ADELIC FOURIER SERIES

SIDDHARTH KOTHARI

Abstract. In this expository paper, we develop Fourier analysis on the p-adics, and highlight a few applications, including Tate's proof of the functional equation for the Riemann-zeta function, and its extensions via Igusa zeta functions, which we survey briefly. We begin with a discussion of ordinary Fourier series, which decomposes a possibly complex periodic function defined on the real numbers into an infinite series of sines and cosines. Moreover, we note that this is just the statement that the sines and cosines from a Hilbert basis of the space of periodic functions; we encounter a similar phenomena when extending Fourier series to finite abelian groups: a particular set of functions defined on the group, called *characters*, form a basis for the vector space of all functions from the group, the group algebra. This allows us to compute the Fourier series of a function defined on the integers modulo n, recovering the discrete Fourier transform. We also use this, along with categorical properties of inverse and direct limits, to compute the characters of the p-adic integers.

We forge ahead, generalizing this setup further by relaxing the finite group assumption, and replacing it with local compactness. However, in this case, our original definition for the inner product on the group algebra will break down, prompting us to replace a finite sum inner product with an 'integral'. The Haar measure, a translation invariant measure that is guaranteed to exist on a locally compact abelian group, is used to pin down this integral, and so allowing us to rigorously define Fourier transform on the p-adics, and the reals, both of which are examples of locally compact groups.

Lastly, we introduce the Adele ring, which is the restricted direct product of all the completions of the rationals, allowing us to consolidate the Fourier transforms on the individual completions into a single global transform on the Adele ring, which we will use to give an arguably more insightful proof of the famous functional equation for the Riemann-zeta function that Riemann's original proof, which relied solely on the Fourier transform on the real numbers.

After looking at the Fourier series of a function $f : [-\pi, \pi] \to \mathbb{F}$ where $\mathbb{F}$ is either $\mathbb{R}$ or $\mathbb{C}$, we turn to the central question of this paper.

Question 0.1. *Is it possible to construct an analogue of the Fourier series of a function $f : G \to \mathbb{C}$ where G is any arbitrary group?*

Note that G could be anything: right from the humble $\mathbb{Z}/n\mathbb{Z}$, to $U(n)$, the group of n by n unitary matrices with complex entries, or even S_4, the symmetric group of order n. Essentially, we would like to break down an f, which might be dauntingly complicated at the moment, into simpler, more manageable parts, just as we decomposed a (periodic) function into a series of trigonometric polynomials, which represented the simplest type of periodic functions.

Before we begin, I must mention that we'll only be considering finite groups G in this section. Even then, we require a good deal of representation theory, which we'll cover here. First, we'll start by defining where the functions $f : G \to \mathbb{C}$ live.

0.1. **The Group Algebra.** The set of all functions $f : G \to \mathbb{C}$ forms a vector space with addition and scalar multiplication given point-wise as usual. Taking inspiration from the inner products on $\mathbb{C}^n$ and $L([-\pi, \pi])$,

$$\langle v, v' \rangle = \sum_{i=1}^{n} v_i \overline{v_i'} \text{ for all } v, v' \in \mathbb{C}^n \quad \text{and} \quad \langle f_1, f_2 \rangle = \int_{-\pi}^{\pi} f_1(x) \overline{f_2} \, dx \text{ for all } f_1, f_2 \in L^2([-\pi, \pi]),$$

we define for all $f_1, f_2 : G \to \mathbb{C}$,

$$\langle f_1, f_2 \rangle = \frac{1}{|G|} \sum_{g \in G} f_1(g)\overline{f_2(g)}.$$

We threw in a factor of $\frac{1}{|G|}$ because results in some neat cancellations, and so formula simplifications, as we'll see later.

Definition 0.2. The inner product space of functions $f : G \to \mathbb{C}$ as defined above is called the *group algebra* of G and is denoted by $\mathbb{C}[G]$.

0.2. **An Algebraic Interlude: Representation Theory.**

0.2.1. *What is representation theory?* Roughly speaking, *representation theory* lies at the intersection of the two cornerstones of modern algebra: group theory, the study of symmetry and linear algebra, the study of maps that deform (vector) spaces in a certain, 'clean way'. More precisely, given a group, we hope to understand it better by studying it's interaction with a vector space.

Definition 0.3. A *representation* of a group G is an ordered pair (ρ, V), where V is a vector space and $\rho : G \to \mathrm{GL}(V)$ is a homomorphism of groups.

First, we scrutinize this definition, as is virtually the foundation for all the theory that follows. $\mathrm{GL}(V)$ is the general linear group of V, the set of invertible $\dim V$ by $\dim V$ matrices which forms a group under the usual matrix multiplication. Remember from linear algebra that these matrices describe invertible linear maps from V to itself (like a rotation of the plane), so here we are viewing a $g \in G$ as *acting on a vector space* via an invertible linear map, namely, $\rho(g)$.

With that out of the way, let us jump into some examples!

Example. Consider $G = \mathbb{Z}_n$, the cyclic group of order n. We could interpret the generator as a rotation by $2\pi/n$ about the origin, meaning G consists of the rotational symmetries of an $n-$gon, so it's reasonable to let $V = \mathbb{R}^2$, the plane, and

$$\rho(k) = \begin{bmatrix} \cos\frac{2\pi k}{n} & -\sin\frac{2\pi k}{n} \\ \sin\frac{2\pi k}{n} & \cos\frac{2\pi k}{n} \end{bmatrix}$$

for all $k \in \mathbb{Z}_n$, which is the matrix corresponding to the rotation.

Example. But who restricted us to rotations? There are *many* other ways to interpret the generator of $\mathbb{Z}_n$, like a representing *reflection* by a line tilted $2\pi/n$ from the positive $x-$axis. Then, $V = \mathbb{R}^2$ and

$$\rho(k) = \begin{bmatrix} \cos\frac{4\pi k}{n} & \sin\frac{4\pi k}{n} \\ \sin\frac{4\pi k}{n} & -\cos\frac{4\pi k}{n} \end{bmatrix}$$

for all $k \in \mathbb{Z}_n$.

Example. Stepping away form $\mathbb{Z}_n$, let $G = S_3$, the symmetric group on three elements. Representing this is quite straightforward: simply use the three by three permutation matrices! For concreteness, we have $V = \mathbb{R}^3$ and

$$\rho\Big((1)(2)(3)\Big) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \rho\Big((1)(23)\Big) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \quad \rho\Big((13)(2)\Big) = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

$$\rho\Big((12)(3)\Big) = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \rho\Big((123)\Big) = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \quad \rho\Big((132)\Big) = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

Notation. Note that $\rho(g)$ is used to denote the linear map $\rho(g) : V \to V$ and $\rho(g)(v)$ to the image of $v \in V$ under the map $\rho(g)$. Somewhat annoyingly, we will use only ρ or only V to denote the representation (ρ, V), whenever the other is clear from context.

Just like we can take the direct sum of two vector spaces and even groups, we can also do the same for representations.

Definition 0.4. Let (ρ_1, V_1) and (ρ_2, V_2) be representations of a group G. The direct sum of the two representations, denoted by $(\rho_1 \oplus \rho_2, V_1 \oplus V_2)$ is defined to be $(\rho_1 \oplus \rho_2)(g) = \big(\rho_1(g), \rho_2(g)\big) \in \mathrm{GL}(V_1 \oplus V_2)$ for all $g \in G$.

Remark 0.5. The matrix representation of the linear map $(\rho_1 \oplus \rho_2)(g)$ for a $g \in G$ is given by the block-diagonal matrix

$$\begin{bmatrix} \rho_1(g) & \mathbf{0} \\ \mathbf{0} & \rho_2(g) \end{bmatrix}.$$

A notion that will be extremely useful in what follows is the *dimension* of a representation.

Definition 0.6. The *dimension* of a representation $\rho : G \to \mathrm{GL}(V)$, is the dimension of the underlying vector space V.

0.2.2. *Decomposing Representations.* In this section, we study the structure of a representation in the hope to break it into simpler, more manageable parts. Just like in linear algebra we have *subspaces* and in group theory *subgroups*, we also have such a sub-structure for representations, called a *subrepresentation* (surprise, surprise!).

How would it look like? It should be a representation of a group G in its own right, while built out of a given representation (ρ, V). Thus, we can simply restrict the domain of $\rho(g) : V \to V$ for all $g \in G$ to some fixed vector subspace W of V. But are we guaranteed that $\rho(g)|_W \in \mathrm{GL}(W)$ for all $g \in G$? We are if and only if W is $G-$invariant—vectors in W should not be thrown out of it by $\rho(g)$.

