Fourier analysis in additive combinatorics

notes by

Marcel K. Goh

Note. I am compiling this set of expository notes primarily to solidify these bread-and-butter concepts in my own mind. Sources that are far more comprehensive exist on the web, so I'm not sure how useful this will be to anyone else. Currently, the bulk of these notes come from a series of YouTube lectures of Timothy Gowers (given in early 2022), though I intend in future to add more relevant topics as I learn about them.

1. Preliminary notions

Let Z be a finite abelian group. A *character* on Z is a homomorphism from Z to the multiplicative group $\mathbf{C} \setminus \{0\}$. If χ is such a homomorphism, then $\big|\chi(x)\big| = 1$ for every $x \in Z$, so we can actually regard χ as being a function from Z to the unit circle $\mathbf{T} = \{z \in \mathbf{C} : |z| = 1\}$. The pointwise product of two characters gives another character, and the function χ_0 that sends every $x \in Z$ to 1 has the property that if χ is any character, then $\chi\chi_0 = \chi = \chi_0\chi$. Lastly, we note that multiplication is commutative and for any character χ, the product of χ with $\overline{\chi}$ gives χ_0, so the set of characters on Z is an abelian group. This is called the *dual group* or sometimes *Pontryagin dual* of Z and is denoted $\widehat{Z}$.

We define an inner product on the space $\mathbf{C}^Z$ of functions from Z to $\mathbf{C}$ by setting

$$\langle f, g\rangle = \mathbf{E}_x\, f(x)\overline{g(x)},$$

where $\mathbf{E}_{x\in Z}\, F(x) = |Z|^{-1}\sum_{x\in Z} F(x)$. We can also make $\widehat{Z}$ into an inner product space by letting

$$\langle \widehat{f}, \widehat{g}\rangle = \sum_{\chi\in\widehat{Z}} \widehat{f}(\chi)\overline{\widehat{g}(\chi)};$$

note that this time we do not normalise by dividing by $|Z|$. Two functions f and g in an inner product space are said to be *orthogonal* if $\langle f, g\rangle = 0$. The first lemma we'll prove concerns certain orthogonality relations.

Lemma 1 (*Orthogonality relations*). *Let Z be a finite abelian group.*

a) If χ_1 and χ_2 are characters on Z, then

$$\langle \chi_1, \chi_2\rangle = \mathbf{E}_{x\in Z}\, \chi_1(x)\overline{\chi_2(x)} = \begin{cases} 1, & \text{if } \chi_1 = \chi_2; \\ 0, & \text{if } \chi_1 \neq \chi_2. \end{cases}.$$

b) For $x, y \in Z$, we have

$$\sum_{\chi \in \widehat{Z}} \chi(x)\overline{\chi(y)} = \begin{cases} |\widehat{Z}|, & \text{if } x = y; \\ 0, & \text{if } x \neq y, \end{cases}$$

Proof. Let χ_0 denote the trivial character. We have

$$\mathbf{E}_{x \in Z}\, \chi_0(x) = \mathbf{E}_{x \in Z}\, 1 = 1.$$

On the other hand, let χ be a nontrivial character and let $u \in Z$ be such that $\chi(u) \neq 1$. Then from

$$\mathbf{E}_{x \in Z}\, \chi(x) = \mathbf{E}_{x \in Z}\, \chi(u + x) = \mathbf{E}_{x \in Z}\, \chi(u)\chi(x) = \chi(u)\, \mathbf{E}_{x \in Z}\, \chi(x),$$

it follows that $\mathbf{E}_{x \in Z}\, \chi(x) = 0$. Now consider $\chi_1\overline{\chi_2}$. If $\chi_1 = \chi_2$, then this is the trivial character and from our first observation, $\langle \chi_1, \chi_2 \rangle = 0$. Otherwise, we are in the second case and the inner product is zero. This proves part (a).

