L-functions and their applications

Jolanta Marzec and Michalis Neururer

Version from Tuesday 25th February, 2020, 11:04

Contents

CHAPTER 1

Motivation

An L-function is a series of the form

$$L(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \qquad s \in \mathbb{C},\, a_n \in \mathbb{C}$$

(which converges for $\operatorname{Re}(s)$ big enough) that has an Euler product and satisfies a certain type of functional equation. In particular, it is a meromorphic function on the complex plane.

Such a function becomes interesting if it can be associated with an interesting mathematical object. Indeed, as we shall see, already the analytic properties mentioned above can tell us a lot about the underlying object, and the additional knowledge on zeros, poles, special values of $L(s)$, etc. provide even better understanding. And there are many objects out there that can be studied via L-functions! This includes prime numbers and - more generally - prime ideals in number fields, elliptic curves and algebraic varieties, modular and automorphic forms, and many more.

There are also situations (broadly known as the Langlands Program, and in general far from being proven) when two families of L-functions - coming from a priori unrelated areas of mathematics - coincide. Such phenomena provide bridges between these areas of mathematics and allow a transfer of results from one side to the other. Perhaps one of the most famous examples is the connection between L-functions of elliptic curves defined over $\mathbb{Q}$ and modular forms, which was the crucial ingredient in Andrew Wiles' proof of Fermat Last Theorem.

Below we list some results which follow from good understanding of the analytic properties of L-functions. An explanation (whenever indicated) and more extensive list will be given throughout the lecture.

1. The Riemann ζ-function

This well known L-function is defined as

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

The fact that it has a pole at $s = 1$ implies that there are infinitely many prime numbers (see Corollary 2.3). If we look closer, we find that this pole is simple and with the residue $\mathrm{Res}_{s=1}\,\zeta(s) = 1$, which may be used to provide an estimate for

$$\pi(x) := \#\{p \in \mathbb{P} : p \leq x\}$$

(see [7, Section 1.1.3]). Furthermore, the facts that $\zeta(s)$ has a meromorphic continuation and that

$$\zeta(s) \neq 0 \qquad \text{whenever} \qquad \mathrm{Re}\,(s) = 1$$

imply

Theorem 1.1 (Prime Number Theorem)

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

where $f(x) \sim g(x)$ *means* $\lim\limits_{x\to\infty} \frac{f(x)}{g(x)} = 1$.

This theorem[1] could be stated equivalently as

$$\pi(x) \sim \mathrm{Li}(x)\,, \qquad \text{where} \qquad \mathrm{Li}(x) = \int_2^x \frac{dt}{\ln t}\,.$$

And in fact, the bigger the zero-free region for $\zeta(s)$, the better an estimate for $|\pi(x) - \mathrm{Li}(x)|$ (see Important Remarks in [2, Section 10.7.1]). The best known approximation may be achieved if one assumes

Riemann Hypothesis *All non-trivial zeros of* $\zeta(s)$ *have* $Re\,(s) = \frac{1}{2}$.

Namely, then there exists a constant C so that for all x big enough

$$|\pi(x) - \mathrm{Li}(x)| \leq C\sqrt{x}\log x\,.$$

Actually, this bound is equivalent to Riemann Hypothesis itself!

2. Dirichlet L-functions

It is possible to generalise $\zeta(s)$ slightly in order to study the number of primes in arithmetic progressions, that is,

$$\#\{p \in \mathbb{P} : p \leq x,\, p \equiv a \bmod m\}\,,$$

where $m \geq 1$ and $a \in \mathbb{Z}$ are coprime.

[1] For a historical account on the Prime Number Theorem see [4]; for a proof consult [2, Section 10.7].

We define a **Dirichlet L-function** to be the meromorphic continuation of a Dirichlet series

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \qquad \mathrm{Re}\,(s) > 1, \tag{1}$$

where $\chi : \mathbb{Z} \to \mathbb{C}^\times$ is an extension of a homomorphism $\chi' : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ such that

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

It is easy to see that χ is completely multiplicative and periodic modulo m; we call it a **Dirichlet character modulo m**. We say that a Dirichlet character χ mod m is trivial if $\chi(n) = 1$ for $\gcd(n,m) = 1$.

We will prove later (Corollary 3.39) that

$$\chi \text{ non-trivial} \qquad \Longrightarrow \qquad L(\chi, 1) \neq 0.$$

This simple looking result implies (see the proof of Theorem 3.40)

Theorem 1.2 (Dirichlet's Prime Number Theorem) *Let a and m be coprime. Every arithmetic progression*

$$a,\ a \pm m,\ a \pm 2m,\ \ldots$$

contains infinitely many prime numbers.

In fact, we will also describe the distribution of primes among the classes $a \bmod m$. This will be done in a much more general setting in section 6 where instead of prime numbers we will consider prime ideals of a Galois extension L of a number field K, and in place of Dirichlet L-functions we will consider Artin L-functions. To appropriately generalise Dirichlet's theorem to arbitrary number fields it is necessary to reformulate it. To a prime ideal $\mathfrak{p}$ in the ring of integers of K we can associate an element $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(L/K)$.[2] Recall that $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$. The Frobenius element associated to a prime ideal (p) in $\mathbb{Z}$ is exactly the residue class of p modulo m. So Dirichlet's theorem states that for every residue class $\overline{a} \in (\mathbb{Z}/m\mathbb{Z})^\times$ there are infinitely many primes whose Frobenius element is $\overline{a}$. Chebotarev's density theorem (Theorem 6.1) makes the same statement for an arbitrary Galois extension L/K.

Theorem 1.3 *Let L/K be a Galois extensions and $C \subseteq \mathrm{Gal}(L/K)$ be a conjugacy class. Then there are infinitely many prime ideals $\mathfrak{p} \lhd \mathcal{O}_K$ with $\mathrm{Frob}_{\mathfrak{p}} \in C$.*

[2] This element depends on a choice of a prime ideal $\mathfrak{q}$ above $\mathfrak{p}$ but the conjugacy class of $\mathrm{Frob}_{\mathfrak{p}}$ is independent of this choice.

3. Generalities on Dirichlet-series

In this course we will study Dirichlet series. These are series of the form

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

where the a_n are complex numbers. The theory of these series has many parallels to the theory of power series. For example the analogue of the radius of convergence of a power series is the abscissa of convergence. To prove our first theorem on Dirichlet-series we need a classic theorem from complex analysis and special case of Abel summation.

Theorem 1.4 (Weierstrass 1861) *Let $U \subseteq \mathbb{C}$ be open and f_n a sequence of analytic functions from U to $\mathbb{C}$. Suppose f_n converge uniformly to f on every compact subset of U. Then f is analytic. Furthermore the sequence of k-th derivatives $f_n^{(k)}$ tends to $f^{(k)}$ uniformly on every compact subset of U.*

Lemma 1.5 (Abel summation) *Let a_n be a sequence of complex numbers and ϕ a continuously differentiable function on the interval $[x, y]$. Define*

$$A(t) = \sum_{0 \le n \le t} a_n.$$

Then

$$\sum_{x \le n \le y} a_n \phi(n) = A(y)\phi(y) - A(x)\phi(x) - \int_x^y A(t)\phi'(t)dt$$

We will use a discrete analogue of this: Let b_n be another sequence in $\mathbb{C}$. Then

$$\sum_{n=M}^{N} a_n b_n = \sum_{n=M}^{N-1} \left(\sum_{k=M}^{n} a_k \right) (b_n - b_{n+1}) + \left(\sum_{k=M}^{N} a_k \right) b_N$$

Theorem 1.6 *Let $f(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ be a Dirichlet-series.*

(1) *If the partial sums $A(M, N) = \sum_{n=M}^{N} a_n$ are uniformly bounded, then $f(s)$ converges locally uniformly on $Re(s) > 0$ to an analytic function.*

(2) *If $f(s)$ is convergent for $s = s_0$, then it is convergent for all s with $Re(s) > Re(s_0)$ and converges uniformly on compact sets. We call*

$$\sigma_0 = \inf\{Re(s) |\, f(s) \text{ converges}\}$$

the abscissa of convergence of f. If f converges everywhere we set $\sigma_0 = -\infty$ and if it converges nowhere we set $\sigma_0 = \infty$. The k-th derivative of f is given *by the Dirichlet-series*

$$f^{(k)}(s) = \sum_{n=1}^{\infty} a_n(-1)^k(\log n)^k n^{-s}$$

and has the same abscissa of convergence.

Sketch of proof. First note that the first statement implies the second. Replacing s with $s - s_0$ and a_n with $a_n n^{-s_0}$ we can assume without loss of generality that $s_0 = 0$. The assumption that $f(s)$ converges at $s_0 = 0$ implies that the partial sums $\sum_{n=M}^{N} a_n$ are bounded and hence we can apply (1) to conclude that $f(s)$ converges locally uniformly on $\mathrm{Re}\,(s) > 0$. The other statements now follow from Theorem 1.4.

Now assume that the partial sums $A(M, N)$ are bounded by B. We will show that the sequence of functions $\sum_{n=1}^{N} a_n n^{-s}$ is a uniformly Cauchy sequence on the domain U defined by

$$-A < \arg(s) < A,\ \mathrm{Re}\,(s) > \delta$$

for fixed positive δ and $0 < A < \pi/2$. This is equivalent to showing that for every $\epsilon > 0$ there exists N_0 such that for every $M, N \geq N_0$ we have $\sum_{n=M}^{N} a_n n^{-s} < 0$. Let $\epsilon > 0$ and choose $N_0 \in \mathrm{N}$ such that $|n^{-s}| < \epsilon$ for all $n > N_0$ and $s \in U$. Let $M, N \geq N_0$. Using Abel summation

$$\begin{aligned}|\sum_{n=M}^{N} a_n n^{-s}| &= |\sum_{n=M}^{N-1} A(M,n)(n^{-s} - (n+1)^{-s}) + A(M,N)N^{-s}| \\ &\leq B\sum_{n=M}^{N-1} |n^{-s} - (n+1)^{-s}| + B\epsilon.\end{aligned}$$

Note that

$$|(n^{-s} - (n+1)^{-s})| = |s\int_{\log n}^{\log(n+1)} e^{-xs}dx| \leq |s| \cdot \int_{\log n}^{\log(n+1)} |e^{-x\sigma}| = \frac{|s|}{\sigma}(n^{-\sigma} - (n+1)^{-\sigma}),$$

where $\sigma = \mathrm{Re}\,(s)$. In U the quotient $\frac{|s|}{\sigma}$ is bounded by a constant C. So we have

$$\begin{aligned}|\sum_{n=M}^{N} a_n n^{-s}| &\leq BC\sum_{n=M}^{N-1}(n^{-\sigma} - (n+1)^{-\sigma}) + B\epsilon \\ & BC(M^{-\sigma} - N^{-\sigma}) + B\epsilon \leq \epsilon(BC + B).\end{aligned}$$

□

Remark 1.7 *Per definition $f(s)$ diverges for all s with Re$\,(s) < \sigma_0$.*

Without proof we state the following theorem which also has its analogue in the theory of power series.

Theorem 1.8 *If two Dirichlet series* $\sum a_n n^{-s}$ *and* $\sum b_n n^{-s}$ *converge and are equal on a domain in* $\mathbb{C}$*, then* $a_n = b_n$ *for all* n*.*

CHAPTER 2

The Riemann ζ-function

The Riemann zeta function is defined as the Dirichlet series

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

This series converges absolutely and uniformly on compact subsets of the half plane $\operatorname{Re} s > 1$. In 1748 Euler proved a formula that connected this function to the prime numbers.

Theorem 2.1 (Euler product) *For $s \in \mathbb{C}$ with $Re\,(s) = \sigma > 1$ we have*

$$\zeta(s) = \prod_{p\in\mathbb{P}} \frac{1}{1-p^{-s}}$$

and $\zeta(s) \neq 0$.

Proof. For $P > 0$, we express the finite product

$$\prod_{p\in\mathbb{P},p<P} \frac{1}{1-p^{-s}} = 1 + n_1^{-s} + n_2^{-s} + \ldots,$$

as a sum taken over all natural numbers whose prime factorisation contains only primes smaller than P. Hence

$$|\zeta(s) - \prod_{p\in\mathbb{P},p<P} \frac{1}{1-p^{-s}}| \leq (P+1)^{-\sigma} + (P+2)^{-\sigma} + \ldots$$

which tends to 0 as $P \to \infty$, and thus proves that $\zeta(s)$ may be written as an Euler product. The non-vanishing of $\zeta(s)$ follows from the fact that

$$\prod_{p\in\mathbb{P},p\leq P} (1-p^{-s}) \cdot \zeta(s) = \prod_{p\in\mathbb{P},p>P} (1-p^{-s})^{-1} = 1 + m_1^{-s} + m_2^{-s} + \ldots,$$

where the sum is taken over all natural numbers whose prime factorisation contains only primes greater than P. Hence, for $P > 0$ large enough

$$|\prod_{p\in\mathbb{P},p\leq P} (1-p^{-s}) \cdot \zeta(s)| > 1 - (P+1)^{-\sigma} - (P+2)^{-\sigma} - \ldots > 0.$$

□

Remark 2.2 *The above proof can be easily generalised to show that the Dirichlet series* (1) *also admits an Euler product for* $Re(s) > 1$*:*

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p \in \mathbb{P}} \frac{1}{1 - \chi(p)p^{-s}} \,.$$

It suffices to notice that $|\chi(n)| \leq 1$ *for all* $n \in \mathbb{Z}$*.*

Corollary 2.3 *There are infinitely many prime numbers.*

Proof. If the set $\mathbb{P}$ of prime numbers was finite, then

$$\lim_{s \to 1^+} \prod_{p \in \mathbb{P}} \frac{1}{1 - p^{-s}} < \infty.$$

On the other hand, we know that $\lim_{s \to 1^+} \sum_{n=1}^{\infty} n^{-s}$ diverges to infinity. This is in contradiction with Theorem 2.1. □

Remark 2.4 *One could prove the above corollary relying only on divergence of* $\zeta(s)$ *at* $s = 1$*, i.e. without using Euler product expansion; see for example* [7]*.*

1. The Mellin transform

Let $f : \mathbb{R}_{>0} \to \mathbb{C}$ be continuous. We define the Mellin transform of f to be

$$\mathcal{M}(f, s) = \int_0^{\infty} f(y) y^s \frac{dy}{y}. \tag{2}$$

Example 2.5 *The Gamma function is the Mellin transform of* $f(y) = e^{-y}$*, i.e.,*

$$\Gamma(s) = \int_0^{\infty} e^{-y} y^s \frac{dy}{y}.$$

which converges absolutely for $Re\, s > 0$*.*

The following properties of the Mellin transform follow from simple transformations of the defining integral.

Lemma 2.6 *The Mellin transform satisfies the following basic properties as long as both sides of the equalities are defined:*

(1) *If* $\lambda > 0$*, define* $g(y) = f(\lambda y)$*. Then* $\mathcal{M}(g, s) = \lambda^{-s} \mathcal{M}(f, s)$*.*
(2) *If* $\alpha \in \mathbb{C}$*, define* $g(y) = y^{\alpha} f(y)$*. Then* $\mathcal{M}(g, s) = \mathcal{M}(f, s + \alpha)$*.*
(3) *If* $g(y) = f(1/y)$ *also satisfies this condition, then for* $Re\, s > 0$ *we have the functional equation*

$$\mathcal{M}(f, s) = \mathcal{M}(g, -s).$$

Lemma 2.7 *If f is of rapid decay at ∞, i.e. $\lim_{y\to\infty} f(y)y^A = 0$ for any $A \in \mathbb{R}$ and $f = O_{y\to 0}(y^{-B})$, then $\mathcal{M}(f,s)$ converges absolutely and uniformly on compact subsets of the half plane $\operatorname{Re} s > B$. If f is of rapid decay at 0, i.e., $\lim_{y\to 0} f(y)y^A = 0$ for any $A \in \mathbb{R}$ and $f = O_{y\to\infty}(y^{-B})$, then $\mathcal{M}(f,s)$ converges absolutely and uniformly on compact subsets of the half plane $\operatorname{Re} s < B$.*

Proof. We only prove the first assertion as the second follows from the first by Lemma 2.6.3. Replacing f with $y^B f$ we can reduce to the case $B = 0$ using Lemma 2.6.2. Then our assumptions imply that f is bounded and hence on any compact subset of $\operatorname{Re} s > 0$ there exists a constant $C > 0$, independent of s, such that $|f(y)| < C$ for $y \in (0,1]$ and $|f(y)y^s| < Cy^{-2}$. Then we can bound the Mellin transform:

$$|\mathcal{M}(f,s)| \leq C\int_0^1 y^{\operatorname{Re} s-1}dy + C\int_1^\infty y^{-2}dy = C\frac{1}{\operatorname{Re} s} + C.$$

Since $\frac{1}{\operatorname{Re} s}$ is bounded on any compact subset of $\operatorname{Re} s > 0$ we get a uniform bound on $|\mathcal{M}(f,s)|$. This implies the uniform convergence of the integral. □

Let us now be more precise: assume that f is of rapid decay at infinity and let $(\lambda_n)_{n\in\mathbb{N}}$ be a monotonly increasing sequence of real numbers that diverges to ∞. We write $f(y) \sim \sum_{n=0}^\infty b_n y^{\lambda_n}$ as $y \to 0$ if $f(y) - \sum_{n=0}^{N-1} b_n y^{\lambda_n} = O(y^{\lambda_N})$ as $y \to 0$ for any integer $N \geq 0$.

Since $f = O_{y\to 0}(y^{\lambda_0})$, $\mathcal{M}(f,s)$ converges absolutely and uniformly on compact subsets of the half plane $\operatorname{Re} s > -\lambda_0$. For $\operatorname{Re} s > -\lambda_0$ we can split the integral

$$\begin{aligned}\mathcal{M}(f,s) &= \int_0^1 f(y)y^s\frac{dy}{y} + \int_1^\infty f(y)y^s\frac{dy}{y}\\ &= \int_0^1 \left(f(y) - \sum_{n=0}^{N-1} b_n y^{\lambda_n}\right) y^{s-1}dy + \sum_{n=0}^{N-1}\frac{b_n}{\lambda_n + s} + \int_1^\infty f(y)y^{s-1}dy.\end{aligned}$$

The first integral converges absolutely and uniformly on compact subsets of the half plane $\operatorname{Re} s > -\lambda_N$. The second integral converges absolutely and uniformly on compacts for all $s \in \mathbb{C}$, since by our assumptions for any $N \in \mathbb{Z}$, $f(y)$ can be bounded by Cy^{-N}. Hence the right hand side defines a meromorphic continuation of $\mathcal{M}(f,s)$ to the half plane $\operatorname{Re} s > -\lambda_N$ with simple poles of residue b_n at $s = -\lambda_n$ for $n = 0, \dots, N-1$ and no other singularities. We have proved the following theorem.

Theorem 2.8 *Let $f : \mathbb{R}_{>0} \to \mathbb{C}$ be continuous. Suppose that f is of rapid decay at ∞ and $f(y) \sim \sum_{n=0}^\infty b_n y^{\lambda_n}$ as $y \to 0$. Then $\mathcal{M}(f,s)$ has meromorphic continuation to the whole complex plane with simple poles of residue b_n for $s = -\lambda_n$ and no other singularities.*

From Theorem 2.8 we can deduce some standard properties of the Gamma function as we will see in 2.10. Of course the properties of $\Gamma(s)$ can be derived in a simpler fashion, using the functional equation $\Gamma(s+1) = s\Gamma(s)$. The first useful application of Theorem 2.8 will appear in relation to the Riemann zeta function.

Theorem 2.9 (Mellin principle) *Let $f, g : \mathbb{R}_{>0} \to \mathbb{C}$ be continuous functions such that*

$$f(y) = a_0 + O(e^{-cy^\alpha}),\ \ g(y) = b_0 + O(e^{-cy^\alpha})$$

for $y \to \infty$ and positive constants c, α. Suppose furthermore that

$$f(1/y) = Cy^k g(y)$$

for a positive real number k and $C \in \mathbb{C} \setminus \{0\}$.

Then $\mathcal{M}(f - a_0, s)$ and $\mathcal{M}(g - b_0, s)$, converge absolutely in the half plane $\operatorname{Re} s > k$ and admit a meromorphic continuation to $\mathbb{C}$ with simple poles at $s = 0$ and $s = k$ of residues $\operatorname{Res}_{s=0} \mathcal{M}(f - a_0, s) = -a_0 = -C \operatorname{Res}_{s=k} \mathcal{M}(g - b_0, s)$ and $\operatorname{Res}_{s=k} \mathcal{M}(f - a_0, s) = Cb_0 = -C^{-1} \operatorname{Res}_{s=0} \mathcal{M}(g - b_0, s)$ and no other poles. Furthermore we have the functional equation

$$\mathcal{M}(f - a_0, s) = C\mathcal{M}(g - b_0, k - s).$$

Proof. The statements on the meromorphic continuation of the Mellin transforms and the location and residues of their poles follow from Theorem 2.8. Indeed $f - a_0$ is of rapid decay and $f(1/y) - a_0 = -a_0 + Cy^k b_0 + O(e^{-cy^\alpha})$. Hence $f(y) \sim Cy^{-k} b_0 - a_0$ as $y \to 0$. The functional equation follows from Lemma 2.6 if $a_0 = b_0 = 0$. If $a_0 \neq 0$ or $b_0 \neq 0$ we need a slightly different approach to prove the functional equation. This approach will also prove the whole theorem without appealing to Theorem 2.8.

Let $\operatorname{Re} s > k$. For the functional equation split the integral defining the Mellin transform and perform the change of variables $y \to 1/y$ on the first integral:

$$\begin{aligned}
\mathcal{M}(f - a_0, s) &= \int_0^1 f(y) y^s \frac{dy}{y} - \frac{a_0}{s} + \int_1^\infty (f(y) - a_0) y^s \frac{dy}{y} \\
&= \int_1^\infty f(1/y) y^{-s} \frac{dy}{y} - \frac{a_0}{s} + \int_1^\infty (f(y) - a_0) y^s \frac{dy}{y} \\
&= \int_1^\infty Cg(y) y^{k-s} + (f(y) - a_0) y^s \frac{dy}{y} - \frac{a_0}{s} \\
&= \int_1^\infty C(g(y) - b_0) y^{k-s} + (f(y) - a_0) y^s \frac{dy}{y} - \frac{a_0}{s} + \frac{Cb_0}{s-k}. \qquad (3)
\end{aligned}$$

Note that the integral in the last line defines a holomorphic function for all $s \in \mathbb{C}$. So the meromorphic continuation of $\mathcal{M}(f - a_0, s)$ can be given by (3) and the location of the poles and their residues follows. Doing the same transformations to $C\mathcal{M}(g-b_0,s)$ for $\operatorname{Re} s > k$ we obtain

$$C\mathcal{M}(g-b_0,s) = \int_1^\infty (f(y)-a_0)y^{k-s} + C(g(y)-b_0)y^s\frac{dy}{y} + \frac{a_0}{s-k} - C\frac{b_0}{s}, \tag{4}$$

and we can check the functional equation by replacing s with $k-s$ in (4). □

1.0.1. *The Gamma function.* We recall some basic properties of the Gamma function

$$\Gamma(s) = \int_0^\infty e^{-y}y^s\frac{dy}{y}. \tag{5}$$

Lemma 2.10 (1) *The Gamma function continues to a meromorphic function on $\mathbb{C}$ with no zeros and simple poles at $s=-n\in\mathbb{Z}_{\leq 0}$ of residue $(-1)^n/n!$ and no other poles.*

(2) *We have the functional equation*

$$\Gamma(s+1) = s\Gamma(s).$$

(3) *Euler's reflection formula:*

$$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin(\pi s)}.$$

(4) *Legendre's duplication formula:*

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

(5) *For $k\in\mathbb{Z}_{\geq 0}$ we have $\Gamma(k+1)=k!$ and $\Gamma(\frac{1}{2})=\sqrt{\pi}$.*

Sketch of proof. Since the Gamma function is the Mellin transform of $f(y) = e^{-y} \sim \sum(-1)^n y^n/n!$ as $y\to 0$ we can apply Theorem 2.8 to see that $\Gamma(s)$ has a meromorphic continuation to $\mathbb{C}$ with simple poles at $s=-n\in\mathbb{Z}_{\leq 0}$ of residue $(-1)^n/n!$. The integral (5) is absolutely convergent for $\operatorname{Re} s>0$ and we can prove the functional equation $\Gamma(s+1)=s\Gamma(s)$ by a simple change of variables. However both $\Gamma(s+1)$ and $s\Gamma(s)$ have holomorphic continuations to $\mathbb{C}\setminus\mathbb{Z}_{\leq 0}$, so they must be equal on the whole of $\mathbb{C}\setminus\mathbb{Z}_{\leq 0}$. Now suppose there exists $s\in\mathbb{C}$ with $\Gamma(s)=0$. For $s\in\mathbb{Z}_{>0}$ we clearly have $\Gamma(s)>0$, so we can assume that $1-s\notin\mathbb{Z}_{\leq 0}$ and $\Gamma(1-s)\in\mathbb{C}$. Now we can derive a contradiction from Euler's reflection formula, since $\frac{\pi}{\sin(\pi s)}$ does not vanish. The proof of Legendre's duplication formula can be found in most texts on the Gamma function so we skip them. □

The crucial connection between the Gamma function and the zeta function follows from the simple equation

$$\pi^{-s}\Gamma(s)n^{-2s} = \int_0^\infty e^{-\pi n^2 y} y^s \frac{dy}{y} \tag{6}$$

which follows from Lemma 2.6.

1.0.2. *Back to the zeta function.* Summing (6) over all $n \in \mathbb{N}$ we obtain

$$\pi^{-s}\Gamma(s)\zeta(2s) = \int_0^\infty \left(\sum_{n\in\mathbb{N}} e^{-\pi n^2 y}\right) y^s \frac{dy}{y} \tag{7}$$

Note that the integral on the right hand side converges absolutely, so we are allowed to swap integration and summation. The function $\sum_{n\in\mathbb{N}} e^{-\pi n^2 y}$ comes from **Jacobi's theta function**

$$\theta(\tau) = \sum_{n\in\mathbb{Z}} e^{\pi i n^2 \tau} = 1 + 2\sum_{n\in\mathbb{N}} e^{\pi i n^2 \tau}. \tag{8}$$

Hence we obtain

$$Z(s) := \pi^{-s/2}\Gamma(s/2)\zeta(s) = \frac{1}{2}\int_0^\infty (\theta(iy) - 1) y^s \frac{dy}{y}.$$

The function Z is called the **completed zeta function** and many of its properties follow directly from the remarkable properties of θ which we cite now.

