \# \text{Gal}(F(\zeta_q)/F) \\
 &= [F(\zeta_q) : F],
 \end{aligned}$$

which implies  $K \cap F(\zeta_q) = F$ . (An alternative proof of the same equality can be obtained as follows: any prime of  $F$  of characteristic  $q$  is unramified in  $K \cap F(\zeta_q)$ , because this is a sub-extension of  $K$ . On the other hand, it is totally ramified in  $K \cap F(\zeta_q)$ , because this is a sub-extension of  $F(\zeta_q)$ . The intersection must therefore be  $F$ , since it is both unramified and totally ramified at the same prime.) We deduce that

$$\text{Gal}(K(\zeta_q)/F) \cong \text{Gal}(K/F) \times \text{Gal}(F(\zeta_q)/F) = G \times H. \tag{1.23}$$

Notice that this implies in particular  $[K(\zeta_q) : F(\zeta_q)] = |G|$ , and in fact, more precisely,  $\text{Gal}(K(\zeta_q)/F(\zeta_q))$  is identified with  $G \times \{\text{id}\}$  under the isomorphism (1.23).

**Remark 1.6.13.** Before giving a formal proof of Proposition 1.6.11, we try to describe the basic idea. The point is that the set  $S_\sigma$  of primes of  $F$  with Frobenius  $\sigma$  in the extension  $K/F$  is the union of the sets  $S_{\sigma,\tau}$ , where for each  $\tau \in H$  we write

$$S_{\sigma,\tau} := \{P \text{ prime of } \mathcal{O}_F \mid \left( \frac{K(\zeta_q)/F}{P} \right) = (\sigma, \tau) \in G \times H\}. \tag{1.24}$$

The trick is that for most<sup>17</sup> (but not all!)  $\tau \in H$  one can compute the density of  $S_{\sigma,\tau}$  using Proposition 1.6.9. Hence, by summing over these ‘good’  $\tau$ , we can at least estimate the density of  $S_\sigma = \cup_\tau S_{\sigma,\tau}$ . By choosing  $H$  appropriately (that is, by choosing  $q$ ), the fraction of the elements of  $H$  for which we can compute the density of  $S_{\sigma,\tau}$  tends to 1, and this will lead to the desired estimate for the density of  $S_\sigma$ .

**Proposition 1.6.14.** *Let  $\tau \in H$  have order multiple of  $n$ . Then*

$$d_F^-(S_{\sigma,\tau}) = \frac{1}{[K(\zeta_q) : F]}.$$

*Proof.* Let  $J$  be the cyclic subgroup of  $G \times H$  generated by  $(\sigma, \tau)$  and let  $L$  be the subfield of  $K(\zeta_q)$  fixed by  $J$ . Let furthermore

$$T = \{P \text{ prime of } L \mid \left(\frac{K(\zeta_q)/L}{P}\right) = (\sigma, \tau)\}$$

We first prove that

$$d_L(T) = \frac{1}{[K(\zeta_q) : L]}. \quad (1.25)$$

By Proposition 1.6.9, it suffices to check that  $K(\zeta_q)/L$  is a cyclotomic extension. We now show this.

Notice that  $J \cap (G \times \{\text{id}\}) = \{(\text{id}, \text{id})\}$ : one has  $(\sigma, \tau)^h = (\rho, \text{id})$  for some  $\rho \in G$  if and only if  $\text{ord}(\tau) \mid h$ , but then  $\rho = \sigma^h = \text{id}$  since  $n \mid \text{ord}(\tau) \mid h$ . Galois theory then gives

$$K(\zeta_q) = K(\zeta_q)^{J \cap (G \times \{\text{id}\})} = K(\zeta_q)^J K(\zeta_q)^{G \times \{\text{id}\}} = LF(\zeta_q) = L(\zeta_q),$$

that is,  $K(\zeta_q)$  is generated over  $L$  by a root of unity, as desired.

Finally, let

$$T' = \{P \text{ prime of } L \mid f(P \mid P \cap F) = 1 \text{ and } \left(\frac{K(\zeta_q)/L}{P}\right) = (\sigma, \tau)\}.$$

By Exercise 1.5.29 we have  $d_L(T) = d_L(T') = d_L^-(T')$ . To finish the proof, we show that

$$d_L^-(T') = [L : F] d_F^-(S_{\sigma,\tau}). \quad (1.26)$$

It suffices to prove:

1. for every prime  $P$  in  $T'$ , the prime  $P \cap \mathcal{O}_F$  of  $F$  is in  $S_{\sigma,\tau}$ ;
2. for every prime  $\mathfrak{p}$  in  $S_{\sigma,\tau}$  there are precisely  $[L : F]$  primes  $P_1, \dots, P_{[L:F]}$  in  $L$  lying over  $\mathfrak{p}$ , and each of those is in  $T'$  (in particular,  $N(P_i) = N(\mathfrak{p})$ , since by definitions the primes in  $T'$  satisfy  $f(P_i \mid \mathfrak{p}) = 1$ ).

<sup>17</sup>specifically, for those  $\tau$  of order multiple of  $n$ : see Proposition 1.6.14.

Indeed, if we have these two properties, we can compute the lower density of  $S_{\sigma,\tau}$  in  $F$  as

$$\begin{aligned}
 \text{Dens}_F^-(S_{\sigma,\tau}) &= \liminf_{s \rightarrow 1^+} \frac{\sum_{\mathfrak{p} \in S_{\sigma,\tau}} N(\mathfrak{p})}{\sum_{\mathfrak{p} \text{ nonzero prime of } \mathcal{O}_F} N(\mathfrak{p})^{-s}} \\
 &= \frac{1}{[L:F]} \liminf_{s \rightarrow 1^+} \frac{\sum_{\mathfrak{p} \in S_{\sigma,\tau}} \sum_{P|\mathfrak{p}, P \in T'} N(P)}{\log\left(\frac{1}{s-1}\right)} \\
 &= \frac{1}{[L:F]} \liminf_{s \rightarrow 1^+} \frac{\sum_{\mathfrak{p} \in S_{\sigma,\tau}} \sum_{P|\mathfrak{p}, P \in T'} N(P)}{\log\left(\frac{1}{s-1}\right)} \\
 &= \frac{1}{[L:F]} \liminf_{s \rightarrow 1^+} \frac{\sum_{P \in T'} N(P)}{\log\left(\frac{1}{s-1}\right)} \\
 &= \frac{1}{[L:F]} \text{Dens}_L^-(T'),
 \end{aligned}$$

as desired. Note that in the next-to-last equality we have used the fact that every prime of  $T'$  lies over a prime in  $S_{\sigma,\tau}$ , that is, (1). We now establish properties (1) and (2) above.

1. Let  $P$  be a prime in  $T'$ . Since the norm of  $P \cap \mathcal{O}_F$  is equal to the norm of  $P$ , the Artin symbols  $\left(\frac{K(\zeta)/L}{P}\right) = (\sigma, \tau)$  and  $\left(\frac{K(\zeta)/F}{P \cap \mathcal{O}_F}\right)$  coincide. Hence,  $P \cap \mathcal{O}_F$  is in  $S_{\sigma,\tau}$ .
2. Conversely, let  $\mathfrak{p}$  be in  $S_{\sigma,\tau}$ . Recall that  $\mathfrak{p}$  is unramified in  $K(\zeta)$  (by convention: we exclude the ramified primes) and let  $\mathfrak{Q}$  be a prime of  $K(\zeta)$  lying over  $\mathfrak{p}$ . The decomposition group  $D(\mathfrak{Q} | \mathfrak{p})$  is by definition generated by  $\left(\frac{K(\zeta)/F}{\mathfrak{p}}\right) = (\sigma, \tau)$ . Hence,  $K(\zeta)^{\langle(\sigma,\tau)\rangle} = L$  is by definition the decomposition field of  $\mathfrak{p}$  (that is,  $\mathfrak{p}$  is totally split in  $L$ ), so that there are  $r = [L:F]$  primes  $P_1, \dots, P_r$  of  $L$  lying over  $\mathfrak{p}$ . Each of these has degree 1 over  $\mathfrak{p}$ , and, as in (1), their Frobenius elements are given by  $(\sigma, \tau)$ .

Finally, combining Equations (1.25) and (1.26) we obtain

$$d_F^-(S_{\sigma,\tau}) = \frac{1}{[L:F]} d_L^-(T) = \frac{1}{[L:F]} \frac{1}{[K(\zeta):L]} = \frac{1}{[K(\zeta):F]},$$

as claimed. □

We are now ready to prove Proposition 1.6.11.

*Proof.* With  $S_{\sigma,\tau}$  as in Equation (1.24) we have

$$S_\sigma = \bigsqcup_{\tau \in H} S_{\sigma,\tau}.$$

(Recall that we are excluding from all our sets the finitely many primes that ramify in  $K(\zeta_q)$ .) In particular,

$$d_F^-(S_\sigma) \geq \sum_{\tau \in H} d_F^-(S_{\sigma,\tau})$$

by Exercise 1.6.16 and the fact that the sets  $S_{\sigma,\tau}$  are clearly pairwise disjoint. We can further estimate the lower density of  $S_\sigma$  as

$$d_F^-(S_\sigma) \geq \sum_{\substack{\tau \in H \\ n | \text{ord}(\tau)}} d_F^-(S_{\sigma,\tau}).$$

Using Proposition 1.6.14 we obtain

$$d_F^-(S_\sigma) \geq \sum_{\substack{\tau \in H \\ n | \text{ord } \tau}} \frac{1}{[K(\zeta_q) : F]} = \frac{\#\{\tau \in H : n \mid \text{ord } \tau\}}{[K(\zeta_q) : F]},$$

hence, by Exercise 1.6.15,

$$d_F^-(S_\sigma) \geq \frac{\#H}{[K(\zeta_q) : F]} \prod_{p_i | n} \left(1 - \frac{1}{p_i^{\alpha_i + 1 - \beta_i}}\right),$$

where  $\alpha_i = v_p(\#H) = v_p(q - 1)$  and  $\beta_i = v_p(n)$ . Since  $n^k m \mid q - 1$ , for every prime  $p$  that divides  $n$  we have  $\alpha_i \geq kv_p(n)$ , so  $\alpha_i - \beta_i + 1 \geq (k - 1)v_p(n) + 1 \geq k$ . Thus, we have shown

$$d_F^-(S_\sigma) \geq \frac{\#H}{[K(\zeta_q) : F]} \cdot \prod_{p | n} \left(1 - \frac{1}{p^k}\right) = \frac{\varphi(q)}{[K : F]\varphi(q)} \cdot \prod_{p | n} \left(1 - \frac{1}{p^k}\right) = \frac{1}{[K : F]} \cdot \prod_{p | n} \left(1 - \frac{1}{p^k}\right)$$

for every  $k \geq 1$ . By passing to the limit  $k \rightarrow \infty$ , we get  $d_F^-(S_\sigma) \geq \frac{1}{[K : F]}$ . Finally, in order to gain information about the *upper* density, it suffices to notice that the set of all primes of  $F$  (with finitely many exceptions, namely the primes that ramify in  $K$ ) is the disjoint union of the sets  $S_{\sigma'}$  for  $\sigma' \in G$ . This immediately implies

$$d_F^+(S_\sigma) \leq 1 - \sum_{\sigma' \neq \sigma} d_F^-(S_{\sigma'}) \leq 1 - \frac{[K : F] - 1}{[K : F]} = \frac{1}{[K : F]},$$

which concludes the proof.  $\square$

Finally, we prove Chebotarev's theorem:

*Proof of Theorem 1.6.1.* We may and do assume that  $C$  itself is a conjugacy class. We can also replace  $S$  by its subset  $S'$  of places for which  $N(\mathfrak{p})$  is a prime number (by Exercise 1.5.29, this does not alter its density).

Choose an element  $g \in C$  and let  $E = K^{\langle g \rangle}$  be the field fixed by the subgroup  $H = \langle g \rangle$ . Consider the set

$$T_g = \{\mathfrak{q} \text{ prime of } E \mid \left(\frac{K/E}{\mathfrak{q}}\right) = g, N(\mathfrak{q}) \text{ is prime}\}.$$

Suppose that  $\mathfrak{q}$  is in  $T_g$ : we claim that  $\mathfrak{p} := \mathfrak{q} \cap \mathcal{O}_F$  is in  $S'$ . Indeed,  $N(\mathfrak{p})$  divides  $N(\mathfrak{q})$ , so  $N(\mathfrak{p}) = N(\mathfrak{q})$  is a prime number. If  $\mathfrak{Q}$  is a prime of  $K$  lying over  $\mathfrak{q}$ , this implies that  $\left(\frac{K/F}{\mathfrak{Q}}\right) = \left(\frac{K/E}{\mathfrak{Q}}\right) = g \in C$ , hence  $\mathfrak{p} \in S'$ . Moreover, we claim that  $\mathfrak{Q}$  is the *unique* prime of  $K$  lying over  $\mathfrak{q}$ . To see this, notice that  $D(\mathfrak{Q} \mid \mathfrak{q})$  is by definition generated by  $\left(\frac{K/E}{\mathfrak{Q}}\right) = g$ , so  $D(\mathfrak{Q} \mid \mathfrak{q}) = H$ : the whole Galois group of  $K$  over  $E$  sends  $\mathfrak{Q}$  to itself, and therefore  $\mathfrak{Q}$  is the only prime of  $K$  over  $\mathfrak{q}$ .

Conversely, given  $\mathfrak{p} \in S'$ , by definition there exists a prime  $\mathfrak{Q}$  of  $K$  lying over  $\mathfrak{p}$  with  $\left(\frac{K/F}{\mathfrak{Q}}\right) \in C$ . Replacing  $\mathfrak{Q}$  by a conjugate if necessary, we can assume that  $\left(\frac{K/F}{\mathfrak{Q}}\right) = g$ . If we define  $\mathfrak{q} = \mathfrak{Q} \cap E$ , then  $\mathfrak{q}$  lies over  $\mathfrak{p}$  (obvious), and we claim that it is in  $T_g$ . To see this, notice that again we have

$$E = K^H = K^{\langle g \rangle} = K^{D(\mathfrak{Q} \mid \mathfrak{p})},$$



so  $E$  is the decomposition field of  $\mathfrak{p}$ . This means that  $f(\mathfrak{q} | \mathfrak{p}) = 1$  and  $f(\mathfrak{Q} | \mathfrak{q}) = |H| = \text{ord}(g)$ . In particular,  $N(\mathfrak{q}) = N(\mathfrak{p})^{f(\mathfrak{q}|\mathfrak{p})}$  is prime, and as above it follows that  $\left(\frac{K/F}{\mathfrak{Q}}\right) = \left(\frac{K/E}{\mathfrak{Q}}\right) = g \in C$ . Hence  $\mathfrak{q}$  is in  $T_g$  as claimed.

Summarising, there is a bijection between the primes in  $T_g$  lying over  $\mathfrak{p} \in S'$  and the primes  $\mathfrak{Q}$  of  $K$  that divide  $\mathfrak{p}$  and satisfy  $\left(\frac{K/F}{\mathfrak{Q}}\right) = g$ .

Now let  $C_G(g)$  be the centraliser of  $g$  in  $G$ . By the orbit-stabiliser lemma,  $|C| = \frac{|G|}{|C_G(g)|}$ . We count the primes in  $T_g$  lying over each prime  $\mathfrak{p} \in S'$ . By the previous paragraph, it suffices to count the primes  $\mathfrak{Q}$  of  $K$  lying over  $\mathfrak{p}$  with  $\left(\frac{K/F}{\mathfrak{Q}}\right) = g$ . We have already shown that there is at least one such prime, call it  $\mathfrak{Q}_1$ . Any other prime  $\mathfrak{Q}'$  of  $K$  lying over  $\mathfrak{p}$  is conjugate to  $\mathfrak{Q}_1$  by an element  $\sigma \in G$ , say  $\mathfrak{Q}' = \sigma\mathfrak{Q}_1$ . Then, the Artin symbol  $\left(\frac{K/F}{\mathfrak{Q}'}\right)$  is given by

$$\left(\frac{K/F}{\mathfrak{Q}'}\right) = \sigma \left(\frac{K/F}{\mathfrak{Q}_1}\right) \sigma^{-1} = \sigma g \sigma^{-1}.$$

Hence,  $\left(\frac{K/F}{\mathfrak{Q}'}\right) = g$  if and only if  $\sigma \in C_G(g)$ . By the orbit-stabiliser lemma again, the number of *distinct* primes  $\mathfrak{Q}'$  with  $\left(\frac{K/F}{\mathfrak{Q}'}\right) = g$  is

$$\frac{|C_G(g)|}{|\text{Stab}(\mathfrak{Q}_1) \cap C_G(g)|} = \frac{|C_G(g)|}{|D(\mathfrak{Q}_1 | \mathfrak{p}) \cap C_G(g)|} = \frac{|C_G(g)|}{|D(\mathfrak{Q}_1 | \mathfrak{p})|},$$

where we have used both the definition of  $D(\mathfrak{Q}_1 | \mathfrak{p})$  and the fact that  $D(\mathfrak{Q}_1 | \mathfrak{p}) = \langle g \rangle \subseteq C_G(g)$ . In conclusion, the number of primes of  $K$  lying over  $\mathfrak{p}$  and having Artin symbol  $g$  is  $\frac{|C_G(g)|}{|D(\mathfrak{Q}_1 | \mathfrak{p})|} = \frac{|G|}{|C| \cdot f}$ , where  $f = |D(\mathfrak{Q}_1 | \mathfrak{p})| = \text{ord}(g) = |H|$ . By what we already argued above, this is also the number of primes in  $T_g$  lying over  $\mathfrak{p}$ .

On the other hand, by Proposition 1.6.11, Chebotarev's theorem holds for the extension  $E \subset K$ , hence we have

$$\text{Dens}_E(T_g) = \frac{1}{|H|} = \frac{1}{f}. \quad (1.27)$$

Recall that we replaced  $S$  by its subset  $S'$  of primes whose residue field is a prime field. From the above discussion, noticing that by definition the norm of a prime  $\mathfrak{p} \in S'$  is the same as the norm of any prime  $\mathfrak{q} \in T_g$  lying over  $\mathfrak{p}$ , we obtain

$$\frac{|G|}{f|C|} \sum_{\mathfrak{p} \in S'} N(\mathfrak{p})^{-s} = \sum_{\mathfrak{q} \in T_g} N(\mathfrak{q})^{-s}.$$

Dividing by  $\log\left(\frac{1}{s-1}\right)$  and passing to the limit for  $s \rightarrow 1^+$ , we obtain

$$\frac{|G|}{f|C|} \lim_{s \rightarrow 1^+} \frac{\sum_{\mathfrak{p} \in S'} N(\mathfrak{p})^{-s}}{\log\left(\frac{1}{s-1}\right)} = \lim_{s \rightarrow 1^+} \frac{\sum_{\mathfrak{q} \in T_g} N(\mathfrak{q})^{-s}}{\log\left(\frac{1}{s-1}\right)} = \text{Dens}_E(T_g) = \frac{1}{f}.$$

This shows as desired that  $\text{Dens}_F(S')$  exists and equals  $\frac{|C|}{|G|}$ . □

### 1.6.3 Exercises

**Exercise 1.6.15.** Let  $G$  be a cyclic group of order  $n = \prod p_i^{\alpha_i}$  and let  $m = \prod p_i^{\beta_i}$  be a divisor of  $n$  (so that  $0 \leq \beta_i \leq \alpha_i$  for every  $i$ ). Prove that

$$\#\{g \in G : \text{ord}(g) \equiv 0 \pmod{m}\} = n \prod_{p_i|m} \left(1 - \frac{1}{p_i^{\alpha_i+1-\beta_i}}\right).$$

**Exercise 1.6.16.** Let  $S_1, S_2$  be disjoint sets of primes in a number field  $F$ . Prove that  $d_F^-(S_1 \cup S_2) \geq d_F^-(S_1) + d_F^-(S_2)$ .

## Chapter 2

### Prerequisites for Tate's thesis

## 2.1 The Haar measure

In this section we review the theory of the Haar measure, the (essentially) canonical choice of measure on a locally compact topological group. We review all the necessary definitions and show the existence of this special measure. We also prove uniqueness (up to constants) in the abelian case.

### 2.1.1 Preliminaries

**Definition 2.1.1.** Let  $X$  be a Hausdorff topological space. The Borel  $\sigma$ -algebra on  $X$ , denoted  $\mathcal{B}(X)$ , is the  $\sigma$ -algebra generated by the open subsets of  $X$ . The elements of  $\mathcal{B}(X)$  are called **Borel subsets** of  $X$ .

**Definition 2.1.2.** Let  $X$  be a Hausdorff topological space, and let  $\mathcal{A}$  be a  $\sigma$ -algebra on  $X$  such that  $\mathcal{B}(X) \subseteq \mathcal{A}$ . A measure  $\mu$  on  $\mathcal{A}$  is called **regular** (or **Radon**) if the following hold.

1.  $\mu(K) < \infty$  for all compact subsets  $K$  of  $X$ ;
2.  $\mu(A) = \inf\{\mu(U) : U \text{ is open and } A \subseteq U\}$  for all  $A \in \mathcal{A}$ , and
3.  $\mu(U) = \sup\{\mu(K) : K \text{ is compact and } K \subseteq U\}$  for all open subsets  $U$  of  $X$ .

A measure satisfying part (2) is called **outer regular**, and a measure satisfying part (3) is called **inner regular**.

**Definition 2.1.3.** Let  $G$  be a group, let  $a \in G$ , and let  $A$  and  $B$  be subsets of  $G$ . We define the following sets.

1.  $aB = \{ab : b \in B\}$ .
2.  $Ba = \{ba : b \in B\}$ .
3.  $AB = \{ab : a \in A, b \in B\}$ .
4.  $A^{-1} = \{a^{-1} : a \in A\}$ .

A set  $A$  such that  $A = A^{-1}$  is called **symmetric**.

**Definition 2.1.4.** A **topological group** is a group  $G$  endowed<sup>1</sup> with a topology  $\tau$  such that the product  $m : G \times G \rightarrow G$  and the inverse  $i : G \rightarrow G$  are continuous with respect to  $(\tau \times \tau, \tau)$  and  $(\tau, \tau)$ , respectively. We will denote by  $e$  the identity of  $G$ .

An **isomorphism** of topological groups  $\varphi : G_1 \rightarrow G_2$  is an isomorphism of groups that is also a homeomorphism of topological spaces. A **locally compact topological group** is a Hausdorff topological group  $G$  with the property that every point (equivalently, the identity) has an open neighbourhood with compact closure.

---

<sup>1</sup>more precisely: the underlying set of  $G$  is endowed

**Definition 2.1.5.** Let  $G$  be a topological group. The functions

$$\begin{aligned} L_a : G &\rightarrow G \\ x &\mapsto ax \end{aligned}$$

and

$$\begin{aligned} R_a : G &\rightarrow G \\ x &\mapsto xa \end{aligned}$$

are called respectively the **left translation by  $a$**  and the **right translation by  $a$** .

**Remark 2.1.6.** For any  $a \in G$ , the functions  $L_a$  and  $R_a$  are homeomorphisms from  $G$  to itself. Note that the inversion map  $\iota : G \rightarrow G$  is also a homeomorphism.

**Lemma 2.1.7.** Let  $G$  be a topological group and fix  $a \in G$ .

1. If  $\mathcal{U}$  is a fundamental system of neighbourhoods for the identity  $e$  of  $G$ , then the collections  $\{aU : U \in \mathcal{U}\}$  and  $\{Ua : U \in \mathcal{U}\}$  are fundamental systems of neighbourhoods for  $a$ .
2. If  $K$  and  $L$  are compact subsets of  $G$ , then the sets  $aK$ ,  $Ka$ ,  $K^{-1}$  and  $KL$  are compact.

*Proof.* 1. We have already observed that  $L_a, R_a$  are homeomorphisms, hence they carry fundamental systems of neighbourhoods to fundamental systems of neighbourhoods.

2. The sets in question are images of  $K$  (respectively,  $K \times L$ ) under the continuous maps  $L_a, R_a, \iota$  (respectively,  $m : G \times G \rightarrow G$ ).

□

**Lemma 2.1.8.** Let  $G$  be a topological group and  $U$  be an open neighbourhood of  $e$ .

1. There exists an open neighbourhood  $V$  of  $e$  such that  $VV \subseteq U$ .
2. There exists a symmetric open neighbourhood  $V$  of  $e$  such that  $V \subseteq U$ .

*Proof.* 1. The set  $m^{-1}(U) \subseteq G \times G$  is open, hence it contains an open set of the form  $V_1 \times V_2$  with  $V_1, V_2$  open in  $G$ . Setting  $V := V_1 \cap V_2$  we then have  $VV = m(V, V) \subseteq m(V_1, V_2) \subseteq U$ .

2. The intersection  $V := U \cap U^{-1}$  is open and symmetric.

□

**Definition 2.1.9.** Let  $X$  be a topological space and let  $f : X \rightarrow \mathbb{C}$  be a continuous function. The **support of  $f$** , denoted  $\text{supp}(f)$ , is the closure of the set  $\{x \in X : f(x) \neq 0\}$ .

If  $X$  is Hausdorff and locally compact, we write  $\mathcal{K}(X)$  for the  $\mathbb{C}$ -vector space of all continuous functions  $f : X \rightarrow \mathbb{C}$  with compact support.

**Remark 2.1.10.** For every function  $f \in \mathcal{K}(X)$ , the real-valued function  $|f|$  is bounded. Moreover, if  $\mu$  is a regular Borel measure on  $X$ , then  $f$  is  $\mu$ -integrable. Indeed,  $f$  is Borel-measurable because it is continuous, and since  $\mu$  is regular,  $\mu(\text{supp}(f)) < \infty$ , so  $\int_X |f| d\mu = \int_{\text{supp}(f)} |f| d\mu \leq \mu(\text{supp}(f)) \cdot \|f\|_\infty$  is certainly finite.

**Proposition 2.1.11.** Let  $G$  be a topological group, let  $K$  be a compact subset of  $G$ , and let  $U$  be an open subset of  $G$  containing  $K$ . There exist open neighbourhoods  $V_R$  and  $V_L$  of  $e$  such that  $KV_R \subseteq U$  and  $V_L K \subseteq U$ .

*Proof.* We give the construction for  $V_R$ , that for  $V_L$  being virtually identical. For every  $x \in K$  consider the open neighbourhood  $x^{-1}U$  of  $e$ . By Lemma 2.1.8 (2), there exists an open neighbourhood  $V_x$  of  $e$  such that  $V_x V_x \subseteq x^{-1}U$ . The set  $\{xV_x\}_{x \in K}$  is an open cover of  $K$ . Let  $x_1 V_{x_1}, \dots, x_n V_{x_n}$  be a finite subcover, and set  $V_R := \bigcap_{i=1}^n V_{x_i}$ . We claim that  $KV_R \subseteq U$ . Indeed, for any  $k \in K$  there exists  $i \in \{1, \dots, n\}$  such that  $k \in x_i V_{x_i}$ , hence (using  $V_R \subseteq V_{x_i}$ ) we obtain

$$kV_R \in x_i V_{x_i} V_{x_i} \subseteq x_i (x_i^{-1}U) = U.$$

□

## 2.1.2 Haar measure: existence

**Definition 2.1.12** (Haar measure). Let  $G$  be a locally compact group. A **left Haar measure** on  $G$  is a nonzero regular Borel measure  $\mu$  on  $G$  that is invariant under left-translations, in the sense that  $\mu(gA) = \mu(A)$  for all  $g \in G$  and all  $A \in \mathcal{B}(G)$ . Right Haar measures are defined similarly.

**Remark 2.1.13.** Note that, since  $L_g$  is a homeomorphism,  $L_g(A) = gA$  is a Borel set if and only if  $A$  is. In particular,  $\mu(gA)$  makes sense.

**Remark 2.1.14.** If  $G$  is commutative, a measure  $\mu$  is a left Haar measure if and only if it is a right Haar measure. In general,  $\mu$  is a left Haar measure if and only if  $A \mapsto \mu(A^{-1})$  is a right Haar measure. From now on, following a well-established tradition, we will only consider the case of left Haar measures, leaving the case of right-invariant measures as a simple exercise.

**Example 2.1.15** (Some basic Haar measures). *The following are examples of (left and right) Haar measures.*

1. Let  $G$  be a finite group endowed with the discrete topology. The counting measure on  $G$  (that is,  $\mu(A) = |A|$ ) is a Haar measure.
2. Let  $G = (\mathbb{R}, +)$  with its usual topology. The restriction of the Lebesgue measure to the  $\sigma$ -algebra  $\mathcal{B}(\mathbb{R})$  is a Haar measure.
3. Let  $G = (\mathbb{R}^+, \cdot)$  and let  $\mu = \frac{1}{x} dx$ , where  $dx$  is the standard Lebesgue measure (restricted to the  $\sigma$ -algebra  $\mathcal{B}(\mathbb{R})$ ). Then  $\mu$  is a Haar measure on  $G$ : this follows from the change-of-variables formula in elementary integration theory, since for any  $g \in \mathbb{R}^+$  we have

$$\mu(gA) = \int_{gA} 1 \, d\mu = \int_{gA} \frac{dx}{x} = \int_A \frac{d(gx)}{gx} = \int_A \frac{dx}{x} = \mu(A).$$

The main theorem in this section shows that every locally compact topological group carries a(t least one) Haar measure:

**Theorem 2.1.16** (Existence of the Haar measure). *Let  $G$  be a locally compact topological group. There exists a left Haar measure  $\mu$  for  $G$ .*

The proof will occupy the rest of this section. We start with four simple lemmas in topology.

**Lemma 2.1.17.** *Let  $X$  be a Hausdorff topological space, and let  $K$  and  $L$  be disjoint compact subsets of  $X$ . There exist disjoint open subsets  $U$  and  $V$  of  $X$  such that  $K \subseteq U$  and  $L \subseteq V$ .*

*Proof.* Easy exercise. □

**Lemma 2.1.18.** *Let  $X$  be a locally compact Hausdorff topological space. Let  $x \in X$  and let  $U$  be an open neighbourhood of  $x$ . There exists an open neighbourhood  $V$  of  $x$  with compact closure that satisfies  $\overline{V} \subseteq U$ .*

*Proof.* Since  $X$  is locally compact, there is an open neighbourhood  $W$  of  $x$  with compact closure. Replacing  $W$  with  $W \cap U$  if necessary, we may assume that  $W \subseteq U$  (note that  $\overline{W} \cap \overline{U}$  is closed in  $\overline{W}$ , hence it is a closed subset of a compact set, and therefore it is itself compact). Consider the sets  $\{x\}$  and  $\overline{W} \setminus W$ , which are compact and disjoint. Lemma 2.1.17 shows the existence of disjoint open subsets  $V_1$  and  $V_2$  such that  $\{x\} \subseteq V_1$  and  $\overline{W} \setminus W \subseteq V_2$ . The set  $V_1 \cap W$  is an open neighbourhood of  $x$  whose closure is compact (proven as above) and satisfies  $\overline{V_1 \cap W} \subseteq W \subseteq U$  (indeed,  $\overline{V_1 \cap W}$  does not meet  $V_2 = \overline{W} \setminus W$ ). □

**Corollary 2.1.19.** *Let  $X$  be a locally compact Hausdorff topological space, let  $K$  be a compact subset of  $X$ , and let  $U$  be an open subset of  $X$  containing  $K$ . There exists an open subset  $V$  of  $X$  such that  $\overline{V}$  is compact and that satisfies  $K \subseteq V \subseteq \overline{V} \subseteq U$ .*

*Proof.* For each point of  $K$  find a neighbourhood  $V_x$  as in the previous lemma. The union of the  $V_x$  covers  $K$ : extract a finite cover  $V_{x_1}, \dots, V_{x_n}$  and set  $V = \cup V_{x_i}$ . □

**Lemma 2.1.20.** *Let  $X$  be a locally compact Hausdorff topological space, let  $K$  be a compact subset of  $X$ , and let  $U_1$  and  $U_2$  be open subsets of  $X$  such that  $K \subseteq U_1 \cup U_2$ . There exist compact sets  $K_1$  and  $K_2$  such that  $K = K_1 \cup K_2$ ,  $K_1 \subseteq U_1$  and  $K_2 \subseteq U_2$ .*

*Proof.* Let  $U, V$  be the open sets obtained from applying Lemma 2.1.17 to the disjoint compact sets  $K \setminus U_1$  and  $K \setminus U_2$ . We can take  $K_1 = K \setminus V$  and  $K_2 = K \setminus U$ : these are closed in  $K$ , hence compact, and  $K_1 \subseteq K \setminus (K \cap U_2) \subseteq U_1$  (and similarly for  $K_2$ ). Finally, their union is all of  $K$  since  $U_1 \cap U_2 = \emptyset$ . □

We now have all the ingredients to construct a Haar measure on any locally compact group. The key idea is that the ‘size’ of a subset  $X$  of  $G$  should be measured as follows: one takes a ‘small’ neighbourhood of the identity  $U$ , and counts how many translates of  $U$  are necessary to cover  $X$ . In order to make sense of this, one should first work with *compact* subsets  $X$  (which ensures that finitely many translates of  $U$  suffice), and of course we also need to somehow normalise this counting (morally, we would like to divide by the size of  $U$  itself). Since we do not know how to assign a measure to  $U$  yet, we declare that its measure is inversely proportional to the number of translates needed to cover a *fixed* reference compact set  $K_0$ . Once we have a notion of size for compact sets, the rest of the construction is standard: we first obtain an outer measure on all Borel subsets of  $G$ , and finally check that this is in fact already a measure. We now start putting this strategy in practice.

**Remark 2.1.21.** The construction sketched above is reminiscent of the Hausdorff measure in  $\mathbb{R}^n$ , which assigns a size to sets by counting how many balls of radius  $\varepsilon$  are needed to cover it, in the limit  $\varepsilon \rightarrow 0$ . The added difficulty we face here is that we don’t know what volume to assign to (the analogue of) a ball of radius  $\varepsilon$ , because for general  $G$  there is no such simple fundamental system of neighbourhoods of the identity as in the case of  $\mathbb{R}^n$ .

*Proof of Theorem 2.1.16.* We start by defining a notion of ‘index’  $(K : V)$ , whenever  $K$  is compact and  $V$  has non-empty interior  $V^\circ$ : we set

$$(K : V) = \min\{n \in \mathbb{N} : \text{there exists a cover of } K \text{ by } n \text{ translates of } V^\circ\}.$$

It is clear that the definition is well-posed:  $\{xV^\circ\}_{x \in G}$  is an open cover of  $K$ , hence we can extract a finite one. Notice that  $(K : V) = 0$  if and only if  $K = \emptyset$ .

Now, using the assumption of local compactness, fix a neighbourhood of the identity with compact closure  $K_0$ . This is our ‘reference compact set’; note that  $K_0^\circ$  is non-empty, hence we can also measure the index  $(K : K_0)$  for any compact set  $K$ .

Let  $\mathcal{C}$  be the collection of all compact subsets of  $G$  and let  $\mathcal{U}$  be the collection of all open neighbourhoods of the identity. For each  $U \in \mathcal{U}$  we define a function

$$\begin{aligned} h_U : \mathcal{C} &\rightarrow \mathbb{R} \\ K &\mapsto \frac{(K:U)}{(K_0:U)}. \end{aligned}$$

The next lemma gives some basic properties of the functions  $h_U$ .

**Lemma 2.1.22.** *Fix  $U \in \mathcal{U}$ ,  $K, K_1, K_2 \in \mathcal{C}$  and  $x \in G$ . The following hold.*

1.  $0 \leq h_U(K) \leq (K : K_0)$ .
2.  $h_U(K_0) = 1$ .
3.  $h_U(xK) = h_U(K)$ .
4. If  $K_1 \subseteq K_2$ , then  $h_U(K_1) \leq h_U(K_2)$ .
5.  $h_U(K_1 \cup K_2) \leq h_U(K_1) + h_U(K_2)$ .
6. If  $K_1U^{-1} \cap K_2U^{-1} = \emptyset$ , then  $h_U(K_1 \cup K_2) = h_U(K_1) + h_U(K_2)$ .

*Proof.* Parts (2) and (4) are clear, as is the lower bound in (1). For the upper bound in (1), let  $\{x_i K_0^\circ\}_{i=1, \dots, (K:K_0)}$  be an open cover of  $K$  with translates of  $K_0^\circ$  and let  $\{y_j U\}_{j=1, \dots, (K_0:U)}$  be an open cover of  $K_0$  with translates of  $U$ . Then, we have

$$K \subseteq \bigcup_{i=1}^{(K:K_0)} x_i K_0^\circ \subseteq \bigcup_{i=1}^{(K:K_0)} x_i K_0 \subseteq \bigcup_{i=1}^{(K:K_0)} x_i \left( \bigcup_{j=1}^{(K_0:U)} y_j U \right) = \bigcup_{i,j} x_i y_j U,$$

hence  $K$  can be covered by at most  $(K : K_0)(K_0 : U)$  translates of  $U$ . This gives  $(K : U) \leq (K : K_0)(K_0 : U)$ , which is equivalent to the desired upper bound.

For (3), observe that translating every element of an open cover of  $K$  by  $x$  gives an open cover of  $xK$  with the same number of elements. For (5), use that the union of an open cover of  $K_1$  and an open cover of  $K_2$ , consisting respectively of  $(K_1 : U)$  and  $(K_2 : U)$  translates of  $U$ , gives an open cover of  $K_1 \cup K_2$  consisting of  $(K_1 : U) + (K_2 : U)$  translates of  $U$ .

Finally, for (6), we need to show the inequality  $h_U(K_1 \cup K_2) \geq h_U(K_1) + h_U(K_2)$ , or equivalently,  $(K_1 \cup K_2 : U) \geq (K_1 : U) + (K_2 : U)$ . Let  $\{xU\}$  be an open cover of  $K_1 \cup K_2$ . We claim that each set  $xU$  in the cover meets at most one of  $K_1, K_2$ : if we had  $xU \cap K_1 \neq \emptyset$  and  $xU \cap K_2 \neq \emptyset$ , then  $x$  would be both in  $K_1U^{-1}$  and in  $K_2U^{-1}$ , contradiction since by assumption  $K_1U^{-1} \cap K_2U^{-1} = \emptyset$ . Hence, from  $\{xU\}$  we can extract two disjoint subsets, one covering  $K_1$  and the other covering  $K_2$ . The desired inequality follows immediately.  $\square$



We now construct a suitable limit of the functions  $h_U$ , arguing by compactness. Let

$$X := \prod_{K \in \mathcal{C}} [0, (K : K_0)]$$

and note that  $X$ , being a product of non-empty compact intervals of  $\mathbb{R}$ , is a non-empty compact space. We consider  $X$  as a subset of  $\mathbb{R}^{\mathcal{C}}$ , the space of functions from  $\mathcal{C}$  to  $\mathbb{R}$ . Lemma 2.1.22 shows that each  $h_U$  is an element of  $X$ .

We now construct the desired ‘limit’ of the functions  $h_U$ . For each open neighbourhood  $V$  of  $e$ , let  $S(V)$  be the closure in  $X$  of the set  $\{h_U : U \in \mathcal{U}, U \subseteq V\}$ . If  $V_1, \dots, V_n$  are in  $\mathcal{U}$  and  $V$  is their intersection, then  $h_V \in \bigcap_{i=1}^n S(V_i)$ . This implies that any finite intersection of sets  $S(V_i)$  is nonempty; by compactness,  $\bigcap_{V \in \mathcal{U}} S(V)$  is also non-empty. Let  $h_o$  be an element of this intersection. The next lemma is the analogue of Lemma 2.1.22 for  $h_o$ .

**Lemma 2.1.23.** *Fix  $K, K_1, K_2 \in \mathcal{C}$  and  $x \in G$ . The following hold:*

1.  $0 \leq h_o(K)$ .
2.  $h_o(\emptyset) = 0$ .
3.  $h_o(K_0) = 1$ .
4.  $h_o(xK) = h_o(K)$ .
5. If  $K_1 \subseteq K_2$ , then  $h_o(K_1) \leq h_o(K_2)$ .
6.  $h_o(K_1 \cup K_2) \leq h_o(K_1) + h_o(K_2)$ .
7. If  $K_1 \cap K_2 = \emptyset$ , then  $h_o(K_1 \cup K_2) = h_o(K_1) + h_o(K_2)$ .

*Proof.* The key point is that, by the definition of the product topology, for any fixed  $K \in \mathcal{C}$ , the projection

$$\begin{array}{ccc} X & \rightarrow & \mathbb{R} \\ h & \mapsto & h(K) \end{array}$$

is continuous. This implies easily all statements (1) through (6): for example, for (6), fix  $K_1, K_2$  and consider the function

$$\begin{array}{ccc} X & \rightarrow & \mathbb{R} \\ h & \mapsto & h(K_1) + h(K_2) - h(K_1 \cup K_2). \end{array}$$

As already argued, this function is continuous. By Lemma 2.1.22 (5) it is non-negative on every  $h_U$ , hence (by continuity) on every  $S(V)$ , and thus, in particular, on  $h_o$ .

Part (7) requires some more care. By Lemma 2.1.17, there exist open sets  $U_1, U_2$  with  $K_1 \subseteq U_1, K_2 \subseteq U_2$  and  $U_1 \cap U_2 = \emptyset$ . Proposition 2.1.11 gives two open neighbourhoods  $V_1, V_2$  of  $e$  such that  $K_i V_i \subseteq U_i$  for  $i = 1, 2$ . Letting  $V = V_1 \cap V_2$ , we have  $K_1 U^{-1} \cap K_2 U^{-1} = \emptyset$  for any  $U \subseteq V^{-1}$ , and therefore  $h_U(K_1 \cup K_2) = h_U(K_1) + h_U(K_2)$  for any such  $U$  (Lemma 2.1.22 (6)). By continuity, the same condition holds for all  $h \in S(V^{-1})$ , and in particular for  $h_o$ .  $\square$

The function  $h_\circ$  is essentially the desired Haar measure. We now carry out the necessary measure-theoretic verifications. We define first an outer measure on open sets by setting

$$\begin{aligned} \mu^* : \mathcal{V} &\rightarrow [0, \infty] \\ U &\mapsto \sup\{h_\circ(K) : K \subseteq U, K \in \mathcal{C}\}, \end{aligned} \quad (2.1)$$

where  $\mathcal{V}$  is the collection of all open sets in  $G$ . It is immediate to check that, if  $U$  is both open and compact, then  $\mu^*(U) = h_\circ(U)$ . Next, we extend  $\mu^*$  to all subsets of  $G$  by setting

$$\begin{aligned} \mu^* : \mathcal{P}(G) &\rightarrow [0, \infty] \\ A &\mapsto \inf\{\mu^*(U) : A \subseteq U, U \in \mathcal{V}\}. \end{aligned} \quad (2.2)$$

Lemma 2.1.23 implies that  $\mu^*$  is monotonic, non-negative, and satisfies  $\mu^*(\emptyset) = 0$ . It remains to check that  $\mu^*$  is countably sub-additive and that all Borel sets are measurable.

It follows easily from the definition (2.2) that it suffices to check the sub-additivity on open sets. Let  $\{U_i\}_{i \geq 1}$  be a countable collection of open sets in  $G$  and let  $K \subseteq \bigcup_i U_i$  be a compact set. Since the  $U_i$  form an open cover of the compact set  $K$ , there is an index  $n$  such that  $K \subseteq \bigcup_{i=1}^n U_i$ . By Lemma 2.1.20 and a straightforward induction, we obtain compact sets  $K_1, \dots, K_n$  such that  $K_i \subseteq U_i$  for  $i = 1, \dots, n$  and  $K = K_1 \cup \dots \cup K_n$ . By Equation (2.1) we have  $\mu^*(K_i) \leq \mu^*(U_i)$ . Combining this with Lemma 2.1.23 (6) we obtain

$$\mu^*(K) \leq \sum_{i=1}^n \mu^*(K_i) \leq \sum_{i=1}^n \mu^*(U_i) \leq \sum_{i=1}^{\infty} \mu^*(U_i).$$

Since this holds for all compact sets  $K \subseteq \bigcup_i U_i$ , taking the supremum in  $K$  we get  $\mu^*(\bigcup_i U_i) \leq \sum_{i=1}^{\infty} \mu^*(U_i)$ , as desired.

