18.704 SPRING 2022 WEEK 1

MINH-TÂM TRINH

1. Monday (1/31)

1.1. **Welcome & Syllabus.** Itinerary:

- Learn everyone's names, year at MIT, and major
- Discuss syllabus
- Discuss textbook & supplements
- Discuss tentative schedule
- Begin sign-ups for block 1 (at least through week 2)

1.2. **Classical Fourier Analysis.** What is Fourier analysis? It begins with the observation that if a function $f : \mathbf{R} \to \mathbf{R}$ is *periodic*, and sufficiently tame, then it can be decomposed as a sum of rescaled cosine and/or sine functions, whose periods are integer subdivisions of the period of f.

For instance, let $\lfloor x \rfloor$ be the largest integer less than or equal to x, and let $s(x) = x - \lfloor x \rfloor$. This is a sawtooth function that satisfies $s(x+1) = s(x)$. It turns out that for any $x \notin \mathbf{Z}$, we have

$$s(x) = \frac{1}{2} - \sum_{m=1}^{\infty} \frac{1}{\pi m} \sin(2\pi m x).$$

The right-hand side is called the Fourier series of s. In general, the sense in which a Fourier series converges to the original function may be more delicate.

Why would we want to decompose a function into trigonometric functions? One reason is our intuition that trigonometric functions are simpler than many other periodic functions. And one way to justify the word "simpler" is to observe that cosine and sine are *eigenfunctions* of the differential operator $\mathscr{D}^2$, where $\mathscr{D} = \frac{d}{dx}$. That is, the set of all (smooth) real-valued functions forms a vector space, $\mathscr{D}^2$ forms a linear operator on this vector space, and $\cos(\alpha x)$ and $\sin(\alpha x)$ belong to the $(-\alpha^2)$-eigenspace of $\mathscr{D}^2$.

Due to this property, trigonometric functions occupy an important role in the theory of linear differential equations. Joseph Fourier (1768–1830) developed the series expansion bearing his name to solve the 1-dimensional heat equation, which governs the flow of heat in a thin conductive rod. Fourier expansion allows us to write the general solution to the heat equation as a superposition of separable solutions, each having an essentially trigonometric form.

But it would be cleaner to use eigenfunctions of $\mathscr{D}$ rather than $\mathscr{D}^2$. For instance, if we allow *complex-valued* functions, then $e^{i\alpha x}$ is a natural choice. This is no loss of richness because $\cos(\alpha x) = \frac{1}{2}(e^{i\alpha x} + e^{-i\alpha x})$ and $\sin(\alpha x) = \frac{1}{2i}(e^{i\alpha x} - e^{-i\alpha x})$.

Moreover, after rescaling, we may assume that the functions we are studying have period 1. Then, instead of working with periodic functions on the real line $\mathbf{R}$, we can work with functions on the quotient group $\mathbf{R}/\mathbf{Z}$.

With these replacements, we arrive at the following version of the Fourier series expansion. For any $\alpha \in \mathbf{R}$, let

$$e_\alpha(x) = e^{2\pi i\alpha x}.$$

If $f : \mathbf{R}/\mathbf{Z} \to \mathbf{C}$ is absolutely integrable, then there are complex numbers $\hat{f}(n)$, indexed by $n \in \mathbf{Z}$, such that

$$f(x) = \sum_n \hat{f}(n)e_n(x)$$

at any point x where f is continuous, where $\sum_n = \lim_{N\to\infty} \sum_{|n|\leq N}$. It turns out there is an explicit formula for the $\hat{f}(n)$: namely,

$$\hat{f}(n) = \int_0^1 f(x)e_n(-x)\,dx.$$

The absolute integrability of f ensures the convergence of the right-hand side. This formula, together with some more analysis, leads to an essentially constructive proof of the expansion.