Theorem 2.11 *The theta function defines a holomorphic function on the upper half plane $\mathcal{H} = \{\tau \in \mathbb{C} | \, Im(\tau) > 0\}$ and satisfies the functional equation*

$$\theta\left(-\frac{1}{\tau}\right) = \sqrt{\frac{\tau}{i}}\theta(\tau).$$

Remark 2.12 *Here the square root is defined by*

$$\sqrt{z} = e^{\frac{1}{2}\log(z)},$$

where log *is the principal branch of the logarithm.*

Proof. We will study the transformation properties of more general theta functions in Section 3 and will prove a much more general statement there. □

Theorem 2.13 *The completed zeta function Z has a meromorphic continuation to $\mathbb{C}$ with simple poles at $s = 0$ and $s = 1$ of residues -1 and 1 respectively and no other poles. It satisfies the functional equation*

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

PROOF. Note that $Z(2s)$ is the Mellin transform of $f(y) = \frac{1}{2}\theta(iy)$. By definition we have $f(y) = \frac{1}{2} + O(e^{-y})$ and by Theorem 2.11

$$f(1/y) = \frac{1}{2}\sqrt{y}\,\theta(iy) = \frac{1}{2} + O(e^{-\pi y}).$$

We can now apply Theorem 2.9, which implies the statement of the theorem. □

We restate Theorem 2.13 in terms of the zeta function:

Theorem 2.14 *The zeta function has a meromorphic continuation to $\mathbb{C}$ with only one simple pole at $s = 1$ of residue 1 and satisfies the functional equation*

$$\zeta(1-s) = 2(2\pi)^{-s}\Gamma(s)\cos\left(\frac{\pi s}{2}\right)\zeta(s)$$

PROOF. Recall that the Gamma function has simple poles at all non-positive integers. Since $Z(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$ has a meromorphic continuation to $\mathbb{C}$ we can use the expression $\zeta(s) = \pi^{s/2}\Gamma(s/2)^{-1}Z(s)$ to obtain a meromorphic continuation of $\zeta(s)$ to $\mathbb{C}$. Furthermore, by Lemma 2.10 $\Gamma(s/2)$ is never zero, so the only possible poles of $\zeta(s)$ are at the poles of $Z(s)$, at $s = 0$ and $s = 1$. Since $\Gamma(s/2)$ has a simple pole at $s = 0$, $\Gamma(s/2)^{-1}Z(s)$ has no pole there. On the other hand $\pi^{s/2}\Gamma(s/2)^{-1}$ has no zero at $s = 1$, so $\zeta(s)$ has a pole there and

$$\operatorname{Res}_{s=1}\zeta(s) = \pi^{1/2}\Gamma(1/2)^{-1}\operatorname{Res}_{s=1}Z(s) = 1.$$

The functional equation follows from the basic properties of the Gamma function in Lemma 2.10; see also [5, VII.(1.7)]. □

Remark 2.15 *Using the fact that the residue of $Z(s)$ at $s = 0$ is -1, we can deduce $\zeta(0) = -\frac{1}{2}$. In the exercise classes we will use Theorem 2.8 to determine all values of ζ at non-positive integers.*

2. The prime number theorem

In this subsection we sketch a proof of the prime number theorem by D. Newman. Instead of studying $\pi(x)$ we study the related function $\psi(x) = \sum_{p\le x}\log(p)$, where the sum is taken over all prime numbers smaller or equal to x. As we will see soon, $\psi(x)$ has close ties to the zeta function.

Proposition 2.16 *The prime number theorem*

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

is equivalent to the fact that

$$\psi(x) \sim x.$$

Proof. Suppose $\psi(x) \sim x$. We have

$$\psi(x) \leq \sum_{p \leq x} \log(x) = \log(x)\pi(x).$$

In the other direction, for any $\epsilon > 0$,

$$\psi(x) \geq \sum_{x^{1-\epsilon} \leq p \leq x} \log p \geq \sum_{x^{1-\epsilon} \leq p \leq x} (1-\epsilon)\log x \geq (1-\epsilon)\log x(\pi(x) - x^{1-\epsilon})$$

Using these inequalities

$$\liminf \pi(x)\frac{\log x}{x} \geq \liminf \frac{\psi(x)}{x} = 1$$

and

$$\limsup \pi(x)\frac{\log x}{x} \leq \limsup (1-\epsilon)^{-1}\frac{\psi(x)}{x} = \frac{1}{1-\epsilon}.$$

Since $\epsilon > 0$ was arbitrary $\limsup \pi(x)\frac{\log x}{x} \leq 1$ and hence the limit $\lim \pi(x)\frac{\log x}{x}$ exists and equals 1. □

So the remainder of this subsection we will show $\psi(x) \sim x$.

Lemma 2.17 *We have $\psi(x) = O(x)$.*

Proof. For $n \in \mathbb{N}$

$$2^{2n} = \sum_{0 \leq k \leq 2n} \binom{2n}{k} \geq \binom{2n}{n} = \frac{(2n)!}{n!^2} \geq \prod_{n < p \leq 2n} p = e^{\psi(2n)-\psi(n)}.$$

This shows $\psi(2n) - \psi(n) \leq \log(2)2n$. From this and the fact that $\psi(x) \leq \psi(x-1) + \log(x)$ we deduce $\psi(x) - \psi(x/2) \leq Cx$ for any constant $C > \log 2$ and $x \geq x_0(C)$. Now sum this inequality for $x, x/2, \ldots, x/2^r$ where r is the highest natural number such that $x/2^r \geq x_0$. We obtain $\psi(x) \leq Cx(1+1/2+\ldots)+\psi(x_0) = 2Cx+O(1)$. □

To obtain better estimates we use powerful tools from complex analysis. The first result was the basis of the original proof of the prime number theorem:

Theorem 2.18 (Hadamard, de la Vallée Poussin)

$$\zeta(s) \neq 0, \text{ for } \mathrm{Re}\, s = 1.$$

Proof. Let $\mathrm{Re}\, s = \sigma > 1$. By the Euler product we have

$$\log(\zeta(s)) = \sum_p \sum_{k \geq 1} \frac{1}{p^{ks}k} \tag{9}$$

and so

$$|\zeta(\sigma+it)| = \exp\left(\sum_p \sum_{k\geq 1} \mathrm{Re}\,(p^{-kit})\frac{1}{kp^{k\sigma}}\right)$$

Note that $\mathrm{Re}\,(p^{-kit}) = \cos(kt\log(p))$. Now we look at

$$\zeta(\sigma)^3|\zeta(\sigma+it)^4\zeta(\sigma+2it)| = \exp\left(\sum_p \sum_{k\geq 1} \frac{3+4\cos(kt\log(p))+\cos(2kt\log(p))}{kp^{k\sigma}}\right) \geq 1.$$

This inequality follows from the simple fact that for any x

$$3+4\cos(x)+\cos(2x) = 2(1+\cos(x))^2 \geq 0.$$

Now assume that $\zeta(1+it_0)=0$ for $t_0\neq 0$. Then $\zeta(\sigma)^3|\zeta(\sigma+it_0)^4\zeta(\sigma+2it_0)|$ would tend to 0 as $\sigma\to 1$, which is a contradiction to the above inequality. □

Lemma 2.19 *Let $\Phi(s)=\sum_p \frac{\log p}{p^s}$. Then $\Phi(s)-1/(s-1)$ is holomorphic in the half plane $Re\, s \geq 1$.*

Proof. By our results on Dirichlet series we can form the derivative of a convergent Dirichlet series by termwise differentiation:

$$-\log(\zeta(s))' = -\frac{\zeta'(s)}{\zeta(s)} = \sum_p \frac{\log p}{p^s-1} = \Phi(s) + \sum_p \frac{\log p}{p^s(p^s-1)}.$$

The last sum converges for $\mathrm{Re}\, s > 1/2$, so $\Phi(s)$ extends meromorphically to the half plane $\mathrm{Re}\, s > 1/2$ with a simple pole at $s=1$ of residue 1. Since $\zeta(s)$ does not vanish on the half plane $\mathrm{Re}\, s \geq 1$ we can conclude. □

Now we relate $\psi(x)$ to the zeta function.

Theorem 2.20 *The integral*

$$\int_1^\infty \frac{\psi(x)-x}{x^2}dx \tag{10}$$

converges.

Proof. Let $\mathrm{Re}\, s > 1$. We apply Abel summation with the following input: The sequence a_n is set to $\log n$ if n is prime and 0 else and $\phi(x)=x^{-s}$. Then Lemma 1.5 implies

$$\sum_{1\leq p\leq N} \frac{\log p}{p^s} = \psi(N)N^{-s} + s\int_1^N \psi(x)x^{-s-1}dx$$

and in the limit

$$\Phi(s) = s\int_1^\infty \psi(x)x^{-s-1}dx = s\int_0^\infty e^{-st}\psi(e^t)dt. \tag{11}$$

We now apply a Theorem from complex analysis that we will not prove. For the proof see [2, Theorem 10.7.12].

Theorem 2.21 *Let $f(t)$ be a bounded and locally integrable function for $t \geq 0$ and assume that the function $g(s) = \int_0^\infty f(t)e^{-st}dt$, defined on $Re\, s > 0$, extends to a holomorphic function for $Re\, s \geq 0$. Then $\int_0^\infty f(t)dt$ converges and is equal to $g(0)$.*

We apply this theorem with $f(t) = \psi(e^t)e^{-t} - 1$. The corresponding function $g(s)$ is $\Phi(s+1)/(s+1) - 1/s$ which extends to a holomorphic function on $\mathrm{Re}\, s \geq 0$ by Lemma 2.19. By (11) $g(0)$ is precisely the integral we want to show convergence for. □

Theorem 2.22

$$\psi(x) \sim x$$

Proof. Assume that for $\lambda > 1$ there exist arbitrarly large x such that $\psi(x) \geq \lambda x$. Then for any such x

$$\int_x^{\lambda x} \frac{\psi(t) - t}{t^2} dt \geq \int_x^{\lambda x} \frac{\lambda x - t}{t^2} dt = \int_1^{\lambda} \frac{\lambda - u}{u^2} du > 0,$$

which contradicts the convergence of $\int_1^\infty (\psi(t) - t)t^{-2}dt$. Similarly we can argue that $\lambda < 1$ there cannot be arbitrarly large x with $\psi(x) \leq \lambda x$. □

CHAPTER 3

The Dedekind ζ-function

The L-function in the title of this section is a generalization of the Riemann zeta function to number fields. We will see that - similarly to $\zeta(s)$ - its analytic properties yield important number theoretic consequences. The proof of meromorphic continuation and functional equation for the Dedekind zeta function follows the same approach: after multiplying it by a (generalized) gamma function, we will express it as a Mellin transform of a (generalized) theta function which satisfies a transformation property required by the Mellin principle, and the Mellin principle will lead to a desired result. Therefore, before we even define the Dedekind zeta function, we introduce the ingredients which are essential for its study.

1. Preliminaries

Definition 3.1 *Let α be an algebraic number and $f \in \mathbb{Q}[x]$ its minimal polynomial (i.e. f is monic, irreducible over $\mathbb{Q}$, and $f(\alpha) = 0$), put $n := \deg(f)$. We call the quotient*

$$\mathbb{Q}(\alpha) := \mathbb{Q}[x]/(f(x))$$

*a **number field** of **degree** n.*
Furthermore, if $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ are the roots of f, we define embeddings by extending the following maps as ring homomorphisms:

$$\tau_i : \mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}, \qquad \alpha \mapsto \alpha_i, \qquad (i = 1, \ldots, n).$$

We say that the embedding τ_i is real if $\alpha_i \in \mathbb{R}$, otherwise we call it complex.

Remark 3.2

(1) *As a vector space $\mathbb{Q}(\alpha) = \{a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} : a_0, a_1, \ldots, a_{n-1} \in \mathbb{Q}\}$.*
(2) *$\tau_1, \ldots, \tau_n$ are all possible embeddings of $\mathbb{Q}(\alpha)$ to $\mathbb{C}$ as rings. The complex embeddings come in pairs: $\tau : \alpha \mapsto \alpha_i$ and $\bar{\tau} : \alpha \mapsto \bar{\alpha}_i$.*
(3) $\overline{\tau_i(a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1})} = \bar{\tau}_i(a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1})$, $i = 1, \ldots, n$.

Proof. Exercise. □

Definition 3.3 *For a number field K we define the **ring of integers***

$$\mathcal{O}_K := \{z \in K : f(z) = 0 \text{ for some monic } f \in \mathbb{Z}[x]\}.$$

The invertible elements in $\mathcal{O}_K$ comprise the ***group $\mathcal{O}_K^\times$ of units*** *of $\mathcal{O}_K$.*

If $\mathcal{O}_K = \mathbb{Z}w_1 \oplus \ldots \oplus \mathbb{Z}w_n$ for some $w_1, \ldots, w_n \in \mathcal{O}_K$, the ***discriminant of a number field*** *K is defined as*

$$d_K := \operatorname{disc}(\mathcal{O}_K) := \operatorname{disc}(w_1, \ldots, w_n) := \det([\tau_i(w_j)]_{i,j})^2 \, .$$

Similarly, for a nonzero ideal $\mathfrak{a} \lhd \mathcal{O}_K$ with an integral basis $\mathfrak{a} = \mathbb{Z}a_1 \oplus \ldots \oplus \mathbb{Z}a_n$, $a_1, \ldots, a_n \in \mathfrak{a}$, the ***discriminant of an ideal*** *$\mathfrak{a}$ is equal to $d_{\mathfrak{a}} := \operatorname{disc}(a_1, \ldots, a_n)$.*

Remark 3.4 *The above definitions do not depend on a choice of integral basis.*

From now on K will denote a number field of degree n, d_K its discriminant, $\mathcal{O}_K$ the ring of integers, and $\{\tau_i : i = 1, \ldots, n\}$ the set of all embeddings $K \hookrightarrow \mathbb{C}$. Sometimes, to differentiate between the embeddings, we will write ρ for the real embeddings and σ, $\bar{\sigma}$ for the pairs of complex embeddings, and we will denote the number of them by r_1 and $2r_2$ respectively.

2. Minkowski theory

Consider the canonical embedding

$$j : K \to K_{\mathbb{C}} := \prod_\tau \mathbb{C}, \qquad a \mapsto ja := (\tau(a))_\tau,$$

where the product is taken over n embeddings $\tau : K \to \mathbb{C}$. The complex vector space $K_{\mathbb{C}}$ is equipped with an involution

$$F : K_{\mathbb{C}} \to K_{\mathbb{C}} \, , \qquad z = (z_\tau)_\tau \mapsto \bar{z} := (\bar{z}_{\bar{\tau}})_\tau$$

and the Hermitian scalar product

$$\langle x, y \rangle = \sum_\tau x_\tau \bar{y}_\tau$$

which satisfies $\langle F(x), F(y) \rangle = \langle y, x \rangle$. In addition, we have the involutions

$$z = (z_\tau)_\tau \mapsto z^* := (z_{\bar{\tau}})_\tau \qquad \text{and} \qquad z = (z_\tau)_\tau \mapsto {}^*z := (\bar{z}_\tau)_\tau \, .$$

Note that $\bar{z} = {}^*z^*$, and that ${}^*z$ is the adjoint element to z with respect to $\langle \, , \, \rangle$, i.e., $\langle xz, y \rangle = \langle x, {}^*zy \rangle$.

We endow the space $K_{\mathbb{C}}$ with the following homomorphisms:

$$Tr : K_{\mathbb{C}} \to \mathbb{C} \, , \qquad Tr(z) = \sum_\tau z_\tau \, ,$$

$$N : \underbrace{K_{\mathbb{C}}^\times}_{\prod_\tau \mathbb{C}^\times} \to \mathbb{C}^\times \, , \qquad N(z) = \prod_\tau z_\tau \, ,$$

which denote respectively the trace and the determinant of the endomorphism

$$K_{\mathbb{C}} \to K_{\mathbb{C}}\,, \qquad x \mapsto zx\,.$$

Observe that if $z = ja$ for some $a \in K$, then Tr and N coincide with the usual trace and norm of $K/\mathbb{Q}$:

$$Tr(ja) = Tr_{K/\mathbb{Q}}(a) := \sum_{i=1}^{n} \tau_i(a)\,, \qquad N(ja) = N_{K/\mathbb{Q}}(a) := \prod_{i=1}^{n} \tau_i(a)\,.$$

Note that for $a \in K$ we have $F(ja) = ja$. Hence, the image of j is actually contained in a smaller vector space

$$K_{\mathbb{R}} := \{z \in K_{\mathbb{C}} : z = \bar{z}\}$$

over $\mathbb{R}$. We can think of it as a tensor product $K \otimes_{\mathbb{Q}} \mathbb{R}$ via

$$K \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\sim} K_{\mathbb{R}}\,, \qquad a \otimes x \mapsto (ja)x\,.$$

It is also easy to see that the restriction of the Hermitian scalar product $\langle\ ,\ \rangle$ from $K_{\mathbb{C}}$ to $K_{\mathbb{R}}$ gives a scalar product $\langle\ ,\ \rangle : K_{\mathbb{R}} \times K_{\mathbb{R}} \to \mathbb{R}$ and yields a norm on $K_{\mathbb{R}}$ given by $\|x\| := \sqrt{\langle x, x\rangle}$. We call $K_{\mathbb{R}}$ the **Minkowski space**.

We distinguish the subspace

$$K_{\mathbb{R},\pm} := \{x \in K_{\mathbb{R}} : x = x^*\} = \{(x_\tau)_\tau \in K_{\mathbb{R}} : \forall_\tau\, x_\tau \in \mathbb{R}\}$$

and the subgroup

$$K_{\mathbb{R},+}^{\times} := \{x \in K_{\mathbb{R},\pm} : x > 0\}\,,$$

where $x > 0$ means that $x_\tau > 0$ for every τ. Together they form the upper half-space associated to K:

$$\mathbb{H}_K := K_{\mathbb{R},\pm} + iK_{\mathbb{R},+}^{\times} = \{z \in K_{\mathbb{C}} : z = z^*, \mathrm{Im}\,(z) > 0\}\,,$$

where we put $\mathrm{Re}\,(z) := \frac{1}{2}(z + \bar{z})$, $\mathrm{Im}\,(z) := \frac{1}{2i}(z - \bar{z})$.

Finally, we define the homomorphisms

$$|\ \ | : K_{\mathbb{R}}^{\times} \to K_{\mathbb{R},+}^{\times}\,, \qquad x = (x_\tau)_\tau \mapsto |x| := (|x_\tau|)_\tau\,,$$

$$\log : K_{\mathbb{R},+}^{\times} \xrightarrow{\sim} K_{\mathbb{R},\pm}\,, \qquad x = (x_\tau)_\tau \mapsto \log x := (\log x_\tau)_\tau\,,$$

and for two tuples $z = (z_\tau)_\tau, p = (p_\tau)_\tau \in K_{\mathbb{C}}$ we define the power

$$z^p = (z_\tau^{p_\tau})_\tau \in K_{\mathbb{C}} \qquad \text{by} \qquad z_\tau^{p_\tau} = e^{p_\tau \log z_\tau}\,,$$

where we choose the principal branch of the logarithm with the plane cut along the negative real axis.

Remark 3.5 *If $a \in K$, then $N(e^{|ja|^2}) = e^{\langle ja, ja\rangle}$.*

PROOF. Observe that $e^{|ja|^2} = (e^{|\tau(a)|^2})_\tau$, and thus

$$N(e^{|ja|^2}) = e^{\sum_\tau |\tau(a)|^2} = e^{\sum_\tau \tau(a)\bar{\tau}(a)} = e^{\langle ja, ja\rangle}\,.$$

□

Example 3.6

(1) *If $K = \mathbb{Q}$, then $K_\mathbb{C} = \mathbb{C}$, $K_\mathbb{R} = \mathbb{R} = K_{\mathbb{R},\pm}$ and $\mathbb{H}_K = \mathbb{R} + i\mathbb{R}_{>0}$ is the usual complex upper half-plane $\mathbb{H}$.*

(2) *If $K = \mathbb{Q}(\sqrt{m})$ with $m < 0$ square-free, then K has 2 complex embeddings:*

$$\tau : \sqrt{m} \mapsto \sqrt{m} \qquad \text{and} \qquad \bar{\tau} : \sqrt{m} \mapsto -\sqrt{m}\,.$$

Hence: $K_\mathbb{C} = \mathbb{C} \times \mathbb{C}$,

$$K_\mathbb{R} = \{(a,b) \in \mathbb{C}^2 : (a,b) = (\bar{b}, \bar{a})\} = \{(a, \bar{a}) : a \in \mathbb{C}\}\,,$$
$$K_{\mathbb{R},\pm} = \{(a,a) : a \in \mathbb{R}\}\,, \qquad K^\times_{\mathbb{R},+} = \{(b,b) : b \in \mathbb{R}_{>0}\}$$

and

$$\mathbb{H}_K = \{(a+ib, a+ib) : a \in \mathbb{R}, b \in \mathbb{R}_{>0}\} = \{(z,z) : z \in \mathbb{H}\}\,.$$

(3) *If $K = \mathbb{Q}(\sqrt{m})$ with $m > 0$ square-free, then K has 2 real embeddings:*

$$\tau_1 : \sqrt{m} \mapsto \sqrt{m} \qquad \text{and} \qquad \tau_2 : \sqrt{m} \mapsto -\sqrt{m}\,.$$

Hence: $K_\mathbb{C} = \mathbb{C} \times \mathbb{C}$,

$$K_\mathbb{R} = \{(a,b) \in \mathbb{C}^2 : (a,b) = (\bar{a}, \bar{b})\} = \mathbb{R}^2\,,$$

$K_{\mathbb{R},\pm} = \mathbb{R}^2$, $K^\times_{\mathbb{R},+} = \mathbb{R}^2_{>0}$, $\mathbb{H}_K = \mathbb{H}^2$.

Observe the difference between examples (2) and (3)!

The point of introducing this general setting, known as Minkowski theory, is that it allows us to interpret integral ideals of K as lattices in the space $K_\mathbb{R}$, as described in Lemma 3.8.

Definition 3.7 *A **lattice** in an n-dimensional $\mathbb{R}$-vector space V is a subgroup of the form*

$$\Gamma = \mathbb{Z}v_1 \oplus \ldots \oplus \mathbb{Z}v_m\,,$$

*where the vectors $v_1, \ldots, v_m \in V$ are linearly independent. The set $\{v_1, \ldots, v_m\}$ is a **basis**, and*

$$\Phi = \{x_1 v_1 + \ldots + x_m v_m : x_i \in \mathbb{R}, 0 \le x_i < 1\}\,,$$

*a **fundamental mesh** of the lattice Γ. The lattice is **complete** if $m = n$.*

Lemma 3.8 *If $\mathfrak{a} \neq 0$ is an ideal of $\mathcal{O}_K$, then $\Gamma = j\mathfrak{a}$ is a complete lattice in $K_\mathbb{R}$. Its fundamental mesh has volume*

$$\mathrm{vol}(\Gamma) := \sqrt{|d_K|}\,(\mathcal{O}_K : \mathfrak{a})\,.$$

Proof. Let $\{\alpha_1, \dots, \alpha_n\}$ be an integral basis for $\mathfrak{a}$, i.e., $\mathfrak{a} = \mathbb{Z}\alpha_1 \oplus \dots \oplus \mathbb{Z}\alpha_n$, $\alpha_1, \dots, \alpha_n \in \mathfrak{a}$. Then $\Gamma = \mathbb{Z}j\alpha_1 \oplus \dots \oplus \mathbb{Z}j\alpha_n$, and thus it is a complete lattice. The fundamental mesh of the lattice Γ has volume equal to $|\det([\langle j\alpha_i, j\alpha_l\rangle]_{i,l})|^{1/2}$. In our case,

$$\langle j\alpha_i, j\alpha_l\rangle = \sum_{\tau} \tau(\alpha_i)\overline{\tau(\alpha_l)}\,.$$

Hence, if we put $A = [\tau_i(\alpha_l)]_{i,l}$, we obtain $\mathrm{vol}(\Gamma) = |\det(A\,\overline{{}^tA})|^{1/2} = |\det A|$. On the other hand, $(\det A)^2 = \det([\tau_i(\alpha_l)]_{i,l})^2 = d_{\mathfrak{a}}$ defines the discriminant of the ideal $\mathfrak{a}$ and satisfies the equality $d_{\mathfrak{a}} = (\mathcal{O}_K : \mathfrak{a})^2 d_K$ (see [5, I.(2.12)]). □

3. Theta function

In this section we extend the definition (8) of a theta series $\theta(z)$ defined on the complex upper half-plane $\mathbb{H}_{\mathbb{Q}}$ to a theta series on $\mathbb{H}_K$. The transformation formula for for the latter (and thus also for $\theta(z)$) will follow from *Poisson summation formula.* In order to present this formula we need to introduce the notions that come into its statement.

Definition 3.9 *For a complete lattice Γ in $K_{\mathbb{R}}$, its* ***dual lattice*** *is defined as*

$$\Gamma' = \{g' \in K_{\mathbb{R}} : \forall_{g\in\Gamma}\langle g, g'\rangle \in \mathbb{Z}\}\,.$$

Example 3.10 *Let $0 \neq \mathfrak{a} \lhd \mathcal{O}_K$ and $\Gamma = j\mathfrak{a}$. We will compute the dual lattice to Γ.*

Let $\alpha_1, \dots, \alpha_n$ be an integral basis of $\mathfrak{a}$. Since the lattice Γ is complete in $K_{\mathbb{R}}$, every $x \in K_{\mathbb{R}}$ can be written as $x = x_1 j\alpha_1 + \dots x_n j\alpha_n$ for some $x_1, \dots, x_n \in \mathbb{R}$. Hence,

$$\Gamma' = \{y \in K_{\mathbb{R}} : \forall_{\alpha\in\mathfrak{a}}\langle j\alpha, y\rangle \in \mathbb{Z}\} = \{y \in K_{\mathbb{R}} : \forall_{\alpha\in\mathfrak{a}} Tr(j\alpha\,{}^*y) \in \mathbb{Z}\}\,,$$

and thus

$$\begin{aligned}
{}^*\Gamma' &= \{x \in K_{\mathbb{R}} : Tr(j\alpha\, x) \in \mathbb{Z}\}\\
&= \{x_1 j\alpha_1 + \dots x_n j\alpha_n : x_1, \dots, x_n \in \mathbb{R}, \forall_{i=1,\dots,n} \sum_{k=1}^{n} x_k Tr(j\alpha_i j\alpha_k) \in \mathbb{Z}\}\\
&= \{x_1 j\alpha_1 + \dots x_n j\alpha_n : x_1, \dots, x_n \in \mathbb{R}, \forall_{i=1,\dots,n} \sum_{k=1}^{n} x_k Tr_{K/Q}(\alpha_i\alpha_k) \in \mathbb{Z}\}\\
&= \{x_1 j\alpha_1 + \dots x_n j\alpha_n : x_1, \dots, x_n \in \mathbb{Q}, \forall_{i=1,\dots,n} \sum_{k=1}^{n} x_k Tr_{K/Q}(\alpha_i\alpha_k) \in \mathbb{Z}\}\\
&= \{jx : x \in K, \forall_{i=1,\dots,n} Tr_{K/Q}(\alpha_i\, x) \in \mathbb{Z}\}\\
&= \{jx : x \in K, Tr_{K/Q}(x\mathfrak{a}) \subseteq \mathbb{Z}\}
\end{aligned}$$

Now recall that the fractional ideal

$$\mathfrak{d}^{-1} := \{x \in K : Tr_{K/\mathbb{Q}}(x\mathcal{O}_K) \subseteq \mathbb{Z}\}$$

defines the ***inverse different*** *of $K/\mathbb{Q}$. We get*

$$\begin{aligned} {}^*\Gamma' &= \{jx : x \in K, \forall_{\alpha\in\mathfrak{a}} Tr_{K/\mathbb{Q}}(x\alpha\mathcal{O}_K) \subseteq \mathbb{Z}\} = \{jx : x \in K, \forall_{\alpha\in\mathfrak{a}} x\alpha \in \mathfrak{d}^{-1}\} \\ &= j\left((\mathfrak{a}\mathfrak{d})^{-1}\right) . \end{aligned}$$

Definition 3.11 *A* ***Schwartz function*** *on a euclidean vector space $K_\mathbb{R}$ is a C^∞-function $f : K_\mathbb{R} \to \mathbb{C}$ such that*

$$\lim_{x\to\infty} f(x)\|x\|^m = 0 \qquad \text{for any} \qquad m \geq 0$$

and the same holds for all derivatives of f.

The ***Fourier transform*** *of a Schwartz function f is*

$$\hat{f}(y) = \int_{K_\mathbb{R}} f(x)e^{-2\pi i\langle x,y\rangle}\, dx\,,$$

where dx is a Haar measure on $K_\mathbb{R}$ normalized so that the cube spanned by an orthonormal basis with respect to $\langle\ ,\ \rangle$ has volume 1.