We now turn to the measurability of Borel sets. Since the set of measurable sets is a  $\sigma$ -algebra, and since by definition  $\mathcal{B}(G)$  is the  $\sigma$ -algebra generated by open sets, it suffices to show that open sets are measurable. Recall that, by definition, a set  $X$  is  $\mu^*$ -measurable if and only if, for all subsets  $Y$  of  $G$  we have

$$\mu^*(Y) = \mu^*(Y \cap X) + \mu^*(Y \setminus X). \quad (2.3)$$

We claim that is enough to show this when  $Y$  is itself an open set. Indeed, suppose that the equality

$$\mu^*(V) = \mu^*(V \cap X) + \mu^*(V \setminus X) \quad (2.4)$$

holds for all open sets  $V$ . Consider the infimum of the above expression over all open sets  $V$  that contain  $Y$ . We have

1.  $\inf_{V \supseteq Y} \mu^*(V) = \mu^*(Y)$ , by definition;
2.  $\inf_{V \supseteq Y} \mu^*(V \cap X) \geq \mu^*(Y \cap X)$ : to see this, recall that we are assuming  $X$  to be open, so the intersection  $V \cap X$  is open and contains  $Y \cap X$ . Thus, the left-hand side of the previous equality is the infimum of  $\mu^*(U)$  over *certain* open subsets  $U$  containing  $Y \cap X$ . Thus, the left-hand side is at least as large as the right-hand side (which is the infimum of  $\mu^*(U)$  over *all* open subsets  $U$  containing  $Y \cap X$ ).

3.  $\inf_{V \supseteq Y} \mu^*(V \setminus X) = \mu^*(Y \setminus X)$ : to see this, write the definition of both sides as

$$\inf_{V \supseteq Y} \inf_{\substack{U_1 \text{ open} \\ U_1 \supseteq V \setminus X}} \mu^*(U_1) = \inf_{U_2 \supseteq Y \setminus X} \mu^*(U_2).$$

Given a set  $U_1$  as on the left-hand side, this is in particular an open that contains  $Y \setminus X$ , hence it also appears in the infimum on the right-hand side. This proves that the LHS is greater than or equal to the RHS. Conversely, let  $U_2$  be an open set that appears in the infimum on the right-hand side. Then  $V = U_2 \cup X$  is an open set containing  $(Y \setminus X) \cup X \supseteq Y$ , and  $U_1 = U_2$  is an open set containing  $V \setminus X = (U_2 \cup X) \setminus X = U_2 \setminus X$ . Thus,  $U_2$  also appears in the infimum on the left-hand side, which establishes the opposite inequality.

Thus, if (2.4) holds for all open sets  $X$  and  $V$ , taking the infimum as above we obtain

$$\mu^*(Y) \geq \mu^*(Y \cap X) + \mu^*(Y \setminus X)$$

for all sets  $Y$ . On the other hand, the opposite inequality is true by sub-additivity (which we have already shown), hence we have obtained (2.3) for all open sets  $X$  and for all sets  $Y$ .

Hence, to finish the proof that Borel sets are measurable, it suffices to prove that if  $U, V$  are open sets with  $\mu^*(V) < \infty$  we have

$$\mu^*(V) \geq \mu^*(V \cap U) + \mu^*(V \cap U^c).$$

Choose a compact subset  $K$  of  $V \cap U$  with  $h_o(K) \geq \mu^*(V \cap U) - \varepsilon$  and a compact subset  $L$  of  $V \cap K^c$  with  $h_o(L) \geq \mu^*(V \cap K^c) - \varepsilon$ . Clearly  $K$  and  $L$  are disjoint and  $V \cap U^c \subseteq V \cap K^c$ . Since  $\mu^*$  is monotonic, we have

$$h_o(L) \geq \mu^*(V \cap K^c) - \varepsilon \geq \mu^*(V \cap U^c) - \varepsilon$$

and from Lemma 2.1.23 (7) we obtain

$$h_o(K \cup L) = h_o(K) + h_o(L) \geq (\mu^*(V \cap U) - \varepsilon) + (\mu^*(V \cap U^c) - \varepsilon) = \mu^*(V \cap U) + \mu^*(V \cap U^c) - 2\varepsilon.$$

Since  $K \cup L \subseteq V$  we have obtained

$$\mu^*(V) \geq h_o(K \cup L) \geq \mu^*(V \cap U) + \mu^*(V \cap U^c) - 2\varepsilon$$

for all  $\varepsilon$ . Taking the limit  $\varepsilon \rightarrow 0$  finishes the proof that  $V$  is  $\mu^*$ -measurable. In particular, the restriction of  $\mu^*$  to the Borel  $\sigma$ -algebra is a measure  $\mu$ . By property (4) in Lemma 2.1.23, the measure  $\mu$  satisfies  $\mu(xA) = \mu(A)$  for every Borel set  $A$  and every  $x \in G$ . Furthermore, it follows from Lemma 2.1.23 (3) and the definition of  $\mu^*$  that  $\mu$  is nonzero. To show that  $\mu$  is the desired Haar measure it now suffices to check that it is regular (see Definition 2.1.2).

If  $K$  a compact set and  $U$  is an open set containing  $K$ , then by definition  $h_o(K) \leq \mu^*(U) = \mu(U)$ . Taking the infimum over all  $U$  we obtain

$$h_o(K) \leq \mu(K). \tag{2.5}$$

Suppose now that  $V$  is open with compact closure. Then for every compact subset  $L$  of  $V$  we have  $h_o(L) \leq h_o(\bar{V})$  by Lemma 2.1.23 (5). Taking the supremum over  $L$  we obtain that

$\mu(V) \leq h_o(\overline{V})$  is finite (notice that  $h_o$  is finite on compact sets by definition). If  $K$  is an arbitrary compact subset of  $G$ , then by Corollary 2.1.19 (applied to  $K$  and  $U = G$ ) there exists an open set  $V$  containing  $K$  whose closure is compact. Thus, by monotonicity we have that  $\mu(K) \leq \mu(V) \leq h_o(\overline{V})$  is finite. We have checked property (1) in the definition of a regular measure. Outer regularity (property (2) in the definition) is an immediate consequence of the definition in Equation (2.2), while inner regularity follows from Equations (2.1) and (2.5).  $\square$

We conclude this section by highlighting the key property of Haar measures from the standpoint of integration:

**Theorem 2.1.24** (Invariance of the Haar integral under translation). *Let  $G$  be a locally compact group and  $\mu$  be a left Haar measure on  $G$ . Let furthermore  $f$  be a  $\mu$ -integrable function on  $G$  and fix  $x \in G$ . We have*

$$\int_G f(t) d\mu(t) = \int_G f(x^{-1}t) d\mu(t).$$

*Sketch of proof.* When  $f$  is the characteristic function of a (measurable) set  $A$ , the function  $f(x^{-1}t)$  is the characteristic function of  $xA$ , so we have

$$\int_G f(t) d\mu(t) = \mu(A) = \mu(xA) = \int_G f(x^{-1}t) d\mu(t),$$

as desired. By linearity, the claim holds for all simple functions, and by passing to the limit we obtain it for all measurable functions.  $\square$

### 2.1.3 Haar measure: uniqueness (up to constants)

In the previous section we have shown that every locally compact group carries at least one (left) Haar measure. It can be shown that this measure is in fact essentially unique:

**Theorem 2.1.25** (Uniqueness of the Haar measure up to constants). *Let  $G$  be a locally compact group and let  $\mu_1, \mu_2$  be two left Haar measures on  $G$ . There exists  $c \in \mathbb{R}, c > 0$ , such that  $\mu_2 = c\mu_1$ .*

It wouldn't be too hard to prove this theorem in general, but since we only need it for the case of abelian groups, we limit ourselves to giving a (shorter and easier) proof for this special case. For the general case, the reader can refer to [RV99, pp. 16–19].

*Proof in the commutative case.* Fix a non-zero, non-negative function  $g \in \mathcal{K}(G)$  (see Definition 2.1.9; that one such function exists follows for example from Urysohn's lemma). It is easy to see that one can choose  $g$  in such a way that  $\int_G g(x^{-1}) d\mu_1(x) > 0$ . Let  $f(x) \in \mathcal{K}(G)$  be arbitrary.

Using the Fubini-Tonelli theorem together with Theorem 2.1.24 we compute

$$\begin{aligned}
\int_G f(x) d\mu_1(x) \cdot \int_G g(y) d\mu_2(y) &= \int_G \int_G f(x)g(y) d\mu_1(x) d\mu_2(y) \\
&= \int_G \int_G f(xy)g(y) d\mu_1(x) d\mu_2(y) \\
&\stackrel{y \mapsto x^{-1}y=yx^{-1}}{=} \int_G \int_G f(y)g(yx^{-1}) d\mu_1(x) d\mu_2(y) \\
&= \int_G f(y) \left( \int_G g(yx^{-1}) d\mu_1(x) \right) d\mu_2(y) \\
&= \int_G f(y) \left( \int_G g(x^{-1}) d\mu_1(x) \right) d\mu_2(y) \\
&= \left( \int_G g(x^{-1}) d\mu_1(x) \right) \int_G f(y) d\mu_2(y).
\end{aligned}$$

Rearranging, we have obtained

$$\int_G f(y) d\mu_2(y) = \frac{\int_G g(y) d\mu_2(y)}{\int_G g(x^{-1}) d\mu_1(x)} \cdot \int_G f(x) d\mu_1(x),$$

where the ratio  $c := \frac{\int_G g(y) d\mu_2(y)}{\int_G g(x^{-1}) d\mu_1(x)}$  is independent of  $f$  (recall that we chose  $g(x)$  so that the denominator is strictly positive). We have thus obtained

$$\int_G f d\mu_2 = c \int_G f d\mu_1$$

for all  $f \in \mathcal{K}(X)$ . Standard arguments in measure theory (e.g., using Riesz's representation theorem 2.1.28, which says that measures are equivalent to positive linear functionals on the space of compactly supported continuous functions) then imply  $\mu_2 = c\mu_1$ , as desired.  $\square$

**Remark 2.1.26.** An alternative proof of the same result, not using Theorem 2.1.28 or Urysohn's lemma, goes as follows. Let  $K$  be a compact set with non-empty interior  $U$  (which exists, because by assumption  $G$  is locally compact). We first claim that  $\mu_1(K)$  and  $\mu_2(K)$  are non-zero. Indeed, suppose by contradiction that  $\mu_j(K) = 0$  (for  $j = 1$  or  $j = 2$ ). Any compact set  $K'$  can be covered with finitely many translates  $x_1U, \dots, x_nU$  of the interior  $U$  of  $K$ . Using the translation-invariance of Haar measures we then have

$$\mu_j(K') \leq \sum_{i=1}^n \mu_j(x_iU) = \sum_{i=1}^n \mu_j(U) \leq n\mu_j(K) = 0,$$

so every compact set has measure 0. By regularity, this implies that  $\mu_j$  is identically 0, contradiction.

Take now  $g = \mathbf{1}_{K^{-1}}$  to be the characteristic function of  $K^{-1}$  and  $f = \mathbf{1}_V$  to be the characteristic function of any open set  $V$  with compact closure. The argument in the previous proof shows that  $\mu_2(V) = c\mu_1(V)$ , where the constant  $c$  is independent of  $V$ . Thus,  $\mu_2$  and  $c\mu_1$  coincide on all open sets with compact closure. By outer regularity, this easily implies that  $\mu_2$  and  $c\mu_1$  coincide on all compact sets; and by inner regularity, this finally implies  $\mu_2 = c\mu_1$ .

This remark is due to Davide Colpo and Giulio Grammatica.

**Definition 2.1.27.** Let  $G$  be a locally compact group. We denote by  $L^1(G)$  the  $\mathbb{C}$ -vector space of functions  $f : G \rightarrow \mathbb{C}$  such that  $\int_G |f| d\mu < \infty$ , where  $\mu$  is any left Haar measure on  $G$ . By Theorem 2.1.25, this definition is independent of the choice of the Haar measure.

We conclude this section by stating the exact form of the Riesz(-Markov-Kakutani) representation theorem we used above. It will also later help us obtain Haar measures on the multiplicative group of a field.

**Theorem 2.1.28** (Riesz–Markov–Kakutani). *Let  $X$  be a locally compact Hausdorff space. For any positive linear functional  $\psi$  on  $\mathcal{K}(X)$ , there is a unique Radon measure  $\mu$  on  $X$  such that*

$$\forall f \in C_c(X) : \quad \psi(f) = \int_X f(x) d\mu(x).$$

## 2.2 Abstract Fourier analysis

Our purpose in this section is to generalise Theorem 1.5.17 to an arbitrary locally compact abelian group. We will not give proofs: the statements should all look familiar and believable, but the detailed arguments get complicated. The interested reader may refer to any of the following sources: the original paper by Cartan and Godement [CG47]; Chapter 4 of [Fol16]; Chapter 3 of [RV99] (Chapter 2 of the same book covers the relevant spectral theory prerequisites).

We mention right at the start that, when working with a general topological group  $G$ , one can consider both

- its **characters**, that is, the continuous homomorphisms  $G \rightarrow \mathbb{S}^1 = \{z \in \mathbb{C} : |z| = 1\}$ ;
- its **quasi-characters**, that is, the continuous homomorphisms  $G \rightarrow \mathbb{C}^\times$ .

Note that the two notions coincide when  $G$  is finite, which is why we didn't have to worry about the distinction in Section 1.5. While in this section we are mostly concerned with the actual *characters* of a group, the more general notion of quasi-character will be central in Tate's thesis.

### 2.2.1 Pontryagin duality: general case

We start by stating Pontryagin duality in general (see Proposition 1.5.8 for the finite case). We omit the proof, for which the reader can refer to [RV99, Proposition 3-2 and Theorem 3-20].

**Definition 2.2.1** (Topological dual group). Let  $G$  be a locally compact abelian group. We denote by

$$\hat{G} = \text{Hom}_{\text{cont}}(G, \mathbb{S}^1)$$

the group of continuous homomorphisms from  $G$  to  $\mathbb{S}^1$ . We endow  $\hat{G}$  with the **compact-open** topology, defined as follows. For every compact neighbourhood  $K$  of  $\text{id}_G$  in  $G$  and every open neighbourhood  $V$  of  $1 \in \mathbb{S}^1$ , denote by

$$U(K, V) = \{\chi \in \hat{G} : \chi(K) \subseteq V\}.$$

The (compact-open) topology on  $\hat{G}$  is by definition the topology having the sets  $\{U(K, V)\}_{K, V}$  as a basis of neighbourhoods of the trivial character. We extend it to a topology on  $\hat{G}$  by using the group structure as usual (that is, a basis of neighbourhoods around a general element  $\chi \in \hat{G}$  is  $\{\chi U(K, V)\}_{K, V}$ ). The topological group thus obtained is called the **Pontryagin dual** of  $G$ .

**Theorem 2.2.2** (Pontryagin duality). *For every locally compact abelian group  $G$  let  $\hat{G}$  be the Pontryagin dual group as in Definition 2.2.1.*

1.  $\hat{G}$  is also a locally compact abelian group.
2. The canonical map

$$\begin{aligned} \Psi : G &\rightarrow \hat{G} \\ g &\mapsto \Psi_g, \end{aligned}$$

where  $\Psi_g$  is given by

$$\begin{aligned} \Psi_g : \hat{G} &\rightarrow \mathbb{C}^\times \\ \chi &\mapsto \chi(g), \end{aligned}$$

is an isomorphism of topological groups.

3.  $G$  is compact if and only if  $\hat{G}$  is discrete.

**Remark 2.2.3.** Every finite group  $G$  is a topological group when equipped with the discrete topology. Moreover, in this case, the compact-open topology on  $\hat{G}$  is also the discrete topology. Thus, applying Theorem 2.2.2 to the case of finite groups recovers Proposition 1.5.8.

We also have the following analogue of Proposition 1.5.10 (see [Fol16, Proposition 4.39, Theorem 4.40] for a proof):

**Proposition 2.2.4** (Functoriality of  $G \mapsto \hat{G}$ , locally compact case). *Let  $G$  be a locally compact abelian group. The following hold:*

1. The association  $G \mapsto \hat{G}$  can be extended to a contravariant functor from the category of locally compact abelian groups to itself by letting it act on arrows as follows: if  $f : G \rightarrow H$  is a continuous group homomorphism between locally compact abelian groups, we define

$$\begin{aligned} \hat{f} : \hat{H} &\rightarrow \hat{G} \\ \chi &\mapsto \chi \circ f. \end{aligned}$$

2. This functor is exact: for every short exact sequence<sup>2</sup>

$$0 \rightarrow H \xrightarrow{\iota} G \xrightarrow{\pi} G/H \rightarrow 0,$$

the dual sequence

$$0 \rightarrow \widehat{G/H} \xrightarrow{\hat{\pi}} \hat{G} \xrightarrow{\hat{\iota}} \hat{H} \rightarrow 0$$

is also exact in the category of locally compact abelian groups. In particular,  $\widehat{G/H}$  is closed in  $\hat{G}$ , and can be identified with the subgroup

$$H^\perp = \{\chi \in \hat{G} : \chi|_H = 1\},$$

which is itself a closed subgroup of  $\hat{G}$ .

---

<sup>2</sup>in the category of locally compact abelian groups: in particular,  $H$  has to be closed in  $G$

We also mention the following analogue of Proposition 1.5.12 for compact groups:

**Proposition 2.2.5.** *Let  $G$  be a compact abelian group and let  $\chi \in \hat{G}$  be a character. We have*

$$\int_G \chi(g) dg = \begin{cases} 0, & \text{if } \chi \neq \text{id}_{\hat{G}} \\ \mu(G), & \text{otherwise} \end{cases}$$

*Proof.* Exactly as in the finite case: if  $\chi$  is nontrivial, there exists  $a \in G$  such that  $\chi(a) \neq 1$ . Using the translation-invariance property of the Haar measure,

$$\chi(a) \int_G \chi(g) dg = \int_G \chi(ag) dg = \int_G \chi(g) dg,$$

hence  $\int_G \chi(g) dg = 0$ . □

## 2.2.2 The abstract Fourier transform

Let  $G$  be a locally compact abelian group and let  $\mu_G$  be a choice of Haar measure on  $G$ . (If  $G$  is compact, we can normalise our choices by taking as  $\mu_G$  the unique *normalised* Haar measure, but this is not important for the discussion of this section.)

Recall from Definition 2.1.27 the  $\mathbb{C}$ -vector space  $L^1(G)$  of complex-valued integrable functions on  $G$ . We now introduce a notion of Fourier transform in this generality, which will generalise both the usual notion of Fourier transform encountered in real and complex analysis and the Fourier transform of Definition 1.5.15.

**Definition 2.2.6** (Abstract Fourier transform). Let  $G$  be a locally compact topological group with a fixed choice  $\mu_G$  of Haar measure and let  $f \in L^1(G)$ . We define the **(abstract) Fourier transform** of  $f$  as

$$\begin{aligned} \hat{f} : \hat{G} &\rightarrow \mathbb{C} \\ \chi &\mapsto \int_G f(g) \overline{\chi(g)} d\mu_G(g). \end{aligned}$$

**Remark 2.2.7.** Note that the integral makes sense:  $\int_G |f(g) \overline{\chi(g)}| d\mu_G(g) = \int_G |f(g)| d\mu_G(g) < \infty$  since  $\chi$  takes values in  $\mathbb{S}^1$ .

It will be useful to single out a class of well-behaved functions:

**Definition 2.2.8.** We denote by  $\mathfrak{B}^1(G)$  the  $\mathbb{C}$ -vector space of functions  $f : G \rightarrow \mathbb{C}$  that satisfy the following three conditions:

1.  $f$  is continuous;
2.  $f$  is in  $L^1(G)$ ;
3.  $\hat{f}$  is in  $L^1(\hat{G})$ .

**Remark 2.2.9.** In the previous definition,  $L^1(G)$ ,  $L^1(\hat{G})$  are defined with respect to any choice of Haar measures on  $G, \hat{G}$ : since any two Haar measures only differ by a constant, the spaces  $L^1(G)$ ,  $L^1(\hat{G})$  are independent of this choice.



The main theorem of abstract Fourier analysis can be stated as follows (for a proof see [Fol16, Theorem 4.33] or [RV99, Theorem 3-9]; notice that in our statement the function  $f$  is assumed to be continuous).

**Theorem 2.2.10** (Fourier inversion for the abstract Fourier transform). *Let  $G$  be a locally compact topological group with a fixed choice  $\mu_G$  of Haar measure. There is a unique Haar measure  $\mu_{\hat{G}}$  on  $\hat{G}$  such that the following holds: for all functions  $f \in \mathfrak{B}^1(G)$  we have*

$$f(g) = \int_{\hat{G}} \hat{f}(\chi) \chi(g) d\mu_{\hat{G}}(\chi) \quad \forall g \in G.$$

**Definition 2.2.11** (Dual measure). In the context of Theorem 2.2.10, we will say that  $\mu_{\hat{G}}$  is the measure on  $\hat{G}$  **dual** to the given Haar measure on  $G$ .

**Remark 2.2.12.** A crucial feature of Theorem 2.2.10 is the fact that the Haar measure  $\mu_{\hat{G}}$  is *independent of the function  $f$* . Notice that Haar measures are determined up to a constant, and therefore, one can determine  $\mu_{\hat{G}}$  in the following way. Let  $\mu$  be *any* Haar measure on  $\hat{G}$ : then  $\mu_{\hat{G}} = \alpha\mu$  for some nonzero  $\alpha$ . The inversion formula yields

$$f(g) = \alpha \int_{\hat{G}} \hat{f}(\chi) \chi(g) d\mu(\chi). \quad (2.6)$$

In particular, if one can compute  $\int_{\hat{G}} \hat{f}(\chi) \chi(g) d\mu(\chi)$  for even a *single* function  $f$  and a *single*  $g \in G$ , the previous equation uniquely determines  $\alpha$  (provided that  $f(g) \neq 0$ ) and hence  $\mu_{\hat{G}}$ .

**Example 2.2.13** (Recovering the finite case). *Let  $G$  be a finite abelian group. We endow  $G$  with the counting measure, which is a Haar measure since it is obviously invariant under translation by an element of  $G$ . Notice that with this choice of Haar measure on  $G$  the Fourier transform coincides with that of Definition 1.5.15.*

*What is the measure  $\mu_{\hat{G}}$  appearing in Theorem 2.2.10? Following Remark 2.2.12, we take  $f = \mathbf{1}_e$ , the characteristic function of the singleton  $\{e\}$ , where  $e$  is the identity of  $G$ . The Fourier transform is*

$$\hat{f}(\chi) = \int_G f(g) \overline{\chi(g)} d\mu_G = \sum_{g \in G} \delta_{g,e} \overline{\chi(g)} = \overline{\chi(e)} = 1,$$

*that is, the constant function 1. The dual measure  $\mu_{\hat{G}}$  is some multiple  $\alpha$  of the counting measure on  $\hat{G}$ . With reference to Equation (2.6), we take  $\mu$  to be the counting measure on  $\hat{G}$ ,  $f = \mathbf{1}_e$  and  $g = e$ . With these choices we obtain*

$$1 = f(e) = \alpha \sum_{\chi \in \hat{G}} \hat{f}(\chi) \chi(e) = \alpha \sum_{\chi \in \hat{G}} 1 = \alpha \cdot |\hat{G}|,$$

*which yields  $\alpha = \frac{1}{|\hat{G}|}$ . Thus,  $\mu_{\hat{G}}$  is  $\frac{1}{|\hat{G}|}$  times the counting measure, and we recover Theorem 1.5.17.*

## 2.3 Review of local fields

In this section, we give a quick review of the basics of the theory of completions of number fields. The standard reference on the general theory of local fields is Serre's classical book [Ser79].

**Definition 2.3.1** (Norm on a number field, place). Let  $K$  be a number field. A (multiplicative) **norm** on  $K$  is a function

$$\begin{aligned} d: K &\rightarrow \mathbb{R}_{\geq 0} \\ x &\rightarrow |x| \end{aligned}$$

that satisfies the following:

1.  $|xy| = |x| \cdot |y|$ ;
2.  $|x + y| \leq |x| + |y|$ ;
3.  $|x| = 0$  if and only if  $x = 0$ .

The norm is called **non-archimedean** if it further satisfies  $|x + y| \leq \max\{|x|, |y|\}$ . Every norm induces a distance, hence a topology, on  $K$ . Two norms  $|\cdot|_1, |\cdot|_2$  on a number field are called **equivalent** if they induce the same topology on  $K$ . An equivalence class of norms is called a **place** of  $K$ .

**Remark 2.3.2.** Note that equivalent norms induce *the same* topology, so to each place we can attach a topology on  $K$ .

The classification of places of a number field is known as Ostrowski's theorem. Before stating it, we describe a way to obtain a norm on a number field starting from a prime of its ring of integers.

**Definition 2.3.3** ( $\mathfrak{p}$ -adic norm). Let  $K$  be a number field and let  $\mathfrak{p}$  be a prime ideal of the ring of integers  $\mathcal{O}_K$ . Let  $q$  be the size of the residue class field  $\mathbb{F}_{\mathfrak{p}} := \mathcal{O}_K/\mathfrak{p}$ .

1. A **uniformiser** at  $\mathfrak{p}$  is an element  $\pi \in \mathcal{O}_K$  such that the factorisation of  $(\pi)$  is of the form  $\mathfrak{p}I$ , with  $(\mathfrak{p}, I) = (1)$ . Equivalently, it is an element in  $\mathfrak{p} \setminus \mathfrak{p}^2$  (the equivalence, and the fact that  $\mathfrak{p} \setminus \mathfrak{p}^2$  is non-empty, follows from unique factorisation in ideals, Theorem 1.3.3).
2. The  $\mathfrak{p}$ -adic valuation  $v_{\mathfrak{p}}$  on  $K$  is the function

$$\begin{aligned} v_{\mathfrak{p}}: K^{\times} &\rightarrow \mathbb{Z} \\ x &\mapsto v_{\mathfrak{p}}(x) \end{aligned}$$

defined as follows. Given  $x \in K^{\times}$ , there exists a unique integer  $n$  such that  $x/\pi^n$  is in  $\mathcal{O}_K^{\times}$ : we set  $n = v_{\mathfrak{p}}(x)$ . We further set, conventionally,  $v_{\mathfrak{p}}(0) = \infty$ .

3. The  $\mathfrak{p}$ -adic norm on  $K$  is then obtained by setting

$$\|x\|_{\mathfrak{p}} := q^{-v_{\mathfrak{p}}(x)}.$$

**Theorem 2.3.4** (Ostrowski). *Let  $K$  be a number field. Denote by  $\sigma_1, \dots, \sigma_{n_1}, \tau_1, \overline{\tau_1}, \dots, \tau_{n_2}, \overline{\tau_{n_2}}$  the embeddings of  $K$  in  $\mathbb{C}$ , as in Section 1.3.6 (in particular, the image of each  $\sigma_i$  is contained in  $\mathbb{R}$ , while the image of each  $\tau_i$  is not). The following is a complete list of non-equivalent norms on  $K$  (that is, a complete list of places of  $K$ ):*

1.  $\|x\|_{\sigma_i} := |\sigma_i(x)|$ , for  $i = 1, \dots, n_1$ , where  $|\cdot|$  is the standard norm on  $\mathbb{R}$ ; the corresponding places are called **real**;
2.  $\|x\|_{\sigma_j} := |\sigma_j(x)|^2$ , for  $j = 1, \dots, n_2$ , where  $|\cdot|$  is the standard Euclidean norm on  $\mathbb{C}$ ; the corresponding places are called **complex**;
3.  $\|x\|_{\mathfrak{p}}$  for each non-zero prime ideal  $\mathfrak{p}$  of the ring of integers  $\mathcal{O}_K$ ; the corresponding places are called **finite**, and are precisely the non-archimedean ones.

Each place is an *equivalence class* of norms. For each place, we will consistently take as representative given in Ostrowski's theorem, with the normalisation of Definition 2.3.3. (We chose a normalisation when we set  $\|\pi\|_{\mathfrak{p}} = q^{-1}$ . One can replace  $q$  with any other real number greater than 1 and obtain an equivalent norm, but our choice has several technical advantages.)

**Example 2.3.5** (Places of  $\mathbb{Q}$ ). *The places  $\Omega_{\mathbb{Q}}$  of  $\mathbb{Q}$  are in bijection with  $\{p : p \text{ prime}\} \cup \{\infty\}$ , with  $\infty$  conventionally representing the place coming from the obvious embedding  $\mathbb{Q} \hookrightarrow \mathbb{R}$ . For every non-zero rational number  $x = \frac{a}{b}$  and every prime  $p$ , write  $x = p^n \frac{a'_p}{b'_p}$ , where  $n$  is a (positive or negative) integer and  $(a'_p, p) = (b'_p, p) = 1$ . The different norms are then given by*

$$\|x\|_p = p^{-n}, \quad \|x\|_{\infty} = |x|.$$

One further piece of notation:

**Definition 2.3.6.** We will write  $\Omega_K$  for the set of all places of  $K$  and  $\Omega_K^{\infty}$  for the subset of 'infinite places', that is, the archimedean ones. As already mentioned in Theorem 2.3.4, a place is called 'finite' if it is non-archimedean, that is, it lies in  $\Omega_K \setminus \Omega_K^{\infty}$ .

We will usually denote a place by  $v$ , or, if it comes from a prime  $\mathfrak{p}$  of  $\mathcal{O}_K$ , simply by  $\mathfrak{p}$ . By a slight abuse of notation, we will write  $\|x\|_v$  for the norm of  $x \in K$ , as measured by our standard norm which represents the place  $v$ . When  $v$  is a finite place, corresponding to the prime ideal  $\mathfrak{p}$  of  $\mathcal{O}_K$ , we denote by  $q_v$  the size of the residue field  $\mathcal{O}_K/\mathfrak{p}$  and by  $p_v$  its characteristic.

**Exercise 2.3.7** (Product formula for  $K = \mathbb{Q}$ ). Check that  $\prod_{v \in \Omega_{\mathbb{Q}}} \|x\|_v = 1$  for every  $x \in \mathbb{Q}^{\times}$ .

The previous exercise is no coincidence:

**Theorem 2.3.8** (General product formula). *Let  $K$  be a number field. The equality*

$$\prod_{v \in \Omega_K} \|x\|_v = 1$$

*holds for every  $x \in K^{\times}$ .*

Possibly the most important use of place is to define the completions of a number field:

**Definition 2.3.9** (Completion of a number field). Let  $K$  be a number field and let  $v$  be a place of  $K$ . We denote by  $K_v$  the completion of  $K$  with respect to the topology induced by  $v$ . It is a topological field, that is, the operations  $+$  :  $K \times K \rightarrow K$ ,  $\cdot$  :  $K \times K \rightarrow K$  and  $^{-1}$  :  $K^\times \rightarrow K^\times$  are continuous. We will usually refer to  $K_v$  as the **completion of  $K$  at  $v$** .

**Remark 2.3.10.** Let  $\|\cdot\|$  be a norm corresponding to  $v$ . By general facts in topology,  $\|\cdot\|$  extends to a norm on  $K_v$  (which we still denote by the same symbol) and makes  $K_v$  into a complete metric space.

**Exercise 2.3.11.** Let  $K$  be a (number) field and let  $\|\cdot\|$  be a norm on  $K$ .

1. Prove that the subspace topology on  $K^\times$  coincides with the subspace topology induced on  $K^\times$  by the topology of  $K \times K$ , where  $K^\times$  is embedded in  $K \times K$  via  $x \mapsto (x, x^{-1})$ .
2. Prove that  $x \mapsto x^{-1}$  is continuous.

**Exercise 2.3.12.** Let  $R$  be the ring  $\mathbb{Q}$  equipped with the topology for which a basis of open neighbourhoods of  $q \in \mathbb{Q}$  is given by  $\{q + m\mathbb{Z}\}_{m \in \mathbb{Z}_{>0}}$ . Prove that  $R$  is a topological ring (that is, the operations  $+$ ,  $-$  and  $\cdot$  are continuous), but  $^{-1}$  :  $R^\times \rightarrow R^\times$  is not continuous for the subspace topology.

Completions of number fields can be described fairly explicitly:

1. when  $v$  is a real place, the completion is isomorphic to  $\mathbb{R}$ ;
2. when  $v$  is a complex place, the completion is isomorphic to  $\mathbb{C}$ ;
3. when  $v$  is a finite place of characteristic  $p$ , the completion is a finite extension of the field  $\mathbb{Q}_p$ , the completion of  $\mathbb{Q}$  with respect to the  $p$ -adic metric. Such fields are called  **$p$ -adic fields**.

In general, the completion of a number field at a (finite or infinite) place is called a **local field**. (There is a more general definition of local fields, but we will not need it here.)

The field  $\mathbb{Q}_p$  of  $p$ -adic numbers, and more generally its finite extensions, have been extensively studied, and a lot is known about their structure. Here, we will limit ourselves to mentioning some of their fundamental properties, starting with the fact that, for every finite extension  $L$  of  $\mathbb{Q}_p$ , there exists a number field  $K$  and a place  $v$  of  $K$  of characteristic  $p$  such that  $L$  is isomorphic to  $K_v$  as a topological field.

**Theorem 2.3.13.** *Let  $L$  be a finite extension of  $\mathbb{Q}_p$  (equivalently: let  $L$  be the completion of some number field  $K$  at a place  $v$  of characteristic  $p$ ). Let  $\|\cdot\|$  be the norm on  $L$  (see Remark 2.3.10 in case  $L$  is obtained as the completion of a number field). The following hold:*

1.  $\mathcal{O}_L = \{x \in L : \|x\| \leq 1\}$  is a subring of  $L$ , called the **ring of integers**;
2.  $\mathcal{O}_L^\times = \{x \in L : \|x\| = 1\}$  is its group of units;
3.  $\mathcal{O}_L$  is a local ring; its maximal ideal  $\mathfrak{m}$  is principal, and any generator of  $\mathfrak{m}$  is called a **uniformiser**  $\pi$  of  $L$ ;
4. every ideal of  $\mathcal{O}_L$  is a power of  $\mathfrak{m}$ ; in particular, every element  $x$  of  $L^\times$  can be written as  $x = u \cdot \pi^n$  for some  $n \in \mathbb{Z}$  and  $u \in \mathcal{O}_L^\times$ ; the integer  $n$  is called the **valuation** of  $x$ ;

5. the quotient  $\kappa_L := \mathcal{O}_L/\mathfrak{m}$  is a finite field, of cardinality  $p^f$ ; the integer  $f$  is called the **inertia degree** of  $L$  over  $\mathbb{Q}_p$ ;
6. the ideal  $(p)\mathcal{O}_L$  is of the form  $(\pi^e)$ ; the integer  $e$  is called the **ramification index** of  $L$  over  $\mathbb{Q}_p$ ;
7. let  $L$  be obtained as the completion of a number field  $K$  at a finite place  $\mathfrak{p}$ . Write  $(p)\mathcal{O}_K = \mathfrak{p}^e I$ , with  $(\mathfrak{p}, I) = (1)$ . The ramification index and inertia degree of  $L$  over  $\mathbb{Q}_p$  coincide with the ramification index and inertia degree of  $\mathfrak{p}$  over  $p$ .

We also mention the fact that, once the completions of  $\mathbb{Q}$  have been constructed, the completions of an arbitrary number field can also be described in the following, more algebraic terms.

**Theorem 2.3.14** (Completions and tensor products). *Let  $K$  be a number field of signature  $(n_1, n_2)$ , and let  $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$  be the factorisation in  $\mathcal{O}_K$  of the ideal  $(p)$ , where  $p$  is a prime of  $\mathbb{Z}$ .*

1. The tensor product  $K \otimes_{\mathbb{Q}} \mathbb{R}$  is isomorphic (as a topological ring) to the product  $\mathbb{R}^{n_1} \times \mathbb{C}^{n_2}$ .
2. The tensor product  $K \otimes_{\mathbb{Q}} \mathbb{Q}_p$  is isomorphic (as a topological ring) to the product  $\prod_{i=1}^r K_{\mathfrak{p}_i}$ . The field  $K_{\mathfrak{p}_i}$  is a finite extension of  $\mathbb{Q}_p$  of degree  $e_i f_i$ , where  $e_i := e(\mathfrak{p}_i | p)$  and  $f_i := f(\mathfrak{p}_i | p)$ . Moreover, the ramification index and inertia degree of  $K_{\mathfrak{p}_i}$  over  $\mathbb{Q}_p$  are given by  $e_i$  and  $f_i$ , respectively.

We will also make use of some fundamental topological properties of the completions  $K_v$ . The most important one is of course their completeness, which is true by construction. Another fact (well-known in the real and complex case, and easy to prove in the  $p$ -adic setting) which we will need is the following:

**Proposition 2.3.15.** *Let  $K_v$  be a completion of a number field and let  $X$  be a subset of  $K_v$ . The topological closure  $\overline{X}$  of  $X$  in  $K_v$  is compact if and only if  $X$  is bounded with respect to the norm on  $K_v$ . In particular,  $K_v$  is locally compact, and so is  $K_v^\times$ .*

**Exercise 2.3.16.** Prove Proposition 2.3.15.

In the next chapter we will need the notion of **different** of an extension of  $p$ -adic fields (in particular when the ground field is  $\mathbb{Q}_p$  itself).

**Definition 2.3.17** (Different). Let  $L/K/\mathbb{Q}_p$  be finite extensions of  $p$ -adic fields. The **different** of  $L$  over  $K$  is the fractional ideal of  $L$  given by

$$\mathfrak{d}_{L/K}^{-1} = \{x \in L : \text{tr}_{L/K}(xy) \in \mathcal{O}_K \ \forall y \in \mathcal{O}_L\}.$$

The **absolute different** of  $L$ , denoted simply by  $\mathfrak{d}_L$ , is the different of the extension  $L/\mathbb{Q}_p$ .

**Remark 2.3.18.** Notice that  $\mathfrak{d}_{L/K}^{-1}$  contains the ring of integers  $\mathcal{O}_L$ ; it follows that its inverse  $\mathfrak{d}_{L/K}$  is contained in  $\mathcal{O}_L$  and is therefore an integral ideal.

It is not hard to show the following result:

**Theorem 2.3.19.** *Let  $L/K$  be a finite extension of  $p$ -adic fields. Define the (**relative**) **discriminant** of  $L$  over  $K$  like in the number field case, that is,*

$$d_{L/K} = \left( \det (\sigma_i(\alpha_j))^2 \right),$$

where the  $\sigma_i$ , for  $i = 1, \dots, [L : K]$  are the embeddings of  $L$  into  $\overline{K}$  that fix  $K$ , and the  $\alpha_j$ , for  $j = 1, \dots, [L : K]$ , are a basis of  $\mathcal{O}_L$  over  $\mathcal{O}_K$ . Notice however that  $d_{L/K}$  is only an integral ideal of  $\mathcal{O}_K$  and not an actual number.

The (absolute value of the) discriminant  $|d_{L/K}|$  is equal to  $N_{L/K}(\mathfrak{d}_{L/K})$ , the norm from  $L$  to  $K$  of the different of  $L$  over  $K$ .

Using Theorem 2.3.14, the study of extensions of number fields can be reduced to a large extent to the local case. For example, one has the following:

**Theorem 2.3.20.** *Let  $K$  be a number field. For every prime  $p$  we have  $K \otimes \mathbb{Q}_p = \prod_{\mathfrak{p}|p} K_{\mathfrak{p}}$ , where  $\mathfrak{p}$  ranges over the primes of  $\mathcal{O}_K$  of characteristic  $p$ . We have*

$$|d_K| = \prod_p \prod_{\mathfrak{p}|p} N(d_{K_{\mathfrak{p}}/\mathbb{Q}_p}) :$$

the global discriminant is the product of all the local ones.

**Remark 2.3.21.** Note that the equality in the previous theorem should be interpreted purely as an equality of ideals, not of numbers.

Since the different and the discriminant can be defined in terms of traces, Theorem 2.3.20 is related to the following statement (see e.g. [Neu99, Proposition II.8.2 and Corollary II.8.3] for a proof):

**Theorem 2.3.22.** *Let  $K$  be a number field and  $p$  be a prime number. Write  $K \otimes \mathbb{Q}_p$  as the direct product  $\prod_{\mathfrak{p}|p} K_{\mathfrak{p}}$ , where  $\mathfrak{p}$  ranges over the primes of  $\mathcal{O}_K$  of characteristic  $p$ . We have*

$$\mathrm{tr}_{K \otimes \mathbb{Q}}(x) = \sum_{\mathfrak{p}|p} \mathrm{tr}_{K_{\mathfrak{p}}/\mathbb{Q}_p}(x)$$

for all  $x \in K$ . Similarly, for  $p = \infty$  write  $K \otimes \mathbb{R}$  as the direct product  $\prod_{v \text{ infinite place}} K_v$ , where  $v$  ranges over the infinite places of  $K$ . We have

$$\mathrm{tr}_{K \otimes \mathbb{R}}(x) = \sum_{v \text{ infinite place}} \mathrm{tr}_{K_v/\mathbb{R}}(x).$$

**Exercise 2.3.23.** Prove the case  $p = \infty$  of Theorem 2.3.22.

*Hint.* Using properties of the trace, reduce to the Galois case. Treat this case explicitly.

## 2.4 Restricted direct products

We discuss the notion of **restricted direct product** from several points of view: abstract group theory, topology, measure theory, Pontryagin duality, and Fourier analysis. In this section, given a set of indices  $I$ , we say that a property holds for *almost all*  $i \in I$  if it holds for all but finitely many  $i$ .

### 2.4.1 Abstract group theory

We start by introducing a general definition of **restricted product**:

**Definition 2.4.1** (Restricted product of groups). Let  $(G_i)_{i \in I}$  be a collection of groups and let  $(H_i)_{i \in I}$  be a collection of subgroups, with  $H_i < G_i$  for each  $i$ . The **restricted product of the groups  $G_i$  with respect to the subgroups  $H_i$**  is the subset of  $\prod_{i \in I} G_i$  given by

$$\{(x_i) \in \prod_i G_i : \text{there exists a finite subset } S \subseteq I : x_i \in H_i \text{ for all } i \notin S\}.$$

Note that the subset  $S$  in the previous definition can depend on  $(x_i)_{i \in I}$ . The restricted product is often denoted by  $\prod'_{i \in I} (G_i, H_i)$ ,  $\prod_{i \in I} (G_i, H_i)$ , or simply  $\prod'_{i \in I} G_i$  if the  $H_i$  are clear from the context.

**Remark 2.4.2.** Note that the definition makes sense even if, for  $i$  in some finite subset  $S_0$  of indices, the group  $H_i$  is not defined: indeed, we may always take  $S$  (as in the definition above) to contain  $S_0$ , and therefore, we don't need to know anything about the groups  $H_i$  for  $i \in S_0$ .

**Exercise 2.4.3.** Check that the restricted product  $\prod' (G_i, H_i)$  is a subgroup of  $\prod G_i$ .

There is also an obvious variant of this definition where the  $G_i$  are replaced by rings  $R_i$  and the  $H_i$  by subrings:

**Definition 2.4.4** (Restricted product of rings). Let  $(R_i)_{i \in I}$  be a collection of rings and let  $(T_i)_{i \in I}$  be a collection of subrings, with  $T_i \subseteq R_i$  for every  $i$ . The **restricted product of the rings  $R_i$  with respect to the subrings  $T_i$**  is the subset of  $\prod_{i \in I} R_i$  given by

$$\{(x_i) \in \prod_i R_i : \text{there exists a finite subset } S \subseteq I : x_i \in T_i \text{ for all } i \notin S\}.$$

For our applications, by far the most interesting examples of restricted products will be the group of idèles and the ring of adèles. We now introduce these objects, which we will then study in more detail in the next subsections.

Let now  $k$  be a number field and let  $\Omega_k$  be the collection of its places. For each  $v \in \Omega_k$ , we can consider:

1. the completion  $k_v$  and its non-zero elements  $k_v^\times$ ;
2. the “integers”  $\mathcal{O}_v$ , which are defined in the usual way if  $v$  is a finite place, and as  $\mathcal{O}_v := k_v$  if  $v$  is an archimedean place;
3. the “units”  $\mathfrak{u}_v$ , which are defined in all cases as  $\mathcal{O}_v^\times$ .