Part (b) is proven similarly. Note that $\chi(x)\overline{\chi(y)} = \chi(x - y)$. If $x = y$, then we have

$$\sum_{\chi \in \widehat{Z}} \chi(x - y) = \sum_{\chi \in \widehat{Z}} \chi(0) = |\widehat{Z}|.$$

If $x \neq y$, then there is some $\psi \in \widehat{Z}$ such that $\psi(x - y) \neq 1$, and then writing

$$\sum_{\chi \in \widehat{Z}} \chi(x - y) = \sum_{\chi \in \widehat{Z}} \psi(x - y)\chi(x - y) = \psi(x - y) \sum_{\chi \in \widehat{Z}} \chi(x - y),$$

we see that $\sum_{\chi \in \widehat{Z}} \chi(x - y)$ must be zero. ∎

Since the space of functions from $Z \to \mathbf{C}$ has dimension $|Z|$, there are at most $|Z|$ characters. Every finite abelian group can be written as a direct product of cyclic groups, and we shall use this fact to show that there are exactly $|Z|$ characters; i.e., $|\widehat{Z}| = |Z|$. For brevity, let $\mathbf{Z}_n$ stand for $\mathbf{Z}/n\mathbf{Z}$ for all $n \in \mathbf{N}$, and for $\alpha \in \mathbf{R}$, let $e(\alpha) = e^{2\pi i \alpha}$.

Lemma 2. *The set of characters on a finite abelian group Z spans the space of functions from Z to $\mathbf{C}$.*

Proof. Write $Z \cong \mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2} \times \cdots \times \mathbf{Z}_{n_r}$. For every $u = (u_1, \ldots, u_r) \in Z$, the function $\chi_u : Z \to \mathbf{C}$ that takes

$$(x_1, \ldots, x_r) \mapsto \prod_{i=1}^{r} e\left(\frac{u_i x_i}{n_i}\right)$$

is a character (this is easy to show, since $e(x_i + x_i') = e(x_i)e(x_i')$). If $u \neq u'$, then $\chi_u \neq \chi_{u'}$ and $\langle \chi_u, \chi_{u'} \rangle = 0$ by the previous lemma. Hence the set $\{\chi_u : u \in Z\}$

comprises $|Z|$ linearly independent elements in a space of dimension $|Z|$, which must be spanning. ∎

Note that the map $u \mapsto \chi_u$ gives an isomorphism from Z to $\widehat{Z}$. The two main examples we shall consider are when $Z = \mathbf{Z}_n$ and when $Z = \mathbf{F}_p^n$. In the first case, χ_u takes $x \mapsto e(ux/N)$ and in the second case χ_u takes $x \mapsto e(u \cdot x/p)$. (Recall that if $u = (u_1, \ldots, u_n)$ and $x = (x_1, \ldots, x_n)$ then the dot product $u \cdot x$ is the sum $\sum_{i=1}^n u_i x_i$.)

For a finite set X, we shall denote by $L_p(X)$ the normed vector space of all functions $f : X \to \mathbf{C}$ under the norm

$$\|f\|_p = \big(\mathbf{E}_{x \in X} \big|f(x)\big|^p\big)^{1/p}.$$

The notation $l_p(X)$ denotes the same set, but with the norm

$$\|f\|_p = \Big(\sum_{x \in X} \big|f(x)\big|^p\Big)^{1/p}$$

instead. Note that $\|f\|_2^2 = \langle f, f\rangle$ and $\|f\|_\infty = \max_{x \in X} \big|f(x)\big|$.

The Fourier transform. If $f : Z \to \mathbf{C}$, the *Fourier transform* of f is the function $\widehat{f} : \widehat{Z} \to \mathbf{C}$ given by

$$\widehat{f}(\chi) = \langle f, \chi\rangle = \mathbf{E}_{x \in Z}\, f(x)\overline{\chi(x)}.$$

We shall now state and prove an identity which is extremely useful in Fourier analysis.

Lemma 3 (*Parseval's identity*). *Let Z be a finite abelian group and let f and g be functions from Z to $\mathbf{C}$. If $\widehat{f}$ and $\widehat{g}$ are the Fourier transforms of f and g respectively, then $\langle f, g\rangle = \langle \widehat{f}, \widehat{g}\rangle$.*