Remark 3.12 *The Fourier transform of a Schwartz function is again a Schwartz function.*

Remark 3.13 *The Haar measure dx is very closely related with the Lebesgue measure. This follows from the fact that the map*

$$\begin{array}{rcl} \iota : K_\mathbb{R} & \longrightarrow & \mathbb{R}^n\,, \\ x = (x_\tau)_\tau & \longmapsto & w = (w_\tau)_\tau \end{array} \qquad \text{where} \quad \begin{cases} w_\rho = x_\rho \\ w_\sigma = \sqrt{2}Re\,(x_\sigma),\ w_{\bar{\sigma}} = \sqrt{2}Im\,(x_\sigma) \end{cases}$$

is an isomorphism which preserves the inner product ($\mathbb{R}^n$ being equipped with the standard inner product). In particular, for a cube $\mathcal{C} \subseteq K_\mathbb{R}$ spanned by an orthonormal basis with respect to $\langle\ ,\ \rangle$,

$$\int_\mathcal{C} dx = \int_{\iota(\mathcal{C})} dw\,,$$

where dw denotes the Lebesgue measure on $\mathbb{R}^n$. Because of this correspondence we will sometimes switch to Lebesgue integrals or use without further explanation some results from the Lebesgue integration theory. This will be explained in detail (i.e. with use of the isomorphism ι) only in the Example 3.14.

Example 3.14 *The function $h : K_\mathbb{R} \to \mathbb{C}$, $h(x) = e^{-\pi\langle x,x\rangle}$ is a Schwartz function with Fourier transform $\hat{h}(x) = h(x)$.*

PROOF. We identify $K_{\mathbb{R}}$ with $\mathbb{R}^n$ via the isomorphism ι explained in Remark 3.13. Denote by $(\ ,\ )$ the Euclidean inner product. Then for $\iota(y) = u = (u_1, \ldots, u_n)$ and $w = (w_1, \ldots, w_n)$,

$$\hat{h}(y) = \int_{K_{\mathbb{R}}} e^{-\pi\langle x,x\rangle} e^{-2\pi i\langle x,y\rangle}\, dx = \int_{\mathbb{R}^n} e^{-\pi(w,w)} e^{-2\pi i(w,u)}\, dw$$
$$= \prod_{j=1}^{n} \int_{\mathbb{R}} e^{-\pi w_j^2} e^{-2\pi i w_j u_j}\, dw_j =: \prod_{j=1}^{n} \hat{H}(u_j)$$

By Lebesgue dominated convergence theorem and by partial integration,

$$\frac{d}{du_j}\hat{H}(u_j) = -2\pi i \int_{-\infty}^{\infty} w_j e^{-\pi w_j^2} e^{-2\pi i w_j u_j}\, dw_j = -2\pi u_j \hat{H}(u_j)\,.$$

Hence, $\hat{H}(u_j) = Ce^{-\pi u_j^2}$ for some constant C; and if we substitute $u_j = 0$, we obtain $C = \hat{H}(0) = \int_{-\infty}^{\infty} e^{-\pi w_j^2}\, dw_j = 1$. In this way,

$$\hat{h}(y) = \prod_{j=1}^{n} e^{-\pi u_j^2} = e^{-\pi(u,u)} = e^{-\pi\langle y,y\rangle}\,.$$

□

Theorem 3.15 (Poisson summation formula) *Let Γ be a complete lattice in $K_{\mathbb{R}}$ and Γ' its dual. Then for any Schwartz function f on $K_{\mathbb{R}}$:*

$$\sum_{g\in\Gamma} f(g) = \frac{1}{\mathrm{vol}(\Gamma)} \sum_{g'\in\Gamma'} \hat{f}(g')\,. \tag{12}$$

PROOF. After the identification of $K_{\mathbb{R}}$ with $\mathbb{R}^n$ (see Remark 3.13) this becomes a standard result in complex analysis. The interested reader will find a proof for example in [5, VII.(3.2)]. □

Definition 3.16 *For a complete lattice Γ in $K_{\mathbb{R}}$, we define the* ***theta series***

$$\theta_\Gamma(z) := \sum_{g\in\Gamma} e^{\pi i\langle gz,g\rangle}\,, \qquad z \in \mathbb{H}_K\,.$$

More generally, for $a, b \in K_{\mathbb{R}}$ and any ***admissible*** *$p \in \prod_\tau \mathbb{Z}_{\geq 0}$, i.e.,*

$$p = (p_\tau)_\tau,\ p_\tau \in \mathbb{Z}_{\geq 0} \qquad \textit{satisfies} \qquad \begin{cases} p_\tau \in \{0,1\} & \textit{if } \tau = \bar{\tau} \\ p_\tau p_{\bar{\tau}} = 0 & \textit{otherwise} \end{cases},$$

we put

$$\theta_\Gamma^p(a,b,z) := \sum_{g\in\Gamma} N((a+g)^p) e^{\pi i\langle (a+g)z, a+g\rangle + 2\pi i\langle b,g\rangle}\,.$$

Proposition 3.17 *The series $\theta^p_\Gamma(a, b, z)$ converges absolutely and uniformly on every compact subset of $K_\mathbb{R} \times K_\mathbb{R} \times \mathbb{H}_K$.*

Proof. Fix a positive $\delta \in \mathbb{R}_{>0}$. Then for all $z \in \mathbb{H}_K$ such that $\mathrm{Im}\,(z) \geq \delta$,

$$\sum_{g\in\Gamma} |N((a+g)^p) e^{\pi i\langle (a+g)z, a+g\rangle + 2\pi i \langle b, g\rangle}| \leq \sum_{g\in\Gamma} |N((a+g)^p)| e^{-\pi\delta\langle a+g, a+g\rangle} \,.$$

Further, fix a compact subset $\mathcal{C} \subseteq K_\mathbb{R}$ and let $M := \sup_{x\in\mathcal{C}} \|x\|$. We have to show that

$$\sum_{g\in\Gamma} \sup_{a\in\mathcal{C}} \{|N((a+g)^p)| e^{-\pi\delta\langle a+g, a+g\rangle}\} < \infty \,.$$

Let $g_1, \dots, g_n$ be a $\mathbb{Z}$-basis of Γ, write $g = \sum_{i=1}^n m_i^g g_i$ for some $m_i^g \in \mathbb{Z}$ and put $\mu_g = \max_i |m_i^g|$. Then for all $g \in \Gamma$ such that $\|g\| \geq 4M$ and for all $a \in \mathcal{C}$ we have

$$\begin{aligned}
\langle a+g, a+g\rangle = \|a+g\|^2 \geq (\|a\| - \|g\|)^2 &\geq \frac{1}{2}\|g\|^2 + \|g\| \left(\frac{1}{2}\|g\| - 2\|a\|\right) \\
&\geq \frac{1}{2}\|g\|^2 = \frac{1}{2}\sum_{i=1}^n m_i^g m_j^g \langle g_i, g_j\rangle \\
&= \frac{1}{2}\sum_{l=1}^n (m_l^g)^2 \cdot \sum_{i,j} \frac{m_i^g}{\sqrt{\sum_{l=1}^n (m_l^g)^2}} \frac{m_j^g}{\sqrt{\sum_{l=1}^n (m_l^g)^2}} \langle g_i, g_j\rangle \geq \frac{1}{2}\mu_g^2 \varepsilon \,,
\end{aligned}$$

where $\varepsilon := \inf_{\sum_i y_i^2 = 1} \{\sum_{i,j=1}^n y_i y_j \langle g_i, g_j\rangle\} > 0$ is the smallest eigenvalue of the matrix $[\langle g_i, g_j\rangle]_{i,j}$. (Indeed: Note that for $y = (y_1, \dots, y_n)$ with $\sum_i y_i^2 = 1$, the sum $\sum_{i,j=1}^n y_i y_j \langle g_i, g_j\rangle = \frac{yA\,{}^ty}{|y\,{}^ty|}$, where $A = [\langle g_i, g_j\rangle]_{i,j}$ as a Gram matrix is diagonalizable by some orthogonal matrix P. Hence, if we put $D := {}^tPAP$ and denote by $\lambda_1, \dots, \lambda_n$ the eigenvalues of A of which λ_{i_0} is the smallest, we obtain $\frac{yA\,{}^ty}{|y\,{}^ty|} = \frac{y(PD\,{}^tP)\,{}^ty}{|yP\,{}^t(yP)|} = \sum_{i=1}^n \lambda_i \tilde{y}_i^2 \geq \sum_{i=1}^n \lambda_{i_0} \tilde{y}_i^2 = \lambda_{i_0}$.)

Now, to bound the norm, observe that $N((a + \sum_{i=1}^n m_i^g g_i)^p)$ is a polynomial in the m_i^g of total degree $Tr(p)$ whose coefficients $b_0(a), \dots, b_r(a)$ (r depends only on p and n) are continuous functions of a. Hence, there exist $B_i := \sup_{a\in\mathcal{C}} b_i(a)$, $i = 0, \dots, r$ and $B := r \max_i B_i$, and thus

$$\sup_{a\in\mathcal{C}} |N((a+g)^p)| \leq B\mu_g^{Tr(p)} \,.$$

In this way,

$$\sum_{g\in\Gamma} \sup_{a\in\mathcal{C}} \{|N((a+g)^p)| e^{-\pi\delta\langle a+g, a+g\rangle}\} \leq C + \sum_{\|g\|\geq 4M} B\mu_g^{Tr(p)} e^{-\frac{\pi}{2}\delta\mu_g^2\varepsilon}$$

$$\leq C + \sum_{\mu=0}^{\infty} P(\mu) B \mu^{Tr(p)} e^{-\frac{\pi}{2}\delta\mu^2\varepsilon} < \infty \,,$$

where $P(\mu) := \#\{(m_1, \dots, m_n) \in \mathbb{Z}^n : \max_i |m_i| = \mu\} = (2\mu+1)^n - (2\mu-1)^n$ and C denotes the finite sum over $\|g\| < 4M$. □

Theorem 3.18 (Theta transformation formula) *For all $z \in \mathbb{H}_K$*

$$\theta^p_\Gamma\left(a, b, -\frac{1}{z}\right) = \left(i^{Tr(p)} e^{2\pi i\langle a,b\rangle} \mathrm{vol}(\Gamma)\right)^{-1} N\left(\left(\frac{z}{i}\right)^{p+1/2}\right) \theta^p_{\Gamma'}\left(-b, a, z\right) \,. \tag{13}$$

In particular, for the function $\theta_\Gamma(z) = \theta^0_\Gamma(0,0,z)$:

$$\theta_\Gamma\left(-\frac{1}{z}\right) = \frac{\sqrt{N(\frac{z}{i})}}{\mathrm{vol}(\Gamma)}\, \theta_{\Gamma'}\left(z\right) \,.$$

Proof. Note that both sides of the transformation formula are holomorphic functions in z, so by the identity theorem it suffices to check it for $z = iy$ with $y \in K^\times_{\mathbb{R},+}$. We put $t = \frac{1}{\sqrt{y}}$ so that $z = \frac{i}{t^2}$ and $-\frac{1}{z} = it^2$. Note also that since $t = t^* = {}^t t$, the multiplication by t is a self-adjoint operator. We obtain

$$\theta^p_\Gamma\left(a, b, -\frac{1}{z}\right) = N(t^{-p}) \sum_{g\in\Gamma} \underbrace{N((ta+tg)^p) e^{-\pi\langle ta+tg, ta+tg\rangle + 2\pi i\langle b/t, tg\rangle}}_{f_p(ta,\, b/t,\, tg)}$$

and similarly

$$\theta^p_\Gamma(-b, a, z) = N(t^p) \sum_{g'\in\Gamma'} f_p(-b/t, ta, g'/t) \,.$$

Now it suffices to apply the Poisson summation formula (12) to the function $f(g) = f_p(ta, b/t, tg)$. In order to do this we need the following lemma:

Lemma 3.19

(i) *If f is an arbitrary Schwartz function and A is a linear transformation of $K_\mathbb{R}$, then the function $f_A(x) := f(Ax)$ has Fourier transform*

$$\hat{f}_A(y) = \frac{1}{|\det A|}\, \hat{f}\left({}^t A^{-1} y\right) ,$$

where ${}^t A$ is the adjoint transformation of A.

(ii) *The function $f(x) := f_p(a,b,x) = N((a+x)^p) e^{-\pi\langle a+x, a+x\rangle + 2\pi i\langle b,x\rangle}$ is a Schwartz function on $K_\mathbb{R}$. If p is admissible, its Fourier transform is*

$$\hat{f}(y) = \left(i^{Tr(p)} e^{2\pi i\langle a,b\rangle}\right)^{-1} f_p(-b, a, y) \,. \tag{14}$$

We can combine the two statements of the Lemma to see that the Fourier transform of $f_t(x) = f_p(ta, b/t, tx)$ is $\hat{f}_t(y) = \left(i^{Tr(p)}N(t)e^{2\pi i\langle a,b\rangle}\right)^{-1} f_p(-b/t, ta, y/t)$. Once the Lemma is proved

$$\begin{aligned}\theta^p_\Gamma\left(a, b, -\frac{1}{z}\right) &= N(t^{-p})\sum_{g\in\Gamma} f_p(ta, b/t, tg) = N(t^{-p})\sum_{g\in\Gamma} f(g)\\ &\overset{(12),\text{ Lemma } 3.19}{=} \frac{1}{\mathrm{vol}(\Gamma)}N(t^{-p-1})\sum_{g'\in\Gamma'}\left(i^{Tr(p)}e^{2\pi i\langle a,b\rangle}\right)^{-1} f_p(-b/t, ta, g'/t)\\ &= \left(\mathrm{vol}(\Gamma)N(t^{2p+1})i^{Tr(p)}e^{2\pi i\langle a,b\rangle}\right)^{-1}\theta^p_\Gamma(-b, a, z)\,.\end{aligned}$$

□

Proof of Lemma 3.19.

(i) By Remark 3.13 we can apply standard results from Lebesgue integration:

$$\begin{aligned}\hat{f}_A(y) &= \int_{K_\mathbb{R}} f(Ax)e^{-2\pi i\langle x,y\rangle}\,dx \overset{x\mapsto A^{-1}x}{=\!=} \int_{K_\mathbb{R}} f(x)e^{-2\pi i\langle x,\,{}^tA^{-1}y\rangle}|\det A|^{-1}\,dx\\ &= \frac{1}{|\det A|}\hat{f}({}^tA^{-1}y)\,.\end{aligned}$$

(ii) It is clear that $f_p(a, b, x)$ is a Schwartz function because

$$|f_p(a, b, x)| = |N((x+a)^p)|e^{-\pi\langle a+x,a+x\rangle}\,,$$

where $N((x+a)^p)$ is a polynomial in x of degree $Tr(p)$. We compute first the Fourier transform of $f(x) = f_p(a, b, x)$ when $p = 0$. Note that then $f_0(a, b, x) = h(a+x)e^{2\pi i\langle b,x\rangle}$, where $\hat{h}(a+x) = h(a+x)$ by Example 3.14. Hence,

$$\begin{aligned}\hat{f}(y) &= \int_{K_\mathbb{R}} h(a+x)e^{-2\pi i\langle -b+y,x\rangle}\,dx\\ &\overset{x\mapsto -a+x}{=\!=} \int_{K_\mathbb{R}} h(x)e^{-2\pi i\langle -b+y,x\rangle}e^{2\pi i\langle -b+y,a\rangle}\,dx\\ &= e^{2\pi i\langle -b+y,a\rangle}\hat{h}(-b+y) = e^{-2\pi i\langle a,b\rangle}f_0(-b, a, y).\end{aligned}$$

We proceed by induction. Suppose we know (14) for an admissible p and we want to know it for the admissible $p' = p + \epsilon^\tau$, where $\epsilon^\tau_{\tau'} = \delta_{\tau,\tau'}$ for all τ'.

$$\langle a+x, a+x\rangle = \sum_{\rho=\overline{\rho}}(a_\rho + x_\rho)^2 + 2\sum_{\substack{\text{pairs }\{\sigma,\overline{\sigma}\}\\ \text{with }\sigma\neq\overline{\sigma}}}(a_\sigma + x_\sigma)(a_{\overline{\sigma}} + x_{\overline{\sigma}}),$$

so $\frac{\partial}{\partial a_{\bar\tau}}\langle a+x, a+x\rangle = 2(a_\tau + x_\tau)$. Using this we check

$$\begin{aligned}
\frac{\partial}{\partial a_{\bar\tau}} \widehat{f_p(a,b,y)} &= \frac{\partial}{\partial a_{\bar\tau}} \int_{K_\mathbb{R}} e^{-\pi\langle a+x,a+x\rangle + 2\pi i\langle b,x\rangle} N((x+a)^p) e^{-2\pi i\langle x,y\rangle} dx \\
&= -2\pi \int_{K_\mathbb{R}} e^{-\pi\langle a+x,a+x\rangle + 2\pi i\langle b,x\rangle} (x_\tau + a_\tau) N((x+a)^p) e^{-2\pi i\langle x,y\rangle} dx \\
&= -2\pi \widehat{f_{p'}(a,b,y)}.
\end{aligned}$$

Note that here we used that since both p and p' are assumed to be admissible we have $p_{\bar\tau} = 0$. On the other hand we can use (14) to see

$$\begin{aligned}
\frac{\partial}{\partial a_{\bar\tau}} \widehat{f_p(a,b,y)} &= i^{Tr(p)} \frac{\partial}{\partial a_{\bar\tau}} \left(e^{2\pi i\langle a,x-b\rangle} N((x-b)^p) e^{-\pi\langle -b+x,-b+x\rangle}\right) \\
&= i^{Tr(p)}(2\pi i)(x_\tau - b_\tau) N((x-b)^p) e^{-\pi\langle -b+x,-b+x\rangle} \\
&= (-2\pi) i^{Tr(p')} f_{p'}(-b,a,y).
\end{aligned}$$

□

4. The higher dimensional gamma function

Assume that the number field K has r_1 real embeddings and $2r_2$ complex embeddings, so that $n = r_1 + 2r_2$. We group them into r_1 real conjugation classes $\mathfrak{p} = \{\tau\}$ and r_2 complex conjugation classes $\mathfrak{p} = \{\tau, \bar\tau\}$, depending whether the embedding τ is real or complex. Hence, we can write

$$K_{\mathbb{R},+}^\times = \prod_{\mathfrak{p}} K_{\mathbb{R},+,\mathfrak{p}}^\times\,, \qquad \text{where} \qquad K_{\mathbb{R},+,\mathfrak{p}}^\times := \begin{cases} \mathbb{R}_+^\times\,, & \mathfrak{p} \text{ real} \\ \{(y,y) : y \in \mathbb{R}_+^\times\}\,, & \mathfrak{p} \text{ complex}\,. \end{cases}$$

Consider the isomorphism

$$\varphi : K_{\mathbb{R},+}^\times \xrightarrow{\sim} \prod_{\mathfrak{p}} \mathbb{R}_+^\times\,,$$

where

$$K_{\mathbb{R},+,\mathfrak{p}}^\times \xrightarrow{\sim} \mathbb{R}_+^\times \qquad \text{with} \qquad \begin{cases} y \mapsto y\,, & \mathfrak{p} \text{ real} \\ (y,y) \mapsto y^2\,, & \mathfrak{p} \text{ complex}\,. \end{cases}$$

We denote by $\frac{dy}{y}$ the Haar measure on $K_{\mathbb{R},+}^\times$, which via φ corresponds to the product measure $\prod_\mathfrak{p} \frac{dt}{t}$, where $\frac{dt}{t}$ is the usual (multiplicative) Haar measure on $\mathbb{R}_+^\times$. If we would further compose the map φ pointwise with the logarithm:

$$\mathfrak{p} \text{ real} : y_\mathfrak{p} \mapsto y_\mathfrak{p} \mapsto \log(y_\mathfrak{p})\,, \qquad \mathfrak{p} \text{ complex} : (y_\mathfrak{p}, y_\mathfrak{p}) \mapsto y_\mathfrak{p}^2 \mapsto 2\log(y_\mathfrak{p})\,,$$

the measure $\frac{dy}{y}$ would correspond to the Lebesgue measure on $\prod_\mathfrak{p} \mathbb{R}$.

Definition 3.20 *For a number field K and $s = (s_\tau)_\tau \in K_{\mathbb{C}}$ such that $\forall_\tau Re(s_\tau) > 0$, we define the* ***gamma function***

$$\Gamma_K(s) := \int_{K^\times_{\mathbb{R},+}} N(e^{-y}y^s)\,\frac{dy}{y}\,.$$

The gamma function $\Gamma_K(s)$ associated with a number field K is related to the usual Γ-function

$$\Gamma(s) = \int_0^\infty e^{-t}t^s\,\frac{dt}{t}\,, \qquad s \in \mathbb{C}$$

via the following formula.

Proposition 3.21 *For $s = \prod_{\mathfrak{p}} s_{\mathfrak{p}} \in K_{\mathbb{C}}$ such that $\forall_\tau Re(s_\tau) > 0$ with $s_{\mathfrak{p}} = s_\tau$ for $\mathfrak{p}$ real and $s_{\mathfrak{p}} = (s_\tau, s_{\bar\tau})$ for $\mathfrak{p}$ complex, we have*

$$\Gamma_K(s) = \prod_{\mathfrak{p}\ \mathit{real}} \Gamma(s_{\mathfrak{p}}) \times \prod_{\mathfrak{p}\ \mathit{complex}} 2^{1-Tr(s_{\mathfrak{p}})}\Gamma(Tr(s_{\mathfrak{p}}))\,,$$

where $Tr(s_{\mathfrak{p}}) := s_\tau + s_{\bar\tau}$.

Proof. Since $\frac{dy}{y} = \prod_{\mathfrak{p}} \frac{dy_{\mathfrak{p}}}{y_{\mathfrak{p}}}$ is a product measure over conjugation classes $\mathfrak{p}$ on $\prod_{\mathfrak{p}} K^\times_{\mathbb{R},+,\mathfrak{p}}$

$$\begin{aligned}\Gamma_K(s) &= \int_{K^\times_{\mathbb{R},+}} \prod_{\mathfrak{p}\ \text{real}} e^{-y_{\mathfrak{p}}}y_{\mathfrak{p}}^{s_{\mathfrak{p}}} \prod_{\mathfrak{p}=\{\sigma,\bar\sigma\}\ \text{complex}} e^{-2y_\sigma}y_\sigma^{s_\sigma+s_{\bar\sigma}}\,\frac{dy}{y}\\ &= \prod_{\mathfrak{p}\ \text{real}} \int_{\mathbb{R}^\times_+} e^{-y}y^{s_{\mathfrak{p}}}\frac{dy}{y} \times \prod_{\mathfrak{p}=\{\sigma,\bar\sigma\}\ \text{complex}} \int_{\mathbb{R}^\times_+} e^{-2t^{1/2}}t^{\frac{1}{2}Tr(s_{\mathfrak{p}})}\frac{dt}{t}\end{aligned}$$

The integrals corresponding to real places are $\Gamma(s_{\mathfrak{p}})$. The integrals corresponding to complex places are

$$\int_{\mathbb{R}^\times_+} e^{-2t^{1/2}}t^{\frac{1}{2}Tr(s_{\mathfrak{p}})}\frac{dt}{t} \overset{t\mapsto(t/2)^2}{=} 2^{1-Tr(s_{\mathfrak{p}})}\int_{\mathbb{R}^\times_+} e^{-t}t^s\frac{dt}{t} = 2^{1-Tr(s_{\mathfrak{p}})}\Gamma(Tr(s_{\mathfrak{p}})).$$

□

Corollary 3.22 $\Gamma_K(s)$ *inherits analytic properties from $\Gamma(s)$. In particular,*

1. *$\Gamma_K(s)$ converges for $s = (s_\tau)_\tau$ when $\forall_\tau Re(s_\tau) > 0$,*
2. *$\Gamma_K(s)$ admits a meromorphic continuation to $K_{\mathbb{C}}$ with poles at the points indicated by the Γ-function.*

Corollary 3.23 *If $s \in \mathbb{C}$, then*

$$\Gamma_K(s) := \Gamma_K(s(1,\ldots,1)) = 2^{(1-2s)r_2}\Gamma(s)^{r_1}\Gamma(2s)^{r_2}\,.$$

5. The Dedekind ζ-function and its meromorphic continuation

Definition 3.24 *The **Dedekind zeta function** of the number field K is defined by the series*

$$\zeta_K(s) = \sum_{0 \neq \mathfrak{a} \lhd \mathcal{O}_K} \frac{1}{\mathfrak{N}(\mathfrak{a})^s}\,,$$

where $\mathfrak{N}(\mathfrak{a}) := \#\left(\mathcal{O}_K/\mathfrak{a}\right)$ denotes the absolute norm of an ideal $\mathfrak{a}$.

Proposition 3.25 *The series $\zeta_K(s)$ converges absolutely and uniformly on compact subsets of the domain Re$(s) > 1$. Moreover,*

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

where $\mathfrak{p}$ runs through the prime ideals of K.

Proof. Exercise.[1] □

Recall that the set J_K of **fractional ideals** in K, i.e. the set of

$$\mathfrak{f} = (a_1, \ldots, a_m)\mathcal{O}_K := a_1\mathcal{O}_K + \ldots + a_m\mathcal{O}_K \;\; \text{where} \;\; a_1, \ldots, a_m \in K\backslash\{0\},\; m \in \mathrm{N}\,,$$

together with multiplication given by $\mathfrak{f}\mathfrak{g} = \{\sum_{i=1}^k a_i b_i : a_i \in \mathfrak{f}, b_i \in \mathfrak{g}, k \in \mathrm{N}\}$ forms a group with the identity element $\mathcal{O}_K$ and the inverse of $\mathfrak{f}$ given by

$$\mathfrak{f}^{-1} = \{x \in K : x\mathfrak{f} \subseteq \mathcal{O}_K\}\,.$$

Furthermore, we say that two fractional ideals $\mathfrak{f}$, $\mathfrak{g}$ are equivalent if there exists $0 \neq a \in K$ such that $\mathfrak{g} = (a)\mathfrak{f}$, i.e. $\mathfrak{f}$ and $\mathfrak{g}$ are equal up to multiplication by **principal fractional ideals**, denoted P_K. The equivalence classes are called **ideal classes**, the (finite) set $\mathrm{Cl}_K := J_K/P_K$ of ideal classes is the **ideal class group** of K, and $h_K = \#\mathrm{Cl}_K$ is the **class number** of K.

Observe that since every fractional ideal $\mathfrak{f}$ is of the form $\mathfrak{f} = \frac{1}{\delta}\mathfrak{a}$ for some $0 \neq \delta \in \mathcal{O}_K$ and $\mathfrak{a} \lhd \mathcal{O}_K$, each of the classes $\mathfrak{K}$ of Cl_K may be represented by an integral ideal, or - equivalently - by a fractional ideal $\mathfrak{a}^{-1}$ for some $0 \neq \mathfrak{a} \lhd \mathcal{O}_K$.