Both the *ring* of adèles and the *group* of idèles are suitable restricted products:

**Definition 2.4.5** (Adèles and idèles). We call

$$\mathbb{A}_k := \prod' (k_v, \mathcal{O}_v)$$

the **ring of adèles** of  $k$ , and

$$I_k := \prod' (k_v^\times, \mathcal{O}_v^\times)$$

the **group of idèles** of  $k$ .

The following exercise is essential:

**Exercise 2.4.6.** The group of units of  $\mathbb{A}_k$  (as a ring) is  $I_k$ .

## 2.4.2 Topological groups

The definitions of the last section already cover the basic algebraic properties of adèles and idèles. However, matters become more complicated (and interesting) when we want to equip  $\mathbb{A}_K$  and  $I_K$  with a topology. To this end, we give yet another definition of restricted product, this time in a topological setting.

**Definition 2.4.7** (Restricted product of locally compact abelian groups). Let  $I$  be a set of indices and let  $\{G_i\}_{i \in I}$  be a collection of locally compact abelian groups. Suppose that, for almost all  $i \in I$  (meaning ‘for all but a finite number of elements of  $I$ ’), we are also given a subgroup  $H_i \subset G_i$  which is open and compact. We define the topological group  $G := \prod'_i (G_i, H_i)$  as follows:

- as a group, it is the restricted product of Definition 2.4.1 (with the interpretation of Remark 2.4.2);
- a fundamental system of neighbourhoods of 1 in  $G$  is given by the sets  $\prod_{i \in I} N_i$ , where each  $N_i$  is a neighbourhood of 1 in  $G_i$  for all  $i$  and  $N_i = H_i$  for almost all  $i$ .

**Remark 2.4.8.** 1. Naturally, we can and will identify each  $G_{i_0}$  to a subgroup of the restricted product (specifically, the subgroup of elements  $x = (x_i)$  for which  $x_i = 1$  for all  $i \neq i_0$ ). The natural map is an isomorphism of topological groups.

2. Let  $S$  be a finite set of indices, including those for which  $H_i$  is not defined. The set  $G_S := \{x = (x_i) \in G : x_i \in H_i \ \forall i \notin S\}$  is a subgroup of  $G$ , and is an open neighbourhood of 1.
3. Let  $G_S$  be as above. Then,  $G_S \cong \prod_{i \in S} G_i \times \prod_{i \notin S} H_i$  is a direct product of locally compact groups, almost all of which are compact. It follows that  $G_S$  is locally compact, hence (since  $G_S$  is a neighbourhood of 1 in  $G$ ) that  $G$  is also locally compact.
4. By definition,  $G = \bigcup_{\substack{S \subseteq I \\ S \text{ finite}}} G_S$ .

The groups  $G_S$ , being direct products, are already easier to analyse than the restricted product  $G$ . An even simpler class of subgroups is given in the next definition:

**Definition 2.4.9.** Notation as in Definition 2.4.7. Let  $S$  be a finite subset of  $I$ . We denote by  $G^S \subset G_S$  the subgroup of those elements  $x = (x_i) \in G$  such that  $x_i = 1$  for  $i \in S$  and  $x_i \in H_i$  for  $i \notin S$ .

A useful property of the topology on a restricted direct product is given in the following lemma:

**Lemma 2.4.10.** *Notation as in Definition 2.4.7. A subset  $C \subseteq G$  is relatively compact (that is, has compact closure) if and only if it is contained in a product  $\prod_{i \in I} B_i$  where each  $B_i$  is a compact subset of the corresponding  $G_i$  and  $B_i = H_i$  for almost all  $i$  (recall that the  $H_i$  are compact by definition). Moreover, every compact subset of  $G$  is contained in some  $G_S$ .*



*Proof.* Let  $K$  be a compact subset of  $G$ : we claim that there exists  $S$  such that  $K \subseteq G_S$ . To see this, recall that we have already observed that the groups  $G_S$  cover  $G$ , so  $K \subseteq_S \bigcup G_S$ , and by compactness we have  $K \subseteq G_{S_1} \cup \cdots \cup G_{S_r}$  (recall that the  $G_{S_i}$  are open). Notice furthermore that  $G_{S_1} \cup \cdots \cup G_{S_r} \subseteq G_{S_1 \cup \cdots \cup S_r}$ , so – setting  $S = \bigcup S_i$  – we have that  $K$  is a subset of  $G_S = \prod_{i \in S} G_i \times \prod_{i \notin S} H_i$ . (This shows the last statement in the lemma.) Finally, let  $K_i := \pi_i(K)$  for  $i \in S$ : then  $K_i$  is compact (continuous image of a compact set), and by construction we have  $K \subseteq \prod_{i \in S} K_i \times \prod_{i \notin S} H_i$ , as desired.

Conversely, Tychonoff's theorem implies the compactness of any product  $\prod_i B_i$  (where each  $B_i$  is compact and  $B_i = H_i$  for almost all  $i$ ); any such set is contained in some  $G_S$ , hence it is a compact subset of  $G$ . Hence, if  $K$  is contained in  $\prod_i B_i$  with the  $B_i$  as above, its closure is contained in a compact set and is therefore compact.  $\square$

### 2.4.3 (Quasi-)Characters of a restricted product

Let  $G = \prod'(G_i, H_i)$  be a restricted direct product in the sense of Definition 2.4.7. We now wish to study the quasi-characters of  $G$ , that is, the continuous homomorphisms from  $G$  to  $\mathbb{C}^\times$ . Given a  $c : G \rightarrow \mathbb{C}^\times$ , we denote by  $c_i$  its restriction to  $G_i$ , that is,

$$\begin{aligned} c_i : G_i &\rightarrow \mathbb{C}^\times \\ x_i &\mapsto c((1, 1, \dots, 1, x_i, 1, \dots)). \end{aligned}$$

It is clear that  $c_i$  is a homomorphism  $G_i \rightarrow \mathbb{C}^\times$ . The next two lemmas show how to factor any continuous  $c : G \rightarrow \mathbb{C}^\times$  as a product of  $c_i$ .

**Lemma 2.4.11.** *The homomorphism  $c_i$  is trivial on  $H_i$  for almost all  $i$ , and for every  $x \in G$  we have*

$$c(x) = \prod_{i \in I} c_i(x_i),$$

where almost all of the factors of the product are equal to 1.

*Proof.* Let  $U$  be a neighbourhood of 1 in the complex plane that contains no multiplicative subgroup (Exercise 3.1.18). Let  $N = \prod_i N_i$  be a neighbourhood of the identity in  $G$  such that  $c(N) \subseteq U$ . By Definition 2.4.7, we may assume that  $N_i = H_i$  for almost all  $i$ . If we let  $S$  be a finite set containing all the indices  $i$  for which  $N_i \neq H_i$ , then  $N$  contains  $G^S$ , and therefore  $c(G^S) \subseteq U$  is a subgroup of  $U$ , hence is trivial. It follows that  $c(N_i) = c(H_i) = \{1\}$  for  $i \notin S$ . Now, for a given  $x \in G$ , enlarging  $S$  if necessary we can assume  $x \in G_S$ . Identify  $x_i \in G_i$  (the  $i$ -th component of  $x$ ) to the element of  $G$  that coincides with  $x$  in position  $i$  and is 1 elsewhere, and denote by  $x^S \in G^S$  the element such that  $x = \prod_{i \in S} x_i \cdot x^S$ . We already know that  $c(G^S) \subseteq c(N) = \{1\}$ , hence

$$c(x) = \prod_{i \in S} c(x_i) \cdot c(x^S) = \prod_{i \in S} c_i(x_i) = \prod_i c_i(x_i)$$

as desired (the last equality holds since  $c_i(x_i) = 1$  for  $i \notin S$ ).  $\square$

Conversely, starting from a collection of  $c_i$  that are almost all trivial on the corresponding  $H_i$  we obtain a global homomorphism  $c$ :

**Lemma 2.4.12.** *For each  $i \in I$  fix a continuous homomorphism  $c_i : G_i \rightarrow \mathbb{C}^\times$ . Suppose that  $c_i$  is trivial on  $H_i$  for all but finitely many  $i$ . The map*

$$c(x) = \prod_i c_i(x_i)$$

*is a well-defined continuous homomorphism  $G \rightarrow \mathbb{C}^\times$ .*

*Proof.* It is clear that  $c$  is well-defined (almost all factors in the product are equal to 1) and multiplicative (it is by restriction to any  $G_S$ ). To prove continuity, let  $U$  be an open neighbourhood of 1 in the complex plane and choose a finite set  $S$  containing all the  $i$  for which  $c_i(H_i) \neq \{1\}$ . Let furthermore  $V$  be a neighbourhood of 1 in  $\mathbb{C}$  such that  $V^{\#S} \subseteq U$ . For each  $i \in I$ , define

$$N_i = \begin{cases} \text{an open neighbourhood of the identity in } G_i \text{ such that } c(N_i) \subseteq V, & \text{if } i \in S \\ H_i, & \text{if } i \notin S \end{cases}$$

Letting  $N = \prod_i N_i$ , we have

$$c(N) \subseteq \prod_i c_i(N_i) \subseteq V^{\#S} \subseteq U.$$

To check continuity in general, consider now an arbitrary open subset  $V$  of  $\mathbb{C}^\times$ . Either  $c^{-1}(V)$  is empty, in which case we are done, or it is not. If it is not, let  $g$  be a point in  $c^{-1}(V)$ . By definition of the topology on  $\mathbb{C}^\times$ , the open set  $V$  contains an open neighbourhood of  $c(g)$  of the form  $c(g)U_g$ , where  $U_g$  is an open neighbourhood of 1 in  $\mathbb{C}^\times$ . By what we already showed, there is an open neighbourhood  $N_g$  of 1 in  $G$  such that  $c(N_g) \subseteq U_g$ . It follows that  $c^{-1}(V)$  contains  $gN_g$ , which is an open neighbourhood of  $g$ . Since this holds for every  $g$ , the set  $c^{-1}(V)$  is open and  $c$  is continuous.  $\square$

We summarise the above discussion as follows:

**Proposition 2.4.13.** *The quasi-characters  $c$  of  $G$  are in bijection with the collections  $(c_i)_{i \in I}$ , where each  $c_i$  is a quasi-character of  $G_i$  and  $c_i|_{H_i}$  is trivial for almost all  $i$ .*

The same arguments apply verbatim to characters, and show that the characters of  $G$  are of the form  $\prod_i c_i$ , where each  $c_i$  is a character (and not just a quasi-character) of  $G_i$  and almost all  $c_i$  are trivial on  $H_i$ . This already suggests that the dual group of  $G$  is itself a restricted product. We now make this precise.

For each  $i$  where  $H_i$  is defined, let  $H_i^\perp \subseteq \widehat{G}_i$  be the subgroup

$$H_i^\perp = \{c_i \in \widehat{G}_i \mid c_i(H_i) = \{1\}\}.$$

By Theorem 2.2.2 and Proposition 2.2.4, the fact that  $H_i$  is compact implies that its dual  $\widehat{H}_i \cong \widehat{G}_i / H_i^\perp$  is discrete, and hence  $H_i^\perp$  is open in  $\widehat{G}_i$ . Similarly, the fact that  $H_i$  is open implies that  $G_i/H_i$  is discrete, and hence  $\widehat{G}_i/H_i \cong H_i^\perp$  is compact. Thus, the subgroups  $H_i^\perp$  have all the necessary characteristics to form a restricted product, and we have:

**Theorem 2.4.14** (Dual group of a topological restricted product). *The dual group of  $\prod_i'(G_i, H_i)$  is  $\prod_i'(\widehat{G}_i, H_i^\perp)$ .*

*Proof.* Restricting the bijection of Proposition 2.4.13 to characters yields an isomorphism  $\varphi$  of abstract groups  $\prod'_i(\widehat{G}_i, H_i^\perp) \cong \widehat{G}$ , sending  $(c_i)_{i \in I}$  to  $\prod_{i \in I} c_i$ . We check that this isomorphism is also a homeomorphism.

Fix a basis element for the topology  $\widehat{G}$ , say  $U(K, V)$ , where  $K$  is a compact neighbourhood of the identity in  $G$  and  $V$  is an open neighbourhood of 1 in  $\mathbb{S}^1$ . Restricting  $V$  if necessary, we assume that  $V$  contains no non-trivial subgroup of  $\mathbb{C}^\times$ .

We want to find a neighbourhood  $\prod_i N_i$  of 1 in  $\prod'_i(\widehat{G}_i, H_i^\perp)$  such that  $(c_i)_{i \in I} \in \prod'_i(\widehat{G}_i, H_i^\perp)$  implies  $\prod_i c_i \in U(K, V)$ . Now, since  $K$  is compact, by Lemma 2.4.10 it is contained in a product of the form  $\prod_{i \in I} B_i$ , where each  $B_i$  is compact and  $B_i = H_i$  for almost all  $i$ . Let  $S$  be the (finite) set of indices for which  $B_i \neq H_i$ . Choose furthermore  $V'$  to be an open neighbourhood of 1 in  $\mathbb{S}^1$  that satisfies  $(V')^{\#S} \subseteq V$ . Setting

$$N_i = \begin{cases} U(B_i, V') & \text{if } i \in S \\ H_i^\perp & \text{if } i \notin S \end{cases}$$

we obtain that  $\prod N_i$  is a neighbourhood of 1 in  $\prod'_i(\widehat{G}_i, H_i^\perp)$  and  $\varphi(\prod_i N_i) \subseteq U(K, V)$ . Indeed, if  $(c_i)_{i \in I}$  is in  $\prod_i N_i$  we have

$$\left(\prod_i c_i\right)(K) \subseteq \left(\prod_i c_i\right)\left(\prod_i B_i\right) = \prod_{i \in S} c_i(B_i) \subseteq (V')^{\#S} \subseteq V,$$

that is,  $\varphi((c_i)_{i \in I}) \in U(K, V)$ . This shows continuity of  $\varphi$ .

Continuity of  $\varphi^{-1} : \widehat{G} \rightarrow \prod'_i(\widehat{G}_i, H_i^\perp)$  is similar. Let  $\prod_i N_i$  be an open neighbourhood of 1 in  $\prod'_i(\widehat{G}_i, H_i^\perp)$ , where all but finitely many of the  $N_i$  coincide with  $H_i^\perp$ . Write  $S$  for the finite set of indices for which  $N_i \neq H_i^\perp$ . Restricting the neighbourhood (which we can certainly do), we may and do assume that, for  $i \in S$ , we have  $N_i = U(K_i, V_i)$  for certain compact neighbourhoods  $K_i$  of the identity in  $G_i$  and neighbourhoods  $V_i$  of 1 in  $\mathbb{S}^1$ . Let  $V = \bigcap_{i \in S} V_i$ . Shrinking  $V$  if necessary, we can assume that  $V$  contains no non-trivial subgroups of  $\mathbb{S}^1$ . Set  $K_i = H_i$  for  $i \notin S$  and consider the open subset  $U(\prod K_i, V)$  of  $\widehat{G}$ .

Since  $(\varphi^{-1})^{-1} = \varphi$  simply sends  $c$  to the collection  $(c_i)_{i \in I}$  of the restrictions of  $c$  to each factor  $G_i$ , for  $c \in U(\prod K_i, V)$  we have  $\varphi^{-1}(c)_i \in N_i$  for every  $i$ . Indeed:

- if  $i \notin S$ , then  $c_i(K_i) = c_i(H_i) \subseteq V$  implies  $c_i(H_i) = \{1\}$ , hence  $c_i \in H_i^\perp = N_i$ .
- if  $i \in S$ , then  $c_i(K_i) \subseteq V \subseteq V_i$  implies  $c_i \in N_i$  by definition.

□

### 2.4.4 Measure theory

Consider again a collection of locally compact topological groups  $G_i$ , and fix (for almost all  $i$ ) an open, compact subgroup  $H_i$  of  $G_i$ . Fix furthermore a Haar measure  $dg_i$  on each  $G_i$  and suppose that  $\int_{H_i} dg_i = 1$  for almost all  $i$ . Notice that we require  $dg_i$  to be defined for *all* indices  $i$ ; it's only the condition  $\int_{H_i} dg_i = 1$  that is allowed to fail (for finitely many indices).

We now define a Haar measure  $dg$  on  $G = \prod'_i(G_i, H_i)$  which is morally the product of the measures  $dg_i$ . To do this, fix any finite subset  $S$  of the indices (containing those for which  $H_i$  is

not defined) and write  $G_S = (\prod_{i \in S} G_i) \times G^S$ . Notice that  $G^S \cong \prod_{i \notin S} H_i$  is compact. It carries a unique Haar measure  $dg^S$  normalised in such a way that

$$\int_{G^S} dg^S = \prod_{i \notin S} \left( \int_{H_i} dg_i \right). \quad (2.7)$$

The product measure  $dg_S = (\prod_{i \in S} dg_i) \times dg^S$  is therefore well-defined on  $G_S = (\prod_{i \in S} G_i) \times G^S$ . Furthermore, it is a Haar measure (one can check translation-invariance one coordinate at a time). Since  $G_S$  is open in  $G$ , there exists a unique measure Haar  $dg$  on  $G$  such that the restriction of  $dg$  to  $G_S$  coincides with  $dg_S$ . In principle, the measure  $dg$  thus constructed could depend on the set  $S$ . To show that it is well-defined, it suffices to check that, if  $T$  is another set of indices, the restriction of  $dg_S$  to  $G_S \cap G_T$  coincides with the restriction of  $dg_T$  to  $G_S \cap G_T$ . Replacing  $T$  with  $T \cup S$ , we can and do assume that  $S \subseteq T$ , so that  $G_S \subseteq G_T$ . There is an obvious decomposition

$$G^S = \left( \prod_{i \in T \setminus S} H_i \right) \times G^T,$$

and we claim that

$$dg^S = \left( \prod_{i \in T \setminus S} dg_i \right) \times dg^T.$$

Indeed, both are Haar measures, so – in order to check that they coincide – it suffices to show that they give the same (non-zero) volume to some subset. In particular, evaluating the right-hand side of the previous (claimed) equality on  $G^S$  we obtain

$$\prod_{i \in T \setminus S} \int_{H_i} dg_i \cdot \int_{G^T} dg^T = \prod_{i \in T \setminus S} \int_{H_i} dg_i \cdot \prod_{i \notin T} \left( \int_{H_i} dg_i \right) = \prod_{i \notin S} \left( \int_{H_i} dg_i \right) = \int_{G^S} dg^S,$$

as desired. Thus, upon restriction to  $G_S$  we have

$$dg_S = \left( \prod_{i \in S} dg_i \right) \times dg^S = \left( \prod_{i \in S} dg_i \right) \times \left( \prod_{i \in T \setminus S} dg_i \right) \times dg^T = dg_T,$$

as claimed.

**Definition 2.4.15** (Haar measure on a restricted product). We denote the measure  $dg$  just constructed by  $\prod_i dg_i$ .

**Definition 2.4.16** (Limit over  $S$ ). Let  $\mathcal{S}$  be the collection of all finite subsets of  $I$ , let  $X$  be a topological space, and let  $\varphi : \mathcal{S} \rightarrow X$  be a function we write  $\lim_S \varphi(S) = x$  if the following holds: for every open subset  $U$  of  $X$  containing  $x$ , there exists a finite set  $V(U) \in \mathcal{S}$  such that  $V(U) \subseteq S \Rightarrow \varphi(S) \in U$ .

Equivalently: add to  $\mathcal{S}$  a formal point  $\infty$  and make  $\mathcal{S} \cup \{\infty\}$  into a topological space by declaring that a basis consists of the sets  $W_V := \{\infty\} \cup \{S : S \supseteq V\}$ . We then have  $\lim_S \varphi(S) = x$  if and only if the extended function  $\tilde{\varphi} : \mathcal{S} \cup \{\infty\} \rightarrow X$  that sends  $\infty$  to  $x$  is continuous at  $x$ .

In particular, if  $f$  is a function on indices, we define

$$\prod_{i \in I} f(i) = \lim_S \prod_{i \in S} f(i).$$

Intuitively, one can think of  $\lim_S \varphi(S)$  as the limit of the values  $\varphi(S)$  as the set  $S$  gets larger and larger.

**Lemma 2.4.17.** *Let  $f : G \rightarrow \mathbb{C}$  satisfy one of the following:*

1.  *$f$  is measurable, real-valued and non-negative, or*
2.  *$f$  is in  $L^1(G)$ .*

*Then,  $\int_G f(g) dg = \lim_S \int_{G_S} f(g) dg$ .*

*Proof.* Under either assumption,  $\int_G f(g) dg$  is the limit of  $\int_B f(g) dg$  for larger and larger compacts  $B \subseteq G$ . We know that each compact is contained in some  $G_S$ , see Lemma 2.4.10.  $\square$

**Definition 2.4.18** (Product functions). For each  $i \in S$  fix a continuous function  $f_i : G_i \rightarrow \mathbb{C}$  with  $f_i \in L^1(G_i)$ . Suppose that  $f_i|_{H_i} = 1$  for almost all  $i$ . We define the function

$$f = \prod_{i \in I} f_i : \quad G \quad \rightarrow \quad \mathbb{C}$$

$$g = (g_i)_{i \in I} \mapsto \prod_{i \in I} f_i(g_i).$$

Notice that the product  $\prod_{i \in I} f_i(g_i)$  contains only finitely many terms different from 1, for each  $g = (g_i) \in G$ .

**Lemma 2.4.19.** *Let  $f = \prod_{i \in I} f_i$  be a product function as in Definition 2.4.18.*

1.  *$f$  is continuous on  $G$ .*
2. *Let  $S$  be a finite subset of  $I$  containing the (finitely many) indices  $i$  for which  $f_i(H_i) \neq \{1\}$  and those for which  $\int_{H_i} dg_i \neq 1$ . We have*

$$\int_{G_S} f(g) dg = \prod_{i \in S} \left( \int_{G_i} f_i(g_i) dg_i \right).$$

*Proof.* 1. Upon restriction to a set of the form  $G_S$ ,  $f$  is the product of finitely many continuous functions, hence continuous. Since the  $G_S$  are open and cover  $G$ ,  $f$  is continuous on  $G$ .

2. For  $g \in G_S$ , say  $g = (g_i)_{i \in I}$ , we have as above

$$f(g) = \prod_{i \in S} f_i(g_i).$$

Hence (recalling the defining property (2.7) of  $dg^S$ )

$$\begin{aligned} \int_{G_S} f(g) dg &= \int_{G_S} f(g) dg_S = \int_{G_S} \left( \prod_{i \in S} f_i(g_i) \right) \left( \prod_{i \in S} dg_i \times dg^S \right) \\ &= \prod_{i \in S} \left( \int_{G_i} f_i(g_i) dg_i \right) \times \int_{G^S} dg^S = \prod_{i \in S} \left( \int_{G_i} f_i(g_i) dg_i \right) \times \prod_{i \notin S} \left( \int_{H_i} dg_i \right) \\ &= \prod_{i \in S} \left( \int_{G_i} f_i(g_i) dg_i \right), \end{aligned}$$

where in the last equality we used the fact that  $\int_{H_i} dg_i = 1$  for every  $i \notin S$ .  $\square$

The previous two lemmas yield the following result:

**Theorem 2.4.20.** *Let  $f$  be a product function as in Definition 2.4.18. Assume*

$$\prod_i \left( \int_{G_i} |f_i(g_i)| dg_i \right) < \infty,$$

where the meaning of the product is as in Definition 2.4.16. Then  $f(g)$  is in  $L^1(G)$ , and

$$\int_G f(g) dg = \prod_i \left( \int_{G_i} f_i(g_i) dg_i \right).$$

*Proof.* Apply Lemmas 2.4.17 and 2.4.19 to  $|f(g)| = \prod_i |f_i(g_i)|$  shows that  $f \in L^1(G)$ , at which point the same lemmas (applied to  $f(g)$  itself) yield the result.  $\square$

### 2.4.5 Fourier analysis

We have seen in Theorem 2.4.14 that for a restricted direct product  $G = \prod'_{i \in I} (G_i, H_i)$  we have

$$\hat{G} = \prod'_{i \in I} (\widehat{G}_i, H_i^\perp).$$

Denote by  $c = (c_i)_{i \in I}$  an element of  $\hat{G}$ , that is, a continuous homomorphism  $G \rightarrow \mathbb{S}^1$ . Let  $dc_i$  be the measure on  $\widehat{G}_i$  dual to the measure  $dg_i$  on  $G_i$  (see Definition 2.2.11).

**Lemma 2.4.21.** *The following hold.*

1. Let  $f_i$  be the characteristic function of  $H_i$ . Its Fourier transform is  $\int_{H_i} dg_i$  times the characteristic function of  $H_i^\perp$ .
2.  $\left( \int_{H_i} dg_i \right) \left( \int_{H_i^\perp} dc_i \right) = 1$ .

*Proof.* 1. By definition,

$$\hat{f}_i(c_i) = \int_{G_i} f_i(g_i) \overline{c_i(g_i)} dg_i = \int_{H_i} \overline{c_i(g_i)} dg_i.$$

By Proposition 2.2.5, this integral is 0 if  $c_i(g_i)$  is nontrivial on  $H$  (that is, if  $\mathbf{1}_{H_i^\perp}(c_i) = 0$ ), and is  $\int_{H_i} dg_i$  otherwise.

2. Since  $f = \mathbf{1}_{H_i}$  is in  $L^1(G_i)$ , is continuous, and has its Fourier transform in  $L^1(\hat{G}_i)$  (by part (1) of the lemma), Fourier inversion (Theorem 2.2.10) gives

$$\mathbf{1}_{H_i}(g) = \int_{\hat{G}_i} \hat{f}(c_i) c_i(g) dc_i = \int_{\hat{G}_i} \left( \int_{H_i} dg_i \right) \mathbf{1}_{H_i^\perp}(c_i) c_i(g) dc_i = \left( \int_{H_i} dg_i \right) \left( \int_{H_i^\perp} c_i(g) dc_i \right).$$

Evaluating at  $g \in H_i$  yields

$$1 = \left( \int_{H_i} dg_i \right) \left( \int_{H_i^\perp} dc_i \right)$$

as claimed.  $\square$

Thus, we see that the collection  $\{dc_i\}_{i \in I}$  of the dual measures satisfies the condition to give a measure  $\prod dc_i$  on  $\hat{G} = \prod'_{i \in I} (\widehat{G}_i, H_i^\perp)$ . We denote this measure by  $dc$ .

**Lemma 2.4.22** (Product decomposition for the Fourier transform). *If  $f_i$  belongs to  $\mathfrak{V}^1(G_i)$  for all  $i \in I$  and  $f_i(g_i) = \mathbf{1}_{H_i}$  for almost all  $i$ , then the function  $f(g) = \prod_i f_i(g_i)$  belongs to  $\mathfrak{V}^1(G)$  and has Fourier transform  $\hat{f}(c) = \prod_i \hat{f}_i(c_i)$ .*

*Proof.* Apply Theorem 2.4.20 to the function  $f(g)\bar{c}(g) = \prod_i f_i(g_i)\overline{c_i(g_i)}$ : it implies that  $\hat{f}(c) = \prod_i \hat{f}_i(c_i)$ .

Since  $f_i \in \mathfrak{V}^1(G_i)$  for all  $i$ , we have  $\hat{f}_i \in L^1(\widehat{G}_i)$  for all  $i$ . Moreover, by Lemma 2.4.21,  $\hat{f}_i$  is the characteristic function of  $H_i^\perp$  for almost all  $i$ . From this, Lemma 2.4.19 and Lemma 2.4.21 (2) we then obtain  $\hat{f} \in L^1(\hat{G})$ . Since  $f$  is continuous and in  $L^1(G)$  (again by Lemma 2.4.19), we get that  $f$  is in  $\mathfrak{V}^1(G)$ .  $\square$

**Corollary 2.4.23.** *The measure  $dc = \prod_i dc_i$  is dual to  $dg = \prod_i dg_i$ .*

*Proof.* The previous lemma (applied to  $\hat{G}$ , with the measure  $dc$ ) shows that the Fourier inversion formula

$$f(g) = \int_{\hat{G}} \hat{f}(c)c(g) dc$$

holds at least for the product functions considered in the lemma. Since the dual measure of  $(G, dg)$  is unique, it must be  $dc$ .  $\square$





## Chapter 3

### Tate's thesis

### 3.1 The local theory

In this section we let  $k := K_v$  be the completion of a number field  $K$  at a place  $v$ . If  $v$  is a finite place, so that  $k$  is a  $p$ -adic field, we denote by  $\mathcal{O}$  its ring of integers. We denote by  $x$  the variable in the additive group  $(k, +)$ , and by  $\alpha$  the variable in  $(k^\times, \cdot)$ . In particular, we will eventually denote by  $dx$  and  $d\alpha$  certain Haar measures on  $(k, +)$  and on  $(k^\times, \cdot)$ , respectively.

#### 3.1.1 The additive group

Recall our choice of norm on  $k = K_v$ :

1. the ordinary absolute value if  $k \cong \mathbb{R}$ ;
2. the square of the ordinary absolute value if  $k \cong \mathbb{C}$ ;
3.  $\|\alpha\| = (N\mathfrak{p})^{-v_{\mathfrak{p}}(\alpha)}$ , if  $v$  is the finite place corresponding to the prime  $\mathfrak{p}$ .

We begin by studying the group of characters of the locally compact group  $k^+ := (k, +)$ .

**Proposition 3.1.1.** *Let  $\chi$  be any non-trivial character of  $k^+$ .*

1. *For each  $\eta \in k$ , the map  $x \mapsto \chi(\eta x)$  is a continuous character.*
2. *The map  $\alpha_\chi : k^+ \rightarrow \widehat{k^+}$  given by  $\eta \mapsto \chi_\eta$ , where  $\chi_\eta(x) := \chi(\eta x)$ , is an isomorphism (of topological groups) between  $k^+$  and its character group.*

*Proof.* Since  $x \mapsto \eta x$  is a continuous homomorphism of  $k^+$  into itself, by composition with  $\chi$  we see that  $\chi_\eta$  is indeed a continuous character of  $k^+$ . One checks easily that  $\eta \mapsto \chi_\eta$  is a homomorphism. Moreover,  $\alpha_\chi$  is injective, because  $\chi_\eta$  is the trivial character 1 if and only if  $\chi(\eta x) = 1$  for all  $x \in k$ . Since  $\chi$  is non-trivial, there exists  $y \in k$  such that  $\chi(y) \neq 1$ . If  $\eta \neq 0$ , setting  $x = y/\eta$  gives a contradiction, so  $\chi_\eta$  is trivial only for  $\eta = 0$ .

Next we show that  $\alpha_\chi$  is a topological isomorphism between  $k$  and its image (and in particular, that  $\alpha_\chi$  is open). We start by recalling the topology on  $\widehat{k^+}$ . By definition, a basis of neighbourhoods of the identity in  $\widehat{k^+}$  is given by the  $U(K, V)$  (see Definition 2.2.1), where  $K$  is a compact neighbourhood of  $0 \in k$  and  $V$  is a neighbourhood of  $1 \in \mathbb{S}^1$ . Clearly, it suffices to let  $K$  and  $V$  range over a basis of neighbourhoods of 0 and 1 in  $k$  and  $\mathbb{S}^1$ , respectively. Thus, we may only consider

$$K = C_m = \{x \in F : \|x\| \leq m\} \text{ and } V = V_\varepsilon = \{z \in \mathbb{S}^1 : \|z - 1\| < \varepsilon\}.$$

Since  $\chi$  is continuous, for all  $\varepsilon > 0$  there exists a  $\delta > 0$  such that

$$\|\chi(x) - 1\| < \varepsilon \text{ whenever } \|x\| < \delta. \tag{3.1}$$

Since  $\alpha_\chi$  is a group homomorphism, to show that it is continuous it suffices to show that it is continuous at the identity. Explicitly, we have to show that for every  $U(C_m, V_\varepsilon)$  there exists an open neighbourhood  $W$  of 0 in  $k^+$  such that

$$\alpha_\chi(W) \subseteq U(C_m, V_\varepsilon),$$

that is, we must choose  $W$  in such a way that for every  $x \in W$

$$\|\alpha_\chi(x)(y) - 1\| < \varepsilon \quad \forall y \in C_m,$$

or equivalently,

$$\|\chi(xy) - 1\| < \varepsilon \quad \forall y \in C_m.$$

Thus, it suffices to take as  $W$  the open set  $\{x \in F : \|x\| < \frac{\delta}{m}\}$ : for  $x \in W$  and  $y \in C_m$  one has  $\|xy\| < \frac{\delta}{m}m = \delta$ , and hence  $\|\chi(xy) - 1\| < \varepsilon$  by (3.1).

Now we show continuity of  $\alpha_\chi^{-1} : \alpha_\chi(k) \rightarrow k$ . Again by definition of the respective topologies, we have to show that, for every  $\delta > 0$ , there exist  $\varepsilon > 0, m \in \mathbb{R}$  such that

$$\alpha_\chi(x) \in \alpha_\chi(k) \cap U(C_m, V_\varepsilon) \implies \|x\| < \delta.$$

Since  $\chi$  is nontrivial, there exists  $x_0 \in k$  such that  $\chi(x_0) \neq 1$ . Set

$$\varepsilon = \|\chi(x_0) - 1\|, \quad m = \frac{2\|x_0\|}{\delta}.$$

Suppose now that  $x$  is such that  $\alpha_\chi(x) \in U(C_m, V_\varepsilon)$ , that is to say,

$$\|\chi(xy) - 1\| < \varepsilon \quad \forall y \text{ with } \|y\| < m.$$

Note that  $y = x^{-1}x_0$  does *not* satisfy  $\|\chi(xy) - 1\| < \varepsilon$ , hence  $y = x^{-1}x_0$  does *not* satisfy  $\|y\| < m$ . This implies

$$\|x^{-1}x_0\| \geq m = \frac{2\|x_0\|}{\delta} \implies \|x\|^{-1} \geq \frac{2}{\delta} \implies \|x\| \leq \frac{\delta}{2} < \delta,$$

as desired.

Since  $\alpha_\chi$  is a topological isomorphism,  $\alpha_\chi(k)$  is locally compact, hence closed (see Exercise 3.1.2). Thus, in order to show that  $\alpha_\chi(k) = \widehat{k^+}$ , it suffices to prove that  $H := \alpha_\chi(k)$  is everywhere dense in  $\widehat{k^+}$ . We now observe that

$$H^\perp = \{x \in k : \psi(x) = 1 \quad \forall \psi \in H\} = \{x \in k : \chi(xy) = 1 \quad \forall y \in k\} = \{0\},$$

which, by Proposition 2.2.4, yields

$$0 = \widehat{H^\perp} = \widehat{k^+}/H,$$

hence  $H = \widehat{k^+}$ , as desired.  $\square$

**Exercise 3.1.2.** Let  $H$  be a locally compact subgroup of a topological group  $G$ . Prove that  $H$  is closed in  $G$ .

*Sketch of solution.* Let  $K$  be the closure of  $H$ . It suffices to prove that  $K = H$ . Clearly,  $H$  is dense in  $K$  (which is Hausdorff, since  $G$  is Hausdorff by assumption!). Given a point  $h \in H$ , let  $U$  be an open neighbourhood of  $h$  in  $H$  whose closure  $C$  in  $H$  is compact. Write  $U = V \cap H$  for some open  $V$  in  $K$ . Since  $C$  is compact and  $G$  (hence  $K$ ) is Hausdorff,  $C$  is also closed in  $K$ . Now observe that  $V \setminus C$  is open in  $K$  and does not meet  $H$  (since  $V \cap H = U \subseteq C$ ). As  $H$  is dense in  $K$  but does not meet the open set  $V \setminus C$ , we must have  $V \setminus C = \emptyset$ , that is,  $V \subseteq C \subseteq H$ , so  $H$  contains a neighbourhood of  $h$ . As  $h$  was arbitrary, we see that  $H$  is open in  $K$ . Every open subgroup of a topological group is closed (consider the partition given by its cosets), so in particular  $H$  is closed in  $K$ . Since  $K$  is the closure of  $H$ , we have  $K = H$  as desired.

Using Proposition 3.1.1, we may identify  $k^+$  with its dual provided that we fix a non-trivial character. We start by defining a certain function  $\lambda : \mathbb{Q}_p \rightarrow \mathbb{R}/\mathbb{Z}$  for each  $p \in \{\text{primes}\} \cup \{\infty\}$ .

1. if  $p = \infty$ , the completion  $\mathbb{Q}_p$  is  $\mathbb{R}$ , and we let  $\lambda(x)$  be the class of  $-x$  in the quotient  $\mathbb{R}/\mathbb{Z}$ .

**Note the choice of sign!**

2. if  $p$  is a prime number, one can prove (see Exercise 3.1.3) that  $\mathbb{Q}_p/\mathbb{Z}_p$  is isomorphic to the subgroup of  $\mathbb{Q}/\mathbb{Z}$  given by torsion elements of order a power of  $p$ . Identifying  $\mathbb{Q}/\mathbb{Z}$  to a subset of  $\mathbb{R}/\mathbb{Z}$ , we take  $\lambda$  to be the projection

$$\lambda : \mathbb{Q}_p \rightarrow \frac{\mathbb{Q}_p}{\mathbb{Z}_p} \hookrightarrow \frac{\mathbb{Q}}{\mathbb{Z}} \hookrightarrow \frac{\mathbb{R}}{\mathbb{Z}}.$$

Concretely,  $\lambda(x)$  can be described as follows: let  $v$  be an integer such that  $p^v x$  is in  $\mathbb{Z}_p$ , and let  $n$  be an integer such that  $n \equiv p^v x \pmod{p^v}$ . We then have  $\lambda(x) = \frac{n}{p^v} \pmod{1}$ . In particular,  $x - \lambda(x)$  is a  $p$ -adic integer.

**Exercise 3.1.3.** Let  $p$  be a prime number.

1. Describe an isomorphism between  $\mathbb{Q}_p/\mathbb{Z}_p$  and the  $p$ -power torsion of  $\mathbb{Q}/\mathbb{Z}$ .
2. Check the description of  $\lambda$  given above.
3. Check that  $\lambda$  is continuous.

Finally, if  $k = K_v$  is an arbitrary completion of a number field and if  $p$  is the prime of  $\mathbb{Q}$  'lying under  $v$ ' (that is,  $p = \infty$  if  $v$  is archimedean, and  $p = p_v$  if  $v$  is finite), we have a natural inclusion  $\mathbb{Q}_p \subseteq k$ . We then give the following definition.

**Definition 3.1.4** (Fundamental character of the additive group). We set  $\Lambda(x) := \lambda(\text{tr}_{k/\mathbb{Q}_p}(x))$ .

Since the trace map is continuous,  $\Lambda$  is a non-trivial, continuous map from  $k$  to  $\mathbb{R}/\mathbb{Z}$ . Using Proposition 3.1.1, we obtain

**Theorem 3.1.5** (Dual group of  $k^+$ ).  $k^+$  is isomorphic to its dual group via the isomorphism  $\eta \mapsto \chi_\eta$ , where

$$\chi_\eta(x) = e^{2\pi i \Lambda(\eta x)}.$$

For later use, we record a lemma connecting properties of characters with the arithmetic of  $k$ .

**Lemma 3.1.6.** Let  $v$  be a finite place of characteristic  $p$ . The character  $e^{2\pi i \Lambda(\eta x)}$  corresponding to  $\eta$  is trivial on  $\mathcal{O}$  if and only if  $\eta$  is in the inverse different ideal  $\mathfrak{d}_k^{-1}$  (see Definition 2.3.17).

*Proof.* The character  $e^{2\pi i \Lambda(\eta x)}$  is trivial if and only if  $\Lambda(\eta x)$  is an integer for every  $x \in \mathcal{O}$ , if and only if  $\text{tr}_{k/\mathbb{Q}_p}(\eta x)$  is in  $\mathbb{Z}_p$  for every  $x \in \mathcal{O}$ , if and only if  $\eta$  is in the inverse different.  $\square$

### Choice of Haar measure

Let  $\mu$  be a Haar measure on  $k^+$ . We now investigate the interactions between  $\mu$  and the multiplicative structure of  $k$ , and describe the measure on the dual group which appears in Theorem 2.2.10 (abstract Fourier inversion).

**Lemma 3.1.7.** *For every  $\alpha \in k^\times$  and for every measurable set  $M$  in  $k$  we have  $\mu(\alpha M) = \|\alpha\|\mu(M)$  for the choice of norm  $\|\cdot\|$  recalled at the beginning of Section 3.1.*

*Proof.* Note that  $M \mapsto \mu(\alpha M)$  is a Haar measure on  $k^+$ , so  $\mu(\alpha M) = \varphi(\alpha)\mu(M)$  for some constant  $\varphi(\alpha) > 0$  which may depend on  $\alpha$  but not on  $M$ . To identify this constant, note that in the real and complex case this is precisely  $\|\alpha\|$ , as follows from the change-of-variables formula for integration that is familiar from analysis (in the complex case, note that  $\alpha = u + iv$  acts on  $\mathbb{C} \cong \mathbb{R}^2$  as the linear transformation

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} u & v \\ -v & u \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix},$$

whose (Jacobian) determinant is  $u^2 + v^2 = \|\alpha\|$ . Finally, in the  $p$ -adic case, consider the set  $M = \mathcal{O}$ . Suppose first that  $\alpha$  is integral: then  $\mathcal{O}/\alpha\mathcal{O}$  has  $N(\alpha)$  elements, which means that  $\mathcal{O} = \bigsqcup_{i=1}^{N(\alpha)} (x_i + \alpha\mathcal{O})$  for some collection  $x_1, \dots, x_{N(\alpha)}$  of points in  $\mathcal{O}$ . Since the Haar measure is translation-invariant, we obtain

$$\mu(\mathcal{O}) = \sum_{i=1}^{N(\alpha)} \mu(x_i + \alpha\mathcal{O}) = N(\alpha)\mu(\alpha\mathcal{O}).$$

If we let  $\pi$  be a uniformiser of  $k$ , we have  $\alpha = \pi^v u$  with  $v \in \mathbb{N}$  and  $u \in \mathcal{O}^\times$ , and  $N(\alpha) = N(\pi)^v = \|\alpha\|^{-1}$ . Thus, we conclude that

$$\mu(\mathcal{O}) = \|\alpha\|^{-1}\mu(\alpha\mathcal{O}),$$

as desired. Finally, if  $\alpha$  has negative valuation, the same argument with  $\alpha$  replaced by  $\alpha^{-1}$  gives the desired statement.  $\square$

By standard results in measure theory, Lemma 3.1.7 implies the following equality for integrable functions  $f$  on  $k^+$  and for  $\alpha \in k^\times$ :

$$\int_{k^+} f(x) d\mu(x) = \int_{k^+} f(\alpha x) d\mu(\alpha x) = \|\alpha\| \int_{k^+} f(\alpha x) d\mu(x).$$

**Remark 3.1.8** (Measure of a fractional ideal). Every fractional ideal of  $k$  is principal, generated by a power of the uniformiser  $\pi$ . Writing  $I = (\pi^v)$  and using Lemma 3.1.7, we obtain

$$\mu(I) = \mu(\pi^v \mathcal{O}) = \|\pi\|^v \mu(\mathcal{O}) = (N\pi)^{-v} \mu(\mathcal{O}) = (N(I))^{-1} \mu(\mathcal{O}).$$

The (essentially) canonical identification of  $k^+$  with its dual group provided by Theorem 3.1.5 allows us to interpret the abstract Fourier transform of a function on  $k^+$  (which would formally be a function on the dual group of  $k^+$ ) as another function on  $k^+$  itself. We now look for a choice of Haar measure on  $k^+$  that is ‘natural’ with respect to Fourier inversion. More specifically, for every Haar measure on  $k^+$ , Theorem 2.2.10 yields the existence of a

corresponding Haar measure on the dual. However, since we have identified  $k^+$  with its dual, this means that from every Haar measure on  $k^+$  we obtain a 'Fourier-dual Haar measure' on  $k^+$  itself. The most natural choice is then to require that the Fourier-dual measure coincide with the original measure! This is achieved by taking  $\mu_{k^+}$  as in the following definition.

**Definition 3.1.9** (Choice of Haar measure). We define  $\mu_{k^+}$  to be

1. the ordinary Lebesgue measure on the the real line, if  $k$  is real;
2. twice the ordinary Lebesgue measure in the plane, if  $k$  is complex;
3. the unique Haar measure for which  $\mu_{k^+}(\mathcal{O}) = N(\mathfrak{d}_k)^{-1/2}$ , if  $k$  is  $p$ -adic.

