BIRKHÄUSER

Applied and Numerical Harmonic Analysis

FOURIER ANALYSIS ON FINITE ABELIAN GROUPS

Bao Luong

BIRKHÄUSER

Applied and Numerical Harmonic Analysis

Bao Luong

Fourier Analysis on Finite Abelian Groups

Birkhäuser
Boston • Basel • Berlin

Bao Luong
Department of Defense
Washington D.C.
bao.rzqv@math.wustl.edu

ISBN 978-0-8176-4915-9 e-ISBN 978-0-8176-4916-6
DOI 10.1007/978-0-8176-4916-6
Springer Dordrecht Heidelberg London New York

Library of Congress Control Number: 2009931929

Mathematics Subject Classification (2000): 42-xx, 42-01

Cover designed by Joseph Sherman.

Printed on acid-free paper

Birkhäuser Boston is part of Springer Science+Business Media (www.birkhauser com)

To my wife Anita for her patience and encouragement

Contents

ANHA Series Preface

The *Applied and Numerical Harmonic Analysis (ANHA)* book series aims to provide the engineering, mathematical, and scientific communities with significant developments in harmonic analysis, ranging from abstract harmonic analysis to basic applications. The title of the series reflects the importance of applications and numerical implementation, but richness and relevance of applications and implementation depend fundamentally on the structure and depth of theoretical underpinnings. Thus, from our point of view, the interleaving of theory and applications and their creative symbiotic evolution is axiomatic.

Harmonic analysis is a wellspring of ideas and applicability that has flourished, developed, and deepened over time within many disciplines and by means of creative cross-fertilization with diverse areas. The intricate and fundamental relationship between harmonic analysis and fields such as signal processing, partial differential equations (PDEs), and image processing is reflected in our state-of-the-art *ANHA* series.

Our vision of modern harmonic analysis includes mathematical areas such as wavelet theory, Banach algebras, classical Fourier analysis, time-frequency analysis, and fractal geometry, as well as the diverse topics that impinge on them.

For example, wavelet theory can be considered an appropriate tool to deal with some basic problems in digital signal processing, speech and image processing, geophysics, pattern recognition, biomedical engineering, and turbulence. These areas implement the latest technology from sampling methods on surfaces to fast algorithms and computer vision methods. The underlying mathematics of wavelet theory depends not only on classical Fourier analysis, but also on ideas from abstract harmonic analysis, including von Neumann algebras and the affine group. This leads to a study of the Heisenberg group and its relationship to Gabor systems, and of the metaplectic group for a meaningful interaction of signal decomposition methods. The unifying influence of wavelet theory in the aforementioned topics illustrates the justification for providing a means for centralizing and disseminating information from the broader, but still focused, area of harmonic analysis. This will be a key role of *ANHA*. We intend to publish with the scope and interaction that such a host of issues demands.

Along with our commitment to publish mathematically significant works at the frontiers of harmonic analysis, we have a comparably strong commitment to publish major advances in the following applicable topics in which harmonic analysis plays a substantial role:

Antenna theory
Biomedical signal processing
Digital signal processing
Fast algorithms
Gabor theory and applications
Image processing
Numerical partial differential equations
Prediction theory
Radar applications
Sampling theory
Spectral estimation
Speech processing
Time-frequency and time-scale analysis
Wavelet theory

The above point of view for the *ANHA* book series is inspired by the history of Fourier analysis itself, whose tentacles reach into so many fields.

In the last two centuries Fourier analysis has had a major impact on the development of mathematics, on the understanding of many engineering and scientific phenomena, and on the solution of some of the most important problems in mathematics and the sciences. Historically, Fourier series were developed in the analysis of some of the classical PDEs of mathematical physics; these series were used to solve such equations. In order to understand Fourier series and the kinds of solutions they could represent, some of the most basic notions of analysis were defined, e.g., the concept of "function." Since the coefficients of Fourier series are integrals, it is no surprise that Riemann integrals were conceived to deal with uniqueness properties of trigonometric series. Cantor's set theory was also developed because of such uniqueness questions.

A basic problem in Fourier analysis is to show how complicated phenomena, such as sound waves, can be described in terms of elementary harmonics. There are two aspects of this problem: first, to find, or even define properly, the harmonics or spectrum of a given phenomenon, e.g., the spectroscopy problem in optics; second, to determine which phenomena can be constructed from given classes of harmonics, as done, for example, by the mechanical synthesizers in tidal analysis.

Fourier analysis is also the natural setting for many other problems in engineering, mathematics, and the sciences. For example, Wiener's Tauberian theorem in Fourier analysis not only characterizes the behavior of the prime numbers, but also provides the proper notion of spectrum for phenomena such as white light; this latter process leads to the Fourier analysis associated with correlation functions in filtering and prediction problems, and these problems, in turn, deal naturally with Hardy spaces in the theory of complex variables.

Nowadays, some of the theory of PDEs has given way to the study of Fourier integral operators. Problems in antenna theory are studied in terms of unimodular trigonometric polynomials. Applications of Fourier analysis abound in signal processing, whether with the fast Fourier transform (FFT), or filter design, or the adaptive modeling inherent in time-frequency-scale methods such as wavelet theory. The coherent states of mathematical physics are translated and modulated Fourier transforms, and these are used, in conjunction with the uncertainty principle, for dealing with signal reconstruction in communications theory. We are back to the raison d'être of the *ANHA* series!

John J. Benedetto
Series Editor
University of Maryland
College Park

Preface

My main reason for writing this book was to present the theory of the Fourier transform (FT) in a clear manner that requires minimal mathematical knowledge without compromising mathematical rigor, so that it would be useful to students, mathematicians, scientists, and engineers.

The path along which I chose to develop the theory is not best, but it is elementary and within reach of many well-prepared undergraduate students. One can give better proofs of many results presented in this book; however, I feel the proofs given are elementary and easy to follow and that they require only minimal mathematical background.

The FT on finite Abelian groups has applications in many different areas of science, such as quantum information, quantum computation, image processing, signal analysis, cryptography, crypt-analytics, pattern recognition, and physics. With that said, my focus is on the theoretical aspect. I have designed this book to serve students in these areas and in other sciences, who have completed a semester of linear algebra and have some knowledge of abstract algebra. Typically, these would be second- or third-year students at American universities. Consequently, this monograph can be used as a one-semester undergraduate textbook in many different disciplines of mathematics and science. The book is self-contained and concise, and I have made an effort to make it easy to read. I hope that it will help students and professionals have a better understanding of the theory of the FT.

I would like to thank Franz Delahan, Robert Kibler, Tristan Nguyen, Glenn Shell, and Anita Woodley for their helpful comments, suggestions, and corrections concerning this book.

Bao Luong
April 2009

Overview

In general, the FT of a function defined on a group is a function defined on the dual group. For finite Abelian groups, the dual of a group is isomorphic to the group itself; this result allows us to define the FT as a linear operator on a finite-dimensional inner product space of scalar-valued functions defined on the group. This approach is clear and it gives much insight into the theory of the FT, since the theory of linear operators on finite-dimensional vector spaces is well understood.

We associate a group G with the inner product space of complex-valued functions defined on G and show that, under this association, spaces associated with isomorphic groups are isometric. Further, spaces associated with direct products of groups equal the tensor product of spaces associated with each factor group. Rather than define an inner product for a tensor product of inner product spaces to be the product of the inner products on factor spaces as is usually done, we obtain this "definition" as a consequence of the tensor decomposition of the FT. We also show that the convolution operator characterizes linear operators commuting with translations, and the tensor decomposition of the FT enables us to reduce the theory of the FT on finite Abelian groups to the transform on cyclic groups $\mathbb{Z}_n$, the integers modulo n. A related topic, quadratic Gaussian sums, is introduced and studied. We show that some quadratic Gaussian sums (evaluated at a point) are eigenvalues of the FT. This result, along with other properties of Gaussian sums, provides the means to find general formulas for these sums in terms of their parameters.

We note that the exercises in this book are numbered sequentially.

1

Foundation Material

In this chapter, we recall some results from elementary group theory, number theory, and approximation theory. In doing so, we also establish notation that will be used consistently throughout the rest of the text.

The symbol $|S|$ denotes the size of S. For example, if S is a finite set, then $|S|$ is the number of elements in S; if z is a complex number, then $|z|$ is the modulus (or absolute value) of z; and if f is a complex-valued function defined on a set S, then $|f|$ is the function (defined on the same set) whose value at a point $s \in S$ is $|f(s)|$.

Suppose S and S' are nonempty sets and $f \colon S \to S'$. We say that f is *injective* if it is one-to-one; *surjective* if it is onto; *bijective* if it is both injective and surjective. If $S = S'$ and f is bijective, we say that f is a *permutation* of S (or in S).

Throughout this book the symbol i denotes the principal square root of -1.

1.1 Results from Group Theory

We present some results from group theory that we will use in Chapter 3 to establish the theory of characters of finite Abelian groups. Since most of the material in this section can be found in either [6] or [14], no proofs are given.

Let $\mathbb{Z}$ be the set of integers and, for a positive integer n, let $\mathbb{Z}_n = \{0, \ldots, n-1\}$ be the set of integers modulo n. The sets $\mathbb{Z}$

B. Luong, *Fourier Analysis on Finite Abelian Groups*, Applied and Numerical Harmonic Analysis, DOI 10.1007/978-0-8176-4916-6_1,

and $\mathbb{Z}_n$ form groups under the operation of addition and addition modulo n, respectively. The binary operations on these two groups are written additively. The identity elements of $\mathbb{Z}$ and $\mathbb{Z}_n$ are both denoted by 0, and the inverse of $k \in \mathbb{Z}$ or $k \in \mathbb{Z}_n$ is denoted by $-k$. If an integer k has a multiplicative inverse in $\mathbb{Z}_n$, that is, if there is $x \in \mathbb{Z}$ such that $kx \equiv 1 \pmod{n}$, then we use k^{-1} to denote x. An element of $\mathbb{Z}_n$ for which a multiplicative inverse exists is called a *unit*; the units of $\mathbb{Z}_n$ are precisely the nonzero elements of $\mathbb{Z}_n$ that are coprime (or relatively prime) with n.

In general, we use the product notation for the binary operation of an arbitrary group; that is, if G is a group and a and b are elements of G, then ab denotes the product of a and b, which is defined with respect to the given binary operation in G. The identity of G is denoted by 1 and the inverse of $g \in G$ is denoted by g^{-1}.

In any group G, the equation $xg = xg'$ is equivalent to $g = g'$; roughly speaking, the cancellation law holds in G. This simple property leads to the following theorem.

Theorem 1.1.1. *Suppose that G is a finite group and x is an element of G. The function $f_x \colon G \to G$ defined by $f_x(g) = xg$ is a permutation of G.*

We use this theorem twice. (1) In a proof of a result about the sum of a character over a subgroup; i.e., Theorem 3.2.1 in Section 3.2. (2) In an evaluation of the quadratic Gaussian sum of order n at 1; i.e., Theorem 9.1.1 of the last chapter.

Though it is not needed in our work, we point out the fact that the map $x \mapsto f_x$ is injective. This follows from the definition of f_x and the cancellation law in G. This result is a prelude to Cayley's theorem, which states that *every group is isomorphic to a subgroup of a group of permutations* (*of some set*). (We will define the term *isomorphic* in the next paragraph.) We outline a proof of Cayley's theorem in Exercise 1.

Let G_1 and G_2 be groups. A map $h \colon G_1 \to G_2$ is called a *homomorphism* if $h(ab) = h(a)h(b)$ for every a, $b \in G_1$. Here, ab is a product of elements in G_1, whereas $h(a)h(b)$ is a product of elements in G_2. A bijective homomorphism is called an *isomorphism*.

We use the expression $G_1 \cong G_2$ to indicate that two groups G_1 and G_2 are isomorphic. There are, up to isomorphism, only one infinite cyclic group and one finite cyclic group of order n, namely, $\mathbb{Z}$ and $\mathbb{Z}_n$, respectively.

Theorem 1.1.2. *Suppose that G is a cyclic group. Then*

(i) *$G \cong \mathbb{Z}$ if G is infinite,*
(ii) *$G \cong \mathbb{Z}_n$ if G is finite and $n = |G|$.*

If $G_1, \ldots, G_m$ are groups and

$$G = G_1 \times \cdots \times G_m = \{(g_1, \ldots, g_m) \mid g_j \in G_j\},$$

then G is a group with respect to the binary operation defined component-wise by

$$(g_1, \ldots, g_m)(g'_1, \ldots, g'_m) = (g_1 g'_1, \ldots, g_m g'_m),$$

where $g_j g'_j$ is the product defined in G_j for $j = 1, \ldots, m$. The identity for this operation is $(1, \ldots, 1)$, an m-tuple of all 1's, which is simply denoted by 1. The inverse of $(g_1, \ldots, g_m)$, denoted by $(g_1, \ldots, g_m)^{-1}$, is given by $(g_1^{-1}, \ldots, g_m^{-1})$. With respect to the defined binary operation, G is called the *external direct product* (or, briefly, direct product) of $G_1, \ldots, G_m$. If $G_j = A$ for every j, then we write $G = A^m$. If for each j, either $G_j = \mathbb{Z}$ or $G_j = \mathbb{Z}_n$, then the binary operation of G is component-wise addition or addition modulo n; that is,

$$g_j g'_j = \begin{cases} g_j + g'_j & \text{if } G_j = \mathbb{Z}, \\ g_j + g'_j \pmod n & \text{if } G_j = \mathbb{Z}_n. \end{cases}$$

The identity of G, i.e., the m-tuple of zeros $(0, \ldots, 0)$, is denoted simply by 0. We also call the identity of G the *zero.*

Theorem 1.1.3 (The fundamental theorem of finite Abelian groups). *If G is a nontrivial finite Abelian group (i.e., G has more than one element), then there are unique positive integers s and $n_1, \ldots, n_s$, where each $n_j \geq 2$, such that $n_j \mid n_{j+1}$ for $j = 1, \ldots, s-1$ and*

$$G \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s}.$$

The number s is the *torsion-rank* of G, and $n_1, \ldots, n_s$ are the *invariants* of G.

There is an equivalent version of this theorem in which the order of each cyclic group in the factorization of G is a power of a prime. We state this equivalent version next.

Theorem 1.1.4. *If G is a nontrivial finite Abelian group, then $G \cong \mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_t}$, where $q_1, \ldots, q_t$ are* (*not necessarily distinct*) *powers of primes. Also, the numbers $q_1, \ldots, q_t$ are uniquely determined* (*up to order*)*.*

The prime powers are the *elementary divisors* of G.

The two versions of the fundamental theorem stated above are equivalent because of the Chinese remainder theorem which we outline in Exercises 2 and 3. A proof of the equivalent of the two versions of the fundamental theorem is outlined in Exercise 4. The fundamental theorem implies that every finite Abelian group is isomorphic to a direct product of cyclic groups, and this statement is the only implication that we will use.

Let n be an integer greater than 2. The *dihedral group D_n* is defined to be the set of all formal symbols $a^s b^t$, where $s = 0$, 1 and $t = 0, \ldots, n-1$, such that the following relations are satisfied:

(i) $a^s b^t = a^{s'} b^{t'}$ if and only if $s = s'$ and $t = t'$,
(ii) $a^2 = b^n = 1$,
(iii) $ab = b^{-1} a$.

These relations imply that D_n is a non-Abelian group of order $2n$. We use D_n in Section 6.4 to indicate one of the difficulties in any attempt to generalize the theory of the FT on finite Abelian groups to finite non-Abelian groups.

Exercises.

1. Let G be a group and let S_G be the set of permutations of G. Let f_x be as in Theorem 1.1. Then $f_x \in S_G$ for each $x \in G$. Define the product in S_G to be the composition of maps.

(i) Show that, with the defined product, S_G is a group and that $f_{xy} = f_x f_y$. Conclude that the map $x \mapsto f_x$ is an injective homomorphism (which is also called a *monomorphism*), hence Cayley's theorem follows. The group S_G is also called the *symmetric group* on G.

(ii) Consider $g \in G$ with $g \neq 1$ (this implicitly assumes that G has at least two elements). Define the map $f \colon G \to G$ by $f(1) = g$, $f(g) = 1$, and f leaves other elements of G fixed. Show that $f \in S_G$.

(iii) Suppose G has more than two elements. Prove that there is no $x \in G$ such that $f_x = f$. Conclude that $\{f_x \mid x \in G\}$ is a proper subgroup of S_G. In general, the size of G is much smaller than that of S_G. An obvious example to illustrate this point is to consider the group $G = \mathbb{Z}_n$ with $n > 2$. Then $|G| = n$ and $|S_n| = n!$. (Note: traditionally we use S_n to denote the group of permutations on n elements.)

For further elementary and clear treatment of Cayley's theorem see [6]. Roughly speaking, Cayley's theorem states that every group is a subgroup of a group of permutations of some set W. By choosing an appropriate set W, one can show the existence of a certain type of group, e.g., the existence of the external free product of groups (for more details see Theorem 68.2 and its proof given in [16], and the explanations followed on pp. 417–418).

2. The Chinese remainder theorem (CRT): *Suppose that $m_1, \ldots, m_n$ are pairwise coprime positive integers; that is, m_s and m_t are coprime if $s \neq t$. Let $m = \prod_{j=1}^{n} m_j$. For any integers $a_1, \ldots, a_n$, the system of congruences*

$$x \equiv a_j \pmod{m_j}, \qquad 1 \leq j \leq n \tag{1.1}$$

has a unique solution $x \in \mathbb{Z}$ modulo m. The uniqueness of the solution means that if x' is another solution, then $x \equiv x' \pmod{m}$. Replace a_j by $a_j + k_j m_j$ for some integer k_j if necessary, we may assume that $0 \leq a_j < m_j$ for each j. Prove this theorem by following the outline below.

(i) Let α be an integer and consider m_j (for any fixed j). Prove that if α and m_j are coprime, then there is an integer y such that $\alpha y \equiv 1 \pmod{m_j}$. The number y is unique if we impose the condition $0 < y < m_j$. (Hint: there are integers y and y' such that $\alpha y + m_j y' = 1$.)

(ii) Set $\alpha_j = m/m_j$. Show that α_j and m_j are coprime. Conclude that there is an integer y_j such that $\alpha_j y_j \equiv 1 \pmod{m_j}$.

(iii) Show that $x = \sum_{j=1}^{n} \alpha_j y_j a_j$ is a solution of the system of equations (1.1).

(iv) Show that if x and x' are two distinct solutions of (1.1), then $x \equiv x' \pmod{m_j}$ for every j. That is, every m_j divides $x - x'$. Since m_s and m_t are coprime if $s \neq t$, deduce that $m \mid (x - x')$ or, equivalently, $x \equiv x' \pmod{m}$.

The CRT can be generalized to the case that does not require the moduli m_j are pairwise coprime (see either p. 59 of [9], p. 29 of [11], or p. 69 of [15], also a good illustration is given in Chapter VIII of [5]). Note that the CRT also holds in rings that are more general than the ring $\mathbb{Z}$ of integers; for example, it holds in principle idea rings (pp. 76 and 329 of [12], also p. 8 of [17]).

3. Theorem: *If* $m_1, \dots, m_n$ *are pairwise coprime positive integers and* $m = \prod_{j=1}^{n} m_j$*, then* $\mathbb{Z}_m \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}$. Prove that this theorem is equivalent to the CRT. For simplicity we outline a proof for the case $n = 2$; the same outline (but with more variables involved) would also produce a proof for the general case. In the outline below we set $p = m_1$ and $q = m_2$.

- CRT ⇒ Theorem.

  Define the map $h\colon \mathbb{Z}_p \times \mathbb{Z}_q \to \mathbb{Z}_{pq}$ as follows: for any $(a, b) \in \mathbb{Z}_p \times \mathbb{Z}_q$, the CRT implies that there is a unique $x \in \mathbb{Z}_{pq}$ such that

$$x \equiv a \pmod{p} \quad \text{and} \quad x \equiv b \pmod{q}.$$

  Set $h(a, b) = x$. The uniqueness of x guarantees that h is a well-defined injective map. Since the domain and codomain of h have the same finite cardinality, h is also surjective. Prove that h is a group homomorphism, i.e.,

$$h(a+a', b+b') = h(a,b) + h(a',b').$$

(A slightly different proof is given in [7], p. 35.)

Observe that the commutativity of the ordinary product of two integers, i.e., $pq = qp$, implies that $\mathbb{Z}_{pq} \cong \mathbb{Z}_q \times \mathbb{Z}_p$. Since the composition of isomorphisms is also an isomorphism (or, equivalently, the isomorphic relation is transitive), we have $\mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_q \times \mathbb{Z}_p$. However, the implication

$$pq = qp \Rightarrow \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_q \times \mathbb{Z}_p$$

via the CRT is unintended. There is an obvious proof which shows that $\mathbb{Z}_s \times \mathbb{Z}_t \cong \mathbb{Z}_t \times \mathbb{Z}_s$ for any positive integers s and t regardless whether s and t are coprime. Can you find this "obvious" proof? Stated differently, if p and q are coprime, the conclusions of the theorem are

(a) the group $\mathbb{Z}_p \times \mathbb{Z}_q$ is cyclic (hence, by Theorem 1.1.2, it is isomorphic with $\mathbb{Z}_{pq}$);
(b) the group $\mathbb{Z}_{pq}$ can be decomposed as $\mathbb{Z}_p \times \mathbb{Z}_q$.

- Theorem ⇒ CRT.

  (i) Suppose that there is a group isomorphism $h\colon \mathbb{Z}_p \times \mathbb{Z}_q \to \mathbb{Z}_{pq}$. It follows that $h(a,b) = ah(1,0) + bh(0,1)$. What can we say about $h(1,0)$ and $h(0,1)$? Consider $h(1,0)$. Show that $(1,0)$ and $h(1,0)$ have the same order p.

  (ii) Show that elements of $\mathbb{Z}_{pq}$ which have order p are of the form zq, where z is coprime with p and $0 < z < p$. Conclude that

    (1) $h(1,0) \equiv 0 \pmod{q}$;

    (2) there is a unique integer s with $0 < s < p$ such that $sh(1,0) \equiv 1 \pmod{p}$ (hint: $h(1,0)$ and p are coprime).

  (iii) By symmetry, conclude that

    (1′) $h(0,1) \equiv 0 \pmod{p}$;

(2′) there is a unique integer t with $0 < t < q$ such that $th(0, 1) \equiv 1 \pmod{q}$.

(iv) Given $(a, b) \in \mathbb{Z}_p \times \mathbb{Z}_q$. Let $x = h(as, bt) = ash(1, 0) + bth(0, 1)$. Note that s and t do not depend on a and b. Prove that x is the unique element of $\mathbb{Z}_{pq}$ such that

$$x \equiv a \pmod{p} \quad \text{and} \quad x \equiv b \pmod{q}.$$

(Hint: for the uniqueness see (iv) of the previous exercise.)

A particular case of the theorem: if $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ is the prime decomposition of n, where all the primes p_j are distinct, then

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}. \tag{1.2}$$

4. Prove that the two stated versions of the fundamental theorem for finite Abelian groups are equivalent. Below is an outline (which requires some knowledge of quotient groups).

- Theorem 1.1.3 ⇒ Theorem 1.1.4.

Decompose each n_j into a product of powers of distinct primes, then use (1.2). To prove the uniqueness of the q_j, we use the fact that the direct product of finite cyclic groups is commutative (which we mentioned in the previous exercise). Suppose also that $G \cong \mathbb{Z}_{q'_1} \times \cdots \times \mathbb{Z}_{q'_r}$. Let p be a prime that divides the product $\prod_{j=1}^{t} q_j$, which equals $\prod_{j=1}^{r} q'_j$. Relabeling the subscripts if necessary, we may assume that

(1) $q_1 = p^e$ is the largest power of p in $\{q_1, \dots, q_t\}$;
(2) $q'_1 = p^f$ is the largest power of p in $\{q'_1, \dots, q'_t\}$.

Suppose $q_1 > q'_1$. Show that the group $\mathbb{Z}_{q_1} \times \cdots \times \mathbb{Z}_{q_t}$ has an element of order q_1, whereas the group $\mathbb{Z}_{q'_1} \times \cdots \times \mathbb{Z}_{q'_r}$ does not. Conclude that these two groups are not isomorphic, which is a contradiction. Similarly, the inequality $q_1 < q'_1$ cannot hold. Hence, we have $q_1 = q'_1$. Next, by considering the quotient group $G/\mathbb{Z}_{q_1}$, we may assume that

$\mathbb{Z}_{q_2} \times \cdots \times \mathbb{Z}_{q_t} \cong \mathbb{Z}_{q'_2} \times \cdots \times \mathbb{Z}_{q'_r}$. Consider this isomorphism and, as before, conclude that $q_2 = q'_2$. Conclude that $r = t$ and $q_j = q'_j$ for $j = 1, \ldots, t$.

- Theorem 1.1.4 ⇒ Theorem 1.1.3.

Set $A_0 = \{q_1, \ldots, q_t\}$ and construct the sets N_j as follows:

(a) Choose the largest number $q_{j_1} \in A_0$ (if there are two equal numbers, choose either one), then choose the largest number $q_{j_2} \in A_0 - \{q_{j_1}\}$ that is coprime with q_{j_1}, then choose the largest number $q_{j_3} \in A_0 - \{q_{j_1}, q_{j_2}\}$ that is coprime with q_{j_1} and q_{j_2}, and continue the process. Let N_0 denote the set of numbers chosen.