In order to study the properties of $\zeta_K(s)$ we split it into the partial zeta functions

$$\zeta(\mathfrak{K}, s) = \sum_{\substack{\mathfrak{a} \in \mathfrak{K} \\ \mathfrak{a} \lhd \mathcal{O}_K}} \frac{1}{\mathfrak{N}(\mathfrak{a})^s}$$

[1] Hint: adjust the proof for the Riemann zeta function to the current situation and use the fact that there are at most $[K : \mathbb{Q}]$ prime ideals lying above each prime number p.

according to the classes $\mathfrak{K}$, so that

$$\zeta_K(s) = \sum_{\mathfrak{K}\in \mathrm{Cl}_K} \zeta(\mathfrak{K}, s)\,.$$

Lemma 3.26 *Let $\mathfrak{a} \neq 0$ be an integral ideal of K and $\mathfrak{K} = \{\delta\mathfrak{a}^{-1} : \delta \in K^\times\}$ the class of the ideal $\mathfrak{a}^{-1}$. Then there is a bijection*

$$(\mathfrak{a}\setminus\{0\})/\mathcal{O}_K^\times \xrightarrow{\sim} \{\mathfrak{b} \in \mathfrak{K} : \mathfrak{b} \lhd \mathcal{O}_K\}\,, \quad a\mathcal{O}_K^\times \mapsto a\mathfrak{a}^{-1}\,.$$

Proof. First note that if $a \in \mathfrak{a}\setminus\{0\}$, then $a\mathfrak{a}^{-1} = (a)\mathfrak{a}^{-1}$ is indeed an integral ideal in $\mathfrak{K}$. Secondly, if $(a)\mathfrak{a}^{-1} = (b)\mathfrak{a}^{-1}$, then $(a) = (b)$ and thus $a\mathcal{O}_K^\times = b\mathcal{O}_K^\times$. Finally, every integral ideal $\mathfrak{b} \in \mathfrak{K}$ is of the form $\delta\mathfrak{a}^{-1}$ for some $\delta \in K^\times$ such that $\delta\mathfrak{a}^{-1} \subseteq \mathcal{O}_K$, which means that $\delta \in \mathfrak{a}\setminus\{0\}$. □

Corollary 3.27 *If $\mathfrak{K}$ is the class of an ideal $\mathfrak{a}^{-1}$ for some $\mathfrak{a} \lhd \mathcal{O}_K$, then*

$$\zeta(\mathfrak{K}, s) = \mathfrak{N}(\mathfrak{a})^s \sum_{\bar{a}\in(\mathfrak{a}\setminus\{0\})/\mathcal{O}_K^\times} \frac{1}{|N(j\bar{a})|^s}\,.$$

Proof. Recall that for $a \in K^\times$ we have equality of the norms:

$$\mathfrak{N}((a)) = |N_{K/\mathbb{Q}}(a)| = |N(ja)|\,.$$

By the above lemma, if a class $\mathfrak{K}$ contains $\mathfrak{a}^{-1}$ for some $\mathfrak{a} \lhd \mathcal{O}_K$, then every integral ideal in $\mathfrak{K}$ is of the form $a\mathfrak{a}^{-1}$ for some $a \in \mathfrak{a}$. Hence, its norm is equal to

$$\mathfrak{N}(a\mathfrak{a}^{-1}) = \frac{\mathfrak{N}((a))}{\mathfrak{N}(\mathfrak{a})} = \frac{|N(ja)|}{\mathfrak{N}(\mathfrak{a})}\,.$$

If a varies over the representatives of $(\mathfrak{a}\setminus\{0\})/\mathcal{O}_K^\times$, this correspondence is bijective. □

As it was the case for the Riemann zeta function, in order to find a functional equation for $\zeta(\mathfrak{K}, s)$, we will relate it first to a gamma function, and then to a Mellin transform of a theta series.

Recall that the gamma function associated to the space $K_\mathbb{R}$ is given by

$$\Gamma_K(s) = \int_{K^\times_{\mathbb{R},+}} N(e^{-y}y^s)\frac{dy}{y}\,, \qquad \mathrm{Re}\,(s) > 0.$$

We restrict to $s \in \mathbb{C}$. If we substitute $y \mapsto \pi|ja|^2 y/d_\mathfrak{a}^{1/n}$ with $a \in \mathfrak{a}\setminus\{0\}$, where $d_\mathfrak{a} = \mathfrak{N}(\mathfrak{a})^2|d_K|$ is a square of volume of a fundamental mesh of lattice $j\mathfrak{a}$ (see Lemma 3.8), then

$$\Gamma_K(s) = \int_{K^\times_{\mathbb{R},+}} N(e^{-\pi|ja|^2 y/d_\mathfrak{a}^{1/n}}) \left(\frac{\pi^n}{d_\mathfrak{a}}\right)^s N(|ja|)^{2s} N(y)^s \frac{dy}{y}$$

and thus by Remark 3.5

$$|d_K|^s \pi^{-ns}\Gamma_K(s)\left(\frac{\mathfrak{N}(\mathfrak{a})}{N(|ja|)}\right)^{2s} = \int_{K^\times_{\mathbb{R},+}} e^{-\pi\langle yja/d_{\mathfrak{a}}^{1/n}, ja\rangle} N(y)^s \frac{dy}{y}\,.$$

For an ideal $\mathfrak{a}$ as in Corollary 3.27, summing the above over all representatives a of $(\mathfrak{a}\setminus\{0\})/\mathcal{O}_K^\times$, we obtain (note the absolute convergence of the integral on the right for $\mathrm{Re}\,(s) > 0$)

$$|d_K|^s \pi^{-ns}\Gamma_K(s)\zeta(\mathfrak{K}, 2s) = \int_{K^\times_{\mathbb{R},+}} g(y) N(y)^s \frac{dy}{y}\,,$$

where $g(y) = \sum_{a\in(\mathfrak{a}\setminus\{0\})/\mathcal{O}_K^\times} e^{-\pi\langle yja/d_{\mathfrak{a}}^{1/n}, ja\rangle}$. This provides a formula for the **completed partial zeta function**

$$Z(\mathfrak{K}, s) := Z_\infty(s)\zeta(\mathfrak{K}, s) \qquad \text{where} \qquad Z_\infty(s) := |d_K|^{s/2}\pi^{-ns/2}\Gamma_K(s/2)\,.$$

Note that $g(y)$ is almost the theta series we were looking for: the sum should be over all $a \in \mathfrak{a}$. We remedy this by a suitable decomposition of the space $K^\times_{\mathbb{R},+}$.

Consider the sequence of maps:

$$\mathcal{O}_K^\times \xrightarrow{j} j\mathcal{O}_K^\times \xrightarrow{|\ |} \underbrace{\{x \in K^\times_{\mathbb{R},+} : N(x) = 1\}}_{S} \xrightarrow{\log} \underbrace{\{x \in K_{\mathbb{R},\pm} : Tr(x) = 0\}}_{H}$$

Clearly the roots of unity in K, denoted by $\mu(K)$ are in the kernel of $|\cdot|\circ j$. The converse is also true.

Lemma 3.28 (Kummer) *Let G be the image of $\mathcal{O}_K^\times$ in H under $\lambda = \log\circ|\cdot|\circ j$. Then the sequence*

$$1 \to \mu(K) \to \mathcal{O}_K^\times \xrightarrow{\lambda} G \to 0$$

is exact.

Theorem 3.29 (Dirichlet's Unit Theorem, Theorem 7.4 in [5], chapter I)

(1) *G is a complete lattice in H.*

(2) *By Kummer's lemma, $\mathcal{O}_K^\times$ is the direct product of the finite group $\mu(K)$ and a free abelian group of rank $r-1$, where $r = r_1 + r_2$ is equal to the number of conjugacy classes of embeddings $K \hookrightarrow \mathbb{C}$.*
More precisely, there exist $\varepsilon_1, \ldots, \varepsilon_{r-1} \in \mathcal{O}_K^\times$, called ***fundamental units****, such that any $\varepsilon \in \mathcal{O}_K^\times$ can be written uniquely as a product $\varepsilon = \xi\varepsilon_1^{\nu_1}\cdot\ldots\cdot\varepsilon_{r-1}^{\nu_{r-1}}$, where $\xi \in \mu(K)$ and $\nu_1, \ldots, \nu_{r-1} \in \mathbb{Z}$.*

Note that every element $y \in K^\times_{\mathbb{R},+}$ may be written as

$$y = \frac{y}{N(y)^{1/n}} t^{1/n} = \left(\frac{y}{N(y)^{1/n}} t^{1/n}\right)_\tau \quad \text{where } t = N(y),\ N\left(\frac{y}{N(y)^{1/n}}\right) = 1.$$

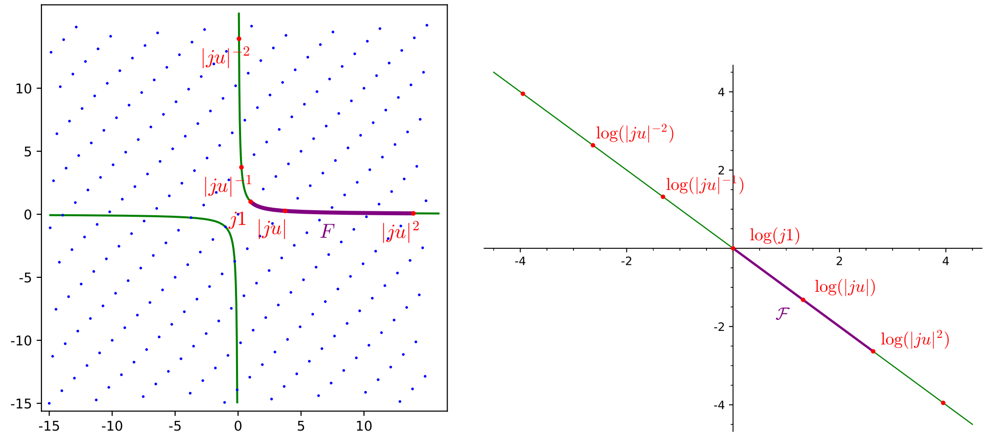

FIGURE 1. Fundamental meshes F and $\mathcal{F}$ for $K = \mathbb{Q}(\sqrt{3})$: In the left picture $\mathcal{O}_K$ is represented by blue dots and S is in green. In the right picture H is in green and the red dots represent G. A fundamental unit of $\mathbb{Q}(\sqrt{3})$ is given by $u = -\sqrt{3} + 2$.

Hence, $K^\times_{\mathbb{R},+} = S \times \mathbb{R}^\times_+$. Similarly, the canonical Haar measure $\frac{dy}{y}$ on $K^\times_{\mathbb{R},+}$ induces the unique Haar measure $d^\times x$ on S such that

$$\frac{dy}{y} = d^\times x \times \frac{dt}{t}\,.$$

Furthermore, by Dirichlet's Unit Theorem, the group $G := (\log \circ |\ | \circ j)(\mathcal{O}_K^\times)$ is a complete lattice in H. This is also the case for $2G = \log |j\mathcal{O}_K^\times|^2$. Hence, if we denote by $\mathcal{F}$ a fundamental mesh of the lattice $2G$, and by F its preimage under log, then $H = \sqcup_{\gamma \in 2G}(\gamma + \mathcal{F})$, and thus $S = \sqcup_{\eta \in |j\mathcal{O}_K^\times|} \eta^2 F$.

Proposition 3.30 *The function $Z(\mathfrak{K}, 2s)$ is the Mellin transform of the function $f(t) - \lim_{y\to\infty} f(y)$, where*

$$f(t) = f_F(\mathfrak{a}, t) = \frac{1}{w} \int_F \theta_{j\mathfrak{a}} \left(\frac{ixt^{1/n}}{d_{\mathfrak{a}}^{1/n}} \right) d^\times x \tag{15}$$

and $w = \#\mu(K)$ denotes the number of roots of unity in K.

PROOF. Set

$$\theta(\mathfrak{a}, ixt^{1/n}) := \theta_{j\mathfrak{a}} \left(\frac{ixt^{1/n}}{d_{\mathfrak{a}}^{1/n}} \right). \tag{16}$$

With the notation as above and putting $t' := (t/d_{\mathfrak{a}})^{1/n}$, we have

$$\begin{aligned}
Z(\mathfrak{K}, 2s) &= \int_0^\infty \int_S \sum_{a \in (\mathfrak{a} \setminus \{0\})/\mathcal{O}_K^\times} e^{-\pi \langle x t' ja, ja \rangle} t^s d^\times x \frac{dt}{t} \\
&= \int_0^\infty \sum_{\eta \in |j\mathcal{O}_K^\times|} \int_{\eta^2 F} \sum_{a \in (\mathfrak{a} \setminus \{0\})/\mathcal{O}_K^\times} e^{-\pi \langle x t' ja, ja \rangle} d^\times x \, t^s \frac{dt}{t} \\
&\overset{(\star)}{=} \int_0^\infty \frac{1}{w} \sum_{\varepsilon \in j\mathcal{O}_K^\times} \int_F \sum_{a \in (\mathfrak{a} \setminus \{0\})/\mathcal{O}_K^\times} e^{-\pi \langle \varepsilon x t' ja, \varepsilon ja \rangle} d^\times x \, t^s \frac{dt}{t} \\
&= \int_0^\infty \frac{1}{w} \int_F (\theta(\mathfrak{a}, ixt^{1/n}) - 1) d^\times x \, t^s \frac{dt}{t} \\
&\overset{(\star\star)}{=} \int_0^\infty (f(t) - f(\infty)) t^s \frac{dt}{t} \,,
\end{aligned}$$

where the equality $(\star)$ follows from the fact that $\mu(K)$ is the kernel of $\mathcal{O}_K^\times \to |\mathcal{O}_K^\times|$, and $(\star\star)$ is a result of

$$\lim_{t \to \infty} f(t) = \lim_{t \to \infty} \frac{1}{w} \int_F \theta(\mathfrak{a}, ixt^{1/n}) d^\times x = \frac{1}{w} \int_F d^\times x \,.$$

□

The functional equation for $Z(\mathfrak{K}, S)$ will follow from the Mellin principle (Theorem 2.9) once we establish a transformation formula for the function $f_F(\mathfrak{a}, t)$ defined above. Recall also that the constant occurring in the functional equation is related to the value $f_F(\mathfrak{a}, \infty)$, which here equals $\frac{1}{w} \int_F d^\times x$. We compute first the volume of F.

Definition 3.31 *Let $\varepsilon_1, \ldots, \varepsilon_{r-1}$ be fundamental units of K, $r = r_1 + r_2$, and $\lambda = (\lambda_1, \ldots, \lambda_r) := \varphi' \circ \log \circ j : \mathcal{O}_K^\times \to \mathbb{R}^r$, where*

$$\varphi' : K_{\mathbb{R},\pm} = \prod_{\mathfrak{p}} K_{\mathbb{R},\pm,\mathfrak{p}} \longrightarrow \prod_{\mathfrak{p}} \mathbb{R} \,, \qquad \begin{cases} x \mapsto x \,, & \mathfrak{p} \text{ real} \\ (x, x) \mapsto 2x \,, & \mathfrak{p} \text{ complex} \,. \end{cases}$$

*The **regulator** of the field K is the absolute value of the determinant of an arbitrary minor of rank $r-1$ of the matrix*

$$\begin{pmatrix} \lambda_1(\varepsilon_1) & \cdots & \lambda_1(\varepsilon_{r-1}) \\ \vdots & & \vdots \\ \lambda_r(\varepsilon_1) & \cdots & \lambda_r(\varepsilon_{r-1}) \end{pmatrix} .$$

Lemma 3.32 *The fundamental domain F of S has volume*

$$\mathrm{vol}(F) = \int_F d^\times x = 2^{r-1} R\,,$$

where $r = r_1 + r_2$ is the number of infinite places and R is the regulator of K.

Proof. Consider the following sequence of mappings:

$$\begin{tikzcd}
S \times \mathbb{R}_+^\times \arrow[r, "\alpha"] & K_{\mathbb{R},+}^\times \arrow[r, "\log"] & K_{\mathbb{R},\pm} \arrow[r, "\varphi'"] & \prod_{\mathfrak{p}|\infty} \mathbb{R} = \mathbb{R}^r \\
(x,t) \arrow[r, mapsto] & xt^{1/n} \arrow[r, mapsto] & \log(x) + \left(\frac{1}{n}\log(t)\right)_\tau &
\end{tikzcd}$$

where φ' is as above. Note that $\varphi' \circ \log = \log \circ \varphi$, where φ is as in section 4; so the measure $\frac{dy}{y} = d^\times x \times \frac{dt}{t}$ on $K_{\mathbb{R},+}^\times$ corresponds to the Lebesgue measure on $\prod_{\mathfrak{p}} \mathbb{R}$.

To compute the volume of F in S we compute instead the volume of $F \times I$ in $S \times \mathbb{R}_+^\times$, where $I \subseteq \mathbb{R}_+^\times$ is of measure 1 with respect to $\frac{dt}{t}$, i.e., $\int_I \frac{dt}{t} = 1$. We choose $I = \{t \in \mathbb{R}_+^\times : 1 \leq t \leq e\}$. Then

$$\mathrm{vol}(F) = \int_F d^\times x = \int_F d^\times x \int_I \frac{dt}{t} = \mathrm{vol}(F \times I) = \mathrm{vol}\left(\alpha(F \times I)\right) .$$

Furthermore,

$$\log\left(\alpha(F \times I)\right) = \{\log(x) + \left(\frac{1}{n}\log(t)\right)_\tau : x \in F, t \in [1,e]\} = \mathcal{F} + \left(\frac{1}{n}[0,1]\right)_\tau \subseteq K_{\mathbb{R},\pm}\,.$$

Now recall that $\mathcal{F}$ is a a fundamental mesh of the lattice $2\log|j\mathcal{O}_K^\times| \subseteq H$ and that every $\varepsilon \in \mathcal{O}_K^\times$ may be written uniquely as $\varepsilon = \xi\varepsilon_1^{\nu_1} \cdot \ldots \cdot \varepsilon_{r-1}^{\nu_{r-1}}$, where $\xi \in \mu(K)$. Hence, if $\lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_{r-1}) \in \mathbb{R}^r$ are the images of fundamental units $\varepsilon_1, \ldots, \varepsilon_{r-1} \in \mathcal{O}_K^\times$ via the map $\lambda = \varphi' \circ \log \circ |\ \ | \circ j$, then $\varphi'(\mathcal{F})$ is the parallelepiped spanned by $2\lambda(\varepsilon_1), \ldots, 2\lambda(\varepsilon_{r-1})$. If $\mathfrak{e} = \varphi'((1,\ldots,1)) = (\mathfrak{e}_1, \ldots, \mathfrak{e}_r) \in \mathbb{R}^r$, then $\varphi'(\mathcal{F} + \left(\frac{1}{n}[0,1]\right)_\tau)$ is the parallelepiped spanned by $2\lambda(\varepsilon_1), \ldots, 2\lambda(\varepsilon_{r-1})$ and $\frac{1}{n}\mathfrak{e}$. Hence,

$$\mathrm{vol}(F) = \mathrm{vol}(\varphi'(\mathcal{F} + \left(\frac{1}{n}[0,1]\right)_\tau)) = \frac{1}{n}2^{r-1}|\det\begin{pmatrix} \lambda_1(\varepsilon_1) & \cdots & \lambda_1(\varepsilon_{r-1}) & \mathfrak{e}_1 \\ \vdots & & \vdots & \vdots \\ \lambda_r(\varepsilon_1) & \cdots & \lambda_r(\varepsilon_{r-1}) & \mathfrak{e}_r \end{pmatrix}|\,.$$

If we add the first $r-1$ lines to the last one, all entries of the last line become zero, except the last one, which is $\sum_{i=1}^r \mathfrak{e}_i = r_1 + 2r_2 = n$. The matrix above these zeros has the absolute value of its determinant equal to the regulator R. In this way, $\mathrm{vol}(F) = 2^{r-1}R$. □

Proposition 3.33 *The functions $f_F(\mathfrak{a},t)$ satisfy the transformation formula*

$$f_F\left(\mathfrak{a},\frac{1}{t}\right)=t^{1/2}f_{F^{-1}}\left((\mathfrak{a}\mathfrak{d})^{-1},t\right)\,.$$

Moreover,

$$f_F(\mathfrak{a},t)=\frac{2^{r-1}}{w}R+O(e^{-ct^{1/n}})\qquad\textit{for } t\to\infty,\ c>0\,.$$

Proof. In order to prove the first statement we will use the transformation formula (13) for the theta function $\theta(\mathfrak{a},z):=\theta_{j\mathfrak{a}}\left(\frac{z}{d_{\mathfrak{a}}^{1/n}}\right)$, where - recall - $\mathrm{vol}(j\mathfrak{a})=\sqrt{d_{\mathfrak{a}}}$. Recall also from Example 3.10 that the lattice dual to $j\mathfrak{a}$ is given by ${}^*j\left((\mathfrak{a}\mathfrak{d})^{-1}\right)$ and note that $\theta_{{}^*j((\mathfrak{a}\mathfrak{d})^{-1})}(z)=\theta_{j((\mathfrak{a}\mathfrak{d})^{-1})}(z)$ by the compatibility $\langle {}^*gz,{}^*g\rangle=\langle gz,g\rangle$.

Since, in the same way as $x\mapsto -x$ fixes a Haar measure on $\mathbb{R}^n$, the transformation $x\mapsto x^{-1}$ fixes the Haar measure $d^\times x$ on S and maps the fundamental domain F onto the fundamental domain F^{-1}, whose image $\log(F^{-1})$ is again a fundamental mesh of the lattice $2\log|\mathcal{O}_K^\times|$, we have

$$\begin{aligned}
f_F\left(\mathfrak{a},\frac{1}{t}\right)&=\frac{1}{w}\int_F\theta_{j\mathfrak{a}}\left(\frac{ix}{\sqrt[n]{td_{\mathfrak{a}}}}\right)\,d^\times x\overset{x\mapsto x^{-1}}{=\!=\!=}\frac{1}{w}\int_{F^{-1}}\theta_{j\mathfrak{a}}\left(\frac{-1}{ix\sqrt[n]{td_{\mathfrak{a}}}}\right)\,d^\times x\\
&\overset{(13)}{=}\frac{\sqrt{td_{\mathfrak{a}}}}{w\cdot\mathrm{vol}(j\mathfrak{a})}\int_{F^{-1}}\theta_{j((\mathfrak{a}\mathfrak{d})^{-1})}(ix\sqrt[n]{td_{\mathfrak{a}}})\,d^\times x\\
&=\frac{\sqrt{t}}{w}\int_{F^{-1}}\theta_{j((\mathfrak{a}\mathfrak{d})^{-1})}(ix\sqrt[n]{t/d_{(\mathfrak{a}\mathfrak{d})^{-1}}})\,d^\times x\\
&=t^{1/2}f_F\left((\mathfrak{a}\mathfrak{d})^{-1},t\right)\,,
\end{aligned}$$

where we have used the fact that $d_{(\mathfrak{a}\mathfrak{d})^{-1}}=\mathfrak{N}(\mathfrak{a}\mathfrak{d})^{-2}d_K$ (see Lemma 3.8) and that $\mathfrak{N}(\mathfrak{d})=N_{K/\mathbb{Q}}(\mathfrak{d})=d_K$ (see [5, III.(2.9)]).

To prove the second formula, we write

$$f_F\left(\mathfrak{a},t\right)=\frac{1}{w}\int_F d^\times x+\frac{1}{w}\int_F\theta(\mathfrak{a},ixt^{1/n})-1\,d^\times x\overset{\text{Lemma 3.32}}{=}\frac{2^{r-1}R}{w}+r(t)\,,$$

where we set $r(t):=\frac{1}{w}\int_F\left(\theta(\mathfrak{a},ixt^{1/n})-1\right)\,d^\times x$. Note that all the summands of $\theta(\mathfrak{a},ixt^{1/n})-1$ are of the form $e^{-\pi\langle xja,ja\rangle(t/d_{\mathfrak{a}})^{1/n}}$ with $a\in\mathfrak{a}$, $a\neq 0$. Further, since $x=(x_\tau)_\tau\in\bar{F}\subseteq K_{\mathbb{R},+}^\times$ varies in the compact closure of F, so there exists $\delta>0$ such that for all $x\in\bar{F}$ and for all τ we have $x_\tau\geq\delta$. Hence,

$$\langle xja,ja\rangle=\sum_\tau x_\tau|\tau(a)|^2\geq\delta\langle a,a\rangle\,,$$

and thus

$$r(t) = \frac{1}{w}\int_F \left(\sum_{a\in\mathfrak{a}} e^{-\pi\langle xja,ja\rangle \sqrt[n]{t/d_\mathfrak{a}}} - 1\right) d^\times x \le \left(\theta_{j\mathfrak{a}}(i\delta\sqrt[n]{t/d_\mathfrak{a}}) - 1\right)\frac{\mathrm{vol}(F)}{w}\,.$$

Further, if we set $m := \min\{\langle ja,ja\rangle : 0 \neq a \in \mathfrak{a}\}$ and $M := \#\{a \in \mathfrak{a} : \langle ja,ja\rangle = m\}$, we obtain

$$\theta_{j\mathfrak{a}}(i\delta\sqrt[n]{t/d_\mathfrak{a}}) - 1 = e^{-\pi\delta m\sqrt[n]{t/d_\mathfrak{a}}}\left(M + \sum_{\langle ja,ja\rangle > m} e^{-\pi\delta(\langle ja,ja\rangle - m)\sqrt[n]{t/d_\mathfrak{a}}}\right) = O\left(e^{-ct^{1/n}}\right)\,,$$

where $c = \frac{\pi\delta m}{d_\mathfrak{a}^{1/n}}$. In this way,

$$f_F(\mathfrak{a},t) = \frac{2^{r-1}R}{w} + O\left(e^{-ct^{1/n}}\right) \qquad \text{as } t \to \infty\,.$$

□

Now the Mellin principle (Theorem 2.9) together with Propositions 3.30, 3.33 prove immediately the sought properties of the completed partial zeta function $Z(\mathfrak{K},s)$ and, as a consequence, of the completed zeta function of the number field K,

$$Z_K(s) := Z_\infty(s)\zeta_K(s) = \sum_{\mathfrak{K}} Z(\mathfrak{K},s)\,.$$

Theorem 3.34 *The function*

$$Z(\mathfrak{K},s) = Z_\infty(s)\zeta(\mathfrak{K},s)\,, \qquad Re(s) > 1,$$

with $Z_\infty(s) = |d_K|^{s/2}\pi^{-ns/2}\Gamma_K(s/2)$, admits an analytic continuation to $\mathbb{C}\backslash\{0,1\}$ and satisfies the functional equation

$$Z(\mathfrak{K},s) = Z(\mathfrak{K}',1-s)\,,$$

where the ideal classes $\mathfrak{K}$ and $\mathfrak{K}'$ correspond to each other via $\mathfrak{K}\mathfrak{K}' = [\mathfrak{d}]$. It has simple poles at $s = 0$ and $s = 1$ with residues $-\frac{2^r}{w}R$ and $\frac{2^r}{w}R$ respectively.

Proof. Let $f(t) = f_F(\mathfrak{a},t)$ and $g(t) = f_{F^{-1}}((\mathfrak{a}\mathfrak{d})^{-1},t)$. By Propositions 3.30, 3.33, $Z(\mathfrak{K},2s)$ is a Mellin transform of the function $f(t) - \frac{2^{r-1}}{w}R$ which satisfies the transformation formula

$$f\left(\frac{1}{t}\right) = t^{1/2}g(t)$$

with

$$f(t) = \frac{2^{r-1}}{w}R + O\left(e^{-ct^{1/n}}\right) \qquad \text{and} \qquad g(t) = \frac{2^{r-1}}{w}R + O\left(e^{-ct^{1/n}}\right)\,.$$

Hence, by Theorem 2.9, $Z(\mathfrak{K},2s)=\mathcal{M}(f(t)-\frac{2^{r-1}}{w}R,s)$ admits an analytic continuation to $s\in\mathbb{C}\backslash\{0,\frac{1}{2}\}$ with simple poles at $s=0$ and $s=\frac{1}{2}$ with residues $-\frac{2^{r-1}}{w}R$ and $\frac{2^{r-1}}{w}R$ respectively, and satisfies the functional equation

$$Z(\mathfrak{K},2s)=\mathcal{M}\left(f(t)-\frac{2^{r-1}}{w}R,s\right)=\mathcal{M}\left(g(t)-\frac{2^{r-1}}{w}R,\frac{1}{2}-s\right)=Z(\mathfrak{K}',1-2s)\,,$$

where $\mathfrak{K}'\in Cl_K$ is the class of the ideal $\mathfrak{ad}$.