We will simply write  $dx$  for  $d\mu_{k^+}(x)$ .

We summarise (and give details for) the above discussion in the next theorem.

**Theorem 3.1.10.** *Let  $dx$  denote the measure on  $k^+$  introduced in Definition 3.1.9. If we define the Fourier transform  $\hat{f}$  of a function  $f \in L^1(k^+)$  by*

$$\hat{f}(\eta) = \int_{k^+} f(x) e^{-2\pi i \Lambda(\eta x)} dx, \quad (3.2)$$

then the inversion formula

$$f(x) = \int_{k^+} \hat{f}(\eta) e^{2\pi i \Lambda(x\eta)} d\eta = \hat{\hat{f}}(-x)$$

holds for  $f \in \mathfrak{B}^1(k^+)$  (see Definition 2.2.8 for the notation  $\mathfrak{B}^1$ ).

*Proof.* Theorem 2.2.10 implies that the identity

$$f(x) = c \int_{k^+} \hat{f}(\eta) e^{2\pi i \Lambda(x\eta)} d\eta$$

holds for some nonzero (in fact, positive) constant  $c$  independent of  $f$ , because the Fourier transform defined in the statement is equivalent to the general, abstract Fourier transform of Definition 2.2.6 under the isomorphism between  $k^+$  and its dual provided by Theorem 3.1.5. Thus, it suffices to check that  $c = 1$  for a single function  $f$ . We distinguish three cases, according to the nature of  $k$ :

1. if  $k$  is real, we take  $f(x) = e^{-\pi \|x\|^2}$ . The result then reduces to the classical calculation of the Fourier transform of a Gaussian, see Exercise 3.1.11.
2. if  $k$  is complex, we similarly take  $f(x) = e^{-2\pi \|x\|}$  (recall that our norm on complex fields is the *square* of the usual absolute value), see again Exercise 3.1.11.
3. if  $k$  is  $p$ -adic, we take as  $f$  the characteristic function of  $\mathcal{O}$ . We compute its Fourier transform: by definition,

$$\hat{f}(\eta) = \int_{\mathcal{O}} e^{-2\pi i \Lambda(\eta x)} dx.$$

We are integrating a character of  $\mathcal{O}$  on the whole group: similarly to Proposition 1.5.12, the result is either 0 (if this character is nontrivial) or  $\mu_{k^+}(\mathcal{O})$ . Using Lemma 3.1.6, we obtain

$$\hat{f}(\eta) = \begin{cases} \mu_{k^+}(\mathcal{O}), & \text{if } \eta \in \mathfrak{d}_k^{-1} \\ 0, & \text{otherwise,} \end{cases}$$

and therefore  $\hat{f}(\eta) = \mu_{k^+}(\mathcal{O})\mathbf{1}_{\mathfrak{d}_k^{-1}} = N(\mathfrak{d}_k)^{-1/2}\mathbf{1}_{\mathfrak{d}_k^{-1}}$ , where the last equality follows from our normalisation  $\mu_{k^+}(\mathcal{O}) = N(\mathfrak{d}_k)^{-1/2}$ . Next, we plug  $\hat{f}(\eta)$  in the Fourier inversion formula:

$$\int_{k^+} \hat{f}(\eta)e^{2\pi i\Lambda(x\eta)} d\eta = \int_{\mathfrak{d}_k^{-1}} N(\mathfrak{d}_k)^{-1/2}e^{2\pi i\Lambda(x\eta)} d\eta.$$

Fix a uniformiser  $\pi$  of  $k$  and write  $\mathfrak{d}_k = \pi^r$ . The change of variables  $\eta = \pi^{-r}y$  leads to

$$\int_{\mathfrak{d}_k^{-1}} N(\mathfrak{d}_k)^{-1/2}e^{2\pi i\Lambda(x\eta)} d\eta = \int_{\mathcal{O}} N(\mathfrak{d}_k)^{-1/2}e^{2\pi i\Lambda(x\pi^{-r}y)} \|\pi^{-r}\| dy,$$

where we have used Lemma 3.1.7. By definition,  $\|\pi^{-r}\| = N(\pi^r) = N(\mathfrak{d}_k)$ . Finally, applying Lemma 3.1.6 again,

$$\int_{k^+} \hat{f}(\eta)e^{2\pi i\Lambda(x\eta)} d\eta = N(\mathfrak{d}_k)^{1/2}\mu_{k^+}(\mathcal{O})\mathbf{1}_{\mathcal{O}}(x) dx = \mathbf{1}_{\mathcal{O}}(x),$$

which concludes the proof.

Finally, we check the equality  $\hat{\hat{f}}(x) = f(-x)$ . By definition,  $\hat{\hat{f}}(x)$  is the Fourier transform of (3.2), hence it is given by

$$\hat{\hat{f}}(\eta) = \int_{k^+} \hat{f}(x)e^{-2\pi i\Lambda(\eta x)} dx = \int_{k^+} \hat{f}(x)e^{2\pi i\Lambda((- \eta)x)} dx = f(-\eta)$$

by what we already showed. □

**Exercise 3.1.11.** Fill in the details of the proof of Theorem 3.1.10 in the real and complex cases. It can be useful to recall (and prove, if necessary) the classical formula

$$\int_{-\infty}^{\infty} e^{-ax^2} e^{-2\pi i kx} dx = \sqrt{\frac{\pi}{a}} e^{-\pi^2 k^2/a}.$$

*Please try this exercise if you've never seen it before! A solution is given by Lemma 3.1.36.*

### 3.1.2 The multiplicative group

We now turn to the study of characters of  $k^*$ , and more generally of **quasi-characters**, that is, continuous homomorphisms  $k^* \rightarrow \mathbb{C}^\times$ . A special such homomorphism is given by the norm itself,  $\alpha \mapsto \|\alpha\| \in \mathbb{R}^\times$ . Of particular importance will be its kernel:

**Definition 3.1.12.** Following Tate, we denote by  $\mathbf{u}$  the subgroup of  $k^\times$  of elements of norm 1, that is, the kernel of  $\|\cdot\| : k^\times \rightarrow \mathbb{R}^\times$ . Note that  $\mathbf{u}$  is nothing else than the group of units  $\mathcal{O}^\times$ . We say that a quasi-character  $\chi : k^\times \rightarrow \mathbb{C}^\times$  is **unramified** if  $\chi(\mathbf{u}) = 1$ .

The unramified quasi-characters are easy to classify:

**Lemma 3.1.13.** *The unramified quasi-characters of  $k^\times$  are the maps of the form  $c(\alpha) = |\alpha|^s := e^{s \log \|\alpha\|}$ , where  $s$  is any complex number. When  $v$  is archimedean,  $s$  is uniquely determined by  $c$ ; when  $v$  is finite, corresponding to a prime  $\mathfrak{p}$ , the number  $s$  is determined modulo  $\frac{2\pi i}{\log N(\mathfrak{p})}$ .*

*Proof.* Clearly, it suffices to classify the continuous homomorphisms from  $\tilde{c} : k^\times/\mathfrak{u}$  to  $\mathbb{C}^\times$ . Since  $\mathfrak{u}$  is the kernel of the norm,  $k^\times/\mathfrak{u}$  is isomorphic to the image of  $\|\cdot\|$  (the ‘value group’), which is the group of positive real numbers when  $v$  is archimedean and  $\langle N(\mathfrak{p}) \rangle \cong \mathbb{Z}$  when  $v$  is finite and corresponds to  $\mathfrak{p}$ . The claim follows easily: when  $v$  is finite, the value group  $\|k^\times\|$  is isomorphic to  $\mathbb{Z}$ , so a homomorphism from  $\|k^\times\|$  to  $\mathbb{C}^\times$  is determined by its value on a generator. For the archimedean case, see Exercise 3.1.14.  $\square$

**Exercise 3.1.14.** Show that every continuous homomorphism from the positive reals to  $\mathbb{C}^\times$  is of the form  $x \mapsto x^s$ , and that different values of  $s$  give different homomorphisms.

We now give a partial description of all the quasi-characters of  $k^\times$ . This will be an immediate consequence of Lemma 3.1.13 once we make the following observations:

1. if  $v$  is archimedean, every element  $\alpha$  of  $k^\times$  can be written uniquely as  $\tilde{\alpha}\rho$  with  $\tilde{\alpha} \in \mathfrak{u}$  and  $\rho > 0$ ;
2. if  $v$  is finite, letting  $\pi$  be a uniformiser of  $k$ , every element  $\alpha$  of  $k^\times$  can be written uniquely as  $\tilde{\alpha}\rho$  with  $\tilde{\alpha} \in \mathfrak{u}$  and  $\rho$  a power of  $\pi$ .

In either case, the map  $\alpha \mapsto \tilde{\alpha}$  is a continuous homomorphism  $k^\times \rightarrow \mathfrak{u}$  which is the identity on  $\mathfrak{u}$ .

**Exercise 3.1.15.** Check that  $\alpha \mapsto \tilde{\alpha}$  is continuous when  $v$  is a finite place.

*Hint.*  $\rho$  is locally constant.

The following classification of quasi-characters is now immediate:

**Theorem 3.1.16.** *The quasi-characters of  $k^\times$  are the maps of the form  $c : \alpha \mapsto \tilde{c}(\tilde{\alpha})\|\alpha\|^s$ , where  $\tilde{c}$  is any (continuous) character of  $\mathfrak{u}$ . The character  $\tilde{c}$  is uniquely determined by  $c$  (it is its restriction to  $\mathfrak{u}$ ), while  $s$  is determined as in Lemma 3.1.13.*

Thus, the classification of the quasi-characters of  $k^\times$  reduces to the classification of those of  $\mathfrak{u}$ .

**Proposition 3.1.17** (Classification of quasi-characters of  $\mathfrak{u}$ ). *The quasi-characters  $\tilde{c}$  of  $\mathfrak{u}$  can be described as follows:*

1. if  $k$  is real,  $\mathfrak{u} = \{\pm 1\}$  and the quasi-characters are  $x \mapsto x^n$  for  $n = 0, 1$ ;
2. if  $k$  is complex,  $\mathfrak{u} \cong \mathbb{S}^1$  and the quasi-characters are of the form  $x \mapsto x^n$  for  $n \in \mathbb{Z}$ ;
3. if  $k$  is  $p$ -adic, with uniformiser  $\pi$ , there is an integer  $n \geq 1$  such that  $\tilde{c}$  factors via the finite set  $\mathfrak{u}/(1 + (\pi)^n)$ .



*Proof.* The real case is obvious. The complex case requires us to classify all continuous homomorphisms from  $\mathbb{S}^1$  to  $\mathbb{C}^\times$ ; the answer is well-known, but we re-derive it here.

Since  $\mathbb{S}^1$  is compact, the image of any continuous homomorphism  $c : \mathbb{S}^1 \rightarrow \mathbb{C}^\times$  is compact, hence contained in  $\mathbb{S}^1$ . Indeed, if  $z$  is an element of the image with  $|z| \neq 1$ , then either  $z$  or  $1/z$  is in the image and has absolute value greater than one. This easily implies that the image of  $c$  is unbounded, hence not compact. Now, every continuous homomorphism  $\mathbb{S}^1 \rightarrow \mathbb{S}^1$  lifts to a continuous homomorphism between their universal covers, that is, to a continuous homomorphism  $f : \mathbb{R} \rightarrow \mathbb{R}$ , where the universal covering map  $\mathbb{R} \rightarrow \mathbb{S}^1$  is given by  $x \mapsto \exp(2\pi ix)$ .

It is well-known that the only continuous endomorphisms of  $\mathbb{R}$  are given by  $x \mapsto ax$  for  $a \in \mathbb{R}$ . In order for  $f$  to descend to a map  $\mathbb{S}^1 \rightarrow \mathbb{S}^1$ ,  $f$  must map 1 to an integer  $n$ . Thus,  $c : \mathbb{S}^1 \rightarrow \mathbb{S}^1$  is of the form  $\exp(2\pi ix) \mapsto \exp(2n\pi ix)$ , hence of the form  $c(z) = z^n$  for  $n \in \mathbb{Z}$ . On the other hand, it is clear that all these maps are characters of  $\mathbb{S}^1$ .

Finally, the  $p$ -adic case follows essentially from topological considerations. Specifically, since  $\tilde{c} : \mathfrak{u} \rightarrow \mathbb{C}^\times$  is continuous, the inverse image of an open subset of  $\mathbb{C}^\times$  is an open subset of  $\mathfrak{u}$ . Choose an open subset  $V$  of  $\mathbb{C}^\times$  that does not contain any non-trivial multiplicative subgroup of  $\mathbb{C}^\times$  (see Exercise 3.1.18). Then,  $\tilde{c}^{-1}(V)$  is an open neighbourhood of 1 in  $\mathfrak{u}$ .

By definition of the  $p$ -adic topology, the subgroups  $1 + (\pi)^n$  form a basis of open neighbourhoods of the identity of  $\mathfrak{u}$ . Hence, there exists  $n \geq 1$  such that  $H := 1 + (\pi)^n \subseteq \tilde{c}^{-1}(V)$ . However, this implies  $\tilde{c}(H) \subseteq V$ , and  $\tilde{c}(H)$  is a subgroup of  $\mathbb{C}^\times$ , so  $\tilde{c}(H)$  must be trivial, which proves that the kernel of  $\tilde{c}$  contains  $1 + (\pi)^n$ , hence that  $\tilde{c}$  factors via  $\mathfrak{u}/(1 + (\pi)^n)$ , as desired.  $\square$

**Exercise 3.1.18.** 1. Show that every sufficiently small neighbourhood of 1 in  $\mathbb{C}^\times$  contains no non-trivial subgroup of  $\mathbb{C}^\times$ .

2. Mimicking the proof of Proposition 3.1.17 in the  $p$ -adic case, show that if  $G$  is a profinite group and  $\rho : G \rightarrow \mathrm{GL}_n(\mathbb{C})$  is a continuous representation, then the image of  $\rho$  is finite.

**Remark 3.1.19.** Let  $K$  be a number field. The second part of Exercise 3.1.18, together with the fact that  $\mathrm{Gal}(\overline{K}/K)$  is a profinite group, shows that the definition of an Artin  $L$ -function may be reformulated by considering – formally more generally – any complex representation of  $\mathrm{Gal}(\overline{K}/K)$ . Indeed, any such representation factors via a finite quotient of  $\mathrm{Gal}(\overline{K}/K)$ , hence via  $\mathrm{Gal}(L/K)$  for some finite extension  $L/K$ . This topological obstruction prevents one from fully understanding  $\mathrm{Gal}(\overline{K}/K)$  by only looking at complex representations: to get a more complete picture, one should also consider continuous  $p$ -adic representations. These constitute a very rich area of research<sup>1</sup>, but we won't discuss them, since this would take us too far afield.

Theorem 3.1.16 justifies the following definition.

**Definition 3.1.20** (Exponent of a quasi-character). Let  $c : k^\times \rightarrow \mathbb{C}^\times$  be a quasi-character. By Theorem 3.1.16, we may write  $c(\alpha) = \tilde{c}(\tilde{\alpha})\|\alpha\|^s$ , hence  $|c(\alpha)| = \|\alpha\|^\sigma$ , where  $\sigma = \Re(s)$  is uniquely determined by the character  $\chi$ . We call  $\sigma$  the **exponent** of  $c$  and denote it by  $\sigma(c)$ .

**Remark 3.1.21.** Notice that a quasi-character  $c : k^\times \rightarrow \mathbb{C}^\times$  is a character if and only if its exponent is zero.

---

<sup>1</sup>I'm biased: it's something I actively do research about

### Choice of Haar measure

We would now like to choose a Haar measure on  $k^\times$  in a way that is compatible with the Haar measure on  $k^+$ . If  $g$  is a function in  $\mathcal{K}(k^\times)$ , then by definition there is an open neighbourhood  $B$  of 0 (for the topology of  $k$ ) such that  $g|_B$  vanishes. Since  $\|x\|$  is bounded away from 0 on the complement of  $B$ , we conclude that  $h(x) := \frac{g(x)}{\|x\|}$  is a continuous function with bounded support on all of  $k$  (where of course we set  $h(0) = 0$ ). In particular, we may consider the (positive) linear functional

$$\begin{aligned} \psi : \mathcal{K}(k^\times) &\rightarrow \mathbb{R} \\ g &\mapsto \int_{k^+} g(x) \frac{dx}{\|x\|}. \end{aligned}$$

By the representation theorem (Theorem 2.1.28), there exists a unique Radon measure  $\mu_{k^\times}$  on  $k^\times$  such that

$$\psi(g) = \int_{k^\times} g(\alpha) d\mu_{k^\times}(\alpha).$$

Moreover,  $\mu_{k^\times}$  is invariant under translation by elements of  $k^\times$ : it suffices to check that  $\psi(g(\beta \cdot)) = \psi(g(\cdot))$  for every  $g \in \mathcal{K}(k^\times)$ , and this follows from the identities

$$\psi(g(\beta \cdot)) = \int_{k^+} g(\beta x) \frac{dx}{\|x\|} = \int_{k^+} g(y) \frac{d(\beta^{-1}y)}{\|\beta^{-1}y\|} = \int_{k^+} g(y) \frac{\|\beta^{-1}\| dy}{\|\beta^{-1}y\|} = \int_{k^+} g(y) \frac{dy}{\|y\|},$$

where we have used Lemma 3.1.7. Hence,  $\mu_{k^\times}$  is a Haar measure on  $k^\times$ . We now select an appropriate multiple that is more suitable to our arithmetic applications:

**Definition 3.1.22** (Haar measure on  $k^\times$ ). We denote by  $d\alpha$  the Haar measure given by

1.  $d\alpha = d\mu_{k^\times} = \frac{d\mu_{k^+}(\alpha)}{\|\alpha\|}$ , if  $v$  is archimedean;
2.  $d\alpha = \frac{N_{\mathfrak{p}}}{N_{\mathfrak{p}-1}} d\mu_{k^\times} = \frac{N_{\mathfrak{p}}}{N_{\mathfrak{p}-1}} \frac{d\mu_{k^+}(\alpha)}{\|\alpha\|}$ , if  $v$  is finite and corresponds to the prime  $\mathfrak{p}$ .

The next lemma gives the measure of the group of units:

**Lemma 3.1.23.** *If  $v$  is discrete,*

$$\int_{\mathfrak{u}} d\alpha = (N\mathfrak{d})^{-1/2}.$$

*Proof.* Let  $\pi$  be a uniformiser. We have

$$\mathcal{O} = \bigsqcup_{n \geq 0} \pi^n \mathfrak{u},$$

hence

$$\mu_{k^+}(\mathcal{O}) = \sum_{n \geq 0} \mu_{k^+}(\pi^n \mathfrak{u}) = \sum_{n \geq 0} \|\mathfrak{p}\|^n \mu_{k^+}(\mathfrak{u}) = \frac{1}{1 - N(\mathfrak{p})^{-1}} \mu_{k^+}(\mathfrak{u}) = \frac{N(\mathfrak{p})}{N(\mathfrak{p}) - 1} \mu_{k^+}(\mathfrak{u}).$$

Recalling that we have defined  $\mu_{k^+}$  so that  $\mu_{k^+}(\mathcal{O}) = N(\mathfrak{d})^{-1/2}$  (see Definition 3.1.9), we obtain

$$\begin{aligned} \int_{\mathfrak{u}} d\alpha &= \int_{\mathfrak{u}} \frac{N_{\mathfrak{p}}}{N_{\mathfrak{p}-1}} d\mu_{k^\times}(\alpha) = \frac{N_{\mathfrak{p}}}{N_{\mathfrak{p}-1}} \int_{\mathfrak{u}} \frac{dx}{\|x\|} = \frac{N_{\mathfrak{p}}}{N_{\mathfrak{p}-1}} \int_{\mathfrak{u}} dx \\ &= \frac{N_{\mathfrak{p}}}{N_{\mathfrak{p}-1}} \mu_{k^+}(\mathfrak{u}) = \mu_{k^+}(\mathcal{O}) = N(\mathfrak{d})^{-1/2}. \end{aligned}$$

□

### 3.1.3 Local zeta functions I: the general functional equation

Fix a function  $f : k \rightarrow \mathbb{C}$ . Continuing with our notation from the previous sections, we will denote by  $f(x)$  the function on the whole of  $k$ , and by  $f(\alpha)$  its restriction to  $k^\times$ .

**Definition 3.1.24** (Class of  $\mathfrak{z}$ -functions). We denote by  $\mathfrak{z}$  the class of all functions  $f : k \rightarrow \mathbb{C}$  that satisfy

1.  $f(x) \in \mathfrak{V}_1(k^+)$  (that is,  $f(x)$  is continuous and in  $L^1(k^+)$ , and  $\hat{f}$  is in  $L^1(k^+)$ , see both Definition 2.2.8 and Theorem 3.1.5);
2.  $f(\alpha)\|\alpha\|^\sigma$  and  $\hat{f}(\alpha)\|\alpha\|^\sigma$  are in  $L^1(k^\times)$  for all  $\sigma > 0$ .

For each function  $f$  of class  $\mathfrak{z}$  we can introduce a generalised Fourier transform where – instead of integrating  $f(x)$  only against characters – we more generally consider all quasi-characters of positive exponent. This is made precise in the following definition.

**Definition 3.1.25** (Tate’s local  $\zeta$  function). Let  $f \in \mathfrak{z}$  and let  $c$  be a quasi-character of  $k^\times$  with strictly positive exponent. We set

$$\zeta(f, c) = \int_{k^\times} f(\alpha)c(\alpha) d\alpha$$

and call such a function a  $\zeta$ -function of  $k$ .

At least ‘locally’ (to be defined shortly), we can consider  $\zeta(f, c)$  as a holomorphic function. More precisely:

**Definition 3.1.26.** We say that two quasi-characters  $c_1, c_2$  are **equivalent** if there exists an unramified quasi-character  $\chi$  such that  $c_2(\alpha) = c_1(\alpha)\chi(\alpha)$ .

By Lemma 3.1.13, the equivalence class of the quasi-character  $c$  is given by the set of all quasi characters of the form

$$\alpha \mapsto c(\alpha)\|\alpha\|^s.$$

This allows us to consider a  $\zeta$  function of  $k$  as a collection of many functions of a complex variable  $s$ : for each quasi-character  $c$  of positive exponent, we can consider the function

$$s \mapsto \zeta(f, c \cdot \|\alpha\|^s).$$

Notice that, by Lemma 3.1.13, this function can (and should) be considered as being defined

1. on the whole complex plane, if  $v$  is archimedean;
2. on the cylinder  $\frac{\mathbb{C}}{\mathbb{Z} \cdot \frac{2\pi i}{\log \|N_{\mathfrak{p}}\|}}$ , if  $v$  is finite and corresponds to  $\mathfrak{p}$ .

Each of these functions turns out to be holomorphic, in the following sense.

**Lemma 3.1.27.** *For every quasi-character  $c$  of positive exponent, the function  $s \mapsto \zeta(f, c \cdot \|\alpha\|^s)$  is well-defined and holomorphic in  $\{\Re s > 0\}$ .*

*Proof.* Convergence of the integral is guaranteed by the fact that  $f(x)$  is a function of class  $\mathfrak{z}$ .

To show holomorphicity, it suffices to check that we can differentiate under the integral sign. By definition,

$$\zeta(f, c \cdot \|\alpha\|^s) = \int_{k^\times} f(\alpha)c(\alpha)\|\alpha\|^s d\alpha = \int_{k^+} f(x)c(x)\|x\|^{s-1} dx.$$

Fix a compact subset  $K$  of  $\{\Re s > 0\}$  with non-empty interior. The derivative (in  $s$ ) of the function being integrated is  $f(x)c(x) \log \|x\| \|x\|^{s-1}$ . For  $s \in K$ , this function is uniformly absolutely integrable: denoting by  $e$  the exponent of  $c$ , the integral of the absolute value is

$$\int_{k^+} |f(x)| \cdot |c(x)| \cdot |\log \|x\|| \cdot \|x\|^{s-1} dx = \int_{k^+} |f(x)| \cdot |\log \|x\|| \cdot \|x\|^{e+\Re s-1} dx$$

with  $\Re s$  bounded above and below. Convergence can only fail around 0 and as  $\|x\| \rightarrow \infty$ . Let  $C = \{x \in k^+ : \|x\| \leq 1\}$  be a compact neighbourhood of 0 in  $k^+$ . Splitting the integral as  $\int_C + \int_{k^+ \setminus C}$ , we have

$$\int_C |f(x)| \cdot |\log \|x\|| \cdot \|x\|^{e+\Re s-1} dx \leq \|f|_C\|_\infty \int_C |\log \|x\|| \cdot \|x\|^{e+\Re s-1} dx.$$

The exponent  $e + \Re s - 1$  is bounded below by a constant  $\kappa_0$  strictly larger than  $-1$  (since  $e > 0$  and  $\Re s \geq \min_{s \in K} \Re s > 0$ ). The integral  $\int_C |\log \|x\|| \cdot \|x\|^{\kappa_0} dx$  converges (Exercise 3.1.28).

As for the integral on  $k^+ \setminus C$ , we have

$$\int_{k^+ \setminus C} |f(x)| \cdot |\log \|x\|| \cdot \|x\|^{e+\Re s-1} dx \leq \int_{k^+ \setminus C} |f(x)| \cdot \|x\|^{e+\Re s} dx,$$

and for  $s \in K$  the exponent  $e + \Re s$  is bounded above by some  $\kappa_1 > 1$ , so that the function being integrated is dominated by the  $L^1$  function  $|f(x)| \cdot \|x\|^{\kappa_1}$ . Thus, thanks to the dominated convergence theorem we may in fact differentiate under the integral sign at any  $s$  in the interior of  $K$ . As  $K$  is arbitrary, this proves the desired holomorphicity.  $\square$

**Exercise 3.1.28.** Prove that  $\int_{\|x\| \leq 1} |\log \|x\|| \cdot \|x\|^\kappa dx$  converges for all local fields  $k$  and all  $\kappa > -1$ .

*Hint.* The cases  $k = \mathbb{R}$  and  $k = \mathbb{C}$  are easy exercises in analysis (but do pay attention to the fact that  $\|z\|$  is the *square* of the usual complex absolute value). For the  $p$ -adic case, reduce to summing over certain annuli  $A_v$  (see Remark 3.1.41 below if necessary).

Remarkably, all  $\zeta$  functions satisfy a functional equation of a very general type. To state it, we introduce the following notation:

**Definition 3.1.29.** For a quasi-character  $c$  we set  $\hat{c}(\alpha) = \|\alpha\|c^{-1}(\alpha)$ .

**Remark 3.1.30.** It is clear from the definitions that  $\sigma(\hat{c}) = 1 - \sigma(c)$ .

The following proposition, while comparatively easy to prove, will be the key to all subsequent results about analytic continuation and functional equations.

**Proposition 3.1.31** (Functional equation of local  $\zeta$  functions). *Let  $f, g \in \mathfrak{z}$ . For every quasi-character  $c$  with  $\sigma(c) \in (0, 1)$  we have*

$$\zeta(f, c)\zeta(\hat{g}, \hat{c}) = \zeta(\hat{f}, \hat{c})\zeta(g, c). \quad (3.3)$$

**Remark 3.1.32.** An equivalent (but perhaps easier to remember) way to state the proposition is that the ‘pairing’  $(f, g) \mapsto \zeta(f, c)\zeta(\hat{g}, \hat{c})$  is symmetric in  $f, g$ .

*Proof.* The condition  $\sigma(c) \in (0, 1)$  guarantees that both sides are well-defined. By definition,  $\hat{c}(\alpha) = \|\alpha\|c(\alpha)^{-1}$ , and so

$$\begin{aligned} \zeta(f, c)\zeta(\hat{g}, \hat{c}) &= \int_{k^\times \times k^\times} c(\alpha)f(\alpha)\hat{g}(\beta)\hat{c}(\beta) d\alpha d\beta = \int_{k^\times \times k^\times} c(\alpha)f(\alpha)\hat{g}(\beta)\|\beta\|c(\beta)^{-1} d\alpha d\beta \\ &= \int_{k^\times \times k^\times} c(\alpha\beta^{-1})f(\alpha)\hat{g}(\beta)\|\beta\| d\alpha d\beta. \end{aligned}$$

Replacing  $(\alpha, \beta) \rightarrow (\alpha, \alpha\beta)$ , which (by properties of the Haar measure) does not change  $d\alpha d\beta$ , we rewrite the above as

$$\int_{k^\times \times k^\times} c(\beta^{-1})f(\alpha)\hat{g}(\alpha\beta)\|\alpha\beta\| d\alpha d\beta.$$

We now express everything in terms of the additive measure on  $k^+$ . Recall from Definition 3.1.22 that  $d\alpha = \frac{d\mu_{k^+}(\alpha)}{\|\alpha\|}$ , up to multiplicative constants. Thus, again up to multiplicative constants independent of  $f, g$ , the above integral is equal to

$$\int_{k \times k} c(\beta^{-1})f(\alpha)\hat{g}(\alpha\beta)\|\alpha\beta\| \frac{1}{\|\alpha\|\|\beta\|} d\mu_{k^+}(\alpha) d\mu_{k^+}(\beta).$$

We finally replace  $\hat{g}$  with its definition (Theorem 3.1.10) to obtain

$$\int_{k \times k} \int_k g(x)e^{-2\pi i\Lambda(\alpha\beta x)}c(\beta^{-1})f(\alpha) d\mu_{k^+}(x) d\mu_{k^+}(\alpha) d\mu_{k^+}(\beta),$$

which is manifestly symmetric in  $f$  and  $g$ . □

The crucial remark is now the following: provided that  $\zeta(\hat{g}, \hat{c})$  and  $\zeta(\hat{f}, \hat{c})$  are not identically zero, Equation (3.3) can be written as

$$\frac{\zeta(f, c)}{\zeta(\hat{f}, \hat{c})} = \frac{\zeta(g, c)}{\zeta(\hat{g}, \hat{c})},$$

where the right-hand side is clearly independent of  $f$ . Hence, the left-hand side must *also* be independent of  $f$ , even though this is not at all obvious. This suggests that one should use the functional equation of Proposition 3.1.31 by letting  $g$  vary, while fixing  $f$  to be a simple enough function that the ratio  $\frac{\zeta(f, c)}{\zeta(\hat{f}, \hat{c})}$  can be evaluated exactly. We turn to the task of computing

$$\rho(c) := \frac{\zeta(f, c)}{\zeta(\hat{f}, \hat{c})}$$

in the next section, but first we establish some formal properties of the function  $\rho(c)$  that follow directly from the functional equation.

**Proposition 3.1.33.** 1.  $\rho(\hat{c}) = \frac{c(-1)}{\rho(c)}$

2.  $\rho(\bar{c}) = c(-1)\overline{\rho(c)}$

3.  $|\rho(c)| = 1$  for  $c$  of exponent  $1/2$ .

*Proof.* 1.  $\zeta(f, c) = \rho(c)\zeta(\hat{f}, \hat{c}) = \rho(c)\rho(\hat{c})\zeta(\hat{f}, \hat{c}) = \rho(c)\rho(\hat{c})\zeta(f(-\alpha), c)$ , where in the last step we used  $\hat{c} = c$  (by definition) and  $\hat{f} = f(-\alpha)$  (by Theorem 3.1.10). On the other hand, by definition,

$$\begin{aligned}\zeta(f, c) &= \int_{k^\times} f(\alpha)c(\alpha)d\alpha = \int_{k^\times} f(-\alpha)c(-\alpha)d(-\alpha) \\ &= c(-1) \int_{k^\times} f(-\alpha)c(\alpha)d(\alpha) = c(-1)\zeta(f(-\alpha), c).\end{aligned}$$

Comparing the two expressions for  $\zeta(f, c)$  we get  $\rho(c)\rho(\hat{c}) = c(-1)$ .

**Remark 3.1.34.** There seems to be a typo in Tate's proof of this relation.

2.  $\overline{\zeta(f, c)} = \zeta(\bar{f}, \bar{c}) = \rho(\bar{c})\zeta(\hat{\bar{f}}, \hat{\bar{c}})$ . Now observe that  $\hat{\bar{c}}(\alpha) = \|\alpha\|\overline{c(\alpha)}^{-1} = \bar{c}(\alpha)$ , while

$$\hat{\bar{f}}(\eta) = \int_{k^+} \overline{f(x)}e^{-2\pi i\Lambda(\eta x)} dx = \int_{k^+} \overline{f(x)e^{2\pi i\Lambda(\eta x)}} dx = \bar{f}(-\eta).$$

Replacing in  $\overline{\zeta(f, c)} = \rho(\bar{c})\zeta(\hat{\bar{f}}, \hat{\bar{c}})$  we get

$$\overline{\zeta(f, c)} = \rho(\bar{c})\zeta(\hat{\bar{f}}(-\eta), \bar{c}) = \rho(\bar{c})c(-1)\zeta(\hat{\bar{f}}, \bar{c}) = \rho(\bar{c})c(-1)\overline{\zeta(\hat{f}, \hat{c})},$$

where the last equality follows immediately from the definition of  $\zeta(f, c)$ . On the other hand,

$$\overline{\zeta(f, c)} = \overline{\rho(c)\zeta(\hat{f}, \hat{c})} = \overline{\rho(c)}\overline{\zeta(\hat{f}, \hat{c})}.$$

Comparing the two expressions yields the result.

3. If  $c$  has exponent  $1/2$ , then  $c(\alpha)\overline{c(\alpha)} = \|c(\alpha)\|^2 = \|\alpha\| = c(\alpha)\hat{c}(\alpha)$ , and therefore  $\bar{c} = \hat{c}$ . Comparing the expressions for  $\rho(\bar{c})$  and  $\rho(\hat{c})$  given in (1) and (2) yields  $\rho(c)\overline{\rho(c)} = 1$ .  $\square$

We will check in the next section that  $\rho(c)$  is a 'familiar' function, for all quasi-characters  $c$ , and in particular it trivially admits analytic continuation to  $\mathbb{C}$ . As a consequence, the local functional equation of Proposition 3.1.31 yields the following important theorem:

**Theorem 3.1.35.** *Any  $\zeta$ -function of  $k$  has an analytic continuation to the domain of all quasi-characters given by a functional equation of the form*

$$\zeta(f, c) = \rho(c)\zeta(\hat{f}, \hat{c}),$$

where  $\rho(c)$  is a meromorphic function of  $c$ .

*Proof.* By Lemma 3.1.27, the function  $\zeta(f, c)$  is defined and holomorphic for  $c$  of positive exponent. The function  $\rho(c)\zeta(\hat{f}, \hat{c})$  is similarly defined and meromorphic (since  $\rho(c)$  is only known to be meromorphic) for  $\hat{c}$  of positive exponent, that is, for  $c$  of exponent strictly less than 1.

In particular, both functions are defined and meromorphic for all  $0 < \text{exponent } c < 1$ , and they coincide in this domain by Proposition 3.1.31. Thus, we get meromorphic continuation of  $\zeta(f, c)$  to the domain of all quasi-characters.  $\square$

### 3.1.4 Local zeta functions II: computation of the local factors

Our objective in this section is to compute the function

$$\rho(c) := \frac{\zeta(f, c)}{\zeta(\hat{f}, \hat{c})}$$

when  $f$  is a particularly simple function taken in class  $\mathfrak{z}$ . We will organise the computation according to the equivalence class of the quasi-character  $c(\alpha) = c_0(\alpha)\|\alpha\|^s$ . For  $c$  in a fixed equivalence class, we will find that  $\rho(c)$ , seen as a function of the complex variable  $s$ , is holomorphic and non-vanishing for  $\Re s \in (0, 1)$ . These functions  $\rho(c)$  will form the basis of all of our discussion concerning the functional equations satisfied by the  $\zeta$  functions.

It will be necessary to distinguish cases according to whether  $k$  is real, complex, or  $p$ -adic. Following Tate, we begin each section by recalling our choices for the map  $\Lambda$ , for the norm on  $k$ , and for the Haar measures on  $k^+$  and on  $k^\times$ .

#### Real case

##### Conventions.

1.  $\Lambda(x) = -x \pmod{1}$
2.  $\|\alpha\|$  is the ordinary absolute value
3.  $d\mu_{k^+}(x) = dx$  is the ordinary Lebesgue measure
4.  $d\alpha = \frac{d\mu_{k^+}(\alpha)}{\|\alpha\|}$

**Equivalence classes of quasi-characters.** According to Lemma 3.1.13 and Proposition 3.1.17, there are two equivalence classes:

$$\alpha \mapsto \|\alpha\|^s \quad \text{and} \quad \alpha \mapsto (\text{sign } \alpha)\|\alpha\|^s.$$

We denote the former by  $\|\cdot\|^s$  and the latter by  $\pm\|\cdot\|^s$ .

**Choice of  $f$ .** We correspondingly take

$$f(x) = e^{-\pi x^2} \quad \text{and} \quad f_\pm(x) = x e^{-\pi x^2}. \quad (3.4)$$

**Fourier transforms.** We have

$$\hat{f}(x) = f(x) \quad \text{and} \quad \hat{f}_\pm(x) = i f_\pm(x).$$

Before we check these equalities, we pause to recall a classical lemma in real Fourier analysis:

**Lemma 3.1.36.** *Let  $a, b \in \mathbb{R}$ . We have*

$$\int_{\mathbb{R}} e^{-2\pi y^2 + 4\pi i a y} dy = \frac{e^{-2\pi a^2}}{\sqrt{2}}$$

and more generally

$$\int_{\mathbb{R}} e^{-2b\pi y^2 + 4\pi i a y} dy = \frac{1}{\sqrt{2b}} e^{-2\pi(a^2/b)}.$$

*Proof.* We have

$$\begin{aligned} \int_{\mathbb{R}} e^{-2\pi y^2 + 4\pi i a y} dy &= \int_{\mathbb{R}} e^{-2\pi(y^2 - 2i a y - a^2 + a^2)} dy \\ &= \int_{\mathbb{R}} e^{-2\pi(y - ia)^2 - 2\pi a^2} dy \\ &= e^{-2\pi a^2} \int_{\mathbb{R}} e^{-2\pi(y - ia)^2} dy. \end{aligned}$$

Since the function  $y \mapsto e^{-2\pi(y - ia)^2}$  is holomorphic, we can shift the integration contour from the real line  $\mathbb{R}$  to  $ia + \mathbb{R}$ , thus rewriting the above integral as

$$e^{-2\pi a^2} \int_{\mathbb{R}} e^{-2\pi y^2} dy.$$

The value  $I := \int_{\mathbb{R}} e^{-2\pi y^2} = \frac{1}{\sqrt{2}}$  is well-known, and can be obtained by the standard trick

$$I^2 = \int_{\mathbb{R}^2} e^{-2\pi(x^2 + y^2)} dx dy = \int_0^\infty \int_0^{2\pi} e^{-2\pi r^2} r dr d\vartheta = \frac{1}{2} \int_0^\infty e^{-2\pi r^2} d(2\pi r^2) = \frac{1}{2} \int_0^\infty e^{-t} dt = \frac{1}{2}.$$

This proves the first formula in the statement. The second follows: upon writing  $y = \frac{z}{\sqrt{b}}$  we obtain

$$\int_{\mathbb{R}} e^{-2b\pi y^2 + 4\pi i a y} dy = \int_{\mathbb{R}} e^{-2\pi z^2 + 4\pi i \frac{a}{\sqrt{b}} z} \frac{dz}{\sqrt{b}} = \frac{1}{\sqrt{2b}} e^{-2\pi(a^2/b)}.$$

□

Let us now compute  $\hat{f}(x)$ . By definition, recalling from Equation (3.2) the definition of the Fourier transform in our setting, we have

$$\hat{f}(x) = \int_{\mathbb{R}} f(y) e^{-2\pi i \Lambda(yx)} dy = \int_{\mathbb{R}} e^{-\pi y^2} e^{2\pi i y x} dy = e^{-\pi x^2},$$

where in the last step we used Lemma 3.1.36 with  $a = \frac{1}{2}x, b = \frac{1}{2}$ . For the sake of completeness, we also derive the expression for  $\hat{f}_\pm$ :

$$\begin{aligned} \hat{f}(x) &= \int_{\mathbb{R}} f(y) e^{-2\pi i \Lambda(yx)} dy = \int_{\mathbb{R}} y e^{-\pi y^2} e^{2\pi i y x} dy \\ &= \int_{\mathbb{R}} e^{-\pi x^2} y e^{-\pi(y - ix)^2} dy = e^{-\pi x^2} \int_{\mathbb{R}} y e^{-\pi(y - ix)^2} dy \\ &= e^{-\pi x^2} \int_{\mathbb{R}} (y + ix) e^{-\pi y^2} dy = ix e^{-\pi x^2} + \int_{\mathbb{R}} y e^{-\pi y^2} dy = ix e^{-\pi x^2}, \end{aligned}$$

where the integral  $\int_{\mathbb{R}} y e^{-\pi y^2} dy$  vanishes since we are summing a (rapidly decaying) odd function over a symmetric domain.

**Remark 3.1.37.** The same result can also be derived more cleanly by recalling that, writing  $g(x) = 2\pi i x f(x)$ , one has  $\frac{d\hat{f}(x)}{dx} = \hat{g}$ . Applying this to  $f(x)$  and  $g(x) = 2\pi i f_\pm(x)$  immediately yields

$$2\pi i \hat{f}_\pm = \frac{d}{dx} \left( e^{-\pi x^2} \right) = -2\pi x e^{-\pi x^2} \Rightarrow \hat{f}_\pm = ix e^{-\pi x^2} = i f_\pm(x).$$



**The  $\zeta$ -functions.** From the definitions we obtain

$$\begin{aligned}\zeta(f, \|\cdot\|^s) &= \int_{\mathbb{R}^*} f(\alpha) \|\alpha\|^s d\alpha = \int_{\mathbb{R}} e^{-\pi x^2} |x|^s \frac{dx}{|x|} \\ &= 2 \int_0^\infty x^{s-1} e^{-\pi x^2} dx \stackrel{y=x^2}{=} \int_0^\infty y^{(s-1)/2} e^{-\pi y} y^{-1/2} dy \\ &\stackrel{z=\pi y}{=} \frac{1}{\pi} \int_0^\infty \left(\frac{z}{\pi}\right)^{s/2-1} e^{-z} dz = \pi^{-s/2} \Gamma(s/2).\end{aligned}$$

**Remark 3.1.38.** Note that we have essentially interpreted the  $\Gamma$  function as a  $\zeta$  function of  $\mathbb{R}$ ! Furthermore, notice that this exact function  $\pi^{-s/2} \Gamma(s/2)$  is precisely the ‘missing factor’ from the completed  $\zeta$  function of Remark 1.1.10. This already strongly suggests that Tate’s local  $\zeta$  functions should have something to do with the ‘global’ Dedekind  $\zeta$  function we met at the beginning of the course.

A similar calculation leads to

$$\begin{aligned}\zeta(f_\pm, \pm\|\cdot\|^s) &= \int_{-\infty}^0 -x e^{-\pi x^2} |x|^s \frac{dx}{|x|} + \int_0^\infty x e^{-\pi x^2} |x|^s \frac{dx}{|x|} \\ &= 2 \int_0^\infty x^s e^{-\pi x^2} dx = \pi^{-\frac{s+1}{2}} \Gamma\left(\frac{s+1}{2}\right).\end{aligned}$$

Now note that  $\widehat{\|\cdot\|^s} = \|\cdot\|^{1-s}$  and  $\widehat{\pm\|\cdot\|^s} = \pm\|\cdot\|^{1-s}$ . Combined with the linearity of  $\zeta(f, c)$  in the first argument, this shows

$$\begin{aligned}\zeta(\hat{f}, \widehat{\|\cdot\|^s}) &= \zeta(f, \|\cdot\|^{1-s}) = \pi^{-\frac{1-s}{2}} \Gamma\left(\frac{1-s}{2}\right), \\ \zeta(\hat{f}_\pm, \widehat{\pm\|\cdot\|^s}) &= \zeta(if_\pm, \pm\|\cdot\|^{1-s}) = i\pi^{-\frac{(1-s)+1}{2}} \Gamma\left(\frac{(1-s)+1}{2}\right).\end{aligned}$$

**The function  $\rho(c)$ .** We have obtained

$$\begin{aligned}\rho(\|\cdot\|^s) &= \frac{\pi^{-s/2} \Gamma\left(\frac{s}{2}\right)}{\pi^{-\frac{1-s}{2}} \Gamma\left(\frac{1-s}{2}\right)} = 2^{1-s} \pi^{-s} \cos\left(\frac{\pi s}{2}\right) \Gamma(s) \\ \rho(\pm\|\cdot\|^s) &= i \frac{\pi^{-\frac{s+1}{2}} \Gamma\left(\frac{s+1}{2}\right)}{\pi^{-\frac{(1-s)+1}{2}} \Gamma\left(\frac{(1-s)+1}{2}\right)} = -i 2^{1-s} \pi^{-s} \sin\left(\frac{\pi s}{2}\right) \Gamma(s).\end{aligned}$$

**Exercise 3.1.39.** Check the funny-looking identities above, using the results of Exercise 1.1.6 (including Euler’s reflection formula).

