Tate's Thesis

Warwick Number Theory Study Group

May 21, 2023

List of Talks:

§1 Talk 1: Introduction and Overview (Speaker: Arshay Sheth)

Tate's thesis is John Tate's 1950 PhD thesis written under the supervision of Emil Artin at Princeton University. Building on the work of Margaret Matchett, Artin's previous student, Tate gave a powerful approach to understand certain aspects of L-functions. Before explaining the main ideas of Tate's thesis, we first give a short overview on L-functions to understand the broader context in which Tate's Thesis fits.

§1.1 Background on L-functions

The simplest example of an L-function is the Riemann zeta function.

Definition 1.1. The Riemann zeta function is defined for all $s \in \mathbb{C}$ with $\operatorname{Re}(s) > 1$ by

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = 1^{-s} + 2^{-s} + 3^{-s} + 4^{-s} + \cdots$$

The Riemann zeta function satisfies three key properties: it has an Euler product, a functional equation and an analytic continuation to the whole complex plane (with a simple pole at $s = 1$). We briefly explain each of these three properties.

The Euler product of $\zeta(s)$ is an analytic way to reflect the fact that every natural number can be written uniquely as a product of prime numbers.

Theorem 1.2 (Euler, 1737)

We have that

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

Proof.

$$\begin{aligned}\prod_p (1-p^{-s})^{-1} &= (1-2^{-s})^{-1}(1-3^{-s})^{-1}(1-5^{-s})^{-1}\cdots \\ &= (1+2^{-s}+4^{-s}+\cdots)(1+3^{-s}+9^{-s}+\cdots)(1+5^{-s}+25^{-s}+\cdots)\cdots \\ &= 1^{-s}+2^{-s}+3^{-s}+4^{-s}+\cdots \\ &= \zeta(s).\end{aligned}$$

□

The functional equation expresses a beautiful symmetry of $\zeta(s)$:

$$\zeta(s) \leftrightarrow \zeta(1-s)$$

i.e. the values of ζ at s are related (but not equal) to the values of ζ at $1-s$. To explain this relationship precisely, let us define the completed Riemann zeta function.

Definition 1.3. Define $\Lambda(s) = \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s)$, where

$$\Gamma(s) := \int_0^\infty x^{s-1}e^{-x}dx \text{ for } \mathrm{Re}(s) > 0.$$

is the Gamma function.

Theorem 1.4 (Riemann, 1859)
We have that

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

In other words, we have that

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

The functional equation can be used to extend the definition of $\zeta(s)$ to the entire complex plane. Indeed, it is possible to extend the definition of $\zeta(s)$ to all $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 0$ without using the functional equation; but since the functional equation relates $\zeta(s)$ to $\zeta(1-s)$ and since the Gamma function has an analytic continuation to all of $\mathbb{C}$ (with simple poles at $s = 0, -1, -2, \ldots$), we can use the functional equation to define $\zeta(s)$ for all $s \in \mathbb{C}$.

Before proceeding further, we briefly explain why having these three properties (Euler product, functional equation and analytic continuation) is so important. We give two examples to illustrate this: one from analytic number theory and one from algebraic number theory.

- The Euler product

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

  implies that $\zeta(s) \neq 0$ for $Re(s) > 1$. However, studying the Euler product more carefully actually reveals something much stronger:

  $$\zeta(s) \neq 0 \text{ for all } s \in \mathbb{C} \text{ with } \mathrm{Re}(s) \geq 1.$$

  Combining this fact with tools from complex analysis yields the prime number theorem.

Theorem 1.5 (Hadamard, de la Vallée Poussin)
We have that
$$\pi(x) \sim \frac{x}{\log x},$$
where $\pi(x) = \#\{p \text{ prime } : p \leq x\}$.

- The first values of $\zeta(s)$ were computed by Euler in 1734. He showed that

$$\zeta(2) = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots = \frac{\pi^2}{6}.$$

$$\zeta(4) = \frac{1}{1^4} + \frac{1}{2^4} + \frac{1}{3^4} + \frac{1}{4^4} + \cdots = \frac{\pi^4}{90}$$

In general, Euler gave an explicit formula for the value of $\zeta(s)$ at an even positive integer:
$$\zeta(2k) = \frac{1}{1^{2k}} + \frac{1}{2^{2k}} + \frac{1}{3^{2k}} + \cdots = \pi^{2k} \cdot (-1)^{k-1} \frac{2^{2k}}{2(2k)!} B_{2k},$$
where B_n is the nth Bernoulli number defined by $\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n$.
Using the functional equation, we obtain that

$$\zeta(-1) = -\frac{1}{12}, \quad \zeta(-3) = \frac{1}{120}, \quad \zeta(-5) = -\frac{1}{252}$$

$$\zeta(-7) = \frac{1}{240}, \quad \zeta(-9) = -\frac{1}{132}, \quad \zeta(-11) = \frac{691}{32760}, \cdots$$

Can we say anything interesting about the numerators and denominators of these rational numbers?

Theorem 1.6
Let r be a positive even integer. Let D_r denote the numerator of $\zeta(1-r)$ when we write it as a reduced fraction. Then
- A prime number p divides D_r if and only if $p-1$ divides r.
- If p divides D_r, $\text{ord}_p(D_r) = \text{ord}_p(r) + 1$.

Thus, the denominator D_r of $\zeta(1-r)$ when r is positive even is completely understood.

Corollary 1.7
12 divides D_r for all r.

Proof. This follows directly from the previous theorem: 2 divides D_r since $1 = 2-1$ divides r; moreover, since r is even, we have that $\text{ord}_2(D_r) = \text{ord}_2(r) + 1 \geq 2$. Hence, 4 divides D_r. Similarly, 3 divides D_r since $2 = 3-1$ divides r. □

The numerators of these rational numbers are much more mysterious and even today remain poorly understood. For example, while extensive computation has revealed that these numerators always seem to be squarefree, we still do not have a proof of this fact. Nevertheless, we definitely know these numerators contain rich arithmetic information. For instance, we have

Theorem 1.8 (Kummer's criterion)
Let p be a prime number. Then p divides the size of the class group of $\mathbb{Q}(\mu_p)$ if and only if p divides the numerator of $\zeta(1-r)$ for some even r with $2 \leq r \leq p-3$.

There is also a connection of between the numerators of $\zeta(s)$ at negative odd integers and modular forms; it is not a coincidence that the prime number 691 appears in both

$$\zeta(-11) = \frac{691}{32760} \qquad \text{and in } \tau(p) \equiv 1 + p^{11} \bmod 691,$$

where the $\tau(p)$'s are the Fourier coefficients of Ramanujan's Delta function

$$\Delta(q) = q \prod_{n=1}^{\infty} (1-q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n.$$

These examples show that the Euler product, functional equation and analytic continuation lead to very interesting results and conjectures in number theory.

We now give a few other example of L-functions, which also a play an important role in Tate's thesis.

Definition 1.9 (Dirichlet L-functions)**.** A Dirichlet character mod q is a group homomorphism

$$\chi : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times.$$

The Dirichlet L-function attached to χ is defined to be

$$L(\chi, s) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p (1 - \chi(p) p^{-s})^{-1}.$$

Dirichlet L-functions also satisfy a functional equation. To explain this, this we introduce the following terminology.

- A Dirichlet character is said to be even if $\chi(-1) = 1$ and odd otherwise i.e if $\chi(-1) = -1$.
- Given a Dirichlet character χ, we set $\epsilon(\chi) = 0$ if χ is even and $\epsilon(\chi) = 1$ if χ is odd.
- We define the Gauss sum $G(\chi) = \sum_{k=0}^{q-1} \chi(k) e^{2\pi i \frac{k}{q}}$.