Therefore $Z(\mathfrak{K},s)$ admits an analytic continuation to $\mathbb{C}\backslash\{0,1\}$ with simple poles at $s=0$ and $s=1$, residues $-\frac{2^r}{w}R$ and $\frac{2^r}{w}R$ respectively, and satisfies the functional equation

$$Z(\mathfrak{K},s)=Z(\mathfrak{K}',1-s)\,.$$

□

Corollary 3.35 *The completed zeta function $Z_K(s)$ admits an analytic continuation to $\mathbb{C}\backslash\{0,1\}$ and satisfies the functional equation*

$$Z_K(s)=Z_K(1-s)$$

It has simple poles at $s=0$ and $s=1$ with residues $-\frac{2^rhR}{w}$ and $\frac{2^rhR}{w}$ respectively, where h is the class number of K.

An explicit formula for $Z_\infty(s)$ together with Corollary 3.35 allows us also to derive analytic properties of the Dedekind zeta function.

Corollary 3.36

(i) *The Dedekind zeta function $\zeta_K(s)$ has an analytic continuation to $\mathbb{C}\backslash\{1\}$.*

(ii) *At $s=1$ it has a simple pole with residue*

$$\mathrm{Res}_{s=1}\zeta_K(s)=\frac{2^{r_1}(2\pi)^{r_2}}{w|d_K|^{1/2}}hR\,, \tag{17}$$

where h denotes the class number, R the regulator of K, d_K the discriminant and $r_1,2r_2$ are the numbers of real and complex embeddings, respectively.

(iii) *It satisfies the functional equation*

$$\zeta_K(1-s)=A(s)\zeta_K(s)$$

with the factor

$$A(s)=|d_K|^{s-1/2}\left(\cos\frac{\pi s}{2}\right)^{r_1+r_2}\left(\sin\frac{\pi s}{2}\right)^{r_2}\left(2(2\pi)^{-s}\Gamma(s)\right)^{r_1}\,.$$

Proof.

(i) $\zeta_K(s) = Z_\infty^{-1}(s) Z_K(s)$, where $Z_K(s)$ has a simple pole at $s=0$ and $s=1$, and where

$$Z_\infty^{-1}(s) = |d_K|^{-s/2} \pi^{ns/2} 2^{(s-1)r_2} \Gamma\left(\frac{s}{2}\right)^{-r_1} \Gamma(s)^{-r_2}$$

has a zero at $s=0$ as $\Gamma(s)$ has a pole there, and

$$Z_\infty^{-1}(1) = |d_K|^{-1/2} \pi^{r_2+r_1/2} \Gamma\left(\frac{1}{2}\right)^{-r_1} = |d_K|^{-1/2} \pi^{r_2} .$$

(ii) $\mathrm{Res}_{s=1} \zeta_K(s) = Z_\infty^{-1}(1) \mathrm{Res}_{s=1} Z_K(s) \overset{\text{Cor. } 3.35}{=} \frac{2^{r_1}(2\pi)^{r_2}}{w|d_K|^{1/2}} hR$.

(iii) The factor $A(s) = \frac{Z_\infty(1-s)}{Z_\infty(s)}$ may be simplified to the form above by applying the basic properties of the Gamma function listed in Lemma 2.10.

□

The identity (17) is known as the analytic ***class number formula***. It may be used to compute the class number h of those number fields K where one knows the decomposition of prime numbers sufficiently well to be able to use an Euler product for $\zeta_K(s)$.

It turns out that properties of a single Dedekind zeta function may be used to derive information on *all* Dirichlet L-functions. This is, again, possible thanks to an Euler product and a fairly good knowledge on splitting of primes in that extension. As a result we will obtain a proof of the previously announced Dirichlet's theorem on primes in arithmetic progression.

First we recall an important fact concerning characters on finite groups.

Theorem 3.37 (Orthogonality relations) *Let G be a finite abelian group and denote by $G^* := Hom(G, \mathbb{C}^\times)$ a group of characters on G. Denote their neutral elements by 1_G and χ_0 respectively. Then for $g \in G$ and $\chi \in G^*$:*

$$\sum_{g \in G} \chi(g) = \begin{cases} \#G, & \chi = \chi_0 \\ 0, & \textit{otherwise} \end{cases} \quad \textit{and} \quad \sum_{\chi \in G^*} \chi(g) = \begin{cases} \#G, & g = 1_G \\ 0, & \textit{otherwise.} \end{cases}$$

Proof. For the first relation, if $\chi \neq \chi_0$, choose $y \in G$ such that $\chi(y) \neq 1$. Then

$$\sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(yg) = \chi(y) \sum_{g \in G} \chi(g) ,$$

and thus $\sum_{g \in G} \chi(g) = 0$. The case $\chi = \chi_0$ is obvious.

To prove the second relation we use the facts, which we leave as an exercise, that $G \cong G^*$[2] and that the map

$$\alpha : G \longrightarrow (G^*)^*\,, \qquad \alpha(g) : \chi \mapsto \chi(g)$$

is an isomorphism. Then:

$$\sum_{\chi\in G^*} \chi(g) = \sum_{\chi \in G^*} (\alpha(g))(\chi) = \begin{cases} \#G^*, & \alpha(g) \text{ trivial} \\ 0, & \text{otherwise} \end{cases} = \begin{cases} \#G, & g = 1_G \\ 0, & \text{otherwise.} \end{cases}$$

□

Proposition 3.38 *If $K = \mathbb{Q}(\mu_m)$ is the field of m-th roots of unity, then for $\mathrm{Re}\, s > 1$*

$$\zeta_K(s) = \prod_{\mathfrak{p}|m} \frac{1}{1-\mathfrak{N}(\mathfrak{p})^{-s}} \prod_{\chi \bmod m} L(\chi, s)\,,$$

where χ varies over all Dirichlet characters mod m and

$$L(\chi, s) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p\in\mathbb{P}} \frac{1}{1-\chi(p)p^{-s}}$$

is a Dirichlet series.

Proof. Recall that $\zeta_K(s) = \prod_{\mathfrak{p}} (1-\mathfrak{N}(\mathfrak{p})^{-s})^{-1}$, $\mathrm{Re}\,(s) > 1$. Since $K = \mathbb{Q}(\mu_m)$ is a Galois extension of $\mathbb{Q}$ of degree $\varphi(m)$ (where $\varphi(m)$ denotes the Euler function), every prime number p has a decomposition in K of the form $p = (\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r)^e$ with $\mathfrak{N}(\mathfrak{p}_i) = f$ for all i, and such that $efr = \varphi(m)$. Hence, $\zeta_K(s)$ is a product of factors

$$\prod_{\mathfrak{p}|p} \left(1-\mathfrak{N}(\mathfrak{p})^{-s}\right)^{-1} = \left(1-p^{-fs}\right)^{-r}.$$

On the other hand, the product of the Dirichlet series over χ gives the factor $\prod_\chi (1-\chi(p)p^{-s})^{-1}$ (see Remark 2.2). Since we vary over the characters modulo m, this product is 1 for all $p|m$.

Assume that $p \nmid m$ and fix the corresponding e, f, r. It suffices to show that $\prod_\chi (1-\chi(p)p^{-s}) = \left(1-p^{-fs}\right)^r$, i.e. that splitting of the polynomial $1-p^{-fs}$ in $\mathbb{Q}(\mu_m)$ is governed by the characters modulo m. By [5, I.(10.3)], we know a precise splitting behaviour of primes in cyclotomic fields $\mathbb{Q}(\mu_m)$:

$$m = \prod_p p^{\nu_p} \quad \Rightarrow \quad p = (\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r)^{\varphi(p^{\nu_p})} \text{ and } p^f \equiv 1 \bmod \frac{m}{p^{\nu_p}}$$

[2] Use the fundamental theorem of finite abelian groups and observe that for a cyclic group G of order m, $G^* \cong \{e^{2\pi i a/m} : a = 1, \ldots, m\} \cong G$.

(and f is the smallest positive integer with such a property). Hence, since $p \nmid m$, $e = \varphi(1) = 1$ and thus

$$r = \frac{\varphi(m)}{f} = \# \left(\underbrace{(\mathbb{Z}/m\mathbb{Z})^\times}_{G} / \underbrace{\{p^x : x \in \mathbb{Z}\}}_{G_p} \right) .$$

This is exactly the number of characters $\chi \in G^*$ modulo m which are trivial on G_p. Indeed, observe that the map $\chi \mapsto \chi(p)$ defines an isomorphism between G_p^* and the group μ_f of f-th roots of unity; this yields an exact sequence

$$1 \longrightarrow (G/G_p)^* \longrightarrow G^* \xrightarrow{\chi \mapsto \chi(p)} \mu_f \longrightarrow 1 ,$$

Hence, $\# (G/G_p)^* = \frac{\# G^*}{\# \mu_f} = r$ and

$$\prod_{\chi} \left(1 - \chi(p) p^{-s}\right) = \prod_{\zeta \in \mu_f} \left(1 - \zeta p^{-s}\right)^r = \left(1 - p^{-fs}\right)^r .$$

□

Note that by Theorem 1.6, if χ is a non-trivial Dirichlet character modulo m, the series $L(\chi, s)$ converges and defines a holomorphic function on the halfplane $\operatorname{Re} s > 0$. Indeed, by Theorem 3.37, the partial sums $\sum_{n=M}^{N} a_n$ are bounded by m.

Corollary 3.39 *For a non-trivial Dirichlet character χ,*

$$L(\chi, 1) \neq 0 .$$

Proof. Denote by m the modulus of the character χ and let χ_0 be the trivial character mod m. Note that

$$L(\chi_0, s) = \prod_{p \nmid m} \frac{1}{1 - p^{-s}} = \zeta(s) \prod_{p \mid m} \left(1 - p^{-s}\right) .$$

Hence, setting $K = \mathbb{Q}(\mu_m)$, we obtain from Proposition 3.38 that

$$\zeta_K(s) = \zeta(s) \prod_{\mathfrak{p} \mid m} \frac{1}{1 - \mathfrak{N}(\mathfrak{p})^{-s}} \prod_{p \mid m} \left(1 - p^{-s}\right) \prod_{\chi \neq \chi_0} L(\chi, s) .$$

Since both $\zeta_K(s)$ and $\zeta(s)$ have a simple pole at $s = 1$, it follows that $L(\chi, 1) \neq 0$ for any $\chi \neq \chi_0$. □

Theorem 3.40 (Dirichlet's Prime Number Theorem) *Every arithmetic progression*

$$a,\ a \pm m,\ a \pm 2m,\ \dots \qquad \textit{with } \gcd(a, m) = 1$$

contains infinitely many prime numbers.

Proof. Let χ be a Dirichlet character mod m and $a \in \mathbb{Z}$ coprime to m. Then for $\operatorname{Re}(s) > 1$,

$$\log L(\chi, s) = -\sum_{p \in \mathbb{P}} \log\left(1 - \chi(p)p^{-s}\right) = \sum_{p}\sum_{k=1}^{\infty} \frac{\chi\left(p^k\right)}{kp^{ks}} = \sum_{p} \frac{\chi(p)}{p^s} + g_\chi(s)\,,$$

where $g_\chi(s) = \sum_p \sum_{k=2}^{\infty} \frac{\chi(p^k)}{kp^{ks}}$ is holomorphic for $\operatorname{Re}(s) > \frac{1}{2}$. Further, summing over all characters mod m, setting $g(s) := \sum_\chi \chi\left(a^{-1}\right) g_\chi(s)$ and using the orthogonality relations (Theorem 3.37), we obtain

$$\begin{aligned}\sum_{\chi} \chi\left(a^{-1}\right) \log L(\chi, s) &= \sum_{\chi}\sum_{p} \frac{\chi\left(a^{-1}p\right)}{p^s} + g(s)\\ &= \sum_{b=1}^{m}\sum_{\chi} \chi\left(a^{-1}b\right) \sum_{p \equiv b \bmod m} \frac{1}{p^s} + g(s)\\ &= \sum_{p \equiv a \bmod m} \frac{\phi(m)}{p^s} + g(s)\,.\end{aligned}$$

(Note that the left hand side makes sense because a is coprime to m.) When we let $s \in \mathbb{R}_{>1}$ tend to 1, by Corollary 3.39 we obtain

- $\chi \neq \chi_0$: $\lim\limits_{s \to 1^+} |\log L(\chi, s)| < \infty$
- $\chi = \chi_0$: $\lim\limits_{s \to 1^+} \log L(\chi_0, s) = \lim\limits_{s \to 1^+} \left(\sum_{p \mid m} \log\left(1 - p^{-s}\right) + \log \zeta(s)\right) = \infty\,,$

so $\lim\limits_{s \to 1^+} \sum_\chi \chi\left(a^{-1}\right) \log L(\chi, s) = \infty$. Hence, because g is holomorphic at $s = 1$,

$$\lim_{s \to 1^+} \sum_{p \equiv a \bmod m} \frac{\phi(m)}{p^s} = \infty\,,$$

and thus the number of primes congruent to $a \bmod m$ (if $\gcd(a, m) = 1$) must be infinite. □

In fact, the proof of the above theorem provides the **Dirichlet density** for the set of prime numbers in an arithmetic progression.

Definition 3.41 *Let M be a set of prime ideals in a number field K. The limit*

$$d(M) = \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in M} \mathfrak{N}(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}} \mathfrak{N}(\mathfrak{p})^{-s}}\,,$$

if it exists, is called the ***Dirichlet density*** *of M.*

Theorem 3.42 *If $\gcd(a,m)=1$, the set of prime numbers congruent to $a \bmod m$ has Dirichlet density $\frac{1}{\phi(m)}$.*

Proof. In the proof of Theorem 3.40 we actually showed that for $s \to 1^+$

$$\sum_{p\equiv a \bmod\ m} p^{-s} = \frac{1}{\phi(m)} \log\zeta(s) + O(1) = \frac{1}{\phi(m)} \sum_{p\in\mathbb{P}} p^{-s} + O(1)\,.$$

□

Remark 3.43 *One can combine this with an estimate $\sum\limits_{p\leq x} \frac{1}{p} = \log\log x + O(1)$ to obtain*

$$\sum_{\substack{p\equiv a \bmod\ m\\ p\leq x}} \frac{1}{p} = \frac{1}{\phi(m)} \log\log x + O(1)\,.$$

Remark 3.44 *Another kind of density of a set of prime ideals in K one might consider is the* ***natural density***

$$\delta(M) = \lim_{x\to\infty} \frac{\#\{\mathfrak{p}\in M |\, \mathfrak{N}(\mathfrak{p}) \leq x\}}{\#\{\mathfrak{p} |\, \mathfrak{N}(\mathfrak{p}) \leq x\}}.$$

If the natural density of M exists, one can show that it is equal to $d(M)$. Theorem 3.42 remains valid if we replace the Dirichlet density with the natural density but it becomes significantly harder to prove, see [6].

Corollary 3.45 *Let a be an integer that is not a square. Then the set of prime numbers p such that a is a square modulo p has Dirichlet density $\frac{1}{2}$.*

Proof. Without loss of generality we can assume that a is square-free. Recall that, for an odd prime p, the Legendre symbol $\left(\frac{b}{p}\right)$ is 1 if b is a square modulo p, 0 if $p|b$ and -1 if b is not a square modulo p. It is not hard to show that $x \mapsto \left(\frac{x}{p}\right)$ is a homomorphism from $(\mathbb{Z}/p\mathbb{Z})^\times$ to $\{\pm 1\}$. We recall the law of quadratic reciprocity. If p and q are distinct odd primes

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

and the two additional equations $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ and $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. Since a is square-free we can write $a = (-1)^{\epsilon_1}2^{\epsilon_2}\prod_{q|a, q \text{ odd}} q$ with $\epsilon_i \in \{\pm 1\}$. By quadratic reciprocity

$$\left(\frac{a}{p}\right) = \left(\frac{-1}{p}\right)^{\epsilon_1}\left(\frac{2}{p}\right)^{\epsilon_2}\prod_q \left(\frac{q}{p}\right) = (-1)^{\epsilon_1\frac{p-1}{2}+\epsilon_2\frac{p^2-1}{8}}\prod_q \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

The map $\chi_a : x \mapsto (-1)^{\epsilon_1 \frac{x-1}{2} + \epsilon_2 \frac{x^2-1}{8}} \prod_q \left(\frac{x}{q}\right) (-1)^{\frac{x-1}{2}\frac{q-1}{2}}$ is a surjective homomorphism from $(\mathbb{Z}/4a\mathbb{Z})^\times$ to $\{\pm 1\}$, so its kernel has index 2 in $(\mathbb{Z}/4a\mathbb{Z})^\times$. Hence by Dirichlet's theorem the Dirichlet density of p such that $\left(\frac{a}{p}\right) = 1$, is $\frac{1}{2}$. □

Remark 3.46 *Corollary 3.45 can be rephrased as follows: Let $a \in \mathbb{Z}$ be squarefree, so that the polynomial $f(X) = X^2 - a$ is irreducible in $\mathbb{Z}[X]$. Then the set of primes such that f splits has Dirichlet density $\frac{1}{2}$. One can study similar problems for any monic irreducible polynomial $f \in \mathbb{Z}[X]$ of degree n. In the following sections we will prove Chebotarev's density theorem which has powerful applications to such questions. Two consequences will be*

(1) *The Dirichlet density of primes such that f decomposes into linear factors modulo p is $\frac{1}{N}$, where N is the degree of the splitting field of f.*
(2) *The Dirichlet density of primes such that f has no roots modulo p is greater than 0.*

Corollary 3.47 *Let K be a number field and $\alpha \in \mathcal{O}_K$ such that $\alpha \bmod \mathfrak{p}$ is a square in $\mathcal{O}_K/\mathfrak{p}$ for almost all prime ideals $\mathfrak{p}$. Then α is a square.*

PROOF. The idea is to compare $\zeta_{K(\sqrt{\alpha})}$ to ζ_K. Details are left to the reader. □

CHAPTER 4

Hecke characters

We have proved the important properties such as meromorphic continuation and the functional equation of L-functions associated to characters of the ideal class group of a number field K following the original approach of Hecke from 1917. Hecke realised that the same approach works for a much more general class of characters, which are characters on fractional ideals of a number field. Before we come to the general definition let us give several examples. The first example we give is a generalisation of characters of the class group Cl_K:

Definition 4.1 *For $\mathfrak{m}$ an integral ideal of K we denote by $J^{\mathfrak{m}}$ the group of all fractional ideals which are relatively prime to $\mathfrak{m}$, i.e.,*

$$J^{\mathfrak{m}} = \{\mathfrak{a} \in J : \gcd(\mathfrak{a}, \mathfrak{m}) = \mathcal{O}_K\}.$$

Let $P^{\mathfrak{m}}$ be the group of principal ideals (a) such that

$$a \text{ is totally positive and } a \equiv 1 \bmod \mathfrak{m}.$$

where we say that

- *a is totally positive if $\tau(a) > 0$ for every real embedding τ,*
- *$a \equiv 1 \bmod \mathfrak{m}$ if $a = b/c$ for $b, c \in \mathcal{O}_K$ that are coprime to $\mathfrak{m}$ and $b \equiv c \bmod \mathfrak{m}$.*

The group

$$\mathrm{Cl}^{\mathfrak{m}} = J^{\mathfrak{m}}/P^{\mathfrak{m}}$$

*is called the **ray class group** modulo $\mathfrak{m}$ and it is finite (exercise). A **(generalised) Dirichlet character** modulo $\mathfrak{m}$ is a character of the group $\mathrm{Cl}^{\mathfrak{m}}$ or, equivalently, a character $\chi : J^{\mathfrak{m}} \to S^1$ with $\chi|_{P^{\mathfrak{m}}} = 1$.*

Example 4.2 *Let $K = \mathbb{Q}$ and $\mathfrak{m} = (m)$ for some integer m. Then, by mapping an ideal $(n) \in J^{\mathfrak{m}}$ to $|n| \bmod m$, we get an isomorphism $J^{\mathfrak{m}}/P^{\mathfrak{m}} \cong (\mathbb{Z}/m\mathbb{Z})^{\times}$. So Dirichlet characters modulo $\mathfrak{m}$ correspond to classical Dirichlet characters modulo m.*

Here we see that characters of quotients of $(\mathbb{Z}/m\mathbb{Z})^{\times}$ can be interpreted as characters on groups of fractional ideals. Starting with a Dirichlet character χ_{f} modulo m we have to be careful about extending it to ideals. For n coprime to m we cannot just define $\chi((n)) = \chi_{\mathrm{f}}(n)$, since the ideals (n) and $(-n)$ are equal but $\chi(n) = \chi(-1)\chi(-n)$. We are led to the definition

$$\chi((n)) := \chi_{\mathrm{f}}(n)\left(\frac{n}{|n|}\right)^p,$$

where $\chi_{\mathrm{f}}(-1) = (-1)^p$, that gives the precise connection between Dirichlet characters modulo (m) defined above and classical Dirichlet characters modulo m.

Definition 4.3 *A* ***Größencharacter*** $\bmod \mathfrak{m}$ *is a character* $\chi : J^{\mathfrak{m}} \to S^1 := \{z \in \mathbb{C} : |z| = 1\}$ *for which there exist a character* $\chi_{\mathrm{f}} : (\mathcal{O}_K/\mathfrak{m})^\times \to S^1$ *and a continuous character* $\chi_\infty : K_{\mathbb{R}}^\times \to S^1$*, called the infinity type of* χ*, such that for all* $a \in \mathcal{O}_K$ *coprime to* $\mathfrak{m}$ *we have*

$$\chi((a)) = \chi_{\mathrm{f}}(a)\chi_\infty(a).$$

Generalised Dirichlet characters are special cases of Größencharacters and we will mostly be interested in them.

Note that χ_∞ is uniquely determined by χ. Define

$$K^{\mathfrak{m}} = \{a \in K : a \equiv 1 \bmod \mathfrak{m}\}$$

Then $K^{\mathfrak{m}}$ is dense in $K_{\mathbb{R}}^\times$ by the Approximation Theorem which you can find in [5, Chapter II (3.4)] and for $a \in K^{\mathfrak{m}}$ we have $\chi_\infty(a) = \chi((a))$. The character χ_{f} is also uniquely determined by χ since for $a \in (\mathcal{O}_K/\mathfrak{m})^\times$ we have $\chi_{\mathrm{f}}(a) = \chi((a))\chi_\infty(a)^{-1}$.

As with Dirichlet characters we can induce Größencharacters from smaller modules. If $\mathfrak{m}'$ divides $\mathfrak{m}$ and χ' is a Größencharacter on $J^{\mathfrak{m}'}$, then we can restrict χ' to a Größencharacter on $J^{\mathfrak{m}}$. A Größencharacter $\bmod \mathfrak{m}$ is the restriction of a Größencharacter $\bmod \mathfrak{m}'$ if and only if χ_{f} factors through $(\mathcal{O}_K/\mathfrak{m}')^\times$ (see [5, Theorem (6.2)]). A Grössencharacter is called **primitive** if it is not the restriction of a Grössencharacter χ' modulo a proper divisor $\mathfrak{m}'|\mathfrak{m}$.

Let us now study the possible infinity types of Größencharacters.

Proposition 4.4 *The continuous characters on* $K_{\mathbb{R}}^\times$ *are given by*

$$\lambda(x) = \mathrm{N}(x^p|x|^{-p+iq}),$$

where $p \in \prod_\tau \mathbb{Z}$ *is admissible and* $q \in K_{\mathbb{R},\pm}$*. Both* p *and* q *are uniquely determined by* λ*.*

Proof. The map $x \mapsto \frac{x}{|x|}|x|$ gives a homeomorphism between $K_{\mathbb{R}}^\times$ and $U \times K_{\mathbb{R},+}^\times$ where $U = \{u \in K_{\mathbb{R}}^\times : |u| = (1, \ldots, 1)\}$. We will determine the characters of U and of $K_{\mathbb{R},+}^\times$ separately. We have

$$U = \prod_{\tau \text{ real}} \{\pm 1\} \times \prod_{\{\tau,\overline{\tau}\} \text{ complex}} \{(a, \overline{a}) : a \in S^1\}$$

The spaces $\{(a, \overline{a}) : a \in S^1\}$ are homeomorphic to S^1 by $a \mapsto (a, \overline{a})$ and the continuous characters on S^1 are given by $x \mapsto x^k$ for $k \in \mathbb{Z}$. Hence the characters on U are given by

$$x \mapsto \mathrm{N}(x^p)$$

for an admissible p. The group $K_{\mathbb{R},+}^\times$ is homeomorphic to

$$K_{\mathbb{R},\pm} = \prod_{\tau \text{ real}} \mathbb{R} \times \prod_{\{\tau,\overline{\tau}\} \text{ complex}} \{(a, a) : a \in \mathbb{R}\}$$

via log. A character on $K_{\mathbb{R},\pm}$ is given with a choice of $q \in K_{\mathbb{R},\pm}$ by

$$x \mapsto \prod_{\tau \text{ real}} e^{iq_\tau x_\tau} \prod_{\{\tau,\overline{\tau}\} \text{ complex}} e^{2iq_\tau x_\tau} = \mathrm{N}(e^{iqx}).$$

Going back to $K_{\mathbb{R},+}^\times$ via log we see that characters on $K_{\mathbb{R},+}^\times$ are given by $y \mapsto \mathrm{N}(y^{iq})$. Finally, using our decomposition $K_\mathbb{R}^\times = U \times K_{\mathbb{R},+}^\times$, we see that characters on $K_\mathbb{R}^\times$ are given by

$$\lambda(x) = \mathrm{N}(x^p |x|^{-p+iq})$$

□

The proposition allows us to denote the infinity type of a Größencharacter simply by (p, q). We are now ready to prove that generalised Dirichlet characters are Hecke Größencharacters.

Proposition 4.5 *The Dirichlet characters χ modulo $\mathfrak{m}$ are precisely the Größencharacters modulo $\mathfrak{m}$ with infinity type $(p, 0)$ where p satisfies $p_\tau = 0$ for all complex τ.*

Proof. Let χ be a Größencharacter modulo $\mathfrak{m}$ of type $(p, 0)$ with $p_\tau = 0$ for complex τ and let $(a) \in P^\mathfrak{m}$. Then

$$\chi((a)) = \chi_\mathrm{f}(a)\mathrm{N}(a^p|a|^{-p}) = 1.$$

So χ factors through $J^\mathfrak{m}/P^\mathfrak{m}$.

Conversely assume χ is a character on $J^\mathfrak{m}/P^\mathfrak{m}$ which we view as a character on $J^\mathfrak{m}$ that is trivial on $P^\mathfrak{m}$. Let $K_+^\mathfrak{m}$ be the elements of $K^\mathfrak{m}$ that are totally positive. Then

$$K^\mathfrak{m}/K_+^\mathfrak{m} \overset{\cong}{\to} K_\mathbb{R}^\times/\{x \in K_\mathbb{R}^\times : \forall_{\tau \text{ real}}\, x_\tau > 0\} \cong \prod_{\tau \text{ real}} \{\pm 1\} \tag{18}$$

Define χ_∞ as the composite of the natural map $K^\mathfrak{m}/K_+^\mathfrak{m} \to J^\mathfrak{m}/P^\mathfrak{m}$ with χ. By (18) we can interpret χ_∞ as a character on $K_\mathbb{R}^\times$ which is trivial on $\{x \in K_\mathbb{R}^\times : \forall_{\tau \text{ real}}\, x_\tau > 0\}$. Since we classified the characters on $K_\mathbb{R}^\times$ we see that $\chi_\infty(x) = \mathrm{N}(x^p|x|^{-p})$ with $p_\tau \in \{0, 1\}$ if τ is real and $p_\tau = 0$ if τ is complex. Now set

$$\chi_\mathrm{f}(a) = \chi((a))\chi_\infty(a)^{-1}$$

for a coprime to $\mathfrak{m}$ and check that this indeed gives a character of $(\mathcal{O}_K/\mathfrak{m})^\times$. □

Example 4.6 *Let $K = \mathbb{Q}$. For any $q \in \mathbb{R}$, the character*

$$\chi_s((a)) = |a|^{iq}$$

is a Größencharacter of infinity type $(0, q)$.