**Complex case**

**Conventions.**

1.  $\xi = x + iy = r e^{i\theta}$
2.  $\Lambda(\xi) = -2\Re(\xi) = -2x$

3.  $\|\alpha\| = \alpha\bar{\alpha} = |\alpha|^2 = r^2$  is the square of the ordinary absolute value
4.  $d\mu_{k^+}(\xi) = 2 dx dy$  is twice the ordinary Lebesgue measure
5.  $d\alpha = \frac{d\mu_{k^+}(\alpha)}{|\alpha|^2}$

**Equivalence classes of quasi-characters.** According to Lemma 3.1.13 and Proposition 3.1.17, the equivalence classes are parametrised by  $n \in \mathbb{Z}$ . Representatives for each equivalence class are given by

$$c_n(re^{i\vartheta}) = e^{in\vartheta},$$

and the corresponding equivalence class consists of all characters of the form  $c_n(\alpha)\|\alpha\|^s$ .

**Choice of  $f$ .** We take

$$f_n(\xi) = \begin{cases} (x - iy)^{|n|} e^{-2\pi(x^2+y^2)}, & \text{for } n \geq 0 \\ (x + iy)^{|n|} e^{-2\pi(x^2+y^2)}, & \text{for } n < 0 \end{cases} \quad (3.5)$$

Notice that, writing  $\alpha = re^{i\vartheta} \neq 0$ , the value  $f_n(\alpha)$  (for  $n \geq 0$ ) can also be written as

$$(r(\cos \vartheta - i \sin \vartheta))^n e^{-2\pi r^2} = r^n e^{-in\vartheta} e^{-2\pi r^2},$$

while for  $n \leq 0$  we have

$$f_n(\alpha) = (r(\cos \vartheta + i \sin \vartheta))^{-n} e^{-2\pi r^2} = r^{-n} e^{-in\vartheta} e^{-2\pi r^2}.$$

We may thus write the uniform formula  $f_n(re^{i\vartheta}) = r^{|n|} e^{-in\vartheta} e^{-2\pi r^2}$ .

**Fourier transforms.** We have

$$\hat{f}_n(\xi) = i^{|n|} f_{-n}(\xi)$$

for all  $n$ . To prove this we proceed as follows:

1. for  $n = 0$  we compute

$$\hat{f}_0(\xi) = \int_{\mathbb{C}} f(\eta) e^{-2\pi i \Lambda(\eta\xi)} d_{k^+}(\eta) = 2 \int_{\mathbb{R}^2} e^{-2\pi(x^2+y^2)} e^{4\pi i \Re(\xi(x+iy))} dx dy.$$

Writing  $\xi = u + iv$ , the previous integral becomes

$$\begin{aligned} \hat{f}_0(\xi) &= 2 \int_{\mathbb{R}^2} e^{-2\pi(x^2+y^2)} e^{4\pi i(ux-bv)} dx dy = 2 \left( \int_{\mathbb{R}} e^{-2\pi x^2 + 4\pi i u x} dx \right) \left( \int_{\mathbb{R}} e^{-2\pi y^2 - 4\pi i v y} dy \right) \\ &= 2 \left( \frac{e^{-2\pi u^2}}{\sqrt{2}} \right) \left( \frac{e^{-2\pi v^2}}{\sqrt{2}} \right) = e^{-2\pi(u^2+v^2)} = f_0(u + iv) = f_0(\xi), \end{aligned}$$

where the single real integrals are treated using the first part of Lemma 3.1.36 (with  $a = u$  and  $a = -v$ , respectively).

2. for  $n \geq 0$  we proceed by induction. Assume that we know  $\widehat{f}_n(\xi) = i^{|n|} f_{-n}(\xi)$ , that is,

$$2 \int_{\mathbb{R}} \int_{\mathbb{R}} (u - iv)^n e^{-2\pi(u^2+v^2)+4\pi i(xu-yv)} du dv = i^n (x + iy)^n e^{-2\pi(x^2+y^2)}. \quad (3.6)$$

Introduce the differential operator  $D = \frac{1}{4\pi i} \left( \frac{\partial}{\partial x} + i \frac{\partial}{\partial y} \right)$  and observe that  $D(x + iy) = 0$ , hence  $D(x + iy)^n = 0$  (this is essentially a consequence of the Cauchy-Riemann equation for the analytic function  $z \mapsto z^n$ ). Applying  $D$  to both sides of (3.6) we obtain

$$2 \int_{\mathbb{R}} \int_{\mathbb{R}} (u - iv)^{n+1} e^{-2\pi(u^2+v^2)+4\pi i(xu-yv)} du dv = i^{n+1} (x + iy)^{n+1} e^{-2\pi(x^2+y^2)},$$

which is nothing but the equality  $\widehat{f_{n+1}}(\xi) = i^{n+1} f_{-(n+1)}(\xi)$ .

3. finally, to handle the case  $n < 0$ , we write  $n = -m$  with  $m \geq 0$  and consider the equality

$$\widehat{f_m}(\xi) = i^n f_{-m}(\xi).$$

Taking the Fourier transform of both sides, we get

$$f_m(-\xi) = \widehat{\widehat{f_m}}(\xi) = i^m \widehat{f_{-m}}(\xi),$$

which, using  $f_m(-\xi) = (-1)^m f_m(\xi)$ , yields the desired equality.

**The  $\zeta$ -functions.** Recall the formula  $f_n(re^{i\vartheta}) = r^{|n|} e^{-in\vartheta} e^{-2\pi r^2}$ . From this, we obtain

$$\begin{aligned} \zeta(f_n, c_n \| \cdot \| ^s) &= \int_{\mathbb{C}^\times} f(\alpha) c_n(\alpha) \|\alpha\|^s d\alpha = \int_{\mathbb{C}} r^{|n|} e^{-in\vartheta} e^{-2\pi r^2} e^{in\vartheta} r^{2s} \frac{2dx dy}{r^2} \\ &= \int_0^\infty \int_0^{2\pi} r^{|n|+2s-2} e^{-2\pi r^2} 2r dr d\vartheta = 2\pi \int_0^\infty (r^2)^{\frac{|n|+2s-2}{2}} e^{-2\pi r^2} d(r^2) \\ &= 2\pi \int_0^\infty t^{\frac{|n|}{2}+(s-1)} e^{-2\pi t} dt = 2\pi \int_0^\infty \left(\frac{u}{2\pi}\right)^{\frac{|n|}{2}+(s-1)} e^{-u} \frac{du}{2\pi} \\ &= (2\pi)^{-\frac{|n|}{2}+(1-s)} \int_0^\infty u^{\frac{|n|}{2}+(s-1)} e^{-u} du = (2\pi)^{-\frac{|n|}{2}+(1-s)} \Gamma\left(s + \frac{|n|}{2}\right). \end{aligned}$$

We highlight two aspects of this calculation that are easy to get wrong: on the one hand, recall that our Haar measure is *twice* the standard Lebesgue measure, which justifies the factor of 2 in front of  $dx dy$ , hence the factor of 2 in  $2r dr d\vartheta$ . On the other hand, note  $\|\alpha\|^s = r^{2s}$  (and not  $r^s$ ).

**Remark 3.1.40.** Speaking of getting computations wrong: Tate finds  $(2\pi)^{\frac{|n|}{2}+(1-s)} \Gamma\left(s + \frac{|n|}{2}\right)$  instead (note the sign change in  $\frac{|n|}{2}$ ). I double-checked my computations and could not find the mistake, but I'm ready to wager that Tate is right and I'm wrong. If you can find the error, I'd be happy to hear about it!

(Luckily, the sign in question is irrelevant for the computation of  $\rho(c)$ .)

Now note that  $\widehat{c_n \| \cdot \| ^s} = c_{-n} \| \cdot \|^{1-s}$ , so

$$\zeta(\widehat{f_n}, \widehat{c_n \| \cdot \| ^s}) = \zeta(i^{|n|} f_{-n}, c_{-n} \| \cdot \|^{1-s}) = i^{|n|} (2\pi)^{-\frac{|n|}{2}+s} \Gamma\left(1 - s + \frac{|n|}{2}\right).$$

**The function  $\rho(c)$ .** We simply take the ratio of the functions computed above to get

$$\rho(c_n \|\cdot\|^s) = (-i)^{|n|} \frac{(2\pi)^{1-s} \Gamma\left(s + \frac{|n|}{2}\right)}{(2\pi)^s \Gamma\left((1-s) + \frac{|n|}{2}\right)}.$$

**$p$ -adic case**

**Conventions.**

1.  $\xi$  is a  $p$ -adic variable
2.  $\Lambda(\xi) = \lambda(\mathrm{tr}_{k/\mathbb{Q}_p}(\xi))$
3.  $d\mu_{k^+}(\xi)$  is normalised in such a way that  $\mathcal{O}$  has measure  $(N\mathfrak{d})^{-1/2}$
4.  $\alpha = \tilde{\alpha}\pi^n$ , where  $\alpha$  is a variable in  $k^\times$ ,  $\pi$  is a uniformiser, and  $\tilde{\alpha}$  is a unit
5.  $\|\alpha\| = (N\mathfrak{p})^{-n}$
6.  $d\mu_{k^\times}(\alpha) = \frac{N\mathfrak{p}}{N\mathfrak{p}-1} \frac{d\mu_{k^+}(\alpha)}{\|\alpha\|}$ , so that  $\mathbf{u}$  gets measure  $(N\mathfrak{d})^{-1/2}$

**Equivalence classes of quasi-characters.** The classification of quasi-characters is complicated (see Proposition 3.1.17). Luckily, for the computation of the local  $\zeta$  function we only need to know the **conductor** of our character (that is, the minimal  $n \geq 0$  such that  $c$  is trivial on the subgroup<sup>2</sup>  $(1 + \mathfrak{p}^n) \cap \mathbf{u}$  of  $\mathbf{u}$ ). Also note that each equivalence class of characters contains a representative for which  $c(\pi) = 1$ . Let then  $c_n$  be a character such that

$$c(\pi) = 1, \quad c(1 + \mathfrak{p}^n) = \{1\}, \quad c(1 + \mathfrak{p}^{n-1}) \neq \{1\} \text{ if } n \geq 1.$$

**Choice of  $f$ .** We take  $f$  to depend only on the conductor. Precisely, we set

$$f_n(\xi) = \begin{cases} e^{2\pi i \Lambda(\xi)}, & \text{if } \xi \in \mathfrak{d}^{-1} \mathfrak{p}^{-n} \\ 0, & \text{otherwise} \end{cases} \quad (3.7)$$

Notice that for  $n = 0$  the function  $f_0(\xi)$  is the characteristic function of  $\mathfrak{d}^{-1}$  (for  $\xi \in \mathfrak{d}^{-1}$  we have  $\Lambda(\xi) = 0$ ).

**Fourier transforms.** We claim that

$$\hat{f}_n(\xi) = \begin{cases} (N\mathfrak{d})^{1/2} (N\mathfrak{p})^n, & \text{if } \xi \equiv 1 \pmod{\mathfrak{p}^n} \\ 0, & \text{if } \xi \not\equiv 1 \pmod{\mathfrak{p}^n}. \end{cases} \quad (3.8)$$

By definition,

$$\hat{f}_n(\xi) = \int_k f_n(\eta) e^{-2\pi i \Lambda(\xi\eta)} d\eta = \int_k e^{2\pi i \Lambda(\eta)} \mathbf{1}_{\eta \in \mathfrak{d}^{-1} \mathfrak{p}^{-n}} e^{-2\pi i \Lambda(\xi\eta)} d\eta = \int_{\mathfrak{d}^{-1} \mathfrak{p}^{-n}} e^{-2\pi i \Lambda((\xi-1)\eta)} d\eta.$$

<sup>2</sup>note that for  $n \geq 1$  the set  $1 + \mathfrak{p}^n$  is contained in  $\mathbf{u}$  and is a subgroup. For  $n = 0$ , we set conventionally  $1 + \mathfrak{p}^0 = \mathbf{u}$ .

If  $\xi \equiv 1 \pmod{\mathfrak{p}^n}$ , then  $(\xi - 1)\eta$  lies in  $\mathfrak{d}^{-1}$  for every  $\eta \in \mathfrak{d}^{-1}\mathfrak{p}^{-n}$ . By definition of the different, we have  $\text{tr}_{k/\mathbb{Q}_p}(\mathfrak{d}^{-1}) \subseteq \mathbb{Z}_p$ , which implies  $\Lambda((\xi - 1)\eta) = 0$ . Thus, if  $\xi \equiv 1 \pmod{\mathfrak{p}^n}$ , the function that is integrated is identically equal to 1, hence we get the measure of the set over which we are integrating, that is,

$$\mu_{k^+}(\mathfrak{d}^{-1}\mathfrak{p}^{-n}) = (N\mathfrak{p})^n (N\mathfrak{d})^{1/2},$$

where we have used Remark 3.1.8.

On the other hand, suppose that  $\xi \not\equiv 1 \pmod{\mathfrak{p}^n}$ . Then (by definition of conductor) the map  $\eta \mapsto \Lambda((\xi - 1)\eta)$  is a non-trivial character of the group  $\mathfrak{d}^{-1}\mathfrak{p}^{-n}$ , hence its integral over this (compact) group vanishes by Proposition 2.2.5.

**The  $\zeta$ -functions.** Let again  $c$  be a character of conductor  $\pi^n$  that satisfies  $c(\pi) = 1$ . We begin by computing the  $\zeta$  function in case  $c$  is unramified, that is,  $n = 0$ . In this case, the conditions  $c(\pi) = 1$  and  $c(\mathbf{u}) = \{1\}$  force  $c$  to be trivial, and its equivalence class is the class of the powers of the norm,  $\|\cdot\|^s$ . The local  $\zeta$  function is then

$$\zeta(f_0, \|\cdot\|^s) = \int_{k^\times} f_0(\alpha) \|\alpha\|^s d_{k^\times}(\alpha) = \int_{\mathfrak{d}^{-1}} e^{2\pi i \Lambda(\alpha)} \|\alpha\|^s d_{k^\times}(\alpha).$$

Next, we observe that  $\Lambda(\alpha) \in \mathbb{Z}_p$  for  $\alpha \in \mathfrak{d}^{-1}$ , hence the integral reduces to

$$\int_{\mathfrak{d}^{-1}} \|\alpha\|^s d_{k^\times}(\alpha).$$

Writing  $\mathfrak{d} = \pi^d$ , we have

$$\mathfrak{d}^{-1} = \bigsqcup_{v=-d}^{\infty} \{x \in k : \|x\| = (N\mathfrak{p})^{-v}\}.$$

Further set  $A_v := \{x \in k : \|x\| = (N\mathfrak{p})^{-v}\}$ .

**Remark 3.1.41.** Since  $\mu_{k^\times}$  is invariant under rescaling by elements of  $k^\times$  (that's the point of the Haar measure!), we have  $\mu_{k^\times}(A_v) = \mu_{k^\times}(\pi^v \mathbf{u}) = \mu_{k^\times}(\mathbf{u}) = (N\mathfrak{d})^{-1/2}$  for all  $v$ .

Using this remark we easily obtain

$$\begin{aligned} \int_{\mathfrak{d}^{-1}} \|\alpha\|^s d_{\mu_{k^\times}}(\alpha) &= \sum_{v=-d}^{\infty} \int_{A_v} \|\alpha\|^s d_{\mu_{k^\times}}(\alpha) = \sum_{v=-d}^{\infty} \int_{A_v} (N\mathfrak{p})^{-vs} d_{\mu_{k^\times}}(\alpha) \\ &= \sum_{v=-d}^{\infty} (N\mathfrak{p})^{-vs} \mu_{k^\times}(A_v) = (N\mathfrak{d})^{-1/2} \frac{(N\mathfrak{p})^{ds}}{1 - (N\mathfrak{p})^{-s}}. \end{aligned}$$

Finally, recalling that  $\mathfrak{d} = \mathfrak{p}^d$  has norm  $(N\mathfrak{p})^d$ , the result may be rewritten as

$$\zeta(f_0, \|\cdot\|^s) = \frac{(N\mathfrak{d})^{s-1/2}}{1 - (N\mathfrak{p})^{-s}}. \tag{3.9}$$

Now for the Fourier transform  $\hat{f}_0$ : we have computed above that this is  $(N\mathfrak{d})^{1/2}\mathbf{1}_{\mathcal{O}}$ , hence

$$\begin{aligned}\zeta(\hat{f}_0, \widehat{\|\cdot\|^s}) &= \zeta(\hat{f}_0, \|\cdot\|^{1-s}) = (N\mathfrak{d})^{1/2} \int_{\mathcal{O}} \|\alpha\|^{1-s} d\mu_{k^\times}(\alpha) \\ &= (N\mathfrak{d})^{1/2} \sum_{v \geq 0} (N\mathfrak{p})^{-v(1-s)} \mu_{k^\times}(A_v) \\ &= (N\mathfrak{d})^{1/2} \sum_{v \geq 0} (N\mathfrak{p})^{-v(1-s)} \mu_{k^\times}(A_v) = \frac{1}{1 - (N\mathfrak{p})^{s-1}},\end{aligned}$$

where we have used again Remark 3.1.41. More generally, essentially by the same computation one shows:

**Theorem 3.1.42.** *Let  $\chi$  be an unramified character of  $k^\times$  (so that  $\chi(u \cdot \pi^v) = \chi(\pi)^v$  for all  $v$  and all  $u \in \mathfrak{u}$ ; we may then evaluate  $\chi$  on any fractional ideal  $(\pi^v)$ ). Let  $f$  be the characteristic function of the fractional ideal  $I = (\pi^n)$ . The local  $\zeta$  function  $\zeta(f, \chi)$  is given by*

$$\zeta(f, \chi) = \frac{(N\mathfrak{d})^{-1/2} \chi(I) (NI)^{-s}}{1 - \chi(\mathfrak{p}) (N\mathfrak{p})^{-s}}.$$

**Exercise 3.1.43.** Check Theorem 3.1.42.

**Remark 3.1.44.** It should be almost unnecessary to point out that if we take  $k = \mathbb{Q}_p$  and  $I = (1)$  in Theorem 3.1.42 we get that the local zeta function  $\zeta(f, \chi)$  looks very much like the local factor at  $p$  of the classical Dirichlet  $L$ -functions (see Equation (1.1)). We will clarify the connection later, when we discuss global zeta functions.

We are left with computing the local zeta functions of ramified characters. Write the different as  $\mathfrak{d} = \mathfrak{p}^d$ . We start by decomposing the integral defining  $\zeta$  as a sum over the annuli  $A_v$ :

$$\zeta(f_n, c_n \|\cdot\|^s) = \int_{\mathfrak{d}^{-1}\mathfrak{p}^{-n}} e^{2\pi i \Lambda(\alpha)} c_n(\alpha) \|\alpha\|^s d\mu_{k^\times}(\alpha) = \sum_{v=-d-n}^{\infty} (N\mathfrak{p})^{-vs} \int_{A_v} e^{2\pi i \Lambda(\alpha)} c_n(\alpha) d\mu_{k^\times}(\alpha).$$

Next, we observe that all but one of the terms in this sum actually vanish:

**Lemma 3.1.45.** *For every  $v > -d - n$  we have  $\int_{A_v} e^{2\pi i \Lambda(\alpha)} c_n(\alpha) = 0$ .*

*Proof.* We distinguish two cases:

1.  $v \geq -d$ . In this case  $A_v \subseteq \mathfrak{d}^{-1}$ , hence  $\Lambda(\alpha) \in \mathbb{Z}_p$  for all  $\alpha \in A_v$  by definition of the different. It follows that  $e^{2\pi i \Lambda(\alpha)} = 1$  on all of  $A_v$ , and the integral in question is

$$\begin{aligned}\int_{A_v} c_n(\alpha) d\mu_{k^\times}(\alpha) &= \int_{\pi^v \mathfrak{u}} c_n(\alpha) d\mu_{k^\times}(\alpha) = \int_{\mathfrak{u}} c_n(\pi^v \alpha) d\mu_{k^\times}(\alpha) \\ &= c_n(\pi)^v \int_{\mathfrak{u}} c_n(\alpha) d\mu_{k^\times}(\alpha) = 0\end{aligned}$$

by Proposition 2.2.5 (notice that  $c_n$ , being ramified, is by definition nontrivial on  $\mathfrak{u}$ ).

2.  $-d > v > -d - n$ . We write  $A_v$  as the disjoint union of sets of the form  $\alpha_0 + \mathfrak{p}^{-d} = \alpha_0(1 + \mathfrak{p}^{-d-v})$ . On each such set,  $\Lambda$  is constant and equal to  $\Lambda(\alpha_0)$ . It follows that

$$\int_{\alpha_0 + \mathfrak{d}^{-1}} e^{2\pi i \Lambda(\alpha)} c_n(\alpha) d\mu_{k \times}(\alpha) = e^{2\pi i \Lambda(\alpha_0)} \int_{\alpha_0 + \mathfrak{d}^{-1}} c_n(\alpha) d\mu_{k \times}(\alpha).$$

We now prove that the last integral is zero. Translating (multiplicatively) by  $\alpha_0$  shows that

$$\begin{aligned} \int_{\alpha_0 + \mathfrak{d}^{-1}} c_n(\alpha) d\mu_{k \times}(\alpha) &= \int_{\alpha_0(1 + \mathfrak{p}^{-v-d})} c_n(\alpha) d\mu_{k \times}(\alpha) \\ &= \int_{1 + \mathfrak{p}^{-v-d}} c_n(\alpha_0 \alpha) d\mu_{k \times}(\alpha) \\ &= c_n(\alpha_0) \int_{1 + \mathfrak{p}^{-v-d}} c_n(\alpha) d\mu_{k \times}(\alpha). \end{aligned}$$

Since  $-v - d > 0$  by assumption,  $1 + \mathfrak{p}^{-v-d}$  is a (compact) subgroup of  $\mathfrak{u}$ . On the other hand,  $c_n(\alpha)$  is nontrivial on it, because by definition of the conductor the smallest exponent  $k$  such that  $c_n$  is trivial on  $1 + \mathfrak{p}^k$  is  $k = n$ , and  $-v - d < n$  by assumption. We conclude once again by applying Proposition 2.2.5. □

Thus, the local zeta function is given simply by

$$\zeta(f_n, c_n \|\cdot\|^s) = (N\mathfrak{p})^{(d+n)s} \int_{A_{-d-n}} e^{2\pi i \Lambda(\alpha)} c_n(\alpha) d\mu_{k \times}(\alpha).$$

As is usual in the  $p$ -adic setting, we can use the fact that the functions we integrate are locally constant to rewrite the remaining integral as a finite sum. More precisely, fix a set  $\{\varepsilon\}$  of representatives for the quotient  $\mathfrak{u}/(1 + \mathfrak{p}^n)$ . Then

$$A_{-d-n} = \mathfrak{u}\pi^{-d-n} = \bigsqcup_{\varepsilon} \varepsilon\pi^{-d-n}(1 + \mathfrak{p}^n) = \bigsqcup_{\varepsilon} (\varepsilon\pi^{-d-n} + \mathfrak{d}^{-1}).$$

On each set  $\varepsilon\pi^{-d-n}(1 + \mathfrak{p}^n)$  the character  $c_n$  is constant by definition of  $n$ , and its value is  $c_n(\varepsilon)c_n(\pi)^{-d-n} = c_n(\varepsilon)$  (recall that we chose our representatives  $c_n$  to satisfy  $c_n(\pi) = 1$ ). Similarly,  $\Lambda$  is also constant and equal to  $\Lambda(\varepsilon\pi^{-d-n})$ . Thus,

$$\zeta(f_n, c_n \|\cdot\|^s) = (N\mathfrak{p})^{s(d+n)} \sum_{\varepsilon} c_n(\varepsilon) e^{2\pi i \Lambda(\varepsilon\pi^{-d-n})} \int_{1 + \mathfrak{p}^n} d\mu_{k \times}(\alpha).$$

Finally, we compute the local zeta functions attached to the Fourier transforms of the  $f_n$  for  $n > 0$ . We have already seen in Equation (3.8) that the Fourier transform of  $f_n$  is  $(N\mathfrak{d})^{1/2}(N\mathfrak{p})^n \mathbf{1}_{1 + \mathfrak{p}^n}$ . On the set  $1 + \mathfrak{p}^n$ , both  $c_n(\alpha)^{-1}$  and  $\|\alpha\|^{1-s}$  are equal to 1 (here we use  $n > 0$ ), and therefore

$$\zeta(\widehat{f_n}, \widehat{c_n \|\cdot\|^s}) = (N\mathfrak{d})^{1/2}(N\mathfrak{p})^n \int_{1 + \mathfrak{p}^n} d\mu_{k \times}(\alpha),$$

which is simply a constant.

**The function  $\rho(c)$ .** For the unramified character  $c_0$  we get

$$\rho(c\|\cdot\|^s) = (N\mathfrak{d})^{s-1/2} \frac{1 - (N\mathfrak{p})^{s-1}}{1 - (N\mathfrak{p})^{-s}}.$$

The situation is slightly more complicated for a ramified character  $c$  of conductor  $\mathfrak{f} = \mathfrak{p}^n$ . Let  $\{\varepsilon\}$  be a set of representatives for the quotient  $\mathfrak{u}/(1 + \mathfrak{f})$  and set

$$\rho_0(c) = (N\mathfrak{f})^{-1/2} \sum_{\varepsilon} c(\varepsilon) e^{2\pi i \Lambda(\varepsilon/\pi^v(\mathfrak{d}))}.$$

The function  $\rho(c)$  is then given by

$$\begin{aligned} \rho(c\|\cdot\|^s) &= \frac{(N\mathfrak{p})^{s(d+n)} \sum_{\varepsilon} c_n(\varepsilon) e^{2\pi i \Lambda(\varepsilon\pi^{-d-n})} \int_{1+\mathfrak{p}^n} d\mu_{k^\times}(\alpha)}{(N\mathfrak{d})^{1/2} (N\mathfrak{p})^n \int_{1+\mathfrak{p}^n} d\mu_{k^\times}(\alpha)} \\ &= \rho_0(c) \frac{(N\mathfrak{p})^{s(d+n)} (N\mathfrak{f})^{1/2}}{(N\mathfrak{d})^{1/2} (N\mathfrak{p})^n} = \rho_0(c) (N\mathfrak{p})^{(s-1/2)(d+n)} \\ &= \rho_0(c) (N\mathfrak{d}\mathfrak{f})^{s-1/2}, \end{aligned}$$

where we have used the definitions  $\mathfrak{d} = \mathfrak{p}^d$ ,  $\mathfrak{f} = \mathfrak{p}^n$ . Setting  $s = \frac{1}{2}$  we obtain  $\rho(c\|\cdot\|^s) = \rho_0(c)$ , which – using Proposition 3.1.33 (3) – shows the nontrivial fact that  $|\rho_0(c)| = 1$ .

### A final remark

We conclude this section with a remark that will be useful when we discuss the ‘global’ theory over number fields.

**Remark 3.1.46** (Non-vanishing of the standard local  $\zeta$  functions). For each character  $c$  of the multiplicative group  $k^\times$  of a local field  $k$ , we have constructed a ‘standard’ function  $f$  (depending on  $c$ ) and computed  $\zeta(f, c)$ . One can check directly that all these local zeta functions are meromorphic and everywhere non-vanishing. (The  $\Gamma$  function has no zeroes, see Exercise 1.1.6). In particular, their *inverses* are everywhere holomorphic.

## 3.2 The global theory

We now let  $k$  be a number field, denote by  $v$  a place of  $k$  (Definition 2.3.1), and by  $k_v$  the corresponding completion. For each  $v$  we then have all the analogues of the quantities defined in the previous section, which we decorate with a subscript  $v$ : the ring of integers  $\mathcal{O}_v$ , the units  $\mathfrak{u}_v$ , the norm  $\|\cdot\|_v$ , the character  $\Lambda_v$ , the different  $\mathfrak{d}_v$  if  $v$  is finite, etc.

### 3.2.1 The additive group: the adèles

Recall from Definition 2.4.5 the notion of ring of adèles, which we consider in the topological sense of Definition 2.4.7. Thus, as a topological group,  $\mathbb{A}_k$  is  $\prod'_v (k_v^+, \mathcal{O}_v)$ . The ring structure is provided by the component-wise multiplication.

Theorem 2.4.14, combined with Theorem 3.1.5 and Lemma 3.1.6, shows that the dual group of  $\mathbb{A}_k$  is the restricted direct product of the groups  $\widehat{k_v^+} \cong k_v^+$  with respect to the subgroups  $\mathfrak{d}_v^{-1}$



(for  $v$  finite). Since  $\mathfrak{d}_v^{-1} = \mathcal{O}_v$  for almost all  $v$ , this shows that the dual group is simply  $\mathbb{A}_k$  itself. More precisely, an adèle  $(\eta_v) \in \mathbb{A}_k$  corresponds to the character

$$(x_v) \mapsto \prod_v e^{2\pi i \Lambda_v(\eta_v x_v)} = e^{2\pi i \sum_v \Lambda_v(\eta_v x_v)}.$$

It is then useful to define the **standard adèlic character**

$$\Lambda((x_v)) = \sum_v \Lambda_v(x_v). \tag{3.10}$$

Since we also have a local measure  $d\mu_{k_v^+}$  for each place  $v$ , from the discussion in Section 2.4.4 we get a product measure  $d\mu_{\mathbb{A}_k} = \prod_v d\mu_{k_v^+}$  on  $\mathbb{A}_k$ . Moreover, since each  $d\mu_{k_v^+}$  is self-dual for the Fourier transform (see Theorem 3.1.10), we obtain from Corollary 2.4.23 that  $d\mu_{\mathbb{A}_k}$  is also self-dual. Thus, the abstract general theory leads to the following:

**Theorem 3.2.1** (Fourier inversion on the adèles). *The additive group of adèles  $\mathbb{A}_k$  is its own character group. An isomorphism is obtained by identifying the adèle  $(\eta_v)$  with the character  $(x_v) \mapsto e^{2\pi i \Lambda(\eta x)}$ . If for a function  $f(x) \in L^1(\mathbb{A}_k)$  we define the Fourier transform by the formula*

$$\hat{f}(\eta) = \int_{\mathbb{A}_k} f(x) e^{-2\pi i \Lambda(\eta x)} d\mu_{\mathbb{A}_k}(x),$$

then for  $f \in \mathfrak{V}^1(\mathbb{A}_k)$  we have the inversion formula

$$f(x) = \int_{\mathbb{A}_k} \hat{f}(\eta) e^{2\pi i \Lambda(x\eta)} d\mu_{\mathbb{A}_k}(\eta).$$

We also recall the following fact (see Exercise 2.4.6):

**Lemma 3.2.2.** *The unit group of  $\mathbb{A}_k$  is  $I_k$ , the group of idèles of  $k$ . In particular, for  $\eta = (\eta_v) \in \mathbb{A}_k$ , the map  $x \mapsto \eta x$  of  $\mathbb{A}_k$  into itself is an automorphism if and only if  $\eta$  is an idèle.*

The following is the analogue of Lemma 3.1.7.

**Lemma 3.2.3** (Rescaling the adèlic Haar measure). *Let  $a$  be an idèle of  $k$ . We have*

$$d\mu_{\mathbb{A}_k}(ax) = \|a\| d\mu_{\mathbb{A}_k}(x),$$

where  $\|a\|$  is the product  $\prod_v \|a_v\|_v$  (the product is finite, in the sense that all but finitely many terms are equal to 1).

*Proof.* Since  $d\mu_{\mathbb{A}_k}(x)$  is a Haar measure and  $x \mapsto ax$  is a ring automorphism,  $d\mu_{\mathbb{A}_k}(ax)$  is another Haar measure. Thus, it suffices to compare the measures of any set of positive measure  $N$ . We take  $N = \prod_v N_v$ , where  $N_v = \mathcal{O}_v$  for  $v$  finite, and  $N_v$  is a compact neighbourhood of 1 if  $v$  is infinite. Applying Lemma 3.1.7 to each place we obtain

$$\int_{aN} d\mu_{\mathbb{A}_k}(x) = \prod_v \int_{a_v N_v} d\mu_{k_v^+}(x_v) = \prod_v \|a_v\|_v \int_{N_v} d\mu_{k_v^+}(x_v) = \left( \prod_v \|a_v\|_v \right) \int_N d\mu_{\mathbb{A}_k}(x).$$

□

### The field as a subgroup of the adèles

We consider  $k$  as embedded in  $\mathbb{A}_k$  via the map  $\xi \mapsto (\xi, \xi, \dots, \xi, \dots)$  which sends an element of  $k$  to the adèle whose components are all equal to  $\xi$ . The next lemma shows that  $k$  acts as a sort of ‘complement’ for the subring of ‘integral adèles’.

To state it, let  $S_\infty$  denote the set of Archimedean places of  $k$ , and observe that  $\mathbb{A}_{k, S_\infty} := (\mathbb{A}_k)_{S_\infty}$  is by definition the set of adèles  $(x_v)$  such that  $x_v$  is in  $\mathcal{O}_v$  for every finite  $v$ .

**Lemma 3.2.4.** *The following hold.*

1.  $k \cap \mathbb{A}_{k, S_\infty} = \mathcal{O}_k$ .
2.  $k + \mathbb{A}_{k, S_\infty} = \mathbb{A}_k$ .

*Proof.* 1. This is simply the statement that a field element that has non-negative valuation at each finite place is an algebraic integer.

2. We need to show that, given an adèle  $x = (x_v)$ , there is  $\xi \in k$  such that  $x + \xi$  is integral at every finite place  $\mathfrak{p}$ . Let  $m$  be an integer divisible by all the primes  $\mathfrak{p}$  such that  $x_{\mathfrak{p}} \notin \mathcal{O}_{\mathfrak{p}}$ . Replacing  $m$  by  $m^N$  for some  $N \gg 0$  we may assume that  $m x_{\mathfrak{p}}$  has non-negative valuation at  $\mathfrak{p}$  for all  $\mathfrak{p}$ .

Denote by  $S$  the finite set of places dividing  $m$ ; note that  $S$  contains all the places at which  $x_{\mathfrak{p}}$  is not integral.

We look for a field element  $\xi$  of the form  $\frac{a}{m}$  with  $a \in \mathcal{O}_k$ . Since both  $x_{\mathfrak{p}}$  and  $\frac{a}{m}$  are integral at  $\mathfrak{p}$  for  $\mathfrak{p} \notin S$ , it suffices to show that we can choose  $a$  in such a way that  $m x_{\mathfrak{p}} + a \equiv 0 \pmod{\mathfrak{p}^{v_{\mathfrak{p}}(m)}}$  for all  $\mathfrak{p} \in S$ . Such an  $a$  exists by the Chinese remainder theorem. Note that, with a slight abuse of notation, we have identified  $m x_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^{v_{\mathfrak{p}}(m)}$  with an element of  $\mathcal{O}_k/\mathfrak{p}^{v_{\mathfrak{p}}(m)}$ . This identification is possible since the canonical map

$$\frac{\mathcal{O}_k}{\mathfrak{p}^{v_{\mathfrak{p}}(m)}} \rightarrow \frac{\mathcal{O}_v}{\mathcal{O}_v \mathfrak{p}^{v_{\mathfrak{p}}(m)}}$$

is an isomorphism (it is injective between groups with the same cardinality). □

We now introduce the following notation:

**Definition 3.2.5** (Infinite part of the adèles). We denote by  $\mathbb{A}_k^\infty$  the product  $\prod_{v \in S_\infty} k_v$  of the archimedean completions of  $\mathbb{A}_k$ . If  $(r_1, r_2)$  is the signature of  $k$  (see Definition 1.3.20), then  $\mathbb{A}_k^\infty$  is isomorphic to  $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ . Given  $x \in \mathbb{A}_k$ , we denote by  $x^\infty$  its projection on  $\mathbb{A}_k^\infty$ .

**Lemma 3.2.6.** *Let  $\omega_1, \dots, \omega_n$  be a  $\mathbb{Z}$ -basis of  $\mathcal{O}_k$  (so that in particular  $[k : \mathbb{Q}] = n$  and  $r_1 + 2r_2 = n$ ).*

1.  $\omega_1^\infty, \dots, \omega_n^\infty$  is a  $\mathbb{R}$ -basis of  $\mathbb{A}_k^\infty$ .
2. Let  $D^\infty = \{\sum_{i=1}^n x_i \omega_i : x_i \in [0, 1)\}$  be the ‘fundamental parallelootope’ spanned by the given basis. The volume of  $D^\infty$  with respect to the measure  $\prod_{v \in S_\infty} dx_v$  is  $\sqrt{|d_k|}$ , where  $d_k$  is the discriminant of  $k$ .

*Proof.* Denote by  $\sigma_1, \dots, \sigma_{r_1}$  the  $r_1$  real embeddings of  $k$  and by  $\sigma_{r_1+1}, \dots, \sigma_{r_1+r_2}$  a choice of  $r_2$  non-equivalent non-real embeddings of  $k$  into  $\mathbb{C}$  (here, by *non-equivalent* we mean that no two of them are complex conjugate of each other). An isomorphism  $\mathbb{A}_k^\infty \cong \mathbb{R}^{r_1} \times \mathbb{R}^{2r_2}$  is given by

$$\xi \mapsto ((\sigma_i(\xi))_{i=1, \dots, r_1}, (\Re \sigma_{r_1+i}(\xi), \Im \sigma_{r_1+i}(\xi))_{i=1, \dots, r_2}).$$

Here we use the fact that  $\mathbb{C}$  (with its **standard** Lebesgue measure) is isomorphic as a measure space to  $\mathbb{R} \times \mathbb{R}$  (with its standard Lebesgue measure) via the map  $z \mapsto (\Re z, \Im z)$ . Via this isomorphism, the elements  $\omega_m$  are sent to the vectors

$$\omega_m^\infty = \begin{pmatrix} \sigma_1(\omega_m) \\ \vdots \\ \sigma_{r_1}(\omega_m) \\ \Re \sigma_{r_1+1}(\omega_m) \\ \Im \sigma_{r_1+1}(\omega_m) \\ \vdots \\ \Re \sigma_{r_1+r_2}(\omega_m) \\ \Im \sigma_{r_1+r_2}(\omega_m) \end{pmatrix} = \begin{pmatrix} \sigma_1(\omega_m) \\ \vdots \\ \sigma_{r_1}(\omega_m) \\ \frac{\sigma_{r_1+1}(\omega_m) + \overline{\sigma_{r_1+1}(\omega_m)}}{2} \\ \frac{\sigma_{r_1+1}(\omega_m) - \overline{\sigma_{r_1+1}(\omega_m)}}{2i} \\ \vdots \\ \frac{\sigma_{r_1+r_2}(\omega_m) + \overline{\sigma_{r_1+r_2}(\omega_m)}}{2} \\ \frac{\sigma_{r_1+r_2}(\omega_m) - \overline{\sigma_{r_1+r_2}(\omega_m)}}{2i} \end{pmatrix}.$$

Consider the matrix  $\omega^\infty$  having  $\omega_m^\infty$  as columns. We want to compute the absolute value of the determinant of this matrix; in order to do so, we can consider  $\omega^\infty$  as a matrix with complex coefficients.

Summing  $1/i$ -times each row  $\Re \sigma_{r_1+j}(\omega_m)$  to the following one (which does not change the determinant of  $\omega^\infty$ ) we replace the  $m$ -th column of  $\omega^\infty$  with

$$\begin{pmatrix} \sigma_1(\omega_m) \\ \vdots \\ \sigma_{r_1}(\omega_m) \\ \frac{\sigma_{r_1+1}(\omega_m) + \overline{\sigma_{r_1+1}(\omega_m)}}{2} \\ \sigma_{r_1+1}(\omega_m)/i \\ \vdots \\ \frac{\sigma_{r_1+r_2}(\omega_m) + \overline{\sigma_{r_1+r_2}(\omega_m)}}{2} \\ \sigma_{r_1+r_2}(\omega_m)/i \end{pmatrix}.$$

We now subtract  $i/2$ -times each row  $\sigma_{r_1+r_2}(\omega_m)/i$  from the previous one, obtaining a matrix (with the same determinant as  $\omega^\infty$ ) having as  $m$ -th column the vector

$$\begin{pmatrix} \sigma_1(\omega_m) \\ \vdots \\ \sigma_{r_1}(\omega_m) \\ \frac{\sigma_{r_1+1}(\omega_m)}{2} \\ \sigma_{r_1+1}(\omega_m)/i \\ \vdots \\ \frac{\sigma_{r_1+r_2}(\omega_m)}{2} \\ \sigma_{r_1+r_2}(\omega_m)/i \end{pmatrix}.$$

Pulling out a factor of  $1/2$  from each row  $\frac{\sigma_{r_1+j}(\omega_m)}{2}$  and a factor  $1/i$  from each row  $\sigma_{r_1+j}(\omega_m)$ , we obtain

$$\det \omega^\infty = i^{-r_2} 2^{-r_2} \det (\sigma_i(\omega_m))_{i,m},$$

hence in absolute value we have

$$|\det(\omega^\infty)| = 2^{-r_2} |\det (\sigma_i(\omega_m))_{i,m}| = 2^{-r_2} \sqrt{|d_k|},$$

see Definition 1.3.1.

1. The previous determinant computation shows in particular that the vectors  $\omega_m^\infty$  are linearly independent.
2. Note that (up to a set of measure zero)  $D^\infty$  is the image of  $[0, 1]^n$  under the linear map

that sends a vector  $\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$  to  $\omega^\infty \mathbf{x}$ , where  $\omega^\infty$  is as above. Thus, one of the basic

properties of the determinant shows that the volume of  $D^\infty$  is  $|\det(\omega^\infty)| \cdot \text{vol}([0, 1]^n)$ . The claim follows from the fact that  $|\det(\omega^\infty)| = 2^{-r_2} \sqrt{|d_k|}$  and  $\text{vol}([0, 1]^n) = 2^{r_2}$ , since our choice of Haar measure on  $\mathbb{R}^{r_2}$  is **twice** the standard Lebesgue measure.

□

**Definition 3.2.7** (Additive fundamental domain). The **additive fundamental domain**  $D$  of  $\mathbb{A}_k$  is the set  $\{x \in \mathbb{A}_k : x \in \mathbb{A}_{k,S_\infty} \text{ and } x^\infty \in D^\infty\}$ . Equivalently,  $D = \mathbb{A}_k^{S_\infty} \times D^\infty$ .

**Theorem 3.2.8** (Properties of the additive fundamental domain). *The following hold:*

1.  $\mathbb{A}_k$  is the disjoint union  $\bigsqcup_{\xi \in k} (\xi + D)$
2. The measure of  $D$  is 1.

*Proof.* 1. We first prove that  $\xi_1 + D$  and  $\xi_2 + D$  intersect trivially if  $\xi_1, \xi_2$  are elements of  $k$  with  $\xi_1 \neq \xi_2$ . Equivalently, we need to show that  $\xi_1 - \xi_2 \in D$  implies  $\xi_1 = \xi_2$ . Since  $D$  is contained in  $\mathbb{A}_{k,S_\infty}$ , by Lemma 3.2.4 we see that  $\xi_1 - \xi_2$  is an algebraic integer, hence an integral linear combination of  $\omega_1, \dots, \omega_n$  (notation as in Lemma 3.2.6). However, by projecting on  $\mathbb{A}_k^\infty$  we obtain that its coordinates in the  $\mathbb{Z}$ -basis  $\omega_1, \dots, \omega_n$  are all strictly less than 1, hence they are all equal to zero, that is,  $\xi_1 - \xi_2 = 0$ .

