Fourier Analysis on Groups

Daniel Penner

1 Finite Abelian Groups

In the theory that follows, we will be concerned with homomorphisms mapping a finite abelian group G to the group $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$, with multiplication as the operation. The following lemma shows that we can restrict our attention further.

Lemma 1.1. *Let G be a finite abelian group, and let $\varphi : G \to \mathbb{C}^\times$ be a homomorphism: that is, $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$ for any $x, y \in G$. Then $|\varphi(x)| = 1$ for every $x \in G$, so φ in fact maps G into the circle S^1.*

Proof. Let $x \in G$, and let n be its order, the least integer such that $x^n = 1$. Then since φ fixes 1, we have $1 = |\varphi(1)| = |\varphi(x^n)| = |\varphi(x)|^n$, so that $|\varphi(x)| = 1$. $\square$

Motivated by the above lemma, we define a **character** on a finite abelian group G as a homomorphism $\varphi : G \to S^1$ (note that S^1 is a group under multiplication, since each element takes the form $e^{i\theta}$ for $\theta \in \mathbb{R}$). For instance, on every group we have the trivial character, defined as $\varphi(x) = 1$ for all $x \in G$.

Lemma 1.2. *Let G be a finite abelian group. The set $\hat{G}$ of characters on G is an abelian group, with the operation defined as $(\varphi_1 \cdot \varphi_2)(x) = \varphi_1(x) \cdot \varphi_2(x)$.*

Proof. This proof consists of simply verifying the group axioms (closure under products, associativity of products, existence of an identity, and existence of unique inverses), so we omit it. $\square$

Now we consider the vector space V of complex-valued functions on a finite abelian group G, which clearly has dimension $|G|$, since we can write each function as a linear combination $f(x) = \sum_{k=1}^{|G|} a_k \chi_k(x)$, where $\chi_k(x)$ is the characteristic function of $x_k \in G$, $a_k \in \mathbb{C}$. We define an inner product on V as follows:

$$(f, g) = \sum_{x \in G} f(x)\overline{g(x)}. \tag{1}$$

The following two theorems, from which all nice Fourier facts will follow, claim that $\hat{G}$ is an orthogonal basis for V under this inner product.

Remark. *We note here that the inner product on V can be taken as in* (1) *above, or multiplied by a factor of $|G|^{-1}$. In the latter case $\hat{G}$ would be an orthonormal basis for V (by Theorem 1.3 below), in analogy with Fourier analysis on the real line. The reason for leaving this factor out will become apparent in Section 2 (particularly, Lemma 2.3).*

Theorem 1.3. *Let G be a finite abelian group. If $\varphi, \psi \in \hat{G}$ are characters of G, then*

$$(\varphi, \psi) = \begin{cases} |G| & \varphi = \psi \\ 0 & \varphi \neq \psi. \end{cases}$$

Proof. First we easily obtain that if $\varphi \in \hat{G}$,

$$(\varphi, \varphi) = \sum_{x \in G} \varphi(x)\overline{\varphi(x)} = \sum_{x \in G} |\varphi(x)|^2 = |G|.$$

Now we wish to show that if $\varphi, \psi \in \hat{G}$ are distinct, then $(\varphi, \psi) = 0$. First we note that for any non-trivial character φ, $\sum_{x \in G} \varphi(x) = 0$. This follows because given $y \in G$ such that $\varphi(y) \neq 1$ we see that

$$\varphi(y) \sum_{x \in G} \varphi(x) = \sum_{x \in G} \varphi(y)\varphi(x) = \sum_{x \in G} \varphi(xy) = \sum_{x \in G} \varphi(x),$$

where we can shuffle around the group elements in the sum since there are finitely many. Now if $\varphi, \psi \in \hat{G}$ are distinct, then $\varphi \cdot \psi^{-1}$ is not the trivial character (since inverses are unique). So by the above we get that

$$(\varphi, \psi) = \sum_{x \in G} \varphi(x)\overline{\psi(x)} = \sum_{x \in G} \varphi(x)\psi^{-1}(x) = 0.$$

∎

Theorem 1.4. *$|\hat{G}| = |G|$, and therefore $\hat{G}$ is an orthonormal basis for V, the vector space of complex-valued functions on G. Furthermore, $\hat{G} \simeq G$.*

Proof. It is clear that $|\hat{G}| \leq |G|$, since $|G|$ is the dimension of V as a complex vector space, and $\hat{G}$ is an orthogonal and thus linearly independent set of elements of V.