Example 4.7 *The Dirichlet characters χ modulo $\mathcal{O}_K$ with infinity type $(p, 0) = (0, 0)$ may be viewed as characters of the ideal class group $\mathrm{Cl}_K = J_K/P_K$. Indeed, for $\mathfrak{m} = \mathcal{O}_K$, χ_{f} is defined on $\{1\}$ and thus must be trivial. Further, for $p = 0$ we must have $\chi_\infty = 1$. By the definition, this means that for all $a \in \mathcal{O}_K$, $\chi((a)) = \chi_{\mathrm{f}}(a)\chi_\infty(a) = 1$.*

Remark 4.8 *Equivalently Grössencharacters are nowadays defined as continuous characters of the idèle class group $\mathbb{A}_K/K^\times$.*

1. Hecke L-functions

To a Grössencharacter $\chi : J^{\mathfrak{m}} \to S^1$ we can associate the L-series

$$L(\chi, s) = \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{\mathfrak{N}(a)^s},$$

where the sum is over all integral ideals of K and we set $\chi(\mathfrak{a}) = 0$ if $(\mathfrak{a}, \mathfrak{m}) \neq \mathcal{O}_K$. These L-functions satisfy similar properties to the L-functions we studied in previous sections and the proofs follow the same startegy. That is, the L-functions are written as Mellin transforms of functions related to general theta functions. The properties of the L-function then follow from transformation and growth properties of the theta functions. For this reason we skip the proofs in this section and just state the results. The proofs can be found in [5, Chapter VII].

Proposition 4.9 *The L-series $L(\chi, s)$ converges absolutely and uniformly on compact subsets of the half plane $Re(s) > 1$. In the region of absolute convergence we have the Euler product*

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

where the product is taken over all prime ideals of K.

In the following theorem we set

$$L_\infty(\chi, s) = \mathrm{N}(\pi^{-s\mathbf{1}/2})\Gamma_K((s\mathbf{1} + p - iq)/2)$$

where $\mathbf{1} = (1, \ldots, 1) \in K_{\mathbb{R}}$.

Theorem 4.10 *Let χ be a primitive Größencharacter modulo $\mathfrak{m}$. Then the completed Hecke L-function*

$$\Lambda(\chi, s) = (|d_K|\mathfrak{N}(\mathfrak{m}))^{s/2} L_\infty(\chi, s)L(\chi, s)$$

has holomorphic continuation to

$$\mathbb{C} \setminus \{Tr(-p + iq)/n, 1 + Tr(p + iq)/n\}$$

and satisfies the functional equation

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

It is holomorphic on all of $\mathbb{C}$ if $\mathfrak{m} \neq 1$ or $p \neq 0$. Here $W(\chi)$ is a complex number of absolute value 1.

We will only give the proof of this theorem in a very special case, when χ is a character of the class group Cl_K. Then χ can be viewed as a character on the group of fractional ideals J_K that is trivial on P_K, the group of principal ideals. In particular χ is trivial on $P^{\mathcal{O}_K}$ and hence it can be viewed as a Dirichlet character modulo $\mathcal{O}_K$. Then

$$L(\chi, s) = \sum_{0 \neq \mathfrak{a} \lhd \mathcal{O}_K} \frac{\chi(\mathfrak{a})}{\mathfrak{N}(\mathfrak{a})^s} = \sum_{\mathfrak{K} \in \mathrm{Cl}_K} \chi(\mathfrak{K})\zeta_K(\mathfrak{K}, s)\,,$$

For such an L-function Theorem 4.10 follows from the properties of the partial Dedekind zeta functions $\zeta_K(\mathfrak{K}, s)$ that we studied in the last section and the orthogonality relations in Theorem 3.37.

Corollary 4.11 *For a non-trivial character χ of Cl_K the completed zeta function*

$$Z_K(\chi, s) = \sum_{\mathfrak{K} \in \mathrm{Cl}_K} \chi(\mathfrak{K})Z_K(\mathfrak{K}, s)$$

is holomorphic on all of $\mathbb{C}$ and satisfies the functional equation

$$Z_K(\chi, s) = \chi(\mathfrak{d})Z_K(\bar{\chi}, 1 - s)\,.$$

CHAPTER 5

Artin L-functions

In this chapter we will get to know a new source of L-functions: Galois representations. We first give some basic properties of decomposition groups and Frobenius elements that we will need later. Let L/K be a Galois extension with Galois group $G = \mathrm{Gal}(L/K)$ and $\mathfrak{P} \lhd \mathcal{O}_L$ be a prime above $\mathfrak{p} \lhd \mathcal{O}_K$. The **decomposition group** of $\mathfrak{P}$ (over $\mathfrak{p}$) is defined by

$$D_{\mathfrak{P}} = \{\sigma \in G : \sigma\mathfrak{P} = \mathfrak{P}\}.$$

Considering the action of $D_{\mathfrak{P}}$ on $\mathcal{O}_L/\mathfrak{P}$ we get a surjection from $D_{\mathfrak{P}}$ to the cyclic Galois group $\mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$. The kernel $I_{\mathfrak{P}}$ of this surjection is called the **inertia group** and the element $\mathrm{Frob}_{\mathfrak{P}}$ of $D_{\mathfrak{P}}/I_{\mathfrak{P}}$ that maps to $\phi(x) = x^{\#(\mathcal{O}_K/\mathfrak{p})}$ is the **Frobenius element**. In all these notations we will sometimes write $\mathfrak{P}/\mathfrak{p}$ instead of $\mathfrak{P}$ in the indices to emphasise the prime that lies below $\mathfrak{P}$.

Lemma 5.1 *Let $\tau \in G$. The Galois action on prime ideals above $\mathfrak{p}$ translates to an action by conjugation on decomposition groups, inertia groups and Frobenius elements:*

$$D_{\tau(\mathfrak{P})} = \tau D_{\mathfrak{P}}\tau^{-1}, \quad I_{\tau(\mathfrak{P})} = \tau I_{\mathfrak{P}}\tau^{-1}, \quad \mathrm{Frob}_{\tau(\mathfrak{P})} = \tau \mathrm{Frob}_{\mathfrak{P}}\tau^{-1}.$$

Proof. Let $\sigma \in G$. Then σ fixes $\tau(\mathfrak{P})$ if and only if $\tau^{-1}\sigma\tau$ fixes $\mathfrak{P}$. Now let $\sigma \in D_{\tau(\mathfrak{P})}$. Then $\sigma(x) \equiv x^i \bmod \tau(\mathfrak{P})$ for all $x \in \mathcal{O}_L$ and a fixed i. This is equivalent to $\tau^{-1} \circ \sigma \circ \tau(x) \equiv x^i \bmod \mathfrak{P}$. If $i = 1$ this proves the statement about $I_{\tau(\mathfrak{P})}$, while if $i = |\mathcal{O}_K/\mathfrak{p}|$ we obtain the statement about $\mathrm{Frob}_{\mathfrak{P}}$. □

Lemma 5.2

$$\#D_{\mathfrak{P}} = e_{\mathfrak{p}} f_{\mathfrak{p}}, \quad \#I_{\mathfrak{P}} = e_{\mathfrak{p}}, \quad \mathrm{ord}(\mathrm{Frob}_{\mathfrak{P}}) = f_{\mathfrak{p}}.$$

Proof. Let m be the number of primes above $\mathfrak{p}$. The Galois group acts transitively on this set and the decomposition groups of each of these primes have the same size by Lemma 5.1. Hence

$$m\#D_{\mathfrak{P}} = \#\,\mathrm{Gal}(L/K) = [L : K] = me_{\mathfrak{p}}f_{\mathfrak{p}}.$$

The other statements follow from the fact that $\mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$ is cyclic of order $f_{\mathfrak{P}/\mathfrak{p}}$. □

Recall that if L/K is the splitting field of an irreducible polynomial $f(X) \in \mathcal{O}_K[X]$ of degree n, then the Galois group $\mathrm{Gal}(L/K)$ can be embedded in the symmetric group S_n. This is because any Galois automorphism in $\mathrm{Gal}(L/K)$ is uniquely determined by the permutation it induces on the roots $\alpha_1, \dots, \alpha_n$ of f.

Proposition 5.3 *If, in the situation above, $\mathfrak{p}$ is a prime of K and*

$$f(X) \equiv g_1(X)g_2(X)\dots g_k(X) \bmod \mathfrak{p},$$

with $g_i(X) \in \mathcal{O}_K/\mathfrak{p}[X]$ distinct irreducible polynomials of degree $\deg g_i = d_i$. Then, if $\mathfrak{q}$ is a prime above $\mathfrak{p}$, $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}} \in \mathrm{Gal}(L/K) \leq S_n$ has cycle type $(d_1, \dots, d_k)$.

Proof. Since $f(X) = \prod_{i=1}^n (X - \alpha_i)$, $f(X) \bmod \mathfrak{q}$ splits into linear factors modulo $\mathfrak{q}$. Note that, because the g_i are distinct, the roots $\alpha_i \bmod \mathfrak{q}$ are distinct. That means that an element $\sigma \in D_{\mathfrak{q}/\mathfrak{p}}$ has exactly the same permutation action on the α_i as $\overline{\sigma} \in \mathrm{Gal}(\mathcal{O}_L/\mathfrak{q} : \mathcal{O}_K/\mathfrak{p})$ does on the roots $\alpha_i \bmod \mathfrak{q}$.

Since $\mathcal{O}_L/\mathfrak{q}$ contains a splitting field of every g_i the cyclic group $\mathrm{Gal}(\mathcal{O}_L/\mathfrak{q} : \mathcal{O}_K/\mathfrak{p})$ acts transitively on the roots of g_i for every i. Any generator of $\mathrm{Gal}(\mathcal{O}_L/\mathfrak{q} : \mathcal{O}_K/\mathfrak{p})$ thus has the correct cycle type. □

Remark 5.4 *If L/K is abelian (i.e., $\mathrm{Gal}(L/K)$ is abelian) and $\mathfrak{p}$ is unramified, by Lemma 5.1 $\mathrm{Frob}_{\mathfrak{P}/\mathfrak{p}}$ is an element of $\mathrm{Gal}(L/K)$ that is independent the choice of $\mathfrak{P}$ above $\mathfrak{p}$. In this case we will write $\mathrm{Frob}_{\mathfrak{p}}$ for the Frobenius element of any prime above $\mathfrak{p}$. An unramified prime $\mathfrak{p}$ splits completely if and only if $f_{\mathfrak{p}} = 1$. By Lemma 5.2 this is the case if and only if $\mathrm{Frob}_{\mathfrak{p}}$ is trivial.*

1. An old example

In Example 4.2 we saw that Dirichlet characters modulo m correspond to ray class group characters modulo $\mathfrak{m} = (m)$. Thus Dirichlet L-functions can be interpreted as Hecke L-functions. Here we will see a new perspective. Let ζ_m be an m-th root of unity. Recall that

$$\begin{aligned} (\mathbb{Z}/m\mathbb{Z})^\times &\xrightarrow{\cong} \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \\ a &\mapsto (\sigma_a : \zeta_m \mapsto \zeta_m^a) \end{aligned}$$

Let $p \nmid m$, so that p does not ramify in $\mathbb{Q}(\zeta_m)$. The Frobenius element associated to a prime p is the element $\mathrm{Frob}_p \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ with

$$\mathrm{Frob}_p(x) \equiv x^p \bmod \mathfrak{p},$$

for any prime ideal $\mathfrak{p}|p$. Since the m-th roots of unity are distinct modulo $\mathfrak{p}$ we must have $\mathrm{Frob}_p = \sigma_p$. If χ is a Dirichlet character modulo m, let $\tilde{\chi}$ be the corresponding character of the group $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ via the above isomorphism. We see that if $p \nmid m$, then the Euler factor

$$L_p(\chi, s) = (1 - \chi(p)p^{-s})^{-1}$$

of the Dirichlet L-series is equal to

$$L_p(\tilde{\chi}, s) = (1 - \tilde{\chi}(\mathrm{Frob}_p)p^{-s})^{-1}. \tag{19}$$

Analogously we can attach such Euler factors to any character of a Galois group. This is the first inspiration for the definition of Artin L-functions.

2. A new example

In the exercise class we studied the extension $L = \mathbb{Q}(\alpha)$, where α has minimal polynomial $P(X) = X^3 - X - 1$, and looked at the following extensions:

$$\begin{tikzcd}
 & H \arrow[dl, dash, "C_3"'] \arrow[dd, dash, "S_3"] \arrow[dr, dash, "C_2"] & \\
K = \mathbb{Q}(\sqrt{-23}) \arrow[dr, dash, "C_2"'] & & L \arrow[dl, dash, "\text{degree 3}"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

The field H is the Galois closure of L. We showed that only $p = 23$ ramifies in H and no prime p of $\mathbb{Q}$ is inert in $H/\mathbb{Q}$. So there are three possible ways p can split in H:

$$p\mathcal{O}_H = \begin{cases} \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3\mathfrak{q}_4\mathfrak{q}_5\mathfrak{q}_6 & \text{and } e_p = f_p = 1,\ \mathfrak{N}(\mathfrak{q}_i) = p \\ \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3 & \text{and } e_p = 1, f_p = 2, \mathfrak{N}(\mathfrak{q}_i) = p^2 \\ \mathfrak{q}_1\mathfrak{q}_2 & \text{and } e_p = 1, f_p = 3,\ \mathfrak{N}(\mathfrak{q}_i) = p^3, \\ \mathfrak{q}_1^2\mathfrak{q}_2^2\mathfrak{q}_3^2, & \text{if } p = 23,\ \mathfrak{N}(\mathfrak{p}_i) = p. \end{cases} \tag{20}$$

We looked at the L-function $L(s) = \zeta_L(s)\zeta(s)^{-1}$, which had the Euler factors

$$L_p(s)^{-1} = \begin{cases} (1 - p^{-s})^2 & \text{if } p\mathcal{O}_H = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3\mathfrak{q}_4\mathfrak{q}_5\mathfrak{q}_6, \\ (1 - p^{-2s}) & \text{if } p\mathcal{O}_H = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3, \\ (1 - \zeta_3 p^{-s})(1 - \zeta_3^{-1}p^{-s}) & \text{if } p\mathcal{O}_H = \mathfrak{q}_1\mathfrak{q}_2, \\ (1 - p^{-s}) & \text{if } p = 23, \end{cases}$$

and we showed that

$$\zeta_H(s) = L(s)^2\zeta_K(s). \tag{21}$$

The situation is similar for all S_3-extensions of $\mathbb{Q}$. Artin realised that the L-function above can be defined similarly to Dirichlet L-functions. His crucial idea was that since $\mathrm{Gal}(H/\mathbb{Q})$ is not abelian, one should look at irreducible representations of $\mathrm{Gal}(H/\mathbb{Q})$ rather than characters, which are only the 1-dimensional representations. The group S_3 has an irreducible 2-dimensional representation St, called the standard representation, defined as follows. It is a group homomorphism from S_3 into $\mathrm{GL}_2(\mathbb{Q})$ such that

$$\mathrm{St}((12)) = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad \mathrm{St}((123)) = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

We now try to imitate the definition of the L-factor in equation (19) and define

$$\tilde{L}_p(s) = \det(1_2 - \mathrm{St}(\mathrm{Frob}_{\mathfrak{q}/p})p^{-s})^{-1},$$

for $p \neq 23$, where $\mathfrak{q}$ is any prime of H above p. Any other choice $\mathfrak{q}'$ would give a Frobenius element that is conjugate to $\mathrm{Frob}_{\mathfrak{q}}$ and since the determinant only depends on the conjugacy class of a matrix, the definition of L_p is independent of the choice of $\mathfrak{q}$. Note that up to conjugacy, every element of S_3 is determined by its cycle type. So it suffices to determine the cycle type of $\mathrm{Frob}_{\mathfrak{q}/p}$. If $p\mathcal{O}_H = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3\mathfrak{q}_4\mathfrak{q}_5\mathfrak{q}_6$, then $\mathrm{Frob}_{\mathfrak{q}_i/p}$ is trivial and hence $\tilde{L}_p(s)^{-1} = (1-p^{-s})^2$. If $p\mathcal{O}_H = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$, then $\mathrm{Frob}_{\mathfrak{q}_i/p}$ has cycle type (12) and hence

$$\tilde{L}_p(s)^{-1} = \det\left(1 - \mathrm{St}((12))p^{-s}\right) = \det(\begin{pmatrix} 1+p^{-s} & -p^{-s} \\ 0 & 1-p^{-s} \end{pmatrix}) = (1-p^{-2s}).$$

Finally, if $p\mathcal{O}_H = \mathfrak{q}_1\mathfrak{q}_2$, then $\tilde{L}_p(s)^{-1} = (1+p^{-s}+p^{-2s}) = (1-\zeta_3 p^{-s})(1-\zeta_3^{-1}p^{-s})$. So for $p \neq 23$ the Euler factors of $\tilde{L}_p(s)$ exactly correspond to the Euler factors of L! Artin's idea of studying L-functions related to Galois representations led to a rich theory that immediately explains equations such as (21) and provides a powerful tool to study the behaviour of prime ideals in extensions of number fields.

3. Representation theory

A **representation** of a finite group G is a homomorphism $\rho : G \to \mathrm{GL}_n(V)$ for some complex vector space V with $n = \dim_{\mathbb{C}} V$; n is the **degree of a representation** (ρ, V). Note that ρ describes an action of the group G on V, and thus V is a G-module. In general, a complex vector space together with an action of a group G gives rise to a representation of G. The representation (ρ, V) is **irreducible** if V does not admit any proper G-invariant subspace.

Example 5.5

(1) *A* 1*-dimensional representation of G is the same as a homomorphism from $\rho : G \to \mathrm{GL}_1(\mathbb{C}) = \mathbb{C}^\times$. If $\rho(g) = 1$ for all $g \in G$ we call it the* ***trivial representation*** *and denote by* **1**.

(2) *The representation* St *is a* 2*-dimensional irreducible representation of* S_3.

A homomorphism of from (ρ, V) to (ρ', V') is a homomorphism $\psi : V \to V'$ such that for all $g \in G$ and $v \in V$ we have $\psi(\rho(g)v) = \rho'(g)\psi(v)$. We say that two representations (ρ, V), (ρ', V') are **equivalent** if there exists an invertible homomorphism between them. Every representation factors into a direct sum of irreducible representations. If $V \cong V_1^{r_1} \oplus \ldots \oplus V_s^{r_s}$ and (ρ_i, V_i) are pairwise non-equivalent irreducible representations, then we call r_i the **multiplicity of ρ_α in ρ.**

The **character of a representation** (ρ, V) is the function

$$\chi_\rho : G \to \mathbb{C}, \qquad \chi_\rho(\sigma) = \operatorname{tr}(\rho(\sigma)),$$

where tr denotes the trace (of a matrix $\rho(\sigma)$). The character χ_ρ is **irreducible** if ρ is irreducible. Note that:

- $\chi_\rho(1_G) = \dim_{\mathbb{C}} V = \deg(\rho)$;
- $\chi_{\mathbf{1}}$ is a constant function equal to 1;
- $\chi_{\rho\oplus\rho'} = \chi_\rho + \chi_{\rho'}$;
- $\chi_\rho(\sigma\tau\sigma^{-1}) = \chi_\rho(\tau)$ for all $\sigma, \tau \in G$.

In general, a function $f : G \to \mathbb{C}$ satisfying $f(\sigma\tau\sigma^{-1}) = f(\tau)$ for all $\sigma, \tau \in G$ is called a **class function**.

Fact 5.6 (1) *Every class function can be written uniquely as a linear combination of irreducible characters.*

(2) *Two representations are equivalent if and only if their characters are equal. In particular,*

$$\rho \sim \sum_{\alpha=1}^{s} r_\alpha \rho_\alpha \quad \Longleftrightarrow \quad \chi_\rho = \sum_{\alpha=1}^{s} r_\alpha \chi_{\rho_\alpha}$$

On the space of class functions we define a hermitian scalar product

$$(\varphi, \psi) := \frac{1}{\#G} \sum_{\sigma \in G} \varphi(\sigma)\bar{\psi}(\sigma)\,,$$

where $\bar{\psi}(\sigma) := \psi(\sigma^{-1})$. One can prove that if $\varphi = \chi$ and $\psi = \chi'$ are irreducible characters of G, then[1]

$$(\chi, \chi') = \frac{1}{\#G} \sum_{\sigma \in G} \chi\bar{\chi}'(\sigma) = \begin{cases} 0, & \text{if } \chi \neq \chi' \\ 1, & \text{if } \chi = \chi', \end{cases}$$

i.e., the irreducible characters form an orthonormal basis of this space. In particular, if $V \cong V_1^{r_1} \oplus \ldots \oplus V_s^{r_s}$ is a decomposition of a representation V with character χ

[1] If G is abelian, this follows from orthogonality relations stated in Theorem 3.37. Indeed, in this case the condition $\chi\bar{\chi}' = \mathbf{1}$ means that $\chi = \chi'$.

such that V_i are pairwise distinct irreducible representations with characters χ_i, then $r_i = (\chi, \chi_i)$ is the multiplicity of V_i in V. If we take $V_1 = \mathbb{C}$ to be the trivial representation, then

$$(\chi, \chi_{\mathbf{1}}) = \dim(\operatorname{span}_{\mathbb{C}}\{v \in V : \forall_{\sigma \in G}\, \sigma \cdot v = v\}) =: \dim_{\mathbb{C}} V^G\,.$$

Of special importance are the following representations:

(1) **(left) regular representation** is given by a vector space

$$V = \mathbb{C}[G] := \{\sum_{\tau \in G} x_\tau \tau : x_\tau \in \mathbb{C}\}$$

(which is freely generated by elements of G) on which G acts via multiplication on the left, i.e., $\sigma \cdot \sum_{\tau\in G} x_\tau \tau := \sum_{\tau \in G} x_\tau \sigma\tau$, $\sigma \in G$. If $\mathbb{C}[G] \cong V_1^{r_1} \oplus \ldots \oplus V_s^{r_s}$ and (ρ_i, V_i) are pairwise non-equivalent irreducible representations, then $r_i = \chi_{\rho_i}(1_G)$ and thus

$$\chi_{\mathbb{C}[G]} = \sum_i \chi_{\rho_i}(1_G)\chi_{\rho_i}\,. \tag{22}$$

Inserting 1_G we see

$$\#G = \sum_{i=1}^{s} (\dim V_i)^2. \tag{23}$$

Corollary 5.7 *Let G be an abelian group. All irreducible representations of G are 1-dimensional.*

Proof. This follows from the fact that the character group $G^* = \operatorname{Hom}(G, \mathbb{C}^\times)$ of G has the same size as G. Since the elements of G^* define $\#G^* = \#G$ pairwise distinct irreducible 1-dimensional representations we see from (23) that there can be no others. □

(2) **restricted representation** is given by restricting a representation (ρ, V) of G to a subgroup H of G; we denote it by $(\rho|_H, V)$ or $(\operatorname{Res}_H^G \rho, V)$.

(3) **induced representation**: let H be a subgroup of G, and (ρ, V) a representation of H. We define $(\operatorname{Ind}_H^G \rho, \operatorname{Ind}_H^G(V))$ to be the vector space

$$\operatorname{Ind}_H^G(V) := \{f : G \to V \,|\, \forall_{\tau \in H} f(\tau x) = \rho(\tau) f(x)\}$$

on which $\sigma \in G$ acts via $(\sigma \cdot f)(x) := f(x\sigma)$. The character of the induced representation $\operatorname{Ind}_H^G \rho$ is given by the formula

$$\chi_{\operatorname{Ind}_H^G \rho}(\sigma) = \sum_{\tau \in G/H} \chi_\rho(\tau\sigma\tau^{-1})\,,$$

where we set $\chi_\rho(\tau\sigma\tau^{-1}) := 0$ if $\tau\sigma\tau^{-1} \notin H$.

4. Representations of decomposition groups

Let L/K be a Galois extension, $\mathfrak{p}$ a prime in K, $\mathfrak{P}$ a prime in L above $\mathfrak{p}$, and $D = D_{\mathfrak{P}/\mathfrak{p}}$ and $I = I_{\mathfrak{P}/\mathfrak{p}}$.

Lemma 5.8 *Let (ρ, V) be an irreducible representation of D and let*

$$V^I = \{v \in V : \forall_{g \in I}\, gv = v\}.$$

Then either $V^I = 0$ or $V^I = V$ is 1-dimensional and factors through D/I.

Proof. Since $I \lhd D$, the subspace V^I is D-invariant (exercise) and hence, since (ρ, V) is irreducible, either $V^I = 0$ or $V^I = V$ defines a representation of D (exercise). In the latter case ρ factors through D/I, so V can be viewed as an irreducible representation of the abelian group D/I. By Corollary 5.7 these representations are 1-dimensional. □

Hence, a general representation of D is a direct sum $A \oplus B$ of vector spaces such that $A^I = 0$ and $B = B^I = V^I$. Let

$$\mathrm{char}_{\mathfrak{p}}(\rho, X) = \det\big(X - \rho|_{V^I}(\mathrm{Frob}_{\mathfrak{P}/\mathfrak{p}})\big)$$

be the characteristic polynomial of $\rho|_{V^I}(\mathrm{Frob}_{\mathfrak{P}/\mathfrak{p}})$. When we write $\rho|_{V^I}(\mathrm{Frob}_{\mathfrak{P}/\mathfrak{p}})$ we mean ρ applied to any lift of $\mathrm{Frob}_{\mathfrak{P}/\mathfrak{p}} \in D/I$ to D. This is well-defined because $I \subseteq \ker(\rho|_{V^I})$. If we choose a different prime $\mathfrak{P}'$ above $\mathfrak{p}$, the corresponding Frobenius automorphism will be conjugate to $\mathrm{Frob}_{\mathfrak{P}/\mathfrak{p}}$. Since characteristic polynomials of conjugate endomorphisms are equal, the definition of $\mathrm{char}_{\mathfrak{p}}$ does not depend on a choice of prime $\mathfrak{P}$ above $\mathfrak{p}$.

Lemma 5.9 *Let $\psi : D \to D/I \to \mathbb{C}^\times$ be the 1-dimensional representation of D with $\psi(\mathrm{Frob}_{\mathfrak{P}/\mathfrak{p}}) = \zeta$ for an $f_{\mathfrak{P}/\mathfrak{p}}$-th root of unity ζ. Then (ψ, χ_ρ) is the multiplicity of $(X - \zeta)$ in $\mathrm{char}_{\mathfrak{p}}(\rho, X)$*

Proposition 5.10 *Let $K \subseteq F \subseteq L$ be an intermediate field and (ρ, V) a representation of $H = \mathrm{Gal}(L/F)$. Then*

$$\mathrm{char}_{\mathfrak{p}}\big(\mathrm{Res}_D^{\mathrm{Gal}(L/K)} \mathrm{Ind}_H^{\mathrm{Gal}(L/K)} \rho, X\big) = \prod_{\mathfrak{s}|\mathfrak{p}} \mathrm{char}_{\mathfrak{p}}\big(\mathrm{Res}^H_{D_{\mathfrak{s}'/\mathfrak{s}}} \rho, X^{f_{\mathfrak{s}/\mathfrak{p}}}\big),$$

where the product is over all prime ideals $\mathfrak{s}$ of F lying above $\mathfrak{p}$ and $\mathfrak{s}'$ are primes of L lying above $\mathfrak{s}$.