Definition 0.7. Let (ρ, V) be a representation of a group G. A linear subspace W of V is said to be $G-$invariant if $\rho(g)(w) \in W$ for all $g \in G$ and $w \in W$.

Now we are ready to define the subrepresentation.

Definition 0.8. A *subrepresentation* of a representation (ρ, V) of a group G, is a $G-$invariant subspace $W \subseteq V$, along with the homomorphism obtained by restricting the domain of $\rho(g)$ to W for all $g \in G$.

With this, the concepts of reducible and irreducible representations naturally come up.

Definition 0.9. A representation (ρ, V) of a group G is said to be *irreducible* if its only subrepresentations are the trivial representation $W = \{0\}$, and itself. A subrepresentation is said to be *reducible* if it is not irreducible.

The first thing that comes to mind when one reads Definition 0.9 are prime numbers! In fact, we have Theorem 0.10 that tells us these irreducibles are indeed the building blocks, the atoms of representation theory [1].

Theorem 0.10. *Let V be a representation of a group G. Then either V is irreducible, or a direct sum of irreducible representations of G.*

[1] These type of theorems crop up a lot in different areas of algebra! For example in group theory, we have that any finite abelian group is isomorphic to a direct product of cyclic groups of prime power order (the 'atoms'), albeit this version is easier to prove.

0.2.3. *Maps Between Representations.* This part of the paper is best understood as a 'helper' section. We present theorems related to maps between representation spaces in quick succession, which while they might seem unmotivated or 'useless' at first, are of utmost importance. We begin with a definition of the type of maps we'll be interested in studying.

Definition 0.11. Let (ρ_V, V) and (ρ_W, W) be irreducible representations for a finite group G. A linear map, $\varphi : V \to W$, is said to be a $G-$equivariant map if for all $g \in G$ and $v \in V$, we have that $\varphi\big(\rho_V(g)(v)\big)= \rho_W(g)(\varphi(v))$. We denote the set of $G-$equivariant maps by $\mathrm{Hom}_G(V, W)$.

The definition for an equivariant[2] map makes sense—the order of application of φ and ρ ought not to matter. In other words, it shouldn't matter what path you take to get to the bottom right W starting from the top left V, we say that the following diagram commutes:

$$\begin{array}{ccc} V & \xrightarrow{\varphi} & W \\ {\scriptstyle \rho_V(g)}\downarrow & & \downarrow{\scriptstyle \rho_W(g)} \\ V & \xrightarrow[\varphi]{} & W \end{array}$$

Why the notation Hom? That's because a *vector space homomorphism* is just a linear map between the two spaces. It might not be much of a surprise, but $\mathrm{Hom}_G(V_1, V_2)$ forms a vector space (with addition and multiplication given pointwise), so we can talk about it's bases and dimension. The definition of a $G-$equivariant map lets us talk about isomorphic representations.

Definition 0.12. Two representations (ρ_1, V_1) and (ρ_2, V_2) are said to be *isomorphic* if there exists a bijective $G-$equivariant map between the two.

Now, we straightaway state the result that will be important to us later, which is actually a corollary of *Schur's lemma.*

Proposition 0.13. *Let V_1 and V_2 be irreducible representations for a group G. Then,*

- *If $V_1 \not\cong V_2$, then* $\dim_{\mathbb{F}} \mathrm{Hom}_G(V_1, V_2) = 0$.
- *If $V_1 \cong V_2$, then* $\dim_{\mathbb{F}} \mathrm{Hom}_G(V_1, V_2) = 1$.

Thus, one check the isomorphism of representations and the level of their underlying vector spaces. As mentioned, to prove Proposition 0.13 we will require *Schur's lemma*, which is split between the next couple of propositions.

Proposition 0.14 (Schur's Lemma Part 1)**.** *Given $\varphi \in \mathrm{Hom}_G(V, W)$, either $\varphi = 0$ or $\varphi =$ a vector space isomorphism.*

Proof. Assume that $\varphi \neq 0$. Then $\ker(\varphi)$ is a *proper* subset of V. Note that $\ker(\varphi)$ is a $G-$invariant subspace (exercise!), so the irreducibilty of V implies that $\ker(\varphi) = 0$, which shows that φ is injective. Next, using a similar argument, $\mathrm{im}(\varphi)$ cannot be the null set (otherwise $\varphi = 0$) and as $\mathrm{im}(\varphi)$ is a $G-$invariant subspace the irreducibility of W implies that $\mathrm{im}(\varphi) = W$, which shows φ is surjective. ■

Proposition 0.15 (Schur's Lemma Part 2)**.** *Given $\varphi \in \mathrm{Hom}_G(V, V)$, we have $\varphi = \lambda I$, a scalar multiple of the identity map.*

Proof. By Proposition 0.14, we have that $\varphi \in \mathrm{Aut}_G(V, V)$, that is, φ is an invertible, G-equivariant, linear map from V to itself. This, and the fact I used a 'λ' in the proposition statement should get you thinking about eigenvalues! In particular, since $\mathbb{F}$ is an algebraically closed field, φ will have at

[2]We have a category! The objects are the representations of a fixed group G over a field $\mathbb{F}$, and the morphisms are the $G-$equivariant maps. Identity and composition are defined as usual. This category is denoted by $\mathrm{Rep}_{\mathbb{F}}(G)$.

least one eigenvalue, say λ. The corresponding eigenspace is the subspace $W = \{v \in V : \varphi(v) = \lambda v\}$, which is G-invariant (a good exercise to verify!). Since this cannot be $\{0\}$, the only way for it to exist without contradicting the irreducibility of V is for $W = V$, which instantly completes the proof. ■

Notice how much of these proofs hinge on irreducibility of the representation space! Now we are ready to prove Proposition 0.13.

Proof. We prove the two parts as mentioned in the proposition.

- The first claim follows directly from Proposition 0.14: since V_1 is not isomorphic to V_2, the only homomorphism that can exist between the two is the 0 map.
- For the second part, consider two non-zero elements ϕ_1 and ϕ_2 of $\mathrm{Hom}_G(V_1, V_2)$. Note that $\phi_2^{-1}\phi_1$ is an element of $\mathrm{Hom}_G(V_1, V_1)$ by a proposition. Hence, by Proposition 0.15, $\phi_2^{-1}\phi_1 = \lambda I$ where I denotes the identity map from V_1 to itself and $\lambda \in \mathbb{F}$. Rearranging, we get $\phi_1 = \phi_2\lambda$, meaning all elements of $\mathrm{Hom}_G(V_1, V_2)$ are multiples of each other, which completes the proof.

■

Now, as promised, we return to the proof that an irreducible representation of an abelian group is always one-dimensional.

Proposition 0.16. *Let (ρ, V) be an irreducible representation of an abelian group G. Then $\dim V = 1$.*

Proof. Since $gh = hg$ for all $g, h \in G$, we have $\rho(gh) = \rho(hg) \implies \rho(g)\rho(h) = \rho(h)\rho(g)$. Written differently, $\rho(g)\big(\rho(h)(v)\big) = \rho(h)\big(\rho(g)(v)\big)$ for all $v \in V$ and $g, h \in G$. Does this ring a bell? Indeed, we have that $\rho(g)$ is a $G-$equivariant map! By Proposition 0.15 there exists a λ for all $g \in G$, such that $\rho(g) = \lambda I$. This implies that any subspace W of V is $G-$invariant, and so is a subrepresentation. At this stage, the irreducibility of V forces $\dim V = 1$. ■

1. Prufer Groups

Definition 1.1 (Inverse system)**.** Let $(I, \leq)$ be a directed poset. Let $(X_i)_{i\in I}$ be a family of objects in a category $\mathcal{C}$, and suppose we have a family of morphisms $f_{ij} : X_j \to X_i$ for all $i \leq j$ with the following properties:

- f_{ii} is the identity on A_i and,
- $f_{ik} = f_{ij} \circ f_{jk}$ for all $i \leq j \leq k$ in I. Then the pair $((X_i)_{i\in I}, (f_{ij})_{i\leq j\in I})$ is called an inverse system of objects and morphisms in the category $\mathcal{C}$ over I.