Theorem 1.10 (Functional equation for Dirichlet L-functions)

Define $\Lambda(\chi, s) = q^{s/2}\pi^{-(s+\epsilon(\chi))/2}\Gamma\left(\frac{s+\epsilon(\chi)}{2}\right) L(s,\chi)$. Then

$$\Lambda(\chi, s) = \frac{G(\chi)}{i^{\epsilon(\chi)}\sqrt{q}} \cdot \Lambda(\overline{\chi}, 1-s).$$

Just as with the Riemann zeta function, we can use Dirichlet L-functions to derive interesting number theoretic information.

Theorem 1.11 (Dirichlet)

Let a and q be positive coprime integers. There are infinitely many primes p such that p is congruent to a mod q. Moreover, the density of such primes is $\frac{1}{\varphi(q)}$.

Corollary 1.12

We have that

- 25% of primes end in 1.
- 25% of primes end in 3.
- 25% of primes end in 7.
- 25% of primes end in 9.

Proof. Apply Dirichlet's theorem with $q = 10$! □

We now recall how to generalize the definition of $\zeta(s)$ to number fields.

Definition 1.13 (Dedekind zeta functions)**.** Let K be a number field. We define the Dedekind zeta function of K by setting

$$\zeta_K(s) := \sum_{\mathfrak{a} \subseteq O_K} \frac{1}{N(\mathfrak{a})^s},$$

where the sum is over all non-zero ideals of O_K.

By the unique factorization of ideals into prime ideals in $\mathcal{O}_K$, it follows that

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

The Dedekind zeta function ζ_K satisfies a functional equation and has an analytic continuation to the entire complex plane with a simple pole at $s = 1$. It has also captures a tremendous information about the number field K:

Theorem 1.14 (The analytic class number formula)
Let K be a number field, ζ_K its Dedekind zeta function, h its class number, D_K its discriminant, R the regulator, w the number of roots of unity in K, r_1 the number of real places and r_2 the number of complex places of K. Then:

$$\lim_{s \to 1}(s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} hR}{w\sqrt{|D_K|}}$$

Just as Dedekind zeta functions are generalizations of the Riemann zeta function to a number field, we can define Hecke L-functions which are generalizations of Dirichlet L-functions to number fields. Hecke L-functions also have Euler products, functional equations and analytic continuation.

We now introduce an example which is slightly different from the previous examples: L-functions attached to modular forms. We again consider Ramanujan's Delta function

$$\Delta(q) = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n.$$

In 1916, Ramanujan considered the L-function

$$L(f,s) := \sum_{n=1}^{\infty}\frac{\tau(n)}{n^s}$$

and observed that

$$L(f,s) = \prod_p (1-\tau(p)p^{-s}+p^{11-2s}).$$

This was historically the first example of a degree two L-function: each term in the Euler product is a degree two polynomial in p^{-s} i.e. the local Euler factor at p is $f_p(p^{-s})$, where $f_p(x) := 1-\tau(p)x+p^{11}x^2$. This discovery of a degree two L-function has played a tremendous role in the development of number theory in the 20th century; for instance, Ramanujan's conjecture that the discriminant of f_p is always negative was only proven by Deligne in the 1970s as a consquence of his proof of the Riemann hypothesis for varieties over finite fields.

A few years after Ramaujan, Artin in 1922 discovered that one can construct degree n L-functions for any natural number n.

Definition 1.15 (Artin L-functions)**.** Let L/K be a Galois extension of number fields and let

$$\rho : \mathrm{Gal}(L/K) \to \mathrm{GL}_n(\mathbb{C}) \cong \mathrm{GL}(V)$$

be a Galois representation. The Artin L-function associated to ρ is defined to be

$$L(\rho,s) := \prod_{\mathfrak{p}} \det(1-\mathrm{Nm}(\mathfrak{p})^{-s}\rho(\mathrm{Frob}_{\mathfrak{p}})|V^{I_{\mathfrak{p}}})^{-1}$$

This is an L-function of degree n, where $n = \dim_{\mathbb{C}} V$. Artin L-functions are not very well understood to this day; the analytic continuation of Artin L-functions is a big open problem that goes under the name of Artin's conjecture.

Having seen many examples of L-functions so far, we can ask the following question: Is there a common source for all the L-functions that we have just considered? The answer to this question is, conjecturally, yes: Langlands conjectured that all these L-functions arise as L-functions of cuspidal automorphic representations of GL_n; indeed, one of the goals of the Langlands program is to unify all zeta functions appearing in number theory.

We briefly summarize the discussion of this section with the following table:

Year	Mathematician	Contribution
1734	Euler	Computed $\zeta(-1), \zeta(-3), \ldots$
1837	Dirichlet	Proved infinitely many primes in APs
1859	Riemann	Proved functional equations for ζ
1896	Dedekind	Proved analytic class number formula
1916	Ramanujan	Introduced degree two L-functions
1923	Artin	Introduced Artin L-functions
1970	Langlands	Formulated the Langlands conjectures

§1.2 Tate's Thesis: the main ideas

Where does Tate's thesis fit into this timeline? Tate's thesis (1950):

- gives a conceptual proof of the analytic continuation and functional equation of all degree one L-functions;
- provides techniques and ideas that are used till today to understand higher degree automorphic L-functions.

Thus, Tate's thesis is so fundamental because it not only provides a new perspective on a substantial portion of the theory of L-functions that was developed prior to 1950, but it is also the origin of techniques that drive current research in the subject. We now briefly explain the main ideas of Tate's thesis; this explanation will be very brief and will be covered in much more detail in the subsequent talks.

The first main theme of Tate's thesis is that it uses the full power of adeles and ideles.

Definition 1.16 (The adele ring of $\mathbb{Q}$)**.** The ring of adeles of $\mathbb{Q}$ is defined to be

$$\mathbb{A}_{\mathbb{Q}} := \{x = (x_\infty) \times (x_p)_p \in \mathbb{R} \times \prod_p \mathbb{Q}_p : x_p \in \mathbb{Z}_p \text{ for almost all } p\}.$$

We have an embedding

$$\mathbb{Q} \hookrightarrow \mathbb{A}_{\mathbb{Q}}, \quad a \mapsto (a, a, a, a, \ldots)$$

We can equip $\mathbb{A}_{\mathbb{Q}}$ with a topology: we define the basis of the topology to be sets of the form $U \times \prod_p V_p$, with $U \subseteq \mathbb{R}$ open, $V_p \subseteq \mathbb{Q}_p$ open and $V_p = \mathbb{Z}_p$ for almost all p.

Definition 1.17 (The group of ideles of $\mathbb{Q}$)**.** The group of ideles of $\mathbb{Q}$ is defined to be

$$\mathbb{A}_{\mathbb{Q}}^\times := \{x = (x_\infty) \times (x_p)_p \in \mathbb{R}^\times \times \prod_p \mathbb{Q}_p^\times : x_p \in \mathbb{Z}_p^\times \text{ for almost all } p\}.$$

As with the case of adeles, we have an embedding

$$\mathbb{Q}^\times \hookrightarrow \mathbb{A}_{\mathbb{Q}}^\times, \quad a \mapsto (a, a, a, a, \ldots)$$

and we can also equip $\mathbb{A}_{\mathbb{Q}}^{\times}$ with a topology: we define the basis of the topology to be sets of the form $U \times \prod_p V_p$, with $U \subseteq \mathbb{R}^{\times}$ open, $V_p \subseteq \mathbb{Q}_p^{\times}$ open and $V_p = \mathbb{Z}_p^{\times}$ for almost all p.

Definition 1.18 (Absolute value of an idele)**.** For $x = (x_v)_v \in \mathbb{A}_{\mathbb{Q}}^{\times}$, define

$$|x| = \prod_v |x_v|_v = |x_\infty|_\infty \cdot \prod_p |x_p|_p.$$

Note that for all but finitely many v, $|x|_v = 1$. Hence, this infinite product is actually a finite product. We make two remarks on the definition of adeles and ideles:

- As the notation might suggest, $\mathbb{A}_{\mathbb{Q}}^{\times}$ is indeed the group of units of the ring $\mathbb{A}_{\mathbb{Q}}$ (but its topology is not the subspace topology!).
- In a similar fashion, we can define $\mathbb{A}_K$ and $\mathbb{A}_K^{\times}$ for any number field K.