(b) Set $A_1 = A_0 - N_0$. If $A_1 \neq \emptyset$, then by construction every number in A_1 divides some number in N_0.

(c) If $A_1 \neq \emptyset$, we construct N_1 from A_1 by the same method as in the construction of N_0 from A_0. That is, choose the largest number $q_{k_1} \in A_1$, then choose the largest number $q_{k_2} \in A_1 - \{q_{k_1}\}$ that is coprime with q_{k_1}, then choose the largest number $q_{k_3} \in A_1 - \{q_{k_1}, q_{k_2}\}$ that is coprime with q_{k_1} and q_{k_2}, and so on. Let N_1 denote the set of numbers chosen (from A_1). Conclude from (b) that every number in N_1 divides some number in N_0.

(d) Repeat steps (b) and (c) to define A_j and to construct N_j, respectively, for $j > 2$.

Since A_0 is a finite set and $A_0 \supsetneq A_1 \supsetneq A_2 \supsetneq \cdots$, there is a smallest positive integer s such that $A_s = \emptyset$. Thus, $A_{s-1} = N_{s-1} \neq \emptyset$. For $j = 0, 1, \ldots, s-1$, let n_{s-j} be the product of all numbers in the set N_j. Show that each $n_k \geq 2$ and $n_k \mid n_{k+1}$ for $k = 1, \ldots, s-1$. Since the direct product of finite cyclic groups is commutative, use the theorem in the previous exercise to conclude that $G \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s}$ and $n_j \mid n_{j+1}$ for $j = 1, \ldots, s-1$. To prove the uniqueness of s and the n_j, assume that there are positive integers t and $m_1, \ldots, m_t$ with $m_j \mid m_{j+1}$ for $j = 1, \ldots, t-1$ such that

$$\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_t} \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s}. \tag{1.3}$$

Prove the following:

(e) $n_s g = 0$ for every $g \in \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_s}$.

(f) Conclude from (1.3) and (e) that $n_s g' = 0$ for every $g' \in \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_t}$. In particular, considered as an element of $\mathbb{Z}_{m_t}$, $n_s = 0$. So n_s is a nonzero multiple of m_t, which implies that $m_t \leq n_s$. By symmetry, we also have $m_t \geq n_s$; thus $m_t = n_s$.

(g) By considering the quotient group $G/\mathbb{Z}_{n_s}$, we may assume that

$$\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_{t-1}} \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_{s-1}}.$$

Conclude from (b) that $m_{t-1} = n_{s-1}$.

(h) Repeat step (g) and conclude that $s = t$ and $m_j = n_j$ for every j.

1.2 Quadratic Congruences

We present some results from elementary number theory, which we will use later in our construction of some particular eigenvalues and eigenvectors of the FT. Then we will use these eigenvalues and eigenvectors in our evaluation of quadratic Gaussian sums. Except for the material from Theorem 1.2.3 and thereafter, most of the other results stated here can be found in many introductory books on number theory, in particular [2].

Suppose that a and n are nonzero integers and that n is positive. If there is an integer x such that $x^2 \equiv a \pmod{n}$, then a is called a *quadratic residue modulo n*. The *Legendre symbol* (a/p), where p is an odd prime and $p \nmid a$ (i.e., p does not divide a), is defined by

$$(a/p) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p\text{, and} \\ -1 & \text{if } a \text{ is not a quadratic residue modulo } p. \end{cases}$$

In the symbol (a/p) we may assume that $0 < a < p$, since $x^2 \equiv a \,(\mathrm{mod} p)$ if and only if $x^2 \equiv (a + kp) \,(\mathrm{mod} p)$ for any integer k.

Example 1.2.1. It is easy to verify that the congruence equation $x^2 \equiv a\,(\bmod\ 11)$ has solutions for $a = 1, 3, 4, 5, 9$ and no solutions for $a = 2, 6, 7, 8, 10$. That is,

$$(1/11) = (3/11) = (4/11) = (5/11) = (9/11) = 1$$

and

$$(2/11) = (6/11) = (7/11) = (8/11) = (10/11) = -1.$$

We may conclude from this example that

$$\begin{aligned} &(6/11)(8/11) = (4/11), \quad (5/11)(9/11) = (1/11), \\ &(5/11)(7/11) = (2/11), \quad (2/11)(4/11) = (8/11). \end{aligned}$$

These equations of product of Legendre's symbol have the form $(a/p)(b/p) = (ab/p)$, which is guaranteed to be true in general by the following theorem.

Theorem 1.2.1. *Suppose that p is an odd prime and a and b are integers.*

(i) *If $p \nmid a$ and $p \nmid b$, then $(ab/p) = (a/p)(b/p)$.*
(ii) *If a has a multiplicative inverse modulo p, i.e., if there is an integer x such that $ax \equiv 1\,(\bmod\,p)$, then $(a/p) = (a^{-1}/p)$.*

Recall that in the symbol (a/p) we assumed that $0 < a < p$. For the same reason, in the equation $x^2 \equiv a\,(\bmod\,p)$ we may assume that $0 < x < p$. With this assumption we can show that if the equation $x^2 \equiv a\,(\bmod\,p)$ has a solution, then it has exactly two solutions.

Theorem 1.2.2. *Suppose that p is an odd prime. If $a \in \mathbb{Z}_p$ and $a \neq 0$, then the equation $x^2 \equiv a\,(\bmod\,p)$ has either exactly two solutions or no solutions in $\mathbb{Z}_p$. Furthermore, if x is a solution, then the other solution is $p - x$.*

Proof. Fix a nonzero element $a \in \mathbb{Z}_p$ and suppose that there is an element $x \in \mathbb{Z}_p$ such that $x^2 \equiv a\,(\bmod\,p)$. It is clear that we also have $(p - x)^2 \equiv a\,(\bmod\,p)$. To show there are no solutions other than x and $p - x$, we assume that $y^2 \equiv a \pmod{p}$ and show that either $y = x$ or $y = p - x$.

Since $x^2 \equiv a \pmod{p}$ and $y^2 \equiv a \pmod{p}$, by the transitivity property of the congruence modulo p, we have $x^2 \equiv y^2 \pmod{p}$. It follows that $(x - y)(x + y) \equiv 0 (\mathrm{mod} p)$ or, equivalently, $p \mid (x - y)(x + y)$. Thus, either $p \mid (x - y)$ or $p \mid (x + y)$.

If $p \mid (x - y)$, then, since $|x - y| < p$, we have $x - y = 0$ or $y = x$. If $p \mid (x + y)$, then, since $0 < x + y < 2p$, we have $x + y = p$ or $y = p - x$. ■

Example 1.2.2. If $k \in \mathbb{Z}_{17}$ and $k \neq 0$, then the following table

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$k^2 \pmod{17}$	1	4	9	16	8	2	15	13	13	15	2	8	16	9	4	1

shows that the equation $x^2 \equiv a \pmod{17}$ has solutions in $\mathbb{Z}_{17}$ for $a = 1$, 2, 4, 8, 9, 13, 15, 16 and has no solutions for $a = 3$, 5, 6, 7, 10, 11, 12, 14.

The example illustrates that half of the nonzero members of the group $\mathbb{Z}_{17}$ are quadratic residues modulo 17 and the other half of the nonzero members are not. In general, Theorem 1.2.2 implies that the equation $x^2 \equiv a \pmod{p}$ has two solutions in $\mathbb{Z}_p$ for $(p-1)/2$ values of a and no solutions for the remaining $(p-1)/2$ values of a. Thus, if the range of (a/p) is extended to include zero by allowing p divides a, that is,

$$(a/p) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ 0 & \text{if } p \mid a, \text{ and} \\ -1 & \text{if } a \text{ is not a quadratic residue modulo } p, \end{cases}$$

then

$$\sum_{a \in \mathbb{Z}_p} (a/p) = 0. \tag{1.4}$$

Part (i) of Theorem 1.2.1 may be stated in terms of the extended definition of the Legendre symbol as follows:

$$(ab/p) = (a/p)(b/p). \tag{1.5}$$

Since $x^2 \equiv (p-x)^2 \pmod{p}$, the entries in a table similar to that given in Example 1.2.2 are symmetric about $p/2$ and the same quadratic residues modulo p appear in each half. Hence, if Q_1 is the subset of $\mathbb{Z}_p$ consisting of quadratic residues, then $|Q_1| = (p-1)/2$ and, as k runs through $\mathbb{Z}_p$, the set $\{k^2 \pmod{p}\}$ produces 0 and two copies of Q_1. It follows that for any integer a,

$$1 + 2 \sum_{k \in Q_1} e^{-\frac{2\pi i}{p} ak} = \sum_{k \in \mathbb{Z}_p} e^{-\frac{2\pi i}{p} ak^2}. \tag{1.6}$$

We will use this result in the proof of the next theorem.

Note. The set Q_1 is a group with respect to multiplication modulo p.

Theorem 1.2.3. *If p is an odd prime and a is an integer that is not divisible by p, then*

$$\sum_{k \in \mathbb{Z}_p} e^{-\frac{2\pi i}{p} ak} (k/p) = \sum_{k \in \mathbb{Z}_p} e^{-\frac{2\pi i}{p} ak^2}.$$

Proof. If Q_0 is the subset of $\mathbb{Z}_p$ that consists of quadratic nonresidues, then the sets $\{0\}$, Q_0, and Q_1 are pairwise disjoint and their union is $\mathbb{Z}_p$. Thus, since $(0/p) = 0$, we have

$$\begin{aligned}
&\sum_{k \in \mathbb{Z}_p} e^{-\frac{2\pi i}{p} ak} (k/p) \\
&\quad = \sum_{k \in Q_1} e^{-\frac{2\pi i}{p} ak} - \sum_{k \in Q_0} e^{-\frac{2\pi i}{p} ak} \\
&\quad = 1 + 2 \sum_{k \in Q_1} e^{-\frac{2\pi i}{p} ak} - \left(1 + \sum_{k \in Q_1} e^{-\frac{2\pi i}{p} ak} + \sum_{k \in Q_0} e^{-\frac{2\pi i}{p} ak} \right) \\
&\quad = 1 + 2 \sum_{k \in Q_1} e^{-\frac{2\pi i}{p} ak} - \sum_{k \in \mathbb{Z}_p} e^{-\frac{2\pi i}{p} ak}.
\end{aligned}$$

It follows from (1.6) that

$$\sum_{k \in \mathbb{Z}_p} e^{-\frac{2\pi i}{p} ak} (k/p) = \sum_{k \in \mathbb{Z}_p} e^{-\frac{2\pi i}{p} ak^2} - \sum_{k \in \mathbb{Z}_p} e^{-\frac{2\pi i}{p} ak}.$$

To complete the proof we show that $\sum_{k \in \mathbb{Z}_p} e^{-\frac{2\pi i}{p}ak} = 0$. For this we set $r = e^{-\frac{2\pi i}{p}a}$. Then $r \neq 1$ (since $p \nmid a$), by the geometric progression formula we have

$$\sum_{k=0}^{p-1} r^k = \frac{1 - r^p}{1 - r}$$

or

$$\sum_{k \in \mathbb{Z}_p} e^{-\frac{2\pi i}{p}ak} = \sum_{k=0}^{p-1} (e^{-\frac{2\pi i}{p}a})^k = \frac{1 - e^{-2\pi i a}}{1 - e^{-\frac{2\pi i}{p}a}} = 0. \qquad \blacksquare$$

In Section 7.2, we rephrase the result of Theorem 1.2.3 in terms of the FT and Gaussian sums and show that sums of the type given in the theorem are eigenvalues of the FT.

Finally, we derive a result that we will use in a later section. Set $p = 2$ and let ν be an integer greater than one. We will show that the set $\{k^2 \,(\text{mod } 2^\nu) \mid k \in \mathbb{Z}_{2^\nu}\}$ contains two copies of the set $\{k^2 \,(\text{mod}\, 2^\nu) \mid k \in \mathbb{Z}_{2^{\nu-1}}\}$. The following example illustrates the case $\nu = 4$.

Example 1.2.3. Let $\nu = 4$ and consider the following table of values of k^2 when k takes its values in $\mathbb{Z}_{2^4}$.

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$k^2\,(\text{mod}\,16)$	0	1	4	9	0	9	4	1	0	1	4	9	0	9	4	1

Since the first eight elements of the first row are members of $\mathbb{Z}_8$, it is clear from the table that the set $\{k^2 \,(\text{mod}\,16) \mid k \in \mathbb{Z}_{16}\}$ contains two copies of the set $\{k^2 \,(\text{mod}\,16) \mid k \in \mathbb{Z}_8\}$.

In general, since

(i) the first half of $\mathbb{Z}_{2^\nu}$ (i.e., the set $\{0, 1, \ldots, 2^{\nu-1} - 1\}$) is $\mathbb{Z}_{2^{\nu-1}}$ and

(ii) $x^2 \equiv (x - 2^{\nu-1})^2 \,(\text{mod } 2^\nu)$ for every x in the second half of $\mathbb{Z}_{2^\nu}$ (i.e., $x > 2^{\nu-1} - 1$),

it follows that the two halves of the second row in a table similar to that given in Example 1.2.3 are identical. That is, as k runs through $\mathbb{Z}_{2^\nu}$ the set $\{k^2 \pmod{2^\nu}\}$ produces two copies of the set $\{k^2 \pmod{2^\nu} \mid k \in \mathbb{Z}_{2^{\nu-1}}\}$. Hence, for any integer a we have

$$\sum_{k \in \mathbb{Z}_{2^\nu}} e^{-\frac{2\pi i a k^2}{2^\nu}} = 2 \sum_{k \in \mathbb{Z}_{2^{\nu-1}}} e^{-\frac{2\pi i a k^2}{2^\nu}}. \tag{1.7}$$

We use equation (1.7) in Section 9.2 of the last chapter to evaluate Gaussian sums of degree 2^ν.

1.3 Chebyshev Systems of Functions

Consider the functions f_j for $j = 0, \ldots, n-1$, where these functions are defined on the set of real numbers by $f_0(x) = 1$ and $f_j(x) = x^j$ if $j > 0$. By the fundamental theorem of algebra,[1] the equation

$$c_0 f_0(x) + \cdots + c_{n-1} f_{n-1}(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} = 0,$$

where the coefficients $c_1, \ldots, c_{n-1}$ are real numbers and $c_{n-1} \neq 0$, has at most $n-1$ real roots. In other words, a linear combination of n continuous functions f_j has at most $n-1$ distinct real zeros. (A real zero of a function f is a real number r such that $f(r) = 0$.) We generalize this notion for arbitrary real-valued continuous functions on an interval.

Definition 1.3.1. *Suppose that $\phi_1, \ldots, \phi_n$ are real-valued continuous functions defined on an interval I, where I can be either closed, open, half-closed, or half-open, and of finite or infinite length. The set $\{\phi_k \mid k = 1, \ldots, n\}$ is called a Chebyshev system (or, briefly, C-system) if for every set $\{c_k \mid k = 1, \ldots, n\}$ of real numbers, not all zero, the equation $c_1\phi_1(x) + \cdots + c_n\phi_n(x) = 0$ has at most $n-1$ distinct (real) roots.*

Since the equation $c_1\phi_1(x) + \cdots + c_n\phi_n(x) = 0$ has at most $n-1$ roots, the function $c_1\phi_1(x) + \cdots + c_n\phi_n(x)$ changes sign at most $n-1$ times.

The following theorem is an immediate consequence of the definition.

[1] An equivalent statement of the fundamental theorem of algebra: every nonconstant polynomial of positive degree n, whose coefficients are complex numbers, has exactly n complex roots, counting multiplicity.

Theorem 1.3.1. *If the set* $\{\phi_k \mid k = 1, \ldots, n\}$ *is a C-system on an interval* I*, then the set* $\{\alpha_k \phi_k \mid k = 1, \ldots, n\}$ *is also a C-system on* I *for any nonzero constants* $\alpha_1, \ldots, \alpha_n$*.*

Example 1.3.1. The set $\{1, x, \ldots, x^n\}$ forms a C-system on any interval.

C-systems are studied in the theories of approximation and methods of interpolation, (e.g., [10] and [19]). Our goals in this section are

(a) to show that the sets $\{\cos(kx)\}_{k=0}^n$ and $\{\sin(kx)\}_{k=1}^n$ are C-systems (on appropriate intervals), and
(b) if the functions $\phi_1, \ldots, \phi_n$ form a C-system on an interval I, then, for every n distinct points $x_1, \ldots, x_n$ in I, the $n \times n$ matrix $(\phi_s(x_t))$, where s, $t = 1, \ldots, n$, is nonsingular.

These results are used in Section 7.3 to determine the multiplicity of the eigenvalues of the FT.

Theorem 1.3.2. *For each positive integer* n*, the sets* $\{\cos(kx)\}_{k=0}^n$ *and* $\{\sin(kx)\}_{k=1}^n$ *are C-systems on the intervals* $[0, \pi]$ *and* $[0, \pi)$*, respectively.*

Proof. First, we show that the set $\{\cos(kx)\}_{k=0}^n$ is a C-system on the interval $[0, \pi]$. Suppose that $a_0, \ldots, a_n$ are real numbers, not all zero, and that Φ is a real-valued function defined on the interval $[0, \pi]$ by

$$\Phi(x) = \sum_{k=0}^{n} a_k \cos(kx).$$

Since $\cos(kx) = (e^{ikx} + e^{-ikx})/2$, we can express Φ in terms of the exponential function as

$$\begin{aligned}\Phi(x) &= \frac{1}{2} \sum_{k=0}^{n} a_k (e^{ikx} + e^{-ikx}) \\ &= \frac{1}{2} \sum_{k=-n}^{n} b_k e^{ikx}\end{aligned}$$

$$= \frac{1}{2e^{inx}} \sum_{k=-n}^{n} b_k e^{i(k+n)x}$$

$$= \frac{1}{2e^{inx}} \sum_{k=0}^{2n} c_k e^{ikx},$$

where

$$b_k = \begin{cases} a_k & \text{if } k > 0, \\ 2a_0 & \text{if } k = 0, \\ a_{-k} & \text{if } k < 0, \end{cases}$$

and $c_k = b_{k-n}$.

The equation $\Phi(x) = 0$ is equivalent to the equation $H(z) \overset{\text{def}}{=} \sum_{k=0}^{2n} c_k z^k = 0$, where $z = e^{ix}$ is a point on the unit circle $S^1 = \{e^{ix} \mid -\pi \leq x \leq \pi\}$. Since the coefficients $c_0, \ldots, c_{2n}$ are real numbers, it follows that if $z = e^{ix}$ is a root of H, then $\bar{z} = e^{-ix}$ is also a root of H. Equivalently, considered as a function of x, $H(x) = 0$ if and only if $H(-x) = 0$. Consequently, the intervals $[-\pi, 0]$ and $[0, \pi]$ contain the same number of roots of H. Since H is a polynomial of degree at most $2n$, it has at most $2n$ roots in the complex plane; hence the unit circle S^1, being a subset of the complex plane, contains no more than $2n$ roots of H. Therefore, the interval $[0, \pi]$ contains at most n roots of H. Since H and Φ have the same roots in the interval $[0, \pi]$, the function Φ has at most n distinct roots. This proves that the set $\{\cos(kx)\}_{k=0}^{n}$ is a C-system on the interval $[0, \pi]$.

To prove that the set $\{\sin(kx)\}_{k=1}^{n}$ is a C-system on the interval $[0, \pi)$, we assume that $a_1, \ldots, a_n$ are real numbers, not all zero, and that Φ is a real-valued function defined on the interval $[0, \pi)$ by

$$\Phi(x) = \sum_{k=1}^{n} a_k \sin(kx).$$

Since $\sin(kx) = (e^{ikx} - e^{-ikx})/(2i)$, we can express Φ in terms of the exponential function as

$$\begin{aligned}\Phi(x) &= \frac{1}{2i}\sum_{k=1}^{n} a_k(e^{ikx} - e^{-ikx})\\ &= \frac{1}{2i}\sum_{k=-n}^{n} b_k e^{ikx}\\ &= \frac{1}{2ie^{inx}}\sum_{k=-n}^{n} b_k e^{i(k+n)x}\\ &= \frac{1}{2ie^{inx}}\sum_{k=0}^{2n} c_k e^{ikx},\end{aligned}$$

where

$$b_k = \begin{cases} a_k & \text{if } k > 0,\\ 0 & \text{if } k = 0,\\ -a_{-k} & \text{if } k < 0,\end{cases}$$

and $c_k = b_{k-n}$.

The equation $\Phi(x) = 0$ is equivalent to the equation $H(z) \overset{\text{def}}{=} \sum_{k=0}^{2n} c_k z^k = 0$, where $z = e^{ix}$ is a point on the unit circle $S^1 = \{e^{ix} \mid -\pi \leq x \leq \pi\}$. The same arguments given before (in the case for cosine) show that the interval $[0, \pi]$ contains at most n roots of H. Since $H(\pi) = 0$ and since H and Φ have the same roots in the interval $[0, \pi)$, the function Φ has at most $n - 1$ distinct roots in $[0, \pi)$. This proves that the set $\{\sin(kx)\}_{k=1}^{n}$ is a C-system on the interval $[0, \pi)$. ■

The following lemma is a basic result from linear algebra, which we will use in the proof of the next theorem.

Lemma 1.3.1. *Consider two matrices*

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n}\\ a_{21} & a_{22} & \dots & a_{2n}\\ \vdots & & \ddots & \vdots\\ a_{n1} & a_{n2} & \dots & a_{nn}\end{pmatrix}_{n\times n}$$

and

$$B = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & & \ddots & \vdots \\ b_{k1} & b_{k2} & \dots & b_{kn} \end{pmatrix}_{k\times n},$$

where A is nonsingular and B has an arbitrary number of rows. Suppose that the entries of A and B are real numbers and M is a $(k+n)\times n$ matrix formed by the rows of A and B (in any order). Then the columns of M form n linearly independent vectors (in $\mathbb{R}^{n+k}$).

Proof. Denote the column vectors of A and M by $A_1, \dots, A_n$ and $M_1, \dots, M_n$, respectively. If $c_1, \dots, c_n$ are real numbers such that $c_1M_1 + \dots + c_nM_n = 0$, the zero vector, then

$$c_1A_1 + \dots + c_nA_n = 0.$$

Since A is nonsingular, its column vectors $A_1, \dots, A_n$ are linearly independent, which implies that $c_1 = \dots = c_n = 0$. Thus, the vectors $M_1, \dots, M_n$ are linearly independent. ■

Another proof of the lemma is given as follows: since A is nonsingular, its row vectors are linearly independent, so the row rank of M is at least n. Since the row rank and column rank of a matrix are equal and M has only n columns, these column vectors are linearly independent.

Essentially, the lemma says that after inserting into a nonsingular square matrix any number of arbitrary row vectors, in any order, the column vectors of the new matrix are linearly independent.

Example 1.3.2. Consider the nonsingular matrix

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}_{2\times 2}.$$

By the lemma, the column vectors of each of the following matrices

$$\begin{pmatrix} 1 & 2 \\ 0 & 5 \\ 3 & 4 \end{pmatrix}_{3\times 2}, \quad \begin{pmatrix} 1 & 2 \\ 7 & 7 \\ 3 & 4 \\ 14 & 14 \end{pmatrix}_{4\times 2}, \quad \text{and} \quad \begin{pmatrix} 105 & -79 \\ \pi & 27.1 \\ 1 & 2 \\ -5 & 6.25 \\ 3 & 4 \\ -1.3 & \pi^2 \end{pmatrix}_{6\times 2}$$

are linearly independent.

Theorem 1.3.3. *Suppose that $\phi_1, \ldots, \phi_n$ are continuous real-valued functions defined on an interval I. Then the following statements are true*:

(i) *The functions $\phi_1, \ldots, \phi_n$ form a C-system on the interval I if and only if for every n distinct points $x_1, \ldots, x_n$ in I the matrix $(\phi_s(x_t))_{n\times n}$ is nonsingular.*

(ii) *Let $b_1, \ldots, b_{n+1}$ be alternating sign nonzero real numbers and let $x_1, \ldots, x_{n+1}$ be points in I, where $x_j < x_k$ if $j < k$. If the functions $\phi_1, \ldots, \phi_n$ form a C-system on I, then the matrix*

$$\begin{pmatrix} \phi_1(x_1) & \phi_2(x_1) & \ldots & \phi_n(x_1) & b_1 \\ \phi_1(x_2) & \phi_2(x_2) & \ldots & \phi_n(x_2) & b_2 \\ \vdots & & & & \vdots \\ \phi_1(x_{n+1}) & \phi_2(x_{n+1}) & \ldots & \phi_n(x_{n+1}) & b_{n+1} \end{pmatrix}_{(n+1)\times(n+1)} \tag{1.8}$$

is nonsingular.

Proof. Suppose that $\phi_1, \ldots, \phi_n$ are continuous real-valued functions defined on the interval I.