Now we show that every adèle  $x$  is in some  $\xi + D$ . By Lemma 3.2.4, there exists  $\xi_1$  such that  $y := x - \xi_1$  is in  $\mathbb{A}_{k,S_\infty}$ . Now consider  $y^\infty$ : by Lemma 3.2.6 the set  $\omega_1, \dots, \omega_n$  is a basis of this vector space, so we can write  $y^\infty = \sum_{i=1}^n c_i \omega_i + \sum_{i=1}^n \delta_i \omega_i$  with  $c_i \in \mathbb{Z}$  and  $\delta_i \in [0, 1)$ . The field element  $\xi_2 = \sum_{i=1}^n c_i \omega_i$  is in  $\mathcal{O}_k$ , so  $y - \xi_2$  is still in  $\mathbb{A}_{k,S_\infty}$ , and furthermore, by construction,  $(y - \xi_2)^\infty$  is in  $D^\infty$ . It follows as desired that  $x - \xi_1 - \xi_2$  is in  $D$ .

2. By definition we have  $D = \mathbb{A}_k^{S_\infty} \times D^\infty \subseteq \mathbb{A}_{k,S_\infty}$ . Since the adèlice measure coincides with the product measure on subsets of the form  $(\mathbb{A}_k)_S$ , the adèlic measure of  $D$  is

$$\mu_{\mathbb{A}_k}(D) = \left( \int_{\mathbb{A}_k^{S_\infty}} d\mu_{\mathbb{A}_k^{S_\infty}} \right) \left( \int_{D^\infty} \prod_{v \in S_\infty} d\mu_{x_v} \right).$$

The second factor is equal to  $\sqrt{|d_k|}$  by Lemma 3.2.6. As for the first, we have

$$\int_{\mathbb{A}_k^{S_\infty}} d\mu_{\mathbb{A}_k^{S_\infty}} = \prod_{v \notin S_\infty} \int_{\mathcal{O}_v} d\mu_v = \prod_{v \notin S_\infty} N(\mathfrak{d}_v)^{-1/2} = \prod_{v \notin S_\infty} |d_{k_v}|^{-1/2},$$

where we used our normalisation for the additive Haar measures on the local fields  $k_v$  (Definition 3.1.9) and Theorem 2.3.19. Finally, using Theorem 2.3.20 we conclude that  $\prod_{v \notin S_\infty} |d_{k_v}|^{-1/2} = |d_k|^{-1/2}$ , which simplifies  $\int_{D^\infty} \prod_{v \in S_\infty} d\mu_{x_v} = |d_k|^{1/2}$ , giving the result.  $\square$

**Corollary 3.2.9** (Position of  $k$  inside  $\mathbb{A}_k$ ). *The field  $k$  is a discrete subgroup of  $\mathbb{A}_k$  and the quotient  $\mathbb{A}_k/k$  is compact.*

*Proof.* It is clear that Theorem 3.2.8 remains true if we replace our choice of  $D^\infty$  with the set  $\tilde{D}^\infty = \{\sum_{i=1}^n x_i \omega_i : x_i \in [-1/2, 1/2)\}$ . Define  $\tilde{D}$  as the corresponding additive fundamental domain. Since  $\tilde{D}$  contains a neighbourhood of 0, the decomposition  $\mathbb{A}_k = \bigsqcup_{\xi \in k} (\xi + \tilde{D})$  of Theorem 3.2.8(1) shows that each point of  $\xi$  has a neighbourhood that is disjoint from a neighbourhood of any other point. Thus,  $k$  is discrete in  $\mathbb{A}_k$ . The quotient  $\mathbb{A}_k/k$  is compact since there is a continuous surjection  $\overline{D} \rightarrow \mathbb{A}_k/k$  with  $\overline{D}$  compact.  $\square$

**Lemma 3.2.10.** *The character  $\Lambda$  of Equation (3.10) vanishes on  $k$ .*

*Proof.* For each place  $v$  of  $k$ , let  $\mathbb{Q}_v$  be the completion of  $\mathbb{Q}$  at its unique place lying under  $v$  (equivalently: the closure of  $\mathbb{Q}$  in  $k_v$ ). By definition,

$$\Lambda(\xi) = \sum_v \Lambda_v(\xi) = \sum_v \lambda_v(\text{tr}_{k_v/\mathbb{Q}_v} \xi) = \sum_{w \in \Omega_{\mathbb{Q}}} \lambda_w \left( \sum_{v|w} \text{tr}_{k_v/\mathbb{Q}_w}(\xi) \right) = \sum_{w \in \Omega_{\mathbb{Q}}} \lambda_w(\text{tr}_{k/\mathbb{Q}}(\xi)),$$

where we used Theorem 2.3.22. Setting  $x = \text{tr}_{k/\mathbb{Q}}(\xi)$  we are then reduced to showing

$$\sum_{w \in \Omega_{\mathbb{Q}}} \lambda_w(x) \equiv 0 \pmod{1} :$$

we have reduced the lemma to the case  $k = \mathbb{Q}$ . To treat this, we need to show that  $\sum_v \lambda_v(x)$  is an integer for every  $x \in \mathbb{Q}$ . Clearly it suffices to show that is  $q$ -integral at each (finite) prime  $q$ . This is achieved by looking at the decomposition

$$\sum_v \lambda_v(x) = \left( \sum_{p \neq q, \infty} \lambda_p(x) \right) + \lambda_q(x) + \lambda_\infty(x) = \left( \sum_{p \neq q, \infty} \lambda_p(x) \right) + (\lambda_q(x) - x) \pmod{\mathbb{Z}} :$$

each  $\lambda_p(x)$  is a rational number with denominator a power of  $p$ , hence it is  $q$ -integral, while  $\lambda_q(x) - x$  is  $q$ -integral by definition.  $\square$

**Theorem 3.2.11** (Dual of  $\mathbb{A}_k/k$ ). *The map*

$$\begin{aligned} \beta : k &\rightarrow \widehat{\mathbb{A}_k/k} \\ \eta &\mapsto \exp(2\pi i \Lambda(\eta \cdot)) \end{aligned}$$

*is an isomorphism of topological groups.*

*Proof.* By Proposition 2.2.4, we have  $\widehat{\mathbb{A}_k/k} \cong k^\perp$ , where  $k^\perp$  is the closed subgroup of  $\widehat{\mathbb{A}_k}$  given by those characters that vanish on  $k$ . By Lemma 3.2.10 we have  $k \subseteq k^\perp$ . We now show that they are equal, by combining the following three observations:

1. By Proposition 2.2.4 there is an isomorphism of  $\widehat{\mathbb{A}_k/k}$  with  $k^\perp$ . Note that  $\widehat{\mathbb{A}_k/k}$  is discrete, because  $\mathbb{A}_k/k$  is compact (apply Theorem 2.2.2 and Corollary 3.2.9). We have already observed that  $k \subseteq k^\perp$ , so we can consider the quotient  $k^\perp/k$ , which is therefore discrete<sup>3</sup>.
2. On the other hand, via the self-duality  $\mathbb{A}_k \cong \widehat{\mathbb{A}_k}$ , the quotient  $k^\perp/k$  can be considered as a subgroup  $\mathbb{A}_k/k$ , which is compact by Corollary 3.2.9. Combined with (1), this shows that  $k^\perp/k$  is both discrete and compact, hence finite.
3. Finally,  $k^\perp$  has a natural structure of  $k$ -vector space (for  $\psi \in k^\perp, \xi \in k$  we set  $(\xi \cdot \psi)(\eta) := \psi(\xi\eta)$ ), and  $k$  is a  $k$ -vector subspace. Thus,  $k^\perp/k$  is a  $k$ -vector space of finite cardinality. Since  $k$  is infinite, this implies  $k^\perp = k$ , as desired.

□

### The Riemann-Roch theorem

In this section we want to work with (continuous) functions  $\tilde{\varphi} : \mathbb{A}_k/k \rightarrow \mathbb{C}$ . We find it technically simpler to consider them as functions  $\mathbb{A}_k \rightarrow \mathbb{C}$  that are invariant under translation by any  $\xi \in k$ . We give this as a formal definition:

**Definition 3.2.12** (Periodic function). Let  $\pi : \mathbb{A}_k \rightarrow \mathbb{A}_k/k$  be the canonical projection. A function  $\varphi : \mathbb{A}_k \rightarrow \mathbb{C}$  is called *periodic* if  $\varphi(x + \xi) = \varphi(x)$  for all  $x \in \mathbb{A}_k$  and all  $\xi \in k \subseteq \mathbb{A}_k$ . Such a function induces, by passage to the quotient, a function  $\tilde{\varphi} : \mathbb{A}_k/k \rightarrow \mathbb{C}$ . Conversely, given  $\tilde{\varphi} : \mathbb{A}_k/k \rightarrow \mathbb{C}$ , we denote by  $\varphi = \tilde{\varphi} \circ \pi$  the corresponding function on  $\mathbb{A}_k$ .

**Remark 3.2.13.** Notice that  $\tilde{\varphi} : \mathbb{A}_k/k \rightarrow \mathbb{C}$  is continuous if and only if the corresponding function  $\varphi : \mathbb{A}_k \rightarrow \mathbb{C}$  is continuous and periodic.

**Lemma 3.2.14.** *Let  $\varphi(x) : \mathbb{A}_k \rightarrow \mathbb{C}$  be continuous and periodic, and let  $\tilde{\varphi} : \mathbb{A}_k/k \rightarrow \mathbb{C}$  be the corresponding continuous function on  $\mathbb{A}_k/k$ . We have*

$$\int_D \varphi(x) d\mu_{\mathbb{A}_k}(x) = \int_{\mathbb{A}_k/k} \tilde{\varphi}(x) d\mu(x),$$

where the measure  $d\mu$  on  $\mathbb{A}_k/k$  is the unique Haar measure on this (compact, by Corollary 3.2.9) group such that  $\mu(\mathbb{A}_k/k) = 1$ .

<sup>3</sup>note that if  $X$  is a discrete topological group and  $Y$  is any subgroup, then  $X/Y$  is discrete: each point is open!

*Proof.* Follows from Theorem 3.2.8(2). More precisely, denote by  $\pi$  the canonical projection  $\mathbb{A}_k \rightarrow \mathbb{A}_k/k$  and introduce the function

$$I : L^1(\mathbb{A}_k/k) \rightarrow \mathbb{C} \\ \tilde{\varphi}(x) \mapsto \int_D \tilde{\varphi} \circ \pi(x) d\mu_{\mathbb{A}_k}(x).$$

It is easy to check that  $I$  has the properties required to be a Haar integral<sup>4</sup>. Moreover, it gives measure 1 to  $\mathbb{A}_k/k$  by Theorem 3.2.8(2).

We check in greater detail the invariance of  $I$  under translation. Let  $y \in \mathbb{A}_k$  and let  $\psi(x) = \varphi(x + y)$ . Denote by  $\tilde{\psi}$  the corresponding function on the quotient  $\mathbb{A}_k/k$ . We need to check that

$$\int_D \tilde{\varphi} \circ \pi(x) d\mu_{\mathbb{A}_k}(x) = \int_D \tilde{\psi} \circ \pi(x) d\mu_{\mathbb{A}_k}(x),$$

or equivalently

$$\int_D \varphi(x) d\mu_{\mathbb{A}_k}(x) = \int_D \psi(x) d\mu_{\mathbb{A}_k}(x),$$

which can further be rewritten as

$$\int_D \varphi(x) d\mu_{\mathbb{A}_k}(x) = \int_D \varphi(x + y) d\mu_{\mathbb{A}_k}(x).$$

Since  $d\mu_{\mathbb{A}_k}$  is translation-invariant, we are reduced to showing

$$\int_D \varphi(x) d\mu_{\mathbb{A}_k}(x) = \int_{y+D} \varphi(x) d\mu_{\mathbb{A}_k}(x).$$

Now, since  $\mathbb{A}_k = \bigsqcup_{\xi \in k} (\xi + D)$ , we have

$$y + D = \bigsqcup_{\xi \in k} ((\xi + D) \cap (y + D)),$$

where only finitely many sets in the union are non-empty.

We rewrite the integral  $\int_{y+D} \varphi(x) d\mu_{\mathbb{A}_k}(x)$  as the series (really a finite sum)

$$\begin{aligned} \sum_{\xi \in k} \int_{(\xi+D) \cap (y+D)} \varphi(x) d\mu_{\mathbb{A}_k}(x) &= \sum_{\xi \in k} \int_{(\xi+D) \cap (y+D)} \varphi(x + \xi) d\mu_{\mathbb{A}_k}(x) \\ &= \sum_{\xi \in k} \int_{D \cap (y - \xi + D)} \varphi(x) d\mu_{\mathbb{A}_k}(x), \end{aligned} \tag{3.11}$$

where we have used the translation-invariance of both the measure  $d\mu_{\mathbb{A}_k}$  and the function  $\varphi$ . Now, it is immediate to check that  $y + D$  is another additive fundamental domain for  $\mathbb{A}_k$ , hence the sets  $\{-\xi + (y + D)\}_{\xi \in k}$  are disjoint and cover  $\mathbb{A}_k$ . It follows that the sets  $\{D \cap (y - \xi + D)\}_{\xi \in k}$  are disjoint and cover  $D$ , and therefore the last integral in (3.11) is also equal to  $\int_D \varphi(x) d\mu_{\mathbb{A}_k}(x)$ , as desired.  $\square$

<sup>4</sup>to be precise: if we only consider functions  $\tilde{\varphi}$  that are the characteristic functions of subsets of  $\mathbb{A}_k/k$ , the functional  $I$  clearly gives a measure on  $\mathbb{A}_k/k$ . We will see below that this measure is translation-invariant and gives mass 1 to  $\mathbb{A}_k/k$ , so it is the unique normalised Haar measure. *A posteriori*, this implies that  $I$  is the integration against this Haar measure, hence it is well-defined on all of  $L^1(\mathbb{A}_k/k)$ .

Recall from Theorem 3.2.11 that  $k$  is the character group of  $\mathbb{A}_k/k$ . It follows that the Fourier transform of a function on  $\mathbb{A}_k/k$  can be identified with a function on  $k$ , and precisely we have:

**Definition 3.2.15** (Fourier transform on  $\mathbb{A}_k/k$ ). Let  $\varphi$  be a complex-valued, periodic, continuous function on  $\mathbb{A}_k$ . Its Fourier transform is the function

$$\begin{aligned} \hat{\varphi} : k &\rightarrow \mathbb{C} \\ \xi &\mapsto \int_D \varphi(x) e^{-2\pi i \Lambda(\xi x)} d\mu_{\mathbb{A}_k}(x). \end{aligned}$$

Note that, by compactness of  $\mathbb{A}_k/k$  (Corollary 3.2.9), any continuous function on this quotient is automatically  $L^1$ . We exploit this in the next lemma:

**Lemma 3.2.16.** *Let  $\varphi(x)$  be continuous and periodic with  $\sum_{\xi \in k} |\hat{\varphi}(\xi)| < \infty$ . We have the Fourier inversion formula*

$$\varphi(x) = \sum_{\xi \in k} \hat{\varphi}(\xi) e^{2\pi i \Lambda(x\xi)}.$$

*Proof.* As already observed,  $\varphi(x)$  induces a continuous function  $\tilde{\varphi}(x)$  in  $L^1(\mathbb{A}_k/k)$ . The hypothesis of the lemma means that the Fourier transform of  $\tilde{\varphi}(x)$  is in  $L^1(k)$ . Thus,  $\tilde{\varphi}(x)$  satisfies the assumptions of the abstract Fourier inversion theorem (Theorem 2.2.10). The conclusion of the lemma is then simply the inversion formula, once we check that the measure  $\mu_k$  on  $k$  dual to the Haar measure we fixed on  $\mathbb{A}_k/k$  is the counting measure (and not a nontrivial multiple thereof).

To see that this holds, we apply Lemma 2.4.21 (2) to  $H_i = \mathbb{A}_k/k$ . The group  $H_i^\perp$  is clearly trivial (hence can be identified to the singleton  $\{0\}$  of  $k \cong \widehat{\mathbb{A}_k/k}$ ), so we obtain  $1 = \mu_{\mathbb{A}_k/k}(\mathbb{A}_k/k) \cdot \mu_k(\{0\}) = 1 \cdot \mu_k(\{0\})$ , which shows that  $\mu_k$  is the counting measure, as desired.  $\square$

Now, the simplest (and most ‘traditional’!) way to build a periodic function is to take an arbitrary function  $f(x)$  and consider the sum of all its translates  $f(x + \xi)$ . The next lemma describes what assumptions are necessary to obtain a well-behaved function in this way.

In order to state it formally, we need a notion of *uniform convergence* for sums indexed by elements of  $k$ . Since  $k$  is a number field (which is a discrete object, without any natural topology), the only possible definition is the following:

**Definition 3.2.17** (Uniform convergence of a series of functions). Let  $a_\xi(x) : \mathbb{A}_k \rightarrow \mathbb{C}$  be a set of complex-valued functions and let  $X$  be a subset of  $\mathbb{A}_k$ . We say that the series  $\sum_{\xi \in k} a_\xi(x)$  **converges uniformly** for  $x \in X$  if the following holds: for every  $\varepsilon > 0$  there exists a finite set  $F \subset k$  such that

$$\sum_{\xi \notin F} |a_\xi(x)| < \varepsilon$$

for all  $x \in X$ .

Note that, by standard arguments, the sum of a uniformly convergent series of continuous functions is itself a continuous function.

**Lemma 3.2.18.** *Let  $f(x)$  be a continuous function in  $L^1(\mathbb{A}_k)$  and suppose that  $\sum_{\eta \in k} f(x + \eta)$  is uniformly convergent for  $x \in D$ . The continuous periodic function  $\varphi(x) = \sum_{\eta \in k} f(x + \eta)$  satisfies  $\hat{\varphi}(\xi) = \hat{f}(\xi)$  for all  $\xi \in k$ .*



**Remark 3.2.19.** Note that the equality  $\hat{\varphi}(\xi) = \hat{f}(\xi)$  only makes sense for  $\xi \in k$ : we consider  $\varphi$  as a function on  $\mathbb{A}_k/k$ , so its Fourier transform is defined on  $k$ ).

*Proof.* This is essentially a direct calculation. We have

$$\begin{aligned}
\hat{\varphi}(\xi) &= \int_D \varphi(x) e^{-2\pi i \Lambda(\xi x)} d\mu_{\mathbb{A}_k}(x) \\
&= \int_D \left( \sum_{\eta \in k} f(x + \eta) e^{-2\pi i \Lambda(x\xi)} \right) d\mu_{\mathbb{A}_k}(x) \\
&\stackrel{(1)}{=} \sum_{\eta \in k} \int_D f(x + \eta) e^{-2\pi i \Lambda(x\xi)} d\mu_{\mathbb{A}_k}(x) \\
&\stackrel{(2)}{=} \sum_{\eta \in k} \int_{\eta + D} f(x) e^{-2\pi i \Lambda((x-\eta)\xi)} d\mu_{\mathbb{A}_k}(x) \\
&\stackrel{(3)}{=} \int_{\mathbb{A}_k} f(x) e^{-2\pi i \Lambda(x\xi)} d\mu_{\mathbb{A}_k}(x) \\
&= \hat{f}(\xi),
\end{aligned}$$

where

- in (1) we have used the fact that the series converges uniformly in  $D$ , which is of finite measure;
- in (2) we have used the translation-invariance of the Haar measure;
- in (3) we have applied the relation  $\Lambda(\eta\xi) = 0$  for all  $\eta, \xi \in k$ , which follows from Lemma 3.2.10.

□

We now have all the ingredients to prove the two main results of this section:

**Proposition 3.2.20** (Poisson formula). *Let  $f(x) : \mathbb{A}_k \rightarrow \mathbb{C}$  satisfy the following three conditions:*

1.  $f(x)$  is continuous and in  $L^1(\mathbb{A}_k)$ ;
2.  $\sum_{\xi \in k} f(x + \xi)$  is uniformly convergent for  $x \in D$ ;
3.  $\sum_{\xi \in k} |\hat{f}(\xi)|$  converges.

The following equality holds:

$$\sum_{\xi \in k} \hat{f}(\xi) = \sum_{\xi \in k} f(\xi).$$

*Proof.* Let  $\varphi(x) = \sum_{\eta \in k} f(x + \eta)$ . By assumption, we can apply Lemma 3.2.18 to obtain

$$\hat{\varphi}(\xi) = \hat{f}(\xi),$$

where  $\varphi(x)$  is continuous and periodic. Taking absolute values and summing over  $\xi \in k$  we obtain

$$\sum_{\xi \in k} |\hat{\varphi}(\xi)| = \sum_{\xi \in k} |\hat{f}(\xi)| < \infty,$$

so the assumption of Lemma 3.2.16 is satisfied. That lemma then implies

$$\varphi(x) = \sum_{\xi \in k} \hat{\varphi}(\xi) e^{2\pi i \Lambda(x\xi)}.$$

Replacing  $\varphi(x)$  with its definition and  $\hat{\varphi}(\xi)$  with  $\hat{f}(\xi)$  (Lemma 3.2.18 again) we arrive at

$$\sum_{\eta \in k} f(x + \eta) = \sum_{\xi \in k} \hat{f}(\xi) e^{2\pi i \Lambda(x\xi)}.$$

Setting  $x = 0$  gives the result. □

In turn, the Poisson formula leads immediately the most important result of this section, that Tate calls ‘an arithmetic analogue of the Riemann-Roch theorem’ (more on that in a moment!).

**Theorem 3.2.21** (Riemann-Roch). *Let  $f(x) : \mathbb{A}_k \rightarrow \mathbb{C}$  satisfy the following three conditions:*

1.  $f(x)$  is continuous and in  $L^1(\mathbb{A}_k)$ ;
2.  $\sum_{\xi \in k} f(a(x + \xi))$  is convergent for all idèles  $a$  and all adèles  $x$ , uniformly for  $x \in D$ ;
3.  $\sum_{\xi \in k} |\hat{f}(a\xi)|$  is convergent for all  $a \in I_k$ .

The following holds for every idèle  $a \in I_k$ :

$$\frac{1}{\|a\|} \sum_{\xi \in k} \hat{f}(\xi/a) = \sum_{\xi \in k} f(a\xi).$$

*Proof.* Fix an idèle  $a$  and define  $g(x) = f(ax)$ . We check that  $g(x)$  satisfies the hypotheses of Proposition 3.2.20. It is clear that  $g(x)$  is continuous and  $L^1$ , and  $\sum_{\xi \in k} g(x + \xi)$  is uniformly convergent for  $x \in D$  by assumption. As for the third condition, we compute the Fourier transform of  $g(x)$  as follows:

$$\begin{aligned} \hat{g}(x) &= \int g(\eta) e^{-2\pi i \Lambda(x\eta)} d\mu_{\mathbb{A}_k}(\eta) \\ &= \int f(a\eta) e^{-2\pi i \Lambda(x\eta)} d\mu_{\mathbb{A}_k}(\eta) \\ &= \frac{1}{\|a\|} \int f(\eta) e^{-2\pi i \Lambda(x\eta/a)} d\mu_{\mathbb{A}_k}(\eta) \\ &= \frac{1}{\|a\|} \hat{f}(x/a), \end{aligned}$$

where in the only non-trivial equality we used Lemma 3.2.3. We now have  $\sum_{\xi \in k} |\hat{g}(\xi)| = \frac{1}{\|a\|} \sum_{\xi \in k} |\hat{f}(a^{-1}\xi)| < \infty$  by assumption. Thus, the Poisson formula holds and yields

$$\sum_{\xi \in k} g(\xi) = \sum_{\xi \in k} \hat{g}(\xi),$$

that is,

$$\sum_{\xi \in k} f(a\xi) = \frac{1}{\|a\|} \sum_{\xi \in k} \hat{f}(\xi/a).$$

□

**Analogy with the geometric Riemann-Roch theorem (★)**

In this short optional section, we try to connect Theorem 3.2.21 to the classical statement known as the Riemann-Roch theorem in the geometry of curves (over finite fields).

Let  $k$  be the function field of a curve  $C$  over a finite field  $\mathbb{F}_q$ . In this setting, the *places* of  $k$  (that are trivial on  $\mathbb{F}_q$ ) are in bijection with the Galois orbits of points of  $C(\overline{\mathbb{F}_q})$  (aka the closed points of the scheme). Each valuation has a **degree**  $\deg v$ , defined as the degree over  $\mathbb{F}_q$  of the residue field of the point corresponding to  $v$ . The **local ring at  $v$** , or **ring of integers at  $v$** , is the subring  $\mathcal{O}_v$  of  $k$  consisting of those elements for which  $v(f) \geq 0$ . This ring is local, with unique maximal ideal  $\mathfrak{p}_v = \{0\} \cup \{f \in k^\times : v(f) > 0\}$ .

We define a **divisor** to be a formal linear combination  $\sum_v n_v v$ , where each  $n_v$  is an integer and all but finitely many of them are zero. We denote by  $\text{Div}(k)$  the set of all divisors. There is a notion of **degree**, namely  $\deg(\sum n_v v) = \sum n_v \deg(v)$ , and a notion of **principal divisor**: given  $f \in k^\times$ , the principal divisor corresponding to  $f$  is

$$\text{div}(f) = \sum_v v(f)v.$$

The (analogue of the) product formula, Theorem 3.2.27 below, holds in this context, and gives

$$1 = \|f\|_{\mathbb{A}_k} = \prod_v \|f\|_v = \prod_v (q^{\deg v})^{v(f)} = q^{\sum_v v(f) \deg(v)},$$

which shows that  $\deg(\text{div } f) = 0$ . Finally, it is not hard to see that an element  $f \in k^\times$  satisfies  $\text{div } f = 0$  if and only if  $f \in \mathbb{F}_q^\times$ .

We define a partial ordering on the set of divisors by

$$\sum_v n_v v \geq \sum_v n'_v v \iff n_v \geq n'_v \quad \forall v.$$

To each divisor  $D$  we then associate the **linear system**

$$L(D) = \{0\} \cup \{f \in k^\times : \text{div}(f) \geq -D\}.$$

It is immediate to see that  $L(D)$  is an  $\mathbb{F}_q$ -vector space. We write  $l(D)$  for its dimension. It is not hard to show that  $l(D)$  is finite for every  $D$ , but we will simply admit this.

Before connecting Theorem 3.2.21 to the classical statement of Riemann-Roch, we make two further remarks. One is that, given a divisor  $D = \sum n_v v$ , we can always find an idèle  $x(D) = (x(D)_v)$  such that  $v(x(D)_v) = n_v$ . If we further define

$$f = \prod_v \mathbf{1}_{\mathcal{O}_v}, \tag{3.12}$$

the product of the characteristic functions of the local rings at all valuations, for every  $\xi \in k$  we have

$$f(\xi x(D)) = \prod_v \mathbf{1}_{\mathcal{O}_v}(\xi x(D)_v) = \prod_v \begin{cases} 1, & \text{if } v(x(D)_v) + v(\xi) \geq 0 \\ 0, & \text{otherwise} \end{cases} = \begin{cases} 1, & \text{if } v(\xi) \geq -n_v \forall v \\ 0, & \text{otherwise} \end{cases},$$

and therefore, by definition, this number is 1 if  $\xi$  is in  $L(D)$  and is 0 otherwise. Thus,

$$\sum_{\xi \in k} f(\xi x(D)) = \#L(D) = q^{l(D)}.$$

**Theorem 3.2.22** (Riemann-Roch, geometric form). *There exists an integer  $g \geq 0$  and a divisor  $K_C$  of degree  $2g - 2$  such that*

$$l(D) - l(K_C - D) = \deg(D) - g + 1.$$

*Proof.* Fix a character  $\Lambda : \mathbb{A}_k \rightarrow \mathbb{S}^1$  which gives rise to a self-duality, as in Theorem 3.2.1. For each place  $v$ , let  $\mathfrak{p}_v^{m_v}$  be the minimal power of  $\mathfrak{p}_v$  on which  $\Lambda_v$  is trivial (note that  $m_v$  can easily be negative, see Lemma 3.1.6). We define

$$K_C = - \sum_v m_v v;$$

it is a divisor, because  $m_v = 0$  for almost all  $v$ .

We now compute the Fourier transform of the function  $f$  defined in (3.12). By Lemma 2.4.22, this is given by the product of the Fourier transforms of the functions  $\mathbf{1}_{\mathcal{O}_v}$ . By the exact same calculation as in the proof of Theorem 3.1.10, we obtain that

$$\widehat{\mathbf{1}_{\mathcal{O}_v}}(x) = N(\mathfrak{p}_v^{m_v})^{1/2} \cdot \mathbf{1}_{\mathfrak{p}_v^{m_v}}.$$

Multiplying over all  $v$ , we obtain the Fourier transform of  $f$  as

$$\prod_v N(\mathfrak{p}_v^{m_v})^{1/2} \cdot \prod_v \mathbf{1}_{\mathfrak{p}_v^{m_v}} = q^{\frac{1}{2} \sum_v m_v \deg(v)} \cdot \prod_v \mathbf{1}_{\mathfrak{p}_v^{m_v}} = q^{-\frac{1}{2} \deg K_C} \cdot \prod_v \mathbf{1}_{\mathfrak{p}_v^{m_v}}.$$

Applying this formula to  $\xi x(D)^{-1}$ , where  $x(D)$  is as above, we obtain

$$\hat{f}(\xi x(D)^{-1}) = \begin{cases} q^{-\frac{1}{2} \deg K_C}, & \text{if } v(\xi) \geq m_v + n_v \forall v \\ 0, & \text{otherwise.} \end{cases}$$

Notice that this is nonzero precisely if  $v(\xi) \geq -v(D) + v(K_C) = -v(D - K_C)$ , so

$$\sum_{\xi \in k} \hat{f}(\xi x(D)^{-1}) = q^{-\frac{1}{2} \deg K_C} \#L(K_C - D) = q^{-\frac{1}{2} \deg K_C + l(K_C - D)}.$$

Finally, we apply Theorem 3.2.21 to the function  $f$  and the idèle  $x(D)$ . It yields

$$\sum_{\xi \in k} f(\xi x(D)) = \|x(D)\|^{-1} \sum_{\xi \in k} \hat{f}(\xi x(D)^{-1}),$$

that is,

$$q^{l(D)} = \|x(D)\|^{-1} q^{-\frac{1}{2} \deg K_C + l(K_C - D)}.$$

Since  $\|x(D)\|^{-1} = \prod_v (q^{\deg v})^{n_v} = q^{\deg D}$ , we have obtained

$$q^{l(D)} = q^{\deg D - \frac{1}{2} \deg(K_C) + l(K_C - D)},$$

that is,

$$l(D) - l(K_C - D) = \deg D - \frac{1}{2}(\deg K_C).$$

We conclude by setting  $\deg(K_C) = 2g - 2$ : it is clear from the statement of the theorem that  $g$  is automatically an integer (since every other term in the formula is), and non-negativity follows from the fact that replacing  $D = K_C$  in the statement we obtain  $l(K_C) - l(0) = 2g - 2 - g + 1$ , that is,  $g = l(K_C) - l(0) + 1 = l(K_C) \geq 0$ .  $\square$

### 3.2.2 The multiplicative group: the idèles

Recall from Definition 2.4.5 the group of idèles  $I_k$  of  $k$ . We shall presently regard  $I_k$  as a topological group, with the topology coming from its structure as a restricted product.

**Exercise 3.2.23** (Two topologies on  $I_k$ ). Check that the restricted product topology of  $I_k$  is **strictly** finer than the subspace topology that  $I_k$  inherits from  $\mathbb{A}_k$ .

**Definition 3.2.24** (Map to ideals). For every idèle  $a = (a_v)_v$  we define  $\varphi(a)$  as the fractional ideal of  $\mathcal{O}_k$  given by  $\varphi(a) = \prod_{\mathfrak{p} \notin S_\infty} \mathfrak{p}_v^{v_{\mathfrak{p}}(a_{\mathfrak{p}})}$ , where we identify the set of finite places of  $k$  to the set of (non-zero) prime ideals of  $\mathcal{O}_k$ .

**Remark 3.2.25.** The map  $a \mapsto \varphi(a)$  is a homomorphism with kernel  $I_{S_\infty}$  (the idèles that are units at all finite places).

Following the general structure of our analysis, we now fix a measure on  $I_k$  and describe its quasi-characters.

**Definition 3.2.26** (Idèlic Haar measure). We take as Haar measure on the idèles the product  $\prod_v d\alpha_v$  of the local multiplicative measures  $d\alpha_v$  of Definition 3.1.22.

By Theorem 2.4.14, the quasi-characters of  $I_k = \prod'_v (k_v^\times, \mathbf{u}_v)$  are of the form  $c(a) = \prod_v c_v(a_v)$ , where – for almost all  $v$  – the character  $c_v$  belongs to  $\mathbf{u}_v^\perp$ , that is to say,  $c_v(\mathbf{u}_v) = \{1\}$  (such a character, as already mentioned, is said to be *unramified*).

We embed  $k^\times$  into  $I_k$  by sending  $\alpha \in k^\times$  to the idèle  $\alpha = (\alpha, \alpha, \dots, \alpha, \dots)$ . As was the case with the additive group, the most interesting questions about  $I_k$  concern the ‘position’ of  $k^\times$  inside it.

The next result is well-known (in fact, we have already met it as Theorem 2.3.8), but we give a proof in our language.

**Theorem 3.2.27** (Product formula). *The following hold.*

1. Let  $\alpha \in k^\times$ . The ideal  $\varphi(\alpha)$  is the principal ideal  $(\alpha)$ .

2. For every  $\alpha \in k^\times$  we have

$$\|\alpha\| = \prod_v \|\alpha\|_v = 1.$$

*Proof.* 1. This is almost tautological: for any finite place  $\mathfrak{p}$  of  $k$  we have  $v_{\mathfrak{p}}(\varphi(\alpha)) = v_{\mathfrak{p}}(\alpha_{\mathfrak{p}}) = v_{\mathfrak{p}}(\alpha)$ , so the (fractional) ideals  $\varphi(\alpha)$  and  $(\alpha)$  have the same prime factorisation, hence they are equal.

2. Let  $D$  be the additive fundamental domain of Definition 3.2.7. The point is that  $\alpha D$  is another additive fundamental domain, hence one expects  $D$  and  $\alpha D$  to have the same volume. Since  $\mu(\alpha D) = \|\alpha\| \mu(D)$  by Lemma 3.2.3, this should imply  $\|\alpha\| = 1$ . We now make this precise.

Notice first that  $\bigsqcup_{\xi \in k} (\xi + \alpha D) = \bigsqcup_{\xi \in k} (\alpha \xi + \alpha D) = \bigsqcup_{\xi \in k} \alpha(\xi + D)$  is still a disjoint union, and that this union covers  $\bigsqcup_{\xi \in k} \alpha(\xi + D) = \alpha \left( \bigsqcup_{\xi \in k} (\xi + D) \right) = \alpha \mathbb{A}_k = \mathbb{A}_k$ .

Now

$$\begin{aligned} \mu_{\mathbb{A}_k}(\alpha D) &= \sum_{\xi \in k} \int_{\alpha D \cap (\xi + D)} d\mu_{\mathbb{A}_k}(x) = \sum_{\xi \in k} \int_{(-\xi + \alpha D) \cap D} d\mu_{\mathbb{A}_k}(x) \\ &\stackrel{\xi \mapsto -\alpha \xi}{=} \sum_{\xi \in k} \int_{(\alpha \xi + \alpha D) \cap D} d\mu_{\mathbb{A}_k}(x) = \int_{\bigsqcup_{\xi} ((\alpha \xi + \alpha D) \cap D)} d\mu_{\mathbb{A}_k}(x) \\ &= \int_D d\mu_{\mathbb{A}_k}(x) = \mu_{\mathbb{A}_k}(D). \end{aligned}$$

Using  $\mu_{\mathbb{A}_k}(\alpha D) = \|\alpha\| \mu_{\mathbb{A}_k}(D)$  (Lemma 3.2.3) and the fact that  $\mu_{\mathbb{A}_k}(D) \neq 0$  (Theorem 3.2.8(2)), the proof is complete.  $\square$

**Definition 3.2.28** (Idèles of norm 1). We let  $J$  denote the kernel of the map

$$\begin{aligned} I_k &\rightarrow \mathbb{R}^+ \\ a &\mapsto \|a\|. \end{aligned}$$

Let  $v_0$  be an (arbitrarily chosen) archimedean place of  $k$ . Denote by  $T$  the subgroup of idèles that are trivial away from  $v_0$ , and that are positive real numbers in the component  $k_{v_0}^\times$  (which can be either  $\mathbb{R}^\times$  or  $\mathbb{C}^\times$ ). For a positive real number  $t$ , we also denote by  $t$  the unique idèle in  $T$  with absolute value  $t$  (notice that, when  $k_{v_0} \cong \mathbb{C}$ , the identification is that  $t$  represents the idèle  $(1, 1, \dots, 1, \sqrt{t}, 1, \dots)$ ).

**Remark 3.2.29.** Tate writes that it is ‘aesthetically disturbing and not really necessary’ to make this arbitrary choice of  $T$ . What I think he means is that one could take as  $T$  a **canonical** subgroup of  $I_k$  isomorphic to  $\mathbb{R}^+$ , given by the image of the map that sends  $t \in \mathbb{R}^+$  to the idèle that is 1 at each finite place and is equal to  $t$  (respectively,  $\sqrt{t}$ ) at each real (respectively, complex) place. However, Tate’s choice of  $T$  is more convenient for certain calculations, so we will make peace with it.

The following lemma is obvious:

**Lemma 3.2.30.** *We have  $I = J \times T$ .*

We will write idèles as  $a = \|a\| \cdot b$ , where  $\|a\| \in T$  and  $b = a/\|a\| \in J$ .

Since  $T$  is isomorphic to a copy of  $(\mathbb{R}_{>0}, \cdot)$ , its Haar measure is (proportional to)  $\frac{dt}{t}$ . Moreover, the Haar measure(s) on a product are products of Haar measures on the factors, so, if we choose  $\frac{dt}{t}$  as our Haar measure on  $T$ , this determines a unique measure  $db$  on  $J$  such that our already-defined measure  $da$  is equal to  $db \frac{dt}{t}$ . Fubini's theorem then yields the equalities

$$\int_I f(a) da = \int_0^\infty \left( \int_J f(tb) db \right) \frac{dt}{t} = \int_J \left( \int_0^\infty f(tb) \frac{dt}{t} \right) db \tag{3.13}$$

for any  $f \in L^1(I_k)$ .

### Multiplicative fundamental domain

The product formula (Theorem 3.2.27) implies that  $k^\times$  is contained in  $J$ . Our next objective is to describe the relative position of  $k^\times$  inside of  $J$ , and in particular to find a fundamental domain for  $J/k^\times$ .

**Definition 3.2.31.** We set  $J_{S_\infty} = J \cap I_{S_\infty}$ . Thus,  $J_{S_\infty}$  is the group of idèles of norm 1 that are units at all finite places. We further introduce the set  $S'_\infty = S_\infty \setminus \{v_0\}$  of the infinite places of  $k$  different from our chosen place  $v_0$ , and the function

$$\begin{aligned} l: J_{S_\infty} &\rightarrow \prod_{v \in S'_\infty} \mathbb{R} \\ b &\mapsto (\log \|b_v\|_v)_{v \in S'_\infty}. \end{aligned}$$

**Lemma 3.2.32.**  $l$  is a continuous, surjective homomorphism.

*Proof.* That  $l$  is a homomorphism is obvious from the elementary properties of log. Continuity is equally easy. To see that it is surjective, simply notice that, given any point  $(t_v)_{v \in S'_\infty} \in \mathbb{R}^{S'_\infty}$ , we can certainly find  $(b_v)_{v \in S'_\infty}$  such that  $\log \|b_v\|_v = t_v$  for all  $v \in S'_\infty$ . We extend this to an idèle in  $J_{S_\infty}$  by choosing  $b_{v_0} \in k_{v_0}^\times$  in such a way that  $\prod_{v \in S_\infty} \|b_v\|_v = 1$ , at which point the idèle with finite components equal to 1 and infinite components equal to the  $b_v$  maps to  $(t_v)_{v \in S'_\infty} \in \mathbb{R}^{S'_\infty}$  under  $l$ , as desired.  $\square$

We now describe the intersection  $k^\times \cap J_{S_\infty}$ .

**Lemma 3.2.33.** *The following hold*

1.  $k^\times \cap J_{S_\infty} = \mathcal{O}_k^\times$ ;
2.  $k^\times \cap \ker l = \mu(k)$ , the (finite cyclic) group of roots of unity in  $k$ .

*Proof.* 1. By definition, an idèle in  $J_{S_\infty}$  is a unit at all finite places. If it also an element of  $k$ , then it is a unit of  $\mathcal{O}_k$ .

2. It is a well-known theorem of Kronecker that the units of  $\mathcal{O}_k$  that are of absolute value 1 under all complex embeddings are precisely the roots of unity in  $k$ , see Exercise 3.2.34. Notice that, given  $\alpha \in k^\times \cap \ker l$ , we know that  $\|\alpha\|_v = 1$  for all finite  $v$  and for all  $v \in S'_\infty$ . The product formula (Theorem 3.2.27) then implies that also  $\|\alpha\|_{v_0}$  is equal to 1.  $\square$

**Exercise 3.2.34.** Let  $\alpha \in \mathcal{O}_k^\times$  have absolute value 1 under all complex embeddings of  $k$ . Prove that  $\alpha$  is a root of unity.

*Hint.* Let  $\alpha^n$  be any power of  $\alpha$ . The coefficients of the minimal polynomial of  $\alpha^n$  over  $\mathbb{Q}$  are bounded (since they are combinations with constant coefficients of  $\sigma_i(\alpha^n) = \sigma_i(\alpha)^n$ , which are of absolute value 1). The degrees of these characteristic polynomials are also bounded. Thus, the numbers  $\{\alpha^n\}_{n \in \mathbb{N}}$  are roots of finitely many polynomials; in particular, the set  $\{\alpha^n\}$  is finite. Hence, there exist  $m, n$  such that  $\alpha^m = \alpha^n$ .

Recall now Theorem 1.3.21. Together with its proof, it shows the following. Let  $r = r_1 + r_2 - 1$  and  $\varepsilon_1, \dots, \varepsilon_r$  be a system of generators<sup>5</sup> for the free part of  $\mathcal{O}_k^\times$ . The images  $l(\varepsilon_1), \dots, l(\varepsilon_r)$  form a full-dimensional lattice inside  $\mathbb{R}^r$ . In particular, the  $l(\varepsilon_i)$  form an  $\mathbb{R}$ -basis of  $\mathbb{R}^r$ . Thus, for every  $b \in J_{S_\infty}$ , one can write uniquely

$$l(b) = \sum_{i=1}^r x_i l(\varepsilon_i) \quad (3.14)$$

for some  $x_i \in \mathbb{R}$ . By analogy with the additive case (see Definition 3.2.7), it is natural to consider the ‘fundamental parallelotope’

$$P = \left\{ \sum_{i=1}^r x_i l(\varepsilon_i) \mid x_i \in [0, 1) \right\}. \quad (3.15)$$

This is not (yet) the good fundamental domain for the multiplicative action, for reasons that we will explain below, but is closely related to it. For this reason, it is useful to know the measure of  $P$ , which we compute in the next lemma.

**Lemma 3.2.35.**

$$\int_{l^{-1}(P)} db = \frac{2^{r_1} (2\pi)^{r_2}}{\sqrt{|d_k|}} R,$$

where

$$R = \left| \det \left( \log \|\varepsilon_i\|_v \right)_{\substack{1 \leq i \leq r \\ v \in S'_\infty}} \right|$$

is the regulator of  $k$ .