Definition 1.2 (Inverse limit)**.** Let $((X)i)_{i\in I}, (f_{ij})_{i\leq j\in I})$ be an inverse system of objects and morphisms in $\mathcal{C}$. Then, the inverse limit of this system is an object X in $\mathcal{C}$ together with morphisms $\pi_i : X \to X_i$ for all $i \in I$ satisfying $\pi_i = f_{ij} \circ \pi_j$ for all $i \leq j$ in I. The pair $(X, (\pi_i)_{i\in I})$ must be universal in the sense that for any other such pair $(Y, (\tau_i)_{i\in I})$, there exists a unique morphism $\varphi : Y \to X$ such that the following diagram commutes.

Remark 1.3. Just to spell the details out, there must exist a unique morphism $\varphi : Y \to X$ such that we have $\tau_i = \pi_i \circ u$ for all $i \in I$; if I give you another pair $(Y, (\tau_i)_{i\in I})$ that satisfies the same properties as the original $(X, (\pi_i)_{i\in I})$, then all maps from Y to X_i must factor *uniquely* through X.

Remark 1.4. From the universal property of the inverse limit, we see immediately that inverse limit is unique upto *unique* isomorphism!

Definition 1.5 (Category of Locally Compact Abelian Groups)**.** The category of locally compact abelian groups is the category **LCA** whose objects are locally compact abelian groups (surprise, surprise!). For any two objects G_1, G_2 in **LCA**, the set of morphisms, denoted by $\mathrm{Hom}_{\mathbf{LCA}}(G_1, G_2)$ consist of all continuous group homomorphisms $f : G_1 \to G_2$. Composition of morphisms is simply the standard composition of functions, which naturally preserves both continuity and the homomorphism property; the identity morphism is the standard identity function $\mathrm{id}_G : G \to G$.

Proposition 1.6. *Let $((G_i)_{i\in I}, (f_{ij})_{i\leq j\in I})$ be an inverse system of objects and morphisms in* ***LCA*** *over I. Then, assuming the inverse limit $\varprojlim G_i$ and the direct limit $\varinjlim \widehat{G_i}$ exist in* ***LCA****, we have*

$$Hom_{\mathbf{LCA}}(\varprojlim G_i, \mathbb{R}/\mathbb{Z}) \cong \varinjlim Hom_{\mathbf{LCA}}\left(G_i, \mathbb{R}/\mathbb{Z}\right).$$

That is, the dual of the inverse limit is isomorphic the direct limit of the duals as objects in ***LCA****.*

Proof. To show that $\mathrm{Hom}_{\mathbf{LCA}}(\varprojlim G_i, \mathbb{R}/\mathbb{Z})$ is isomorphic to $\varinjlim \mathrm{Hom}_{\mathbf{LCA}}\left(G_i, \mathbb{R}/\mathbb{Z}\right)$, we leverage universal properties. In particular, we'll show that $\mathrm{Hom}_{\mathbf{LCA}}(\varprojlim G_i, \mathbb{R}/\mathbb{Z})$ satisfies the universal property of the direct limit of the $\mathrm{Hom}_{\mathbf{LCA}}\left(G_i, \mathbb{R}/\mathbb{Z}\right)$'s.

First, a clarification. What are maps $f'_{ij} : \mathrm{Hom}_{\mathbf{LCA}}\left(G_i, \mathbb{R}/\mathbb{Z}\right) \to \mathrm{Hom}_{\mathbf{LCA}}\left(G_j, \mathbb{R}/\mathbb{Z}\right)$ of the direct system with objects $\mathrm{Hom}_{\mathbf{LCA}}\left(G_i, \mathbb{R}/\mathbb{Z}\right)$? Recalling that $((G_i)_{i\in I}, (f_{ij})_{i\leq j\in I})$ is an inverse limit, we set $f'_{ij} = \chi \circ f_{ij}$ for all $\chi \in \mathrm{Hom}_{\mathbf{LCA}}\left(G_i, \mathbb{R}/\mathbb{Z}\right)$.

Next, we construct maps $a_i : \mathrm{Hom}_{\mathbf{LCA}}\left(G_i, \mathbb{R}/\mathbb{Z}\right) \to \mathrm{Hom}_{\mathbf{LCA}}(\varprojlim G_i, \mathbb{R}/\mathbb{Z})$; a_i takes as input a continuous homomorphism $\chi : G_i \to \mathbb{R}/\mathbb{Z}$ and spits out a continuous homomorphism $a_i(\chi) : \varprojlim G_i \to \mathbb{R}/\mathbb{Z}$.

The most natural choice is to let $a_i(\chi)$ to be such that $a_i(\chi)((g_\mu)_{\mu\in I}) = \chi(g_i)$ for all compatible tuples $(g_\mu)_{\mu\in J} \in \varprojlim G_i$. To ensure that these injections a_i are valid, we have to show that $a_i = a_j \circ f'_{ij}$ for all $i \leq j$. We have

$$(a_j \circ f'_{ij})(\chi)((g_\mu)_{\mu\in I}) = a_j\left(f'_{ij}((g_\mu)_{\mu\in I})\right) = f'_{ij}(g_j) = (\chi \circ f_{ij})(g_j) = \chi\left(f_{ij}(g_j)\right)\chi(g_i) = a_i(\chi)((g_\mu)_{\mu\in I}).$$

Lastly, we must show universality.

■

2. Character Theory

After embarking on a seemingly pointless, rambling journey in representation theory, we return to answer Question 0.1. First, a slight caveat: instead of considering an arbitrary $f \in \mathbb{C}[G]$, we will deal with class functions, for now, as defined below.

Definition 2.1. An function $f \in \mathbb{C}[G]$ is said to be a *class function* if $f(g) = f(hgh^{-1})$ for all $h, g \in G$. The set of class functions is denoted by $\mathcal{C}_G$.

Remark 2.2. Essentially, a class function is one that is constant over a conjugacy class—it does not discriminate between members of the same conjugacy class.

Remark 2.3. If G is an abelian group, say $\mathbb{Z}/n\mathbb{Z}$, the conjugacy classes are simply the singletons, so $\mathbb{C}[G] = \mathcal{C}_G$.

Definition 2.4. Let (ρ, V) be a representation of a group G. The *character* of the representation (ρ, V) is a function $\chi_V : G \to \mathbb{F}$ defined by $\chi_V(g) = \mathrm{Tr}\big(\rho(g)\big)$ for all $g \in G$. A character of an irreducible representation is said to be an *irreducible character*.

Proposition 2.5. *A character χ of a group G is a class function.*

Proof. Consider a representation (ρ, V) of a group G and let χ_V denote it's character. Then, $\chi_V(h^{-1}gh) = \mathrm{Tr}\big(\rho(h^{-1}gh)\big) = \mathrm{Tr}\big(\rho(h^{-1})\rho(g)\rho(h)\big)\big)$. Since the trace is invariant under cyclical shifts, we get $\mathrm{Tr}\big(\rho(h^{-1})\rho(g)\rho(h)\big)\big)= \mathrm{Tr}\big(\rho(g)\rho(h)\big)\rho(h^{-1})\big)= \mathrm{Tr}\big(\rho(g)\rho(hh^{-1})\big)\big)= \mathrm{Tr}(\rho(g)) = \chi_V(g)$, which completes the proof. ∎

Now we present the central result of this whole paper! The one that allows us to generalize Fourier analysis beyond the realm of $\mathbb{R}$.

Theorem 2.6. *Let G be a finite group and $\mathcal{C}_G$ the vector space of complex-valued class functions defined on G. Then, the set of irreducible characters of G, denoted by $\mathcal{A} = \{\chi_\alpha\}_{\alpha\in A}$ forms an orthonormal basis for $\mathcal{C}_G$.*

But why is this result so important? As we shall see, these irreducible characters play the same role for $\mathbb{C}[G]$ as the exponential basis $E = \left\{\frac{1}{\sqrt{2\pi}}e^{inx} : n \in \mathbb{Z}\right\}$ does for $L^2([-\pi, \pi])$. Just like the density of E in $L^2([-\pi, \pi])$ allows us to decompose an $f : [-\pi, \pi] \to \mathbb{C}$ into a series of sines and cosines, the fact that $\mathcal{A}$, the set of irreducible characters of G, forms a basis for $\mathbb{C}[G]$ allows us to rewrite f in a simpler, more manageable way. To this end, we define the *Fourier series* of an $f \in \mathbb{C}[G]$.