Example 1.1. For the sawtooth function s, we compute:

$$\hat{s}(n) = \int_0^1 xe^{-2\pi inx}\,dx = \begin{cases} \frac{1}{2} & n = 0 \\ \frac{i}{2\pi n} & n \neq 0 \end{cases}$$

So the Fourier series is

$$\begin{aligned} \sum_n \hat{s}(n)e^{2\pi inx} &= \hat{s}(0) + \sum_{m=1}^{\infty} \left(\hat{s}(m)e^{2\pi imx} + \hat{s}(-m)e^{-2\pi imx}\right) \\ &= \frac{1}{2} + \sum_{m=1}^{\infty} \left(\frac{i}{2\pi m}e^{2\pi imx} - \frac{i}{2\pi m}e^{-2\pi imx}\right) \\ &= \frac{1}{2} - \sum_{m=1}^{\infty} \frac{1}{\pi m}\sin(2\pi mx), \end{aligned}$$

as we claimed before.

This entire story admits an analogue for *non-periodic* functions on the real line. If $f : \mathbf{R} \to \mathbf{C}$ is integrable, then we define its Fourier transform $\hat{f} : \mathbf{R} \to \mathbf{C}$ by:

$$\hat{f}(\alpha) = \int_{-\infty}^{\infty} f(x)e_\alpha(-x)\,dx.$$

It turns out that if f and $\hat{f}$ are both absolutely integrable, then we have

$$f(x) = \int_{-\infty}^{\infty} \hat{f}(\alpha)e_\alpha(x)\,d\alpha$$

at any point x where f is continuous. This so-called Fourier inversion formula is the analogue of the Fourier series expansion.

1.3. **General Groups.** We will be interested in the algebraic structure of Fourier analysis. In particular, we want to generalize it beyond $\mathbf{R}/\mathbf{Z}$ and $\mathbf{R}$.

To motivate what follows, note that there is another class of operators for which the e_α are eigenfunctions. If $\mathcal{T}_\beta$ is the translation-by-β operator $\mathcal{T}_\beta f(x) = f(x-\beta)$, then $\mathcal{T}_\beta e_\alpha = e^{-2\pi i\alpha\beta} e_\alpha$. This just reformulates the fact that e_α turns addition into multiplication, or in other words, that e_α defines a group homomorphism from the additive group $\mathbf{R}$ into the multiplicative circle group

$$\begin{aligned} \mathbf{T} &\coloneqq \exp(2\pi i(\mathbf{R}/\mathbf{Z})) \\ &= \{z \in \mathbf{C} \mid |z| = 1\}. \end{aligned}$$

The homomorphism factors through $\mathbf{R}/\mathbf{Z}$ if and only if α is an integer.

Going somewhat beyond the scope of the course, let us give the big picture, following Chapter 3 of the book [1] by Ramakrishnan and Valenza.

Let G be a locally-compact, Hausdorff topological abelian group. (If you don't know topology, just ignore the first three adjectives.) There is another topological group called the *dual* of G and denoted $\hat{G}$. The elements of $\hat{G}$ are the continuous homomorphisms $\chi : G \to \mathbf{T}$, also known as the *(degree-*1*, unitary) characters* of G. The group operation on $\hat{G}$ is pointwise composition, meaning $(\chi_1 \cdot \chi_2)(x) = \chi_1(x)\chi_2(x)$, and the identity element is the constant map $1 : G \to \mathbf{T}$.

A deep theorem states that G admits a nonzero, translation-invariant measure, known as a *Haar measure*. It induces a corresponding Haar measure on $\hat{G}$. It moreover lets us define the vector space $L^1(G)$ of (absolutely) integrable functions $f : G \to \mathbf{C}$. The *Fourier transform* of f is the function $\hat{f} : \hat{G} \to \mathbf{C}$ given by

$$\hat{f}(\chi) = \int_G f(x)\chi(x^{-1})\,dx. \tag{1.1}$$

If $\hat{f} \in L^1(\hat{G})$, then we have a Fourier inversion formula

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

at any element x where f is continuous. This formalism does indeed generalize our earlier discussion:

Example 1.2. If $G = \mathbf{R}/\mathbf{Z}$, then the dual group $\hat{G}$ consists of the exponential functions $e_n(x) = e^{2\pi i n x}$ for $n \in \mathbf{Z}$. The map $n \mapsto e_n$ is an isomorphism $\mathbf{Z} \xrightarrow{\sim} \widehat{\mathbf{R}/\mathbf{Z}}$. In this way, we recover classical Fourier series.