The second main feature of Tate's thesis is that Tate performs Fourier analysis or harmonic analysis on adeles and ideles. The main idea of Fourier analysis is as follows: Suppose we have a compact group G and we are interested in functions from $G \to \mathbb{C}$. These functions from a $\mathbb{C}$-vector space and we can equip this set of functions with an inner product. The idea of Fourier analysis is to select an orthonormal basis $(e_i)_{i\in I}$ for this set of functions; these functions are called characters. Hence, for any $f : G \to \mathbb{C}$, we have

$$f = \sum_{i \in I} \widehat{f}(e_i) e_i, \quad \widehat{f}(e_i) \in \mathbb{C}$$

where $\widehat{f} : \widehat{G} \to \mathbb{C}$ is called the Fourier transform of f. Thus, we have written f as $\mathbb{C}$-linear combination of "nice functions" (the characters). There is a similar theory (which is often called harmonic analysis) for locally compact abelian groups by replacing the sum above with an integral.

To perform harmonic analysis on adeles and ideles, we will work with Schwartz Bruhat functions: these are functions $f : \mathbb{A}_K \to \mathbb{C}$ that behave well with respect to Fourier Transform. We will also need the following notion:

Definition 1.19 (Hecke characters)**.** A Hecke character is a continuous group homomorphism $\chi : \mathbb{A}_K^{\times} \to \mathbb{C}^{\times}$ that is trivial on $K^{\times}$.

Equipped with a Schwartz Bruhat function f and a Hecke character χ, Tate introduces the following important definition.

Definition 1.20 (Adelic zeta function)**.** Define the adelic zeta function of f and χ by setting

$$\zeta(f, \chi, s) = \int_{\mathbb{A}_K^{\times}} f(x)\chi(x)|x|^s d^{\times}x,$$

where $d^{\times}x$ is a suitably chosen measure on $\mathbb{A}_K^{\times}$.

The adelic zeta function $\zeta(f, \chi, s)$ is a function of $s \in \mathbb{C}$ and Tate showed that it converges when $\mathrm{Re}(s)$ is sufficiently large. The key point of Tate's thesis is :

All degree one L-functions can be viewed as adelic zeta functions with suitably chosen f and χ. .

Thus, to prove the functional equation and analytic continuation of degree one L-functions, it suffices to prove that these more general adelic zeta functions satisfy a functional equation and have analytic continuation. Using the full power of the adelic machinery (in particular, the Adelic Poisson summation formula), Tate shows that this is indeed the case.

Theorem 1.21 (Main Theorem of Tate's thesis)
We have that

- $\zeta(f, \chi, s)$ admits an analytic continuation to the entire complex plane with the only possible poles at $s = 0$ and $s = 1$.
- $\zeta(f, \chi, s) = \zeta(\widehat{f}, \chi^{-1}, 1 - s)$.

We conclude by very briefly outlining how this gives us the functional equation for the Riemann zeta function.

Example 1.22 (The case of the Riemann zeta function)
Let $K = \mathbb{Q}$, χ be the trivial character and $f : \mathbb{A}_\mathbb{Q} \to \mathbb{C}$ be defined by

$$f((x_\infty) \times (x_p)_p) = e^{-\pi x_\infty^2} \cdot \prod_p \mathbf{1}_{\mathbb{Z}_p}(x_p)$$

Then

$$\begin{aligned}\zeta(f, \chi, s) &= \int_{\mathbb{A}_\mathbb{Q}^\times} f(x)\chi(x)|x|^s d^\times x \\ &= 2\int_0^\infty e^{-x_\infty} x_\infty^{s-1} dx_\infty \cdot \prod_p \int_{\mathbb{Q}_p^\times} \mathbf{1}_{\mathbb{Z}_p} |x_p|_p^s d^\times x_p \\ &= \pi^{-s/2}\Gamma(s/2) \cdot \prod_p (1 - p^{-s})^{-1} \\ &= \Lambda(s)\end{aligned}$$

By the adelic functional equation,

$$\zeta(f, \chi, s) = \zeta(\widehat{f}, \chi^{-1}, 1 - s).$$

Since $\widehat{f} = f$ and χ is trivial, we get

$$\zeta(f, \chi, s) = \zeta(f, \chi, 1 - s).$$

Hence,

$$\boxed{\Lambda(s) = \Lambda(1 - s)}$$

Our study group will be divided in three parts: we will first introduce the necessary background on adeles and ideles and on harmonic analysis on locally compact abelian groups; we will then study Tate's thesis itself and carry out the preceding steps in much more detail (Tate's thesis works for all degree one L-functions, but we will restrict to the case of Dirichlet L-functions for simplicity); finally, we will see some powerful applications of these ideas beyond Tate's thesis.

§2 Talk 2: Adeles, Ideles and their properties (Speaker: Katerina Santicola)

The goal of this talk is to introduce adeles and ideles and explain some of their basic properties. For any number field K, these are obtained by collecting together all the local fields associated to K (all completions of K); they provide a very good way to relate local properties with global properties. In this talk, we restrict to the case when $K = \mathbb{Q}$.

§2.1 Adeles

Definition 2.1 (The adele ring of $\mathbb{Q}$)**.** The ring of adeles of $\mathbb{Q}$ is defined to be

$$\mathbb{A}_{\mathbb{Q}} := \{x = (x_\infty) \times (x_p)_p \in \mathbb{R} \times \prod_p \mathbb{Q}_p : x_p \in \mathbb{Z}_p \text{ for almost all } p\}.$$

Note that $\mathbb{A}_{\mathbb{Q}}$ is a ring under pointwise addition and multiplication.

Proposition 2.2 ($\mathbb{Q}$ embeds in $\mathbb{A}_{\mathbb{Q}}$)

We have an injective ring homomorphism

$$\mathbb{Q} \hookrightarrow \mathbb{A}_{\mathbb{Q}}, \quad a \mapsto (a, a, a, a, \ldots)$$

Proof. We only need to check that this map is well-defined; if we write $a = \frac{m}{n}$, where m and n are integers, then for all $p \nmid n$, we have that $a \in \mathbb{Z}_p$. Thus, $(a, a, a, a, \ldots)$ is a well-defined element of $\mathbb{A}_{\mathbb{Q}}$. □

We can equip $\mathbb{A}_{\mathbb{Q}}$ with a topology: we define the basis of the topology to be sets of the form $U \times \prod_p V_p$, with $U \subseteq \mathbb{R}$ open, $V_p \subseteq \mathbb{Q}_p$ open and $V_p = \mathbb{Z}_p$ for almost all p. The ring of adeles satisfies two key properties:

Proposition 2.3

We have that

- $\mathbb{Q}$ is discrete in $\mathbb{A}_{\mathbb{Q}}$ (via the subspace topology).
- $\mathbb{A}_{\mathbb{Q}}/\mathbb{Q}$ is compact (via the quotient topology).