Definition 2.7. Let $\{\chi_\alpha\}_{\alpha\in A}$ denote the set irreducible representations for a finite group G. The *Fourier coefficient* of $f \in \mathcal{C}_G$ corresponding to an irreducible character χ_α is defined by

$$\langle f, \chi_\alpha\rangle = \frac{1}{|G|}\sum_{g\in G} f(g)\overline{\chi_\alpha(g)}.$$

The *Fourier series* of f is defined by

$$\sum_{\alpha\in A}\langle f, \chi\rangle\chi_\alpha(x).$$

Remark 2.8. Again, this is nothing but a *change of basis transformation*. Specifying an $f \in \mathcal{C}_G$ means writing down it's coordinates with respect to the 'trivial' basis $B = \{f_{\mathcal{O}_i} \in \mathcal{C}_G : i \in I\}$ where $\{\mathcal{O}_i\}_{i\in I}$ denotes the set of conjugacy classes of G, and $f_{\mathcal{O}_i}(g) = 1$ if $g \in \mathcal{O}_i$ and $f_{\mathcal{O}_i}(g) = 0$ if $g \notin \mathcal{O}_i$ for all $i \in I$, whereas $\{\langle f, \chi_\alpha\rangle\}_{\alpha\in A}$ are the coordinates of f with respect to $\mathcal{A}$, the 'character basis'. Each $\langle f, \chi_\alpha\rangle$ quantifies the contribution of χ_α to f, which effectively decomposes f into pieces. On the other hand, the *Fourier series* can be viewed as a *synthesis* formula, reconstructing f from it's Fourier coefficients.

Remark 2.9. Note that since B as defined above forms a basis for $\mathcal{C}_G$, Theorem 2.6 says that $|\mathcal{A}| = |B|$, or the number of distinct irreducible characters is equal to the number of conjugacy classes of G, which is finite for finite G.

That's great, but actually computing all the irreducible representations and then the corresponding characters looks daunting, at least at first glance. Luckily for us, if we restrict our attention to abelian groups, the irreducible characters can be completely described fairly easily.

Proposition 2.10. *An irreducible character of an abelian group G is a group homomorphism from G to $\mathbb{F}^\times$, the multiplicative group of the field $\mathbb{F}$.*

Proof. This proof relies heavily on Proposition 0.16: an irreducible representation (ρ, V), of an abelian group G is one-dimensional—$\rho(g)$ is nothing but a 1 by 1 matrix—essentially a scalar. Thus, quite obviously $\mathrm{Tr}\big(\rho(g)\big)= \rho(g)$ for all $g \in G$, which allows us to simplify $\chi_\rho(g_1g_2)$:

$$\begin{aligned}\chi_\rho(g_1g_2) &= \mathrm{Tr}\big(\rho(g_1g_2)\big)\\ &= \rho(g_1g_2)\\ &= \rho(g_1)\rho(g_2)\\ &= \mathrm{Tr}\big(\rho(g_1)\big)\mathrm{Tr}\big(\rho(g_2)\big)\\ &= \chi_\rho(g_1)\chi_\rho(g_2).\end{aligned}$$

Hence, each irreducible character is simply a group homomorphism to $\mathbb{F}^\times$—something that *seems* more manageable. ■

Note that we can go the other way round as well: each group homomorphism $\phi : G \to \mathbb{F}^\times$ is an irreducible representation of G. To see this, simply note $\mathbb{F}^\times \cong \mathrm{Aut}(\mathbb{F})$, where $\mathbb{F}$ forms a one dimensional vector space over itself (essentially, linear maps from a field to itself can be represented by single numbers, which have the effect of squeezing/stretching the $\mathbb{F}$ number line). Hence, there is a one-to-one relationship between the two sets, so to talk of one is to talk of the other. With that out of the way, let's jump into an example!

Example. First, we'll have exactly N irreducible characters, and since $\mathbb{Z}/N\mathbb{Z}$ is a abelian, they'll be functions $\chi : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ such that $\chi(x+y) = \chi(x)\chi(y)$ for all x and y in $\mathbb{Z}/N\mathbb{Z}$—which naturally hints at the exponential function: we literally have $e^{a+b} = e^a e^b$ for real a and b, as we were taught so long ago. Hopefully then, it shouldn't be too surprising that $\chi_k(x) = e^{2\pi i k x/N}$ for $k = 0, \cdots, N-1$ are the irreducible characters for $\mathbb{Z}/N\mathbb{Z}$—this matches up with our experience in $\mathbb{R}$!

As before, the Fourier series of f will be given by

$$\sum_{\alpha \in A} \langle f, \chi \rangle \chi_\alpha(x),$$

which, in this case, becomes

$$\sum_{k=0}^{N-1} \langle f, e^{2\pi i k x/N} \rangle e^{2\pi i k x/N} = \sum_{k=0}^{N-1} X_i e^{2\pi i k x/N}$$

where

$$X_k = \frac{1}{|G|} \sum_{x \in \mathbb{Z}_N} f(x)\overline{\chi_k(x)} = \frac{1}{N} \sum_{n=0}^{N-1} f(n) e^{-2\pi i k n/N}.$$

Again, another way to think about it is simply as a change of basis linear transformation $\mathcal{F} : \mathbb{C}^N \to \mathbb{C}^N$ given by

$$\mathcal{F}(\mathbf{x}) = \mathcal{F}\big((x_0, \cdots, x_{N-1})\big) = (X_0, \cdots, X_{N-1}) \text{ where } X_k = \frac{1}{N} \sum_{n=0}^{N-1} x_n e^{-2\pi i n k/N}.$$

This, as you might already have recognized, is the Discrete Fourier Transform[3] of $\mathbf{x}$ —just one of the many, *somewhat identical*, offsprings of Definition 2.7!

Remark 2.11. Even though we can't apply this machinery when $G = \mathbb{R}/\mathbb{Z}$ (as $|G| = \infty$) to re-derrive the Fourier series of a $f \in L^2([-1,1])$, we can be cheeky and use the above analysis as $N \to \infty$. More precisely, the idea is to pick an $N \in \mathbb{N}$ and sample the function f at N points: $x_k = \frac{2k}{N-1} - 1$ where k ranges from 0 to $N-1$. Thus, for each $N \in \mathbb{N}$, we have a function, $f_N : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ defined by $f_N(k) = f(x_k)$ for all $k \in \mathbb{Z}/N\mathbb{Z}$. It's quite clear that as $N \to \infty$, f_N approximates f better and better. Next, the Fourier series of f_N will be given by

$$\sum_{k=0}^{N-1} \langle f_N, e^{2\pi i k x/N} \rangle e^{2\pi i k x/N} \quad \text{where} \quad \langle f_N, e^{2\pi i k x/N} \rangle = \frac{1}{N} \sum_{n=0}^{N-1} f\left(\frac{2n}{N-1} - 1\right) e^{-2\pi i k n/N}.$$

Try seeing what happens now when $N \to \infty$!

[3]Well, almost. In the actual discrete Fourier transform, that 'pesky' factor of $1/N$ is not present.

3. What Next?

That's great, but as mentioned earlier, this machinery that we have developed to compute the Fourier series of a function $f \in \mathbb{C}[G]$ only works when G is finite; and, arguably, the most *interesting* groups out there such as $\mathbb{R}/\mathbb{Z}$, and $\mathrm{SO}(n)$ aren't finite. For starters, the inner product that we had defined on $\mathbb{C}[G]$:

$$\langle f_1, f_2 \rangle = \frac{1}{|G|} \sum_{g \in G} f_1(g)\overline{f_2(g)},$$

completely breaks down when $|G| = \infty$. This question, of summing infinitely many numbers, is a quintessential example of developing the integral over any set, as answered by measure theory. Almost instinctively, one would set

$$\langle f_1, f_2 \rangle = \int_G f_1(x)\overline{f_2(x)}\, d\mu(x),$$

but that raises another question: what is the measure μ here? What's the $\sigma-$algebra? Is it even guaranteed that a measure μ always exists on a group G?

To answer this question, we equip G with additional structure: specifically, we put a topology on G to turn it into a **topological group**—a structure that's simultaneously a group and a topological space. However, as a techincal side, note that the topology must be such that it's compatible with the pre-existing group structure, that is, the inversion map $g \mapsto g^{-1}$ and the multiplication map $(g, h) \mapsto gh$ must be continuous with respect to the topology on G, and the product topology on $G \times G$ respectively. Then, the sigma algebra is simply the one generated by the open sets of G, called the **Borel sigma algebra**.