*Proof.* Let  $Q$  be unit cube  $Q = \{(x_v)_{v \in S'_\infty} : 0 \leq x_v < 1 \ \forall v \in S'_\infty\}$  and let  $X = \prod_{v \in S'_\infty} \mathbb{R}$  be the real vector space in which  $P, Q$  live. Since  $l$  is a surjective homomorphism, we have (see Exercise 3.2.36)

$$\frac{\mu_{I_k}(l^{-1}(P))}{\mu_{I_k}(l^{-1}(Q))} = \frac{\mu_X(P)}{\mu_X(Q)}.$$

By definition, there is a linear map taking  $Q$  to  $P$  whose matrix has the  $l(\varepsilon_i)$  as columns, so the above ratio is equal to the absolute value of the determinant of this matrix, that is,  $R$ . It remains to show that

$$\int_{l^{-1}(Q)} db = \frac{2^{r_1} (2\pi)^{r_2}}{\sqrt{|d_k|}}.$$

<sup>5</sup>this means that the classes of  $\varepsilon_1, \dots, \varepsilon_r$  in  $\mathcal{O}_k^\times / \{\text{roots of unity}\} \cong \mathbb{Z}^r$  form a basis



By definition,  $l^{-1}(Q)$  is the set of  $b \in J_{S_\infty}$  that satisfy  $1 \leq |b|_v < e$  for  $v \in S'_\infty$ . Consider the (more canonical) set  $Q^*$  given by

$$Q^* = \{a \in I_{S_\infty} : 1 \leq \|a\|_v < e \quad \forall v \in S_\infty\}$$

(notice the change from  $S'_\infty$  to  $S_\infty$ ). Fubini's theorem gives

$$\begin{aligned} \int_{Q^*} da &= \int_J \left( \int_{t:tb \in Q^*} \frac{dt}{t} \right) db = \int_{l^{-1}(Q)} \left( \int_{t:1 \leq \|tb\|_{v_0} < e} \frac{dt}{t} \right) db \\ &= \int_{l^{-1}(Q)} \left( \int_{\|b\|_{v_0}^{-1}}^{e\|b\|_{v_0}^{-1}} \frac{dt}{t} \right) db = \int_{l^{-1}(Q)} db, \end{aligned}$$

where we have used:

1.  $tb \in l^{-1}(Q)$  if and only if  $b \in l^{-1}(Q)$  and  $1 \leq \|tb\|_{v_0} < e$  (recall that  $t$  is an idèle whose only non-unitary component is along  $v_0$ );
2. the integral  $\int_{\|b\|_{v_0}^{-1}}^{e\|b\|_{v_0}^{-1}} \frac{dt}{t}$  can be evaluated exactly: it gives  $\log(e\|b\|_{v_0}^{-1}) - \log(\|b\|_{v_0}^{-1}) = \log(e) = 1$ .

Thus, the claim of the lemma is equivalent to the fact that

$$\int_{Q^*} da = \frac{2^{r_1}(2\pi)^{r_2}}{\sqrt{|d_k|}}.$$

Now,  $Q^*$  is a product set: it can be written as  $I^{S_\infty} \times \prod_{v \in S_\infty} \{a_v : 1 \leq \|a_v\|_v < e\}$ . By (2.7), its measure is therefore given by

$$\prod_{v \in S_\infty} \int_{\{a_v: 1 \leq \|a_v\|_v < e\}} d\mu_{k_v^\times} \times \prod_{v \text{ finite}} \int_{\mathfrak{u}_v} d\mu_{k_v^\times}.$$

We compute the factors in this product:

1. if  $v$  is real,

$$\int_{\{a_v: 1 \leq \|a_v\|_v < e\}} d\mu_{k_v^\times} = \int_{(-e, -1] \cup [1, e)} \frac{dt}{t} = 2 \int_1^e \frac{dt}{t} = 2.$$

2. if  $v$  is complex,

$$\int_{\{a_v: 1 \leq \|a_v\|_v < e\}} d\mu_{k_v^\times} = \int_{\{z \in \mathbb{C}: 1 \leq |z| < \sqrt{e}\}} \frac{dz}{|z|^2} = \int_1^{\sqrt{e}} \frac{2rdr}{r^2} \int_0^{2\pi} d\vartheta = 2\pi.$$

For this calculation, one needs to pay attention to the fact that  $\|z\| = |z|^2$ , where  $|\cdot|$  is the usual complex norm. This justifies both the appearance of  $\sqrt{e}$  and the denominator  $r^2$ .

3. for  $v$  finite, by definition  $\mu_{k_v^\times}(\mathfrak{u})$  is  $N(\mathfrak{d}_{k_v})^{-1/2}$ .

Putting everything together we obtain that the measure of  $Q^*$  (hence of  $l^{-1}(Q)$ ) is

$$2^{r_1}(2\pi)^{r_2} \prod_{v \text{ finite}} N(\mathfrak{d}_{k_v})^{-1/2} = 2^{r_1}(2\pi)^{r_2} |d_k|^{-1/2},$$

where the last equality is obtained using Theorem 2.3.20.  $\square$

**Exercise 3.2.36.** Let  $f : G \rightarrow H$  be a surjective homomorphism of locally compact abelian groups and let  $X_1, X_2$  be measurable subsets of  $H$ , with  $0 < \mu_H(X_2) < \infty$ . Prove that

$$\frac{\mu_G(f^{-1}(X_1))}{\mu_G(f^{-1}(X_2))} = \frac{\mu_H(X_1)}{\mu_H(X_2)}.$$

*Hint.* Prove that  $X \mapsto \mu_G(f^{-1}(X))$  is a Haar measure on  $H$ , and rescale by the correct factor.

**Definition 3.2.37** (Multiplicative fundamental domain). Let  $h$  be the class number of  $k$  and let  $b_1, \dots, b_h \in J$  be chosen so that the corresponding ideals  $\varphi(b_1), \dots, \varphi(b_h)$  represent all the ideal classes. Let  $w$  be the number of roots of unity in  $k$ . Let  $l$  be the logarithmic map of Equation (3.14) and  $P$  be the fundamental paralleloptope of Equation (3.15). Define

$$E_0 = \{b \in l^{-1}(P) : 0 \leq \arg(b_{v_0}) < \frac{2\pi}{w}\} \subseteq J_{S_\infty}$$

and

$$E := E_0 b_1 \cup E_0 b_2 \cup \dots \cup E_0 b_h.$$

We call  $E$  the **multiplicative fundamental domain** for  $J \bmod k^\times$ .

**Theorem 3.2.38** (Properties of the multiplicative fundamental domain). 1. *The union*

$$E_0 b_1 \cup E_0 b_2 \cup \dots \cup E_0 b_h$$

*appearing in the definition is disjoint.*

2.  $J = \bigsqcup_{\alpha \in k^\times} \alpha E$  (so that  $E$  deserves its name: it is a set of representatives for  $J \bmod k^\times$ ).

3.

$$\int_E db = \frac{2^{r_1}(2\pi)^{r_2} h R}{\sqrt{|d|} w}.$$

*Proof.* 1. It suffices to observe that  $\varphi(E_0 b_i) = \varphi(b_i)$  since  $E_0$  is by definition a subset of  $J_{S_\infty}$ , which is in the kernel of  $\varphi$  by Lemma 3.2.33.

2. To show that the union is disjoint, it suffices to prove that if we have a solution to

$$\alpha e_1 = e_2$$

with  $e_1, e_2 \in E$  and  $\alpha \in k^\times$ , then  $\alpha = 1$ . Suppose that  $e_i$  is in  $E_0 b_i$  for  $i = 1, 2$ : applying  $\varphi$  we then obtain  $(\alpha)\varphi(b_1) = \varphi(b_2)$ , hence (since the ideal classes  $\varphi(b_i)$  are distinct)  $b_1 = b_2$ . Write  $e_i = c_i b_i$  with  $c_i \in E_0$ . After simplifying a factor  $b_1 = b_2$ , we are left with showing that the equation  $\alpha c_1 = c_2$  with  $c_1, c_2 \in E_0$  and  $\alpha \in k^\times$  has solutions only for  $\alpha = 1$ .

Applying again  $\varphi$  shows  $\varphi(\alpha)\varphi(c_1) = \varphi(c_2)$ , where the principal ideals  $\varphi(c_1), \varphi(c_2)$  are trivial, since  $c_i \in E_0 \subseteq J_{S_\infty}$ . Hence  $\varphi(\alpha)$  is not just principal, but also trivial, and  $\alpha$  is a unit of  $\mathcal{O}_k^\times$ . Writing  $\alpha = \zeta \prod_{j=1}^r \varepsilon_j^{n_j}$  and applying the homomorphism  $l$  we then obtain

$$\sum_j n_j l(\varepsilon_j) = l(\alpha) = l(c_2) - l(c_1).$$

Now observe that the  $n_j$  are integers, while the coefficients of  $l(c_2) - l(c_1)$  in the basis  $l(\varepsilon_1), \dots, l(\varepsilon_r)$  lie in the open interval  $(-1, 1)$ . Hence, the  $n_j$  are all 0, and  $\alpha = \zeta$  is a root of unity in  $E_0$ . It is also a root of unity in  $k^\times$ , hence its order divides  $w$ . On the other hand, by definition,  $0 \leq \arg \alpha_{v_0} < \frac{2\pi}{w}$ , which implies  $\alpha_{v_0} = \zeta_{v_0} = 1$ . Thus, the archimedean embedding  $v_0$  sends  $\alpha$  to 1, and therefore  $\alpha = 1$  as desired.

To show that the union is all of  $J$  we reason essentially in the same way. Start with any idèle  $b \in J$ . There is a unique  $i \in \{1, \dots, r\}$  such that  $bb_i^{-1}$  represents a principal ideal, say  $\alpha\mathcal{O}$  for some  $\alpha \in k^\times$ . The idèle  $bb_i^{-1}\alpha^{-1}$  is then an element of  $J$  representing the trivial ideal, so it is in  $J_{S_\infty}$ . Apply  $l$  and write

$$l(bb_i^{-1}\alpha^{-1}) = \sum_{j=1}^r (n_j + x_j)l(\varepsilon_j),$$

with  $n_j \in \mathbb{Z}$  and  $x_j \in [0, 1)$ . The idèle

$$bb_i^{-1}\alpha^{-1} \prod_{j=1}^r \varepsilon_j^{-n_j}$$

is in  $l^{-1}(P)$ . To land in  $E_0$  we need to adjust the argument of the  $v_0$ -component so that it lies in the interval  $[0, \frac{2\pi}{w})$ . There is a (unique) choice of root of unity  $\zeta$  such that the  $v_0$ -component of  $\zeta^{-1} \left( bb_i^{-1}\alpha^{-1} \prod_{j=1}^r \varepsilon_j^{-n_j} \right)$  satisfies the desired inequality on the argument. The idèle  $bb_i^{-1}\zeta^{-1}\alpha^{-1} \prod_{j=1}^r \varepsilon_j^{-n_j}$  is then in  $E_0$ , which means that we have  $b \in \left( \zeta\alpha \prod_{j=1}^r \varepsilon_j^{n_j} \right) b_i E_0 \subseteq k^\times b_i E_0 \subseteq k^\times E$ , as desired.

3. By definition we have the equalities

$$E = \bigsqcup_{j=1}^h E_0 b_j, \quad l^{-1}(P) = \bigsqcup_{\zeta \in \mu_w} E_0 \zeta,$$

which (together with Lemma 3.2.35) imply

$$\int_E db = h \int_{E_0} db, \quad \frac{2^{r_1} (2\pi)^{r_2}}{\sqrt{|d_k|}} R = \int_{l^{-1}(P)} db = w \int_{E_0} db.$$

Combining these equations gives the claim. □

**Corollary 3.2.39** (Position of  $k^\times$  inside  $J$ ). *The subgroup  $k^\times$  is discrete in  $J$  (hence in  $I_k$ ). The quotient  $J \bmod k^\times$  is compact.*

*Proof.* As in Corollary 3.2.9:  $E$  has non-empty interior (so, up to translation, contains 1 in its interior) and is contained in a compact set.  $\square$

**Remark 3.2.40.** Let  $\tilde{E}$  be another fundamental domain for the multiplicative action (for example,  $\tilde{E} = E^{-1}$ ). Arguing as in the proof of Theorem 3.2.27(2), one sees that if  $f(x) : \mathbb{A}_k \rightarrow \mathbb{C}$  satisfies  $f(\xi x) = f(x)$  for all  $\xi \in k^\times$ , then  $\int_{\tilde{E}} f(a) da = \int_E f(a) da$ .

### The quasi-characters of $I_k/k^\times$

Just like in Section 3.2.1 we worked with functions on  $\mathbb{A}_k$  invariant under translation by  $k$  (because we were secretly interested in functions on  $\mathbb{A}_k/k$ ), we now consider functions (in fact, quasi-characters) of  $I_k$  that trivial on  $k^\times$ . We shall work exclusively with such (quasi-)characters: we will call them **(quasi-)characters of  $I_k/k^\times$** , but we will always treat them as functions defined on  $I_k$  and  $k^\times$ -periodic.

**Remark 3.2.41.** Let  $c$  be a quasi-character of  $I_k/k^\times$ . The restriction of  $c$  to  $J$  is a character (that is, it takes values in  $\mathbb{S}^1$ ), because  $\|c(J)\| = \|c(J \bmod k^\times)\|$  is a continuous image of a compact set, but it is also a group, so it is a compact subgroup of  $\mathbb{R}_{>0}$ . The only such subgroup is  $\{1\}$ .

Suppose moreover that  $c$  is a quasi-character of  $I_k/k^\times$  that is trivial on  $J$ . We claim that  $c$  is of the form  $c(a) = \|a\|^s$  for some complex number  $s$  uniquely determined by  $c$ . Indeed,  $c$  factors via  $I_k/J = T \cong \mathbb{R}^\times$ , and the quotient map is precisely  $a \mapsto \|a\|$ . We are thus reduced to describing the characters of  $\mathbb{R}^\times$ , which we have already done in Exercise 3.1.14.

**Definition 3.2.42** (Exponent of a quasi-character of  $I_k/k^\times$ ). Let  $c$  be a quasi-character of  $I_k/k^\times$ . By the previous remark,  $\|c(a)\| = \|a\|^s$  for some  $s \in \mathbb{C}$ . Since  $\|c(a)\|$  is real and positive,  $s$  is a real number  $\sigma$ . We call this  $\sigma$  the **exponent** of  $c$ .

Note that a quasi-character of  $I_k/k^\times$  is a character if and only if its exponent is 0.

### 3.2.3 Global zeta functions

We now develop the global analogue of the local zeta functions of Section 3.1.3. We begin by introducing the analogue of the class of functions of Definition 3.1.24 in the global setting.

**Definition 3.2.43** (Class of  $\mathfrak{z}$ -functions, global case). We denote by  $\mathfrak{z}$  be the class of all functions  $f : \mathbb{A}_k \rightarrow \mathbb{C}$  that satisfy

1.  $f(x) \in \mathfrak{W}^1(\mathbb{A}_k)$  (that is,  $f(x)$  and its Fourier transform are in  $L^1(\mathbb{A}_k)$  and  $f(x)$  is continuous) and  $\hat{f}(x)$  is continuous.
2. the series  $\sum_{\xi \in k} f(a(x + \xi))$  and  $\sum_{\xi \in k} \hat{f}(a(x + \xi))$  are convergent for every idèle  $a$  and adèle  $x$ . The convergence is uniform in  $(a, x)$  ranging over any (fixed) subset of the form  $K \times D$ , where  $D$  is the additive fundamental domain and  $K$  is a compact subset of  $I_k$ .
3.  $f(a)\|a\|^\sigma$  and  $\hat{f}(a)\|a\|^\sigma$  are in  $L^1(I_k)$  for  $\sigma > 1$ .

**Remark 3.2.44.** We have not asked that  $f$  be continuous on  $I_k$ . However, Exercise 3.2.23 shows that the topology on  $I_k$  is finer than the subspace topology, hence  $f|_{I_k}$  is automatically continuous (both for the subspace topology, which is obvious, and for the restricted product topology).

It should be clear that properties (1) and (2) in Definition 3.2.43 are precisely the hypotheses needed to apply the Riemann-Roch theorem 3.2.21. On the other hand, property (3) is what is needed to mimic the definition of the local zeta functions:

**Definition 3.2.45** ( $\zeta$ -function, global case). Let  $f \in \mathfrak{z}$ . We introduce the function  $\zeta(f, c)$  of quasi-characters  $c$  of  $I_k/k^\times$ , defined for all quasi-characters of exponent greater than 1, by

$$\zeta(f, c) = \int_{I_k} f(a)c(a)da.$$

We call such a function a  $\zeta$ -function of the global field  $k$ .

Notice the complete analogy with the local case: these global  $\zeta$  functions are essentially Fourier transforms on the multiplicative group of idèles, just like the local ones were defined as Fourier transforms on  $k^\times$ . As was the case in Section 3.1.3, we are interested in working with equivalence classes of quasi-characters. The *local* definition of equivalence is that two characters are equivalent if they coincide on the units; its *global* counterpart is the following:

**Definition 3.2.46** (Equivalence class of quasi-character). Let  $c_1, c_2$  be two quasi-characters of  $I_k/k^\times$ . We say that they are **equivalent** if they coincide on  $J$ . The equivalence class of the quasi-character  $c$  is the set of all quasi-characters of the form  $c(a)\|a\|^s$  for  $s \in \mathbb{C}$ .

All the considerations of Section 3.1.3 now apply:  $\zeta(f, c)$  can be considered ‘locally’ (that is, on each equivalence class of quasi-characters) as a function of a complex variable  $s$ , and – when regarded as such – it is a holomorphic function in the domain of quasi-characters of exponent greater than 1 (see Lemma 3.1.27).

The next, and most important, step is now to establish the functional equation and analytic continuation of these global  $\zeta$  functions.

**Theorem 3.2.47** (Analytic continuation and functional equation of the global  $\zeta$ -functions). *Let  $k$  be a number field with standard invariants  $(r_1, r_2)$  (signature),  $h_k, R_k$  (class number and regulator),  $d_k$  (discriminant) and  $w_k$  (number of roots of unity). Let  $f$  be a function of class  $\mathfrak{z}$  and define the constant*

$$\kappa := \frac{2^{r_1}(2\pi)^{r_2}h_kR_k}{\sqrt{|d_k|}w_k},$$

*which (by Theorem 3.2.38(3)) gives the volume of the multiplicative fundamental domain  $E$ . The  $\zeta$ -function  $\zeta(f, c)$  may be extended by analytic continuation to the domain of all quasi-characters. The extended function is meromorphic and has poles only at the quasi-characters  $c(a) = 1$  and  $c(a) = \|a\|$ , where it has simple poles with residues  $-\kappa f(0)$  and  $+\kappa \hat{f}(0)$ . Moreover,  $\zeta(f, c)$  satisfies the functional equation*

$$\zeta(f, c) = \zeta(\hat{f}, \hat{c}),$$

*where  $\hat{c}(a) = \|a\|c(a)^{-1}$ , as in the local theory.*

**Remark 3.2.48.** The reader might find it strange that these  $\zeta$  functions also have a pole at 0, whereas the global zeta functions we are used to from Chapter 1 (say, the Dedekind zeta functions) only have a pole at  $s = 1$ . Two remarks are in order: the first and most important one is that Tate’s global  $\zeta$  functions are analogues of the ‘completed’  $\zeta$  functions

(see e.g. Remark 1.1.10 or the definition of  $\Lambda_K$  in Theorem 1.3.33), and not of the Dedekind zeta functions themselves. The second is that a functional equation of the form  $\Lambda(s) = \Lambda(1-s)$  as in Theorem 1.3.33 certainly implies that any pole at  $s = 1$  should also show up at  $s = 0$ .

Before showing the theorem we state and prove some auxiliary lemmas. We begin with the following simple observation, which can be shown much in the spirit of Lemma 3.2.14:

**Lemma 3.2.49.** *Let  $f : J \rightarrow \mathbb{C}$  be a continuous function such that  $f(x) = f(\alpha x)$  for every  $x \in J, \alpha \in k^\times$ . Then, for any two fundamental domains  $E, E'$  for  $J/k^\times$  having the same measure<sup>6</sup> we have  $\int_E f(b)db = \int_{E'} f(b)db$ .*

*Proof.* The function  $f$  induces a function on the quotient  $J/k^\times$ , and both integrals equal  $\int_{J/k^\times} f(b)db$ , where the Haar measure on the quotient is normalised so that  $\text{vol}(J/k^\times) = \text{vol}(E) = \text{vol}(E')$ .  $\square$

**Remark 3.2.50.** In fact, the lemma is true (with the same proof) under the slightly weaker assumptions that  $f$  is measurable, satisfies  $f(x) = f(\alpha x)$ , and that the induced function  $\bar{f} : J/k^\times \rightarrow \mathbb{C}$  is in  $L^1(J/k^\times)$ . Note that a continuous function on the compact set  $J/k^\times$  is automatically bounded and hence in  $L^1$ .

Our next lemma is a consequence of the Riemann-Roch theorem (Theorem 3.2.21) and will be the crucial ingredient in the proof of Theorem 3.2.47.

**Lemma 3.2.51.** *For a fixed  $t \in T$  define*

$$\zeta_t(f, c) = \int_J f(tb)c(tb) db.$$

*For all quasi-characters  $c$  of  $I_k/k^\times$  we have*

$$\zeta_t(f, c) + f(0) \int_E c(tb) db = \zeta_{1/t}(\hat{f}, \hat{c}) + \hat{f}(0) \int_E \hat{c}\left(\frac{1}{t}b\right) db.$$

*Proof.* Recall from Theorem 3.2.38 that  $J = \bigsqcup_{\alpha \in k^\times} \alpha E$ . We start by writing

$$\zeta_t(f, c) + f(0) \int_E c(tb) db = \sum_{\alpha \in k^\times} \int_{\alpha E} f(tb)c(tb) db + f(0) \int_E c(tb) db.$$

Using the translation-invariance of the Haar measure and writing  $b = \alpha b$ , we rewrite this as

$$\sum_{\alpha \in k^\times} \int_E f(\alpha tb)c(\alpha tb) db + f(0) \int_E c(tb) db.$$

Now use the fact that  $c(\alpha) = 1$  since  $c$  is trivial on  $k^\times$  and the uniform convergence of the sum  $\sum_{\alpha \in k^\times} f(\alpha tb)$  (property (2) in Definition 3.2.43, applied to the relatively compact subset  $E$ ) to further rewrite the above as

$$\begin{aligned} \zeta_t(f, c) + f(0) \int_E c(tb) db &= \int_E \left( \sum_{\alpha \in k^\times} f(\alpha tb) \right) c(tb) db + \int_E f(0)c(tb) db \\ &= \int_E \left( \sum_{\xi \in k} f(\xi tb) \right) c(tb) db. \end{aligned} \tag{3.16}$$

<sup>6</sup>this property is in fact automatic: one can show it as in the proof of Theorem 3.2.27.

We are now in a position to apply Theorem 3.2.21 to the inner sum, which yields

$$\zeta_t(f, c) + f(0) \int_E c(tb) db = \int_E \left( \sum_{\xi \in k} \hat{f} \left( \frac{\xi}{tb} \right) \right) \frac{1}{\|tb\|} c(tb) db.$$

We now observe that  $b \mapsto 1/b$  is an involution of the abelian group  $J$ , hence sends the Haar measure to itself (indeed, let  $g$  be this automorphism. Then  $g^* db = \gamma db$  for some constant  $\gamma > 0$ , hence  $db = g^* g^* db = \gamma^2 db$  and  $\gamma = 1$ ). We also recall that  $E^{-1}$  is another multiplicative fundamental domain (Remark 3.2.40), and observe that the function  $g(tb) = \left( \sum_{\xi \in k} \hat{f} \left( \frac{\xi}{tb} \right) \right) \frac{1}{\|tb\|} c(tb)$  satisfies  $g(\eta tb) = g(tb)$  for all  $\eta \in k^\times$ , so that  $\int_E f(a) da = \int_{E^{-1}} f(a) da$  (see Lemma 3.2.49). Combining these observations, we arrive at the representation

$$\zeta_t(f, c) + f(0) \int_E c(tb) db = \int_E \left( \sum_{\xi \in k} \hat{f} \left( \frac{\xi b}{t} \right) \right) \frac{\|b\|}{\|t\|} c(t/b) db = \int_E \left( \sum_{\xi \in k} \hat{f} \left( \xi \frac{1}{t} b \right) \right) \hat{c}(b/t) db.$$

On the other hand, we can restart from Equation (3.16) and replace  $f \rightarrow \hat{f}, t \rightarrow 1/t, c \rightarrow \hat{c}$  to obtain

$$\zeta_{1/t}(\hat{f}, \hat{c}) + \hat{f}(0) \int_E \hat{c}(b/t) db = \int_E \left( \sum_{\xi \in k} \hat{f} \left( \xi \frac{1}{t} b \right) \right) \hat{c}(b/t) db.$$

Comparing the last two equations yields the lemma. □

**Lemma 3.2.52.** *Let  $c$  be a quasi-character of  $I_k/k^\times$  and let  $t \in T$ . We have*

$$\int_E c(tb) db = \begin{cases} \kappa t^s, & \text{if } c(a) = \|a\|^s \\ 0, & \text{if } c \text{ is non-trivial on } J \end{cases}$$

*Proof.* Hopefully, this should be familiar by now: the condition  $c(a) = \|a\|^s$  is equivalent to  $c$  being trivial on  $J$ , see Remark 3.2.41. Since  $E$  is a fundamental domain for  $J \bmod k^\times$  (Theorem 3.2.38), the integral in the statement is simply

$$\int_{J \bmod k^\times} c(tb) db = c(t) \int_{J \bmod k^\times} c(b) db.$$

Furthermore,  $c(b)$  is a character on  $J \bmod k^\times$  (Remark 3.2.41 again), so we are integrating a character on a compact group: the result is either the measure of that compact group, if the character is trivial, or 0, if it is not. In the former case, we also need to apply Theorem 3.2.38(3) and observe that  $\|t\| = t$  since  $t$  is essentially a positive real number (hence  $c(t) = \|t\|^s = t^s$ ). □

*Proof of Theorem 3.2.47.* Using Fubini's theorem, for  $c$  of exponent greater than 1 we can write the integral over  $I_k = J \times T$  that defines  $\zeta(f, c)$  as

$$\zeta(f, c) = \int_{I_k} f(a) c(a) da = \int_0^\infty \left( \int_J f(tb) c(tb) db \right) \frac{dt}{t} = \int_0^\infty \zeta_t(f, c) \frac{dt}{t},$$

where

$$\zeta_t(f, c) = \int_J f(tb) c(tb) db$$

as in Lemma 3.2.51. We split the integral from 0 to  $\infty$  as

$$\zeta(f, c) = \int_0^1 \zeta_t(f, c) \frac{dt}{t} + \int_1^\infty \zeta_t(f, c) \frac{dt}{t}.$$

Notice that (using Fubini in reverse) we have

$$\int_1^\infty \zeta_t(f, c) \frac{dt}{t} = \int_{\substack{a \in I \\ \|a\| \geq 1}} f(a)c(a) da.$$

By assumption (property (3) in Definition 3.2.43), the integral over all of  $I$  converges (absolutely) for  $c$  of exponent greater than 1. But if the exponent of  $c'$  is smaller than the exponent of  $c$  we have  $|f(a)c'(a)| \leq |f(a)c(a)|$  for  $\|a\| \geq 1$ , so convergence of the integral  $\int_{\|a\| \geq 1} f(a)c(a) da$  for  $c$  implies convergence for  $c'$ . Since the integral converges for  $c$  of exponent greater than 1, it converges for all  $c$ . Consider then  $\int_0^1 \zeta_t(f, c) \frac{dt}{t}$ . We rewrite this integral using Lemmas 3.2.51 and 3.2.52. Consider first the case when  $c$  is non-trivial on  $J$ . Then, Lemmas 3.2.51 and 3.2.52 together imply  $\zeta_t(f, c) = \zeta_{1/t}(\hat{f}, \hat{c})$ , hence

$$\int_0^1 \zeta_t(f, c) \frac{dt}{t} = \int_0^1 \zeta_{1/t}(\hat{f}, \hat{c}) \frac{dt}{t}.$$

On the other hand, if  $c$  is trivial on  $J$  then it is of the form  $c(a) = \|a\|^s$  for some  $s \in \mathbb{C}$ , and Lemmas 3.2.51 and 3.2.52 yield

$$\begin{aligned} \int_0^1 \zeta_t(f, c) \frac{dt}{t} &= \int_0^1 \left( \zeta_{1/t}(\hat{f}, \hat{c}) + \hat{f}(0) \int_E \hat{c} \left( \frac{1}{t}b \right) db - f(0) \int_E c(tb) db \right) \frac{dt}{t} \\ &= \int_0^1 \left( \zeta_{1/t}(\hat{f}, \hat{c}) + \hat{f}(0) \int_E \left\| \frac{1}{t}b \right\|^{1-s} db - f(0)\kappa t^s \right) \frac{dt}{t} \\ &= \int_0^1 \left( \zeta_{1/t}(\hat{f}, \hat{c}) + \hat{f}(0)\kappa t^{s-1} - f(0)\kappa t^s \right) \frac{dt}{t}. \end{aligned}$$

Now observe that  $t \mapsto t^{-1}$  preserves the Haar measure on  $\mathbb{R}_{>0}$ , yielding

$$\int_0^1 \zeta_{1/t}(\hat{f}, \hat{c}) \frac{dt}{t} = \int_1^\infty \zeta_t(\hat{f}, \hat{c}) \frac{dt}{t}.$$

By the same argument used above, this integral is analytic for all  $c$ .

Carrying out the (trivial) integration of  $t^{s-1}$ ,  $t^s$  (assuming  $\Re s > 1$ ), we have thus obtained

$$\zeta(f, c) = \int_1^\infty \zeta_t(f, c) \frac{dt}{t} + \int_1^\infty \zeta_t(\hat{f}, \hat{c}) \frac{dt}{t} + \mathbf{1}_{c=\|\cdot\|^s} \cdot \kappa \left( \frac{\hat{f}(0)}{s-1} - \frac{f(0)}{s} \right)$$

for all quasi-characters of exponent greater than 1. The first two summands in this expression are analytic for all  $c$ , while the last two terms (when  $c = \|\cdot\|^s$ ) clearly have meromorphic continuation to  $\mathbb{C}$ . They also let us read off the poles and residues of  $\zeta(f, c)$  directly.

Finally, the functional equation follows trivially: if  $c$  is not of the form  $c(a) = \|a\|^s$ , the expression above is unchanged under the substitution  $(f, c) \leftrightarrow (\hat{f}, \hat{c})$ . When  $c(a) = \|a\|^s$ , the dual character is  $\hat{c}(a) = \|a\|^{1-s}$ , so the substitution  $(f, c) \leftrightarrow (\hat{f}, \hat{c})$  also replaces  $s \leftrightarrow 1-s$ , which shows the desired invariance.  $\square$



### 3.3 Hecke $L$ -functions, reprise

Following Tate, in the development of the global theory we have worked with (quasi-)characters of  $I_k$  that are trivial on  $k^\times \subset I_k$ . We have not fully motivated this choice yet. In this section we try to give some background for why this choice is natural, and how characters of  $I_k/k^\times$  relate to our previous definition of Hecke  $L$ -functions (Definition 1.4.9).

This is a good time for the following definition:

**Definition 3.3.1** (Hecke character, idèlic version). A **Hecke (quasi-)character** of  $k$  is a quasi-character of  $I_k$  that is trivial on  $k^\times$ .

**Remark 3.3.2.** Following the general use, in this section we shall simply write *Hecke characters* even when we mean *Hecke quasi-characters*.

Hecke had an ideal-theoretic definition of his characters that is however substantially less easy to work with than the previous one. The interested reader can find it in [Wik23a]; we shall essentially re-derive Hecke's formulas for his characters below, where however they will not be taken as the *definition*, but purely as a *consequence* of the general theory (see Remark 3.4.2).

To each Hecke character we can attach an  $L$ -function in a way that looks different from Definition 1.4.9. We will discuss below the relationship between the two.

**Definition 3.3.3** (Hecke  $L$ -function). Given an (idèlic) Hecke character  $\chi$ , let  $S$  be the set of finite places of  $k$  at which  $\chi$  is ramified (=not unramified). We define the corresponding  $L$ -function as

$$L(s, \chi) = \prod_{\mathfrak{p} \notin S} \left( 1 - \frac{\chi(\mathfrak{p})}{(N\mathfrak{p})^s} \right)^{-1},$$

for  $\Re s$  sufficiently large to make the product converge (when  $\chi$  is of exponent 0 – that is, when  $\chi$  is a character in the strict sense of the word – the product converges at least over  $\{\Re s > 1\}$ ).

In the previous formula, the symbol  $\chi(\mathfrak{p})$  is taken to mean the character  $\chi$  evaluated at any idèle  $b(\mathfrak{p})$  that is trivial at all  $v \neq \mathfrak{p}$  and such that  $b(\mathfrak{p})_{\mathfrak{p}}$  is a uniformiser at  $\mathfrak{p}$ .

**Remark 3.3.4.** By assumption,  $\chi$  is unramified at all places  $v \notin S$ . Any two choices of uniformisers at  $\mathfrak{p}$  differ by a unit in  $u_{\mathfrak{p}}$ , and since  $\chi$  is unramified at  $\mathfrak{p}$  (=trivial on  $u_{\mathfrak{p}}$ ) we obtain that  $\chi(\mathfrak{p})$  is well-defined.

Connecting Definitions 1.4.9 and 3.3.3 is not at all trivial, and largely depends on class field theory. Developing class field theory would require a substantial effort, so we keep this discussion to a minimum. The following theorem condenses many results in class field theory in a form that is suitable for our application:

**Theorem 3.3.5** (Class field theory for number fields). *Let  $k$  be a number field and denote by  $k^{\text{ab}}$  the maximal abelian extension of  $k$  (inside a fixed algebraic closure). There is a canonical surjective map  $\vartheta : I_k \rightarrow \text{Gal}(k^{\text{ab}}/k)$  that satisfies:*

1.  $\vartheta$  is trivial on  $k^\times$ .
2. let  $L/k$  be a finite Galois extension of  $k$  with abelian Galois group, so that there is a canonical surjection  $I_k \xrightarrow{\vartheta} \text{Gal}(k^{\text{ab}}/k) \xrightarrow{\pi} \text{Gal}(L/k)$ . Let  $\mathfrak{p}$  be a place of  $k$  that is unramified in  $L$ , and define a corresponding idèle<sup>7</sup>  $b(\mathfrak{p})$  as in Definition 3.3.3. Then, the Artin symbol

<sup>7</sup>by abuse of notation, the idèle  $b(\mathfrak{p})$  is usually denoted simply by  $\mathfrak{p}$ . From now on, we adopt this convention.

$\left(\frac{L/k}{\mathfrak{p}}\right)$  (which is well-defined, because the extension is abelian) coincides with  $\pi(\vartheta(b(\mathfrak{p})))$ .

3. with the same notation as in the previous part, for every prime  $\mathfrak{q}$  of  $k$ ,  $\pi(\vartheta(\mathfrak{u}_{\mathfrak{q}}))$  is the inertia group at (any place lying over)  $\mathfrak{q}$  for the extension  $L/k$ .

With this (hard) theorem in hand, it is not too difficult to reconnect Definitions 1.4.9 and 3.3.3. Fix a finite Galois extension  $L/k$  with group  $G$  and a character  $\chi : G \rightarrow \mathbb{C}^\times$ . The character  $\chi$  factors via the abelianisation of  $G$ , hence it factors via  $\tilde{\chi} : \text{Gal}(F/k) \rightarrow \mathbb{C}^\times$ , where  $F/k$  is the maximal abelian sub-extension of  $L/k$ . By Theorem 1.4.12, the  $L$ -functions of  $\chi$  and  $\tilde{\chi}$  coincide, hence we can and do assume that  $L = F$  is abelian over  $k$  and that  $\tilde{\chi} = \chi$ . The character  $\chi$  now gives an idèlic Hecke character  $\chi_{\text{Hecke}}$ , defined simply as the composition

$$\chi_{\text{Hecke}} = \chi \circ \pi \circ \vartheta,$$

where  $\vartheta$  is the map of Theorem 3.3.5 and  $\pi$  is the canonical projection  $\text{Gal}(k^{\text{ab}}/k) \rightarrow \text{Gal}(L/k)$ . The two Hecke  $L$ -functions are now easily seen to have the same local factors:

1. both  $L$ -functions have trivial local factors at primes  $v \in S$ . This is true by definition for the  $L$ -function of Definition 3.3.3, and is easy to check for the (Artin)  $L$ -function of Definition 1.4.9: we simply need to show that  $V^{I_{\mathfrak{p}}}$  is trivial, and this follows immediately from part (3) of Theorem 3.3.5 together with the construction of the set  $S$  in Definition 3.3.3.
2. both  $L$ -functions have the same local factor at primes  $\mathfrak{p} \notin S$ . We have to check that

$$\chi_{\text{Hecke}}(\mathfrak{p}) = \chi \left( \left( \frac{L/k}{\mathfrak{p}} \right) \right),$$

and this is a consequence of Theorem 3.3.5(2) (simply use the definition  $\chi_{\text{Hecke}}(\mathfrak{p}) = \chi(\pi(\vartheta(\mathfrak{p})))$ ).

Thus, we see that Definition 1.4.9 captures a large part of the class of Hecke  $L$ -functions, but not all of them: essentially, in Definition 1.4.9 we were only considering those characters that factor via the Galois group  $\text{Gal}(k^{\text{ab}}/k)$  and (in particular) have finite image (so that they further factor via the Galois group of some finite abelian extension  $L/k$ ). Hecke's original definition is more general. However, we will see below (Example 3.4.4) that in the case  $k = \mathbb{Q}$  both definitions are essentially the same, and reduce to Dirichlet's  $L$ -functions.

### 3.4 Characters of the idèles

We now describe the equivalence classes of (quasi-)characters of  $I_k$  that are trivial on  $k^\times$ , where  $k$  is a number field. We begin by noticing that each equivalence class of quasi-characters of  $I_k$  contains a character. If  $c$  is a quasi-character of  $I_k$ , then  $c|_J$  is a quasi-character of a compact group, hence a character. In particular, the restriction of  $|c|$  to  $J$  is trivial. This implies that  $|c|$  is a quasi-character of the group  $I_k/J \cong \mathbb{R}_{>0}$  (recall that  $J$  is the kernel of the norm map  $I_k \rightarrow \mathbb{R}_{>0}$  sending  $a$  to  $\|a\|$ ), and as such,  $|c(a)| = \|a\|^s$  for some  $s \in \mathbb{C}$ . Since  $|c(a)|$  is a real number,  $s$  is also a real number. The quasi-character  $c$  lies in the same equivalence class as the character  $c(a) \cdot \|a\|^{-s}$ . From now on, we shall therefore only work with *characters*.

By Theorem 2.4.14, any character of  $I_k$  is a product

$$c(a) = \prod_v c_v(a_v)$$

of local characters  $c_v$ , where all but finitely many  $c_v$  are trivial on  $\mathfrak{u}_v$ . We say that  $c$  is **unramified** at  $v$  if and only if  $c_v|_{\mathfrak{u}_v}$  is trivial.

We fix a finite set  $S$  of places (containing all the archimedean ones) such that  $c_v$  is trivial on  $\mathfrak{u}_v$  for every  $v \notin S$  (which we say concisely as ‘ $c$  is unramified outside  $S$ ’). We start by observing that, for  $v \notin S$ , the characters  $c_v$  ‘factor via the group of ideals prime to  $S$ ’, in the following precise sense.

**Definition 3.4.1.** We let  $\varphi_S$  be the map

$$\begin{aligned} \varphi_S : \quad I_k &\rightarrow \mathcal{F}(S) := \{\text{fractional ideals } I \mid v(I) = 0 \quad \forall v \in S, v \text{ finite}\} \\ a = (a_v)_v &\mapsto \prod_{v \notin S} \mathfrak{p}_v^{v(a_v)}. \end{aligned}$$

It is a homomorphism (with respect to the natural product structure on the set on the right) with kernel  $I_S$ .

Define now  $c^*(a) = \prod_{v \notin S} c_v(a_v)$ . Since  $c_v(a_v)$  only depends on the  $v$ -adic valuation of  $a_v$ , the character  $c^*$  factors via  $\varphi_S$ . We write

$$c^*(a) = \chi(\varphi_S(a))$$

for some character  $\chi$  of  $\mathcal{F}(S)$ . On the other hand, by Theorem 3.1.16, each character  $c_v$  for  $v \in S$  can be written as

$$c_v(a_v) = \tilde{c}_v(\tilde{a}_v) \|a_v\|_v^{it_v},$$

where for each  $a_v \in K_v^\times$  we have written  $a_v = \|a_v\| \cdot \tilde{a}_v$  for some  $\tilde{a}_v$  of norm 1 (and  $\tilde{c}_v$  is a character of  $\mathfrak{u}_v$ ). We have thus expressed our character  $c$  in the form

$$c(a) = \prod_{v \in S} \tilde{c}_v(\tilde{a}_v) \cdot \prod_{v \in S} \|a_v\|_v^{it_v} \cdot \chi(\varphi_S(a)).$$

Thus, the choice of  $c$  amounts to the choice of the following data:

1. the characters  $\tilde{c}_v$  of  $\mathfrak{u}_v$ , for  $v \in S$ ;
2. the real numbers  $t_v$ ;
3. a character  $\chi$  of the group  $\mathcal{F}(S)$ ,

subject to the condition that  $c(\alpha) = 1$  for all  $\alpha \in k^\times$ . We now make this condition more explicit.

Suppose that  $|S| = m + 1$  and fix a system of generators<sup>8</sup>  $\varepsilon_1, \dots, \varepsilon_m$  for the group of  $S$ -units of  $k$  (see Theorem 1.3.25). Also denote by  $\varepsilon_0$  a generator of the finite group of roots of unity in  $k^\times$ , so that  $\langle \varepsilon_0, \dots, \varepsilon_m \rangle = \mathcal{O}_{k,S}^\times$ . Notice that every  $\varepsilon \in \mathcal{O}_{k,S}^\times = k^\times \cap I_S$  satisfies  $\varphi_S(\varepsilon) = (1)$ ,

---

<sup>8</sup>a **system of generators** is a set of elements in  $\mathcal{O}_{k,S}^\times$  whose images in  $\mathcal{O}_{k,S}^\times/\text{torsion}$  form a basis of this free abelian group.

and so  $\chi(\varphi_S(a)) = 1$ . The condition that  $c$  be trivial on  $\mathcal{O}_{k,S}^\times$  implies in particular  $c(\varepsilon_0) = 1$ , hence

$$\prod_{v \in S} \tilde{c}_v(\varepsilon_0) = 1. \quad (3.17)$$

Notice that  $\|\varepsilon_0\|_v = 1$  for all  $v \in \Omega_k$ .

Suppose now that we have fixed a family  $\tilde{c}_v$  for  $v \in S$  that satisfies condition (3.17). The equality  $c(\varepsilon_i) = 1$  for  $i = 1, \dots, m$  is satisfied if and only if (for *some* determination of the logarithms) we have

$$\prod_{v \in S} \tilde{c}_v(\tilde{\varepsilon}_{i,v}) \|\varepsilon_{i,v}\|_v^{it_v} = 1 \Leftrightarrow \sum_{v \in S} t_v \log \|\varepsilon_{i,v}\|_v = i \log \left( \prod_{v \in S} \tilde{c}_v(\varepsilon_v) \right), \quad (3.18)$$

which is a linear system of  $m$  equations in the  $m+1$  unknowns  $t_v$ . One can show (it is part of Theorem 1.3.25) that the matrix of the linear system (3.18) has maximal rank, hence the space of solutions is non-empty (and more precisely is 1-dimensional). We can be even more explicit: since for every  $S$ -unit  $\varepsilon$  and every place  $v \notin S$  we have  $\|\varepsilon\|_v = 1$ , it follows from Theorem 2.3.8 (which we have now proved as Theorem 3.2.27) that

$$0 = \log 1 = \log \prod_v \|\varepsilon\|_v = \sum_v \log \|\varepsilon\|_v = \sum_{v \in S} \log \|\varepsilon\|_v.$$

In particular,  $\sum_{v \in S} \log \|\varepsilon_{i,v}\|_v = 0$  for all  $i = 1, \dots, m$ , so a generator for the kernel of the matrix corresponding to the linear system (3.18) is the vector all of whose coordinates are equal to 1. Thus, given a solution  $\{t_v\}_{v \in S}$ , all other solutions are of the form  $\{t_v + t\}_{v \in S}$  for some  $t \in \mathbb{R}$ .