Proof.
- Consider the open set $U := (-1/2, 1/2) \times \prod_p \mathbb{Z}_p$ of $\mathbb{A}_{\mathbb{Q}}$. Then $U \cap \mathbb{Q} = \{0\}$ and so $\{0\}$ is an open subset of $\mathbb{Q}$. By continuity of addition, $\{a\}$ is open in $\mathbb{Q}$ for all $a \in \mathbb{Q}$. Thus, $\mathbb{Q}$ is discrete in $\mathbb{A}_{\mathbb{Q}}$.
- Let $W := [0, 1) \times \prod_p \mathbb{Z}_p$. We first prove the following claim.
  Claim: Every $x \in \mathbb{A}_{\mathbb{Q}}$ can be uniquely expressed in the form $q + w$ for some $q \in \mathbb{Q}$ and $w \in W$.
  Proof of claim: Pick $x = (x_v)_v \in \mathbb{A}_{\mathbb{Q}}$. Then, there exists a finite set of primes S such that for all primes $p \notin S$, $x_p \in \mathbb{Z}_p$. For each $p \in S$, we let

$$x_p = \sum_{j=-N_p}^{\infty} a_j p^j,$$

where $N_p \in \mathbb{N}_{\geq 1}$ and $a_j \in \{0, \ldots, p-1\}$ for all j. We define

$$r_p := \sum_{j=-N_p}^{-1} a_j p^j$$

and note that $r_p \in \mathbb{Q}$ and $x_p - r_p \in \mathbb{Z}_p$ for all $p \in S$. If $\ell \neq p$ is a prime, note that

$$|r_p|_\ell \leq \max_{-N_p \leq i \leq -1} |a_i|_\ell \leq 1.$$

Thus, if we let $r := \sum_{p \in S} r_p$, the $x - r$ lies in $\mathbb{R} \times \prod_p \mathbb{Z}_p$. Let $z := \lfloor x - r \rfloor$. Then

$$w := x - r - z \in W$$

and so we can write $x = w + (r + z)$ with $w \in W$ and $r + z \in \mathbb{Q}$ as claimed. The uniqueness of this decomposition follows from the fact that $W \cap \prod_p \mathbb{Z}_p = \{0\}$.
The claim implies that the image of the set $[0,1] \times \mathbb{Z}_p$ under the quotient map $\mathbb{A} \twoheadrightarrow \mathbb{A}_{\mathbb{Q}}/\mathbb{Q}$ is $\mathbb{A}_{\mathbb{Q}}/\mathbb{Q}$. Thus, $\mathbb{A}_{\mathbb{Q}}/\mathbb{Q}$ is compact, being the image of a compact set under a continuous map.

□

We can also define the following variant of $\mathbb{A}_{\mathbb{Q}}$.

Definition 2.4 (The ring of finite adeles of $\mathbb{Q}$)**.** The ring of finite adeles of $\mathbb{Q}$ is defined to be

$$\mathbb{A}_{\mathbb{Q},\mathrm{fin}} := \{x = (x_p)_p \in \prod_p \mathbb{Q}_p : x_p \in \mathbb{Z}_p \text{ for almost all } p\}.$$

In a similar fashion as before, we can equip $\mathbb{A}_{\mathbb{Q},\mathrm{fin}}$ with a topology and we also have that $\mathbb{Q}$ embeds in $\mathbb{A}_{\mathbb{Q},\mathrm{fin}}$. We now list some other properties of $A_{\mathbb{Q},\mathrm{fin}}$ without proof. To do so, we first introduce the ring of profinite integers.

Definition 2.5 (Profinite integers)**.** We define the ring of profinite integers by

$$\widehat{\mathbb{Z}} := \varprojlim_n \mathbb{Z}/n\mathbb{Z},$$

where the inverse limit is taken over natural numbers n and we have transition maps $\mathbb{Z}/n_1\mathbb{Z} \to \mathbb{Z}/n_2\mathbb{Z}$ if and only if n_2 divides n_1.

In subsequent discussions, we will often use the fact that $\widehat{\mathbb{Z}}$ is isomorphic to $\prod_p \mathbb{Z}_p$ as topological rings.

Proposition 2.6 (Properties of $\mathbb{A}_{\mathbb{Q},\mathrm{fin}}$)

We have that

- $\mathbb{A}_{\mathbb{Q},\mathrm{fin}} \cong \mathbb{Q} \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$.
- $\mathbb{Q}$ is dense in $\mathbb{A}_{\mathbb{Q},\mathrm{fin}}$.

§2.2 Ideles

Definition 2.7 (The group of ideles of $\mathbb{Q}$)**.** The group of ideles of $\mathbb{Q}$ is defined to be

$$\mathbb{I}_{\mathbb{Q}} := \{x = (x_\infty) \times (x_p)_p \in \mathbb{R}^\times \times \prod_p \mathbb{Q}_p^\times : x_p \in \mathbb{Z}_p^\times \text{ for almost all } p\}.$$

As with the case of adeles, we have an embedding

$$\mathbb{Q}^\times \hookrightarrow \mathbb{I}_{\mathbb{Q}}, \quad a \mapsto (a, a, a, a, \dots)$$

and we can also equip $\mathbb{I}_{\mathbb{Q}}$ with a topology: we define the basis of the topology to be sets of the form $U \times \prod_p V_p$, with $U \subseteq \mathbb{R}^\times$ open, $V_p \subseteq \mathbb{Q}_p^\times$ open and $V_p = \mathbb{Z}_p^\times$ for almost all p.

Proposition 2.8 (The ideles are the the units of the adeles)

We have that $\mathbb{A}_{\mathbb{Q}}^\times = \mathbb{I}_{\mathbb{Q}}$.

Proof. Pick $x = (x_v)_v \in \mathbb{I}_{\mathbb{Q}}$. Then $x_p \in \mathbb{Z}_p^\times$ for almost all primes p. Hence, $y := (x_v^{-1})_v \in \mathbb{A}_{\mathbb{Q}}$ and we have $xy = 1$ in $\mathbb{A}_{\mathbb{Q}}$ and so x is an invertible element of $\mathbb{A}_{\mathbb{Q}}$ i.e. $x \in \mathbb{A}_{\mathbb{Q}}^\times$. Conversely, suppose that $x = (x_v)_v \in \mathbb{A}_{\mathbb{Q}}^\times$. Then there exists $y = (y_v)$ in $\mathbb{A}_{\mathbb{Q}}$ such that $x \cdot y = 1$ in $\mathbb{A}_{\mathbb{Q}}$. For all but finitely many p, x_p is in $\mathbb{Z}_p$; on the other hand, for all but finitely many p, y_p is also in $\mathbb{Z}_p$. Thus, for all but finitely many p, x_p is in $\mathbb{Z}_p^\times$ and so $x \in \mathbb{I}_{\mathbb{Q}}$ by definition. □

Example 2.9 (The topology on $\mathbb{I}_{\mathbb{Q}}$ is not the subspace topology)

Even though the above proposition shows that $\mathbb{I}_{\mathbb{Q}}$ is the group of units of the ring $\mathbb{A}_{\mathbb{Q}}$, the topology on $\mathbb{I}_{\mathbb{Q}}$ is not the subspace topology. For instance, for each $n \in \mathbb{N}_{\geq 1}$, define $a_n \in \mathbb{I}_{\mathbb{Q}}$ via the number 1 in the $\mathbb{R}$ component and the number $n! + 1$ in all the other components. Then

- $\{a_n\}_n$ converges to 1 in $\mathbb{I}_{\mathbb{Q}}$ equipped with the subspace topology: the reason for this is essentially that, for each prime number p, $\mathrm{ord}_p(n!)$ tends to zero in $\mathbb{Z}_p$ as n tends to infinity.
- However, note that $U := \mathbb{R}^\times \times \prod_p \mathbb{Z}_p^\times \subseteq \mathbb{I}_{\mathbb{Q}}$ is an open neighbourhood of 1 in the topology of $\mathbb{I}_{\mathbb{Q}}$ defined above. Since $a_n \notin U$ for all $n \geq 1$, $\{a_n\}_n$ does not converge to 1 in the topology we equipped $\mathbb{I}_{\mathbb{Q}}$ with.

Definition 2.10 (Absolute value of an idele)**.** For $x = (x_v)_v \in \mathbb{A}_{\mathbb{Q}}^\times$, define

$$|x| = \prod_v |x|_v.$$

Note that for all but finitely many v, $|x|_v = 1$. Hence, this infinite product is actually a finite product.