Proof. First, we expand all the definitions and rearrange sums to obtain

$$\begin{aligned}
\langle \widehat{f}, \widehat{g}\rangle &= \sum_{\chi \in \widehat{Z}} \widehat{f}(\chi)\overline{\widehat{g}(\chi)} \\
&= \sum_{\chi \in \widehat{Z}} \mathbf{E}_{x \in Z}\, f(x)\overline{\chi(x)}\, \mathbf{E}_{y \in Z}\, g(y)\overline{\chi(y)} \\
&= \mathbf{E}_{x \in Z}\, f(x)\, \mathbf{E}_{y \in Z}\, g(y) \sum_{\chi \in \widehat{Z}} \overline{\chi(x)\chi(y)}.
\end{aligned}$$

By the second orthogonality relation and the fact that $|\widehat{Z}| = |Z|$, the inner sum equals $|Z|$ when $y = x$ and 0 otherwise. Thus for any given x, we have

$$\mathbf{E}_{y \in Z}\, g(y) \sum_{\chi \in \widehat{Z}} \chi(x)\overline{\chi(y)} = g(x),$$

which is exactly what we need for the whole thing to equal $\langle f, g\rangle$. ∎

We also have the following inversion formula that recovers the original function f from $\widehat{f}$.

Lemma 4 (*Fourier inversion formula*). *Let Z be a finite abelian group and let $f : Z \to \mathbf{C}$. We have*

$$f(x) = \sum_{\chi \in \widehat{Z}} \widehat{f}(\chi)\chi(x).$$

Proof. We expand

$$\sum_{\chi \in \widehat{Z}} \widehat{f}(\chi)\chi(x) = \sum_{\chi \in \widehat{Z}} \mathbf{E}_{y \in Z}\, f(y)\overline{\chi(y)}\chi(x) = \mathbf{E}_{y \in Z}\, f(y) \sum_{\chi \in \widehat{Z}} \chi(x)\overline{\chi(y)},$$

and we noted in the proof of Parseval's theorem that the right-hand side is exactly $f(x)$. ∎

The inversion formula tells us that two functions from $Z \to \mathbf{C}$ are equal if and only if their Fourier transforms are equal. For the next lemma, which concerns dilates of a function $f : Z \to \mathbf{C}$, we will establish some notation. If $x \in Z$, we define nx recursively for all integers $n \geq 0$ by $0x = 0$ and $nx = x + (n-1)x$. We then set $nz = -(-n)x$ for all negative integers. Since the group operation on characters is multiplication, we will not write $n\chi$ but instead χ^n for χ multiplied with itself n times.

Lemma 5 (*Dilation rule*). *Let Z be a finite abelian group and let $a \in \mathbf{Z}$ be an integer that is coprime to $|Z|$. Denote the multiplicative inverse of a modulo $|Z|$ by a^{-1}. Letting $f_a : Z \to \mathbf{C}$ be the function given by $f_a(x) = f(a^{-1}x)$, we have $\widehat{f_a}(\chi) = \widehat{f}(\chi^a)$.*

Proof. We have

$$\widehat{f_a}(\chi) = \mathbf{E}_{x \in Z}\, f_a(x)\overline{\chi(x)} = \mathbf{E}_{x \in Z}\, f(a^{-1}x)\overline{\chi(x)}.$$

Since $x \mapsto ax$ is a bijection from Z to itself, we can replace x formally by ax in the above to get

$$\widehat{f_a}(\chi) = \mathbf{E}_{x \in Z}\, f(x)\overline{\chi(ax)} = \mathbf{E}_{x \in Z}\, f(x)\overline{\chi(ax)}^a = \widehat{f}(\chi^a). \quad ∎$$

Convolutions. For functions f and g from a finite abelian group Z to $\mathbf{C}$, the *convolution* $f * g$ is defined by

$$(f * g)(x) = \mathbf{E}_{y+z=x}\, f(y)g(z).$$

If instead $\widehat{f}$ and $\widehat{g}$ are functions from $\widehat{Z}$ to $\mathbf{C}$, then

$$(\widehat{f} * \widehat{g})(\chi) = \sum_{\chi_1\chi_2 = \chi} \widehat{f}(\chi_1)\widehat{g}(\chi_2).$$

Lemma 6 (*Convolution law*). *Let Z is a finite abelian group and $f, g : \mathbf{Z} \to \mathbf{C}$. For all $\chi \in \widehat{Z}$, we have $\widehat{f * g}(\chi) = \widehat{f}(\chi)\widehat{g}(\chi)$.*