Sketch of proof. Since both the left and the right hand side are polynomials whose roots are $f_{\mathfrak{P}/\mathfrak{p}}$-th roots of unity it suffices to show that the multiplicity of $(X - \zeta)$ is equal on both sides for every $f_{\mathfrak{P}/\mathfrak{p}}$-th root of unity. By Lemma 5.9 this can be translated into a statement about the multiplicity of a character ψ in

$\operatorname{Res}_D^{\operatorname{Gal}(L/K)}\operatorname{Ind}_H^{\operatorname{Gal}(L/K)}\rho$. And this in turn can be treated with Mackey's formula and Frobenius reciprocity, two classic tools in representation theory. We skip this last part of the proof. □

5. Artin L-functions

Definition 5.11 *Let L/K be a Galois extension of algebraic number fields with Galois group $\operatorname{Gal}(L/K)$ and let (ρ, V) be a representation of $\operatorname{Gal}(L/K)$. Then the **Artin L-series** attached to ρ (or equivalently to χ) is defined to be*

$$\mathcal{L}(L/K,\rho,s) := \prod_{\mathfrak{p}} \frac{1}{\det\left(1-\rho|_{V^{I_{\mathfrak{P}}}}(\mathrm{Frob}_{\mathfrak{P}})\mathfrak{N}(\mathfrak{p})^{-s}\right)} =: \prod_{\mathfrak{p}} \mathcal{L}_{\mathfrak{p}}(L/K,\rho,s)\,,$$

where $\mathfrak{p}$ runs through all prime ideals of K, $\mathfrak{P}$ is a prime above $\mathfrak{p}$.

Since $\mathcal{L}_{\mathfrak{p}}(L/K,\rho,s)^{-1} = \mathfrak{N}(\mathfrak{p})^{-s\dim V^{I_{\mathfrak{P}}}}\operatorname{char}_{\mathfrak{p}}(\operatorname{Res}_{D_{\mathfrak{P}}}^{\operatorname{Gal}(L/K)}\rho, \mathfrak{N}(\mathfrak{p})^s)$ the local L-factor $\mathcal{L}_{\mathfrak{p}}(L/K,\rho,s)$ does not depend on a choice of prime ideal $\mathfrak{P}$ above $\mathfrak{p}$.

Remark 5.12 *Taking the logarithm we see more directly the dependence of $\mathcal{L}(L/K,\rho,s)$ on the character χ:*

$$\log\mathcal{L}(L/K,\rho,s) = \sum_{\mathfrak{p}}\sum_{m\geq 1}\frac{\chi(\mathrm{Frob}_{\mathfrak{P}}^m; V^{I_{\mathfrak{P}}})}{m\mathfrak{N}(\mathfrak{p})^{ms}} = \sum_{\mathfrak{p}}\frac{\chi(\mathrm{Frob}_{\mathfrak{p}}; V^{I_{\mathfrak{P}}})}{\mathfrak{N}(\mathfrak{p})^s} + O_{s\to 1^+}(1),$$

where we define $\chi(\mathrm{Frob}_{\mathfrak{P}}^m; V^{I_{\mathfrak{P}}}) = \operatorname{tr}\left(\rho|_{V^{I_{\mathfrak{P}}}}(\mathrm{Frob}_{\mathfrak{P}})\right)$. Using this expression we can, by comparing to $\log\zeta_K(s)$, show that $\mathcal{L}(L/K,\rho,s)$ converges absolutely and locally uniformly for $\mathrm{Re}\, s > 1$.

Example 5.13 *Recall the L-function $L(s) = \zeta_L(s)\zeta(s)^{-1}$ from Example 2. We can now identify it as*

$$L(s) = \mathcal{L}(H/\mathbb{Q}, \mathrm{St}, s),$$

where χ_{St} is the character of the standard representation of $\operatorname{Gal}(H/\mathbb{Q})\cong S_3$. Indeed we already checked that for the unramified primes $p\neq 23$ the local Euler factors $L_p(s)$ and $\mathcal{L}_p(H/\mathbb{Q},\mathrm{St},s)$ are equal, so it just remains to check

$$\mathcal{L}_{23}(H/\mathbb{Q},\mathrm{St},s) = (1-p^{-s})^{-1}.$$

The following proposition presents a relation between Artin L-series attached to representations of various Galois extensions. In particular, if ρ is trivial, it coincides with a Dedekind zeta function.

Theorem 5.14 (Artin formalism) *Let L/K be a Galois extension with Galois group $G = \operatorname{Gal}(L/K)$.*

(i) *For the trivial representation $\mathbf{1}$,*

$$\mathcal{L}(L/K,\mathbf{1},s) = \zeta_K(s)\,.$$

(ii) *If ρ, ρ' are two representations of* $\mathrm{Gal}(L/K)$*, then*

$$\mathcal{L}(L/K, \rho \oplus \rho', s) = \mathcal{L}(L/K, \rho, s)\mathcal{L}(L/K, \rho', s)\,.$$

(iii) *If $N \triangleleft G$ lies in* $\ker(\rho)$*, so that ρ induces a representation $\overline{\rho}$ of $G/N \cong$* $\mathrm{Gal}(L^N/K)$*. Then*

$$\mathcal{L}(L/K, \rho, s) = \mathcal{L}(L^N/K, \overline{\rho}, s)\,.$$

(iv) *If F is an intermediate field, $L \supseteq F \supseteq K$ with $H =$* $\mathrm{Gal}(L/F)$ *and τ is a representation of H, then*

$$\mathcal{L}(L/K, \mathrm{Ind}_H^G \tau, s) = \mathcal{L}(L/F, \tau, s)\,.$$

Proof.

(i) Clear.

(ii) Note that for two representations (ρ, V), (ρ', V') of $\mathrm{Gal}(L/K)$, the representation $(\rho \oplus \rho', V \oplus V')$ evaluated at $g \in \mathrm{Gal}(L/K)$ is given by a block diagonal matrix $\begin{pmatrix} \rho(g) & \\ & \rho'(g) \end{pmatrix}$. Hence,

$$\begin{aligned} &\det\left(1 - (\rho \oplus \rho')|_{(V \oplus V')^{I_{\mathfrak{P}}}}(\mathrm{Frob}_{\mathfrak{P}})\mathfrak{N}(\mathfrak{p})^{-s}\right) \\ &\qquad = \det\left(1 - \rho|_{V^{I_{\mathfrak{P}}}}(\mathrm{Frob}_{\mathfrak{P}})\mathfrak{N}(\mathfrak{p})^{-s}\right) \det\left(1 - \rho'|_{V'^{I_{\mathfrak{P}}}}(\mathrm{Frob}_{\mathfrak{P}})\mathfrak{N}(\mathfrak{p})^{-s}\right)\,. \end{aligned}$$

(iii) Let $\mathfrak{P}'|\mathfrak{P}|\mathfrak{p}$ be prime ideals of L, L^N and K respectively, each lying above the next, and let $h : G \to G/N$ be the natural projection. It suffices to prove that $h(\mathrm{Frob}_{\mathfrak{P}'}) = \mathrm{Frob}_{\mathfrak{P}}$ and $h : I_{\mathfrak{P}'/\mathfrak{p}} \to I_{\mathfrak{P}/\mathfrak{p}}$. This follows easily from the observation that $D_{\mathfrak{P}/\mathfrak{p}} = (D_{\mathfrak{P}'/\mathfrak{p}}N)/N$ and $I_{\mathfrak{P}/\mathfrak{p}} = (I_{\mathfrak{P}'/\mathfrak{p}}N)/N$.

(iv) Let $\mathfrak{s}'|\mathfrak{s}|\mathfrak{p}$ be prime ideals of L, F and K respectively, each lying above the next. We check the equality of Artin L-series for every Euler factor: by Proposition 5.10 and the fact that $\mathfrak{N}(\mathfrak{s}) = \mathfrak{N}(\mathfrak{p})^{f_{\mathfrak{s}/\mathfrak{p}}}$,

$$\begin{aligned} \mathfrak{N}(\mathfrak{p})^{s \dim \mathrm{Ind}_H^G(V)^{I_{\mathfrak{s}'/\mathfrak{p}}}} \mathcal{L}_{\mathfrak{p}}(L/K, \rho, s)^{-1} &= \mathrm{char}_{\mathfrak{p}}(\mathrm{Res}^G_{D_{\mathfrak{s}'/\mathfrak{p}}} \mathrm{Ind}_H^G \tau, \mathfrak{N}(\mathfrak{p})^s) \\ &= \prod_{\mathfrak{s}|\mathfrak{p}} \mathrm{char}_{\mathfrak{p}}\big(\mathrm{Res}^H_{D_{\mathfrak{s}'/\mathfrak{s}}} \tau, \mathfrak{N}(\mathfrak{p})^{s f_{\mathfrak{s}/\mathfrak{p}}}\big) \\ &= \mathfrak{N}(\mathfrak{p})^{s \sum_{\mathfrak{s}|\mathfrak{p}} f_{\mathfrak{s}/\mathfrak{p}} \dim V^{I_{\mathfrak{s}'/\mathfrak{s}}}} \prod_{\mathfrak{s}|\mathfrak{p}} \mathcal{L}_{\mathfrak{s}}(L/F, \tau, s)^{-1} \\ &= \mathfrak{N}(\mathfrak{p})^{s \dim \mathrm{Ind}_H^G(V)^{I_{\mathfrak{s}'/\mathfrak{p}}}} \prod_{\mathfrak{s}|\mathfrak{p}} \mathcal{L}_{\mathfrak{s}}(L/F, \tau, s)^{-1}. \end{aligned}$$

The equality $\sum_{\mathfrak{s}|\mathfrak{p}} f_{\mathfrak{s}/\mathfrak{p}} \dim V^{I_{\mathfrak{s}'/\mathfrak{s}}} = \dim \mathrm{Ind}_H^G(V)^{I_{\mathfrak{s}'/\mathfrak{p}}}$ follows automatically from the equality of characteristic polynomials in Proposition 5.10.

□

Corollary 5.15

$$\zeta_L(s) = \zeta_K(s) \prod_{\rho \neq \mathbf{1}} \mathcal{L}(L/K, \rho, s)^{\deg \rho}\,, \tag{24}$$

where the product runs over the non-trivial irreducible representations of $G = \mathrm{Gal}(L/K)$.

Proof. Note that $\mathrm{Ind}_{\{1\}}^G(\mathbf{1}) = \mathbb{C}[G]$ (exercise) and by (22) $\mathbb{C}[G] \cong \bigoplus_\rho \rho^{\deg(\rho)}$, where the sum is over all irreducible representations of G. By Theorem 5.14

$$\begin{aligned}\zeta_L(s) &= \mathcal{L}(L/L, \mathbf{1}, s) = \mathcal{L}(L/K, \mathrm{Ind}_{\{1\}}^G(\mathbf{1}), s)\\ &= \prod_\rho \mathcal{L}(L/K, \rho, s)^{\deg \rho} = \zeta_K(s) \prod_{\rho \neq \mathbf{1}} \mathcal{L}(L/K, \rho, s)^{\deg \rho}.\end{aligned}$$

□

Neukirch writes that "The starting point of Artin's investigations on L-series had been the question whether, for a Galois extension L/K, the quotient $\zeta_L(s)/\zeta_K(s)$ is an entire function, i.e., a holomorphic function on the whole complex plane." In fact, Artin conjectured

Conjecture 5.16 (Artin) *For every irreducible representation $\rho \neq \mathbf{1}$ of $\mathrm{Gal}(L/K)$, the Artin L-series $\mathcal{L}(L/K, \rho, s)$ defines an entire function.*

The simplest case of this conjecture is when L/K is an **abelian extension**, that is, when the Galois group $\mathrm{Gal}(L/K)$ is abelian.

Recall from section 1 and Example 4.2 that for an integral ideal $\mathfrak{m} = (m) \lhd \mathbb{Z}$ we have an isomorphism

$$J^{\mathfrak{m}}/P^{\mathfrak{m}} \cong (\mathbb{Z}/m\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})\,.$$

In this way generalized Dirichlet characters mod $\mathfrak{m}$ correspond to (classical Dirichlet characters mod m and further to) characters of $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. This correspondence can be extended to Dirichlet characters mod $\mathfrak{m}$ for any integral ideal $\mathfrak{m}$ in any number field K. As we will explain in more detail in Section 7, for any number field K and any $\mathfrak{m} \lhd \mathcal{O}_K$ there exists an abelian extension $K^{\mathfrak{m}}/K$, called **ray class field modulo $\mathfrak{m}$**, that is characterised by the property that the only primes that ramify in $K^{\mathfrak{m}}/K$ divide $\mathfrak{m}$, and the primes that split completely in $K^{\mathfrak{m}}/K$ are precisely those which are congruent to principal ideals in $P^{\mathfrak{m}}$. For this extension there is an isomorphism between $J^{\mathfrak{m}}/P^{\mathfrak{m}}$ and $\mathrm{Gal}(K^{\mathfrak{m}}/K)$ called the **Artin reciprocity law**, defined by

$$J^{\mathfrak{m}}/P^{\mathfrak{m}} \xrightarrow{\sim} \mathrm{Gal}(K^{\mathfrak{m}}/K)\,, \qquad \mathfrak{a} \bmod P^{\mathfrak{m}} \longmapsto \prod_{\mathfrak{p}} (\mathrm{Frob}_{\mathfrak{p}})^{\mathrm{ord}_{\mathfrak{p}} \mathfrak{a}}\,, \tag{25}$$

where $\mathfrak{p}$ varies over prime ideals in $\mathcal{O}_K$ and $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\operatorname{ord}_{\mathfrak{p}} \mathfrak{a}}$. The isomorphism (25) provides a correspondence between generalized Dirichlet characters mod $\mathfrak{m}$ and characters of the (abelian) Galois group $\operatorname{Gal}(K^{\mathfrak{m}}/K)$.

In fact, one can show that every abelian extension L/K is contained in a ray class field $K^{\mathfrak{m}}$ for some $\mathfrak{m} \lhd \mathcal{O}_K$. Then $L = (K^{\mathfrak{m}})^H$ for some subgroup $H \leq \operatorname{Gal}(K^{\mathfrak{m}}/K)$. Since every character of $\operatorname{Gal}(L/K) \cong \operatorname{Gal}(K^{\mathfrak{m}}/K)/H$ can be viewed as a character of $\operatorname{Gal}(K^{\mathfrak{m}}/K)$ that is trivial on H, we can also view characters of $\operatorname{Gal}(L/K)$ as generalised Dirichlet characters modulo $\mathfrak{m}$. Moreover, if $\mathfrak{m}$ is chosen to be minimal, then the primes that ramify in L are precisely those which divide $\mathfrak{m}$; we call such $\mathfrak{m}$ the **conductor** of L.

The next theorem describes a relation between the corresponding Hecke L-function and Artin L-series.

Theorem 5.17 *Let L/K be an abelian extension contained in a ray class field $K^{\mathfrak{m}}$, χ an irreducible character of $\operatorname{Gal}(L/K)$ and $\tilde{\chi}$ the associated Dirichlet character mod $\mathfrak{m}$, i.e., the character $\tilde{\chi}$ of $J^{\mathfrak{m}}/P^{\mathfrak{m}}$ defined by $\tilde{\chi}(\mathfrak{p}) := \chi(\operatorname{Frob}_{\mathfrak{p}})$. Then the Artin L-series for the character χ and the Hecke L-series for $\tilde{\chi}$ satisfy the identity*

$$\mathcal{L}(L/K, \chi, s) = \prod_{\mathfrak{p} \in S} \frac{1}{1 - \chi(\operatorname{Frob}_{\mathfrak{P}})\mathfrak{N}(\mathfrak{p})^{-s}} L(\tilde{\chi}, s)\,,$$

where $S = \{\mathfrak{p} | \mathfrak{m} : \chi(I_{\mathfrak{P}/\mathfrak{p}}) = 1\}$.

PROOF. We compare the Euler factors of the two L-series:

(1) If $\mathfrak{p} \nmid \mathfrak{m}$ we have
$$\mathcal{L}_{\mathfrak{p}}(L/K, \chi, s) = (1 - \chi(\operatorname{Frob}_{\mathfrak{p}})\mathfrak{N}(\mathfrak{p})^{-s})^{-1}$$
and
$$L_{\mathfrak{p}}(\tilde{\chi}, s) = (1 - \tilde{\chi}(\mathfrak{p})\mathfrak{N}(\mathfrak{p})^{-s})^{-1}$$
and so these Euler factors correspond by the definition of $\tilde{\chi}$.

(2) If $\mathfrak{p} \mid \mathfrak{m}$ and $\chi(I_{\mathfrak{P}/\mathfrak{p}}) = 1$, then the Euler factor $L_{\mathfrak{p}}(\tilde{\chi}, s)$ is 1, while the Euler factor $\mathcal{L}_{\mathfrak{p}}(L/K, \chi, s)$ equals $(1 - \chi(\operatorname{Frob}_{\mathfrak{p}})\mathfrak{N}(\mathfrak{p})^{-s})^{-1}$.

(3) If $\mathfrak{p} \mid \mathfrak{m}$ and $\chi(I_{\mathfrak{P}/\mathfrak{p}}) \neq 1$ the Euler factors $L_{\mathfrak{p}}(\tilde{\chi}, s)$ and $\mathcal{L}_{\mathfrak{p}}(L/K, \chi, s)$ are both 1.

□

Hence, whenever the set S is empty, the above theorem together with Theorem 4.10 on meromorphic continuation of Hecke L-series prove Artin's conjecture for abelian extensions. As we will see later the condition on $S = \emptyset$ translates precisely to the conditions on χ required by the conjecture.

We finish this section a very powerful corollary from the above theorem.

Corollary 5.18 *Let L/K be an abelian extension and χ a non-trivial character of $\mathrm{Gal}(L/K)$. Choose $\mathfrak{m}$ such that $L \subseteq K^{\mathfrak{m}}$ and let $\tilde{\chi}$ be the character of $J^{\mathfrak{m}}/P^{\mathfrak{m}}$ associated to χ. Then $\mathcal{L}(L/K, \chi, s)$ has holomorphic continuation to $\mathbb{C}$ and both $L(\tilde{\chi}, s)$ and $\mathcal{L}(L/K, \chi, s)$ do not vanish at $s = 1$.*

Proof. First note that the Hecke L-series $L(\tilde{\chi}, s)$ may be holomorphically continued to $\mathbb{C}$:

- if $\mathfrak{m} \neq 1$ or the infinity type $(p, 0)$ of $\tilde{\chi}$ is different than $(0, 0)$, this follows from Theorem 4.10;
- if $\mathfrak{m} = 1$ and $(p, 0) = (0, 0)$, then $\tilde{\chi}$ is in fact a character of the ideal class group Cl_K (see Example 4.7), and thus the hypothesis follows from Corollary 4.11.

Now we prove that this is also the case for the Artin L-series $\mathcal{L}(L/K, \chi, s)$. Let $L^{\ker \chi}$ be the fixed field of $\ker \chi$, so that by Artin formalism $\mathcal{L}(L/K, \chi, s) = \mathcal{L}(L^{\ker \chi}/K, \overline{\chi}, s)$. Let $\mathfrak{f}$ be the conductor of $L^{\ker \chi}/K$. Then $\overline{\chi}$ corresponds to a Hecke character $\tilde{\chi}_{\mathfrak{f}}$ on $J^{\mathfrak{f}}/P^{\mathfrak{f}}$. Since $\overline{\chi}$ is injective, the set S that appears in Lemma 5.2 is

$$S = \{\mathfrak{p} | \mathfrak{f} : \ \chi(I_{\mathfrak{P}/\mathfrak{p}}) = 1\} = \{\mathfrak{p} | \mathfrak{f} : \mathfrak{p} \text{ unramified}\} = \emptyset \, .$$

Hence by Theorem 5.17 $\mathcal{L}(L^{\ker \chi}/K, \overline{\chi}, s) = L(\tilde{\chi}_{\mathfrak{f}}, s)$, and the latter Hecke L-function is holomorphic.

By Corollary 5.15 and the fact that both ζ_K and ζ_L have a simple pole at $s = 1$ (Corollary 3.36), it follows that for every non-trivial character ψ of $\mathrm{Gal}(L/K)$, $\mathcal{L}(L/K, \psi, 1) \neq 0$ (note that a character being a degree 1 representation is automatically irreducible). Hence the same is the case for $L(\tilde{\chi}, 1)$. □

Using Artin formalism we can treat 1-dimensional representations of non-abelian Galois groups as well:

Corollary 5.19

(1) *Let L/K be a finite Galois extension and ρ be a 1-dimensional representation of $\mathrm{Gal}(L/K)$. Then $\mathcal{L}(L/K, \rho, s)$ extends to an entire function on $\mathbb{C}$ and does not vanish at $s = 1$.*

(2) *If L/K is an abelian extension, then $\zeta_L(s)/\zeta_K(s)$ extends to an entire function on $\mathbb{C}$ that does not vanish at $s = 1$.*

Proof.

(1) By Artin formalism $\mathcal{L}(L/K, \rho, s) = \mathcal{L}(L^{\ker \rho}/K, \overline{\rho}, s)$ and the extension $L^{\ker \rho}/K$ is abelian, since $\mathrm{Gal}(L^{\ker \rho}/K)$ is isomorphic to the image of ρ in $\mathbb{C}^{\times}$. Now we can apply Corollary 5.18.

(2) If $\mathrm{Gal}(L/K)$ is abelian, the second statement clearly follows from the first and Corollary 5.15, since all irreducible representations of the abelian group are 1-dimensional.

□

The above result is only a tip of the iceberg of the properties of the Artin L-series that can be deduced from the Hecke L-series thanks to the isomorphism (25). In order to extend Corollary 5.18 to Artin L-series associated to any non-trivial irreducible representation, we employ the following standard result from representation theory.

Theorem 5.20 (Brauer's induction theorem) *For every representation ρ of a finite group G there exist characters χ_i, ψ_j of some subgroups H_i, F_j of G and $a_i, b_j \in \mathbb{N}$ such that*

$$\oplus_i \operatorname{Ind}_{H_i}^{G} \chi_i^{a_i} \oplus \rho = \oplus_j \operatorname{Ind}_{F_j}^{G} \psi_j^{b_j} \,.$$

Moreover, if $(\chi_\rho, \chi_{\mathbf{1}}) = 0$, then χ_i, ψ_j can be chosen to be non-trivial.

Corollary 5.21 *Let (ρ, V) be a non-trivial irreducible representation of* $\mathrm{Gal}(L/K)$*. Then*

$$\mathcal{L}(L/K, \rho, 1) \neq 0\,.$$

Proof. By Artin formalism (Theorem 5.14) and Brauer theorem, there exist characters χ_i, ψ_j of some subgroups H_i, F_j of $\mathrm{Gal}(L/K)$ and $a_i, b_j \in \mathrm{N}$ such that

$$\mathcal{L}(L/K, \rho, s) = \frac{\prod_j \mathcal{L}(L/L^{F_j}, \psi_j, s)^{b_j}}{\prod_i \mathcal{L}(L/L^{H_i}, \chi_i, s)^{a_i}}\,.$$

In particular, by Corollary 5.18, the L-series $\mathcal{L}(L/K, \rho, s)$ admits meromorphic continuation to $\mathbb{C}$ and is well-defined at $s = 1$. Moreover, $\mathcal{L}(L/K, \rho, 1) \neq 0$. □

CHAPTER 6

The Chebotarev Density Theorem

Let $K \subset L$ be a Galois extension and $\mathfrak{p}$ be a prime ideal in K. Recall that a conjugacy class of a group G has the form $\mathcal{C}_h = \{g^{-1}hg : g \in G\}$ for some $h \in G$. By Lemma 5.1 the conjugacy class in $\mathrm{Gal}(L/K)$ of $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$ is independent of the choice of a prime $\mathfrak{q}$ above $\mathfrak{p}$. For a conjugacy class $\mathcal{C} \subset \mathrm{Gal}(L/K)$ we define the set

$$P_{L/K}(\mathcal{C}) = \{\mathfrak{p} \lhd \mathcal{O}_K : \mathfrak{p} \text{ unramified}, \forall_{\mathfrak{q}|\mathfrak{p}} \, \mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}} \in \mathcal{C}\}.$$

Dirichlet's theorem 3.42 can be restated as follows. For any $m \geq 1$ and a with $\gcd(a, m) = 1$ the set $P_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\{a\})$ has Dirichlet density $\frac{1}{\phi(m)}$. This is a special case of:

Theorem 6.1 (Chebotarev Density Theorem, 1922) *Let $K \subset L$ be a Galois extension and $\mathcal{C} \subset \mathrm{Gal}(L/K)$ be a conjugacy class. Then the Dirichlet density of $P_{L/K}(\mathcal{C})$ is given by*

$$d(P_{L/K}(\mathcal{C})) = \frac{\#\mathcal{C}}{\#\,\mathrm{Gal}(L/K)}.$$

Proof. Let $I_{\mathcal{C}} : \mathrm{Gal}(L/K) \to \{0, 1\}$ be the characteristic function of $\mathcal{C}$, i.e. $I_{\mathcal{C}}(g) = 1$ if and only if $g \in \mathcal{C}$. Since $I_{\mathcal{C}}$ is a class function, it can be written as a linear combination of irreducible characters (see Fact 5.6): $I_{\mathcal{C}} = \sum_\rho c_\rho \chi_\rho$. We have

$$c_{\mathbf{1}} = (I_{\mathcal{C}}, \mathbf{1}) = \frac{\#\mathcal{C}}{\#\,\mathrm{Gal}(L/K)}.$$

For $\mathrm{Re}\, s > 1$,

$$\begin{aligned}\sum_{\substack{\mathfrak{p} \lhd \mathcal{O}_K \\ \mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}} \in \mathcal{C}}} \mathfrak{N}(\mathfrak{p})^{-s} &= \sum_{\mathfrak{p} \lhd \mathcal{O}_K} I_{\mathcal{C}}(\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}) \mathfrak{N}(\mathfrak{p})^{-s} = \sum_\rho c_\rho \sum_{\mathfrak{p} \lhd \mathcal{O}_K} \chi_\rho(\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}) \mathfrak{N}(\mathfrak{p})^{-s} \\ &= \frac{\#\mathcal{C}}{\#\,\mathrm{Gal}(L/K)} \sum_{\mathfrak{p} \lhd \mathcal{O}_K} \mathfrak{N}(\mathfrak{p})^{-s} + \sum_{\rho \neq \mathbf{1}} c_\rho \sum_{\mathfrak{p} \lhd \mathcal{O}_K} \chi_\rho(\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}) \mathfrak{N}(\mathfrak{p})^{-s}.\end{aligned}$$

Now, by Remark 5.12, for $\rho \neq \mathbf{1}$,

$$\sum_{\mathfrak{p} \lhd \mathcal{O}_K} \chi_\rho(\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}) \mathfrak{N}(\mathfrak{p})^{-s} + \sum_{\mathfrak{p} \lhd \mathcal{O}_K} \sum_{m \geq 2} \frac{\chi_\rho(\mathrm{Frob}^m_{\mathfrak{q}/\mathfrak{p}})}{m \mathfrak{N}(\mathfrak{p})^{ms}} = \log \mathcal{L}(L/K, \rho, s)\,,$$

where the second sum is absolutely convergent for $\operatorname{Re} s \geq 1/2$ (recall that there are at most $n = [K : \mathbb{Q}]$ primes $\mathfrak{p}$ above every $p \in \mathbb{P}$ and $\mathfrak{N}(\mathfrak{p}) = p^{f_{\mathfrak{p}/p}} \geq p$). By Corollary 5.21, $|\log \mathcal{L}(L/K, \rho, 1)| < \infty$ and thus the sum over $\rho \neq \mathbf{1}$ converges as $s \to 1^+$. Since there are only finitely many primes $\mathfrak{p}$ which ramify, this finishes the proof. □

Corollary 6.2 *Let $f \in \mathbb{Z}[X]$ be a monic irreducible polynomial of degree n and $\operatorname{Gal}(f) \leq S_n$ the Galois group of its splitting field. Then the set of primes p such that $f \bmod p$ factors as a product of irreducible polynomials of degrees $d_1, \dots, d_r$ has Dirichlet density*

$$\frac{\#\{g \in \operatorname{Gal}(f) : g \text{ has cycle type } (d_1, \dots, d_r) \text{ on the roots of } f\}}{\# \operatorname{Gal}(f)}.$$

Proof. Let $\mathbb{Q}(f)$ be the splitting field of f. Since only finitely many primes ramify in $\mathbb{Q}(f)$ and this is a question about densities, we can restrict our attention to unramified primes. By Proposition 5.3, the unramified primes p for which $f \bmod p$ factors as a product of irreducible polynomials of degrees $d_1, \dots, d_r$ are precisely the primes whose Frobenius element has cycle type $(d_1, \dots, d_r)$. The density of primes with Frobenius element in this conjugacy class is given in Theorem 6.1. □

We can now prove the statements made in Remark 3.46.