Example 1.3. If instead, $G = \mathbf{R}$, then the dual group $\hat{G}$ consists of the functions $e_\alpha(x) = e^{2\pi i\alpha x}$ for arbitrary $\alpha \in \mathbf{R}$. The map $\alpha \mapsto e_\alpha$ is an isomorphism $\mathbf{R} \xrightarrow{\sim} \hat{\mathbf{R}}$. In this way, we recover the classical Fourier transform.

Sometimes it is more useful to work with square-integrable, rather than integrable, functions. The vector space $L^2(G)$ of square-integrable functions $f : G \to \mathbf{C}$ forms a Hilbert space, equipped with the inner product

$$\langle f, g\rangle = \int_G f(x)\overline{g(x)}\,dx.$$

We can use (1.1) to define the Fourier transform on $L^1(G) \cap L^2(G) \subseteq L^2(G)$; then, by a density argument, it extends to a linear map

$$\mathscr{F} : L^2(G) \to L^2(\hat{G}).$$

A result called the Parseval–Plancherel theorem states that this map is an isometry with respect to $\langle -, - \rangle$, meaning $\langle \mathscr{F} f, \mathscr{F} g \rangle = \langle f, g \rangle$.

As this is an algebra course, we want to avoid the technicalities of integration as much as possible. So we will stick to the case where G is *finite* (and hence discrete). We will be interested in what Fourier *a.k.a.* harmonic analysis on G can tell us about other branches of mathematics. For instance, if p is a prime, then the Parseval–Plancherel theorem on $\mathbf{Z}/p\mathbf{Z}$ can be used to compute the magnitude of the Gauss sum associated with p in number theory. We will also study how harmonic analysis can be extended to nonabelian groups: a subject better known as representation theory.

2. Wednesday (2/2)

2.1. **Anatomy of a Talk.** Susan Ruff came to this class to speak about the components of a good talk. She discussed the findings of education research about the relative effectiveness of different methods of instruction. Lecturing is relatively ineffective, and "discovery-based learning" has mixed outcomes, but lecturing with a significant interactive component (*e.g.*, clicker questions) does much better.

On the chalkboards, we brainstormed different ways that teachers could keep their students engaged during class time. We then discussed ways for a speaker to handle questions met with silence, like breaking the question into simpler pieces, or backing up slightly in the material.

Finally, Susan presented an outline of the steps involved in preparing a talk:

(1) Learning the content.
(2) Deciding what the audience needs.
(3) Deciding what is hard or subtle, and how to help.
(4) Structuring the talk.
(5) Planning board space.
(6) Practicing.
(7) Revising.

This outline is only meant as a guide. The key takeaway is that "learning the content" is merely the first step of many.

2.2. **The Space of Functions.** We now follow Terras, Chapter 2, pages 31-37.

Let X be a finite set. (Terras starts out with a group G in place of X, but we won't use any group structure on X today.) We write $L^2(X)$ for the vector space of all complex-valued functions on S. For all $f, g \in L^2(X)$, we set

$$\langle f, g \rangle = \sum_{x \in X} f(x)\overline{g(x)},$$

where $\overline{(-)}$ means complex conjugation. Then $\langle -, - \rangle$ is a hermitian inner product on $L^2(X)$. This means:

(1) $\langle af_1 + f_2, g\rangle = a\langle f_1, g\rangle + \langle f_2, g\rangle$ for any $a \in \mathbf{C}$.
(2) $\langle f, g\rangle = \overline{\langle g, f\rangle}$.
(3) $\langle f, f\rangle \geq 0$, with equality if and only if f is the zero function.

In particular, we can define a norm on $L^2(X)$ by setting

$$\|f\| = \sqrt{\langle f, f\rangle}.$$

This means:

(1) $\|af\| = |a|\|f\|$ for any $a \in \mathbf{C}$.
(2) $\|f\| \geq 0$, with equality if and only if f is the zero function.
(3) Triangle inequality. $\|f + g\| \leq \|f\| + \|g\|$.

One can also derive the Cauchy–Schwarz inequality $|\langle f, g\rangle| \leq \|f\|\|g\|$.