(i) Assume that the set $\{\phi_k\}_{k=1}^n$ is a C-system on I and $x_1, \ldots, x_n$ are distinct points in I. Suppose that the matrix $(\phi_s(x_t))_{n\times n}$ is singular. Then its transpose is also singular, so the column vectors of the transposed matrix

$$\begin{pmatrix} \phi_1(x_1) & \phi_2(x_1) & \ldots & \phi_n(x_1) \\ \phi_1(x_2) & \phi_2(x_2) & \ldots & \phi_n(x_2) \\ \vdots & & & \vdots \\ \phi_1(x_n) & \phi_2(x_n) & \ldots & \phi_n(x_n) \end{pmatrix}_{n\times n}$$

are linearly dependent. Hence there are constants $c_1, \dots, c_n$, not all zero, such that the equation $c_1\phi_1(x) + \cdots + c_n\phi_n(x) = 0$ has n distinct roots, namely, $x_1, \dots, x_n$. This is a contradiction.

Conversely, assume that the matrix $(\phi_s(x_t))_{n\times n}$ is nonsingular for every n distinct points $x_1, \dots, x_n$ in I. Let $v_1, \dots, v_n$ be real numbers and consider the real-valued function $\varPhi$ defined on I by

$$\varPhi(x) = v_1\phi_1(x) + \cdots + v_n\phi_n(x).$$

If the equation $\varPhi(x) = 0$ has more than $n-1$ distinct roots in I, then it has at least n distinct roots in I. Denote these n roots by $r_1, \dots, r_n$. We have

$$\begin{aligned} v_1\phi_1(r_1) + \cdots + v_n\phi_n(r_1) &= 0 \\ v_1\phi_1(r_2) + \cdots + v_n\phi_n(r_2) &= 0 \\ &\vdots \\ v_1\phi_1(r_n) + \cdots + v_n\phi_n(r_n) &= 0. \end{aligned}$$

This system of equations is equivalent to $Mv = 0$, where

$$M = \begin{pmatrix} \phi_1(r_1) & \phi_2(r_1) & \dots & \phi_n(r_1) \\ \phi_1(r_2) & \phi_2(r_2) & \dots & \phi_n(r_2) \\ \vdots & & & \vdots \\ \phi_1(r_n) & \phi_2(r_n) & \dots & \phi_n(r_n) \end{pmatrix}_{n\times n}$$

and

$$v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}.$$

By the assumption, the matrix M is nonsingular. It follows that $v = 0$, i.e., every v_k equals zero. Thus, if the numbers $v_1, \dots, v_n$ are not all zero, then the equation $\varPhi(x) = 0$ has no more than $n-1$ distinct roots in I. That is, the functions $\phi_1, \dots, \phi_n$ form a C-system on the interval I.

(ii) Assume that the functions $\phi_1, \dots, \phi_n$ form a C-system on the interval I and $x_1, \dots, x_{n+1}$ are distinct points in I such that $x_j < x_k$ if $j < k$. By (i) the matrix

$$\begin{pmatrix} \phi_1(x_1) & \phi_2(x_1) & \dots & \phi_n(x_1) \\ \phi_1(x_2) & \phi_2(x_2) & \dots & \phi_n(x_2) \\ \vdots & & & \vdots \\ \phi_1(x_n) & \phi_2(x_n) & \dots & \phi_n(x_n) \end{pmatrix}_{n\times n}$$

is nonsingular. By the lemma, the column vectors of the matrix

$$\begin{pmatrix} \phi_1(x_1) & \phi_2(x_1) & \dots & \phi_n(x_1) \\ \vdots & & & \vdots \\ \phi_1(x_n) & \phi_2(x_n) & \dots & \phi_n(x_n) \\ \phi_1(x_{n+1}) & \phi_2(x_{n+1}) & \dots & \phi_n(x_{n+1}) \end{pmatrix}_{(n+1)\times n}, \tag{1.9}$$

which is obtained by inserting the row vector $\big(\phi_1(x_{n+1}),\, \phi_2(x_{n+1}),\, \dots,\, \phi_n(x_{n+1})\big)$ into the previous matrix, are linearly independent. These vectors are the first n column vectors of the matrix (1.8). We aim to show that the vector

$$b = \begin{pmatrix} b_1 \\ \vdots \\ b_{n+1} \end{pmatrix}$$

is linearly independent of the column vectors of the matrix (1.9).

Suppose that b is linearly dependent on the column vectors of the matrix (1.9); i.e., there are constants $c_1, \dots, c_n$, not all zero, such that

$$c_1\phi_1(x_j) + \dots + c_n\phi_n(x_j) = b_j.$$

Since none of the numbers $b_1, \dots, b_{n+1}$ is zero and they have alternating sign, the function $c_1\phi_1 + \dots + c_n\phi_n$ has a root in the open interval $(x_j,\, x_{j+1})$ for every $j = 1, \dots, n$. Since there are n of these open intervals and no two of them have a point in common, the function $c_1\phi_1 + \dots + c_n\phi_n$ has at least n distinct roots. These roots all lie in I, since each interval $(x_j,\, x_{j+1})$ is a subset of I. The last sentence contradicts the assumption that the functions $\phi_1, \dots, \phi_n$ form a C-system on I or, equivalently, that any linear combination $c_1\phi_1 + \dots + c_n\phi_n$ with at least one nonzero coefficient cannot have more than $n - 1$ distinct roots in I. Thus the vector b is linearly independent of the column vectors of the matrix (1.9) or, equivalently, the matrix (1.8) is nonsingular. ■

2

Linear Algebra

The FT is a linear operator defined, for our purposes, on finite-dimensional inner product spaces. Given a finite Abelian group G, we will define the FT (in Chapter 4) to be a linear operator on a finite-dimensional inner product space associated with G. More generally, in this chapter, we define an association of sets with inner product spaces. We also define dual bases and a special type of linear operator, i.e., a type of operator that carries orthonormal bases to orthonormal bases. These operators are then formulated in terms of orthonormal bases and the dual of these bases.

The following definition will be used throughout this book: For any nonempty set S and any complex-valued function f defined on S, the *complex conjugate* of f, denoted by $\bar{f}$, is defined, for $s \in S$, by $\bar{f}(s) = \overline{f(s)}$.

2.1 Inner Product Spaces

Let V be a complex vector space, i.e., a vector space over the field of complex numbers $\mathbb{C}$. An *inner product* in V is a function $\langle \cdot, \cdot \rangle \colon V \times V \to \mathbb{C}$ which is required to satisfy the following properties: for x, y, $z \in V$ and $c \in \mathbb{C}$,

$$\begin{aligned} \langle x, y\rangle &= \overline{\langle y, x\rangle} && \text{(conjugate symmetric)},\\ \langle x, x\rangle &> 0 \quad \text{if } x \neq 0 && \text{(positive)},\\ \langle x, x\rangle = 0 &\Rightarrow x = 0 && \text{(definite)},\\ \langle cx + y, z\rangle &= c\langle x, z\rangle + \langle y, z\rangle && \text{(linear in the first variable)}. \end{aligned}$$

B. Luong, *Fourier Analysis on Finite Abelian Groups*, Applied and Numerical Harmonic Analysis, DOI 10.1007/978-0-8176-4916-6_2,

A vector space in which an inner product is defined is called an *inner product space.*

Example 2.1.1. The complex Euclidean vector space $\mathbb{C}^n$ is an inner product space with the inner product defined by

$$\langle x, y\rangle = \sum_{j=1}^{n} x_j \bar{y}_j,$$

where $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ are vectors in $\mathbb{C}^n$.

Suppose that V is a complex inner product space. The *norm* (or *length*) of a vector $x \in V$, denoted by $\|x\|$, is defined to be the (nonnegative) number $\sqrt{\langle x, x\rangle}$. Two vectors x and y in V are said to be *orthogonal* or *perpendicular* (in symbols, $x \perp y$) if $\langle x, y\rangle = 0$. The linear, positive and definite properties of the inner product imply that the zero vector is the only vector that is orthogonal to every vector in V. Consequently, the norm of the zero vector is equal to zero. A nonzero vector x is called a *unit vector* if $\|x\| = 1$. A subset E of V is called an *orthonormal set* if every vector in E is a unit vector and if every vector in E is orthogonal to every other vector in E. If, in addition to being an orthonormal set, E is a basis of V, then E is called an *orthonormal basis*.

There is a very useful inequality which guarantees that the absolute value of the inner product of two vectors is never greater than the product of the norms of the vectors involved. The mentioned inequality is known as Schwarz's inequality. Although we will use only Schwarz's inequality (in the remark at the end of Section 2.2 below, and in Sections 5.2 and 5.3), we also list other well-known inequalities and identities involving norm of vectors in the following theorem.

Theorem 2.1.1. *Suppose that V is a complex inner product space. The following inequalities and identities hold: for any x, $y \in V$,*

(i) (*Bessel's inequality*) *if $\{e_j \mid j = 1, \ldots, k\}$ is an orthonormal subset of V, then*

$$\sum_{j=1}^{k} |\langle x, e_j\rangle|^2 \le \|x\|^2,$$

equality holds if and only if $x = \sum_{j=1}^{k} \langle x, e_j\rangle e_j$;

(ii) (*Schwarz's inequality*) $|\langle x, y\rangle| \le \|x\|\|y\|$, *furthermore, if* $y \neq 0$, *then equality holds if and only if* $x = cy$, *where* $c = \langle x, y\rangle / \|y\|^2$;

(iii) (*Triangle inequality*) $\|x + y\| \le \|x\| + \|y\|$, *furthermore, if* $y \neq 0$, *then equality holds if and only if* $x = cy$ *for some nonnegative constant* c;

(iv) (*Pythagorean theorem*) $\|x + y\|^2 = \|x\|^2 + \|y\|^2$ *if* $x \perp y$;

(v) (*Parallelogram law*) $\|x + y\|^2 + \|x - y\|^2 = 2\|x\|^2 + 2\|y\|^2$.

Proof. (i) For the Bessel inequality, we note that

$$\begin{aligned}
0 &\le \Big\| x - \sum_{s=1}^{k} \langle x, e_s\rangle e_s \Big\|^2 \\
&= \|x\|^2 - \sum_{s=1}^{k} \langle x, e_s\rangle \langle e_s, x\rangle - \sum_{s=1}^{k} \overline{\langle x, e_s\rangle} \langle x, e_s\rangle \\
&\quad + \sum_{s,\,t=1}^{k} \langle x, e_s\rangle \overline{\langle x, e_t\rangle} \langle e_s, e_t\rangle \\
&= \|x\|^2 - \sum_{s=1}^{k} |\langle x, e_s\rangle|^2.
\end{aligned}$$

(ii) The Schwarz inequality holds trivially if $y = 0$. For $y \neq 0$ it is a special case of the Bessel inequality, in which the orthonormal set is taken to be the set $\{y/\|y\|\}$ consisting of only one vector.

(iii) We use the Schwarz inequality to prove the triangle inequality. Denote the real part of a complex number z by $\operatorname{Re} z$. Since

$$\|x + y\|^2 = \|x\|^2 + \|y\|^2 + 2\operatorname{Re}\langle x, y\rangle \tag{2.1}$$

$$\le \|x\|^2 + \|y\|^2 + 2|\langle x, y\rangle| \quad \text{(by the fact that } \operatorname{Re} z \le |z|\text{)} \tag{2.2}$$

$$\le \|x\|^2 + \|y\|^2 + 2\|x\|\|y\| \quad \text{(by the Schwarz inequality)} \tag{2.3}$$

$$= (\|x\| + \|y\|)^2,$$

the triangle inequality follows.

If $y \neq 0$, then $\|x+y\| = \|x\| + \|y\|$ if and only if we have equality in (2.2) and (2.3) or, equivalently, $\mathrm{Re}\langle x, y\rangle = \langle x, y\rangle = \|x\|\|y\|$. By the Schwarz inequality, the latter equality is equivalent to $x = cy$, where $c = \langle x, y\rangle / \|y\|^2 \geq 0$.

The remaining statements (iv) and (v), that is, the Pythagorean theorem and the parallelogram law, follow from (2.1). ■

There is a simple geometric interpretation of the Bessel inequality. Since the sum $\sum_{j=1}^{k} \langle x, e_j\rangle e_j$ is the *orthogonal projection* of x in the subspace spanned by the orthonormal vectors e_j, $j = 1, \ldots, k$, the Bessel inequality states that the norm of any vector x is always greater than the norm of its orthogonal projection in any finite-dimensional subspace, unless the subspace in consideration contains x, in which case x and its orthogonal projection are identical.

Remark. We shall use the same notation for inner products in all inner product spaces; consequently, we shall use the same notation to denote norms in all inner product spaces.

Let $\Lambda\colon V \to W$ be a linear operator, where W is also a complex inner product space. The operator Λ is said to be an operator on V if $W = V$, a *linear functional* if $W = \mathbb{C}$, and an *isometry* if it is one-to-one, onto, and preserves the inner product, i.e.,

$$\langle \Lambda(x), \Lambda(y)\rangle = \langle x, y\rangle$$

for all x, $y \in V$. It is easy to verify that the inverse of an isometry is also an isometry. Hence, we can speak of an isometry between two inner product spaces. Two complex inner product spaces V and W are said to be *isometric* (in symbols, $V \simeq W$) if there is an isometry between them.

2.2 Linear Functionals and Dual Spaces

Suppose that V is a complex inner product space (not necessarily finite-dimensional). The set V^* of linear functionals on V is a complex vector space with respect to the pointwise definition of addition and scalar multiplication defined as follows: for f, $g \in V^*$

and $c \in \mathbb{C}$, the sum of f and g, denoted by $f + g$, and the scalar multiplication of f by c, denoted by cf, are defined by

$$(f+g)(x) = f(x) + g(x)$$
$$cf(x) = c(f(x))$$

for all $x \in V$. The vector space V^* is called the *dual space* of V.

To exhibit some elements of V^*, for each $y \in V$, we define the function $\ell_y \colon V \to \mathbb{C}$ by setting $\ell_y(x) = \langle x, y \rangle$. Since the inner product is linear in the first variable, ℓ_y is a linear functional on V, that is, $\ell_y \in V^*$. In fact, every linear functional on V can be obtained in this way if V is finite-dimensional. This is the main content of the next theorem, which is a special case of a famous theorem known as the Riesz representation theorem.

Theorem 2.2.1. *Let V be a finite-dimensional complex inner product space. The function $\ell \colon V \to \mathbb{C}$ is a linear functional if and only if there is a unique vector y in V such that $\ell(x) = \langle x, y \rangle$ for all x in V.*

Proof. It remains to show only that if ℓ is a linear functional on V, then there is a unique $y \in V$ such that $\ell(x) = \langle x, y \rangle$ for every $x \in V$. Let $n = \dim V$ and let $\{b_j\}_{j=1}^n$ be an orthonormal basis for V. If $x \in V$, then x can be written uniquely as

$$x = \sum_{j=1}^n \langle x, b_j \rangle b_j.$$

Since ℓ is linear, we have

$$\begin{aligned} \ell(x) &= \sum_{j=1}^n \langle x, b_j \rangle \ell(b_j) \\ &= \sum_{j=1}^n \langle x, \bar{\ell}(b_j) b_j \rangle \\ &= \left\langle x, \sum_{j=1}^n \bar{\ell}(b_j) b_j \right\rangle \\ &= \langle x, y \rangle, \end{aligned}$$

where $y = \sum_{j=1}^n \bar{\ell}(b_j) b_j$. To prove the uniqueness of y, assume that there is another $y' \in V$ such that $\ell(x) = \langle x, y' \rangle$ for all x in

V. It follows that $\langle x, y - y' \rangle = 0$ for every vector x in V, whence $y - y' = 0$ or $y = y'$. ■

By Theorem 2.2.1, there is a one-to-one correspondence between V and V^*, which is given by $v \leftrightarrow \ell_v$, where $\ell_v(x) = \langle x, v \rangle$ for all $x \in V$. Since

$$\ell_{cv} = \bar{c}\ell_v \quad \text{and} \quad \ell_{v+v'} = \ell_v + \ell_{v'}, \tag{2.4}$$

for all v, $v' \in V$ and $c \in \mathbb{C}$, the correspondence $v \leftrightarrow \ell_v$, which is conjugate linear, induces an inner product in V^* defined in terms of the inner product in V by the equation

$$\langle \ell_v, \ell_{v'} \rangle = \overline{\langle v, v' \rangle}. \tag{2.5}$$

Consequently, the relation $\|\ell_v\| = \|v\|$ holds for every $v \in V$; i.e., every linear functional on V has finite norm or, equivalently, bounded.

For each $v \in V$, the linear functional ℓ_v, called the *dual* of v, is often denoted by v^*. With this notation, we have

$$v^*(x) = \langle x, v \rangle. \tag{2.6}$$

In general, bases of V induce bases of V^*. Furthermore, orthonormal bases induce orthonormal bases. A special case is illustrated next. Suppose that $n = \dim V$ and $E = \{e_j \mid j = 1, \ldots, n\}$ is an orthonormal basis for V. Since every element of V^* is of the form v^* for some

$$v = \sum_{j=1}^{n} \langle v, e_j \rangle e_j \in V,$$

by (2.4) we have

$$v^* = \sum_{j=1}^{n} \overline{\langle v, e_j \rangle}\, e_j^*.$$

It follows that the set $E^* = \{e_j^* \mid j = 1, \ldots, n\}$ spans the space V^*. Moreover, the relation (2.5) implies that E^* is an orthonormal set, hence it is an orthonormal basis of V^*. Consequently, we have $\dim V = \dim V^*$. The basis E^* is called the *dual basis* of E.

Remark. As mentioned, Theorem 2.2.1 is the finite-dimensional case of the Riesz representation theorem. The main conclusion of Theorem 2.2.1 is that every linear functional ℓ is given in terms of the inner product. Consequently, ℓ is bounded. Observe that any linear functional ℓ defined in terms of the inner product as $\ell(x) = \langle x, y\rangle$ for some fixed y is bounded regardless of the dimension of V. That is, $|\ell(x)| \leq \|x\|\|y\|$ for all x. This fact follows from the Schwarz inequality. Thus, to modify the statement of Theorem 2.2.1 to get a general version of the Riesz theorem for infinite-dimensional Hilbert spaces we must add the hypothesis that ℓ is bounded. For a beautiful introduction to the topic of Hilbert spaces and a nice proof of the Riesz representation theorem see [4].

2.3 A Special Class of Linear Operators

It is simpler to define a general family of operators of which the FT is a member than to define the FT itself. This is what we do in this section.

Let S be any nonempty finite set and let V_S be the set of all complex-valued functions defined on S. Then V_S is a complex vector space with respect to the pointwise definition of addition and scalar multiplication. Furthermore, V_S becomes an inner product space with an inner product defined by setting

$$\langle f, g\rangle = \sum_{s \in S} f(s)\bar{g}(s).$$

With this definition, it is simple to construct an orthonormal basis for V_S. For each $s \in S$, let $\delta_s \colon S \to \mathbb{C}$ be the function defined by

$$\delta_s(t) = \begin{cases} 1 & \text{if } s = t, \\ 0 & \text{if } s \neq t. \end{cases}$$

Then it is obvious that the set $\mathit{\Delta}_S = \{\delta_s \mid s \in S\}$ is an orthonormal basis for V_S, called the *standard basis*. Since S is a finite set, V_S is a finite-dimensional complex inner product space. In fact, $V_S \simeq \mathbb{C}^n$, where $n = |S|$. Hence, S can serve as an index set for any basis of V_S.

Suppose, in addition to $\mathit{\Delta}_S$, that $B_S = \{B_s \mid s \in S\}$ is another orthonormal basis of V_S. Since every $x \in V_S$ can be written uniquely as

$$x = \sum_{s \in S} \langle x, B_s \rangle B_s = \sum_{s \in S} B_s B_s^*(x),$$

the identity operator on V_S can be expressed uniquely in terms of the basis B_S and its dual B_S^* as

$$I = \sum_{s \in S} B_s B_s^*. \tag{2.7}$$

In terms of the dual basis $\mathit{\Delta}_S^*$, we have

$$B_s^* = \sum_{t \in S} \langle B_s^*, \delta_t^* \rangle \delta_t^* = \sum_{t \in S} \langle \delta_t, B_s \rangle \delta_t^*,$$

whence

$$I = \sum_{s,t \in S} \langle \delta_t, B_s \rangle B_s \delta_t^*.$$

It follows that the image of any $x \in V_S$ under any linear operator $\mathit{\Lambda}$ on V_S is given by

$$\mathit{\Lambda}(x) = \sum_{s,t \in S} \langle \delta_t, B_s \rangle \mathit{\Lambda}(B_s) \delta_t^*(x).$$

Hence,

$$\mathit{\Lambda} = \sum_{s,t \in S} \langle \delta_t, B_s \rangle \mathit{\Lambda}(B_s) \delta_t^*. \tag{2.8}$$

In equation (2.8), for each $s \in S$, $\mathit{\Lambda}(B_s)$ can be any vector in V_S. Now we single out an operator that maps B_s to the unique element of the basis $\mathit{\Delta}_S$ that is associated with B_s in a very natural way: for a fixed $s \in S$, by (2.7),

$$B_s = \sum_{t \in S} B_t B_t^*(B_s) = \sum_{t \in S} \delta_s(t) B_t. \tag{2.9}$$

The uniqueness of this expression (of B_s in the basis B_S) induces a one-to-one correspondence $B_s \leftrightarrow \delta_s$, which is independent of any enumeration (or indexing of elements) of the basis B_S. Through this correspondence, we define a linear operator $\mathcal{F}$ on V_S by setting $\mathcal{F}(B_s) = \delta_s$ for every $s \in S$.

The next theorem follows from the definition of $\mathcal{F}$ and equation (2.8).

Theorem 2.3.1. *Assume the following*:

(a1) *S is a nonempty finite set and V_S is the associated inner product space of complex-valued functions on S;*

(a2) *$\varDelta_S = \{\delta_s \mid s \in S\}$ and $B_S = \{B_s \mid s \in S\}$ are two orthonormal bases of V_S, where $\varDelta_S$ is the standard basis;*

(a3) *$\mathcal{F}$ is the linear operator on V_S such that $\mathcal{F}(B_s) = \delta_s$ for every $s \in S$, where δ_s is the unique vector in $\varDelta_S$ associated with B_s by equation* (2.9).

Then

(c1) $\mathcal{F} = \sum_{s,\, t \in S} \langle \delta_t, B_s \rangle \delta_s \delta_t^*$,

(c2) *$\mathcal{F}$ is an isometry, and*

(c3) *$\mathcal{F}f(s) = \langle f, B_s \rangle$, for any $f \in V_S$.* (*Here we write $\mathcal{F}f$ for $\mathcal{F}(f)$.*)

The complex number $\langle f, B_s \rangle$ is called the *s-coefficient* of f in the orthonormal basis B_S.

If G is a finite Abelian group, the FT on G is the linear operator $\mathcal{F}$ described in Theorem 2.3.1 with respect to a particular orthonormal basis B_G, which we will define in the next chapter.

Exercises.

5. Let V be a complex vector space, not necessarily finite-dimensional. Is every non-identically zero linear functional on V surjective?

6. Let V be a finite-dimensional complex vector space, not necessarily an inner product space.

(i) Assume that f and g are linear functionals on V and that $f(x) = 0$ whenever $g(x) = 0$. Show that $f = cg$ for some constant c.

(ii) Let $\{b_1, \dots, b_n\}$ be a basis of V and let $\{c_1, \dots, c_n\}$ be any set of constants. Show that there is a unique linear functional f on V such that $f(b_j) = c_j$ for $j = 1, \dots, n$.

(iii) Let x be a nonzero vector in V. Prove that there is a linear functional f on V such that $f(x) = 1$.

(iv) Let f be a nonzero linear functional on V. Prove that there is at least one vector $x \in V$ such that $f(x) = 1$.

(v) Let $f_1, \dots, f_n$ be linear functionals on V, where $n < \dim V$. Prove that there is a nonzero vector $x \in V$ such that $f_j(x) = 0$ for $j = 1, \dots, n$.

7. Let V be an inner product space, not necessarily finite-dimensional, with the underlying field of scalars $\mathbb{F}$, where either $\mathbb{F} = \mathbb{R}$ or $\mathbb{F} = \mathbb{C}$. Let x and y be two vectors in V, prove the following statements:

(i) If $\mathbb{F} = \mathbb{R}$ and $\|x\| = \|y\|$, then $(x + y) \perp (x - y)$.

(ii) If $\mathbb{F} = \mathbb{R}$, then $x \perp y$ if and only if $\|x+y\|^2 = \|x\|^2+\|y\|^2$.

(iii) If $\mathbb{F} = \mathbb{C}$, then $x \perp y$ if and only if $\|x + cy\|^2 = \|x\|^2 + \|cy\|^2$ for every complex number c.

8. Let $\mathcal{F}^{-1}$ denote the inverse of $\mathcal{F}$. For $f \in V_S$, prove that

$$f = \sum_{s \in S} \langle \mathcal{F} f, \delta_s \rangle B_s \quad \text{and} \quad \mathcal{F}^{-1} f = \sum_{s \in S} \langle f, \delta_s \rangle B_s.$$

3

Characters of Finite Groups

There are two goals in this chapter. The first goal is to sufficiently develop the theory of characters of groups, which will enable us to reduce the study of characters of finite Abelian groups to the study of characters of finite cyclic groups. Second, we investigate the characters of finite cyclic groups. Throughout the rest of the book, we use the symbol $\mathbb{C}^*$ to denote the multiplicative group of nonzero complex numbers.

