(*April 1, 2012*)

Fourier analysis on finite abelian groups

Paul Garrett garrett@math.umn.edu http://www.math.umn.edu/~garrett/

There are Fourier expansions on finite abelian groups essentially identical in form to Fourier expansions of periodic functions on the real line.

---

1. *Fourier analysis on finite abelian groups*

The main consequence for *Fourer expansions* can be stated without mentioning many of the key ideas of the proofs.

Let G be a finite abelian group, and $L^2(G)$ the complex vectorspace of complex-valued functions [1] on G, with inner product [2]

$$\langle f, \varphi \rangle \;=\; \sum_{x \in G} f(x)\, \overline{\varphi}(x)$$

A **character** χ on a group is a group homomorphism [3]

$$\chi \;:\; G \;\longrightarrow\; \mathbb{C}^\times$$

Let $\widehat{G}$ be the collection of characters $\chi : G \to \mathbb{C}^\times$. For f a complex-valued function on G, the **Fourier transform** $\widehat{f}$ of f is the function on $\widehat{G}$ defined by

$$\widehat{f}(\chi) \;=\; \langle f, \chi \rangle \qquad\qquad (\text{for } \chi \in \widehat{G})$$

The **Fourier expansion** or **Fourier series** of f is

$$f \;\sim\; \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \widehat{f}(\chi)\, \chi$$

---

[1] In general, for a space X with some sort of *integral* on it, the notation $L^2(X)$ means functions f so that $\int_X |f|^2 < \infty$. On *finite* sets integrals become sums, possibly weighted, and this finiteness condition becomes *vacuous*. Nevertheless, it is good to use this notation as a reminder of the larger context.

[2] The notation $L^2(G)$ is meant to suggest the presence of the *inner product* on this space of functions. On a general space X with an integral, the iner product is $\langle f_1, f_2 \rangle = \int_X f_1 \overline{f}_2$.

[3] The term *character* has different meanings in different contexts. The simplest sense is a group homomorphism to $\mathbb{C}^\times$. However, an equally important use is for the *trace* of a group homomorphism $\rho : G \to GL_n(k)$ from G to invertible n-by-n matrices with entries in a field k. In the latter sense,

$$(\text{character of } \rho)(g) \;=\; \text{trace}\Big(\rho(g)\Big)$$

For *infinite*-dimensional representations, further complications appear. Except from context, there is no way to know which sense is intended.

[1.0.1] Theorem: On a finite abelian group, the Fourier expansion of a complex-valued function f *represents* f, in the sense that, for every $g \in G$,

$$f(g) \;=\; \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \widehat{f}(\chi)\, \chi(g)$$

The elements of $\widehat{G}$ form an orthogonal basis for $L^2(G)$. In particular, the Fourier coefficients are *unique*.

[1.0.2] Remark: What are we *not* doing? The theorem asserts nothing directly about the collection $\widehat{G}$ of characters of G. Its proof uses no information about these characters. Its proof uses nothing about the structure theorem for finite abelian groups. All that is used is a *spectral theorem*.

The proof is in the following paragraphs.

[1.1] Translation action on functions

The distinguishing feature of functions on a *group* is that the group acts on itself by right or left multiplication (or whatever the group operation is called), thereby moving around the *functions on it*.

The group operation in G will be written *multiplicatively*, not *additively*, to fit better with other notational conventions.

The group G *acts* on the vector space $L^2(G)$ of functions on itself by *translation*: for $g \in G$, the *translate* $T_g f$ of a function f by g is the function on G defined by [4]

$$(T_g f)(x) \;=\; f(xg) \qquad \text{(for function } f\text{, and } x, g \in G)$$

The maps-on-function T_g are vectorspace endomorphisms of the vectorspace of functions on G:

$$\begin{cases} T_g(f_1 + f_2)(x) \;=\; (f_1+f_2)(xg) \;=\; f_1(xg) + f_2(xg) \;=\; T_g f_1(x) + T_g f_2(x) & \text{(additivity)} \\ T_g(c \cdot f)(x) \;=\; (c \cdot f)(gx) \;=\; c\big(f(gx)\big) \;=\; \big(c \cdot (T_g f)\big)(x) & \text{(scalar } c) \end{cases}$$

To reduce clutter, the action of $g \in G$ on functions f may be written simply gf or $g \cdot f$. The **associativity** property

$$(gh)f \;=\; g(hf) \qquad \text{(for } g, h \in G\text{, function } f)$$

comes from the associativity of the group operation itself:

$$\big((gh)f\big)(x) \;=\; f(x(gh)) \;=\; f((xg)h) \;=\; (hf)(xg) \;=\; \big(g(hf)\big)(x)$$

[4] For *non-abelian* groups G, there are two translation actions, namely, *left* and *right*

$$\begin{cases} T_g^{\text{right}} f(x) \;=\; f(xg) \\ T_g^{\text{left}} f(x) \;=\; f(g^{-1}x) \end{cases}$$

The inverse in the left translation is for *associativity*

$$T_{gh}^{\text{left}} f \;=\; T_g\Big(T_h f\Big)$$

For abelian groups, the two translation actions become the same thing. Also, for abelian groups, the inverse in the definition of the left translation action loses some of its significance, since for *abelian* groups $g \to g^{-1}$ is a group automorphism.