It was proved by the revolutionary french mathematician André Weil, that if G is a *locally compact* topological group, that is, if there exists a compact neighbourhood for each point in G, then there exists a unique measure μ on G [4], that apart from satisfying a few technical conditions, is *invariant*, that is, translating a Borel set S of G around by a $g \in G$ doesn't affect the measure of S [5], exactly how we have $\lambda(B) = \lambda(a + B) = \lambda(\{a + b : b \in B\})$ where λ denotes the Lebesgue measure on $\mathbb{R}$, which can be viewed as a (locally compact) topological group under addition. This measure is called the **Haar measure**, named after the Hungarian mathematician Alfréd Haar, who first studied it in connection with Hilbert's fifth problem on Lie groups, which are special types of topological groups.

4. The Haar Measure

4.1. **Measure Theory Pre-requisites.**

4.1.1. *Basic Notions.*

Definition 4.1 (Sigma algebra)**.** Let X be an arbitrary set, and let $\mathcal{P}(X)$ denote its power set, the set of all subsets of X. Then a σ-algebra is a subset $\mathcal{A}$ of $\mathcal{P}(X)$ such that:

- $X \in \mathcal{A}$,
- if $A \in \mathcal{A}$ then $X \setminus A \in \mathcal{A}$, and
- if $\{A_i\}_{i \in I}$ is a collection of countably many elements in $\mathcal{A}$, then $\bigcup_{i \in I} A_i \in \mathcal{A}$.

Definition 4.2 (Measurable space)**.** A measurable space is an ordered pair $(X, \mathcal{A})$ where X is a set and $\mathcal{A}$ is a $\mathcal{A} \subseteq \mathcal{P}(X)$ is a σ-algebra.

---

[4]Note that the measure is unique up to multiplication by a scalar. Note also that we have two types of invariance of measures: a left invariant measure μ is such that $\mu(S) = \mu(gS) = \mu(\{gs : s \in S\})$ and a right invariant measure ν is such that $\nu(S) = \nu(Sg) = \nu(\{sg : g \in G\})$ for all $g \in G$ and open sets S.

[5]Throwing a ball up doesn't make it shrink spontaneously.

Definition 4.3 (Extended real numbers)**.** The extended real number system is the set $\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, +\infty\}$, the ordinary real numbers along with the symbols $-\infty$ and $+\infty$; $\overline{\mathbb{R}}$ can be turned into a totally ordered set by defining $-\infty \leq a$ and $a \leq +\infty$ for all $a \in \overline{\mathbb{R}}$.

The usual arithmetic operations $(+, -, \cdot, /)$ on $\mathbb{R}$ can be partially extended to $\overline{\mathbb{R}}$, in the way you would expect:

- $a \pm \infty = \pm\infty + a = \pm\infty, \quad a \neq \mp\infty,$
-

Definition 4.4 (Measure)**.** A *measure* μ on a measurable space $(X, \mathcal{A})$ is a function $\mu : \mathcal{A} \to [0, \infty]$ such that:

- $\mu(\varnothing) = 0$ and,
- if $\{A_i\}_{i\in I}$ is a collection of countably many elements in $\mathcal{A}$ that are pairwise disjoint, then

$$\mu\left(\bigcup_{i\in I} A_i\right) = \sum_{i\in I} \mu(A_i).$$

A measure space is the triple $(X, \mathcal{A}, \mu)$ where μ is a measure on the measurable space $(X, \mathcal{A})$.

Example. Let X be a finite set. Then we may take $\mathcal{A} = \mathcal{P}(X)$ and $\mu(A) = |A|$ for all $A \in \mathcal{P}(X)$, where $|A|$ denotes the cardinality of the set A; this is known as the counting measure.

Remark 4.5. We can use this definition to derive other basic properties of a measure. For instance, let $A_1, A_2 \in \mathcal{A}$ such that $A_1 \subseteq A_2$. Then, the countable additivity of of μ means that

$$\mu(A_2) = \mu\left((A_2 \setminus A_1) \cup A_1\right) = \mu(A_2 \setminus A_1) + \mu(A_1) \geq \mu(A_1),$$

where the last inequality follows as μ takes non-negative extended real numbers. Thus, if A_1 is contained within A_2, then its size is bounded by the size of A_2, exactly as one would expect.

4.1.2. *Integration via Measures.* To see why a measure could be used to define the integral of a function $f : X \to \mathbb{R}$ (where $(X, \mathcal{A}, \mu)$ is a measure space), let's consider an indicator-like function. In particular, define $f_A : X \to \mathbb{R}$ for a $A \in \mathcal{A}$ by $f_A(x) = a$ for $x \in A$ and $f_A(x) = 0$ otherwise. What should be expect the integral of f over X to be? Well, it should be a, the scale factor, times the size of the set A, or $a\mu(A)$ in symbols!

Similarly, we define the integral of a general step function.

Definition 4.6. Let (X, A, μ) be a measure space, and A be a measurable set. The indicator function $\mathbf{1}_A : X \to \mathbb{R}$ is defined by $\mathbf{1}_A(x) = 1$ if $x \in A$ and $\mathbf{1}_A(x) = 0$ otherwise. The integral of the $\mathbf{1}_A$ over X with respect to the measure μ is defined by

$$\int_X \mathbf{1}_A \, d\mu = \mu(A).$$

Furthermore, we require that for all measurable functions $f_1, f_2 : X \to \mathbb{R}$ we have

$$\int_X (f_1 + f_2) \, d\mu = \int_X f_1 \, d\mu + \int_{X_2} f_2 \, d\mu$$

Let $A_1, \cdots, A_n$ be a collection of pairwise disjoint measurable sets. Then,

$$\int_X \sum_{i=1}^{n} a_1 \mathbf{1}_{A_i} \, d\mu = \sum_{i=1}^{n} a_i \mu(A_i).$$

Let $f : X \to \mathbb{R}$ be a measurable function such that $f(x) \geq 0$. Then, we define

$$\int_X f \, d\mu = \sup\left\{ \int \varphi \, d\mu : \varphi \text{ is a step function and } \varphi \leq f \right\}.$$

4.2. **The Haar Measure.**

4.3. **The Haar Measure on $\mathbb{Q}_p$.** Let $\mu_{\mathbb{Q}_p}$ denote the Haar measure on $\mathbb{Q}_p$. Hang on, though. A Haar measure on a LCA group G is unique only upto multiplication by a constant, so we normalize $\mu_{\mathbb{Q}_p}$ so that $\mu_{\mathbb{Q}_p}(\mathbb{Z}_p) = 1$. This is analogous to how $\lambda([0,1]) = 1$. Let's investigate $\mu_{\mathbb{Q}_p}$!

Proposition 4.7. *We have* $\mu(p\mathbb{Z}_p) = \frac{1}{p}$.

Proof. We're going to leverage the translation invariance of $\mu_{\mathbb{Q}_p}$. As $p\mathbb{Z}_p$ is a subgroup of $\mathbb{Z}_p$, we can decompose $\mathbb{Z}_p$ as the union of the $p\mathbb{Z}_p$-cosets of $\mathbb{Z}_p$:

$$\mathbb{Z}_p = \bigcup_{a \in \mathbb{Z}/p\mathbb{Z}} (a + p\mathbb{Z}_p). \tag{4.1}$$

Taking the measure of both sides, we see that

$$1 = \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \mu_{\mathbb{Q}_p}(a + p\mathbb{Z}_p), \tag{4.2}$$

where we used the σ-additivity to simplify the right hand side. Notice that $a + p\mathbb{Z}_p$ is a translate of $p\mathbb{Z}_p$, so that $\mu(a + p\mathbb{Z}_p) = \mu(p\mathbb{Z}_p)$ for all $a \in \mathbb{Z}/p\mathbb{Z}_p$. Thus, as there are $|\mathbb{Z}/p\mathbb{Z}| = p$ translates on the right side, the equation boils down to

$$1 = p \cdot \mu_{\mathbb{Q}_p}(p\mathbb{Z}_p).$$

Dividing both sides by p to solve for $\mu_{\mathbb{Q}_p}(p\mathbb{Z}_p)$, we get $\mu_{\mathbb{Q}_p}(p\mathbb{Z}_p) = \frac{1}{p}$, as promised. ∎

In general, we have the following.

Proposition 4.8. *We have* $\mu_{\mathbb{Q}_p}(p^k\mathbb{Z}_p) = p^{-k}$ *for all integers* k.

Exercise. Prove Proposition 4.8.

We can use Proposition 4.8 to compute some basic p-adic integrals. For instance, straight from the definition of an integral we see that

$$\int_{\mathbb{Q}_p} \mathbf{1}_{p^k\mathbb{Z}_p} \, d\mu_{\mathbb{Q}_p} = p^{-k},$$

where $\mathbf{1}_{p^k\mathbb{Z}_p}$ is the indicator function of $p^k\mathbb{Z}_p$ as a subset of $\mathbb{Q}_p$, we can also handle slightly more complex integrals by splitting the domain of integration suitably.