Proposition 2.11 (The adelic absolute value of every rational number is one)

For all $a \in \mathbb{Q}^\times$,

$$|a| = \prod_v |a|_v = 1.$$

Proof. Write $x = \pm p_1^{n_1} \cdots p_m^{n_m}$ for some primes $p_1, \dots, p_m$ and $n_1, \dots, n_m \in \mathbb{Z}$. Then $|a|_\infty = p_1^{n_1} \cdots p_m^{n_m}$, $|a|_{p_i} = p^{-n_i}$ for all $i \in \{1, \dots, m\}$ and $|a|_v = 1$ for all $v \neq \infty, p_1, \dots, p_m$. Thus, $\prod_v |a|_v = 1$. □

While $\mathbb{Q}^\times$ is discrete in $\mathbb{I}_\mathbb{Q}$, it is not true that $\mathbb{I}_\mathbb{Q}/\mathbb{Q}^\times$ is compact. However, if we define,

$$\mathbb{I}_\mathbb{Q}^1 := \{x \in \mathbb{I}_\mathbb{Q} : |x| = 1\},$$

then $\mathbb{I}^1/\mathbb{Q}^\times$ is compact. We prove these statements below.

Proposition 2.12

We have that

- $\mathbb{Q}^\times$ is discrete in $\mathbb{I}_\mathbb{Q}$.
- $\mathbb{I}_\mathbb{Q}^1/\mathbb{Q}^\times \cong \widehat{\mathbb{Z}}^\times$. In particular, $\mathbb{I}_\mathbb{Q}^1/\mathbb{Q}^\times$ is compact.
- $\mathbb{I}_\mathbb{Q}/\mathbb{Q}^\times \cong \mathbb{R}_{>0} \times \widehat{\mathbb{Z}}^\times$ In particular, $\mathbb{I}_\mathbb{Q}/\mathbb{Q}^\times$ is not compact.

Proof.

- Consider the open set $U := (1/2, 3/2) \times \prod_p \mathbb{Z}_p^\times$ of $\mathbb{I}_\mathbb{Q}$. Then $U \cap \mathbb{Q}^\times = \{1\}$ and so $\{1\}$ is an open subset of $\mathbb{Q}^\times$. By continuity of multiplication, $\{a\}$ is open in $\mathbb{Q}^\times$ for all $a \in \mathbb{Q}^\times$. Thus, $\mathbb{Q}^\times$ is discrete in $\mathbb{I}_\mathbb{Q}$.
- For any $x = (x_v)_v \in \mathbb{I}_\mathbb{Q}^1$, note that $x_\infty \in \mathbb{Q}$ and also that we have a well-defined map
$$\mathbb{I}_\mathbb{Q}^1 \to \widehat{\mathbb{Z}}^\times = \prod_p \mathbb{Z}_p^\times \qquad (x_v)_v \mapsto (x_p/x_\infty)_p.$$
Since $\mathbb{Q}^\times$ is in the kernel of this map, we get an induced map
$$\mathbb{I}_\mathbb{Q}^1/\mathbb{Q}^\times \to \widehat{\mathbb{Z}}^\times = \prod_p \mathbb{Z}_p^\times.$$
One can check that the inverse of this map is
$$\widehat{\mathbb{Z}}^\times = \prod_p \mathbb{Z}_p^\times \to \mathbb{I}_\mathbb{Q}^1 \qquad z = (z_p) \mapsto \overline{(1, z)}.$$
Hence, $\mathbb{I}_\mathbb{Q}^1/\mathbb{Q}^\times \cong \widehat{\mathbb{Z}}^\times$ and so $\mathbb{I}_\mathbb{Q}^1/\mathbb{Q}^\times$ is compact.
- Note that the natural short exact sequence
$$1 \to \mathbb{I}_\mathbb{Q}^1/\mathbb{Q}^\times \to \mathbb{I}_\mathbb{Q}/\mathbb{Q}^\times \to \mathbb{R}_{>0} \to 1$$
splits: we can define a section $\mathbb{R}_{>0} \to \mathbb{I}_\mathbb{Q}/\mathbb{Q}^\times$ by $r \mapsto \overline{(r, 1)}$. The desired isomorphism now follows from the previous part.

□

§3 Talk 3: Proof of finiteness of class groups and Dirichlet's Unit Theorem (Speaker: Philip Holdridge)

To demonstrate the power of adeles and ideles, we will use them to prove the two most important theorems in classical algebraic number theory: finitness of class groups and Dirichlet's Unit Theorem.

§3.1 Preliminary background

We begin by generalizing the definition of adeles and ideles to an aribtrary number fields.

Let K be a number field with ring of integers $\mathcal{O}_K$.

Definition 3.1 (Finite places of a number field)**.** A non-zero prime ideal of $\mathcal{O}_K$ is called a finite place of K.

Definition 3.2 (Infinite places of a number field)**.** An infinite place of K is a field homomorphism $K \hookrightarrow \mathbb{R}$ or $K \hookrightarrow \mathbb{C}$ (up to complex conjugation). Embeddings of the former type are called real embeddings and embeddings of the latter type are called complex embeddings.

If $v = \mathfrak{p}$ is a finite place of K, then v gives rise to an absolute value on K: we define

$$|a|_v := q^{-\mathrm{ord}_{\mathfrak{p}}(a)},$$

where q is the cardinality of the residue field $O_K/\mathfrak{p}$ and $\mathrm{ord}_{\mathfrak{p}}(a) \in \mathbb{Z}$ is the exponent of $\mathfrak{p}$ in the prime ideal factorisation of (a). We let K_v to be the completion of K with respect to the absolute value $|\cdot|_v$ induced by v on K. When v is a real place, we let $K_v := \mathbb{R}$ equipped with the usual absolute value on $\mathbb{R}$ and v is a complex place, we let $K_v := \mathbb{C}$ with absolute value the square of the usual absolute value on $\mathbb{C}$. In particular, for any place v (finite or infinite), we have an embedding $K \hookrightarrow K_v$.

Definition 3.3. The ring of adeles of K is defined to be

$$\mathbb{A}_K := \{(x_v)_v \in \prod_v K_v : x_v \in \mathcal{O}_v \text{ for almost all } v\}.$$

The group of ideles of K is defined to be

$$\mathbb{I}_K := \{(x_v)_v \in \prod_v K_v : x_v \in \mathcal{O}_v^\times \text{ for almost all } v\}.$$

We make $\mathbb{A}_K$ into a topological rings by declaring the basis of topology for $\mathbb{A}_K$ to be open sets of the form $\prod_{v\in S} U_v \times \prod_{v\notin S} K_v$, where S is a finite set containing all the infinite places of K and U_v is an open set of $\mathcal{O}_v$. Similarly, we make $\mathbb{I}_K$ into a topological group by declaring the basis of the topology to be open sets of the form $\prod_{v\in S} U_v \times \prod_{v\notin S} \sqsubseteq^\times$, where S is a finite set containing all the infinite places of K and U_v is an open set of $K_v^\times$. Just as in the $K = \mathbb{Q}$ case, we have the following facts:

- K is discrete in $\mathbb{A}_K$ and $\mathbb{A}_K/K$ is compact.
- $K^\times$ is discrete in $\mathbb{I}_K$ and $\mathbb{I}_K^1/K$ is compact,

where $\mathbb{I}_K^1 := \{a \in \mathbb{I}_K : |a| = 1\}$ and for $a = (a_v)_v \in \mathbb{I}_K$, we define

$$|a| := \prod_v |a_v|_v$$

§3.2 Finiteness of class groups

Recall that the class group of a number field K is defined by

$$\mathrm{Cl}(K) = J_K/P_K,$$

where J_K is the multiplicative group of fractional ideals and $P_K \subseteq J_K$ is the subgroup of principal fractional ideals. Note that

$$\mathrm{Cl}(K) = \mathrm{coker}(K^\times \to J_K, a \mapsto (a)).$$

To prove the finiteness of class groups, a key role will be played by the following "adelic version" of the class group.

Definition 3.4 (Idele class groups)**.** The group $C_K := \mathbb{I}_K/K^\times$ is called the idele class group of K. We also let $C_K^1 := \mathbb{I}_K^1/K^\times$.