For the opposite inequality, we first consider the case $G = \mathbb{Z}/n\mathbb{Z}$. Here, we have precisely $|G|$ characters of the form $\varphi_x(\xi) = e^{2\pi i x \xi / n}$ for $x = 0, 1, \ldots, n-1$. It is clear that these map $G \to S^1$, and that these form a group, since $\varphi_x \varphi_y = e^{2\pi i (x+y)\xi/n} = \varphi_{x+y}$, and that they are homomorphisms.

To generalize to all finite groups, we recall the Structure Theorem for Finite Abelian Groups, which states that if G is a finite abelian group, then it is a direct product of cyclic groups:

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_m\mathbb{Z}$$

for some integers $n_1, \ldots, n_m$. Accordingly we can define $|G| = \prod_{k=1}^{m} n_k$ distinct characters on G by taking the products of the characters on $\mathbb{Z}/n_k\mathbb{Z}$, for all $k = 1, \ldots, m$. That is, if $\xi \in G$

is $\xi = (\xi_1, \ldots, \xi_m)$ and $x = (x_1, \ldots, x_m)$, then $\varphi_x(\xi) = \prod_{k=1}^m \varphi_{x_k}(\xi_k) = \prod_{k=1}^m e^{2\pi i x_k \xi_k / n_k}$. The proof that these are distinct homomorphisms is routine. To see that $G \simeq \hat{G}$, then, we simply check that the map $h : G \to \hat{G}$ which sends $x \mapsto \varphi_x$ as defined above is an isomorphism (we omit this). $\square$

Now that we have an orthogonal basis for the space V of functions on G, the basic Fourier theory follows very quickly. Let $f \in V$, and φ be a character on G. Then we define the **Fourier transform** of f for φ as

$$\hat{f}(\varphi) = (f, \varphi) = \sum_{x \in G} f(x)\overline{\varphi(x)}.$$

Remark. *We note here that we can think of the Fourier transform as a function on G, since $G \simeq \hat{G}$. Precisely, for $x \in G$ we can write $\hat{f}(x) = \hat{f}(\varphi_x)$, and therefore we can consider its inner product and thus its norm in V: $(\hat{f}, \hat{f}) = \|\hat{f}\|^2$.*

Theorem 1.5 (Fourier Inversion and Plancherel Formula). *Let G be a finite abelian group, and V be the vector space of complex-valued functions on G. Then if $f \in V$,*

$$f = \frac{1}{|G|} \sum_{\varphi \in \hat{G}} \hat{f}(\varphi)\varphi,$$

and the Plancherel formula holds:

$$\|f\|^2 = \frac{1}{|G|} \|\hat{f}\|^2.$$

Proof. Since $\hat{G}$ is a basis for V, we have a set of complex numbers a_φ such that $f = \sum_{\varphi \in \hat{G}} a_\varphi \varphi$. But since the φ are orthogonal, we have $(f, \varphi) = |G| a_\varphi$, and therefore

$$f = \sum_{\varphi \in \hat{G}} a_\varphi \varphi = \frac{1}{|G|} \sum_{\varphi \in \hat{G}} (f, \varphi)\varphi = \frac{1}{|G|} \sum_{\varphi \in \hat{G}} \hat{f}(\varphi)\varphi.$$

The Plancherel formula follows just as quickly:

$$\|f\|^2 = (f, f) = \frac{1}{|G|} \sum_{\varphi \in \hat{G}} (f, \varphi)\overline{\hat{f}(\varphi)} = \frac{1}{|G|} \sum_{\varphi \in \hat{G}} \hat{f}(\varphi)\overline{\hat{f}(\varphi)} = \frac{1}{|G|} \|\hat{f}\|^2,$$

where the second equality follows from the Fourier inversion formula. $\square$

With these results we can easily obtain a discrete version of the Heisenberg uncertainty principle.