3.1 Definition and Basic Properties of Characters

Definition 3.1.1[1] *A character of a group G is a homomorphism from G into the multiplicative group of nonzero complex numbers. That is, a character of G is a function $\chi\colon G \to \mathbb{C}^*$ that satisfies the equation $\chi(ab) = \chi(a)\chi(b)$ for all a, $b \in G$. A character χ is called trivial (or principal) if $\chi(g) = 1$ for all $g \in G$.*

It follows from this definition that: (1) every group has a character, namely, the trivial character. The trivial character of a group is often denoted by χ_T. (2) Every character maps the identity of G to 1.

Let χ and χ' be characters of G. The *pointwise product* of χ and χ' is the function $\chi\chi'\colon G \to \mathbb{C}^*$ defined by $\chi\chi'(g) = \chi(g)\chi'(g)$.

[1] The type of character defined in this definition is also known as Abelian character or one-dimensional representation of G in $\mathbb{C}$.

B. Luong, *Fourier Analysis on Finite Abelian Groups*, Applied and
Numerical Harmonic Analysis, DOI 10.1007/978-0-8176-4916-6_3,

Theorem 3.1.1. *The characters of an arbitrary group G form an Abelian group with respect to the pointwise product.*

Proof. Suppose that χ, χ', and χ'' are characters of G. We must verify the following five properties that define an Abelian group:

(i) the pointwise product $\chi\chi'$ is a character of G (closure);
(ii) $\chi\chi' = \chi'\chi$ (commutative);
(iii) $(\chi\chi')\chi'' = \chi(\chi'\chi'')$ (associative);
(iv) $\chi\chi_{T} = \chi$ (existence of the identity);
(v) for each χ, there is a character χ^{-1} (necessarily unique) such that $\chi\chi^{-1} = \chi_{T}$ (existence of the inverse).

Statements (i)–(iv) are trivial. To prove (v) let $\chi^{-1}\colon G \to \mathbb{C}^*$ be the function defined, for each $g \in G$, by

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

It is easy to check that χ^{-1} is a character of G and $\chi\chi^{-1} = \chi_{T}$. ∎

The group of characters of G is denoted by $\hat{G}$ and is called the *character group* or the *dual group* of G.

Suppose that $h\colon G_1 \to G_2$ is a homomorphism of groups and χ is a character of G_2. The *pullback* of χ by h, denoted $h^\star\chi$, is defined by $h^\star\chi = \chi \circ h$, the composition of χ and h. Since the composition of two homomorphisms is again a homomorphism, it follows that the pullback of a character of G_2 is a character of G_1. Consequently, there is a one-to-one correspondence between the groups of characters of any two isomorphic groups. In fact, we can say more.

Theorem 3.1.2. *Isomorphic groups have isomorphic character groups. That is, if G_1 and G_2 are groups and $G_1 \cong G_2$, then $\hat{G}_1 \cong \hat{G}_2$.*

Proof. Suppose that $h\colon G_1 \to G_2$ is an isomorphism and χ_2 is a character of G_2. Consider the diagram

$$\begin{tikzcd} G_1 \arrow[r, "h"] \arrow[dr, "\chi_1"'] & G_2 \arrow[d, "\chi_2"] \\ & \mathbb{C}^* \end{tikzcd}$$

Note that the pullback $\chi_2 \circ h$ of χ_2 is a character of G_1. Conversely, every character χ_1 of G_1 is a pullback of some character χ_2 of G_2 (simply set $\chi_2 = \chi_1 \circ h^{-1}$). Thus the function $h^\star \colon \hat{G}_2 \to \hat{G}_1$ is surjective. Now we show that $h^\star$ is an isomorphism in steps (a) and (b) as follows:

(a) Homomorphism: If χ_2, $\chi_2' \in \hat{G}_2$, then, by the pointwise definition,

$$h^\star(\chi_2\chi_2') = (h^\star\chi_2)(h^\star\chi_2').$$

(b) Kernel($h^\star$)={identity}: For $j = 1, 2$, let χ_{T_j} be the trivial character of G_j. If $h^\star\chi_2 = \chi_{T_1}$, then $\chi_2 \circ h(g_1) = 1$ for every $g_1 \in G_1$. The bijectivity of h forces $\chi_2 = \chi_{T_2}$. ■

Next we define the tensor product of characters and show that a character of a direct product of groups is the tensor product of characters of its summands. Suppose that G_1 and G_2 are groups and χ_1 and χ_2 are characters of G_1 and G_2, respectively. The *tensor product* of χ_1 and χ_2 is the function $\chi_1 \otimes \chi_2 \colon G_1 \times G_2 \to \mathbb{C}^*$ defined by

$$\chi_1 \otimes \chi_2(g_1, g_2) = \chi_1(g_1)\chi_2(g_2). \tag{3.1}$$

There are two immediate consequences of this definition:

(i) The tensor product is not commutative. In general, $\chi_1 \otimes \chi_2$ and $\chi_2 \otimes \chi_1$ have different domains.

(ii) It follows from the definition of the binary operation of the group $G_1 \times G_2$, the definition of $\chi_1 \otimes \chi_2$, and the commutativity of the product of complex numbers that the tensor product $\chi_1 \otimes \chi_2$ is a character of $G_1 \times G_2$. Furthermore, every character of $G_1 \times G_2$ is of the form $\chi_1 \otimes \chi_2$; the truth of this is guaranteed by the next theorem.

Theorem 3.1.3. *Suppose that G_1 and G_2 are groups. Then χ is a character of $G_1 \times G_2$ if and only if $\chi = \chi_1 \otimes \chi_2$, for some $\chi_1 \in \hat{G}_1$ and $\chi_2 \in \hat{G}_2$.*

Proof. It remains to show that if χ is a character of $G_1 \times G_2$, then there are characters χ_1 of G_1 and χ_2 of G_2 such that $\chi = \chi_1 \otimes \chi_2$. Since the injection $\imath_1 \colon G_1 \hookrightarrow G_1 \times G_2$ given by $\imath_1(g_1) =$

$(g_1, 1)$ is a homomorphism, the pullback of χ by $\imath_1$ is a character of G_1. Similarly, the pullback of χ by $\imath_2$ is a character of G_2. It is straightforward to check that if $\chi_1 = \imath_1^\star \chi$ and $\chi_2 = \imath_2^\star \chi$, then $\chi = \chi_1 \otimes \chi_2$. ■

A consequence of Theorem 3.1.3 is that the dual of a direct product is the tensor product of the duals. In the following corollary, $\hat{G}_1 \otimes \hat{G}_2 = \{\chi_1 \otimes \chi_2 \mid \chi_1 \in \hat{G}_1 \text{ and } \chi_2 \in \hat{G}_2\}$.

Corollary 3.1.1. *If G_1 and G_2 are groups, then*

$$\widehat{G_1 \times G_2} = \hat{G}_1 \otimes \hat{G}_2.$$

It is clear that the complex conjugate of a character is also a character. It turned out that, for finite groups, the complex conjugate of a character is exactly its inverse, as we shall see shortly.

Suppose that χ is a character of G and g is an element of G having finite order k. Since $\chi(g)^k = \chi(g^k) = \chi(1) = 1$, it follows that characters send elements of finite order to roots of unity. In particular, *if G is a group and n is the smallest positive integer such that $g^n = 1$ for every $g \in G$, then elements of G are mapped to nth roots of unity by characters.* In this case, the codomain $\mathbb{C}^*$ in the definition of characters can be replaced by the set $U_n = \{\xi_n^k \mid \xi_n = e^{2\pi i/n},\ 0 \leq k < n\}$ consisting of all nth roots of unity, which is a cyclic subgroup of $\mathbb{C}^*$ having ξ_n as a generator.[2] Therefore, if $\chi \in \hat{G}$, then $|\chi(g)| = 1$ for all $g \in G$. Hence

$$\bar{\chi}(g) = \overline{\chi(g)} = \frac{1}{\chi(g)} = \chi(g^{-1}) = \chi^{-1}(g),$$

which gives

$$\bar{\chi} = \chi^{-1}. \tag{3.2}$$

We emphasize that equation (3.2) is a consequence of the existence of a positive integer n such that $g^n = 1$ for every $g \in G$; the

[2] Though it is not needed in our work, we point out the fact that other generators of U_n have the form ξ_n^k where k is relatively prime to n. There are $\varphi(n)$ of such. Here φ is the Euler phi function; $\varphi(n)$ is the number of positive integers less than n that are relatively prime to n and $\varphi(1) = 1$. Note that if $n > 1$, then $0 < \varphi(n) < n$.

smallest of such integers is known as the *exponent* of G. This is the case if G is a finite group.

Since Theorem 1.1.3, Theorem 3.1.2, and Corollary 3.1.1 reduce the study of characters of finite Abelian groups to the study of characters of cyclic groups of finite order, we concentrate our investigation on characters of groups of the latter type in the remainder of this section.

The characters of U_n are easy to find. Suppose that g is a generator of U_n and $h\colon U_n \to U_n$ is a homomorphism. If $h(g)$ is known, then, since $h(g^k) = h(g)^k$, $h(g^k)$ is determined, so $h(u)$ is determined for all $u \in U_n$. Thus a choice for $h(g)$ determines h uniquely. Since the group U_n has n elements, there are n choices for $h(g)$. Therefore, the character group $\hat{U}_n$ has n elements, i.e., $|\hat{U}_n| = n$. Also, since the identity function on U_n is an element of $\hat{U}_n$ of order n, the dual group $\hat{U}_n$ is cyclic. Thus the groups U_n and its dual, $\hat{U}_n$, are both cyclic and have n elements. By Theorems 1.1.2 and 3.1.2, we can summarize this result as follows.

Theorem 3.1.4. *If n is a positive integer, then $\mathbb{Z}_n \cong \hat{\mathbb{Z}}_n$.*

Corollary 3.1.2. *If G is a finite Abelian group, then $G \cong \hat{G}$.*

Proof. Corollary 3.1.2 follows from Theorem 1.1.3, Theorem 3.1.2, Corollary 3.1.1, and Theorem 3.1.4 (in that order). ■

Example 3.1.1. Using additive notation for the binary operation on $\mathbb{Z}_n$, a character of $\mathbb{Z}_n$ is a function $\chi\colon \mathbb{Z}_n \to U_n$ such that

$$\chi(a+b) = \chi(a)\chi(b)$$

for all a, $b \in \mathbb{Z}_n$. Since addition modulo n is a binary operation on $\mathbb{Z}_n$, the sum $a+b$ in the previous equation implicitly means $(a+b)(\bmod n)$. For each $a \in \mathbb{Z}_n$, let $\chi_a\colon \mathbb{Z}_n \to U_n$ be the function defined by

$$\chi_a(b) = \xi_n^{ab}. \tag{3.3}$$

Then for b_1, $b_2 \in \mathbb{Z}_n$ we have

$$\chi_a(b_1+b_2) = \xi_n^{a(b_1+b_2)} = \xi_n^{ab_1}\xi_n^{ab_2} = \chi_a(b_1)\chi_a(b_2).$$

Thus χ_a is a character of $\mathbb{Z}_n$.

Moreover, $\chi_a = \chi_b$ if and only if $a = b$. The truth of this statement can be seen as follows: since it is obvious that if $a = b$, then $\chi_a = \chi_b$, we need only to show that if $\chi_a = \chi_b$, then $a = b$. The equality $\chi_a = \chi_b$ implies that $\chi_a(1) = \chi_b(1)$ or $\xi_n^a = \xi_n^b$, it follows that $a = b \pmod n$. Since $0 \le a,\, b < n$ we have $a = b$.

We have exhibited n characters of $\mathbb{Z}_n$, namely, $\chi_0, \ldots, \chi_{n-1}$. These are all the characters of $\mathbb{Z}_n$, since $|\hat{\mathbb{Z}}_n| = n$. Note that characters of $\mathbb{Z}_n$ are symmetric in the sense that $\chi_a(b) = \chi_b(a)$.

Example 3.1.2. Let χ be a character of the group $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}$. By Theorem 3.1.3, there is a point $x = (x_1, \ldots, x_m) \in G$ such that

$$\chi = \chi_{x_1} \otimes \cdots \otimes \chi_{x_m} \overset{\text{def}}{=} \chi_x,$$

where χ_{x_j} is a character of $\mathbb{Z}_{n_j}$. By definition of the tensor product for characters we have

$$\chi_x(y) = \chi_{x_1}(y_1) \ldots \chi_{x_m}(y_m) = e^{2\pi i\left(\frac{x_1 y_1}{n_1} + \cdots + \frac{x_m y_m}{n_m}\right)} \tag{3.4}$$

for any $y \in G$. Note that the second equality follows from (3.3). It follows that

$$\chi_x(y) = \chi_y(x) \quad \text{and} \quad \bar{\chi}_x(y) = \chi_x(-y) = \chi_{-x}(y), \tag{3.5}$$

where $-y$ is the inverse of y in G.

In particular, if $n_j = n$ for every j, then $\chi_x(y) = e^{\frac{2\pi i}{n} x\cdot y}$, where $x\cdot y = x_1 y_1 + \cdots + x_m y_m$.

Example 3.1.3. A special case of the previous example is the case $n = 2$. Since $\xi_2 = e^{2\pi i/2} = -1$, the characters of $\mathbb{Z}_2^m$ are χ_x as x ranges over $\mathbb{Z}_2^m$ and, for each $x \in \mathbb{Z}_2^m$,

$$\chi_x(y) = (-1)^{x\cdot y}$$

for every $y \in \mathbb{Z}_2^m$.

Exercises.

9. Let G_1 and G_2 be groups. Prove that the tensor product of characters has the following properties: for $\chi_1, \chi_1' \in \hat{G}_1$ and $\chi_2, \chi_2' \in \hat{G}_2$,

$$(\chi_1 \otimes \chi_2)(\chi_1' \otimes \chi_2') = \chi_1\chi_1' \otimes \chi_2\chi_2',$$
$$(\chi_1 \otimes \chi_2)^{-1} = \chi_1^{-1} \otimes \chi_2^{-1}.$$

10. For a nonempty subset S of a finite Abelian group G, let $\hat{G}_S$ be the set of characters of G whose kernels contain S, that is, elements of $\hat{G}$ that map every $s \in S$ to 1. Prove that $\hat{G}_S$ is a subgroup of $\hat{G}$. The group $\hat{G}_S$ is called the *annihilator* of S. Suppose that H and K are subgroups of G, prove the following:

(i) if $H \subset K$, then $\hat{G}_H \supset \hat{G}_K$;
(ii) $\hat{G}_{HK} = \hat{G}_H \cap \hat{G}_K$, where $HK = \{hk \mid h \in H,\, k \in K\}$;
(iii) $\hat{G}_{H\cap K} = \hat{G}_H\hat{G}_K$;
(iv) the map $H \mapsto \hat{G}_H$ is a bijection between subgroups of G and $\hat{G}$;
(v) every character of G restricted to H is a character of H;
(vi) if $R\colon \hat{G} \to \hat{H}$ is the restriction map defined by $R(\chi) = \chi_{|H}$, where $\chi_{|H}$ is the restriction of χ to H, prove that

(a) R is a homomorphism;
(b) the kernel of R is $\hat{G}_H$;
(c) R is surjective.

Conclude that

$$\hat{H} \cong \frac{\hat{G}}{\hat{G}_H}, \quad \hat{G} \cong \hat{H} \otimes \hat{G}_H, \quad \text{and} \quad \hat{G}_H \cong \hat{Q},$$

where $Q = \frac{G}{H}$ is the quotient group of G by H. Note that $\hat{H}$ is not a subgroup of $\hat{G}$.

(vii) If $h \in G$ and $h \neq 1$, then there is a character $\chi \in \hat{G}$ such that $\chi(h) \neq 1$. Equivalently, if a, $b \in G$ and $a \neq b$, there is a character $\chi \in \hat{G}$ such that $\chi(a) \neq \chi(b)$.

11. Let G_1, G_2, G_3 be finite Abelian groups. The sequence $1 \to G_1 \to G_2 \to G_3 \to 1$ is said to be an *exact sequence* if there are homomorphisms α and β, where

$$G_1 \xrightarrow{\alpha} G_2 \xrightarrow{\beta} G_2,$$

such that α is one-to-one, β is onto, and the kernel of β is identical to the range of α. Prove that the exact sequence $1 \to G_1 \to G_2 \to G_3 \to 1$ induces an exact sequence $1 \to \hat{G}_1 \to \hat{G}_2 \to \hat{G}_3 \to 1$.

12. Let G be a finite Abelian group. The *double dual* of G is defined to be the dual of the dual of G; a natural notation for the double dual of G is $\hat{\hat{G}}$. By Corollary 3.1.2, we have $G \cong \hat{\hat{G}}$. This isomorphism depends on the isomorphism given by the fundamental theorem of finite Abelian groups. Alternatively, we can define an isomorphism from G to $\hat{\hat{G}}$ that is independent of the fundamental theorem of finite Abelian groups: let $\kappa\colon G \to \hat{\hat{G}}$ be the map defined by $g \mapsto \kappa_g$, where κ_g is a character of $\hat{G}$ given by $\kappa_g(\chi) = \chi(g)$ for every $\chi \in \hat{G}$. Show that the map κ is well-defined and is an isomorphism. The isomorphism κ is called the *natural isomorphism* between G and $\hat{\hat{G}}$.

3.2 The Orthogonal Relations for Characters

The notion of orthogonality of characters of finite Abelian groups is indispensable in the development of the FT. Most importantly it implies that the characters of a finite Abelian group form an orthogonal basis for the vector space of complex-valued functions defined on the group. Based on this basis we define the FT.

Let G be a finite Abelian group and let H be a subgroup G. We recall from Exercise 10 of the last section that $\hat{G}_H$ is the subgroup of $\hat{G}$ formed by characters of G which are identically 1 on H.

Theorem 3.2.1. *If H is a subgroup of G and $\chi \in \hat{G}$, then*

$$\sum_{h \in H} \chi(h) = \begin{cases} |H| & \text{if } \chi \in \hat{G}_H, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Let A be the sum in the statement of the theorem. If $\chi \in \hat{G}_H$, then $\chi(h) = 1$ for every $h \in H$, so $A = |H|$. On the other hand, if $\chi \notin \hat{G}_H$, then there exists $h_0 \in H$ such that $\chi(h_0) \neq 1$. By Theorem 1.1 we have

$$A = \sum_{h \in H} \chi(h_0 h) = \chi(h_0) \sum_{h \in H} \chi(h) = \chi(h_0) A,$$

whence $A = 0$. ■

In what follows it is convenient to enumerate the elements of G as $g_1, \ldots, g_\eta$, i.e., we consider $G = \{g_1, \ldots, g_\eta\}$. Since, by Corollary 3.1.2, G and $\hat{G}$ have the same number of elements, G can serve as an index set for $\hat{G}$. There are many different ways to enumerate (or to index the elements of) $\hat{G}$. For our purpose it suffices to choose an enumeration of $\hat{G}$ such that χ_{g_1} is the trivial character of G. For simplicity we write s for g_s; that is, we identify elements of G with their subscripts. Let $X = (\chi_s(t))$ be the matrix whose (s, t) entry is the complex number $\chi_s(t)$. It follows from Corollary 3.1.2 that X is a square matrix of dimension η. Further, if $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}$, then (3.4) implies that the characters of G are symmetric (i.e., $\chi_s(t) = \chi_t(s)$), whence X is a symmetric matrix.

Example 3.2.1. If $G = \mathbb{Z}_n$ then

$$X = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \xi_n & \xi_n^2 & \ldots & \xi_n^{n-1} \\ 1 & \xi_n^2 & \xi_n^4 & \ldots & \xi_n^{2(n-1)} \\ \vdots & & & & \vdots \\ 1 & \xi_n^{n-1} & \xi_n^{2(n-1)} & \ldots & \xi_n^{(n-1)(n-1)} \end{pmatrix}_{n \times n},$$

where $\xi_n = e^{2\pi i/n}$. Note that since ξ_n is an nth root of unity, some entries of X may be simplified, e.g., $\xi_n^{(n-1)(n-1)} = \xi_n$.

Corollary 3.2.1. *The sum of the entries in the first row of X is η and the sum of the entries in each of the remaining rows is zero. That is,*

$$\sum_{t=1}^{\eta} \chi_s(t) = \begin{cases} \eta & \text{if } s = 1, \\ 0 & \text{if } s \neq 1. \end{cases}$$

Proof. Set $H = G$ in Theorem 3.2.1. ■

Example 3.2.2. Suppose that $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}$. Then (3.4) and Corollary 3.2.1 imply that the formula

$$\sum_{y \in G} \chi_x(y) = \sum_{y \in G} e^{2\pi i \left(\frac{x_1 y_1}{n_1} + \cdots + \frac{x_m y_m}{n_m} \right)} = \begin{cases} n_1 \cdots n_m & \text{if } x = 0, \\ 0 & \text{if } x \neq 0, \end{cases}$$

holds for any $x = (x_1, \ldots, x_m) \in G$. It follows that if $n_j = n$ for every j, then we have

$$\sum_{y \in \mathbb{Z}_n^m} e^{\frac{2\pi i}{n} x \cdot y} = \begin{cases} n^m & \text{if } x = 0, \\ 0 & \text{if } x \neq 0, \end{cases}$$

for every $x \in \mathbb{Z}_n^m$. In particular, for $n = 2$, since $e^{\pi i} = -1$, the formula

$$\sum_{y \in \mathbb{Z}_2^m} (-1)^{x \cdot y} = \begin{cases} 2^m & \text{if } x = 0, \\ 0 & \text{if } x \neq 0, \end{cases}$$

holds for $x \in \mathbb{Z}_2^m$.

If we denote the adjoint (i.e., conjugate transpose) of X by X^*, then the following corollary states that the inverse of $\left(1/\sqrt{\eta}\right)X$ is $\left(1/\sqrt{\eta}\right)X^*$.

Corollary 3.2.2. *The matrix $\left(1/\sqrt{\eta}\right)X$ is a unitary matrix; that is, $XX^* = \eta I$, where I is the $\eta \times \eta$ identity matrix.*

Proof. Let $M = (m_{st}) = XX^*$. By the definition of matrix multiplication, the definition of the product of characters, the fact that the pointwise product of two characters is again a character, and the previous theorem we have

$$m_{st} = \sum_{k=1}^{\eta} \chi_s(k)\bar{\chi}_t(k) = \sum_{k=1}^{\eta} (\chi_s \bar{\chi}_t)(k) = \begin{cases} \eta & \text{if } \chi_s \bar{\chi}_t = \chi_1, \\ 0 & \text{if } \chi_s \bar{\chi}_t \neq \chi_1. \end{cases}$$

Recall from (3.2) that $\bar{\chi}_t = \chi_t^{-1}$ and since each character has a unique inverse, we have $\chi_s \bar{\chi}_t = \chi_1$ if and only if $s = t$. ■

Since X is a constant (i.e., $\sqrt{\eta}$) multiple of a unitary matrix of complex numbers, the rows (and columns) of X are orthogonal with respect to the standard inner product in $\mathbb{C}^\eta$. Also, the length of each row and column of X is η. These results are the contents of the next corollary.

Corollary 3.2.3 (Orthogonal relations).

(i) *The rows of X, considered as vectors in $\mathbb{C}^\eta$, are orthogonal and each has length η. That is, if χ_s and χ_t are characters of G, then*

$$\sum_{k=1}^{\eta} \chi_s(k)\bar{\chi}_t(k) = \begin{cases} \eta & \textit{if } s = t, \\ 0 & \textit{if } s \neq t. \end{cases}$$

(ii) *The columns of X, considered as vectors in $\mathbb{C}^\eta$, are orthogonal and each has length η. That is, if χ_k is a character of G, then*

$$\sum_{k=1}^{\eta} \bar{\chi}_k(s)\chi_k(t) = \begin{cases} \eta & \textit{if } s = t, \\ 0 & \textit{if } s \neq t. \end{cases}$$

Corollary 3.2.4 (Row and column sums of X).

(i) *The sum of the entries in the ℓth row of X is*

$$\sum_{k=1}^{\eta} \chi_\ell(k) = \begin{cases} \eta & \textit{if } \ell = 1 \ (\textit{the identity of } G), \\ 0 & \textit{if } \ell \neq 1. \end{cases}$$

(ii) *The sum of the entries in the ℓth column of X is*

$$\sum_{k=1}^{\eta} \chi_k(\ell) = \begin{cases} \eta & \textit{if } \ell = 1, \\ 0 & \textit{if } \ell \neq 1. \end{cases}$$

Proof. Set $s = 1$ in the previous corollary. ■

It follows from (i) of Corollary 3.2.3 that the set

$$B_G = \frac{1}{\sqrt{|G|}}\hat{G} = \left\{ \frac{1}{\sqrt{|G|}}\chi \;\middle|\; \chi \in \hat{G} \right\} \tag{3.6}$$

is an orthonormal subset of the complex inner product space V_G associated with G. Since $|B_G| = \dim V_G$, B_G is an orthonormal basis for V_G. We record this fact in the following theorem.

Theorem 3.2.2. *The set B_G is an orthonormal basis of V_G.*

In the remainder of this section, we set some notation for the rest of the exposition, point out the nearly homomorphism property of functions in the basis B_G, and list two properties of the function δ_g.