Let P denote the set of finite places of K and S denote the set of finite places of K. We make two observations that will allow us to relate the class group with the idele class group:

- We have an isomorphism of groups

$$\bigoplus_{\mathfrak{p}\in P} \mathbb{Z} \cong J_K \text{ via } (n_\mathfrak{p})_\mathfrak{p} \mapsto \prod_{\mathfrak{p}} \mathfrak{p}^{n_v}.$$

- Define

$$U := \prod_{v\in S} K_v^\times \times \prod_{v\in P} \mathcal{O}_v^\times.$$

  Note that U is an open subset of $\mathbb{I}_K$. Then

$$\mathbb{I}_K/U \cong \bigoplus_{v\in P} K_v^\times/\mathcal{O}_v^\times \cong \bigoplus_{v\in P} \mathbb{Z}.$$

Combining these observations, we conclude that

$$\begin{aligned}\mathrm{Cl}(K) &= \mathrm{coker}(K^\times \to J_K, a \mapsto (a)) \\ &\cong \mathrm{coker}(K^\times \to \bigoplus_{\mathfrak{p}\in P} \mathbb{Z}) \\ &\cong \mathrm{coker}(K^\times \to \mathbb{I}_K/U) \\ &\cong C_K/\overline{U},\end{aligned}$$

where $\overline{U}$ is the image of U in C_K.

The key point is thus:

We have realized the ideal class group as a quotient of the idele class group.

We now recall/prove three topological facts.

Lemma 3.5
A discrete and compact topological space X is finite.

Proof. Since X is discrete, we have an open cover

$$X = \bigcup_{x \in X} \{x\}.$$

Since X is compact, this cover must have a finite sub-cover and so X must be finite. □

Lemma 3.6
If $f : X \to Y$ is a continuous surjective map and if f is compact, then Y is compact.

Proof. Let $\{U_i\}_{i \in I}$ be an open cover of Y. Then $\{f^{-1}(U_i)\}_{i \in I}$ is an open cover of X. Since X is compact, this cover must have a finite subcover: there exists $i_1, \dots, i_n \in I$ such that

$$X = f^{-1}(U_{i_1}) \cup \cdots \cup f^{-1}(U_{i_n}).$$

Then

$$Y = f(X) = f(f^{-1}(U_{i_1}) \cup \cdots \cup f^{-1}(U_{i_n})) = f(f^{-1}(U_{i_1})) \cup \cdots \cup f(f^{-1}(U_{i_n})) = U_1 \cup \cdots \cup U_n,$$

where the last equality follows since f is surjective. Hence, Y is compact. □

Lemma 3.7
Let H be a subgroup of a topological group G. Then H is open if and only G/H is discrete.

Theorem 3.8
The class group of a number field is finite.

Proof. Since $U \subseteq \mathbb{I}_K$ is open, $\overline{U}$ is open in C_K. By Lemma 3.7, $C_K/\overline{U}$ is discrete. Let f denote the natural map

$$C_K^1 \to C_K/\overline{U}.$$

We claim that f is surjective. To prove this claim, it suffices to prove that

$$g : \mathbb{I}_K^1 \to \mathbb{I}_K/U$$

is surjective. Pick $\overline{a} \in \mathbb{I}_K/U$. Let v be an infinite place of K. Choose $b \in K_v^\times$ such that $|b|_v = |a|$. Define an element $\tilde{b} \in U$ via setting b in the v component and 1 in all the other components. Then $|\tilde{b}| = |a|$ and so $|a\tilde{b}|^{-1} \in \mathbb{I}_K^1$. Hence, $g(a\tilde{b}^{-1}) = \overline{a}$ and so g is surjective.

Thus f is surjective, and so $C_K/\overline{U}$ is compact by Lemma 3.6. Hence, by Lemma 3.5, $\mathrm{Cl}(K) \cong C_K/\overline{U}$ is finite. □

§3.3 Dirichlet's Unit Theorem

In this section, we will give a proof of Dirichlet's Unit Theorem. While we will not prove every fact needed to prove the theorem, we will try to give a hint of how adelic techniques are employed in the proof.

Theorem 3.9

Let K be a number field. Then

$$\mathcal{O}_K^\times \cong \mathbb{Z}^{r_1+r_2-1} \oplus \mu_K,$$

where r_1 is the number of real embedddings of K, r_2 is the number of pairs of complex embeddings and μ_K is the number of roots of unity in K.

Note that $r_1 + r_2 - 1 = |S| - 1$ where S is the set of infinite places of K, so Dirichlet's Unit Theorem states that $\mathcal{O}_K^\times \cong \mathbb{Z}^{|S|-1} \oplus \mu_K$.

The first step in proving this theorem is:

Proposition 3.10 (The roots of unity in a number field are finite.)

The group μ_K is finite.

Proof. For any place v, let

$$C_v := \{x \in K_v : |x|_v = 1\}.$$

Thus, when v is an infinite, C_v is either $\{\pm 1\}$ or the circle S^1, and when v is a finite place, c_v is $\mathcal{O}_v^\times$. Let $C = \prod_v C_v$. By Tychonoff's theorem, C is compact. Since $K^\times$ is discrete in $\mathbb{I}_K$, it is closed in $\mathbb{I}_K$. Thus, $C \cap K^\times$ is a closed subset of a compact set and is thus compact. Also, $C \cap K^\times$ is discrete. Thus, $C \cap K^\times$ is finite.
Now since $C \cap K^\times$ is a finite subgroup of $K^\times$, $C \cap K^\times \subseteq \mu_K$. On the other hand, $\mu_K \subseteq C \cap K^\times$. Thus, $\mu_K = C \cap K^\times$ and so μ_K is finite.

□

We now define a regulator map, which gives us a logarithmic embedding of $\mathcal{O}_K^\times$ into Euclidean space:

$$R : \mathcal{O}_K^\times \to \mathbb{R}^{|S|} \qquad x \mapsto (\log(|x|_v))_{v\in S}.$$

It is a standard fact that any algebraic integer whose all conjugates have absolute value 1 are roots of unity. Thus, $\ker R = \mu_K$. Since units in a number field have norm ± 1, note that the image of R lies in the $|S| - 1$ dimesnional subspace

$$(\mathbb{R}^{|S|})^0 := \{(c_v)_v \in \mathbb{R}^{|S|} : \sum_{v\in S} c_v = 0\}.$$

This is essentially the reason why $\mathcal{O}_K^\times$ has rank $|S|-1$. Using adelic techniques arguments similar to those we have seen before, it is possible to prove that

Proposition 3.11

The image of $\mathcal{O}_K^\times$ is discrete in $(\mathbb{R}^{|S|})^0$ and the quotient $(\mathbb{R}^{|S|})^0/R(\mathcal{O}_K^\times)$ is compact.

We also need the following fact:

Proposition 3.12

Let V be an n-dimensional topological vector space and Γ be a discrete subgroup such that V/Γ is compact. Then $\Gamma \cong \mathbb{Z}^n$ as abelian groups.

Proof of Dirichlet's Unit Theorem. Combining the previous two propositions, we have that

$$R(\mathcal{O}_K^\times) \cong \mathbb{Z}^{|S|-1}.$$

Thus, $\mathcal{O}_K^\times/\mu_K \cong \mathbb{Z}^{|S|-1}$ and since μ_K is finite, it follows that $\mathcal{O}_K^\times$ is a finitely generated abelian group i.e.

$$\mathcal{O}_K^\times \cong \mathbb{Z}^r \oplus T,$$

where $r \in \mathbb{N}$ and T is a finite abelian group. Hence, we must have that $T = \mu_K$ and $r = |S| - 1$. □

§4 Talk 4: Harmonic analysis on locally compact abelian groups (Speaker: Katerina Santicola)

As explained in the first talk, one of the main themes of Tate's Thesis is to perform harmonic analysis on adeles and ideles. In this talk, we will set up a general framework to perform harmonic analysis on any locally compact abelian group.