The associativity property is equivalent to the assertion that the map $g \to T_g$ is a *group homomorphism* from G to $\mathbb{C}$-linear automorphisms of $L^2(G)$ (and that the identity element of g acts trivially).

Since $g \to T_g$ is a group homomorphism, the abelian-ness of G implies that the linear maps T_g, T_h commute: since $gh = hg$,

$$T_g \circ T_h \;=\; T_{gh} \;=\; T_{hg} \;=\; T_h \circ T_g \qquad\qquad \text{(for all } g, h \in G)$$

Since G is finite, there is a positive integer N such that, for all $g \in G$, $g^N = e \in G$. Thus,

$$\chi(g)^N \;=\; \chi(g^N) \;=\; \chi(e) \;=\; 1$$

That is, the values of χ lie on the unit circle in $\mathbb{C}^\times$, so $|\chi(g)| = 1$. In particular, χ is **unitary** in the sense that

$$\chi(g)^{-1} \;=\; \overline{\chi(g)}$$

We claim that the linear operators T_g are also *unitary*, in the sense that

$$\langle T_g f, T_g F\rangle \;=\; \langle f, F\rangle \qquad\qquad \text{(for } g \in G\text{, functions } f, F)$$

To prove this, compute directly:

$$\langle T_g f, T_g F\rangle \;=\; \sum_{h\in G} (T_g f)(h)\, \overline{(T_g F)(h)} \;=\; \sum_{h\in G} f(hg)\, \overline{F(hg)}$$

Change variables in the sum, by replacing h by hg^{-1}. Here the fact that G is a *group* is used: g^{-1} exists, and is closed under the group law:

$$\sum_{h\in G} f(hg)\, \overline{F(hg)} \;=\; \sum_{h\in G} f(h)\, \overline{F(h)} \;=\; \langle f, F\rangle$$

proving the unitarity.

For a *single* linear operator T on a complex vector space V, and for a complex number λ, the λ-eigenspace V_λ of T on V is

$$V_\lambda \;=\; \{v \in V \;:\; Tv = \lambda\cdot v\}$$

The **Spectral Theorem** for a *single* unitary operator T on a finite-dimensional complex vector space with inner product $\langle,\rangle$ asserts that V decomposes as an orthogonal direct sum of eigenspaces of T:

$$V \;=\; \bigoplus_\lambda V_\lambda \qquad\qquad \text{(orthogonal direct sum)}$$

We claim that another unitary operator S *commuting with* T *stabilizes* the T-eigenspaces V_λ. To see this, take $v \in V_\lambda$:

$$T(Sv) \;=\; (TS)v \;=\; (ST)v \;=\; S(Tv) \;=\; S(\lambda v) \;=\; \lambda\cdot Sv$$

since the linearity of S implies that S commutes with scalar multiplication.

This sets up an induction, as follows. We want to prove that a group H of *commuting* unitary operators on a finite-dimensional complex vectorspace V with hermitian inner product $\langle,\rangle$ has an orthogonal direct sum decomposition into *simultaneous* eigenspaces V_λ.

In this situation, the notion of *eigenvalue* must be a little more complicated than individual numbers: for *each* $T \in H$, there must be a number $\lambda_T \in \mathbb{C}$. That is, an *eigenvalue* is really a *map* $T \to \lambda_T$ from H to $\mathbb{C}$.

In this context, for two eigenvalues λ, μ to be *distinct* means that $\lambda_T \neq \mu_T$ for *some* $T \in H$ (not necessarily for *all* $T \in H$).

Now we do the induction. Suppose we have the conclusion for vector spaces of dimension $< n$. Let V be of dimension n. First, a silly case: if all operators $T \in H$ are *scalar*, then *every* vector is a simultaneous eigenvector for all the operators in H, and we are done. So now consider the (serious) case that *not* all operators in H are scalar. Let $T \in H$ be a non-scalar operator. By the spectral theorem for unitary operators, V has an orthogonal decomposition into eigenspaces for T, implicitly with different eigenvalues. Since T is non-scalar, every one of these eigenspaces has dimension $< n$. By induction, and by the fact that the operators all commute, each such eigenspace decomposes as an orthogonal direct sum of *simultaneous* eigenspaces for H. Thus, the whole space V is an orthogonal direct sum of simultaneous eigenspaces. This completes the induction.