1) Since $|G| = |B_G|$, the group G can serve as an index set for B_G. In general, we write $\hat{G} = \{\chi_g \mid g \in G\}$ and

$$B_G = \{\, B_g \mid g \in G, \text{ where } B_g = (1/\sqrt{|G|})\, \chi_g \,\}.$$

In this notation, every $f \in V_G$ can be expressed uniquely as

$$f = \sum_{g \in G} \langle f, B_g \rangle B_g. \tag{3.7}$$

2) Because of the scalar multiplication, functions in B_G are not homomorphisms and hence they are not characters. Nevertheless, we call B_G the *character basis* for V_G. Though not homomorphisms, functions in B_G are "homomorphisms up to the factor $\sqrt{|G|}$"; i.e., for any $B_g \in B_G$, we have

$$B_g(xy) = \sqrt{|G|}\, B_g(x) B_g(y)$$

for all x, $y \in G$. This property of functions in B_G will be used freely.

3) Suppose that $h\colon G_1 \to G_2$ is an isomorphism of finite Abelian groups. Then h induces the isomorphism $h^\star\colon \hat{G}_2 \to \hat{G}_1$, which was defined in the proof of Theorem 3.1.2 as the pullback by h. For $x \in G_2$ and $\chi_x \in \hat{G}_2$, we denote the pullback of χ_x with respect to h by $\chi_{h^{-1}(x)}$, i.e.,

$$h^\star \chi_x = \chi_{h^{-1}(x)}. \tag{3.8}$$

The isomorphism $h^\star$ will play an important role in later development (in Sections 6.3 and 6.4).

4) For any g in G, the function δ_g satisfies the following property: if $f\colon G \to \mathbb{C}$ and S is a nonempty subset of G, then

$$\sum_{x \in S} \delta_g f(x) = \begin{cases} f(g) & \text{if } g \in S, \\ 0 & \text{if } g \notin S, \end{cases}$$

where $\delta_g f$ is the pointwise product of two functions. Thus, we can think of δ_g as *the discrete Dirac delta function supported at g.*

For those who wish to pursue further into character theory we recommend [8].

Exercises.

13. Prove that

$$\sum_{g \in G} \chi_g = |G|\delta_1,$$

where 1 is the identity of G.

14. If $\chi \in \hat{G}$ and $n = |G|$, then on $G \setminus \ker(\chi)$ we have

$$\sum_{k=0}^{n-1} \chi^k = 0.$$

15. For $x = (x_1, \ldots, x_m) \in G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}$, prove that $\delta_x = \delta_{x_1} \otimes \cdots \otimes \delta_{x_m}$.

16. Let n be an integer greater than 2. Prove that if f_1 and f_2 are elements of V_G, then

$$\langle f_1, f_2 \rangle = \frac{1}{n} \sum_{k=0}^{n-1} \|f_1 + \xi_n^k f_2\|^2 \xi_n^k, \tag{3.9}$$

where we recall that $\xi_n = e^{2\pi i/n}$. Equation (3.9) is known as the *polarization identity.*

17. Let $f : S \to G$ be a map from a nonempty finite set S into a finite Abelian group G. For any fixed $g \in G$, the number of points in S which are mapped to g by f, i.e., $|f^{-1}(g)|$, can be expressed by the equation

$$|f^{-1}(g)| = \frac{1}{|G|} \sum_{s \in S} \sum_{\chi \in \hat{G}} \bar{\chi}(f(s))\chi(g).$$

18. Fix a nonzero vector

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{C}^n.$$

Define the *rotation* of x to be the vector

$$\mathrm{rot}(x) = \begin{pmatrix} x_n \\ x_1 \\ \vdots \\ x_{n-1} \end{pmatrix}.$$

The matrix $M_x = [x, \mathrm{rot}(x), \mathrm{rot}^2(x), \ldots, \mathrm{rot}^{n-1}(x)]$, whose jth column is the $(j-1)$th rotation of x, is called the *circulant* matrix generated by x. For example, the circulant matrix generated by a nonzero vector

$$x = \begin{pmatrix} a \\ b \\ c \end{pmatrix} \in \mathbb{C}^3$$

is

$$M_x = \begin{pmatrix} a & c & b \\ b & a & c \\ c & b & a \end{pmatrix}_{3\times 3}.$$

A complex number λ is called an *eigenvalue* of M_x if there is a nonzero vector y such that $M_x y = \lambda y$. Such a vector y is called an *eigenvector* of M_x corresponding to the eigenvalue λ.

(i) Set $p_x(z) = x_n + x_{n-1}z + x_{n-2}z^2 + \cdots + x_1 z^{n-1}$, i.e., $p_x(z)$ is the polynomial in a single variable z whose coefficients are the coordinates of x. For $j = 1, \ldots, n$, show that the jth column of the matrix X in Example 3.2.1 on page 41 is an eigenvector of M_x corresponding to the eigenvalue $\xi_n^{j-1} p_x(\xi_n^{j-1})$.

(ii) Conclude that

$$\det M_x = \prod_{j=1}^{n} \left(\xi_n^{j-1} p_x(\xi_n^{j-1})\right) = \xi_n^{\frac{n(n-1)}{2}} \prod_{j=1}^{n} p_x(\xi_n^{j-1}).$$

(iii) Suppose that n is prime, $p_x(1) \neq 0$, and not all coordinates of x are equal (i.e., $x_s \neq x_t$ for some s and t). Show that $\det M_x \neq 0$.

We will see later in Exercise 26 (page 62) that the FT diagonalizes M_x for all nonzero vectors $x \in \mathbb{C}^n$.

4

The Fourier Transform

As alluded to at the beginning of Chapter 2, the FT on a finite Abelian group G is a linear operator on V_G. A more specific description was given at the end of Section 2.3: the FT on G is an operator of the type described in Theorem 2.3.1 with $S = G$. In the following chapter, we formally define the FT and describe some of its properties in the first section.

4.1 Definition and Some Properties

Suppose that G is a finite Abelian group, V_G is the inner product space associated with G, $\Delta_G = \{\delta_g \,|\, g \in G\}$ and $B_G = \{B_g \,|\, g \in G\}$ are standard and character bases for V_G, respectively. By (3.7), each B_g can be written uniquely as

$$B_g = \sum_{s \in G} \langle B_g, B_s \rangle B_s = \sum_{s \in G} \delta_g(s) B_s.$$

It follows from the uniqueness that the one-to-one correspondence $B_g \leftrightarrow \delta_g$ is independent of the enumeration of vectors in the basis B_G. Through this correspondent we define the FT.

Definition 4.1.1. *The Fourier transform on the group G is the linear operator on the associated complex inner product space V_G which maps B_g to δ_g for every $g \in G$.*

The FT is denoted by either $\mathcal{F}$ or $\hat{}$; i.e., if $f \in V_G$, we denote the FT of f by either $\mathcal{F}f$ or $\hat{f}$. We will use the two notations

B. Luong, *Fourier Analysis on Finite Abelian Groups*, Applied and Numerical Harmonic Analysis, DOI 10.1007/978-0-8176-4916-6_4,

interchangeably. By Theorem 2.3.1, we can express the FT in terms of elements in the bases Δ_G and B_G as

$$\mathcal{F} = \sum_{s,\, t \in G} \langle \delta_t, B_s \rangle \delta_s \delta_t^*. \tag{4.1}$$

The following properties hold: Let f, f_1, and f_2 be complex-valued functions defined on G.

(i) The FT is an isometry, i.e., $\langle f_1, f_2 \rangle = \langle \hat{f}_1, \hat{f}_2 \rangle$. (This is known as the *Plancherel theorem.*) In particular, $\|f\| = \|\hat{f}\|$.
(ii) $\hat{f}$ is the complex-valued function defined on G whose value at g is the g-coefficient of f in the basis B_G, that is, $\hat{f}(g) = \langle f, B_g \rangle$.

Equation (4.1) is the general expression for the FT operator in terms of the bases Δ_G, B_G, and their duals. In practice, to find the FT of a function f, we often use the linearity of the FT, the equation $\hat{B}_g = \delta_g$, and property (ii) listed above. For instance, if $f \in V_G$, applying the FT on both sides of equation (3.7) we obtain

$$\hat{f} = \sum_{g \in G} \langle f, B_g \rangle \delta_g. \tag{4.2}$$

Example 4.1.1. Suppose that $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}$ and f is a complex-valued function defined on G. Then, by (ii), the value of $\hat{f}$ at a point x in G is given by

$$\hat{f}(x) = \langle f, B_x \rangle = \frac{1}{\sqrt{|G|}} \langle f, \chi_x \rangle = \frac{1}{\sqrt{|G|}} \sum_{y \in G} f(y) \bar{\chi}_x(y).$$

From (3.4) and the fact that $|G| = n_1 \ldots n_m$, we have

$$\hat{f}(x) = \frac{1}{\sqrt{n_1 \ldots n_m}} \sum_{y \in G} e^{-2\pi i \left(\frac{x_1 y_1}{n_1} + \cdots + \frac{x_m y_m}{n_m} \right)} f(y). \tag{4.3}$$

In particular, if $n_j = n$ for every j, then

$$\hat{f}(x) = \frac{1}{\sqrt{n^m}} \sum_{y \in \mathbb{Z}_n^m} e^{-\frac{2\pi i}{n} x \cdot y} f(y). \tag{4.4}$$

It follows that if $m = n = 1$, then $\hat{f} = f$ for all $f \in V_{\mathbb{Z}_1}$, i.e., the FT is the identity operator on $V_{\mathbb{Z}_1}$. Since there is nothing interesting about the identity operator, *hereafter, when the group $\mathbb{Z}_n$ is under consideration, we assume that $n \geq 2$.*

Example 4.1.2. Set $n = 2$ in (4.4). Since $e^{\pi i} = -1$, we have

$$\hat{f}(x) = \frac{1}{\sqrt{2^m}} \sum_{y \in \mathbb{Z}_2^m} (-1)^{x \cdot y} f(y)$$

for all $x \in \mathbb{Z}_2^m$.

There are three immediate consequences of equation (4.3):

1) For $a \in G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}$, the *translation* by a is the operator τ_a on V_G defined by $f \mapsto \tau_a f$, where $\tau_a f(x) = f(x+a)$. It follows from this definition that the translation by a is linear and it is straightforward to show that

$$\widehat{\tau_a f} = \chi_a \hat{f} \quad \text{and} \quad \widehat{\chi_a f} = \tau_{-a} \hat{f}, \tag{4.5}$$

where $\chi_a f$ is the pointwise product of χ_a and f. The values of the functions $\widehat{\tau_a f}$ and $\widehat{\chi_a f}$ at a point $x \in G$ are given by

$$\widehat{\tau_a f}\,(x) = e^{2\pi i \sum_{j=1}^{m} (a_j x_j / n_j)} \hat{f}(x) \quad \text{and} \quad \widehat{\chi_a f}(x) = \hat{f}(x - a).$$

For the special case $n_1 = \cdots = n_m = 2$, we have

$$\widehat{\tau_a f}\,(x) = (-1)^{a \cdot x} \hat{f}(x)$$

for every $x \in \mathbb{Z}_2^m$, where $a \in \mathbb{Z}_2^m$.

2) Suppose that $u \in \mathbb{Z}_n$ is a unit. The *dilation* by u is the operator d_u on $V_{\mathbb{Z}_n}$ defined by $f \mapsto d_u f$, where $d_u f(x) = f(ux)$. It is straightforward to show that dilation by u is linear and that

$$\widehat{d_u f} = d_{u^{-1}} \hat{f}. \tag{4.6}$$

Since the only unit in $\mathbb{Z}_2$ is the multiplicative identity, there is no dilation on $V_{\mathbb{Z}_2}$ other than the identity operator.

3) The equation $\hat{\bar{f}}(x) = \bar{\hat{f}}(-x)$ holds for every complex-valued function f defined on $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}$, where $x \in G$ and $-x$ is the inverse of x in G.

The following theorem, which characterizes nonzero constant functions in terms of the FT, follows directly from the definition of the FT. First, some terminology: the *support* of a function f defined on G is the set

$$\operatorname{supp}(f) = \{g \in G \mid f(g) \neq 0\}.$$

Theorem 4.1.1. *Suppose that G is a finite Abelian group and f is a complex-valued function defined on G. A necessary and sufficient condition that f is a nonzero constant is that $\hat{f}$ is supported only at the identity. Furthermore, if c is a constant (zero or nonzero), then*

$$\hat{c} = c\sqrt{|G|}\,\delta_1.$$

Proof. By the linearity of the FT and the fact that $B_1 = 1/\sqrt{|G|}$, for any constant c, we have

$$\hat{c} = c\hat{1} = c\sqrt{|G|}\frac{\hat{1}}{\sqrt{|G|}} = c\sqrt{|G|}\hat{B}_1 = c\sqrt{|G|}\,\delta_1.$$

So, the FT of a nonzero constant function is supported only at 1.

Conversely, if $\operatorname{supp}(\hat{f}) = \{1\}$, then $\hat{f} = c\sqrt{|G|}\,\delta_1$ for some nonzero constant c. By taking the inverse FT, we have

$$f = c\sqrt{|G|}B_1 = c. \qquad \blacksquare$$

It follows from Theorem 4.1.1 that the FT of the uniform distribution on G, given by $p(g) = 1/|G|$, is concentrated at the identity with weight $1/\sqrt{|G|}$.

The characters of the group $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}$ have some special properties, namely, properties (3.5). Using these properties we can derive a simple formula for the second FT of a function defined on G in terms of itself.

Theorem 4.1.2. *If f is a complex-valued function defined on $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}$, then*

$$\hat{\hat{f}}(x) = f(-x)$$

for every $x \in G$, where $-x$ is the inverse of x in G.

Proof. By the linearity property of the FT, it suffices to prove the theorem only for members of the basis B_G. For $x \in G$, we have

$$\hat{\hat{B}}_g(x) = \langle \hat{B}_g, B_x \rangle = \langle \delta_g, B_x \rangle = \bar{B}_x(g).$$

Since, by (3.5), $\bar{B}_x(g) = B_g(-x)$, we have $\hat{\hat{B}}_g(x) = B_g(-x)$. ■

Theorem 4.1.2, the definition of the FT, and (3.5) imply the following corollary.

Corollary 4.1.1. *For every x in $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}$, we have $\hat{\delta}_x = \bar{B}_x = B_{-x}$, where $-x$ is the inverse of x in G.*

There are algorithms for computing the FT on $\mathbb{Z}_n$,[1] many of which are relatively fast and they are known collectively as the FFT (fast Fourier transform). There are many books on the FFT, in particular, we refer the readers to [20].

Exercises.

19. Prove the formulas in (4.5) and (4.6).

20. Let f be a complex-valued function defined on G. Prove the following:

(i) $\hat{f}$ is identically zero if and only if f is identically zero.

(ii) The formula

$$\hat{f}(1) = \frac{1}{\sqrt{|G|}} \sum_{g \in G} f(g)$$

holds.

[1] We will see later that, by Theorem 6.4.1, the FT on any finite Abelian group is determined by the FT on $\mathbb{Z}_n$.

21. Let n be an integer greater than 2. Prove that if f_1 and f_2 are elements of V_G, then

$$\langle \hat{f}_1, f_2 \rangle = \frac{1}{n} \sum_{k=0}^{n-1} \left\langle (f_1 + \xi_n^k f_2)\hat{}, (f_1 + f_2) \right\rangle \xi_n^k,$$

where we recall that $\xi_n = e^{2\pi i/n}$.

22. Let f be a real-valued function defined on G. Consider the following two statements:

(i) $f(g) > 0$ for all $g \in G$.

(ii) $f(g) \geq 0$ for all $g \in G$, and there are at least two points in G where f is not zero.

If either (i) or (ii) holds, then $|\hat{f}(g)| < \hat{f}(1)$ for every $g \in G$ and $g \neq 1$.

4.2 The Fourier Transform of Periodic Functions

Let G be either the group $\mathbb{Z}_n$ or $\mathbb{Z}$. Once G is defined, it is fixed throughout the following definition: A complex-valued function defined on G is said to be *periodic* if there is a positive integer $\sigma \in G$ such that $f(x + \sigma) = f(x)$ for all $x \in G$. The smallest of such σ is called the *period* of f. If σ is the period of f, then the subset $\{1, \ldots, \sigma\}$ of G is called the *fundamental set* of f; f is determined if its values on the fundamental set are known.

We consider periodic functions on $\mathbb{Z}_n$ and $\mathbb{Z}$ separately.

4.2.1 Periodic functions on $\mathbb{Z}_n$

We begin with a theorem which describes a relationship between the period of $f\colon \mathbb{Z}_n \to \mathbb{C}$ and n, the number of elements of its domain.

Theorem 4.2.1. *The period of any periodic function defined on $\mathbb{Z}_n$ divides n. Consequently, if p is prime, then the only periodic functions defined on $\mathbb{Z}_p$ are constants.*

Proof. Suppose that σ is the period of f. If $\sigma \nmid n$, then, by the Euclidean algorithm, $n = q\sigma + r$ for a unique pair of integers q and r, where $q \geq 1$ and $0 < r < \sigma$. As an element of the group $\mathbb{Z}_n$, $q\sigma + r = 0$, thus for any $x \in \mathbb{Z}_n$ the periodicity of f implies that

$$f(x) = f(x + r + q\sigma) = f(x + r).$$

Since this equation holds for all x in $\mathbb{Z}_n$, by definition of the period we have $\sigma \leq r$, which is impossible. ■

Assume that $f \colon \mathbb{Z}_n \to \mathbb{C}$ is a nonconstant periodic function with period σ. Since f is nonconstant, $\sigma > 1$. Also, by Theorem 4.2.1, $n = k\sigma$ for some positive integer k. The periodicity of f implies that

$$\begin{aligned}
\hat{f}(s) &= \frac{1}{\sqrt{n}} \sum_{t=0}^{n-1} e^{-\frac{2\pi i}{n} st} f(t) \\
&= \frac{1}{\sqrt{n}} \sum_{j=0}^{k-1} \sum_{t=j\sigma}^{(j+1)\sigma-1} e^{-\frac{2\pi i}{n} st} f(t) \\
&= \frac{1}{\sqrt{n}} \sum_{j=0}^{k-1} \sum_{t=0}^{\sigma-1} e^{-\frac{2\pi i}{n} s(t+j\sigma)} f(t + j\sigma) \\
&= \frac{1}{\sqrt{n}} \sum_{j=0}^{k-1} e^{-\frac{2\pi i}{n} sj\sigma} \sum_{t=0}^{\sigma-1} e^{-\frac{2\pi i}{n} st} f(t) \\
&= \left(\frac{1}{\sqrt{k}} \sum_{j=0}^{k-1} \left[e^{-\frac{2\pi i}{k} s} \right]^j \right) \left(\frac{1}{\sqrt{\sigma}} \sum_{t=0}^{\sigma-1} e^{-\frac{2\pi i}{n} st} f(t) \right),
\end{aligned}$$

whence, with the aid of the geometric progression formula, we obtain

$$\hat{f}(s) = \begin{cases} 0 & \text{if } s \text{ is not a multiple of } k, \\ \frac{\sqrt{k}}{\sqrt{\sigma}} \sum_{t=0}^{\sigma-1} e^{-\frac{2\pi i}{\sigma} mt} f(t) & \text{if } s = mk \text{ for some integer } m, \\ & \quad \text{where } 0 \leq m < \sigma. \end{cases}$$

Thus, if f_σ is the function defined on the group $\mathbb{Z}_\sigma$ by $f_\sigma(m) = f(m)$, then

$$\hat{f}(s) = \begin{cases} 0 & \text{if } s \text{ is not a multiple of } k, \\ \sqrt{k}\hat{f}_\sigma(m) & \text{if } s = mk \text{ for some integer } m, \\ & \quad \text{where } 0 \le m < \sigma. \end{cases}$$

Theorem 4.2.2. *Suppose that $f\colon \mathbb{Z}_n \to \mathbb{C}$ is a nonconstant periodic function with period σ. If $f_\sigma\colon \mathbb{Z}_\sigma \to \mathbb{C}$ is defined by $f_\sigma(m) = f(m)$, then*

$$\hat{f}(s) = \begin{cases} 0 & \textit{if } s \textit{ is not a multiple of } n/\sigma, \\ \sqrt{n/\sigma}\hat{f}_\sigma(m) & \textit{if } s = m(n/\sigma) \textit{ for some integer } m, \\ & \quad 0 \le m < \sigma, \end{cases}$$

where $\hat{f}_\sigma$ is the FT of f_σ on $\mathbb{Z}_\sigma$. Consequently, the number of points where $\hat{f} \neq 0$ is at most σ.

Note that if f and f_σ are considered as functions defined on sets $\mathbb{Z}_n$ and $\mathbb{Z}_\sigma$, respectively, then f_σ is the restriction of f to the subset $\mathbb{Z}_\sigma$. If the group structures on the domains of f and f_σ are taken into account, then f_σ is not the restriction of f to $\mathbb{Z}_\sigma$. With respect to the addition in $\mathbb{Z}_\sigma$, the sum of two elements of $\mathbb{Z}_\sigma$ is again an element of $\mathbb{Z}_\sigma$; on the other hand, the sum of the same two elements with respect to the addition in $\mathbb{Z}_n$ might not be in $\mathbb{Z}_\sigma$.

For a periodic function f with period σ, we have $\tau_\sigma f = f$, whence

$$\hat{f}(x) = \widehat{\tau_\sigma f}\,(x) = e^{\frac{2\pi i}{n}\sigma x}\hat{f}(x) \tag{4.7}$$

for every $x \in \mathbb{Z}_n$. If f is nonconstant, then $\sigma > 1$ and, by Theorem 4.1.1, $\hat{f}(x) \neq 0$ for some nonzero $x \in \mathbb{Z}_n$. We may conclude from (4.7) that $e^{(2\pi i/n)\sigma x} = 1$, which in turns implies that $\gcd(x, n) > 1$ (i.e., the greatest common divisor of x and n is greater than 1). This result has a theoretical application to the *factoring problem*: given an odd positive integer n, which is not a prime, find a nontrivial divisor of n, i.e., a divisor that is greater than 1 and less than n. We outline a three-step algorithm for a solution to this problem as follows:

Step 1: Define a nonconstant periodic function $f\colon \mathbb{Z}_n \to \mathbb{C}$.
Step 2: Find a positive $x \in \mathbb{Z}_n$ such that $\hat{f}(x) \neq 0$.
Step 3: Find $d = \gcd(x, n)$.

Of the three steps, Step 1 seems to be the most difficult and for a large value of n Step 2 is also difficult. Once the first two steps are done, the Euclidean algorithm can be used in Step 3. Because of the difficulty in Step 1, the given algorithm is not useful in practice.

4.2.2 Periodic functions on $\mathbb{Z}$

Suppose that $f\colon \mathbb{Z} \to \mathbb{C}$ is a periodic function with period σ. If $f_\sigma\colon \mathbb{Z}_\sigma \to \mathbb{C}$ is the function defined by $f_\alpha(k) = f(k)$, then f is the *periodic extension* of f_σ to $\mathbb{Z}$. The FT of f is defined by setting $\hat{f}(k) = \hat{f}_\sigma(\tilde{k})$, where $\tilde{k}$ is the projection of k in $\mathbb{Z}_\sigma$, i.e., $\tilde{k} \in \mathbb{Z}_\sigma$ and $k \equiv \tilde{k} \pmod{\sigma}$. Explicitly, for any $j \in \mathbb{Z}$,

$$\hat{f}(j) = \frac{1}{\sqrt{\sigma}} \sum_{k=0}^{\sigma-1} e^{-\frac{2\pi i}{\sigma}\tilde{j}k} f_\sigma(k).$$

Since $e^{-\frac{2\pi i}{\sigma}jk} = e^{-\frac{2\pi i}{\sigma}\tilde{j}k}$ and $f(k) = f_\sigma(k)$ for $k = 0, \ldots, \sigma - 1$, we can write the previous equation as

$$\hat{f}(j) = \frac{1}{\sqrt{\sigma}} \sum_{k=0}^{\sigma-1} e^{-\frac{2\pi i}{\sigma}jk} f(k). \tag{4.8}$$

Since constant functions have period 1, it follows from (4.8) that $\hat{c} = c$ for any $c \in \mathbb{C}$, that is, the FT of constant functions defined on $\mathbb{Z}$ are supported everywhere. Notice that the result just obtained is different from that of Theorem 4.1.1; this occurs because there is a distinction between the definitions of the FT of functions defined on $\mathbb{Z}$ and $\mathbb{Z}_n$.

For each integer a, the translation by a is the linear operator $\tau_a\colon V_\mathbb{Z} \to V_\mathbb{Z}$ given by $f \mapsto \tau_a f$, where $\tau_a f(x) = f(x + a)$. For a periodic function $f\colon \mathbb{Z} \to \mathbb{C}$ with period σ, the relations (4.5) still hold, i.e.,

$$\widehat{\tau_a f} = \chi_a \hat{f} \quad \text{and} \quad \widehat{\chi_a f} = \tau_{-a} \hat{f}, \tag{4.9}$$

where in these equations $\chi_a(x) = e^{\frac{2\pi i}{\sigma}ax}$. It follows from the second equation in (4.9) that *the FT of any periodic function defined on* $\mathbb{Z}$ *is again a periodic function with the same period.*

4.3 The Inverse Fourier Transform

Being an isometry, the FT has a unique inverse which is called the *inverse Fourier transform* (IFT). The IFT is denoted by either $\mathcal{F}^{-1}$ or $\check{}$; i.e., for $f \in V_G$, we denote the IFT of f by either $\mathcal{F}^{-1}f$ or $\check{f}$. We will use the two notations interchangeably. Since the inverse of an isometry is also an isometry, the IFT is an isometry of V_G. Consequently,

$$\langle f_1, f_2 \rangle = \langle \check{f}_1, \check{f}_2 \rangle$$

for every f_1, $f_2 \in V_G$. In particular, $\|f\| = \|\check{f}\|$ for every $f \in V_G$.