Theorem 1.6 (Heisenberg Inequality on Finite Abelian Groups). *Let G be a finite abelian group, and let $f \in V$, the space of complex-valued functions on G, be not identically zero. Then if $supp(f) = \{x \in G : f(x) \neq 0\}$ denotes the support of f, we have*

$$supp(f) \cdot supp(\hat{f}) \geq |G|.$$

Proof. Fourier inversion and triangle inequality give us that

$$|f(x)| \leq \frac{1}{|G|} \sum_{\varphi \in \hat{G}} |\hat{f}(\varphi)| \leq \frac{\text{supp}(\hat{f})}{|G|} \max_{\varphi \in \hat{G}} |\hat{f}(\varphi)|.$$

But similarly we have that for any $\varphi \in \hat{G}$,

$$|\hat{f}(\varphi)| \leq \sum_{x \in G} |f(x)| \leq \text{supp}(f) \max_{x \in G} |f(x)|.$$

Combining the two gives us that for any $x \in G$,

$$|f(x)| \leq \frac{\text{supp}(\hat{f})\text{supp}(f)}{|G|} \max_{x \in G} |f(x)|.$$

Taking the maximum from below and multiplying through by $|G|$ gives the result. $\square$

2 The General Case

In this section we expand the theory to functions defined on finite non-abelian groups. This requires some basic familiarity with the theory of finite group representations, and for brevity's sake we will omit the proofs of some standard results (for the proofs, as well as some background, see [1], chapter 10). For those already familiar with the theory, the motivation here is that the characters of a group G as described in Section 1 are simply one-dimensional representations of G (whose single entry is its character, in the representation theoretic sense - hence the use of the name "character" in the previous section). This should be unsurprising, in light of the fact that every irreducible representation of a finite abelian group G is one-dimensional, and that there are precisely $|G|$ distinct irreducible representations of G.

Let G be a finite group, and V be a nonzero n-dimensional complex vector space. Then a **representation** of G is a homomorphism $\rho : G \to GL(V)$, the group of linear operators on V (each of which is, for a fixed basis of V, a complex $n \times n$ matrix). The **character** of a representation ρ is the function $\chi_\rho : G \to \mathbb{C}$ which sends $g \mapsto \text{Tr}(\rho(g))$. We say two representations, ρ, π of G are **equivalent** if there is a matrix $S \in GL(V)$ such that $S\rho(g)S^{-1} = \pi(g)$ for all $g \in G$. If W is an m-dimensional subspace of V, we say W is G-invariant if for all $g \in G$ and $w \in W$ we have that $\rho(g)w \in W$. Then the restriction of the image of ρ is a sub-representation π of ρ. We say ρ is **irreducible** if V has no proper G-invariant subspaces, or equivalently, if ρ has no proper sub-representations (that is, aside from itself and the zero representation). If $V = W_1 \oplus W_2$, where both W_i are G-invariant, then we obtain corresponding subrepresentations π_1, π_2 of ρ, and we say that $\rho = \pi_1 \oplus \pi_2$. In this case the matrix of $\rho(g)$ under some basis of V will have the block form

$$\rho(g) = \begin{bmatrix} \pi_1(g) & 0 \\ 0 & \pi_2(g) \end{bmatrix},$$

where the blocks are of course determined by the choice of basis. The following theorem states that every representation takes this form, where the blocks are in fact irreducible.

Theorem 2.1 (Maschke's Theorem)**.** *Let G be a finite group, and let V be a nonzero finite-dimensional complex vector space. Every representation $\rho : G \to GL(V)$ is a direct sum of irreducible sub-representations.*

Proof. First, if V is a Hermitian inner product space, we say that a representation $\rho : G \to GL(V)$ is **unitary** if for every $g \in G$, the matrix $\rho(g)$ is a unitary matrix, that is with the given inner product we have that for any $v, w \in V$ and any $g \in G$, $(gv, gw) = (v, w)$.

Now, given a representation on a vector space V, we say that a Hermitian form $(\cdot, \cdot)$ on V is G-invariant if $(gv, gw) = (v, w)$ for all $v, w \in V$ and $g \in G$. As it turns out, for any n-dimensional vector space V and representation $\rho : G \to GL(V)$, the Hermitian form $(v, w) = \frac{1}{|G|} \sum_{g \in G} \langle gv, gw \rangle$, where $\langle \cdot, \cdot \rangle$ is the standard n-dimensional Hermitian product (that is, the complex dot product), is G-invariant. We omit the proof of this fact, which is simply verifying that the form is Hermitian, positive definite, and G-invariant.

