Theorem 2.8 *If f is a function on G, then* $\|f\|^2 = \sum_{e\in\hat{G}} |\hat{f}(e)|^2$.

Proof. Since the characters of G form an orthonormal basis for the vector space V, and $(f,e) = \hat{f}(e)$, we have that

$$\|f\|^2 = (f,f) = \sum_{e\in\hat{G}} (f,e)\overline{\hat{f}(e)} = \sum_{e\in\hat{G}} |\hat{f}(e)|^2.$$

The apparent difference of this statement with that of Theorem 1.2 is due to the different normalizations of the Fourier coefficients that are used.

3 Exercises

1. Let f be a function on the circle. For each $N \geq 1$ the discrete Fourier coefficients of f are defined by

$$a_N(n) = \frac{1}{N}\sum_{k=1}^{N} f(e^{2\pi ik/N})e^{-2\pi ikn/N}, \qquad \text{for } n \in \mathbb{Z}.$$

We also let

$$a(n) = \int_0^1 f(e^{2\pi ix})e^{-2\pi inx}\,dx$$

denote the ordinary Fourier coefficients of f.

(a) Show that $a_N(n) = a_N(n+N)$.

(b) Prove that if f is continuous, then $a_N(n) \to a(n)$ as $N \to \infty$.

2. If f is a C^1 function on the circle, prove that $|a_N(n)| \leq c/|n|$ whenever $0 < |n| \leq N/2$.
[Hint: Write

$$a_N(n)[1 - e^{2\pi i\ell n/N}] = \frac{1}{N}\sum_{k=1}^{N}[f(e^{2\pi ik/N}) - f(e^{2\pi i(k+\ell)/N})]e^{-2\pi ikn/N},$$

and choose ℓ so that $\ell n/N$ is nearly 1/2.]

3. By a similar method, show that if f is a C^2 function on the circle, then

$$|a_N(n)| \leq c/|n|^2, \qquad \text{whenever } 0 < |n| \leq N/2.$$

As a result, prove the inversion formula for $f \in C^2$,

$$f(e^{2\pi ix}) = \sum_{n=-\infty}^{\infty} a(n)e^{2\pi inx}$$

from its finite version.

[Hint: For the first part, use the second symmetric difference

$$f(e^{2\pi i(k+\ell)/N}) + f(e^{2\pi i(k-\ell)/N}) - 2f(e^{2\pi ik/N}).$$

For the second part, if N is odd (say), write the inversion formula as

$$f(e^{2\pi ik/N}) = \sum_{|n|<N/2} a_N(n)e^{2\pi ikn/N}.]$$

4. Let e be a character on $G = \mathbb{Z}(N)$, the additive group of integers modulo N. Show that there exists a unique $0 \leq \ell \leq N-1$ so that

$$e(k) = e_\ell(k) = e^{2\pi i\ell k/N} \qquad \text{for all } k \in \mathbb{Z}(N).$$

Conversely, every function of this type is a character on $\mathbb{Z}(N)$. Deduce that $e_\ell \mapsto \ell$ defines an isomorphism from $\hat{G}$ to G.

[Hint: Show that $e(1)$ is an N^{th} root of unity.]

5. Show that all characters on S^1 are given by

$$e_n(x) = e^{2\pi inx} \qquad \text{with } n \in \mathbb{Z},$$

and check that $e_n \mapsto n$ defines an isomorphism from $\widehat{S^1}$ to $\mathbb{Z}$.

[Hint: If F is continuous and $F(x+y) = F(x)F(y)$, then F is differentiable. To see this, note that if $F(0) \neq 0$, then for appropriate δ, $c = \int_0^\delta F(y)\,dy \neq 0$, and $cF(x) = \int_x^{\delta+x} F(y)\,dy$. Differentiate to conclude that $F(x) = e^{Ax}$ for some A.]

6. Prove that all characters on $\mathbb{R}$ take the form

$$e_\xi(x) = e^{2\pi i\xi x} \qquad \text{with } \xi \in \mathbb{R},$$

and that $e_\xi \mapsto \xi$ defines an isomorphism from $\widehat{\mathbb{R}}$ to $\mathbb{R}$. The argument in Exercise 5 applies here as well.

7. Let $\zeta = e^{2\pi i/N}$. Define the $N \times N$ matrix $M = (a_{jk})_{1\leq j,k\leq N}$ by $a_{jk} = N^{-1/2}\zeta^{jk}$.