Thus, in the case that H is the group of automorphisms T_g with $g \in G$ and $V = L^2(G)$,

$$L^2(G) \;=\; \bigoplus_\lambda L^2(G)_\lambda \qquad\qquad \text{(with simultaneous eigenvalues } \lambda : G \to \mathbb{C}^\times\text{)}$$

In fact, for H an abelian group of unitary automorphisms, we claim that the eigenvalues $T \to \lambda_T$ for $T \in H$ are *group homomorphisms* $H \to \mathbb{C}^\times$: for $S, T \in H$, and for v in the λ-eigenspace,

$$\lambda_{ST} \cdot v \;=\; (ST)(v) \;=\; S(T(v)) \;=\; S(\lambda_T \cdot v) \;=\; \lambda_T \cdot S(v) \;=\; \lambda_T \cdot \lambda_S \cdot v$$

Thus,

$$\lambda_{ST} \;=\; \lambda_T \cdot \lambda_S \qquad\qquad \text{(for all } S, T \in H\text{, simultaneous eigenvalue } \lambda : H \to \mathbb{C}^\times\text{)}$$

That is, for *groups* of automorphisms, *eigenvalues are characters*. We'll write V_χ instead of V_λ to emphasize this information, and for $L^2(G)$ write

$$L^2(G) \;=\; \bigoplus_{\chi \in \widehat{G}} L^2(G)_\chi$$

On one hand, every $\chi \in \widehat{G}$ is a complex-valued function on G, so is in $L^2(G)$. In fact, we claim that $\chi \in V_\chi$:

$$(T_g \chi)(h) \;=\; \chi(hg) \;=\; \chi(h)\,\chi(g) \;=\; \chi(g)\,\chi(h) \qquad\qquad \text{(since } \mathbb{C}^\times \text{ is abelian)}$$

On the other hand, we claim that V_χ is *exactly* scalar multiples $\mathbb{C} \cdot \chi$ of χ. To see this, let $f \in V_\chi$. Then

$$f(g) \;=\; f(e \cdot g) \;=\; (T_g f)(e) \;=\; \chi(g) \cdot f(e) \;=\; f(e) \cdot \chi(g)$$

That is,

$$f \;=\; f(e) \cdot \chi \qquad\qquad \text{(for } f \in V_\chi\text{)}$$

By the orthogonality of V_χ and V_τ for distinct χ, τ, the characters are an *orthogonal basis* for $L^2(G)$. Their lengths are readily determined, using the earlier-noted *unitariness* $\overline{\chi} = \chi^{-1}$:

$$\langle \chi, \chi \rangle \;=\; \sum_{g \in G} \chi(g) \cdot \overline{\chi}(g) \;=\; \sum_{g \in G} \chi(g) \cdot \chi(g)^{-1} \;=\; \sum_{g \in G} 1 \;=\; |G|$$

Any $f \in L^2(G)$ can be written as a linear combination of orthogogonal basis elements e_i

$$f \;=\; \sum_i \frac{\langle f, e_i \rangle \cdot e_i}{\langle e_i, e_i \rangle}$$

Using the orthogonal basis $\chi \in \widehat{G}$,

$$f \;=\; \sum_{\chi \in \widehat{G}} \frac{\langle f, \chi\rangle \cdot \chi}{\langle \chi, \chi\rangle} \;=\; \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \langle f, \chi\rangle \cdot \chi$$

This is an equality of functions on the finite set G, and $\widehat{f}(\chi)$ is defined to be $\langle f, \chi\rangle$, so

$$f(g) \;=\; \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \langle f, \chi\rangle \cdot \chi(g) \;=\; \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \widehat{f}(\chi) \cdot \chi(g) \qquad \text{(for all } g \in G)$$

This proves the representability of functions on finite abelian groups by their Fourier series. ///

---

2. *Appendix: spectral theorem for unitary operators*

Let V be a finite-dimensional complex vector space with a hermitian inner product $\langle, \rangle$. A linear map $T : V \to V$ is *unitary* if it preserves the inner product, in the sense that

$$\langle Tv, Tw\rangle \;=\; \langle v, w\rangle \qquad \text{(for all } v, w \in V)$$

Thus, the *adjoint* T^* of a unitary operator T has the property

$$\langle v, w\rangle \;=\; \langle Tv, Tw\rangle \;=\; \langle v, T^*Tw\rangle$$

Subtracting, $\langle v, T^*Tw - w\rangle \neq 0$ for all v, so $T^*Tw = w$ for all $w \in V$. That is, unitary T is *invertible*, and $T^* = T^{-1}$. This also shows that $T^*T = TT^*$.