By definition of the inverse, $\check{\delta}_g = B_g$ for every $g \in G$. This result enables us to express $\check{f}$ in terms of f. Applying the operator $\check{}$ on both sides of the equation

$$f = \sum_{g \in G} \langle f, \delta_g \rangle \delta_g \tag{4.10}$$

we obtain

$$\check{f} = \sum_{g \in G} \langle f, \delta_g \rangle B_g. \tag{4.11}$$

(Also, see Exercise 8, page 32.)

Comparing (4.2) and (4.11) we see that these equations for $\hat{f}$ and $\check{f}$, respectively, are symmetric in B_g and δ_g in the sense that we can obtain one equation from another by interchanging the role of B_g and δ_g. This symmetry is a reflection of the fact that the FT maps each B_g to δ_g, so its inverse maps each δ_g to B_g, for every $g \in G$. Thus, many statements about the FT and the IFT are symmetric. For instance, statements about the inversion formulas for the FT (as we will see shortly in the next section) and the IFT in Exercise 23 are symmetric.

Example 4.3.1. Let G be the group $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}$ and let f be a complex-valued function defined on G. By (4.11), the value of $\check{f}$ at a point x in G is given by

$$\check{f}(x) = \sum_{y \in G} f(y) B_y(x) = \frac{1}{\sqrt{|G|}} \sum_{y \in G} f(y) \chi_y(x).$$

From (3.4) and the fact that $|G| = n_1 \ldots n_m$, we have

$$\check{f}(x) = \frac{1}{\sqrt{n_1 \ldots n_m}} \sum_{y \in G} e^{2\pi i \left(\frac{x_1 y_1}{n_1} + \cdots + \frac{x_m y_m}{n_m} \right)} f(y). \tag{4.12}$$

In particular, if $n_j = n$ for every j, then

$$\check{f}(x) = \frac{1}{\sqrt{n^m}} \sum_{y \in \mathbb{Z}_n^m} e^{\frac{2\pi i}{n} x \cdot y} f(y). \tag{4.13}$$

Comparing (4.3) and (4.12), we can conclude that $\hat{\bar{f}}(x) = \bar{\check{f}}(x) = \bar{\hat{f}}(-x)$.

Example 4.3.2. Since $e^{\pi i} = -1$, by setting $n = 2$ in equation (4.13), we have

$$\check{f}(x) = \frac{1}{\sqrt{2^m}} \sum_{y \in \mathbb{Z}_2^m} (-1)^{x \cdot y} f(y)$$

for all $x \in \mathbb{Z}_2^m$. Comparing this example to Example 4.1.2, we may conclude that $\hat{f} = \check{f}$. The converse also holds; that is, if $\hat{f} = \check{f}$ on $V_{\mathbb{Z}_n^m}$, then $n = 2$, which is proved later in Theorem 4.7.1. In other words, the FT on $\mathbb{Z}_2^m$ is a linear operator of order 2. Also, see Theorem 4.1.2.

4.4 The Inversion Formula

Our next goal is to find the inversion formula for the FT, that is, the formula which expresses f in terms of $\hat{f}$ and functions in the character basis. Let G be a finite Abelian group and let f be a complex-valued function defined on G. Since

$$f = \sum_{g\,\in\,G} \langle f, B_g \rangle B_g$$

and $\langle f, B_g \rangle = \langle \hat{f}, \delta_g \rangle$, we have

$$f = \sum_{g\,\in\,G} \langle \hat{f}, \delta_g \rangle B_g .$$

This equation is called the *inversion formula* for the FT. (Compare to Exercise 8, page 32.)

Example 4.4.1. Suppose that $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}$ and f is a complex-valued function defined on G. For $x \in G$, by the inversion formula, we have

$$\begin{aligned} f(x) &= \sum_{y\,\in\,G} \hat{f}(y) B_y(x) \\ &= \frac{1}{\sqrt{|G|}} \sum_{y\,\in\,G} \hat{f}(y) \chi_y(x) \\ &= \frac{1}{\sqrt{n_1 \ldots n_m}} \sum_{y\,\in\,G} e^{2\pi i \left(\frac{x_1 y_1}{n_1} + \cdots + \frac{x_m y_m}{n_m} \right)} \hat{f}(y). \end{aligned}$$

In particular, if $n_j = n$ for every j, then

$$f(x) = \frac{1}{\sqrt{n^m}} \sum_{y\,\in\,\mathbb{Z}_n^m} e^{\frac{2\pi i}{n} x \cdot y} \hat{f}(y).$$

Example 4.4.2. If $n = 2$, then

$$f(x) = \frac{1}{\sqrt{2^m}} \sum_{y \in \mathbb{Z}_2^m} (-1)^{x \cdot y} \hat{f}(y)$$

for all $x \in \mathbb{Z}_2^m$.

Exercises.

23. Prove the inversion formula for the IFT: if $f \in V_G$, then

$$f = \sum_{g\,\in\,G} \langle \check{f}, B_g \rangle \delta_g .$$

24. Prove that the formula

$$f(1) = \frac{1}{\sqrt{|G|}} \sum_{g \in G} \hat{f}(g)$$

holds for every complex-valued function f defined on G.

25. Suppose that $f\colon \mathbb{Z} \to \mathbb{C}$ is a periodic function with period σ. Prove the inversion formula: for every $j \in \mathbb{Z}$,

$$f(j) = \frac{1}{\sqrt{\sigma}} \sum_{k=0}^{\sigma-1} e^{\frac{2\pi i}{\sigma} jk} \hat{f}(k).$$

4.5 Matrices of the Fourier Transform

As a linear operator on V_G, the FT has a unique matrix representation with respect to the standard basis Δ_G.

Theorem 4.5.1. *The matrix of the FT with respect to the standard basis is $\overline{X}/\sqrt{|G|}$, where $\overline{X}$ is obtained by taking the complex conjugate of the entries of X (the matrix defined in Example* 3.2.1 *on page* 41*).*

Proof. We enumerate G and write $G = \{g_1, \dots, g_\eta\}$. Also, for simplicity we write δ_s for δ_{g_s} and B_t for B_{g_t}. Then the (s,t) entry of the FT with respect to the basis Δ_G is $\langle \hat{\delta}_t, \delta_s \rangle$. Since

$$\hat{\delta}_t = \sum_{j=1}^{\eta} \langle \delta_t, B_j \rangle \delta_j = \sum_{j=1}^{\eta} \bar{B}_j(t)\delta_j = \frac{1}{\sqrt{\eta}} \sum_{j=1}^{\eta} \bar{\chi}_j(t)\delta_j,$$

we have

$$\langle \hat{\delta}_t, \delta_s \rangle = \frac{1}{\sqrt{\eta}} \bar{\chi}_s(t).$$

Hence the matrix of the FT is $\overline{X}/\sqrt{|G|}$. ■

We identify the FT with its matrix and write $\mathcal{F} = \overline{X}/\sqrt{|G|}$. Since $\mathcal{F}$ is the matrix of the FT and since it is unitary (by Corollary 3.2.2), it follows that the matrix of the IFT is $\mathcal{F}^{-1} = \mathcal{F}^* =$

$X^t/\sqrt{|G|}$, where X^t is the transpose of X. Therefore, *the adjoint of the FT is the IFT, and conversely the adjoint of the IFT is the FT*. Equivalently, if f_1 and f_2 are complex-valued functions defined on G, then

$$\langle \hat{f}_1, f_2 \rangle = \langle f_1, \check{f}_2 \rangle.$$

This is expected since the FT is an isometry.

We can express the FT and IFT in terms of the matrices $\mathcal{F}$ and $\mathcal{F}^{-1}$, respectively, as

$$\mathcal{F} f = \hat{f} \quad \text{and} \quad \mathcal{F}^{-1} f = \check{f}.$$

In these equations, f, $\hat{f}$, and $\check{f}$ are considered as column vectors whose coordinates consist of their values on G, respectively.

Exercise.

26. Set $c_n = e^{-2\pi i/n}$. Recall the matrix M_x and the polynomial $p_x(z)$ from Exercise 18 (page 46). Show that the FT on $\mathbb{Z}_n$ diagonalizes M_x, that is,

$$\mathcal{F}^* M_x \mathcal{F} = \operatorname{diag}[\lambda_1, \ldots, \lambda_n],$$

where $\lambda_j = c_n^{j-1} p_x(c_n^{j-1})$.

4.6 Iterated Fourier Transforms

Let $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}$ and let f be a complex-valued function defined on G. A point $x = (x_1, \ldots, x_m)$ in G can also be written as $x = (x_1, w)$, where $w = (x_2, \ldots, x_m)$ is a point in $\mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_m}$. If w is fixed, then the equation $f_w(x_1) = f(x_1, w)$ defines the function f_w on $\mathbb{Z}_{n_1}$. The FT of f_w, denoted $\mathcal{F}_1 f_w$, is given pointwise by

$$\mathcal{F}_1 f_w(x_1) = \langle f_w, B_{x_1} \rangle = \sum_{y_1 \in \mathbb{Z}_{n_1}} f_w(y_1) \bar{B}_{x_1}(y_1),$$

where B_{x_1} is a character of the group $\mathbb{Z}_{n_1}$. We can express $\mathcal{F}_1 f_w$ in terms of f as

$$\mathcal{F}_1 f(x_1, w) = \sum_{y_1 \in \mathbb{Z}_{n_1}} f(y_1, w) \bar{B}_{x_1}(y_1)$$

or

$$\mathcal{F}_1 f(x) = \sum_{y_1 \in \mathbb{Z}_{n_1}} f(y_1, x_2, \ldots, x_m) \bar{B}_{x_1}(y_1).$$

In general, for $j = 1, \ldots, m$, *the FT of* f *in the* j*th-coordinate* is defined pointwise by the equation

$$\mathcal{F}_j f(x) = \sum_{y_j \in \mathbb{Z}_{n_j}} f(x_1, \ldots, y_j, \ldots, x_m) \bar{B}_{x_j}(y_j),$$

where B_{x_j} is a character of the group $\mathbb{Z}_{n_j}$. Since the inner product is linear in the first argument, the operator $\mathcal{F}_j$ is linear.

Theorem 4.6.1. *Consider the group* $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}$ *and any complex-valued function* f *defined on* G*. For any* j, $k = 1, \ldots, m$, *we have*

$$\mathcal{F}_j \mathcal{F}_k f = \mathcal{F}_k \mathcal{F}_j f,$$

i.e., the operators $\mathcal{F}_1, \ldots, \mathcal{F}_m$ *are commutative* (*with respect to composition*).

Proof. If f is a complex-valued function defined on G, then for $j < k$ we have

$$\begin{aligned}
&\mathcal{F}_j \mathcal{F}_k f(x) \\
&\quad = \mathcal{F}_j \left(\sum_{y_k \in \mathbb{Z}_{n_k}} f(x_1, \ldots, y_k, \ldots, x_m) \bar{B}_{x_k}(y_k) \right) \\
&\quad = \sum_{y_k \in \mathbb{Z}_{n_k}} \mathcal{F}_j f(x_1, \ldots, y_k, \ldots, x_m) \bar{B}_{x_k}(y_k) \\
&\quad = \sum_{y_k \in \mathbb{Z}_{n_k}} \sum_{y_j \in \mathbb{Z}_{n_j}} f(x_1, \ldots, y_j, \ldots, y_k, \ldots, x_m) \bar{B}_{x_j}(y_j) \bar{B}_{x_k}(y_k) \\
&\quad = \sum_{y_j \in \mathbb{Z}_{n_j}} \sum_{y_k \in \mathbb{Z}_{n_k}} f(x_1, \ldots, y_j, \ldots, y_k, \ldots, x_m) \bar{B}_{x_k}(y_k) \bar{B}_{x_j}(y_j) \\
&\quad = \sum_{y_j \in \mathbb{Z}_{n_j}} \mathcal{F}_k f(x_1, \ldots, y_j, \ldots, x_m) \bar{B}_{x_j}(y_j)
\end{aligned}$$

$$= \mathcal{F}_k \left(\sum_{y_j \in \mathbb{Z}_{n_j}} f(x_1, \ldots, y_j, \ldots, x_m) \bar{B}_{x_j}(y_j) \right)$$
$$= \mathcal{F}_k \mathcal{F}_j f(x).$$

Thus $\mathcal{F}_j$ and $\mathcal{F}_k$ commute. ■

The following theorem states that the FT of f can be obtained by applying the operators $\mathcal{F}_1, \ldots, \mathcal{F}_m$ sequentially, in any order, to f.

Theorem 4.6.2. *Suppose that $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}$ and ϵ is a permutation of the set $\{1, \ldots, m\}$. As a linear operator on the inner product space V_G, the FT, $\mathcal{F}$, satisfies the equation $\mathcal{F} = \mathcal{F}_{\epsilon(1)} \cdots \mathcal{F}_{\epsilon(m)}$, the composition of the linear operators $\mathcal{F}_1, \ldots, \mathcal{F}_m$.*

Proof. By Theorem 4.6.1, it suffices to show that $\mathcal{F} = \mathcal{F}_1 \cdots \mathcal{F}_m$ and we prove this by induction on m. The case $m = 1$ is trivially true since $\mathcal{F} = \mathcal{F}_1$. Suppose that the theorem holds for $m = k-1$, where $k > 1$, and consider the case $m = k$. Let f be a complex-valued function defined on $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$. For each $y = (y', w_y) \in \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$, where $y' \in \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_{k-1}}$ and $w_y \in \mathbb{Z}_{n_k}$, let f_{w_y} be the function on $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_{k-1}}$ defined by $f_{w_y}(y') = f(y', w_y)$. By the induction hypothesis, we have $\mathcal{F} f_{w_y} = \mathcal{F}_1 \ldots \mathcal{F}_{k-1} f_{w_y}$; i.e.,

$$\mathcal{F}_1 \ldots \mathcal{F}_{k-1} f_{w_y}(x') = \sum_{y'} f_{w_y}(y') \bar{B}_{x'}(y')$$

for all $x' \in \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_{k-1}}$. For $x = (x', w_x) \in \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$, we have

$$\mathcal{F} f(x) = \sum_{y} f(y) \bar{B}_x(y)$$
$$= \sum_{y', w_y} f(y', w_y) \bar{B}_{x'}(y') \bar{B}_{w_x}(w_y)$$
$$= \sum_{w_y} \sum_{y'} f_{w_y}(y') \bar{B}_{x'}(y') \bar{B}_{w_x}(w_y)$$
$$= \sum_{w_y} \mathcal{F}_1 \ldots \mathcal{F}_{k-1} f_{w_y}(x') \bar{B}_{w_x}(w_y)$$

$$
\begin{aligned}
&= \mathcal{F}_1 \ldots \mathcal{F}_{k-1}\left(\sum_{w_y} f_{w_y}(x')\bar{B}_{w_x}(w_y)\right)\\
&= \mathcal{F}_1 \ldots \mathcal{F}_{k-1}\left(\sum_{w_y} f(x', w_y)\bar{B}_{w_x}(w_y)\right)\\
&= \mathcal{F}_1 \ldots \mathcal{F}_{k-1}\mathcal{F}_k f(x', w_x)\\
&= \mathcal{F}_1 \ldots \mathcal{F}_{k-1}\mathcal{F}_k f(x).
\end{aligned}
$$

The proof is complete. ■

Concerning the inverse operator $\mathcal{F}_j^{-1}$, by the equation for the IFT (i.e., eq. (4.11)) we have

$$\mathcal{F}_j^{-1} f(x) = \sum_{y_j \in \mathbb{Z}_{n_j}} f(x_1, \ldots, y_j, \ldots, x_m) B_{y_j}(x_j).$$

From this equation it is clear that the operator $\mathcal{F}_j^{-1}$ is linear. Also, the operators $\mathcal{F}_1^{-1}, \ldots, \mathcal{F}_m^{-1}$ satisfy Theorems 4.6.1 and 4.6.2, i.e.,

$$\mathcal{F}_j^{-1}\mathcal{F}_k^{-1} = \mathcal{F}_k^{-1}\mathcal{F}_j^{-1} \quad \text{and} \quad \mathcal{F}^{-1} = \mathcal{F}_{\epsilon(1)}^{-1} \cdots \mathcal{F}_{\epsilon(m)}^{-1}.$$

We leave the proof of these facts as an exercise.

For each fixed permutation ϵ, the products $\mathcal{F}_{\epsilon(1)} \cdots \mathcal{F}_{\epsilon(m)}$ and $\mathcal{F}_{\epsilon(1)}^{-1} \cdots \mathcal{F}_{\epsilon(m)}^{-1}$ are called the *iterated FT* and *iterated IFT*, respectively.

Exercise.

27. Prove that Theorems 4.6.1 and 4.6.2 hold if we replace each $\mathcal{F}_j$ and $\mathcal{F}_{\epsilon(j)}$ by their inverses $\mathcal{F}_j^{-1}$ and $\mathcal{F}_{\epsilon(j)}^{-1}$, respectively.

4.7 Is the Fourier Transform a Self-Adjoint Operator?

The FT on a finite Abelian group G is self-adjoint if and only if $\langle \hat{f}_1, f_2 \rangle = \langle f_1, \hat{f}_2 \rangle$ for all complex-valued functions f_1 and f_2 defined on G. In terms of the matrix X, the FT is self-adjoint if and only if $\overline{X} = X^t$ or, equivalently,

$$\bar{\chi}_x(y) = \chi_y(x) \tag{4.14}$$

for all x, $y \in G$. In general, condition (4.14) does not hold, for it implies that $\chi_x(x)$ is real for all $x \in G$. However, by Example 3.1.3, we have $\chi_x(y) = \chi_y(x) = (-1)^{x \cdot y}$ for all x, $y \in \mathbb{Z}_2^m$ and hence the FT is self-adjoint on $V_{\mathbb{Z}_2^m}$.

Next we show that if the FT is self-adjoint on $V_{\mathbb{Z}_n^m}$, then $n = 2$. Assume that $\mathbb{Z}_n^m$ is nontrivial, i.e., $n > 1$, and the FT is self-adjoint on $V_{\mathbb{Z}_n^m}$. Condition (4.14) and Example 3.1.2 imply that

$$e^{-\frac{2\pi i}{n} x \cdot y} = e^{\frac{2\pi i}{n} x \cdot y}$$

for all x, $y \in \mathbb{Z}_n^m$. It follows that $2x \cdot y = 0 \, (\mathrm{mod}\, n)$ for all x, $y \in \mathbb{Z}_n^m$. In particular, we can choose x and y such that $x \cdot y = 1 \, (\mathrm{mod}\, n)$; e.g., $x = y = (1, 0, \dots, 0)$, an m-tuple. In this case we have $2 \equiv 0 \, (\mathrm{mod}\, n)$, whence $n = 2$. We have proved the following theorem.

Theorem 4.7.1. *Suppose that $\mathbb{Z}_n^m$ is a nontrivial group. The FT on $\mathbb{Z}_n^m$ is self-adjoint if and only if $n = 2$.*

Note that this theorem also follows from the spectral theorem, as we will see in Section 7.3.

Another proof of the fact that the FT, in general, is not self-adjoint, using the complexity of its eigenvalues, is indicated in Exercise 41 of Section 7.2.

5

Convolution, Banach Algebras, and the Uncertainty Principle

There is a bilinear map on V_G (i.e., a map from $V_G \times V_G$ to V_G which is linear in each variable) which becomes the pointwise product of functions under the FT. This map is called the *convolution of functions* for the FT. The inner product space V_G together with the convolution form a Banach algebra. The discussion of convolution and Banach algebras comprises the first two sections of this chapter. In the final section, we prove that the order of G does not exceed the product of the cardinalities of the supports of f and $\hat{f}$ provided f is nonzero. This result is known as the *uncertainty principle.*

5.1 The Convolution Operator

As in the nondiscrete case, there is the notion of convolution which we now define.

Definition 5.1.1. *Suppose that G is a finite Abelian group and f_1 and f_2 are complex-valued functions defined on G. The convolution of f_1 and f_2 is the complex-valued function $f_1 * f_2$ defined on G by*

$$f_1 * f_2(x) = \frac{1}{\sqrt{|G|}} \sum_{g \in G} f_1(xg^{-1}) f_2(g).$$

We proceed to show that the convolution is a symmetric bilinear operator on V_G, i.e., a symmetric bilinear transformation from $V_G \times V_G$ to V_G. This fact will be established by Theorem 5.1.1 after the following lemma.

B. Luong, *Fourier Analysis on Finite Abelian Groups*, Applied and Numerical Harmonic Analysis, DOI 10.1007/978-0-8176-4916-6_5,

Lemma 5.1.1. *Suppose that G is a finite Abelian group.*

(i) *For any s, $t \in G$,*

$$B_s * B_t = \begin{cases} B_s & \textit{if } s = t, \\ 0 & \textit{if } s \neq t. \end{cases}$$

Consequently, B_s and B_t commute, i.e., $B_s * B_t = B_t * B_s$.

(ii) *$(B_r * B_s) * B_t = B_r * (B_s * B_t)$ for any r, s, $t \in G$.*

Proof. (i) For each $x \in G$,

$$\begin{aligned} B_s * B_t(x) &= \frac{1}{\sqrt{|G|}} \sum_{g \in G} B_s(xg^{-1}) B_t(g) \\ &= B_s(x) \sum_{g \in G} B_s(g^{-1}) B_t(g) \\ &= B_s(x) \sum_{g \in G} \bar{B}_s(g) B_t(g) \\ &= B_s(x) \langle B_t, B_s \rangle \\ &= \begin{cases} B_s(x) & \text{if } s = t, \\ 0 & \text{if } s \neq t. \end{cases} \end{aligned}$$

(ii) follows from (i) by noting that

$$(B_r * B_s) * B_t = B_r * (B_s * B_t) = \begin{cases} B_s & \text{if } r = s = t, \\ 0 & \text{otherwise.} \end{cases} \qquad \blacksquare$$

Some properties of the convolution are listed in the following theorem, most of which are consequences of Lemma 5.1.1.

Theorem 5.1.1. *Suppose that G is a finite Abelian group. Set $\delta = \sum_{g \in G} B_g$ and let f, f_1, and f_2 be complex-valued functions defined on G. Then*

(i) *$f * (cf_1 + f_2) = c(f * f_1) + (f * f_2)$ for any $c \in \mathbb{C}$.*

(ii)
$$f_1 * f_2 = \sum_{g \in G} \hat{f}_1(g)\hat{f}_2(g)B_g.$$

Consequently,

$$\operatorname{supp}(\hat{f}_1) \cap \operatorname{supp}(\hat{f}_2) = \varnothing \text{ if and only if } f_1 * f_2 = 0.$$

(iii) $(f_1 * f_2)\hat{} = \hat{f}_1\hat{f}_2$.

(iv) $f_1 * f_2 = f_2 * f_1$ (*commutative*).

(v) $(f * f_1) * f_2 = f * (f_1 * f_2)$ (*associative*).

(vi) $f * \delta = f$*, furthermore, if* $\operatorname{supp}(\hat{f}) = G$*, then* δ *is uniquely determined* (*existence of identity*).

(vii) *If* $\operatorname{supp}(\hat{f}) = G$*, then there is a unique complex-valued function* ϕ *on* G *such that* $\phi * f = \delta$ (*existence of inverse*).

Proof. (i) is straightforward from the definition. (ii) follows from the inversion formula, (i), and Lemma 5.1.1 (i). (iii) follows from (ii). (iv) follows from (i) and Lemma 5.1.1 (i). (v) follows from (i) and Lemma 5.1.1 (ii). Both (vi) and (vii) follow from (ii). ■

It follows from (i) and (iv) of Theorem 5.1.1 that the convolution is a symmetric bilinear operator on V_G. Also, by the same theorem, the set of all functions $f\colon G \to \mathbb{C}$ such that $\operatorname{supp}(\hat{f}) = G$ form an Abelian group with respect to the operation of convolution.

Theorem 5.1.1 (i) also implies that, for a fixed $\hbar \in V_G$, the map $C_\hbar\colon V_G \to V_G$ defined by $C_\hbar(f) = \hbar * f$ is linear, so it is completely determined once its values on a basis are known.

Definition 5.1.2. *Let* $\hbar$ *be a complex-valued function defined on* G*. The convolution operator with respect to* $\hbar$ *is the linear operator* $C_\hbar\colon V_G \to V_G$ *defined on the basis* B_G *by*

$$C_\hbar(B_g) = \hbar * B_g.$$

By (ii) of Theorem 5.1.1 we have

$$C_\hbar(B_g) = \hat{\hbar}(g)B_g. \tag{5.1}$$

This equation has several consequences, which are listed in the following theorem.