So under this inner product on V, ρ is a unitary representation. It is easy enough to see that every unitary representation is the direct sum of irreducible representations, from which the theorem immediately follows. To see this we note that if W is a G-invariant subspace of V (which exists with our inner product), then $V = W \oplus W^\perp$, the orthogonal complement. It is clear that $W^\perp$ is also G-invariant, since if for any $w \in W$ we have $u \perp w$, then $gu \perp gw \in W$. So for every $u \in W^\perp$, $gu \in W^\perp$. We proceed by induction on the G-invariant subspaces of W and $W^\perp$ (this is finitely many steps because V is finite-dimensional and W, $W^\perp$ are proper subspaces), decomposing the subspaces until V is decomposed into G-invariant subspaces whose corresponding representations are irreducible. □

Since every representation can be thought of as a unitary representation under some basis (that is, with the correctly chosen inner product), we can restrict our attention to unitary representations, and define $\hat{G}$ to be the set of non-equivalent, irreducible unitary representations of G. Also, we denote by $L^2(G)$ the complex vector space of functions $f : G \to \mathbb{C}$, with inner product $(f, g) = \sum_{x \in G} f(x)\overline{g(x)}$, and norm $\|f\|^2 = (f, f)$.

We require a few further results in order to define the basics of Fourier theory on finite groups. For these we define the **dimension** d_ρ of a representation $\rho : G \to GL(V)$ to be the dimension of V as a complex vector space (equivalently, the size of the matrices of ρ).

Theorem 2.2 (Orthogonality Relations)**.** *(a) If π, ρ are two different irreducible unitary representations of G, then the matrix entries of π and ρ are pairwise orthogonal. That is, for any i, j, k, l, we have*

$$(\pi_{ij}, \rho_{kl}) = \sum_{g \in G} \pi_{ij}(g)\overline{\rho_{kl}} = 0.$$

(b) With π as in part (a), if d_π is the degree of π,

$$(\pi_{ij}, \pi_{kl}) = \frac{|G|}{d_\pi} \delta_{ik}\delta_{jl},$$

and thus the matrix entries of π are pairwise orthogonal.

(c) With π, ρ as in part (a), the characters of π and ρ are orthogonal. Particularly, we have

$$(\chi_\pi, \chi_\rho) = \begin{cases} |G| & \text{if } \pi \text{ and } \rho \text{ are equivalent} \\ 0 & \text{if } \pi \text{ and } \rho \text{ are not equivalent.} \end{cases}$$

Theorem 2.2 is somewhat more involved than the rest of the results described here, so we defer to [3], p. 248-252, for a detailed proof. The next lemma, whose proof we omit because it requires some beautiful but otherwise irrelevant character theory (see [3] p. 256), relays the crucial facts about a particularly important representation on finite groups G, the regular representation.

Lemma 2.3. *If G is a finite group, denote by $L(g)$, called the* **(left) regular representation** *of G, the $|G|$-dimensional representation associated with the operation of G on itself by left multiplication.*

(a) The character of $L(g)$ is $\chi_L(g) = \begin{cases} |G| & g \text{ is the identity} \\ 0 & \text{otherwise.} \end{cases}$

(b) $L(g)$ contains every irreducible representation π of G as a subrepresentation of multiplicity d_π. So if $\hat{G} = \{\pi_1, \ldots, \pi_n\}$, then $L \simeq d_{\pi_1}\pi_1 \oplus \cdots \oplus d_{\pi_n}\pi_n$.

(c) $\sum_{\pi \in \hat{G}} d_\pi^2 = |G|$.

The following result is the analogue of Theorem 1.4 from section one, in which we found an orthogonal basis of characters.