The *inverse* of a unitary operator is unitary, since

$$\langle T^{-1}v, T^{-1}w\rangle \;=\; \langle T^*v, T^{-1}w\rangle \;=\; \langle v, TT^{-1}w\rangle \;=\; \langle v, w\rangle$$

Eigenvalues λ of a unitary operator T are of absolute value 1, since for a λ-eigenvector v

$$\lambda\overline{\lambda}\langle v, v\rangle \;=\; \langle \lambda v, \lambda v\rangle \;=\; \langle Tv, Tv\rangle \;=\; \langle v, v\rangle$$

In particular, eigenvalues λ are non-zero, and $\lambda^{-1} = \overline{\lambda}$.

Given $\lambda \in \mathbb{C}$, let

$$\lambda\text{-eigenspace of } T \;=\; V_\lambda \;=\; \{v \in V \;:\; Tv = \lambda \cdot v\}$$

[2.0.1] Theorem: The vectorspace is an *orthogonal* direct sum

$$V \;=\; \bigoplus_\lambda V_\lambda \qquad \text{(eigenspaces of unitary } T)$$

Proof: We grant ourselves the more elementary fact that, because V is finite-dimensional and $\mathbb{C}$ is algebraically closed, there is at least *one* one eigenvalue λ and non-zero eigenvector v for T. Thus, the λ-eigenspace V_λ is not $\{0\}$.

Now the unitariness is used, to set up an induction on dimension. We claim that T stabilizes the orthogonal complement

$$V_\lambda^\perp \;=\; \{w \in V \;:\; \langle w, v\rangle = 0 \text{ for all } v \in V_\lambda\}$$

Indeed, for w in that orthogonal complement and $v \in V_\lambda$,

$$\langle Tw, v\rangle \;=\; \langle w, T^* v\rangle \;=\; \langle w, T^{-1} v\rangle \;=\; \langle w, \lambda^{-1} v\rangle \;=\; \lambda \langle w, v\rangle \;=\; 0 \qquad \text{(for all } v \in V_\lambda)$$

The restriction of a unitary operator T to a T-stable subspace is obviously still unitary. By induction on the dimension of the vectorspace, $V_\lambda^\perp$ is an orthogonal direct sum of T-eigenspaces: $V_\lambda^\perp = \bigoplus_\mu V'_\mu$. Then

$$V \;=\; V_\lambda \oplus \bigoplus_\mu V'_\mu$$

is the orthogonal direct sum decomposition of the whole space. ///

---

3. *Appendix: cancellation lemma*

The orthogonality of distinct characters can be proven directly.

Let G be a finite group, not necessarily abelian. First, we have the **cancellation lemma:**

[3.0.1] Lemma: For a non-trivial group homomorphism $\sigma : G \to \mathbb{C}^\times$,

$$\sum_{g \in G} \sigma(g) \;=\; 0$$

Proof: Let $g_o \in G$ be such that $\sigma(g_o) \neq 1$. Then

$$\sum_{g \in G} \sigma(g) \;=\; \sum_{g \in G} \sigma(g_o g) \;=\; \sum_{g \in G} \sigma(g_o)\, \sigma(g) \;=\; \sigma(g_o) \sum_{g \in G} \sigma(g)$$

by replacing g by $g_o g$ in the sum, using the fact that left multiplication by g_o is a bijection of G to itself. Subtracting,

$$(1 - \sigma(g_o) \cdot \sum_{g \in G} \sigma(g) \;=\; 0$$

Since $\sigma(g_o) \neq 1$, necessarily the sum is 0. ///

[3.0.2] Corollary: Let $\sigma \neq \tau$ be group homomorphisms $G \to \mathbb{C}^\times$. Then

$$\sum_{g \in G} \sigma(g)\, \overline{\tau}(g) \;=\; 0$$

Proof: Since G is finite, there is N such that $g^N = e$ for every $g \in G$. Thus,

$$\tau(g)^N \;=\; \tau(g^N) \;=\; \tau(e) \;=\; 1$$

Thus, $\tau(g)$ is a root of unity, and $|\tau(g)| = 1$. In particular, $\overline{\tau}(g) = \tau(g)^{-1}$. Then $\sigma\overline{\tau} = \sigma\tau^{-1}$ is a character of G, and is not the trivial character. The previous lemma gives the vanishing. ///