(a) Show that M is unitary.

(b) Interpret the identity $(Mu, Mv) = (u, v)$ and the fact that $M^* = M^{-1}$ in terms of Fourier series on $\mathbb{Z}(N)$.

8. Suppose that $P(x) = \sum_{n=1}^{N} a_n e^{2\pi i n x}$.

(a) Show by using the Parseval identities for the circle and $\mathbb{Z}(N)$, that

$$\int_0^1 |P(x)|^2 \, dx = \frac{1}{N} \sum_{j=1}^{N} |P(j/N)|^2.$$

(b) Prove the reconstruction formula

$$P(x) = \sum_{j=1}^{N} P(j/N) K(x - (j/N))$$

where

$$K(x) = \frac{e^{2\pi i x}}{N} \frac{1 - e^{2\pi i N x}}{1 - e^{2\pi i x}} = \frac{1}{N}(e^{2\pi i x} + e^{2\pi i 2x} + \cdots + e^{2\pi i N x}).$$

Observe that P is completely determined by the values $P(j/N)$ for $1 \leq j \leq N$. Note also that $K(0) = 1$, and $K(j/N) = 0$ whenever j is not congruent to 0 modulo N.

9. To prove the following assertions, modify the argument given in the text.

(a) Show that one can compute the Fourier coefficients of a function on $\mathbb{Z}(N)$ when $N = 3^n$ with at most $6N \log_3 N$ operations.

(b) Generalize this to $N = \alpha^n$ where α is an integer > 1.

10. A group G is **cyclic** if there exists $g \in G$ that generates all of G, that is, if any element in G can be written as g^n for some $n \in \mathbb{Z}$. Prove that a finite abelian group is cyclic if and only if it is isomorphic to $\mathbb{Z}(N)$ for some N.

11. Write down the multiplicative tables for the groups $\mathbb{Z}^*(3)$, $\mathbb{Z}^*(4)$, $\mathbb{Z}^*(5)$, $\mathbb{Z}^*(6)$, $\mathbb{Z}^*(8)$, and $\mathbb{Z}^*(9)$. Which of these groups are cyclic?

12. Suppose that G is a finite abelian group and $e : G \to \mathbb{C}$ is a function that satisfies $e(x \cdot y) = e(x)e(y)$ for all $x, y \in G$. Prove that either e is identically 0, or e never vanishes. In the second case, show that for each x, $e(x) = e^{2\pi i r}$ for some $r \in \mathbb{Q}$ of the form $r = p/q$, where $q = |G|$.

13. In analogy with ordinary Fourier series, one may interpret finite Fourier expansions using convolutions as follows. Suppose G is a finite abelian group, 1_G its unit, and V the vector space of complex-valued functions on G.

(a) The convolution of two functions f and g in V is defined for each $a \in G$ by

$$(f * g)(a) = \frac{1}{|G|} \sum_{b \in G} f(b)g(a \cdot b^{-1}).$$

Show that for all $e \in \hat{G}$ one has $\widehat{(f * g)}(e) = \hat{f}(e)\hat{g}(e)$.

(b) Use Theorem 2.5 to show that if e is a character on G, then

$$\sum_{e \in \hat{G}} e(c) = 0 \qquad \text{whenever } c \in G \text{ and } c \neq 1_G.$$

(c) As a result of (b), show that the Fourier series $Sf(a) = \sum_{e \in \hat{G}} \hat{f}(e)e(a)$ of a function $f \in V$ takes the form

$$Sf = f * D,$$

where D is defined by

$$D(c) = \sum_{e \in \hat{G}} e(c) = \begin{cases} |G| & \text{if } c = 1_G, \\ 0 & \text{otherwise.} \end{cases} \tag{4}$$

Since $f * D = f$, we recover the fact that $Sf = f$. Loosely speaking, D corresponds to a "Dirac delta function"; it has unit mass

$$\frac{1}{|G|} \sum_{c \in G} D(c) = 1,$$

and (4) says that this mass is concentrated at the unit element in G. Thus D has the same interpretation as the "limit" of a family of good kernels. (See Section 4, Chapter 2.)

Note. The function D reappears in the next chapter as $\delta_1(n)$.

4 Problems

1. Prove that if n and m are two positive integers that are relatively prime, then

$$\mathbb{Z}(nm) \approx \mathbb{Z}(n) \times \mathbb{Z}(m).$$