Corollary 6.3 *Let $f \in \mathbb{Z}[X]$ be a monic irreducible polyonomial of degree $\deg f > 1$ and $\mathbb{Q}(f)$ its splitting field. Then*

(1) *The Dirichlet density of primes such that f decomposes into linear factors modulo p is $\frac{1}{[\mathbb{Q}(f):\mathbb{Q}]}$.*
(2) *The Dirichlet density of primes such that f has no roots modulo p is greater than 0.*

Proof. Let $\operatorname{Gal}(f)$ be the Galois group of $\mathbb{Q}(f)$.

(1) By Proposition 5.3 the set of unramified primes such that f decomposes into linear factors is equal to the set of primes with trivial Frobenius element in $\mathbb{Q}(f)/\mathbb{Q}$. The Dirichlet density of these primes is given by $\frac{1}{\# \operatorname{Gal}(f)} = \frac{1}{[\mathbb{Q}(f):\mathbb{Q}]}$.
(2) Let p be unramified in $\mathbb{Q}(f)/\mathbb{Q}$. If p is unramified, the polynomial $f \bmod p$ has no roots in $\mathbb{F}_p$ if and only if no root of f in $\mathbb{Q}(f)$ is fixed by a Frobenius element of p. Hence, we need to find an element $g \in \operatorname{Gal}(f)$ that fixes no roots of f. If such an element of $\operatorname{Gal}(f)$ exists, Theorem 6.1 guarantees that the set of primes with Frobenius element fixing no root of f has a positive Dirichlet density. For a root α of f let

$$\operatorname{Stab}_{\operatorname{Gal}(f)}(\alpha) = \{\sigma \in \operatorname{Gal}(f) : \sigma(\alpha) = \alpha\}$$

be the stabiliser subgroup of α. By the orbit-stabiliser theorem $\#\mathrm{Stab}_{\mathrm{Gal}(f)}(\alpha) = \frac{\#\,\mathrm{Gal}(f)}{\deg f}$. Since every stabiliser subgroup contains the identity element and there is more than one root of f

$$\#\left(\bigcup_{\alpha \text{ a root of } f} \mathrm{Stab}_{\mathrm{Gal}(f)}(\alpha)\right) < \deg(f)\frac{|\,\mathrm{Gal}(f)|}{\deg(f)}.$$

Hence there is an element in $\mathrm{Gal}(f) \setminus \bigcup_{\alpha \text{ a root of } f} \mathrm{Stab}_{\mathrm{Gal}(f)}(\alpha)$.

□

Definition 6.4 *For an extension L/K of number fields, we define*

$$\mathrm{Split}(L/K) := \{\mathfrak{p} \lhd \mathcal{O}_K : \exists_{\mathfrak{P}|\mathfrak{p}}\, f_{\mathfrak{P}/\mathfrak{p}} = 1\}.$$

If L/K is Galois, $\mathrm{Split}(L/K)$ is just the set of primes of K that split completely in L. In the following we will use the signs $\overset{\text{almost all}}{=}$ and $\overset{\text{almost all}}{\subseteq}$ to mean 'equality up to finitely many primes' and 'containment up to finitely many primes'. The following theorem is an important consequence of Chebotarev's density theorem:

Theorem 6.5 *Let L/K be finite Galois and F/K an aribtrary finite extension of K. Then*

$$\mathrm{Split}(F/K) \overset{\text{almost all}}{\subseteq} \mathrm{Split}(L/K) \Leftrightarrow L \subseteq F.$$

Before we prove this theorem we need a Lemma on the sets $\mathrm{Split}(L/K)$:

Lemma 6.6 *Let $K \subseteq F \subseteq L$ be finite extensions of K with L/K Galois and set $\mathrm{Gal}(L/F) = H \leq G = \mathrm{Gal}(L/K)$. Then*

$$\mathrm{Split}(F/K) \overset{\text{almost all}}{=} \bigsqcup_{\substack{\mathcal{C}_\sigma \subseteq G \\ C_\sigma \cap H \neq \emptyset}} P_{L/K}(\mathcal{C}_\sigma).$$

Proof. An unramified prime $\mathfrak{p}$ (in the extension L/K) of K lies in $\mathrm{Split}(F/K)$ if there exists $\mathfrak{P} \lhd \mathcal{O}_F$ with $\mathfrak{P}|\mathfrak{p}$ and $f_{\mathfrak{P}/\mathfrak{p}} = 1$. This is equivalent to saying $\mathcal{O}_F/\mathfrak{P} = \mathcal{O}_K/\mathfrak{p}$. Let $\mathfrak{P}'$ be a prime of L above $\mathfrak{P}$. This is equivalent to $\mathrm{Frob}_{\mathfrak{P}'/\mathfrak{p}} = \mathrm{Frob}_{\mathfrak{P}'/\mathfrak{P}} \in H$ for any prime $\mathfrak{P}'$ of L above $\mathfrak{P}$. This is equivalent to the conjugacy class $\mathcal{C}_{\mathrm{Frob}_{\mathfrak{P}'/\mathfrak{p}}}$ having non-empty intersection with H and $\mathfrak{p} \in P_{L/K}(\mathrm{Frob}_{\mathfrak{P}'/\mathfrak{p}})$. This argument started with the assumption that $\mathfrak{p}$ is an unramified prime of L/K, so it is valid for almost all primes of K. □

Proof of Theorem 6.5. Let M be a Galois extension that contains both L and F:

$$\begin{tikzcd}
 & M \arrow[dl, dash, "N = \mathrm{Gal}(M/L)"'] \arrow[dr, dash, "H = \mathrm{Gal}(M/F)"] \arrow[dd, dash, "\mathrm{Gal}(M/K)"'] & \\
L \arrow[dr, dash, "\mathrm{Gal}(L/K)"'] & & F \arrow[dl, dash] \\
 & K &
\end{tikzcd}$$

By Galois theory the statement $L \subseteq F$ is equivalent to $H \leq N$, so we need to show that $\mathrm{Split}(F/K) \overset{\text{almost all}}{\subseteq} \mathrm{Split}(L/K)$ is equivalent to $H \leq N$.

By Lemma 6.6

$$\mathrm{Split}(F/K) \overset{\text{almost all}}{=} \bigsqcup_{\substack{\mathcal{C}_\sigma \subseteq \mathrm{Gal}(M/K) \\ \mathcal{C}_\sigma \cap H \neq \emptyset}} P_{M/K}(\mathcal{C}_\sigma).$$

$$\mathrm{Split}(L/K) \overset{\text{almost all}}{=} \bigsqcup_{\substack{\mathcal{C}_\sigma \subseteq \mathrm{Gal}(M/K) \\ \mathcal{C}_\sigma \cap N \neq \emptyset}} P_{M/K}(\mathcal{C}_\sigma).$$

By Chebotarev's density theorem each of the sets $P_{M/K}(\mathcal{C}_\sigma)$ contains infinitely many elements. So $\mathrm{Split}(F/K) \overset{\text{almost all}}{\subseteq} \mathrm{Split}(L/K)$ is equivalent to

$$\begin{aligned} &\forall \mathcal{C}_\sigma \subseteq \mathrm{Gal}(M/K),\, \mathcal{C}_\sigma \cap H \neq \emptyset \Rightarrow \mathcal{C}_\sigma \cap N \neq \emptyset \\ \Leftrightarrow\ &\forall \mathcal{C}_\sigma \subseteq \mathrm{Gal}(M/K),\, \mathcal{C}_\sigma \cap H \neq \emptyset \Rightarrow \sigma \in N. \end{aligned}$$

The last step follows because $N = \mathrm{Gal}(M/L)$ is a normal subgroup of $\mathrm{Gal}(M/K)$. Any conjugacy class $\mathcal{C}_\sigma$ with non-empty intersection with H is equal to $\mathcal{C}_h$ for an element $h \in H$. Hence finally we conclude that $\mathrm{Split}(F/K) \overset{\text{almost all}}{\subseteq} \mathrm{Split}(L/K)$ is equivalent to $H \leq N$. □

CHAPTER 7

Class field theory

Let K be a number field, $\mathfrak{m} \lhd \mathcal{O}_K$, $J^{\mathfrak{m}}$ and $P^{\mathfrak{m}}$ the groups of fractional and principal ideals of K mod $\mathfrak{m}$ as in Definition 4.1.

Definition 7.1 *A* ***congruence subgroup*** *H for $\mathfrak{m}$ is a subgroup of $J^{\mathfrak{m}}$ containing $P^{\mathfrak{m}}$. An extension L/K is a* ***class field*** *for $(\mathfrak{m}, H)$ if the primes $\mathfrak{p} \nmid \mathfrak{m}$ of K that split completely in L are exactly those that lie in H. If $H = P^{\mathfrak{m}}$, we call such an extension a* ***ray class field modulo*** *$\mathfrak{m}$ and denote it by $K^{\mathfrak{m}}$.*

Example 7.2 *If $K = \mathbb{Q}$, $\mathfrak{m} = (m) \lhd \mathbb{Z}$ and $H = P^{\mathfrak{m}} = \{\alpha\mathbb{Z} : \alpha \equiv 1 \pmod{m}\}$, then a class field for $(\mathfrak{m}, H)$ is $\mathbb{Q}(\mu_m)$, where μ_m is a primitive m-th root of unity (see the proof of Proposition 3.38 or G2 in Exercise sheet 4).*

The following theorem summarizes most important results in class field theory, some of which were used in section 5. Unfortunately we don't have time to prove it.

Theorem 7.3 (Artin, Takagi)

(i) *Every finite abelian extension L/K is a class field for some $(\mathfrak{m}, H)$.*

(ii) *Every $(\mathfrak{m}, H)$ has a unique class field L. Moreover L is abelian over K.*

(iii) *Among $(\mathfrak{m}, H)$ in (i) there is a minimal one, in the sense that other $(\mathfrak{m}', H')$ have $\mathfrak{m}|\mathfrak{m}'$. The minimal modulus $\mathfrak{m}$ is called the* ***conductor*** *of L/K. The primes that ramify in L/K are precisely those that divide the conductor.*

(iv) ***Artin Reciprocity Law****: If L/K is a class field for $(\mathfrak{m}, H)$, then the Artin map*

$$\varphi : J^{\mathfrak{m}}/P^{\mathfrak{m}} \to \mathrm{Gal}(L/K), \qquad \varphi(\mathfrak{p}) := \mathrm{Frob}_{\mathfrak{p}}$$

is a surjective homomorphism with kernel H. (Note that since L/K is abelian, the Frobenius $\mathrm{Frob}_{\mathfrak{p}}$ is independent of the choice of $\mathfrak{P}|\mathfrak{p}$; see Remark 5.4.)

Corollary 7.4 (Kronecker, Weber) *Every finite abelian extension $L/\mathbb{Q}$ is contained in some cyclotomic extension $\mathbb{Q}(\mu_m)/\mathbb{Q}$.*

Proof. By Theorem 7.3, every finite abelian extension $L/\mathbb{Q}$ is a class field for some $(\mathfrak{m}, H)$, and every such H - by definition - contains $P^{\mathfrak{m}}$. Hence $\mathrm{Gal}(L/\mathbb{Q}) \cong (J^{\mathfrak{m}}/P^{\mathfrak{m}})/H$ is a subgroup of $J^{\mathfrak{m}}/P^{\mathfrak{m}} \cong \mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q})$, and thus $L \subseteq \mathbb{Q}(\mu_m)$. □

Of particular interest are a ray class field $K^{\mathcal{O}_K}$ and a class field $K_{\mathcal{O}_K}$ for $(\mathcal{O}_K, P_K)$, called **big Hilbert class field** and **(small) Hilbert class field** respectively, as then by Theorem 7.3 the Galois groups over K are isomorphic to the ray class group mod $\mathcal{O}_K$(called the **narrow class group**) and the ideal class group respectively:

$$\mathrm{Gal}(K^{\mathcal{O}_K}/K) \cong \mathrm{Cl}^{\mathcal{O}_K} \qquad \text{and} \qquad \mathrm{Gal}(K_{\mathcal{O}_K}/K) \cong \mathrm{Cl}_K\,.$$

The Hilbert class field $K_{\mathcal{O}_K}$ is a maximal subfield of $K^{\mathcal{O}_K}$ such that every real embedding of $K_{\mathcal{O}_K}$ extends to a real embedding of $K^{\mathcal{O}_K}$. In particular, if K is a totally imaginary extension of $\mathbb{Q}$, then $K^{\mathcal{O}_K} = K_{\mathcal{O}_K}$.

Example 7.5 *Recall the example 2:*

$$\begin{tikzcd}
 & H \arrow[dl, dash, "C_3"'] \arrow[dr, dash, "C_2"] \arrow[dd, dash, "S_3"] & \\
K = \mathbb{Q}(\sqrt{-23}) \arrow[dr, dash, "C_2"'] & & L \arrow[dl, dash, "\textit{degree } 3"] \\
 & \mathbb{Q} &
\end{tikzcd}$$

We showed that the only rational prime which ramifies in H is $p = 23$ and its ramification degree is 2. Since p also ramifies in K, the extension H/K is unramified and thus H is the big Hilbert class field for K. Moreover, since K is an imaginary extension of $\mathbb{Q}$, we also have

$$C_3 \cong \mathrm{Gal}(H/K) \cong \mathrm{Cl}_K\,.$$

CHAPTER 8

Modular forms and irreducible 2-dimensional Galois representations

In Corollary 5.19 we saw that for 1-dimensional representations Artin's conjecture 5.16 holds. This is essentially because by class field theory these Artin L-functions correspond to Hecke L-functions. The next case to study is Artin's conjecture for irreducible 2-dimensional Galois representations. In this case Artin's conjecture is still open, however much progress has been made in the 20th and 21st century. The idea was to relate Artin L-series to L-functions of modular forms.

Below we define modular forms and explain their properties in a very concise way, just so that we are able to relate them to Artin L-series. Therefore the reader should consult other sources, e.g. [1] or [3], for further explanation.

Let $N \in \mathbb{Z}_{>0}$, χ a Dirichlet character mod N and

$$\Gamma_0(N) := \{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : N | c \} \,.$$

Note that we can view the character χ as a character of the group $\Gamma_0(N)$ by setting $\chi(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)) := \chi(d)$.

Definition 8.1 *Let $f\colon \mathbb{H} \to \mathbb{C}$ be a holomorphic function on the complex upper half-plane and $k \in \mathbb{Z}_{\geq 0}$. For $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{R})$ with $\det g > 0$ we define*

$$f|_k g\,(\tau) := (\det g)^{k/2}(c\tau + d)^{-k} f\left(\frac{a\tau + b}{c\tau + d}\right), \ \tau \in \mathbb{H}\,. \tag{26}$$

*We say that f is a **modular form of weight k, character χ and level N** if*

$$f|_k\gamma = \chi(\gamma) f \quad \text{for all} \quad \gamma \in \Gamma_0(N) \tag{27}$$

and for every $g \in \mathrm{SL}_2(\mathbb{Z})$ there exists $t \in \mathbb{Z}_{>0}$ such that $f|_k g$ has a Fourier expansion

$$f|_k g\,(\tau) = \sum_{n=0}^{\infty} a_g(n) e^{2\pi i n \tau/t}\,, \qquad a_g(n) \in \mathbb{C}\,. \tag{28}$$

*We denote the space of such functions by $\mathcal{M}_k(\Gamma_0(N), \chi)$. We say that $f \in \mathcal{M}_k(\Gamma_0(N), \chi)$ is **cuspidal** (or a **cusp form**) if in equation (28) $a_g(0) = 0$ for all $g \in \mathrm{SL}_2(\mathbb{Z})$; we denote the subspace of cusp forms by $\mathcal{S}_k(\Gamma_0(N), \chi)$.*

Remark 8.2

(1) *Note that the action of* $\mathrm{GL}_2(\mathbb{R})^+ := \{g \in \mathrm{GL}_2(\mathbb{R}) : \det g > 0\}$ *on* f *in equation* (26) *is well-defined: for* $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{R})^+$ *and* $\tau \in \mathbb{H}$,

$$g \cdot \tau := \frac{a\tau + b}{c\tau + d} \in \mathbb{H}\,.$$

Moreover for $g, h \in \mathrm{GL}_2(\mathbb{R})^+$,

$$f|_k gh = f|_k g|_k h\,.$$

(2) *The condition* (28) *means that* f *is holomorphic at cusps of* $\Gamma_0(N)$. *See also* [3, section 1.2].

(3) *Every modular form* $f \in \mathcal{M}_k(\Gamma_0(N), \chi)$ *admits a Fourier expansion*

$$f(\tau) = \sum_{n=0}^{\infty} a(n) e^{2\pi i n \tau}\,.$$

Below we write $q := e^{2\pi i \tau}$, $\tau \in \mathbb{H}$.

(4) *It easily follows from* (27) *that the space* $\mathcal{M}_k(\Gamma_0(N), \chi)$ *is non-zero only if* $\chi(-1) = (-1)^k$.

Example 8.3 *A square of the theta function* $\theta(\tau) = \sum_{n\in\mathbb{Z}} e^{\pi i n^2 \tau}$ *is a modular form:* $\theta^2 \in \mathcal{M}_1(\Gamma_0(4), \chi)$, *where* χ *is the unique non-trivial Dirichlet character mod* 4. *In fact,* $\theta(\tau)$ *is a modular form of weight* $\frac{1}{2}$.

For a fixed N and k, with varying character χ, the space of modular forms of weight k and level N is finite dimensional. If we restrict to cuspidal modular forms, it is a Hilbert space with the **Petersson inner product** given by

$$\langle f, g \rangle := \int_{\Gamma_0(N)\backslash\mathbb{H}} f(\tau)\overline{g(\tau)} \mathrm{Im}\,(\tau)^k \frac{d\tau}{\mathrm{Im}\,(\tau)^2}\,.$$

In fact, this inner product also makes sense if one of the modular forms is not cuspidal.

Every space $\mathcal{M}_k(\Gamma_0(N), \chi)$ enjoys the action of **Hecke operators**. The ones of particular interest are the operators

$$T_p := \Gamma_0(N) \left(\begin{smallmatrix} 1 & \\ & p \end{smallmatrix}\right) \Gamma_0(N) = \bigsqcup_i \Gamma_0(N)\alpha_i\,,$$

where $p \in \mathbb{P}$ (is usually coprime to the level N) and α_i's are coset representatives (finitely many). They act on $f \in \mathcal{M}_k(\Gamma_0(N), \chi)$ according to the rule (26):

$$f|_k T_p := \sum_i f|_k \alpha_i\,.$$

One can show that this action is independent of the choice of α_i and takes cusp forms to cusp forms. In fact the Hecke operators T_p are a commuting family of operators which, when $\gcd(p,N)=1$, are normal with respect to $\langle\ ,\ \rangle$. Hence by the spectral theorem, the space $\mathcal{S}_k(\Gamma_0(N),\chi)$ admits a basis consisting of functions which are simultaneous eigenfunctions for all the T_p with $\gcd(p,N)=1$. In case $\gcd(p,N)\neq 1$, the operators T_p are not necessarily normal and thus the spectral theorem does not apply. If $f\in\mathcal{S}_k(\Gamma_0(N),\chi)$ is an eigenform of all the Hecke operators T_p with $\gcd(p,N)=1$, we call it a **Hecke eigenform**. Knowing explicit representatives α_i for the T_p operators, it is easy to show that Fourier coefficients of Hecke eigenforms with eigenvalues λ_p satisfy relations

$$a(np)+\chi(p)p^{k-1}a\left(n/p\right)=\lambda_p a(n)\,,\qquad \gcd(p,N)=1 \tag{29}$$

where we set $a\left(n/p\right):=0$ if $p\nmid n$.

If we restrict $\mathcal{S}_k(\Gamma_0(N),\chi)$ to the so-called new space $\mathcal{S}_k(\Gamma_0(N),\chi)^{\mathrm{new}}$, then we can find a basis consisting of eigenforms of *all* the Hecke operators. The **new space** is defined as the orthogonal complement of $\mathcal{S}_k(\Gamma_0(N),\chi)^{\mathrm{old}}$ with respect to $\langle\ ,\ \rangle$, where $\mathcal{S}_k(\Gamma_0(N),\chi)^{\mathrm{old}}$ is the space of **oldforms** defined by

$$\mathcal{S}_k(\Gamma_0(N),\chi)^{\mathrm{old}}:=\{g(D\tau): g\in\mathcal{S}_k(\Gamma_0(M),\psi), M|N, D|\frac{N}{M}\},$$

where ψ is a Dirichlet character modulo M that induces χ. We have

$$\mathcal{S}_k(\Gamma_0(N),\chi)=\mathcal{S}_k(\Gamma_0(N),\chi)^{\mathrm{new}}\oplus\mathcal{S}_k(\Gamma_0(N),\chi)^{\mathrm{old}}.$$

A Hecke eigenform in $f\in\mathcal{S}_k(\Gamma_0(N),\chi)^{\mathrm{new}}$ satisfies $a(1)\neq 0$ and, normalising it so that $a(1)=1$, we call such a form a **newform**. A newform is automatically also an eigenform of the Hecke operators T_p for $p\mid N$. From (29) it follows that $a(p)$ equals λ_p, the eigenvalue of f under T_p. Moreover, since the Hecke operators are commutative, the Fourier coefficients of Hecke eigenforms are multplicative. At $p|N$ we have

$$a(np)=\lambda_p a(n)\ \text{ if } p\nmid n,\qquad\text{and}\qquad a(pn)=0\ \text{ otherwise}\,.$$

For $f=\sum_{n=0}^{\infty}a(n)q^n\in\mathcal{M}_k(\Gamma_0(N),\chi)$ we define the L-series

$$L(f,s):=\sum_{n=1}^{\infty}\frac{a(n)}{n^s}.$$

This series converges for $\operatorname{Re}s>k$ by the estimate $a(n)=O(n^{k+1})$. Now let $W_N=\left(\begin{smallmatrix}0&-1\\N&0\end{smallmatrix}\right)$ and consider $g:=f|W_N=\sum_{n=0}^{\infty}b(n)q^n$. It is easy to show that $g\in\mathcal{M}_k(\Gamma_0(N),\overline{\chi})$, and thus by the Mellin principle the completed L-function

$$\Lambda(f,s):=N^{s/2}(2\pi)^{-s}\Gamma(s)L(f,s)$$

has meromorphic continuation to $\mathbb{C}$ and satisfies the functional equation

$$\Lambda(f,s)=i^k\Lambda(g,k-s)$$

with (possibly) simple poles at $s = 0$ and $s = k$ of residues a_0 and $-b_0$ respectively. If f is a newform, then $L(f, s)$ may be written as an Euler product

$$L(f,s) = \prod_{p \in \mathbb{P}} \frac{1}{1 - a(p)p^{-s} + \chi(p)p^{k-1-2s}}.$$

It turns out that in the case $k = 1$ these L-functions are closely related to Artin L-functions.

Definition 8.4 *Let ρ be a representation of a finite Galois group $\mathrm{Gal}(L/K)$.*

(1) *We say that the* ***represenation*** *ρ is* ***unramified*** *at $\mathfrak{p} \lhd \mathcal{O}_K$ if $\rho|_{I_\mathfrak{p}}$ is trivial.*
(2) *The representation ρ is* ***odd*** *if for any embedding of L into $\mathbb{C}$ and the corresponding automorphism $c \in \mathrm{Gal}(L/K)$ induced by the complex conjugation, $\det(\rho(c)) = -1$.*

Theorem 8.5 (Deligne–Serre, 1974) *Let $f \in \mathcal{M}_1(\Gamma_0(N), \chi)$ be a Hecke eigenform. Then there exists a number field K and an odd Galois representation*

$$\rho_f : \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C})$$

that is unramified at every $p \nmid N$, and for all $p \nmid N$ satisfies $\mathrm{tr}(\rho_f(\mathrm{Frob}_p)) = a(p)$ and $\det(\rho_f(\mathrm{Frob}_p)) = \chi(p)$. Moreover ρ_f is irreducible if f is cuspidal.

By Chebotarev's density theorem ρ_f is uniquely determined up to isomorphism by the condition $\mathrm{tr}(\rho_f(\mathrm{Frob}_p)) = a(p)$ for $p \nmid N$.

Exercise 8.6 *For primitive Dirichlet characters ϕ, ψ of modulo N_1, N_2 with $\phi(-1)\psi(-1) = -1$ we define Eisenstein series*

$$E_1^{\phi,\psi} = \frac{1}{2}(\delta(\phi)L(\psi,0) + \delta(\psi)L(\phi,0)) + \sum_{n\geq 1}\left(\sum_{m|n}\phi(m)\psi(n/m)\right)q^n,$$

where $\delta(\phi) = 1$ if $\phi = \mathbf{1}$ and zero otherwise, similarly for $\delta(\psi)$. One can show that $E_1^{\phi,\psi} \in \mathcal{M}_1(\Gamma_0(N_1N_2), \phi\psi)$ are Hecke eigenforms with Fourier coefficients $a(p) = \phi(p) + \psi(p)$ for every $p \nmid N_1N_2$. Hence by Theorem 8.5 there should be a representation ρ of a finite Galois group with $\mathrm{tr}(\rho(\mathrm{Frob}_p)) = a(p)$ for all $p \nmid N_1N_2$. Find it!

Example 8.7 *The modular form*

$$f_{23} = \eta(\tau)\eta(23\tau) = q\prod_{n\geq 1}(1-q^n)(1-q^{23n})$$

is a Hecke eigenform in $\mathcal{M}_1(\Gamma_0(23), \chi)$ for some Dirichlet character modulo 23. We showed numerically in the exercise classes that the Galois representation $\mathrm{St} : \mathrm{Gal}(H/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C})$ from example 2 has the same L-function as f_{23}.

Fairly recently the converse of Theorem 8.5 was proved:

Theorem 8.8 (Khare-Wintenberger, Kisin, 2004-2006) *Let $\rho : \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C})$ be an odd, irreducible representation. Then there exists a cuspidal Hecke eigenform $f \in \mathcal{M}_1(\Gamma_0(N), \chi)$ of some level N and character χ such that $\rho \cong \rho_f$. In particular $\mathcal{L}(K/\mathbb{Q}, \rho, s)$ is entire.*

Bibliography

[1] D. Bump, *Automorphic forms and representations*, Cambridge University Press, Cambridge, 1998.

[2] H. Cohen, *Number theory. Volume II: Analytic and modern tools*, Graduate Texts in Mathematics, 240. Springer, New York, 2007.

[3] F. Diamond, J. Shurman, *A First Course in Modular Forms*, Graduate Texts in Mathematics, 228. Springer, New York, 2005.

[4] D. Goldfeld, *The Elementary Proof of the Prime Number Theorem: An Historical Perspective*. In: Number Theory. Springer, New York, 2004. Also available at https://www.math.columbia.edu/ goldfeld/ErdosSelbergDispute.pdf

[5] J. Neukirch, *Algebraic number theory*, Springer-Verlag, Berlin, 1999.

[6] K. Prachar, *Primzahlverteilung*, Springer Verlag, Berlin, 1978.

[7] N. Snyder, *Artin's L-functions: a historical approach*, thesis available at https://pdfs.semanticscholar.org/36c9/f39a44e13ec1a04cbc673e7d8c29ca5859f2.pdf