§4.1 The Haar measure

We begin by recalling some notions from measure theory.

Definition 4.1 (σ-algebra)**.** A σ-algebra of a set X is a set $\mathcal{A}$ of subsets of X such that

- $X \in \mathcal{A}$.
- $\mathcal{A}$ is closed under complements.
- $\mathcal{A}$ is closed under countable union.

Definition 4.2 (Measure)**.** A measure on a set X with a σ algebra $\mathcal{A}$ is a function

$$\mu : \mathcal{A} \to \mathbb{R} \cup \{\infty\}$$

such that

- $\mu(\emptyset) = 0$.
- μ is countably additive: if $E_1, E_2, \ldots$ are disjoint sets in $\mathcal{A}$, then

$$\mu(\bigcup_{i=0}^{\infty} E_i) = \sum_{i=1}^{\infty} \mu(E_i).$$

Example 4.3 (The Lebesgue measure)

The Borel σ-algebra of a topological space X is the smallest σ-algebra containing all the open sets of X. A Borel measure is a measure on the Borel σ-algebra of X. The usual Lebesgue measure μ on $\mathbb{R}$ ($\mu([0,1]) = 1, \mu([21,24)) = 3$) etc.) is an example of a Borel measure.

We would like to generalize this concept to general locally compact abelian groups.

Definition 4.4 (Locally compact abelian groups)**.** A topological group G is a group equipped with a topology such that the multiplication map $G \times G \to G$ and the inverse map $G \to G$ is continuous. A topological group G is called locally compact if it is Hausdorff and if for every $x \in G$, there is an open set $U \subseteq X$ and a compact set $K \subseteq X$ such that $x \in U$ and $U \subseteq K$.

Henceforth, we will use the term "LCA" to denote "locally compact abelian".

Example 4.5

- Any finite abelian group with discrete topology is compact and hence is LCA.
- The circle group $\mathbb{T} := \{z \in \mathbb{C} : |z| = 1\}$ is compact and hence is LCA.
- The group $(\mathbb{R}, +)$ of real numbers is LCA.
- The group $(\mathbb{Q}_p, +)$ of p-adic numbers is LCA; for any $x \in \mathbb{Q}_p$, the set $x + \mathbb{Z}_p$ is an open compact set containing x.
- Let K be a number field. Then both the adeles $\mathbb{A}_K$ and the ideles $\mathbb{I}_K$ are locally compact abelian groups.
- The group of rational numbers $\mathbb{Q}$ is not LCA.

Definition 4.6 (Haar measure)**.** Let G be LCA. A Haar measure on G is a Borel measure μ on G satisfying the following conditions:

- μ is inner regular: for any $A \in \mathcal{B}(G)$,
$$\mu(X) = \sup\{\mu(A) | K \subseteq A \text{ compact}\}.$$
- μ is outer regular: for any $A \in \mathcal{B}(G)$,
$$\mu(X) = \inf\{\mu(U) | A \subseteq U \text{ open}\}.$$
- μ is locally finite: for any compact set $K \subseteq G$, we have $\mu(K) < \infty$.
- μ is translation invariant: for any $g \in G$ and any $X \in \mathcal{B}(G)$, we have that
$$\mu(g + X) = \mu(g)$$
.

Theorem 4.7 (Existence of Haar measure)

For any locally compact abelian group G, there exists a Haar measure on G. Moreover, this measure is unique up to scaling by a constant.

Corollary 4.8

If G is an LCA which is also compact, there is a unique Haar measure μ on G such that $\mu(G) = 1$.

Example 4.9

- The counting measure on a discrete group (the measure which assigns the value one to every singleton) is a Haar measure.
- The Lebesgue measure μ on $\mathbb{R}$ is an example of a Haar measure.
- There is a unique Haar measure μ on $\mathbb{Q}_p$ such that $\mu(\mathbb{Z}_p) = 1$. This measure has the property that for an open set of the form $a + p^n\mathbb{Z}_p$, where $a \in \mathbb{Q}_p$ and $n \in \mathbb{Z}$, we have that
$$\mu(a + p^n\mathbb{Z}_p) = p^{-n}.$$

We now explain an important construction: given a measure μ on an LCA group and a function $f : G \to \mathbb{C}$, we explain what it means to integrate a function with respect to this measure. This procedure is done in three steps:

1. If A is a measurable set (i.e. A lies in the σ algebra) and $\mathbf{1}_A$ denotes the characteristic function of A (i.e. $f(x) = 0$ if $x \notin A$ and $f(x) = 1$ if $x \in A$), then we define
$$\int_G \mathbf{1}_A d\mu := \mu(A).$$

2. Let $A_1, \ldots, A_n$ be a finite collection of measurable sets and $c_1, \ldots, c_n$ be complex numbers. We define
$$\int_G (\sum_{i=1}^n c_i \mathbf{1}_{Ai}) d\mu := \sum_{i=1}^n c_i \mu(A_i).$$
Functions of these kind (i.e. those which are linear combination of characteristic functions) are called simple functions.

3. If $f : G \to \mathbb{C}$ is a function such that $f = \lim_{n\to\infty} f_i$, where each f_i is a simple function, we define
$$\int_G f d\mu := \lim_{n\to\infty} \int_G f_i d\mu \quad \text{(provided the latter limit exists).}$$

These integrals satisfy the usual properties properties that Riemann integrals satisfy: for instance, they are additive and we have a "change of variables formula".

Example 4.10 (A p-adic integral)

Let $s \in \mathbb{C}$ and let us consider a function
$$f : \mathbb{Z}_p \to \mathbb{C}, \qquad x \mapsto |x|_p^s.$$
Then
$$\begin{aligned}
\int_{\mathbb{Z}_p} f d\mu &= \int_{\mathbb{Z}_p \setminus \{0\}} f d\mu \\
&= \sum_{n=0}^{\infty} \int_{p^n\mathbb{Z}_p^\times} f d\mu \quad (\text{since } \mathbb{Z}_p \setminus \{0\} = \bigsqcup_{n=0}^{\infty} p^n \mathbb{Z}_p^\times) \\
&= \sum_{n=0}^{\infty} \int_{p^n\mathbb{Z}_p^\times} p^{-ns} d\mu \quad (\text{since } f \text{ is the constant function } p^{-ns} \text{ on } p^n\mathbb{Z}_p^\times) \\
&= \sum_{n=0}^{\infty} p^{-ns} \mu(p^n \mathbb{Z}_p^\times) \quad (\text{by definition of integration}) \\
&= \sum_{n=0}^{\infty} p^{-ns}(p-1)p^{-(n+1)} \quad (\text{since } p^n\mathbb{Z}_p^\times = p^n \cdot \bigsqcup_{i=1}^{p-1} i + p\mathbb{Z}_p = \bigsqcup_{i=1}^{p-1} i + p^{n+1}\mathbb{Z}_p) \\
&= \frac{p-1}{p} \cdot \frac{1}{1-p^{-(s+1)}} \quad (\text{by summing the geometric series})
\end{aligned}$$

§4.2 Fourier Theory on LCA groups

Definition 4.11 (Pontryagin dual)**.** Let G be an LCA group.

(a) A character of G is a continuous group homomorphism $f : G \to \mathbb{T}$, where $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$ is the circle group.

(b) The Pontraygin dual $\widehat{G}$ of G is defined to be the set of all characters of G.

We equip the Pontryagin dual $\widehat{G}$ with the compact open topology: a basis of open sets is given by $\{V(K,U)\}_{K,U}$, where

$$V(K,U) := \{f : G \to \mathbb{T} | f \text{ is a character } \& f(K) \subseteq U\}$$

and where K runs over all compact sets of G and U runs over all open sets of $\mathbb{T}$.

Theorem 4.12 (G LCA $\implies$ $\widehat{G}$ LCA)
If G is LCA, its Pontryagin dual group $\widehat{G}$ is also LCA.