Proposition 4.9. *Let* $s \geq 0$ *be a real number and* $d \geq 0$ *be an integer. Then we have*

$$\int_{\mathbb{Z}_p} |x^d|_p^s \, d\mu_{\mathbb{Q}_p} = \frac{p-1}{p - p^{-ds}}.$$

Proof. While this integral may look significantly more complicated than that of $\mathbf{1}_{p^k\mathbb{Z}_p}$ over $\mathbb{Z}_p$ at first glance, the integrand here is just a sum of scaled indicator functions. Indeed, if $x \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$, then $|x|_p = 1$, so $\left|x^d\right|_p^s = 1$; if $x \in p\mathbb{Z}_p \setminus p^2\mathbb{Z}_p$ then $|x|_p = p^{-1}$, so $\left|x^d\right|_p^s = p^{-ds}$, and so on. In general, if $x \in p^k\mathbb{Z}_p \setminus p^{k+1}\mathbb{Z}_p$, then $\left|x^d\right|_p^s = p^{-kds}$ for all $k \geq 0$. Thus, we have

$$|x^d|_p^s = \sum_{k \geq 0} p^{-kds} \mathbf{1}_{p^k\mathbb{Z}_p \setminus p^{k+1}\mathbb{Z}_p}(x),$$

for all $x \in \mathbb{Z}_p$. Now, we can easily evaluate the integral of $|x^d|_p^s$ over $\mathbb{Z}_p$:

$$\begin{aligned}\int_{\mathbb{Z}_p} |x^d|_p^s \, d\mu_{\mathbb{Q}_p} &= \int_{\mathbb{Z}_p} \sum_{k\geq 0} p^{-kds} \mathbf{1}_{p^k\mathbb{Z}_p \setminus p^{k+1}\mathbb{Z}_p} \, d\mu_{\mathbb{Q}_p} = \sum_{k\geq 0} p^{-kds} \int_{\mathbb{Z}_p} \mathbf{1}_{p^k\mathbb{Z}_p \setminus p^{k+1}\mathbb{Z}_p} \, d\mu_{\mathbb{Q}_p} \\ &= \sum_{k\geq 0} p^{-kds} \left(\mu_{\mathbb{Q}_p}(p^k\mathbb{Z}_p \setminus p^{k+1}\mathbb{Z}_p)\right) = \sum_{k\geq 0} p^{-kds} \left(\mu_{\mathbb{Q}_p}\left(p^k\mathbb{Z}_p\right) - \mu_{\mathbb{Q}_p}\left(p^{k+1}\mathbb{Z}_p\right)\right) \\ &= \sum_{k\geq 0} p^{-kds} \left(p^{-k} - p^{-(k+1)}\right) = \left(1 - p^{-1}\right) \sum_{k\geq 0} p^{-k(1+ds)} = \left(1 - p^{-1}\right) \cdot \frac{1}{1 - p^{-(1+ds)}} \\ &= \frac{p-1}{p - p^{-ds}},\end{aligned}$$

as desired. ∎

5. Fourier Analysis: The General Setup

Definition 5.1 (Character)**.** A character of a locally compact abelian group G is a continuous homomorphism $\chi : G \to \mathbb{S}$.

Definition 5.2 (Dual group)**.** The group of all characters of a group G is called the dual group of G and is denoted by $\widehat{G}$.

Proposition 5.3 (Double dual)**.** *There is a canonical isomorphism* $G \cong \widehat{\widehat{G}}$.

Definition 5.4. A character of a locally compact abelian group G is a continuous group homomorphism $\chi : G \to \mathbb{S}$.

Remark 5.5. Spelling the details out, $\chi(x \cdot y) = \chi(x)\chi(y)$ for $x, y \in G$, and for any open set V in the unit circle $\mathbb{S}$, $\chi^{-1}(V)$ is *also* open in G.

Definition 5.6 (Generalized L^p-spaces)**.** Define the inner product of two functions $f_1, f_2 : G \to \mathbb{C}$ by

$$\langle f_1, f_2 \rangle_G = \int_G f_1(x)\overline{f_2(x)} \, d\mu(x).$$

The norm induced by this inner product is

$$\|f\|_G = \sqrt{\langle f, f \rangle_G} = \sqrt{\int_G |f(x)|^2 \, d\mu(x)}.$$

In general, we define

$$L^p(G) = \left\{ f : G \to \mathbb{C} : \int_G |f(x)|^p \, d\mu(x) < \infty \right\}.$$

For instance, when $p = 2$, we have $L^2(G) = \{f : G \to \mathbb{C} : \|f\|_G < \infty\}$.

Definition 5.7 (Fourier Transform)**.** Let $f \in L^1(G)$. Then the Fourier transform $\hat{f} : \widehat{G} \to \mathbb{C}$ is defined by

$$\hat{f}(\chi) = \int_{\widehat{G}} f(x)\overline{\chi(x)} \, d\mu(x).$$

Proposition 5.8. *For each Haar measure μ on G, there is a unique Haar measure ν on $\widehat{G}$ such that whenever $f \in L^1(G)$ and $\hat{f} \in L^1(\widehat{G})$, we have*

$$f(x) = \int_{\widehat{G}} \widehat{f}(\chi)\chi(x) \, d\nu(\chi),$$

holds μ-almost everywhere.

6. Characters of $\mathbb{Q}_p$

Definition 6.1. Write an $x \in \mathbb{Q}_p$ as the series $x = \sum_{n=-N}^{\infty} a_n p^n$, where N is a non-negative integer. Then the fractional part $\{x\}_p$ of x is defined to be the rational number $\{x\}_p = \sum_{n=-N}^{-1} a_n p^n$.

We can now characterize all the characters of $\mathbb{Q}_p$.

Proposition 6.2. *Define the function $\chi_1 : \mathbb{Q}_p \to \mathbb{S}$ by $\chi_1(x) = e^{2\pi i \{x\}_p}$ for all $x \in \mathbb{Q}_p$, and $\chi_y : \mathbb{Q}_p \to \mathbb{S}$ for $y \in \mathbb{Q}_p$ by $\chi_y(x) = \chi_1(xy)$. Then all the χ_y's are characters of $\mathbb{Q}_p$, and, conversely, all characters of $\mathbb{Q}_p$ are of the form χ_y for a $y \in \mathbb{Q}_p$.*

Proof. For the other inclusion, let $\chi \in \hat{\mathbb{R}}$. As χ is a homomorphism, it must take the identity of $\mathbb{R}$ to the identity of $\mathbb{S}$. In symbols, $\chi(0) = 1$.

So,

Moreover, as χ is continuous, we can ensure that $\chi(x)$ is arbitrarily close to 1 by choosing x sufficiently close to 0. Another possible way to phrase this is that there exists a $\delta > 0$ such that

$$\int_0^{\delta} \chi(t)\, dt = a,$$

where a is a non-zero complex number. Thus,

$$a\chi(x) = \chi(x) \int_0^{\delta} \chi(t)\, dt = \int_0^{\delta} \chi(x)\chi(t)\, dt = \int_0^{\delta} \chi(x+t)\, dt = \int_x^{x+\delta} \chi(t)\, dt.$$

Solving for $\chi(x)$, we see

$$\chi(x) = a^{-1} \int_x^{x+\delta} \chi(t)\, dt$$

∎

7. An Integral Representation for the Zeta Function

Proposition 7.1. *For s such that $\Re(s) > 1$, we have that*

$$\zeta(s) = \lim_{\varepsilon \to 0^+} \int_{\varepsilon}^{\infty} \frac{x^{s-1}}{e^x - 1}\, dx = \int_0^{\infty} \frac{x^{s-1}}{e^x - 1}\, dx.$$

Proof. Multiplying the numerator and denominator of the integrand by the function e^{-x} yields

$$I(s) = \int_0^{\infty} x^{s-1} \frac{e^{-x}}{1 - e^{-x}}\, dx.$$

The $(1 - e^{-x})^{-1}$ ∎

8. Diversion: Riemann Surfaces

8.0.1. *The Complex Logarithm.* In this section, we will attempt to define the logarithm function on the complex numbers. As we'll see, this is significantly more tricky than the real case, and will lead us to the notion of a Riemann surface. Let z be a non-zero complex number, and let $w \in \mathbb{C}$ be such that $e^w = z$; write w as $a + bi$, where a is the real part of w and b is its imaginary part. Our goal is to solve for a and b in terms of z. First, note that

$$e^w = e^{a+bi} = e^a(\cos b + i \sin b) = z.$$

Taking the absolute value of both sides, we get $e^a = |z|$, and solving for a yields $a = \log |z|$, where $\log : \mathbb{R}^+ \to \mathbb{R}$ here is just the usual logarithm function on the positive real numbers.