Exercise 2.1. Fix $f, g \in L^2(X)$ and let $P(t) = \|tf + g\|^2$. This is a quadratic polynomial in t. Using the nonnegativity of $P(t)$ for real t, together with the quadratic formula, deduce the Cauchy–Schwarz and triangle inequalities.

There is an obvious basis for $L^2(X)$: namely, the collection of delta functions δ_a as we run over all $a \in X$. By definition, $\delta_a(x)$ equals 1 when $x = a$, and equals 0 otherwise. Tautologically, this basis is orthonormal with respect to $\langle -, -\rangle$, meaning $\langle \delta_a, \delta_b\rangle$ equals 1 when $a = b$, and equals 0 otherwise.

Now set $X = \mathbf{Z}/n\mathbf{Z}$. There is a less obvious orthogonal basis for $L^2(\mathbf{Z}/n\mathbf{Z})$. Namely, for all $a \in \mathbf{Z}/n\mathbf{Z}$, let

$$e_a(x) = e^{2\pi i a x/n},$$

modifying our notation from Monday. We can view e_a as a homomorphism from $\mathbf{Z}/n\mathbf{Z}$ into the circle group $\mathbf{T} = \{z \in \mathbf{C} \mid |z| = 1\}$. In particular, $\overline{e_a(x)} = e_a(-x)$.

Lemma 2.2 ([2, 38])**.** *The functions e_a, as a runs over $\mathbf{Z}/n\mathbf{Z}$, form a basis for $L^2(\mathbf{Z}/n\mathbf{Z})$ such that*

$$\langle e_a, e_b\rangle = \begin{cases} n & a \equiv b \\ 0 & \textit{else} \end{cases}$$

In particular, the functions $\frac{1}{\sqrt{n}}e_a$ are orthonormal with respect to $\langle -, -\rangle$.

In fact, the linear independence of the functions e_a is a *consequence* of the orthogonality identity above.

3. Friday (2/4)

3.1. **The Fourier Transform.** The discrete Fourier transform (DFT) of a function $f \in L^2(\mathbf{Z}/n\mathbf{Z})$ is the function $\mathscr{F}f \in L^2(\mathbf{Z}/n\mathbf{Z})$ defined by

$$\mathscr{F}f(a) := \langle f, e_a\rangle = \sum_{x \in \mathbf{Z}/n\mathbf{Z}} f(x)e_a(-x).$$

This can be viewed as a linear operator on $L^2(\mathbf{Z}/n\mathbf{Z})$.

For instance, if $n = 4$, then the matrix of $\mathscr{F}$ with respect to the ordered basis $(\delta_0, \delta_1, \delta_2, \delta_3)$ is given (in column notation) by

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{pmatrix}$$

because $i = e_4(1)$. In general, we find:

- $\mathscr{F}\delta_b = \bar{e}_b$, because $e_b(-a) = e_a(-b)$.
- $\mathscr{F}e_b = n\delta_b$, by Lemma 2.2.

Above, we are implicitly using the notation $\bar{e}_b(x) \coloneqq \overline{e_b(x)}$.

3.2. **Convolution.** One big motivation for $\mathscr{F}$ is that it intertwines two natural notions of multiplication on $\mathbf{Z}/n\mathbf{Z}$.

More generally, let G be a finite group with binary operation $\circ$. We already know that $L^2(G)$ forms a ring via pointwise addition and multiplication:

$$(f + g)(x) = f(x) + g(x),$$
$$(f \cdot g)(x) = f(x) \cdot g(x).$$

That is, $L^2(G)$ inherits a ring structure from $\mathbf{C}$. But at the same time, $L^2(G)$ inherits a different multiplication from G. For all $f, g \in L^2(G)$, we define the *convolution* of f and g to be the function $f * g \in L^2(G)$ such that

$$(f * g)(x) = \sum_{\substack{y,z \in G \\ y \circ z = x}} f(y)g(z).$$

The associativity of $\circ$ implies the associativity of $*$:

$$((f * g) * h)(x) = \sum_{\substack{y,z,w \in G \\ y \circ z \circ w = x}} f(y)g(z)h(w) = (f * (g * h))(x).$$

If e is the identity of G, then δ_e is the identity of $L^2(G)$ with respect to convolution. By contrast, the constant function $1 \in L^2(G)$ is the identity of $L^2(G)$ with respect to pointwise multiplication.