Theorem 2.4 (Peter-Weyl Theorem)**.** *The matrix entries of the representations $\rho \in \hat{G}$ form an orthogonal basis of $L^2(G) = \{f : G \to \mathbb{C}\}$ over $\mathbb{C}$.*

Proof. By the Orthogonality Relations (Theorem 2.2), these entries are all pairwise orthogonal. The dimension of $L^2(G)$ as a complex vector space is clearly $|G|$, since we can take the characteristic functions on the group elements as a basis. By Lemma 2.3(c), the total number of matrix entries of distinct irreducible unitary representations is $|G|$, and therefore the set of matrix entries is a basis for $L^2(G)$ (since there is a linearly independent set of size $|G| = \dim(L^2(G))$). $\square$

The Peter-Weyl theorem suffices to prove the basic facts about Fourier analysis on finite groups. If $f \in L^2(G)$, we define the **Fourier transform** $\hat{f}$ of f as $\hat{f}(\rho) = (f, \rho) = \sum_{g \in G} f(g)\overline{\rho(g)}$. Note that $\hat{f}$ is defined on $\hat{G}$, and the image of $\rho \in \hat{G}$ is a $d_\rho \times d_\rho$ complex matrix.

Theorem 2.5 (Fourier Inversion and Plancherel Formula)**.** *If $f \in L^2(G)$, then we have the following Fourier inversion formula:*

$$f(x) = \frac{1}{|G|} \sum_{\substack{\rho \in \hat{G} \\ 1 \le i,j \le d_\rho}} d_\rho \hat{f}(\rho_{ij}) \rho_{ij}(x).$$

Also, we have the following analogue of the Plancherel formula:

$$\|f\|^2 = \frac{1}{|G|} \sum_{\substack{\rho \in \hat{G} \\ 1 \leq i,j \leq d_\rho}} d_\rho |\hat{f}(\rho_{ij})|^2.$$

Proof. First for each matrix entry ρ_{ij} we define $\rho'_{ij} = \rho_{ij}\sqrt{d_\rho/|G|}$. Then by the Peter-Weyl Theorem, the set of all ρ'_{ij} forms an orthogonal basis for $L^2(G)$. We see that $\|\rho'_{ij}\| = 1$, since

$$\|\rho'_{ij}\|^2 = \frac{1}{|G|} \sum_{x \in G} d_\rho |\rho_{ij}|^2 = \frac{d_\rho}{|G|}(\rho_{ij}, \rho_{ij}) = 1,$$

where the last equality follows from Theorem 2.2(b). Then since the set is an orthonormal basis of a finite-dimensional vector space, we have that if $f \in L^2(G)$, we can write, as desired, that

$$f(x) = \sum_{\substack{\rho \in \hat{G} \\ 1 \leq i,j \leq d_\rho}} (f, \rho'_{ij})\rho'_{ij}(x) = \frac{1}{|G|} \sum_{\substack{\rho \in \hat{G} \\ 1 \leq i,j \leq d_\rho}} d_\rho (f, \rho_{ij})\rho_{ij}(x) = \frac{1}{|G|} \sum_{\substack{\rho \in \hat{G} \\ 1 \leq i,j \leq d_\rho}} d_\rho \hat{f}(\rho_{ij})\rho_{ij}(x).$$

The Plancherel formula follows immediately from the Fourier inversion formula:

$$\|f\|^2 = (f, f) = \frac{1}{|G|} \sum_{\substack{\rho \in \hat{G} \\ 1 \leq i,j \leq d_\rho}} d_\rho \hat{f}(\rho_{ij})(\rho_{ij}, f) = \frac{1}{|G|} \sum_{\substack{\rho \in \hat{G} \\ 1 \leq i,j \leq d_\rho}} d_\rho |\hat{f}(\rho_{ij})|^2.$$

□

With this theorem we have established the basic Fourier theory on general finite groups. To conclude, we briefly discuss one further analogue with the abelian (i.e. one-dimensional) case. Recall that, for a finite abelian group G, we obtained in Theorem 1.4 that $|\hat{G}| = |G|$. A fundamental result of character theory, involving the orthonormality of characters, implies that there exist precisely as many non-equivalent irreducible representations of G as there are conjugacy classes of G (for details see [1], p. 300). That is, $|\hat{G}|$ is the number of conjugacy classes of G.

References

[1] M. Artin. *Algebra*. Second Edition. Pearson Education, Inc. (2011)

[2] S. Stein and R. Shakarchi. *Analysis I: Fourier Analysis*. Princeton University Press. (2003)

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