On the other hand, solving for b is more subtle; let $0 \leq \theta < 2\pi$ be the principal argument of z.[6] Then, upon equating the real and imaginary parts of $z/|z| = e^{i\theta}$ and $w/|w| = e^{ib}$, we see that

$$\cos\theta = \cos b \quad \text{and} \quad \sin\theta = \sin b.$$

Clearly $b = \theta$ works, but is this the only possible value of b?

Recall that cosine and sine both have period 2π. Thus,

$$\cos(b + 2\pi k) = \cos(b) \quad \text{and} \quad \sin(b + 2\pi k) = \sin(b),$$

for all integers k. Hence, the possible values of b are $\theta + 2\pi k$, where k is an arbitrary integer; there are infinitely man choices for b! Instead of a *unique* complex number w such that $e^w = z$, we have the infinite *set set* $W = \{\log|z| + i(\theta + 2\pi k) : k \in \mathbb{Z}\}$, such that $e^w = z$ for all $w \in W$! For instance, when $z = 1 + i$, we have

$$W = \left\{\log\sqrt{2} + i\frac{\pi k}{4} : k \in \mathbb{Z}\right\}.$$

The *distinct* complex numbers

$$\cdots, \log\sqrt{2} + i\frac{\pi}{4}, \log\sqrt{2} + i\frac{9\pi}{4}, \log\sqrt{2} + i\frac{17\pi}{4}, \cdots$$

are *all* valid 'logarithms' of $1 + i$!

At first glance, one possible solution to deal with the apparent multivalued-ness of the complex logarithm is to simply require $0 \leq b < 2\pi$, just as we restricted the argument of z. So, we may define the function $\mathrm{Log}_{[0,2\pi)} : \mathbb{C}^\times \to \mathbb{C}$ by

$$\mathrm{Log}_{[0,2\pi)}(re^{i\theta}) = \log r + i\theta,$$

which is a well-defined function on $\mathbb{C}^\times$.

Alas, this function isn't continuous! To see why, we have to take a walk along the unit circle

$$\mathbb{S} = \{z \in \mathbb{C} : |z| = 1\}.$$

The point 1 is as good as any another, so let's start walking along $\mathbb{S}$ counterclockwise from there. Here, we have $\mathrm{Log}_{[0,2\pi)}(z) = 1$, which has real part $|z| = 1$ and imaginary part $\arg(z) = 0$; as we pass the point $z = e^{i\pi/4}$, the real part of $\mathrm{Log}_{[0\pi,2\pi)}(z)$ is the same as it was at $z = 1$, but the imaginary part has increased to $\arg(z) = \pi/4$.

This phenomena continues all the way. Fast forwarding, we see that for points z_ε on $\mathbb{S}$ *just* below 1, making a tiny but non-zero acute angle of magnitude ε with the positive real axis, $\mathrm{Log}_{[0,2\pi)}(z_\varepsilon)$ is $1 + i(2\pi - \varepsilon)$. Taking the limit of both sides as $\varepsilon \to 0^+$, we see

$$\lim_{\varepsilon \to 0^+} \mathrm{Log}_{[0,2\pi)}(z_\varepsilon) = 1 + 2\pi i.$$

Now, *if* $\mathrm{Log}_{[0,2\pi)}(z)$ were continuous, then the left hand side would reduce to $\mathrm{Log}_{[0,2\pi)}(1)$ (as the z_ε's go to 1 as ε diminishes), which we already computed to be 1; this implies $1 = 1 + 2\pi i$, which is nonsense!

8.0.2. *Post-mortem Analysis.* From our stroll above, we see that $\mathrm{Log}_{[0,2\pi)}$ *wants* differentiate between the input complex number 1, and the input number 1 *after traversing the unit circle once.* Now, there's nothing special about 1 or just a *single* round around a circle encircling 0: the logarithm function *wants* to consider the 'complex number with magnitude r and argument θ to be distinct from the complex number with the same magnitude but argument $2\pi k + \theta$', where $k \in \mathbb{Z}\setminus\{0\}$ (the latter is obtained from the former number by going around zero k times). If we can force this to happen, then the function $\mathrm{Log}(re^{i\theta}) = \log r + i\theta$ would be well-defined and continuous. While we won't be able to do such a thing in $\mathbb{C}$, we will be able to on an object that contains

[6] That is, $z = |z|e^{i\theta}$.

infinitely many copies of $\mathbb{C}$, the so-called Riemann surface (of the logarithm function), which we define formally below.

Definition 8.1 (Riemann surface)**.** For each integer k, define the set S_k as a subset of $\mathbb{R}^2$ by

$$S_k := \{(r, \theta) : r > 0, 2\pi k \leq \theta \leq 2\pi(k+1)\}.$$

Note that S_k can be viewed as a topological space, with the usual Euclidean topology inherited from $\mathbb{R}^2$. Then, the Riemann surface of the logarithm function, denoted by X or $\widetilde{\mathbb{C}^\times}$, is defined to be the topological space

$$X = \bigsqcup_{k \in \mathbb{Z}} S_k / \sim,$$

where $\sim$ is the equivalence relation on the disjoint union $\bigsqcup_{k\in\mathbb{Z}} S_k$ defined by $(r, 2\pi(k+1), k) \sim (r, 2\pi k(k+1), k+1)$ for all $r > 0$ and integers k.

Remark 8.2. Most of the times, we write X as the set of all ordered pairs (r, θ), where $r > 0$ and $\theta \in \mathbb{R}$, dropping the index introduced by the disjoint union.

Informally, if we begin walking around 0, we start on S_0, and for each round completed, we move from the kth surface, S_k to *next* surface, S_{k+1}, a fresh copy of $\mathbb{C}$, instead of staying stuck at S_k, as we would have with in the usual complex numbers. However, to ensure continuity, we need to ensure that the place where where we make our last footstep in S_k is the same place where we make our first footstep in S_{k+1}, which is taken care of by the equivalence relation $\sim$.

The Riemann surface also comes with a canonical projection map $\pi : X \to \mathbb{C}^\times$, which essentially collapses all the copies of $\mathbb{C}^\times$ in X into a single instance (that is, it re-glues), defined by $\pi((r, \theta)) = re^{i\theta}$, for all $(r, \theta) \in X$.

And, of course, we can now define our continuous logarithm function!

Definition 8.3. Define the function $\mathrm{Log} : X \to \mathbb{C}^\times$ by $\mathrm{Log}((r, \theta)) = \log r + i\theta$, where the logarithm on the right side is the usual logarithm on the positive real numbers.

8.0.3. *Integration on Manifolds.*

Definition 8.4 (Manifold)**.** An n-dimensional *manifold* is a Hausdorff topological space X such that for each $x \in X$, there exists an open neighborhood $U \subseteq X$ of x that is homeomorphic to an open set of $\mathbb{R}^n$.

Let $\mathbb{S}$ be the unit circle. As a subset of $\mathbb{R}^2$, this is written as $\mathbb{S} = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$ or $\mathbb{S} = \{(\cos\theta, \sin\theta) : \theta \in [0, 2\pi)\}$.

Definition 8.5. An *Euclidean neighborhood* U of a n-dimensional manifold X is an open set of X that is homeomorphic to an open set of $\mathbb{R}^n$. A *coordinate chart* an Euclidean neighborhood U is a homeomorphism $\phi : U \to \phi(U) \subseteq \mathbb{R}^n$.

Remark 8.6. A topological space X is locally Euclidean if and only if there exists a family of Euclidean neighborhoods $\{U_i\}_{i\in I}$ of X that cover X, i.e., $X = \bigcup_{i\in I} U_i$. A set of Euclidean neighborhoods that cover X, along with their coordinate charts, is said to be an *atlas* of X.