Theorem 5.1.2. *Suppose that G is a finite Abelian group and $\hbar$ is a complex-valued function defined on G. Then the following statements are true*:

(i) *The functions in the character basis B_G are eigenvectors of $C_\hbar$; the eigenvector B_g belongs to the eigenvalue $\hat{\hbar}(g)$.*
(ii) *The operator $C_\hbar$ is normal, that is, $C_\hbar$ commutes with its adjoint $C_\hbar^*$.*
(iii) *The operator $C_{\check{f}}$ is an isometry for every $f \in V_G$ for which $|f| = 1$. In particular, $C_{\check{\chi}}$ is an isometry for every $\chi \in \hat{G}$.*

Proof. (i) follows from (5.1). To prove (ii) we enumerate G as $G = \{g_1, \ldots, g_\eta\}$. Then by (5.1) the matrix of $C_\hbar$ with respect to the character basis is the diagonal matrix

$$D_\hbar = \operatorname{diag}\big[\hat{\hbar}(g_1), \ldots, \hat{\hbar}(g_\eta)\big].$$

Hence $D_\hbar$ commutes with its adjoint.

(iii) The matrix of $C_{\check{f}}$ with respect to the basis B_G is $D_{\check{f}} = \operatorname{diag}\big[f(g_1), \ldots, f(g_\eta)\big]$. Since $|f(g_j)| = 1$ for $j = 1, \ldots, \eta$, it follows that $D_{\check{f}}^{-1} = D_{\check{f}}^*$ or, equivalently, $C_{\check{f}}$ is an isometry. ■

Besides properties listed in Theorem 5.1.2, the linear operator $C_\hbar$ has another property, namely, it commutes with translations. That is, $\tau_a C_\hbar = C_\hbar \tau_a$ for all $a \in G$, where $\tau_a C_\hbar$ and $C_\hbar \tau_a$ are compositions of the operators τ_a and $C_\hbar$. In fact, we will prove shortly that $C_\hbar$ is the only type of linear operator on V_G having this property. Towards this end we recall that, in multiplicative notation, the translation by a is the operator τ_a on V_G defined by $f \mapsto \tau_a f$, where $\tau_a f(g) = f(ga)$. It is clear that translations are linear. In the following example, we consider the translation of functions in the character basis B_G.

Example 5.1.1. For a fixed $a \in G$, we have $\tau_a B_g(x) = B_g(xa) = \sqrt{|G|}B_g(a)B_g(x)$ for every x in G, whence

$$\tau_a B_g = \sqrt{|G|}B_g(a)B_g. \tag{5.2}$$

Thus functions in the character basis are eigenvectors of the translation τ_a, where, according to the previous equation, the eigenvector B_g belongs to the eigenvalue $\sqrt{|G|}B_g(a)$. It follows that if G is enumerated as $G = \{g_1, \ldots, g_\eta\}$, then with respect to the character basis the matrix of τ_a is the diagonal matrix

$$D_a = \sqrt{|G|}\,\mathrm{diag}\left[B_{g_1}(a), \ldots, B_{g_\eta}(a)\right].$$

Consequently, we have $D_a^* D_a = D_a D_a^* = I$, which is expected since translations are obviously isometries.

Theorem 5.1.3. *Let T be a linear operator on V_G. Then T commutes with translations if and only if $T = C_\hbar$ for some $\hbar \in V_G$.*

Proof. In what follows the product $T\tau_a$ (or $\tau_a T$) denotes the composition of the operators τ_a and T. On the other hand, for f in the domain of T, we use Tf to denote the image of f under T. There should be no confusion in the context. In situations where confusion may arise Tf is written as $T(f)$ for clarity.

Assume that T commutes with translations. Let B_g be an element of B_G. If a is a fixed element of G, then, by Example 5.1.1, $\tau_a B_g = \sqrt{|G|} B_g(a) B_g$. By the assumption and the linearity of T, we have

$$\tau_a T(B_g) = T(\tau_a B_g) = \sqrt{|G|} B_g(a) T B_g,$$

which implies that, for all $x \in G$,

$$TB_g(xa) = \tau_a T(B_g)(x) = \sqrt{|G|} B_g(a) T B_g(x).$$

Since $xa = ax$, by interchanging the role (or position) of a and x in the expression on the right-hand side of the last equal sign in the last chain of equations, we also have

$$TB_g(xa) = TB_g(ax) = \sqrt{|G|} B_g(x) T B_g(a).$$

Hence $B_g(a) T B_g(x) = B_g(x) T B_g(a)$ or, equivalently,

$$TB_g = \left[\frac{TB_g(a)}{B_g(a)}\right] B_g = \mu_g B_g$$

for all $g \in G$. Notice, in the last equation, the constant $TB_g(a)/B_g(a)$ is denoted simply by μ_g. Observe that μ is a complex-valued function on G whose value at g is μ_g. The surjection of the FT implies that there is some $\hbar \in V_G$ such that $\hat{\hbar} = \mu$. In terms of $\hbar$, we have

$$TB_g = \hat{\hbar}(g)B_g.$$

Comparing this equation with equation (5.1), we may conclude that $T = C_\hbar$ on the basis B_G. But since both T and $C_\hbar$ are linear, the equation $T = C_\hbar$ holds on the entire space V_G.

For the converse, since $C_\hbar$ and translation are linear, it is sufficient to show that $C_\hbar$ commutes with translations on the basis B_G. If $a \in G$ and $\hbar \in V_G$, then by (5.1) and (5.2) we have

$$\tau_a C_\hbar(B_g) = \tau_a\big(\hat{\hbar}(g)B_g\big) = \hat{\hbar}(g)\tau_a B_g = C_\hbar(\tau_a B_g) = C_\hbar \tau_a(B_g).$$

This chain of equations shows that $C_\hbar$ commutes with translations. ■

Exercises.

28. Suppose that $f \in V_G$ and $g \in G$. Show that $\sqrt{|G|}\,\delta_g * f = \tau_{g^{-1}} f$.

29. Show that $\sqrt{|G|}\,\delta_a * \delta_b = \delta_{ab}$ for all a, $b \in G$.

30. Prove the following:

(i) For the constant 1, we have $1 * B_1 = 1$. Here $B_1 = \chi_1/\sqrt{|G|}$, where χ_1 is the trivial character of G. (The 1 that appears in the subscripts of B_1 and χ_1 is the identity of G.) It follows that $c * B_1 = c$ for every $c \in \mathbb{C}$.

(ii) $\hat{\delta}_1 = 1/\sqrt{|G|} = B_1$.

(iii) Prove that

$$\sum_{g \in G} B_g = \sqrt{|G|}\,\delta_1.$$

31. Given any α and β in V_G, there is an $f \in V_G$ such that $f * \alpha = \beta$. Furthermore, f is uniquely determined if $\operatorname{supp}(\hat{\alpha}) = G$.

32. If $f \in V_G$ and $\operatorname{supp}(\hat{f}) \neq G$, then the solutions of the equation $f * \varphi = 0$, in which φ is the unknown (or variable), form a subspace of V_G of dimension $|G| - |\operatorname{supp}(\hat{f})|$.

33. For every f, g, $h \in V_G$, show that $\langle f, g * h\rangle = \langle g, f * h\rangle$.

34. For $f \in V_G$, the maximum value of $|f|$ is denoted by $\|f\|_\infty$, i.e.,

$$\|f\|_\infty = \max\big\{|f(g)| \,:\, g \in G\big\},$$

and the L^1-*norm* of f, denoted by $\|f\|_1$, is defined by setting

$$\|f\|_1 = \frac{1}{\sqrt{|G|}} \sum_{g \in G} |f(g)|.$$

Prove the following:

(i) $\|\hat{f}\|_\infty \le \|f\|_1$ and $\|f\|_\infty \le \|\hat{f}\|_1$.

(ii) $\|f_1 * f_2\|_\infty \le \min\big\{\|f_1\|_\infty \|f_2\|_1,\ \|f_1\|_1 \|f_2\|_\infty\big\}$ for every $f_1,\ f_2 \in V_G$.

(iii) $\|f_1 * f_2\|_1 \le \|f_1\|_1 \|f_2\|_1$ for every $f_1,\ f_2 \in V_G$.

(iv) For each $f \in V_G$, there is a subset S_f of G such that the following inequality holds:

$$\frac{1}{\sqrt{|G|}} \left| \sum_{s \in S_f} f(s) \right| \ge \frac{1}{\pi} \|f\|_1.$$

5.2 Banach Algebra

Let G be a finite Abelian group. As mentioned in Section 2.3, the inner product space V_G is isometric to the complex Euclidean space $\mathbb{C}^\eta$, where $\eta = |G|$. Thus, V_G is a *Banach space*, that is, a complete normed linear space. We will show shortly that convolution provides V_G with a multiplication operator, which turns V_G into a Banach algebra. In general, a Banach space Ω is called a *Banach algebra* if there is a multiplication defined on Ω such that, for $x,\ y,\ z \in \Omega$ and $c \in \mathbb{C}$, the following four statements hold:

(B1) $\|xy\| \le \|x\|\|y\|$, where $\|\cdot\|$ denotes the norm on Ω,

(B2) $x(yz) = (xy)z$ (associative),

(B3) $x(y+z) = xy + xz,\ (x+y)z = xz + yz$ (distributive), and

(B4) $(cx)y = x(cy) = c(xy)$.

Consider $\Omega = V_G$, where a multiplication on V_G is taken to be the convolution. Then by Theorem 5.1.1 the multiplication defined on V_G satisfies properties (B2), (B3), and (B4). To show that convolution satisfies (B1), let f_1 and f_2 be complex-valued functions defined on G. By the isometric property of the FT,

$$\|f_1 * f_2\|^2 = \|\widehat{f_1 * f_2}\|^2 = \|\hat{f}_1 \hat{f}_2\|^2 = \sum_{g \in G} |\hat{f}_1(g)|^2 \, |\hat{f}_2(g)|^2.$$

Since it is obvious that

$$\begin{aligned} \sum_{g \in G} |\hat{f}_1(g)|^2 \, |\hat{f}_2(g)|^2 &\leq \sum_{g \in G} |\hat{f}_1(g)|^2 \sum_{g \in G} |\hat{f}_2(g)|^2 \\ &= \|\hat{f}_1\|^2 \, \|\hat{f}_2\|^2 \\ &= \|f_1\|^2 \, \|f_2\|^2, \end{aligned}$$

we have $\|f_1 * f_2\| \leq \|f_1\| \|f_2\|$. Hence V_G is a commutative Banach algebra.

Among the linear functionals on V_G, that is, the complex-valued linear functions on V_G, the most important are *Banach algebra homomorphisms*. These are precisely the linear functionals which also preserve multiplications; that is, the functions $\gamma \colon V_G \to \mathbb{C}$ such that

$$\gamma(cf_1 + f_2) = c\gamma(f_1) + \gamma(f_2) \quad \text{and} \quad \gamma(f_1 * f_2) = \gamma(f_1)\gamma(f_2)$$

for all f_1, $f_2 \in V_G$ and $c \in \mathbb{C}$. The next theorem relates Banach algebra homomorphisms and the FT.

Theorem 5.2.1. *If γ is a non-identically zero algebra homomorphism on V_G, then there is a unique $x \in G$ such that $\gamma(f) = \hat{f}(x)$ for every $f \in V_G$. Conversely, for each $x \in G$, the map $\gamma \colon V_G \to \mathbb{C}$ defined by $\gamma(f) = \hat{f}(x)$ is a non-identically zero algebra homomorphism on V_G.*

Proof. By the linearity of γ, it is sufficient to show that there is a unique $x \in G$ such that

$$\gamma(B_g) = \hat{B}_g(x) = \langle B_g, B_x \rangle \tag{5.3}$$

for all basis elements B_g.

Assume that γ is an algebra homomorphism on V_G that is not identically zero. We will prove that the following statements hold for all a, b, $g \in G$:

(i) There is a unique $v_\gamma \in V_G$ such that $\gamma(B_g) = \langle B_g, v_\gamma \rangle$.
(ii) $\delta_{ab} = c\delta_a * \delta_b$, where $c = \sqrt{|G|}$.
(iii) $cv_\gamma(ab) = cv_\gamma(a)cv_\gamma(b)$.

Because (iii) implies that cv_γ is a character of G, hence v_γ is in the basis B_G, from which $v_\gamma = B_x$ for a unique $x \in G$. Then (5.3) follows from (i).

Proof of (i): Since γ is a linear functional, Theorem 2.2.1 guarantees the existence and uniqueness of v_γ such that $\gamma(B_g) = \langle B_g, v_\gamma \rangle$ for every $g \in G$.

Proof of (ii): For a, $b \in G$, the equation $\delta_{ab} = c\delta_a * \delta_b$ follows from the definition of convolution and the definition of δ_g. (Also, see Exercise 29 of the previous section.)

Proof of (iii): It follows from (i) and the linearity of γ that

$$\bar{\gamma}(\delta_g) = \overline{\langle \delta_g, v_\gamma \rangle} = \langle v_\gamma, \delta_g \rangle = v_\gamma(g)$$

for any $g \in G$. Hence,

$$cv_\gamma(ab) = c\bar{\gamma}(\delta_{ab}) = c^2\bar{\gamma}(\delta_a * \delta_b) = c\bar{\gamma}(\delta_a)c\bar{\gamma}(\delta_b) = cv_\gamma(a)cv_\gamma(b),$$

where we used (ii) and the assumption that γ preserves the multiplication.

Thus, we proved that there is a unique $x \in G$ such that $\gamma(f) = \hat{f}(x)$ for every $f \in V_G$.

Conversely, for a given $x \in G$, the map $\gamma \colon V_G \to \mathbb{C}$ defined by $\gamma(f) = \hat{f}(x)$ is obviously linear and not identically zero. Theorem 5.1.1 (iii) implies that γ is an algebra homomorphism. ■

There are two immediate consequences of Theorem 5.2.1; they are listed in Corollary 5.2.1 below after we reformulate the norm of linear functionals in terms of their arguments. By Theorem 2.2.1, to every linear functional γ on V_G there associates a unique vector $v_\gamma \in V_G$ such that $\gamma(f) = \langle f, v_\gamma \rangle$ for all $f \in V_G$, furthermore, $\|\gamma\| = \|v_\gamma\|$ (see (2.5)). Since, by the Schwarz inequality,

$$\|v_\gamma\| = \sup\big\{\, |\langle f, v_\gamma \rangle| \,:\, f \in V_G \text{ and } \|f\| = 1 \,\big\},$$

we have

$$\|\gamma\| = \sup\{\, |\gamma(f)| \,:\, f \in V_G \text{ and } \|f\| = 1 \,\}. \tag{5.4}$$

Equivalently, $\|\gamma\|$ is the smallest number such that the inequality $|\gamma(f)| \leq \|\gamma\|\|f\|$ holds for all $f \in V_G$. Thus, γ maps the closed unit ball, i.e., the set $\{f \in V_G \,:\, \|f\| \leq 1\}$, into the closed disc in $\mathbb{C}$ center at 0 and radius $\|\gamma\|$ (a closed disc with radius equal to zero is a point).

Corollary 5.2.1.

(i) *There are as many nonzero algebra homomorphisms on V_G as the number of elements in G.*

(ii) *The norm of any Banach algebra homomorphism on V_G does not exceed one.*

Proof. (i) For each $x \in G$, let γ_x be an algebra homomorphism on V_G defined by $\gamma_x(f) = \hat{f}(x)$. Then by Theorem 5.2.1 the correspondent $x \leftrightarrow \gamma_x$ is a one-to-one correspondent between G and the set of all nonzero algebra homomorphisms on V_G.

(ii) Let γ be a Banach algebra homomorphism on V_G. It is clear from the definition of the norm of γ that if $\gamma = 0$, then $\|\gamma\| = 0$. If $\gamma \neq 0$, then by Theorem 5.2.1 there is an element x in G such that $\gamma(f) = \hat{f}(x)$ for all $f \in V_G$. It follows from this equation and (5.4) that

$$\begin{aligned}
\|\gamma\| &= \sup\{\, |\gamma(f)| \,:\, \|f\| = 1 \,\} \\
&= \sup\{\, |\hat{f}(x)| \,:\, \|f\| = 1 \,\} \\
&= \sup\{\, |\langle f, B_x\rangle| \,:\, \|f\| = 1 \,\} && \text{(by (c3) of Theorem 2.3.1)} \\
&\leq \sup\{\, \|f\|\,\|B_x\| \,:\, \|f\| = 1 \,\} && \text{(the Schwarz inequality)} \\
&= 1 && \text{(since } \|f\| = \|B_x\| = 1). \quad \blacksquare
\end{aligned}$$

5.3 The Uncertainty Principle

In physics, the Heisenberg uncertainty principle states that it is impossible to measure a particle's position and momentum simultaneously. An equivalent statement in analysis says that it is impossible to localize both a function and its Fourier transform simultaneously. We describe an equivalent version of the uncertainty principle for functions defined on finite Abelian groups.

Recall that the support of a complex-valued function f defined on G is the set

$$\operatorname{supp}(f) = \left\{ g \in G \,:\, f(g) \neq 0 \right\}.$$

Theorem 5.3.1 (The uncertainty principle). *Let G be a finite Abelian group and let f be a complex-valued function defined on G. If f is not identically zero, then*

$$|G| \leq |\operatorname{supp}(f)||\operatorname{supp}(\hat{f})|.$$

Furthermore, if equality holds, then f is a constant on its support. Conversely, if f is a constant, then equality holds.

Proof. In this proof, we will have occasion to use the maximum value of $|f|$, that is, $\|f\|_\infty$. It is convenient to recall its definition (given in Exercise 34 at the end of Section 5.1) here:

$$\|f\|_\infty = \max\left\{ |f(g)| \,:\, g \in G \right\}.$$

Since for each $x \in G$, by the inversion formula,

$$f(x) = \sum_{g \in G} \hat{f}(g) B_g(x),$$

and since $|B_g(x)| = 1/\sqrt{|G|}$, by the triangle inequality, we have

$$|f(x)| \leq \frac{1}{\sqrt{|G|}} \sum_{g \in G} |\hat{f}(g)| = \frac{1}{\sqrt{|G|}} \left\langle |\hat{f}|, 1_{\operatorname{supp}(\hat{f})} \right\rangle,$$

where $1_{\operatorname{supp}(\hat{f})}$ is the characteristic function of the set $\operatorname{supp}(\hat{f})$. By the Schwarz inequality,

$$|f(x)| \leq \frac{1}{\sqrt{|G|}} \|\hat{f}\| \sqrt{|\operatorname{supp}(\hat{f})|},$$

whence

$$\|f\|_\infty \le \frac{1}{\sqrt{|G|}}\|\hat{f}\|\sqrt{|\text{supp}(\hat{f})|} = \frac{1}{\sqrt{|G|}}\|f\|\sqrt{|\text{supp}(\hat{f})|}$$

or, equivalently,

$$\|f\|_\infty^2|G| \le \|f\|^2|\text{supp}(\hat{f})|.$$

Since

$$\|f\|^2 = \sum_{g\in G}|f(g)|^2 \le \|f\|_\infty^2|\text{supp}(f)|,$$

we have

$$\|f\|_\infty^2|G| \le \|f\|^2|\text{supp}(\hat{f})| \le \|f\|_\infty^2|\text{supp}(f)||\text{supp}(\hat{f})|. \qquad (5.5)$$

If f is not identically zero, then $\|f\|_\infty \neq 0$, whence $|G| \le |\text{supp}(f)||\text{supp}(\hat{f})|$.

If f is a nonzero constant function, then $|\text{supp}(f)| = |G|$. By Theorem 4.1.1, $\hat{f}$ is supported only at the identity of G, thus $|\text{supp}(\hat{f})| = 1$. It is clear that $|G| = |\text{supp}(f)||\text{supp}(\hat{f})|$. Conversely, if $|G| = |\text{supp}(f)||\text{supp}(\hat{f})|$, then

(i) $|\text{supp}(f)| > 0$, i.e., $\|f\|_\infty \neq 0$,
(ii) $|\text{supp}(\hat{f})| > 0$, and
(iii) inequalities in (5.5) become equalities.

It follows that $\|f\|^2 = \|f\|_\infty^2|\text{supp}(f)|$, whence f is a constant on its support. ■

It follows from the uncertainty principle that the supports of f and $\hat{f}$ cannot both be small. That is, f and $\hat{f}$ cannot be localized to arbitrarily small subsets of G simultaneously.

Example 5.3.1. For $g \in G$, the function δ_g is supported only at g, i.e., $|\text{supp}(\delta_g)| = 1$. According to the uncertainty principle, the FT of δ_g vanishes nowhere on G. On the other hand, if f is a constant function, then $\hat{f}$ is zero everywhere except at one point and, by Theorem 4.1.1, that point is the identity 1.

Corollary 5.3.1. *If $f\colon \mathbb{Z}_n \to \mathbb{C}$ is a periodic function with period σ and $f(k) \neq 0$ for some $k \in \mathbb{Z}_n$, then*

$$|\text{supp}(f)| \geq \frac{n}{\sigma}.$$

Proof. The corollary follows from the uncertainty principle and Theorem 4.2.2. ■

6

A Reduction Theorem

By the Fundamental Theorem of Finite Abelian Groups, every finite Abelian group is a direct product of cyclic groups. We will show that the FT on a given finite Abelian group is the tensor product of the FT on the cyclic groups in its direct product decomposition. Thus, to understand the FT on finite Abelian groups, it suffices to investigate the FT on cyclic groups. This approach to reduction of the FT is to show that a similar reduction (or decomposition) holds for vector spaces of complex-valued functions on finite Abelian groups.

6.1 The Tensor Decomposition of Vector Spaces

Suppose that G is a finite Abelian group and V_G is the vector space associated with G. Then we can decompose V_G as a tensor product of smaller vector spaces according to the decomposition of G into smaller groups. To be precise, let $\mathcal{A}$ and $\mathcal{B}$ be finite Abelian groups and denote, in general, the characters of $\mathcal{A}$ by χ and those of $\mathcal{B}$ by μ. By Theorem 3.1.3 we have

$$\widehat{\mathcal{A}\times\mathcal{B}} = \hat{\mathcal{A}}\otimes\hat{\mathcal{B}} = \big\{\, \chi_a\otimes\mu_b \mid a\in\mathcal{A},\ b\in\mathcal{B} \,\big\}.$$

Here we recall from (3.1) that $\chi_a\otimes\mu_b$ is the complex-valued function on $\mathcal{A}\times\mathcal{B}$ defined by

$$\chi_a\otimes\mu_b(x,y) = \chi_a(x)\mu_b(y),$$

B. Luong, *Fourier Analysis on Finite Abelian Groups*, Applied and Numerical Harmonic Analysis, DOI 10.1007/978-0-8176-4916-6_6,

where $x \in \mathcal{A}$ and $y \in \mathcal{B}$. We extend this definition in an obvious way to include the tensor product of scalar multiples of characters. That is, if c is a complex number, then the tensor product of $c\chi_a$ and μ_b is the function $c\chi_a \otimes \mu_b \colon \mathcal{A} \times \mathcal{B} \to \mathbb{C}$ defined by

$$c\chi_a \otimes \mu_b(x, y) = c\chi_a(x)\mu_b(y). \tag{6.1}$$

Since $c\chi_a(x) = c(\chi_a(x))$, we have

$$c\chi_a \otimes \mu_b(x, y) = c\chi_a(x)\mu_b(y) = \chi_a(x)c\mu_b(y) = \chi_a \otimes c\mu_b(x, y),$$

whence

$$c(\chi_a \otimes \mu_b) = c\chi_a \otimes \mu_b = \chi_a \otimes c\mu_b. \tag{6.2}$$

In particular, when $c = 0$ we have $0(\chi_a \otimes \mu_b) = \chi_a \otimes 0 = 0 \otimes \mu_b = 0$.

Recall the definition of the set $B_{\mathcal{A}\times\mathcal{B}}$ from (3.6) that

$$B_{\mathcal{A}\times\mathcal{B}} = \frac{1}{\sqrt{|A||B|}}\widehat{\mathcal{A} \times \mathcal{B}} = \left\{ \frac{1}{\sqrt{|A||B|}}\chi_a \otimes \mu_b \mid a \in \mathcal{A},\, b \in \mathcal{B} \right\}.$$

Now, equation (6.2) allows us to write

$$\frac{1}{\sqrt{|A||B|}}\chi_a \otimes \mu_b = \frac{1}{\sqrt{|A|}}\chi_a \otimes \frac{1}{\sqrt{|B|}}\mu_b = B_a \otimes B_b,$$

so that

$$B_{\mathcal{A}\times\mathcal{B}} = \left\{ B_a \otimes B_b \mid a \in \mathcal{A},\ b \in \mathcal{B} \right\} = B_{\mathcal{A}} \otimes B_{\mathcal{B}}.$$

The set $B_{\mathcal{A}} \otimes B_{\mathcal{B}}$ is a basis for the vector space which we will define shortly. In preparation for the mentioned definition, we introduce the following term: a *linear combination* of the elements of $\hat{\mathcal{A}} \otimes \hat{\mathcal{B}}$ is a sum of the form

$$\sum_{a,\,b} c_{ab}\chi_a \otimes \mu_b,$$

where the sum is taken over all $a \in \mathcal{A}$, $b \in \mathcal{B}$, and $\{c_{ab} \mid a \in \mathcal{A} \text{ and } b \in \mathcal{B}\}$ is some set of complex constants. The set of all linear combinations of elements of $\hat{\mathcal{A}} \otimes \hat{\mathcal{B}}$ over $\mathbb{C}$ is a vector space with respect to the pointwise addition and scalar multiplication defined on page 27. This vector space, denoted by $V_{\mathcal{A}} \otimes V_{\mathcal{B}}$, is called the *tensor product* of $V_{\mathcal{A}}$ and $V_{\mathcal{B}}$. From this definition we see that $\hat{\mathcal{A}} \otimes \hat{\mathcal{B}}$ or, equivalently, $B_{\mathcal{A}} \otimes B_{\mathcal{B}}$ is a basis for $V_{\mathcal{A}} \otimes V_{\mathcal{B}}$.