Proof. We start by expanding

$$\widehat{f * g}(\chi) = \mathbf{E}_{x \in Z}(f * g)(x)\overline{\chi(x)} = \mathbf{E}_{x \in Z}\, \mathbf{E}_{y+z=x}\, f(y)g(z)\overline{\chi(y)\chi(z)}.$$

But note that x does not appear in the summand anymore, meaning that we can simply rewrite this as an expectation over *all* y and z (their sum will equal x for some $x \in Z$). Thus we can conclude that

$$\widehat{f * g}(\chi) = \mathbf{E}_{y \in Z}\, \mathbf{E}_{z \in Z}\, f(y)g(z)\overline{\chi(y)\chi(z)} = \widehat{f}(\chi)\widehat{g}(\chi),$$

which is what we wanted to show. ∎

If A is a subset of a finite abelian group Z, we associate to A the *characteristic function* $\mathbf{1}_A : Z \to \mathbf{C}$ given by

$$\mathbf{1}_A(x) = \begin{cases} 1, & \text{if } x \in A; \\ 0, & \text{otherwise.} \end{cases}$$

When it will not cause confusion, we will abuse notation and write $A(x)$ instead of $\mathbf{1}_A(x)$. With the definitions and results stated above, we are now in a position to translate properties of A to Fourier-analytic statements about the function $\mathbf{1}_A$. First off, note that

$$\left\|\widehat{\mathbf{1}_A}\right\|_2^2 = \|\, \mathbf{1}_A \,\|_2^2 = \mathbf{E}_{x \in Z}\, A(x)^2 = \mathbf{E}_{x \in Z}\, A(x) = \frac{|A|}{|Z|}.$$

If $|A|/|Z| = \delta$, then we will say that A has *density* δ. Another way of expressing δ in terms of $\mathbf{1}_A$ is

$$\widehat{\mathbf{1}_A}(\chi_0) = \mathbf{E}_{x \in Z}\, A(x)\chi_0(x) = \mathbf{E}_{x \in Z}\, A(x) = \delta,$$

where χ_0 is the trivial character.

The fact that $\|\, \mathbf{1}_A \,\|_2^2 = \delta$ means that if we sample x and y from Z and condition that $x = y$, the probability that x (or y) is in A is δ. The reason for stating this obvious fact in such a stilted fashion is that it generalises by way of the convolution operation we defined earlier; that is, what if we are interested in the probability that a 4-tuple (x, y, z, w) satisfying $x + y = z + w$ is a member of A^4? Well, the convolution law gives

$$\begin{aligned}
\mathbf{E}_{x+y=z+w}\, A(x)A(y)A(z)A(w) &= \mathbf{E}_{u \in Z}\, \mathbf{E}_{x+y=u}\, \mathbf{E}_{z+w=u}\, A(x)A(y)A(z)A(w) \\
&= \mathbf{E}_{u \in Z}(\mathbf{1}_A * \mathbf{1}_A)(u)^2 \\
&= \|\, \mathbf{1}_A * \mathbf{1}_A \,\|_2^2 \\
&= \left\|\widehat{\mathbf{1}_A * \mathbf{1}_A}\right\|_2^2 \\
&= \left\|\left(\widehat{\mathbf{1}_A}\right)^2\right\|_2^2 \\
&= \sum_{\chi \in \widehat{Z}} \left|\widehat{\mathbf{1}_A}(\chi)\right|^4 \\
&= \|\, \mathbf{1}_A \,\|_4^4,
\end{aligned}$$

and more generally, the probability that a tuple $(a_1, \ldots, a_k, b_1, \ldots, b_k) \in Z^{2k}$ with $a_1 + \cdots + a_k = b_1 + \cdots + b_k$ is a member of A^{2k} is $\| \mathbf{1}_A \|_{2k}^{2k}$. In any case, the number of $(x, y, z, w) \in A^4$ with $x + y = z + w$ is so important in additive combinatorics that is has a name. It is called the *additive energy* of A and is denoted $E(A)$; we just showed above is that $E(A) = |Z|^3 \| \mathbf{1}_A \|_4^4$.

References

Terence Tao and Van Ha Vu, *Additive Combinatorics* (Cambridge: Cambridge University Press, 2006).