Example. Let $X = \mathbb{S}$. Then $\mathscr{A} = \{(U_1, \phi_1), (U_2, \phi_2)\}$ where $U_1 = \mathbb{S} \setminus \{(-1, 0), (0, 1)\}$ and $\phi_1(x, y) = -x/y$ for all $(x, y) \in U_1$ and $U_2 = \mathbb{S} \setminus \{(0, -1), (0, 1)\}$ and $\phi_2(x, y) = -y/x$ for all $(x, y) \in U_2$ is an atlas for the circle $\mathbb{S}$. Note that U_1 is the circle without the equator and U_2 is the circle without the poles: ϕ_1 sends a point in U_1 to the slope of its tangent line, while ϕ_2 sends a point in U_2 to the inverse of the slope of its tangent. See if you can find a similar atlas for $\mathbb{S}^2 \subseteq \mathbb{R}^3$, the sphere.

Let $p \in X$, and U be an Euclidean neighborhood of X with chart ϕ that contains p. Consider all curves $\gamma : (-1, 1) \to X$ such that $\gamma(0) = p$ (that is, all curves on X that are initialized at the point p). The velocity of γ at the point p is the derivative of the function $\phi \circ \gamma : (-1, 1) \to \mathbb{R}^n$ evaluated at 0. The tangent space of X at p, denoted by T_pX, is the set of all such velocities. However,

Definition 8.7. The tangent bundle TX of a manifold X is the disjoint union of its tangent spaces. In symbols,

$$TX := \bigsqcup_{x\in X} T_xX = \bigcup_{x\in X}\{(x,y) : y \in T_xX\} = \bigcup_{x\in X}\{x\} = \{(x,y) : x \in X, y \in T_xX\}.$$

An atlas of $\mathbb{R}^n$ as an n-dimensional manifold is $\{(U,\phi)\}$ where $U = \mathbb{R}^n$ and $\phi : U \to \mathbb{R}^n$ is the identity map. The tangent space of $\mathbb{R}^n$ is simply $\mathbb{R}^n$ itself. Thus, the $T\mathbb{R}^n = \mathbb{R}^n \times \mathbb{R}^n$.

Remark 8.8. Notice that from passing from the original manifold X to its tangent bundle TX, the dimension doubled. This is a phenomena holds in general. If X has dimension n, then TX has dimension $2n$.

Definition 8.9. The *cotangent space* of a manifold X at a point x, denoted by T_x^*X, is the dual of the tangent space of X at x. Symbolically, $T_x^*X = (T_xX)^*$.

For instance,

$$T_x^*\mathbb{R}^n = (T_x\mathbb{R}^n)^* = (\mathbb{R}^n)^* = \{\varphi : \mathbb{R}^n \to \mathbb{R} : \varphi \text{ is linear}\}.$$

Definition 8.10 (Exterior Algebra)**.** The *exterior algebra* $\Lambda(V)$ of a vector space V over a field K is defined as the quotient algebra of an the tensor algebra $T(V)$ by the ideal I generated by all elements of the form $x \otimes x$. Symbolically, $\Lambda(V) = T(V)/I$. Furthemore, the exterior product $\wedge$ of two elements of $\Lambda(V)$ is defined to by

$$x \wedge y = x \otimes y \pmod{I}.$$

Definition 8.11 (Tensor Algebra)**.** Let V be a vector space over a field K. For any non-negative integer k, we define the kth tensor power of V to be the tensor product of V with itself k times.

9. Riemann's proof of the functional equation

Definition 9.1. Define the function $f_u(x) = e^{-\pi u x^2}$ for all real x. Then if $u = 1$ f_u is its own Fourier transform.

Proposition 9.2. *The Riemann-zeta function $\zeta(s)$ satisfies the following functional equation*

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

Alternatively, if we were to define the Xi function, by

$$\Xi(s) := \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s),$$

then we have $\Xi(s) = \Xi(1-s)$.

- $$\Xi(s) = \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \int_0^\infty u^{\frac{s}{2}-1}\psi(u)\,du,$$
  where
  $$\psi(u) = \frac{1}{2}\left(\sum_{n=\infty}^{\infty} f_u(n) - 1\right)$$
- Key to showing the functional equation is the functional equation for ψ:
  $$\psi(u) = \frac{1}{\sqrt{u}}\psi\left(\frac{1}{u}\right) + \frac{1}{2\sqrt{u}} - \frac{1}{2}.$$
- $$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \frac{1}{s-1} - \frac{1}{s} + \int_1^\infty \left(u^{-\frac{s}{2}-\frac{1}{2}} + u^{\frac{s}{2}-1}\right)\psi(u)\,du.$$

10. Restrited Prouects and Adele ring

Let $(X_i)_{i\in I}$ be a family of topological spaces; the index set I can both finite and infinite. We may construct the direct product of the X_i's, denoted by $X = \prod_{i\in I} X_i$, which is simply the set of all tuples $(x_i)_{i\in I}$, where each x_i is in X_i.

This construction should be familiar. After all, the plane $\mathbb{R}^2$ is the direct product of $\mathbb{R}$ with itself. Here, however, we are also concerned with the topology of the direct product, and also the relation between the compactness of the X_i and X.

One might expect the topology on X

With the direct product, we get the canonical projection maps $\pi_i : X \to X_i$ for each i, which takes in a tuple $(x_i)_{i\in I}$ and spits out its ith component. Now, one would like each π_i to be continuous. So, what topology $\mathcal{T}$ on X makes this happen? There might be many topologies, so let's find the smallest such topology $\mathcal{T}$.

Recall that for π_i is continuous if and only if for all open sets $U_i \subseteq X_i$, $\pi_i^{-1}(U_i)$ is also open in X; clearly $\pi_i^{-1}(U_i) = \prod_{j\in I} V_j$, where $V_j = X_j$ for all $j \neq i$ and $V_i = U_i$ (that is, only the ith coordinate is restricted; all other coordinates are free). Thus, $\mathcal{T}$ is the smallest topology on X that contains $\pi^{-1}(U_i)$ for all $i \in I$. In fact, once we add intersections of finitely many $\pi^{-1}(U_i)$, we get a basis for $\mathcal{T}$.

Hence, every open set in X is the union of sets of the from

$$\prod_{i\in I} U_i,$$

where $U_i \neq X_i$ for only finitely many i.

If infinitely many X_i are not compact, then X is not locally compact, even though each X_i may be locally compact.

Definition 10.1. A topological space X is said to be *locally compact* if for every $x \in X$, there exists an open neighborhood U of x such that the closure of U is compact.

Example. The real numbers $\mathbb{R}$ are not compact, but they are locally compact. Similarly, while $\mathbb{Q}_p$ isn't compact, it is also locally compact. Hence, all the completions of $\mathbb{Q}$ are compact.

Alas, this means that $X := \mathbb{R} \times \prod_p \mathbb{Q}_p$ is not locally compact, which isn't too amazing, as locally compact spaces turn out to be a general setting where Fourier analysis can be done. This is the motivation for the restricted product.

Indeed, for the sake of contradiction, assume that X is locally compact; then, there exists $U \subseteq C \subseteq X$ where U is open and C is compact. Taking π_i of this change, we get $\pi_i(U) \subseteq \pi_i(C) \subseteq X_i$. As the image of a compact set under a continuous function is compact, $\pi_i(C)$ is also compact in X_i. Now, for infinitely many i, $\pi_i(U) = X_i$, and so $\pi_i(C) = X_i$ for infinitely many i, and so X_i is compact for infinitely many i, which is a contradiction.

Let $U \subseteq X$ be open. Then, U is a union of sets of the form $\prod_i V_i$, where $V_i \subseteq X_i$ is open; in particular, there $V = \prod_i V_i \subseteq U$ for some such set; thus, $\pi_i(V) = V_i \subseteq \pi_i(U) \subseteq X_i$ for all i. As $V_i = X_i$ for infinitely many i, $\pi_i(U) = X_i$ for infinitely many i.

Definition 10.2 (Restricted Product Topology)**.** Let $(X_i)_{i\in I}$ be a family of topological spaces, and let $(U_i)_{i\in I}$ be a family of open subsets such that $U_i \subseteq X_i$ for each $i \in I$.

The **restricted product** of the spaces X_i with respect to the open sets U_i, denoted by

$$\prod_{i\in I}{}' X_i \quad \text{or} \quad \prod_{i\in I}(X_i, U_i),$$

is the topological space whose underlying set is defined as

$$\left\{ (x_i)_{i\in I} \in \prod_{i\in I} X_i \;\middle|\; x_i \in U_i \text{ for all but finitely many } i \in I \right\}.$$

The **restricted product topology** is the topology generated by the base consisting of sets of the form

$$\prod_{i \in I} V_i$$

where $V_i \subseteq X_i$ is open for all $i \in I$, and $V_i = U_i$ for all but finitely many $i \in I$.