Lastly, note that convolution is both left- and right-distributive over pointwise addition of functions. This means $L^2(G)$ forms a ring under convolution. If G is not abelian, then $*$ is not commutative.

In the case where $G = \mathbf{Z}/n\mathbf{Z}$, convolution looks like

$$(f * g)(x) = \sum_{y \in \mathbf{Z}/n\mathbf{Z}} f(y)g(x - y).$$

For the special functions δ_a and e_a discussed earlier, we find:

- $(f * \delta_a)(x) = f(x - a)$. In particular, $\delta_a * \delta_b = \delta_{a+b}$.
- $(f * e_a)(0) = \mathscr{F}f(a)$.

There is no simple formula for $f * e_a$ itself.

3.3. **Properties of the DFT.** We follow Terras, Chapter 2, pages 37-44.

Theorem 3.1 ([2, 36])**.** *The linear operator* $\mathscr{F} : L^2(\mathbf{Z}/n\mathbf{Z}) \to L^2(\mathbf{Z}/n\mathbf{Z})$ *satisfies these properties:*

(1) $\mathscr{F}(f * g)(x) = \mathscr{F}f(x) \cdot \mathscr{F}g(x)$. *That is,* $\mathscr{F}$ *turns convolution into pointwise multiplication.*
(2) *Fourier inversion.* $f(x) = \frac{1}{n}\mathscr{F}^2 f(-x)$.
(3) *Parseval–Plancherel identity.* $\langle \mathscr{F}f, \mathscr{F}g\rangle = n\langle f, g\rangle$.

In particular, (2) implies that $\mathscr{F}$ *is invertible, hence bijective.*

Proof of part (1). For all $a, b \in \mathbf{Z}/n\mathbf{Z}$, we compute

$$\mathscr{F}(\delta_a * \delta_b) = \mathscr{F}\delta_{a+b} = \bar{e}_{a+b} = \bar{e}_a \cdot \bar{e}_b = \mathscr{F}\delta_a \cdot \mathscr{F}\delta_b.$$

But the δ_a span $L^2(\mathbf{Z}/n\mathbf{Z})$, so by the linearity of $*$ and $\cdot$ and $\mathscr{F}$, we're done. □

Let us sketch an application. Fix a prime number p. Given a residue $a \in \mathbf{Z}/p\mathbf{Z}$, the *Gauss sum* $\Gamma(a)$ is defined by

$$\Gamma(a) = \sum_{x \in \mathbf{Z}/p\mathbf{Z}} \chi(x) e^{2\pi i a x/p},$$

where χ is the *Legendre symbol* defined by:

$$\chi(x) = \begin{cases} 0 & x \equiv 0 \\ 1 & x \text{ is a nonzero square mod } p \\ -1 & \text{else} \end{cases}$$

One of Gauss's proofs of the quadratic reciprocity law relies on an exact calculation of $\Gamma(a)$. Here, we prove a weaker result that Gauss discovered earlier:

Theorem 3.2. *If* $a \in \mathbf{Z}/p\mathbf{Z}$ *is nonzero, then* $|\Gamma(a)| = \sqrt{p}$.

Lemma 3.3. *As* a *runs over nonzero residues, the values of* $\Gamma(a)$ *only differ up to sign. In particular, they all have the same magnitude.*

Proof of Theorem 3.2. Observe that $\Gamma(a) = \mathscr{F}\chi(-a)$. By Parseval–Plancherel,

$$\sum_{a \in \mathbf{Z}/p\mathbf{Z}} \Gamma(a)^2 = \|\mathscr{F}\chi\|^2 = p\|\chi\|^2 = p(p-1).$$

But $\Gamma(0) = \sum_x \chi(x) = 0$, so in the sum on the left, only terms where a is nonzero contribute. There are $p - 1$ such terms, and by Lemma 3.3, they all have the same magnitude. □

References

[1] D. Ramakrishnan & R. J. Valenza. *Fourier Analysis on Number Fields.* Springer–Verlag (1999).

[2] A. Terras. *Fourier Analysis on Finite Groups and Applications.* Cambridge University Press (1999).