Finally, for a given choice of  $(\tilde{c}_v)_{v \in S}$  satisfying (3.17) and a choice of  $(t_v)_{v \in S}$  satisfying (3.18), what conditions should  $\chi$  satisfy? The choice is very constrained (often unique): for all  $\alpha \in k^\times$  we must have

$$1 = c(\alpha) = \prod_{v \in S} \tilde{c}_v(\alpha) \|\alpha\|_v^{it_v} \cdot \chi(\varphi_S(a)),$$

which means that  $\chi(\varphi_S(a))$  is uniquely determined by the formula

$$\chi(\varphi_S(a)) = \prod_{v \in S} \tilde{c}_v(\alpha)^{-1} \|\alpha\|_v^{-it_v}. \quad (3.19)$$

**Remark 3.4.2.** Equations (3.17), (3.18) and (3.19) essentially give Hecke's original description of the Hecke characters.

**Exercise 3.4.3.** Let  $f : k^\times \rightarrow \mathcal{F}(S)$  be the map sending each element  $x \in k^\times$  to the ideal obtained from  $(x)$  by deleting all primes in  $S$  from its factorisation (formally, if  $(x) = \prod_{\mathfrak{p} \in S} \mathfrak{p}^{v_{\mathfrak{p}}(x)} \cdot \prod_{\mathfrak{p} \notin S} \mathfrak{p}^{v_{\mathfrak{p}}(x)}$ , then  $f(x) = \prod_{\mathfrak{p} \notin S} \mathfrak{p}^{v_{\mathfrak{p}}(x)}$ ).

1. Prove that  $f$  is a homomorphism, and therefore its image is a subgroup of  $\mathcal{F}(S)$ .
2. Show that the image of  $f$  is a subgroup of finite index of  $\mathcal{F}(S)$ . Prove that this index is at most  $h$ , the class number of  $k$ .

Using the notation of the previous exercise, we have proved that  $\chi$  is uniquely determined on the subgroup  $f(k^\times)$ . In order to determine  $\chi$ , we must choose one of the (finitely many) extensions of  $\chi|_{f(k^\times)}$  to  $\mathcal{F}(S)$ .

**Example 3.4.4** (Dirichlet characters as idèlic Hecke characters of  $\mathbb{Q}$ ). Take  $k = \mathbb{Q}$ . We claim that the idèles  $I_k$  decompose as the direct product

$$\hat{\mathbb{Z}}^\times \times \mathbb{Q}^\times \times \mathbb{R}_{>0}^\times; \tag{3.20}$$

this is essentially a reflection of the fact that  $\mathbb{Z}$  has unique factorisation. More precisely, given any idèle  $(a_v)_{v \in \Omega_{\mathbb{Q}}} = ((\tilde{a}_p p^{e_p})_p, t)$  with  $t \in \mathbb{R}^\times$ ,  $\tilde{a}_p \in \mathbb{Z}_p^\times$ , and  $e_p = 0$  for almost all  $p$ , introduce the rational number  $r := \text{sgn}(t) \prod_p p^{-e_p}$ . It is then clear that  $ra$  is an idèle that lies in  $\prod_p \mathbb{Z}_p^\times \times \mathbb{R}_{>0}^\times$ ; from this, the decomposition (3.20) follows easily. Moreover, under this isomorphism,  $\mathbb{Q}^\times \subset I_{\mathbb{Q}}$  corresponds to the direct factor  $\{1\} \times \mathbb{Q}^\times \times \{1\}$ . Thus, a quasi-character of  $I_{\mathbb{Q}}$  trivial on  $\mathbb{Q}^\times$  is simply a quasi-character of  $\hat{\mathbb{Z}}^\times \times \mathbb{R}_{>0}^\times$ , hence is the product of a quasi-character of  $\hat{\mathbb{Z}}^\times$  and a quasi-character of  $\mathbb{R}_{>0}^\times$ .

1. We claim that every continuous quasi-character  $\chi$  of  $\hat{\mathbb{Z}}^\times$  factors via a finite quotient. This follows from Exercise 3.1.18: if  $U$  is a sufficiently small neighbourhood of 1 in  $\mathbb{C}^\times$  (containing no non-trivial subgroups),  $\chi^{-1}(U)$  is open. On the other hand,  $\chi(\chi^{-1}(U))$  is a subgroup contained in  $U$ , so it is trivial. It follows that  $\ker \chi$  contains the open neighbourhood of the identity  $\chi^{-1}(U)$ , and therefore is open in  $\hat{\mathbb{Z}}^\times$ . Since every open subgroup of  $\hat{\mathbb{Z}}^\times$  has finite index, the claim follows. In particular,  $\chi$  is a character (and not just a quasi-character), because it factors via a quasi-character of a finite group, and every quasi-character of a finite group is a character.

Finally, it is easy to see that the subgroups of the form  $\{x \in \hat{\mathbb{Z}}^\times : x \equiv 1 \pmod{m}\}$  form a fundamental system of neighbourhoods of the identity in  $\hat{\mathbb{Z}}^\times$ , as  $m$  varies in  $\mathbb{N}$ . We obtain that every quasi-character of  $\hat{\mathbb{Z}}^\times$  factors via a quotient  $\frac{\hat{\mathbb{Z}}^\times}{\{x \in \hat{\mathbb{Z}}^\times : x \equiv 1 \pmod{m}\}} \cong (\mathbb{Z}/m\mathbb{Z})^\times$ . Thus, there is a bijection between the characters of  $\hat{\mathbb{Z}}^\times$  and the pairs  $(m, \tilde{\chi})$  where  $\tilde{\chi}$  is a primitive character modulo  $m$ .

2. The quasi-characters of  $\mathbb{R}_{>0}^\times$  are easy to describe: we have seen in Exercise 3.1.14 that they are all of the form  $t \mapsto t^s$  with  $s \in \mathbb{C}$ .

We can then write every Hecke character of  $\mathbb{Q}$  as

$$\chi((a_v)_{v \in \Omega_{\mathbb{Q}}}) = \tilde{\chi}(\pi_m(a_v)) \cdot |a_\infty|^s,$$

where  $\tilde{\chi}$  is a primitive character modulo  $m$  and  $\pi_m$  is the composition of the isomorphism  $I_{\mathbb{Q}} \cong \hat{\mathbb{Z}}^\times \times \mathbb{Q}^\times \times \mathbb{R}_{>0}^\times$  with the canonical projection  $\hat{\mathbb{Z}}^\times \rightarrow (\mathbb{Z}/m\mathbb{Z})^\times$ . It is easy to see from the definition that  $\chi$  is ramified precisely at the primes dividing  $m$ . Moreover, as  $b(p)$  (see Definition 3.3.3) we can take the idèle  $(1, 1, \dots, p, 1, \dots)$  with  $p$  in the position corresponding to the factor  $\mathbb{Q}_p$ . The  $L$ -function of the character  $\chi$  is therefore

$$\prod_{p \nmid m} (1 - \chi((b_p))p^{-s})^{-1} = \prod_{p \mid m} (1 - \tilde{\chi}(p \pmod{m})p^{-s})^{-1} = L(s, \tilde{\chi}),$$

where  $L(s, \tilde{\chi})$  is the Dirichlet  $L$ -function of the character  $\tilde{\chi}$  from Definition 1.1.23. Since we have already checked that Dirichlet  $L$ -functions are Artin  $L$ -functions (Proposition 1.4.6), we see that for  $k = \mathbb{Q}$  all our many definitions of (abelian)  $L$ -functions coincide.

### 3.5 Recovering the classical theory

Our purpose in this section is to prove the main analytic results we have assumed in Chapter 1, namely the functional equation and analytic continuation for Dedekind  $\zeta$ -functions (Theorem 1.3.33) and Hecke  $L$ -functions (Theorem 1.4.11), and the analytic class number formula (Theorem 1.5.35). We will of course do this by showing that the (completed)  $\zeta$  functions, and suitable completed Hecke  $L$ -functions, are global  $\zeta$  functions in the sense of Tate.

Before treating the general case in detail, we sketch the special case of the Dedekind zeta functions, starting with the case  $k = \mathbb{Q}$  of the Riemann zeta function. Below we will check (in much greater generality) that all the results we invoke can indeed be applied, in the sense that the necessary technical assumptions (e.g., convergence of certain integrals) are all satisfied.

#### 3.5.1 The Riemann zeta function

The ground field is  $k = \mathbb{Q}$ . We take  $c$  to be the trivial character of  $I_k$ , and define a function  $f$  on the adèles by setting

$$f(x) = \prod_p f_p(x_p) \cdot f_\infty(x_\infty),$$

where  $f_p$  is the characteristic function of  $\mathbb{Z}_p \subset \mathbb{Q}_p$  and  $f_\infty$  is  $t \mapsto e^{-\pi t^2}$  (cf. Section 3.1.4). One can show that  $f$  is of class  $\mathfrak{z}$ . We compute the Fourier transform of  $f$  as

$$\hat{f}(y) = \prod_v \hat{f}_v(y) = f_\infty(y) \cdot \prod_p f_p(y) = f(y),$$

where we have used the results of Section 3.1.4, that show  $\hat{f}_p = f_p$  for each prime  $p$  and  $\widehat{f_\infty} = f_\infty$ . Theorem 3.2.47 now implies

$$\zeta(f, \|\cdot\|^s) = \zeta(f, \|\cdot\|^{1-s}).$$

Finally, we express  $\zeta(f, \|\cdot\|^s)$  as a product of local factors as

$$\prod_v \zeta(f_v, \|\cdot\|^s) = \pi^{-s/2} \Gamma\left(\frac{s}{2}\right) \prod_p (1 - p^{-s})^{-1} = \pi^{-s/2} \Gamma\left(\frac{s}{2}\right) \zeta(s).$$

Thus, Theorem 3.2.47 gives us the functional equation and analytic continuation for the  $\zeta$  function, together with the information that the residue at  $s = 1$  is  $\kappa \hat{f}(0) = 1$ . It also finally justifies Remark 1.1.10, in the sense that the function  $\pi^{-s/2} \Gamma\left(\frac{s}{2}\right) \zeta(s)$  naturally appears as a global  $\zeta$  function of the field  $\mathbb{Q}$ .

#### 3.5.2 Dedekind $\zeta$ functions

The case of Dedekind zeta functions is not much harder. We take  $c = 1$  and  $f_v$  to be the 'standard' function considered in Section 3.1.4 for the trivial character. Explicitly,

$$f_v(\xi) = \begin{cases} e^{-\pi \|\xi\|_v^2}, & v \text{ real} \\ e^{-2\pi \|\xi\|_v}, & v \text{ complex} \\ \mathbf{1}_{\mathcal{O}_v}, & v \text{ finite and unramified in } k \\ \mathbf{1}_{\mathfrak{o}_v^{-1}}(\xi), & v \text{ finite and ramified} \end{cases}$$

Note that for all but finitely many  $v$  we have  $f_v = \mathbf{1}_{\mathfrak{u}_v}$ . The Fourier transform is  $\prod_v \hat{f}_v$ , where

$$\hat{f}_v(\xi) = \begin{cases} f_v(\xi), & v \text{ real} \\ f_v(\xi), & v \text{ complex} \\ f_v(\xi), & v \text{ finite and unramified in } k \\ (N\mathfrak{d}_v)^{1/2} \mathbf{1}_{\mathcal{O}_v}(\xi), & v \text{ finite and ramified.} \end{cases}$$

Write

$$\Gamma_{\mathbb{R}}(s) = \pi^{-s/2} \Gamma(s/2), \quad \Gamma_{\mathbb{C}}(s) = (2\pi)^{1-s} \Gamma(s) \quad (3.21)$$

for the local  $\zeta$  functions  $\zeta(f_v, \|\cdot\|^s)$  at the archimedean places (we get different functions according to whether  $v$  is real or complex).

The  $\zeta$  function corresponding to  $f$  is

$$\begin{aligned} \prod_v \zeta(f_v, \|\cdot\|^s) &= \Gamma_{\mathbb{R}}(s)^{r_1} \Gamma_{\mathbb{C}}^{r_2} \prod_{v \text{ finite}} \zeta(f_v, \|\cdot\|^s) \\ &= \Gamma_{\mathbb{R}}(s)^{r_1} \Gamma_{\mathbb{C}}^{r_2} \prod_{v \text{ finite}} \frac{(N\mathfrak{d}_v)^{s-1/2}}{1 - (N\mathfrak{p}_v)^{-s}} \\ &= \Gamma_{\mathbb{R}}(s)^{r_1} \Gamma_{\mathbb{C}}(s)^{r_2} |d_k|^{s-1/2} \zeta_k(s), \end{aligned}$$

where we used Equation (3.9) and Theorem 2.3.20.

On the other hand, we now determine the  $\zeta$  function of  $\hat{f}, \widehat{\|\cdot\|^s} = \|\cdot\|^{1-s}$ . Let  $S_0$  be the set of finite places of  $k$  that are ramified over  $\mathbb{Q}$ . The desired  $\zeta$  function is given by

$$\begin{aligned} \zeta(\hat{f}, \|\cdot\|^{1-s}) &= \prod_v \zeta(\hat{f}_v, \|\cdot\|^{1-s}) \\ &= \Gamma_{\mathbb{R}}(1-s)^{r_1} \Gamma_{\mathbb{C}}(1-s)^{r_2} \prod_{v \text{ finite}, v \notin S_0} (1 - (N\mathfrak{p}_v)^{-(1-s)})^{-1} \prod_{v \in S_0} (1 - (N\mathfrak{p}_v)^{-(1-s)})^{-1} \\ &= \Gamma_{\mathbb{R}}(1-s)^{r_1} \Gamma_{\mathbb{C}}(1-s)^{r_2} \prod_{v \text{ finite}} (1 - (N\mathfrak{p}_v)^{-(1-s)})^{-1} = |d_k|^{s-1/2} \zeta(f, \|\cdot\|^{1-s}) \end{aligned}$$

where we used Theorem 3.1.42. (Notice that the product  $\prod_{v \text{ finite}} (1 - (N\mathfrak{p}_v)^{-(1-s)})^{-1}$  does not converge for  $\Re s > 1$ ; what we mean is that we already know analytic continuation of both sides of the equation, and this equality is true wherever both sides are defined. Also pay attention to the change of variables  $s \rightarrow 1-s$ , which changes  $|d_k|^{s-1/2}$  to  $|d_k|^{1/2-s}$ .)

Using Theorem 3.2.47, which gives  $\zeta(f, \|\cdot\|^s) = \zeta(\hat{f}, \|\cdot\|^{1-s})$ , we obtain

$$\zeta(f, \|\cdot\|^s) = \zeta(\hat{f}, \|\cdot\|^{1-s}) = |d_k|^{s-1/2} \zeta(f, \|\cdot\|^{1-s}).$$

Multiplying by  $|d_k|^{1/2-s/2}$  on both sides we obtain

$$|d_k|^{(1-s)/2} \zeta(f, \|\cdot\|^s) = |d_k|^{s/2} \zeta(f, \|\cdot\|^{1-s}),$$

that is, the function

$$\tilde{\Lambda}_k(s) := |d_k|^{(1-s)/2} \zeta(f, \|\cdot\|^s) = |d_k|^{s/2} \Gamma_{\mathbb{R}}(s)^{r_1} \Gamma_{\mathbb{C}}(s)^{r_2} \zeta_k(s)$$

satisfies analytic continuation and the functional equation  $\tilde{\Lambda}_k(s) = \tilde{\Lambda}_k(1-s)$ .

It is easy to check that  $\tilde{\Lambda}_k(s) = (2\pi)^{r_2} \Lambda_k(s)$ , where  $\Lambda_k(s)$  is the completed  $\zeta$  function appearing in Theorem 1.3.33: indeed, the ‘fudge factors’

$$|d_k|^{s/2} \Gamma_{\mathbb{R}}(s)^{r_1} \Gamma_{\mathbb{C}}(s)^{r_2}$$

multiply out to give

$$\begin{aligned} |d_k|^{s/2} \Gamma_{\mathbb{R}}(s)^{r_1} \Gamma_{\mathbb{C}}^{r_2} &= |d_k|^{s/2} \pi^{-r_1 s/2} \Gamma(s/2)^{r_1} (2\pi)^{r_2 - r_2 s} \Gamma(s)^{r_2} \\ &= |d_k|^{s/2} (2\pi)^{r_2} \frac{1}{\pi^{s/2(r_1 + 2r_2)}} \Gamma(s/2)^{r_1} \Gamma(s)^{r_2} \\ &= |d_k|^{s/2} (2\pi)^{r_2} \frac{1}{\pi^{ns/2} 2^{r_2 s}} \Gamma(s/2)^{r_1} \Gamma(s)^{r_2} \\ &= (2\pi)^{r_2} \left( \frac{|d_k|}{4^{r_2} \pi^n} \right)^{s/2} \Gamma(s/2)^{r_1} \Gamma(s)^{r_2}, \end{aligned}$$

where we used  $r_1 + 2r_2 = n$ . Theorem 3.2.47 tells us that the residue at 1 of  $\zeta(f, \|\cdot\|^s)$  is  $\kappa \hat{f}(0) = \kappa \prod_{v \in S_0} (N\mathfrak{d}_v)^{1/2} = \kappa |d_k|^{1/2}$ .

From the above we have

$$\zeta_k(s) = (|d_k|^{s-1/2} \Gamma_{\mathbb{R}}(s)^{r_1} \Gamma_{\mathbb{C}}(s)^{r_2})^{-1} \zeta(f, \|\cdot\|^s).$$

The factor  $(|d_k|^{s-1/2} \Gamma_{\mathbb{R}}(s)^{r_1} \Gamma_{\mathbb{C}}(s)^{r_2})^{-1}$  is regular at  $s = 1$ , and its value is

$$(|d_k|^{1/2} \pi^{-r_1/2} \Gamma(1/2)^{r_1})^{-1} = |d_k|^{-1/2}.$$

Thus, the residue of  $\zeta_k(s)$  at 1 is

$$|d_k|^{-1/2} \operatorname{Res}_{s=1} \zeta(f, \|\cdot\|^s) = |d_k|^{-1/2} \cdot \kappa |d_k|^{1/2} = \kappa.$$

We have proven Theorems 1.1.18 and 1.5.35!

### 3.5.3 The general case: $L$ -functions of characters

Our final task is to discuss the analytic properties of Dirichlet  $L$ -functions, and more generally Hecke  $L$ -functions (taken as in Definition 3.3.3 – we have already checked that these contain all the Hecke  $L$ -functions of Definition 1.4.9).

#### Idèlic character

We have discussed the characters of  $I_k$  in Section 3.4. With notation as in that section, fix a character

$$c(a) = \prod_{v \in S} \tilde{c}_v(\tilde{a}_v) \cdot \prod_{v \in S} \|a_v\|_v^{it_v} \cdot \chi(\varphi_S(a)) \quad (3.22)$$

where  $\tilde{c}_v, t_v$  and  $\chi$  satisfy conditions (3.17), (3.18) and (3.19).



### Choice of the adèlic function

For each  $v \in S$ , let  $f_v(x_v)$  be the function used in Section 3.1.4 to compute the function  $\rho(c_v \|\cdot\|_v^s)$  corresponding to the character  $c_v$ . For  $v \notin S$ , let  $f_v(x_v)$  be the characteristic function of  $\mathcal{O}_v$ . We set

$$f(x) = \prod_{v \in S} f_v(x_v).$$

We claim, and we will show below, that  $f(x)$  is a function of class  $\mathfrak{z}$ . We begin by noticing that each function  $f_v(x_v)$  is in  $\mathfrak{W}^1(k_v)$  by the direct computations of Section 3.1.4, and that  $f_v = \mathbf{1}_{\mathcal{O}_v}$  for almost all  $v$ . Lemma 2.4.22 yields that  $f$  is in  $\mathfrak{W}^1(\mathbb{A}_k)$ , and that the Fourier transform of  $f(x)$  is  $\hat{f}(x) = \prod_v \hat{f}_v(x_v)$ . We have thus shown that  $f(x)$  satisfies condition 1 in Definition 3.2.43.

### Fourier transform

We have already seen that the Fourier transform of  $f(x)$  is

$$\hat{f}(x) = \prod_v \hat{f}_v(x_v).$$

For  $v \notin S$  and  $v$  unramified in  $k$ , the Fourier transform of  $f_v = \mathbf{1}_{\mathcal{O}_v}$  is given by  $f_v$  itself, as shown by Equation (3.8). For  $v \notin S$  but ramified in  $k$ , we have

$$\hat{f}_v = (N\mathfrak{d}_v)^{-1/2} \mathbf{1}_{\mathfrak{d}_v^{-1}}$$

by a simple direct calculation. Moreover, since each local factor  $f_v$  is one of the standard functions of Section 3.1.4, the Fourier transforms  $\hat{f}_v$  are in  $\mathfrak{W}^1(k_v^\times)$ , and in fact,  $\hat{f}_v \|\cdot\|^\sigma$  is in  $L^1$  for every  $\sigma > 0$  (for  $v \notin S$ , this follows from the explicit expression above; for  $v \in S$ , notice that all the standard functions  $f_v$  considered in Section 3.1.4 are of class  $\mathfrak{z}$  for the local field  $k_v$ ).

We will only need to know this: the Fourier transform  $\hat{f}$  is a product of local functions  $\hat{f}_v$ , almost all of which agree with the corresponding  $f_v(x)$ , and all of which satisfy  $\hat{f}_v \|\cdot\|^\sigma \in L^1(k_v^\times)$  for  $\sigma > 1$ .

### The $\zeta$ -function

The function  $|f(a)| \cdot \|a\|^\sigma = \prod_v (|f_v(a_v)| \cdot \|a_v\|_v^\sigma)$  is a product of local functions, and all but finitely many of these are equal to 1 on  $\mathfrak{u}_v$  by definition. We can then use Theorem 2.4.20 to check that  $|f(a)| \cdot \|a\|^\sigma$  is in  $L^1(I_k)$ . It suffices to verify that the infinite product

$$\prod_{v \in \Omega_k} \int_{k_v^\times} |f_v(a_v)| \|a_v\|_v^\sigma d\mu_{k_v^\times}(a_v)$$

converges. By the choice of standard functions in Section 3.1.4, each single function  $|f_v(a_v)| \|a_v\|_v^\sigma$  is in  $L^1(k_v^\times)$  for all  $\sigma > 1$ , so it suffices to check that the product of  $\int_{k_v^\times} |f_v(a_v)| \|a_v\|_v^\sigma d\mu_{k_v^\times}(a_v)$

over all but finitely many  $v$  converges. In particular, we can consider the product

$$\begin{aligned} \prod_{\substack{v \notin S \\ v \text{ unramified in } k}} \int_{k_v^\times} |f_v(a_v)| \|a_v\|_v^\sigma d\mu_{k_v^\times}(x_v) &= \prod_{\substack{v \notin S \\ v \text{ unramified in } k}} \int_{\mathcal{O}_v \setminus \{0\}} \|a_v\|_v^\sigma d\mu_{k_v^\times}(a_v) \\ &= \prod_{\substack{v \notin S \\ v \text{ unramified in } k}} \frac{1}{1 - (N\mathfrak{p}_v)^{-\sigma}}, \end{aligned}$$

where the last equality uses Equation (3.9) and the fact that  $N\mathfrak{d}_v = 1$  for  $v$  unramified in  $k$ . This infinite product converges for  $\sigma > 1$  by the classical calculation in Proposition 1.4.5. We already observed that the Fourier transform of  $f$  is a product of local functions, and all but finitely many factors coincide with those of  $f$ . From this, it follows easily that  $\hat{f}$  is continuous and that  $\hat{f}(a)\|a\|^\sigma$  is also in  $L^1$  for every  $\sigma > 1$ . We have thus checked that  $f$  satisfies the third condition in Definition 3.2.43.

We now verify condition 2 in Definition 3.2.43, that is, we show that the sum

$$\sum_{\xi \in k} f(a(x + \xi))$$

is uniformly convergent for  $(a, x) \in C \times D$ , where  $C$  is a compact subset of  $I_k$ . As before, the argument for  $\sum_{\xi \in k} \hat{f}(a(x + \xi))$  is completely analogous, so we only treat the case of  $f$ .

**Lemma 3.5.1.** *Let  $f$  and  $C$  be fixed. There is a fractional ideal  $A$  of  $\mathcal{O}_k$  such that, for all  $a \in C$  and  $x \in D$ , we have  $f(a(x + \xi)) = 0$  unless  $\xi$  is in  $A$ .*

*Proof.* Let  $v$  be a finite place. By definition,  $f_v$  vanishes outside of a compact subset  $B_v$  of  $k_v$ , and we can take  $B_v = \mathcal{O}_v$  for all but finitely many  $v$ . Thus,  $f(a(x + \xi))$  can only be non-zero if  $a(x + \xi)$  belongs to  $\prod_v B_v$ . Equivalently,  $x + \xi$  has to belong to  $\prod_v a_v^{-1}B_v$  (which is still a compact set), and  $\xi$  has to belong to  $k \cap \prod_v (-x_v + a_v^{-1}B_v)$ . We claim that the intersection  $k \cap \prod_v (-x_v + a_v^{-1}B_v)$  is contained in a fractional ideal  $A$  of  $\mathcal{O}_k$  independent of  $x$  and  $a$  (provided that these elements lie in  $D$  and  $C$ , respectively). To prove this, we notice that:

1. for each  $v$ , the  $v$ -valuation of elements in  $-x_v + a_v^{-1}B_v$  is bounded below, uniformly as  $x$  varies in  $D$  and  $a$  in  $C$ . This follows from the compactness of  $B_v$ , of  $C$  and of  $\bar{D}$ , which implies the compactness of  $-\bar{D} + C^{-1}B_v$ , combined with the fact that  $v$  (being continuous) is bounded on any compact subset of  $k_v^\times$ .
2. for all but finitely many  $v$ , all elements in  $-x_v + a_v^{-1}B_v$  are  $v$ -integral (for any choice of  $x \in D$  and  $a \in C$ ). To see this, recall from Lemma 2.4.10 that a compact subset of  $I_k = \prod'_v (k_v^\times, \mathfrak{u}_v)$  is contained in a product of compact subsets  $C_v$ , where all but finitely many  $C_v$  are equal to  $\mathfrak{u}_v$ . Moreover, by definition, the elements in  $D$  are  $v$ -integral for all finite  $v$ . Thus, if  $v$  is any place for which  $B_v = \mathcal{O}_v$  (all but finitely many) and  $C_v = \mathfrak{u}_v$  (all but finitely many), then  $-x_v + a_v^{-1}B_v \subset \mathcal{O}_v + \mathfrak{u}_v \mathcal{O}_v \subseteq \mathcal{O}_v$ .

Combining the previous two statements, we obtain that  $e_v = \min\{0, v(-x_v + a_v^{-1}b_v) : x \in D, a \in C, b_v \in B_v\}$  is a well-defined integer, equal to 0 for almost all  $v$ . Thus,  $A := \prod_{v \text{ finite}} \mathfrak{p}_v^{e_v}$  is a well-defined fractional ideal of  $k$ , which by construction contains  $k \cap \prod_v (-x_v + a_v^{-1}B_v)$ . This concludes the proof of the lemma.  $\square$

Let  $A$  be the ideal given by the lemma. Like all fractional ideals of a number field, it is a free  $\mathbb{Z}$ -module of finite rank  $n = [k : \mathbb{Q}]$ . Let  $\omega_1, \dots, \omega_n$  be a  $\mathbb{Z}$ -basis of  $A$ . The series  $\sum_{\xi \in k} f(a(x + \xi))$  can then be rewritten as a sum over  $\xi \in A$ , hence as

$$\sum_{(c_1, \dots, c_n) \in \mathbb{Z}^n} f\left(a\left(x + \sum_{i=1}^n c_i \omega_i\right)\right).$$

By definition,  $f(x) = \prod_v f_v(x_v)$ , and all the non-archimedean factors are bounded by 1 in absolute value (see Equation (3.7)). Each archimedean factor is also bounded (though not necessarily by 1), see Equations (3.4) and (3.5). Thus, it suffices to show that

$$\sum_{(c_1, \dots, c_n) \in \mathbb{Z}^n} \prod_{v \text{ archimedean}} f_v\left(a_v\left(x_v + \sum_{i=1}^n c_i \omega_i\right)\right) \tag{3.23}$$

converges uniformly. The product  $\prod_{v \text{ archimedean}} f_v(a_v(x_v + \sum_{i=1}^n c_i \omega_i))$  is bounded above by a function on  $\mathbb{R}^n$  of the form  $w \mapsto p(w) \exp(c_{a,x} + d_{a,x} \|w\| - B_{a,x} \|w\|^2)$ , where  $p(w)$  is a polynomial,  $c_{a,x}, d_{a,x}$  are numbers depending continuously on  $a, x$ , and  $B_{a,x}$  is a non-singular matrix depending continuously on  $a, x$ . Since  $a_v, x_v$  are bounded (lying respectively in the compact  $C$  and in the relatively compact set  $D$ ) and  $a_v$  is also bounded away from zero (for the same reason), it is easy to see that  $w \mapsto p(w) \exp(c_{a,x} - B_{a,x} \|w\|^2)$  is bounded above by a function  $g(w)$  (independent of  $a, x$ ) of the same form, for which the sum converges (see Exercise 3.5.2; notice that we are summing over a full-rank lattice of  $\mathbb{R}^n$ , so as  $\max |c_i| \rightarrow \infty$ , also  $\|\sum c_i \omega_i\|$  tends to infinity). This completes the verification that our function  $f$  lies in class  $\mathfrak{z}$ .

**Exercise 3.5.2.** Complete the argument for the uniform convergence of (3.23).

**Conclusion: analytic continuation and functional equation**

Let  $\tilde{c}$  be a quasi-character of exponent greater than 1. Applying Theorem 2.4.20, we obtain that the  $\zeta$  function  $\zeta(f, \tilde{c}) = \int_{I_k} f(a) \tilde{c}(a) d\mu_{I_k}(a)$  decomposes as the product

$$\prod_v \left( \int_{k_v^\times} f_v(a_v) \tilde{c}_v(a_v) d\mu_{k_v^\times}(a_v) \right) = \prod_v \zeta(f_v, \tilde{c}_v) \tag{3.24}$$

of the local  $\zeta$  functions of the quasi-characters  $\tilde{c}_v$ . In particular, if  $c$  is our fixed character (of exponent 0)

$$c(a) = \prod_v c_v(a_v) = \prod_{v \in S} c_v(a_v) \cdot \chi(\varphi_S(a)),$$

we can apply the decomposition (3.24) to the quasi-character  $\tilde{c} = c \|\cdot\|^s$  for every  $s$  with  $\Re s > 1$ .

As a next step, we notice that for every  $v \notin S$  and  $\Re s > 1$  we can explicitly compute the integral defining  $\zeta(f_v, c_v \|\cdot\|_v^s)$ . To do this, notice first that every  $a_v \in \mathcal{O}_v$  can be written uniquely as  $\pi_v^i \tilde{a}_v$  with  $i \in \mathbb{N}$  and  $\tilde{a}_v \in \mathfrak{u}_v$ . By definition,  $c_v$  is unramified, so  $c_v(a_v) = c_v(\pi_v^i) = c_v(\pi_v)^i$  only depends on  $i$ , the valuation of  $a_v$ . Furthermore,  $c_v(\pi_v)$  is by definition  $\chi(\mathfrak{p}_v)$ , where  $\mathfrak{p}_v$  is

the prime ideal corresponding to the valuation  $v$ . We may now compute

$$\begin{aligned} \zeta(f_v, c_v \| \cdot \|_v^s) &= \int_{\mathcal{O}_v \setminus \{0\}} c_v(a_v) \|a_v\|_v^s d\mu_{k_v^\times}(a_v) \\ &= \sum_{i=0}^{\infty} \mu_{k_v^\times}(\pi_v^i \mathbf{u}_k) (N\mathfrak{p}_v)^{-is} \chi(\mathfrak{p}_v)^i \\ &= \sum_{i=0}^{\infty} \mu_{k_v^\times}(\mathbf{u}_k) (N\mathfrak{p}_v)^{-is} \chi(\mathfrak{p}_v)^i \\ &= (N\mathfrak{d}_v)^{-1/2} \left( 1 - \frac{\chi(\mathfrak{p}_v)}{(N\mathfrak{p}_v)^s} \right)^{-1}. \end{aligned}$$

(We take this chance to mention that this is basically the same computation necessary to check Theorem 3.1.42.) Thus,

$$\begin{aligned} \zeta(f, c \| \cdot \|_v^s) &= \prod_{v \in S} \zeta(f_v, c_v \| \cdot \|_v^s) \cdot \prod_{v \notin S} \left( (N\mathfrak{d}_v)^{-1/2} \left( 1 - \frac{\chi(\mathfrak{p}_v)}{(N\mathfrak{p}_v)^s} \right)^{-1} \right) \\ &= \prod_{v \in S} \zeta(f_v, c_v \| \cdot \|_v^s) \cdot \prod_{v \notin S} (N\mathfrak{d}_v)^{-1/2} \cdot L(s, c), \end{aligned}$$

where  $L(s, c)$  is the Hecke  $L$ -function of the idèlic character  $c$  in the sense of Definition 3.3.3.

To justify the appearance of  $L(s, c)$ , notice that

$$L(s, c) = \prod_{v \notin S} \left( 1 - \frac{c(\mathfrak{p}_v)}{(N\mathfrak{p}_v)^s} \right)^{-1} = \prod_{v \notin S} \left( 1 - \frac{\chi(\mathfrak{p}_v)}{(N\mathfrak{p}_v)^s} \right)^{-1} = L(s, \chi),$$

because by definition the Hecke  $L$ -function  $L(s, c)$  only depends on  $c(b(\mathfrak{p}))$ , where  $\mathfrak{p}$  ranges over the primes at which  $c$  is unramified. The explicit description (3.22) shows immediately that  $c(b(\mathfrak{p})) = \chi(b(\mathfrak{p}))$ . We have thus shown that  $L(s, c)$  can be represented as

$$L(s, c) = \prod_{v \in S} \zeta(f_v, c_v \| \cdot \|_v^s)^{-1} \prod_{v \notin S} (N\mathfrak{d}_v)^{-1/2} \cdot \zeta(f, c \| \cdot \|_v^s).$$

Theorem 3.2.47 shows that  $\zeta(f, c \| \cdot \|_v^s)$  has meromorphic continuation to  $\mathbb{C}$ , with poles at  $s = 0, 1$  if  $c$  is trivial. Remark 3.1.46 shows that the factor  $\prod_{v \in S} \zeta(f_v, c_v \| \cdot \|_v^s)^{-1}$  is everywhere analytic, and  $(N\mathfrak{d}_v)^{-1/2}$  is clearly a constant. Thus, we obtain analytic continuation to  $\mathbb{C}$  as soon as  $c$  is not the trivial character; when  $c$  is the trivial character, we still need to check that the pole at  $s = 1$  is not cancelled by the local zeta factors, while the pole at  $s = 0$  *does* cancel out. This follows easily from the explicit expressions for the local zeta functions. In particular, the local  $\zeta$  function at any archimedean place is of one of the two forms given in Equation (3.21): both these functions are regular and nonvanishing at  $s = 1$ , while they have a pole at  $s = 0$ . Their inverses thus vanish at  $s = 0$ , and cancel out the pole of  $\zeta(f, \| \cdot \|_v^s)$ . As for the situation at  $s = 1$ , it suffices to check that none of the local zeta functions computed in Section 3.1.4 has a pole at  $s = 1$ , which is easily seen to be the case. This completes the proof of Theorem 1.4.11.

Finally, for the sake of completeness we also briefly discuss the functional equation satisfied by the Hecke  $L$ -functions. We can write the  $\zeta$  function for the dual pair  $(\hat{f}, \widehat{c \| \cdot \|_v^s}) = (\hat{f}, c^{-1} \| \cdot \|_v^{1-s})$  as

$$\zeta(\hat{f}, \widehat{c \| \cdot \|_v^s}) = \prod_{v \in S} \zeta(\hat{f}_v, \widehat{c_v \| \cdot \|_v^s}) \prod_{v \notin S} \chi(\mathfrak{d}_v) (N\mathfrak{d}_v)^{-s} \cdot L(1-s, \chi^{-1})$$

for  $\Re s < 0$ . The global functional equation of Theorem 3.2.47 then yields

$$\zeta(f, c \| \cdot \|_v^s) = \zeta(\widehat{f}, \widehat{c} \| \cdot \|_v^s) \iff$$

$$\prod_{v \in S} \zeta(f_v, c_v \| \cdot \|_v^s) \cdot \prod_{v \notin S} (N\mathfrak{d}_v)^{-1/2} \cdot L(s, \chi) = \prod_{v \in S} \zeta(\widehat{f}_v, \widehat{c}_v \| \cdot \|_v^s) \prod_{v \notin S} \chi(\mathfrak{d}_v) (N\mathfrak{d}_v)^{-s} \cdot L(1-s, \chi^{-1}).$$

Dividing both sides by  $\prod_{v \in S} \zeta(\widehat{f}_v, \widehat{c}_v \| \cdot \|_v^s) \prod_{v \notin S} \chi(\mathfrak{d}_v) (N\mathfrak{d}_v)^{-s}$  we finally obtain the functional equation

$$\prod_{v \in S} \rho(c_v \| \cdot \|_v^s) \cdot \prod_{v \notin S} (\chi(\mathfrak{d}_v) (N\mathfrak{d}_v)^{s-1/2}) \cdot L(s, \chi) = L(1-s, \chi^{-1}),$$

where – using the local functional equations  $\zeta(f_v, c_v \| \cdot \|_v^s) = \rho(c_v) \zeta(\widehat{f}_v, \widehat{c}_v \| \cdot \|_v^s)$  of Theorem 3.1.35 – we have rewritten the ratios

$$\frac{\zeta(f_v, c_v \| \cdot \|_v^s)}{\zeta(\widehat{f}_v, \widehat{c}_v \| \cdot \|_v^s)}$$

in terms of  $\rho$ -factors. Recall that these functions have been explicitly computed in Section 3.1.4 and only depend on the character  $c_v$ , not on the choice of  $f_v$ . Replacing each  $\rho$ -factor with its explicit expression yields the classical functional equation for Hecke  $L$ -functions.



# Chapter 4

## Exam questions

Here are some questions I asked during exams:

1. Let  $K$  be the splitting field over  $\mathbb{Q}$  of  $x^3 - 2$ , let  $G$  be the Galois group of  $K$  over  $\mathbb{Q}$ , and let  $\rho$  be the standard (2-dimensional) representation of  $G$ . Determine the behaviour of  $L(s, \rho)$  around  $s = 1$  (does it have a zero, a pole, or neither?) and, if  $L(1, \rho)$  exists and is nonzero, determine its value in terms of arithmetic quantities.
2. Let  $K_1, K_2$  be two number fields such that  $\zeta_{K_1}(s) = \zeta_{K_2}(s)$ . Prove that  $[K_1 : \mathbb{Q}] = [K_2 : \mathbb{Q}]$ . If at least one among  $K_1, K_2$  is Galois over  $\mathbb{Q}$ , prove that  $K_1 = K_2$ .
3. For a prime number  $p \neq 3, 7$ , define

$$a_p := \#\{x \in \mathbb{F}_p^\times : x^3 \equiv 7 \pmod{p}\}.$$

Prove that  $a_p$  is the  $p$ -th Dirichlet coefficient of the  $\zeta$  function of the field  $K = \mathbb{Q}(\sqrt[3]{7})$  (that is: writing  $\zeta_K(s)$  as the Dirichlet series  $\sum_{n \geq 1} \frac{b_n}{n^s}$ , one has  $b_p = a_p$  for all primes  $p \neq 3, 7$ ). Let  $L$  be the Galois closure of  $K/\mathbb{Q}$  and let  $G$  be the Galois group of  $L/\mathbb{Q}$ : describe a representation  $\rho$  of  $G$  such that  $L(s, \rho) = \zeta_K(s)$ .

4. Let  $K$  be a number field and write  $\zeta_K(s) = \sum_{n \geq 1} \frac{a_n}{n^s}$ . Suppose that, for all primes  $p \equiv 1 \pmod{5}$ , the coefficient  $a_p$  is equal to 4. Prove that  $K = \mathbb{Q}(\zeta_5)$ .

*Hint.*

- a) Prove that  $[K : \mathbb{Q}] \geq 4$ .
  - b) Prove that there exists a prime  $p \equiv 1 \pmod{5}$  that is totally split in  $K$ .
  - c) Deduce that  $[K : \mathbb{Q}] = 4$ .
  - d) Conclude by comparing the primes that split completely in  $K$  and  $\mathbb{Q}(\zeta_5)$ .
5. Let  $K = \mathbb{Q}(i, \sqrt{5})$ .
    - a) Express the residue of  $\zeta_K(s)$  at  $s = 1$  in terms of  $L$ -functions of Dirichlet characters.
    - b) Prove that a fundamental unit of  $\mathcal{O}_{\mathbb{Q}(\sqrt{5})}$  is also a fundamental unit of  $\mathcal{O}_K$  [during the exam we admitted this, but you should still think about it! If you want a hint, consider the norm from  $K$  to  $\mathbb{Q}(\sqrt{5})$  of a fundamental unit of  $K$ ].
    - c) Taking for granted that  $h(\mathbb{Q}(i)) = 1$  and  $h(\mathbb{Q}(\sqrt{-5})) = 2$ , compute  $h(K)$ .



# Bibliography

- [CG47] Henri Cartan and Roger Godement. Théorie de la dualité et analyse harmonique dans les groupes abéliens localement compacts. *Ann. Sci. École Norm. Sup. (3)*, 64:79–99, 1947.
- [Fol16] Gerald B. Folland. *A course in abstract harmonic analysis*. Textbooks in Mathematics. CRC Press, Boca Raton, FL, second edition, 2016.
- [Her32] J. Herbrand. Sur les classes des corps circulaires. *J. Math. Pures Appl. (9)*, 11:417–441, 1932.
- [Lic73] Stephen Lichtenbaum. Values of zeta-functions, étale cohomology, and algebraic  $K$ -theory. In *Algebraic K-theory, II: “Classical” algebraic K-theory and connections with arithmetic (Proc. Conf., Battelle Memorial Inst., Seattle, Wash., 1972)*, Lecture Notes in Math., Vol. 342, pages 489–501. Springer, Berlin, 1973.
- [LO77] J. C. Lagarias and A. M. Odlyzko. Effective versions of the Chebotarev density theorem. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 409–464. Academic Press, London, 1977.
- [Mar18] Daniel A. Marcus. *Number fields*. Universitext. Springer, Cham, 2018. Second edition, With a foreword by Barry Mazur.
- [Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.
- [New80] D. J. Newman. Simple analytic proof of the prime number theorem. *Amer. Math. Monthly*, 87(9):693–696, 1980.
- [Rib76] Kenneth A. Ribet. A modular construction of unramified  $p$ -extensions of  $\mathbb{Q}(\mu_p)$ . *Invent. Math.*, 34(3):151–162, 1976.
- [RV99] Dinakar Ramakrishnan and Robert J. Valenza. *Fourier analysis on number fields*, volume 186 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1999.
- [Sch08] René Schoof. *Catalan’s conjecture*. Universitext. Springer-Verlag London, Ltd., London, 2008.
- [Ser77] Jean-Pierre Serre. *Cours d’arithmétique*. Le Mathématicien, No. 2. Presses Universitaires de France, Paris, 1977. Deuxième édition revue et corrigée.
- [Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg.
- [Tao21] Terence Tao. 246B, Notes 4: The Riemann zeta function and the prime number theorem, 2021. Available at <https://terrytao.wordpress.com/2021/02/12/246b-notes-4-the-riemann-zeta-function-and-the-prime-number-theorem/#more-12315>.

- [Tat67] J. T. Tate. Fourier analysis in number fields, and Hecke's zeta-functions. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 305–347. Thompson, Washington, D.C., 1967.
- [Wik23a] Wikipedia. Hecke character — Wikipedia, the free encyclopedia. <http://en.wikipedia.org/w/index.php?title=Hecke%20character&oldid=1142048381>, 2023. [Online; accessed 26-March-2023].
- [Wik23b] Wikipedia. Selberg class — Wikipedia, the free encyclopedia. <http://en.wikipedia.org/w/index.php?title=Selberg%20class&oldid=1129548802>, 2023. [Online; accessed 27-February-2023].
- [Zag97] D. Zagier. Newman's short proof of the prime number theorem. *Amer. Math. Monthly*, 104(8):705–708, 1997.