Example 4.13

- If $G = \mathbb{Z}$, then $\widehat{G} \cong S^1$ since any group homomorphism (which is always continuous) is determined by the image of 1.
- If $G = S^1$, then then $\widehat{G} \cong \mathbb{Z}$ since it is a fact that all characters of S^1 are of the form $x \mapsto x^n$.
- If $G = \mathbb{Z}/n\mathbb{Z}$, then $\widehat{G} \cong \mathbb{Z}/n\mathbb{Z}$ since any character is determined by the image of 1 which must be an n-th root of unity.

The above examples show that $\widehat{\widehat{\mathbb{Z}}} \cong \mathbb{Z}$ and $\widehat{\widehat{\mathbb{Z}/n\mathbb{Z}}} \cong \mathbb{Z}/n\mathbb{Z}$. This fact is true in in general:

Theorem 4.14 (Pontryagin duality)
Let G be an LCA group. Then

$$G \cong \widehat{\widehat{G}} \qquad \text{via } g \mapsto (f \mapsto (f(g)).$$

Before proceeding to explain Fourier Theory on LCA groups, we record the following lemma which will be useful for us later.

Lemma 4.15 (Integrating characters)
For any compact group $(G, \cdot)$, a character χ on G and a Haar measure μ on G, we have that

$$\int_G \chi d\mu = \begin{cases} \mu(G) & \text{if } \chi \text{ trivial} \\ 0 & \text{otherwise} \end{cases}$$

Proof. If χ is trivial, then we have by definition

$$\int_G \chi d\mu = \int_G \mathbf{1}_G d\mu = \mu(G).$$

If χ is not trivial, there exists an $h \in G$ such that $\chi(h) \neq 1$. Then, since Haar meausures are translation invariant,

$$\int_G \chi(g)d\mu = \int_G \chi(gh)d\mu = \chi(h)\int_G \chi(g)d\mu.$$

Since $\chi(h) \neq 1$, we have that

$$\int_G \chi(g)d\mu = 0$$

as desired. □

Example 4.16 (Integrating characters over the circle)

. We saw above that all non-trivial characters of the circle $\mathbb{T}$ are of the form $z \mapsto z^n$ for $n \in \mathbb{N}_{>1}$. The above lemma is thus a generlisation of the following well-known fact from complex analysis: $\int_{\mathbb{T}} z^n dz = 0$. for $n \in \mathbb{N}_{\geq 1}$.

Definition 4.17. We say that two complex measurable functions agree everywhere if the set $\{x \in G : f(x) \neq h(x)\}$ has measure zero. This defines an equivalanece relation $\sim$ on the space of complex measurable functions. For $p \in \mathbb{N}_{\geq 1}$, we define

$$L^p(G) := \{f : G \to \mathbb{C} | \int_G |f|^p d\mu < \infty\}/\sim .$$

and define a norm $||\cdot||_p$ on $L^p(G)$ by

$$||f||_p := \left(\int_G |f|^p d\mu\right)^{1/p}.$$

Theorem 4.18 (Fourier Theory on LCA groups)

Let G be a locally compact abelian group with Haar measure μ.

- For $f \in L^2(G) \cap L^1(G)$, the Fourier transform

  $$\widehat{f}(\chi) := \int_G f(x)\bar{\chi}(x)d\mu(x)$$

  gives a well-defined map

  $$L^2(G) \cap L^1(G) \to L^1(\widehat{G}), f \mapsto \widehat{f}.$$

  There is a unique Haar measure $\widehat{\mu}$, called the dual Haar meausre of μ, such that $||f||_{L^2(G)} = ||\widehat{f}||_{L^2(\widehat{G})}$.

- The Fourier transform above extends to a well-defined isometry

  $$L^2(G) \to L^2(\widehat{G})$$

  such that

  $$\widehat{\widehat{f}}(x) = f(-x)$$

  almost everywhere.

§4.3 Two examples: $\mathbb{R}$ and $\mathbb{Q}_p$

.

Definition 4.19. We define a character $e_\infty \in \widehat{\mathbb{R}}$ by setting

$$e_\infty : \mathbb{R} \to \mathbb{T}, \qquad x \mapsto \exp(2\pi i x).$$

Proposition 4.20 ($\mathbb{R}$ is self-dual)
We have an isomorphism of LCA groups

$$\mathbb{R} \cong \widehat{\mathbb{R}} \qquad \text{via } y \mapsto (x \mapsto e_\infty(x \cdot y)).$$

Remark 4.21. From now on, we let μ_∞ denote the Lebesgue measure on $\mathbb{R}$. This is a very natural choice, but it also satisfies the following property: the dual measure $\widehat{\mu_\infty}$ on $\widehat{\mathbb{R}} \cong \mathbb{R}$ is again the Lebesgue measure.

Corollary 4.22 (Fourier Theory on $\mathbb{R}$)
We have that

- For $f \in L^2(\mathbb{R}) \cap L^1(\mathbb{R})$, the Fourier transform

  $$\widehat{f}(y) := \int_{\mathbb{R}} f(x) e_\infty(-xy) d\mu_\infty(x)$$

  gives a well-defined map

  $$L^2(\mathbb{R}) \cap L^1(\mathbb{R}) \to L^2(\mathbb{R}), f \mapsto \widehat{f},$$

  such that $||f||_{L^2(\mathbb{R})} = ||\widehat{f}||_{L^2(\widehat{\mathbb{R}})}$.

- The Fourier transform above extends to a well-defined isometry

  $$L^2(\mathbb{R}) \to L^2(\widehat{\mathbb{R}}).$$

  such that

  $$\widehat{\widehat{f}}(x) = f(-x)$$

  almost everywhere.

Proof. This follows by combining Theorem 4.18, Proposition 4.20 and Remark 4.21. □

Definition 4.23. We define a character $e_p \in \widehat{\mathbb{Q}_p}$ by setting

$$e_p : \mathbb{Q}_p \to \mathbb{T}, \qquad x = \sum_{j=-N}^{\infty} a_j p^j \mapsto \exp\left(-2\pi i \sum_{j=-N}^{-1} a_j p^j\right).$$

Proposition 4.24 ($\mathbb{Q}_p$ is self-dual)

We have an isomorphism of LCA groups

$$\mathbb{Q}_p \cong \widehat{\mathbb{Q}_p} \qquad \text{via } y \mapsto (x \mapsto e_p(x \cdot y)).$$

Remark 4.25. From now on, we let μ_p denote the unique Haar measure on $\mathbb{Q}_p$ such that $\mu(\mathbb{Z}_p) = 1$. As before, not only is this is a very natural choice, but it also satisfies the following property: the dual measure $\widehat{\mu_p}$ on $\widehat{\mathbb{Q}_p} \cong \mathbb{Q}_p$ is again μ_p.

Corollary 4.26 (Fourier Theory on $\mathbb{Q}_p$)

We have that

- For $f \in L^2(\mathbb{Q}_p) \cap L^1(\mathbb{Q}_p)$, the Fourier transform

  $$\widehat{f}(y) := \int_{\mathbb{Q}_p} f(x) e_p(-xy) d\mu_p(x)$$

  gives a well-defined map

  $$L^2(\mathbb{Q}_p) \cap L^1(\mathbb{Q}_p) \to L^2(\mathbb{Q}_p), f \mapsto \widehat{f},$$

  such that $||f||_{L^2(\mathbb{Q}_p)} = ||\widehat{f}||_{L^2(\widehat{\mathbb{Q}_p})}$.

- The Fourier transform above extends to a well-defined isometry

  $$L^2(\mathbb{Q}_p) \to L^2(\widehat{\mathbb{Q}_p}).$$

  such that

  $$\widehat{\widehat{f}}(x) = f(-x)$$

  almost everywhere.

Proof. This follows by combining Theorem 4.18, Proposition 4.24 and Remark 4.25. □