On the other hand, $B_{\mathcal{A}} \otimes B_{\mathcal{B}} = B_{\mathcal{A}\times\mathcal{B}}$ is a basis for $V_{\mathcal{A}\times\mathcal{B}}$. Thus the vector spaces $V_{\mathcal{A}\times\mathcal{B}}$ and $V_{\mathcal{A}} \otimes V_{\mathcal{B}}$ have the same basis; hence they are equal. We record this result as a theorem.

Theorem 6.1.1. *If $\mathcal{A}$ and $\mathcal{B}$ are finite Abelian groups, then $V_{\mathcal{A}\times\mathcal{B}} = V_{\mathcal{A}} \otimes V_{\mathcal{B}}$.*

Warning. $B_{\mathcal{A}} \otimes B_{\mathcal{B}}$ is a set, not a vector space; an element in $B_{\mathcal{A}} \otimes B_{\mathcal{B}}$ equals the tensor product of an element in $B_{\mathcal{A}}$ and an element in $B_{\mathcal{B}}$. This is not true, in general, for elements in the vector space $V_{\mathcal{A}}\otimes V_{\mathcal{B}}$. An element in $V_{\mathcal{A}}\otimes V_{\mathcal{B}}$ is a linear combination of vectors in the basis $B_{\mathcal{A}} \otimes B_{\mathcal{B}}$.

Although none of the sets $B_{\mathcal{A}}$, $B_{\mathcal{B}}$, and $B_{\mathcal{A}} \otimes B_{\mathcal{B}}$ is a vector space, we call the set $B_{\mathcal{A}} \otimes B_{\mathcal{B}}$ the *tensor product of $B_{\mathcal{A}}$ and $B_{\mathcal{B}}$*. With this terminology, the character basis of a tensor product of (a finite number of) vector spaces is the tensor product of the character bases of each factor space. The basis $B_{\mathcal{A}} \otimes B_{\mathcal{B}}$ is called the *character basis for $V_{\mathcal{A}} \otimes V_{\mathcal{B}}$*.

Finally, it follows from the pointwise definition of addition and scalar multiplication for functions[1] that the defining equation (6.1) implies that the tensor product is a bilinear mapping from $V_{\mathcal{A}} \times V_{\mathcal{B}}$ to $V_{\mathcal{A}} \otimes V_{\mathcal{B}}$. To prove this, we note that by (6.2), it suffices to show that the equations

$$(B_a + B_\alpha) \otimes B_b = B_a \otimes B_b + B_\alpha \otimes B_b$$

$$B_a \otimes (B_b + B_\beta) = B_a \otimes B_b + B_a \otimes B_\beta$$

hold for all B_a, $B_\alpha \in B_{\mathcal{A}}$ and B_b, $B_\beta \in B_{\mathcal{B}}$. Since proofs for these two equations are similar, we prove only the latter equation by showing that the functions on both sides of the equality are equal at an arbitrary point $(x, y) \in \mathcal{A} \times \mathcal{B}$. For $(x, y) \in \mathcal{A} \times \mathcal{B}$, we have

$$\begin{aligned} B_a \otimes (B_b + B_\beta)(x, y) &= B_a(x)(B_b + B_\beta)(y) \\ &= B_a(x)[B_b(y) + B_\beta(y)] \\ &= B_a(x)B_b(y) + B_a(x)B_\beta(y) \end{aligned}$$

[1] Defined on page 27.

$$= B_a \otimes B_b(x, y) + B_a \otimes B_\beta(x, y)$$
$$= (B_a \otimes B_b + B_a \otimes B_\beta)(x, y).$$

Consequently, if $f_\alpha \in V_{\mathcal{A}}$ and $f_b \in V_{\mathcal{B}}$, then $f_\alpha \otimes f_b(x, y) = f_a(x)f_b(y)$ for all $(x, y) \in \mathcal{A} \times \mathcal{B}$.

We conclude this section by a note on the notation: we recall that

$$B_{\mathcal{A}\times\mathcal{B}} = \{B_a \otimes B_b \mid a \in \mathcal{A},\ b \in \mathcal{B}\}.$$

It follows also from the notation convention after Theorem 3.2.2 that

$$B_{\mathcal{A}\times\mathcal{B}} = \{B_{(a,\,b)} \mid a \in \mathcal{A},\ b \in \mathcal{B}\}.$$

Thus, for each pair (a, b), $B_{(a,\,b)} = B_\alpha \otimes B_\beta$ for some $\alpha \in \mathcal{A}$ and $\beta \in \mathcal{B}$. We choose the notation for the indices so that

$$B_{(a,\,b)} = B_a \otimes B_b. \tag{6.3}$$

In fact, we have used this indexing convention in (a special case) Example 3.1.2.

6.2 The Tensor Decomposition of the Fourier Transform

If $\mathcal{A}$ and $\mathcal{B}$ are finite Abelian groups, then it follows from (6.3) and the definition of the FT that the following chain of equations holds:

$$(B_a \otimes B_b)\hat{} = \hat{B}_{(a,\,b)} = \delta_{(a,\,b)}.$$

Since $\delta_{(a,\,b)} = \delta_a \otimes \delta_b$ (Exercise 36) and $\hat{B}_x = \delta_x$, we have $(B_a \otimes B_b)\hat{} = \hat{B}_a \otimes \hat{B}_b$; that is, $\mathcal{F}_{\mathcal{A}\times\mathcal{B}} = \mathcal{F}_{\mathcal{A}} \otimes \mathcal{F}_{\mathcal{B}}$ on the basis $B_{\mathcal{A}\times\mathcal{B}}$, where $\mathcal{F}_G$ is the FT on G and

$$\mathcal{F}_{\mathcal{A}} \otimes \mathcal{F}_{\mathcal{B}}(B_a \otimes B_b) = \mathcal{F}_{\mathcal{A}}(B_a) \otimes \mathcal{F}_{\mathcal{B}}(B_b) = \hat{B}_a \otimes \hat{B}_b.$$

The linearity and bilinearity properties of the FT and the tensor product, respectively, imply that $\mathcal{F}_{\mathcal{A}\times\mathcal{B}} = \mathcal{F}_{\mathcal{A}} \otimes \mathcal{F}_{\mathcal{B}}$ on the entire space $V_{\mathcal{A}\times\mathcal{B}}$.

Theorem 6.2.1. *If $\mathcal{A}$ and $\mathcal{B}$ are finite Abelian groups, then $\mathcal{F}_{\mathcal{A}\times\mathcal{B}} = \mathcal{F}_{\mathcal{A}} \otimes \mathcal{F}_{\mathcal{B}}$. Consequently, $(f_a \otimes f_b)\hat{} = \hat{f}_a \otimes \hat{f}_b$ for every $f_a \in V_{\mathcal{A}}$ and $f_b \in V_{\mathcal{B}}$.*

It follows from this theorem that the inner product in $V_{\mathcal{A}} \otimes V_{\mathcal{B}}$ when restricted to the subset $\{\alpha \otimes \beta \mid \alpha \in V_{\mathcal{A}},\, \beta \in V_{\mathcal{B}}\}$ equals the product of the inner products on factor spaces. A more precise statement of this is given in the following corollary.

Corollary 6.2.1. *Suppose that $\mathcal{A}$ and $\mathcal{B}$ are finite Abelian groups. The following relations hold for any $\alpha, \alpha' \in V_{\mathcal{A}}$ and $\beta, \beta' \in V_{\mathcal{B}}$:*

(i) $\langle \alpha \otimes \beta,\, \alpha' \otimes \beta' \rangle = \langle \alpha, \alpha' \rangle \langle \beta, \beta' \rangle$;
(ii) $\|\alpha \otimes \beta\| = \|\alpha\| \|\beta\|$;
(iii) $(\alpha \otimes \beta)^* = \alpha^* \otimes \beta^*$; *consequently, by Theorem* 6.1.1,

$$(V_{\mathcal{A}} \otimes V_{\mathcal{B}})^* = V_{\mathcal{A}}^* \otimes V_{\mathcal{B}}^*.$$

Proof. It is clear that (ii) and (iii) are consequences of (i), so we prove (i) only. Since the inner product and the tensor product are both bilinear, it suffices to prove the theorem for basis elements only. Recall that the sets

$$\{B_a \mid a \in \mathcal{A}\},\ \{B_b \mid b \in \mathcal{B}\},\ \text{ and }\ \{B_{(a,\,b)} = B_a \otimes B_b \mid a \in \mathcal{A},\, b \in \mathcal{B}\}$$

are bases of $V_{\mathcal{A}}$, $V_{\mathcal{B}}$, and $V_{\mathcal{A}} \otimes V_{\mathcal{B}}$, respectively. For $a, a' \in \mathcal{A}$ and $b, b' \in \mathcal{B}$, we have

$$\begin{aligned}
&\langle B_a \otimes B_b, B_{a'} \otimes B_{b'} \rangle \\
&\quad = \langle B_a \otimes B_b, B_{(a',\,b')} \rangle \\
&\quad = (B_a \otimes B_b)\hat{}(a', b') \qquad \text{(by (c3) of Theorem 2.3.1)} \\
&\quad = \hat{B}_a \otimes \hat{B}_b(a', b') \qquad \text{(by Theorem 6.2.1)} \\
&\quad = \hat{B}_a(a')\hat{B}_b(b') \\
&\quad = \langle B_a, B_{a'} \rangle \langle B_b, B_{b'} \rangle.
\end{aligned}$$

The proof is complete. ■

Another consequence of Theorem 6.2.1 is that the matrix of the FT can be decomposed into a tensor product of smaller matrices. This is made precise in the following corollary, the proof of which is left as an exercise.

Corollary 6.2.2. *Let $\mathcal{A}$ and $\mathcal{B}$ be finite Abelian groups. Assume that*

(i) *$M_{\mathcal{A}}$ is the matrix of the FT on $\mathcal{A}$,*
(ii) *$M_{\mathcal{B}}$ is the matrix of the FT on $\mathcal{B}$,*
(iii) *$M_{\mathcal{A}\times\mathcal{B}}$ is the matrix of the FT on $\mathcal{A}\times\mathcal{B}$,*

and these matrices are formed with respect to the standard bases for each of the corresponding vector spaces.[2] *Then we have $M_{\mathcal{A}\times\mathcal{B}} = M_{\mathcal{A}} \otimes M_{\mathcal{B}}$.*

Note. If $M_{\mathcal{A}} = (m_{st})_{p\times p'}$ and $M_{\mathcal{B}}$ has dimension $q \times q'$, then $M_{\mathcal{A}} \otimes M_{\mathcal{B}} = (m_{st}M_{\mathcal{B}})_{pq\times p'q'}$. The tensor product of matrices is also called the *Kronecker product*.

Example 6.2.1. Consider the group $\mathbb{Z}_2$. By Example 3.1.3, it is easy to verify that

$$M_{\mathbb{Z}_2} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Hence, by Corollary 6.2.2, we have $M_{\mathbb{Z}_2^m} = M_{\mathbb{Z}_2} \otimes \cdots \otimes M_{\mathbb{Z}_2}$ (m factors).

Theorem 6.2.1 also implies a formula known as the Poisson summation formula.

Theorem 6.2.2 (The Poisson summation formula). *If $\mathcal{A}$ and $\mathcal{B}$ are finite Abelian groups and f is a complex-valued function defined on $\mathcal{A}\times\mathcal{B}$, then the following formula holds:*

$$\frac{1}{\sqrt{|\mathcal{A}|}}\sum_{a\in\mathcal{A}} f(a,1) = \frac{1}{\sqrt{|\mathcal{B}|}}\sum_{b\in\mathcal{B}} \hat{f}(1,b).$$

[2] First, enumerate $\mathcal{A}$ and $\mathcal{B}$ by writing $\mathcal{A} = \{a_s \mid s = 1,\ldots,m\}$ and $\mathcal{B} = \{b_t \mid t = 1,\ldots,n\}$. Next, we write δ_s for δ_{a_s} and $\delta_{(s,\,t)}$ for $\delta_{(a_s,\,b_t)}$. The standard bases for the vector spaces $V_{\mathcal{A}}$, $V_{\mathcal{B}}$, and $V_{\mathcal{A}\times\mathcal{B}}$, respectively, are $\{\delta_s \mid s = 1,\ldots,m\}$, $\{\delta_t \mid t = 1,\ldots,m\}$, and $\{\delta_{(s,\,t)} \mid s = 1,\ldots,m,\, t = 1,\ldots,m\}$, where the latter basis is ordered with the lexicographical ordering.

Proof. Since $V_{\mathcal{A}\times\mathcal{B}} = V_{\mathcal{A}} \otimes V_{\mathcal{B}}$ and the set $B_{\mathcal{A}} \otimes B_{\mathcal{B}} = \{B_a \otimes B_b \mid a \in \mathcal{A},\ b \in \mathcal{B}\}$ is a basis for $V_{\mathcal{A}} \otimes V_{\mathcal{B}}$, it follows that any $f \in V_{\mathcal{A}\times\mathcal{B}}$ is a linear combination of elements in $B_{\mathcal{A}} \otimes B_{\mathcal{B}}$; i.e.,

$$f = \sum_{s,\, t} c_{st} B_s \otimes B_t$$

for some set of constants $\{c_{st}\}$, where the sum is taken over all $s \in \mathcal{A}$, $t \in \mathcal{B}$. For $a \in \mathcal{A}$, the evaluation of f at $(a, 1)$ gives

$$\begin{aligned} f(a,1) &= \sum_{s,\, b} c_{sb} B_s \otimes B_b(a,1) \\ &= \sum_{s,\, b} c_{sb} B_s(a) B_b(1) \\ &= \frac{1}{\sqrt{|A||B|}} \sum_{s,\, b} c_{sb} \chi_s(a), \end{aligned}$$

where $b \in \mathcal{B}$. Hence, by Corollary 3.2.1 we have

$$\begin{aligned} \frac{1}{\sqrt{|A|}} \sum_{a \in \mathcal{A}} f(a,1) &= \frac{1}{|A|\sqrt{|B|}} \sum_{s,\, b} c_{sb} \sum_{a \in \mathcal{A}} \chi_s(a) \\ &= \frac{1}{\sqrt{|B|}} \sum_{b \in \mathcal{B}} c_{1b} \\ &= \frac{1}{\sqrt{|B|}} \sum_{b \in \mathcal{B}} \sum_{s,\, t} c_{st} \delta_s(1) \delta_t(b) \\ &= \frac{1}{\sqrt{|B|}} \sum_{b \in \mathcal{B}} \sum_{s,\, t} c_{st} \delta_s \otimes \delta_t(1,b) \\ &= \frac{1}{\sqrt{|B|}} \sum_{b \in \mathcal{B}} \sum_{s,\, t} c_{st} \hat{B}_s \otimes \hat{B}_t(1,b) \\ &= \frac{1}{\sqrt{|B|}} \sum_{b \in \mathcal{B}} \hat{f}(1,b). \qquad \blacksquare \end{aligned}$$

If $\mathcal{A}$ and $\mathcal{B}$ are subgroups of a finite Abelian group G and $G = \mathcal{A}\mathcal{B} = \{ab \mid a \in \mathcal{A},\ b \in \mathcal{B}\}$ is the internal direct product of $\mathcal{A}$ and $\mathcal{B}$, and if $f \in V_G$, then the Poisson formula has the form

$$\frac{1}{\sqrt{|\mathcal{A}|}} \sum_{a \in \mathcal{A}} f(a) = \frac{1}{\sqrt{|\mathcal{B}|}} \sum_{b \in \mathcal{B}} \hat{f}(b).$$

This formula equates a sum over a set $\mathcal{A}$ with a sum over a set $\mathcal{B}$, which may be useful if one of these sets is small and the other is large.

Exercises.

35. Show that the FT is not self-adjoint on the space $V_{\mathbb{Z}_2^k} \otimes V_{\mathbb{Z}_n^m}$, where $n > 2$.

36. Suppose that $\mathcal{A}$ and $\mathcal{B}$ are finite Abelian groups and that $G = \mathcal{A} \times \mathcal{B}$. Prove that $\delta_{(a,\,b)} = \delta_a \otimes \delta_b$, where $a \in \mathcal{A}$ and $b \in \mathcal{B}$.

37. Prove Corollary 6.2.2.

38. Suppose that $\mathcal{A}$ and $\mathcal{B}$ are finite Abelian groups. Prove that the formula

$$\frac{1}{\sqrt{|\mathcal{A}|}} \sum_{a \in \mathcal{A}} \hat{f}(a, 1) = \frac{1}{\sqrt{|\mathcal{B}|}} \sum_{b \in \mathcal{B}} f(1, b)$$

holds for every complex-valued function f defined on $\mathcal{A} \times \mathcal{B}$.

6.3 The Fourier Transform and Isometries

Suppose that $h \colon G_1 \to G_2$ is an isomorphism of finite Abelian groups. First, we show that $V_{G_2} \simeq V_{G_1}$ as follows: By Theorem 3.1.2, $\hat{G}_2 \cong \hat{G}_1$, moreover, this isomorphism is given by $h^\star$, the pullback by h of complex-valued functions on G_2. Since $\hat{G}_j$ is a basis for V_{G_j}, $j = 1, 2$, the linear extension of $h^\star$ to V_{G_2}, also denoted by $h^\star$, is a one-to-one mapping from V_{G_2} onto V_{G_1}. To see that $h^\star$ preserves the inner product, let f_2 and f_2' be elements of V_{G_2}. We have

$$\begin{aligned} \langle h^\star f_2, h^\star f_2' \rangle &= \sum_{g_1 \in G_1} h^\star f_2(g_1) \overline{h^\star f_2'}(g_1) \\ &= \sum_{g_1 \in G_1} f_2(h(g_1)) \bar{f}_2'(h(g_1)) \end{aligned}$$

$$
\begin{aligned}
&= \sum_{g_2 \in G_2} f_2(g_2)\bar{f}_2'(g_2) \\
&= \langle f_2, f_2' \rangle.
\end{aligned}
$$

Theorem 6.3.1. *Isomorphic finite Abelian groups induce isometric associated finite-dimensional inner product spaces. Furthermore, if G_1 and G_2 are finite Abelian groups, then*

$$G_1 \overset{h}{\cong} G_2 \Rightarrow V_{G_2} \overset{h^\star}{\simeq} V_{G_1},$$

where $h^\star$ is the pullback by h.

Second, we show that the FT and $h^\star$ commute, that is, the following diagram is commutative:

$$\begin{tikzcd}
V_{G_2} \arrow[r, "h^\star"] \arrow[d, "\hat{}"'] & V_{G_1} \arrow[d, "\hat{}"] \\
V_{G_2} \arrow[r, "h^\star"] & V_{G_1}
\end{tikzcd} \tag{6.4}$$

Since $h^\star$ and the FT are linear, it suffices to show that these two operators commute on the basis B_{G_2} of the vector space V_{G_2}. If $x \in G_2$, then, by (3.8),

$$
\begin{aligned}
(h^\star B_x)\hat{} &= \sum_{g \in G_1} \langle h^\star B_x, B_g \rangle \delta_g \\
&= \sum_{g \in G_1} \langle B_{h^{-1}(x)}, B_g \rangle \delta_g = \delta_{h^{-1}(x)} = h^\star \delta_x = h^\star \hat{B}_x.
\end{aligned}
$$

Thus we have proved the following theorem.

Theorem 6.3.2. *If G_1 and G_2 are isomorphic finite Abelian groups, then the diagram* (6.4) *is commutative.*

6.4 Reduction to Finite Cyclic Groups

Suppose that G is a finite Abelian group. By the Fundamental Theorem of Finite Abelian Groups, there are positive integers $n_1, \ldots, n_m$ and an isomorphism h such that

$$\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m} \overset{h}{\cong} G.$$

The vector spaces associated with these groups are related as follows:

$$V_G \overset{h^\star}{\simeq} V_{\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}} = V_{\mathbb{Z}_{n_1}} \otimes \cdots \otimes V_{\mathbb{Z}_{n_m}},$$

where the isometry $h^\star$ is given by Theorem 6.3.1 and the equality is guaranteed by Theorem 6.1.1. By Theorem 6.3.2, the following diagram is commutative:

$$\begin{tikzcd}
V_G \arrow[r, "h^\star"] \arrow[d, "\hat{}"'] & V_{\mathbb{Z}_{n_1}} \otimes \cdots \otimes V_{\mathbb{Z}_{n_m}} \arrow[d, "\hat{}"] \\
V_G \arrow[r, "h^\star"] & V_{\mathbb{Z}_{n_1}} \otimes \cdots \otimes V_{\mathbb{Z}_{n_m}} .
\end{tikzcd}$$

Consequently,

$$\big(h^\star f\big)\hat{} = h^\star \hat{f} \tag{6.5}$$

for all $f \in V_G$. For a given $f \in V_G$, we have

$$h^\star f = \sum_{k_1,\ldots,k_m} c(k_1,\ldots,k_m) B_{k_1} \otimes \cdots \otimes B_{k_m}, \tag{6.6}$$

where, for each $j = 1,\ldots,m$, k_j runs over $\mathbb{Z}_{n_j}$, B_{k_j} is an element of the character basis for $V_{\mathbb{Z}_{n_j}}$, and $c(k_1,\ldots,k_m)$ is a constant. It follows from (6.5), (6.6), Theorem 6.2.1, and the identity $\hat{B}_{k_j} = \delta_{k_j}$ that

$$h^\star \hat{f} = \sum_{k_1,\ldots,k_m} c(k_1,\ldots,k_m) \delta_{k_1} \otimes \cdots \otimes \delta_{k_m}.$$

Thus

$$\hat{f} = \sum_{k_1,\ldots,k_m} c(k_1,\ldots,k_m) (h^\star)^{-1} (\delta_{k_1} \otimes \cdots \otimes \delta_{k_m}),$$

where the inverse of $h^\star$ is the pullback by h^{-1}, i.e., $(h^\star)^{-1} = (h^{-1})^\star$. This result is concluded in the following theorem.

Theorem 6.4.1. *The FT is completely determined, up to an isometry, by the transforms on $V_{\mathbb{Z}_n}$ (for some positive values of n). Furthermore, the isometry is the pullback by the isomorphism of groups given by the fundamental theorem of finite Abelian groups.*

A note about the FT on G, where G is a finite non-Abelian group: let n be an integer greater than 2 and consider the dihedral group D_n, which is defined at the end of Section 1.1 of Chapter 1 as

$$D_n = \left\{ a^s b^t \mid s = 0, 1,\ 0 \leq t < n,\ a^2 = b^n = 1,\ ab = b^{-1}a \right\}.$$

Suppose that χ is a character of D_n. Then

(i) $\chi(a)^2 = \chi(a^2) = \chi(1) = 1$. Thus, $\chi(a) = \pm 1$.

(ii) From the relation $ab = b^{-1}a$ we have

$$\chi(a)\chi(b) = \chi(ab) = \chi(b^{-1}a) = \chi(b^{-1})\chi(a) = \chi(b)^{-1}\chi(a),$$

whence $\chi(b)^2 = 1$ or $\chi(b) = \pm 1$. Hence, $\chi(b)$ can have at most two values, namely, ± 1.

Since elements of D_n are of the form $a^s b^t$ and $\chi(a^s b^t) = \chi(a)^s \chi(b)^t$, the character χ is uniquely determined once the values of $\chi(a)$ and $\chi(b)$ are given. From (i) there are two choices for $\chi(a)$ and from (ii) there are at most two choices for $\chi(b)$, thus there are at most four possible choices for the pairs $\chi(a)$ and $\chi(b)$. It follows that there are at most four possible characters of D_n, therefore $|\hat{D}_n| \leq 4 < |D_n|$. In particular, if $n = 3$, then $\chi(b)^3 = 1$, which implies that $\chi(b) = 1$. The smallest non-Abelian group D_3 has six elements whereas its character group $\hat{D}_3$ has only two elements. This shows that any generalization of the FT to finite non-Abelian groups must be more subtle than that for finite Abelian groups.

7

Eigenvalues and Eigenvectors of the Fourier Transform

Having reduced the general theory of the FT on finite Abelian groups to the theory of the FT on finite cyclic groups, it suffices to study the FT of functions defined on the cyclic group $\mathbb{Z}_n$ for an arbitrary value of n, where $n > 1$. Our next goals are the following:

- Determine the form of eigenvectors of the FT (Section 7.2).
- Find the spectral decomposition of the FT on $\mathbb{Z}_n$ or, equivalently, the decomposition of the space $V_{\mathbb{Z}_n}$ as a direct sum of its invariant subspaces (Section 7.3).
- Determine the multiplicity of the eigenvalues of the FT (Section 7.5).

We will use symmetric and antisymmetric functions on $\mathbb{Z}_n$ to achieve these goals.

7.1 Symmetric and Antisymmetric Functions

A function $F\colon \mathbb{Z}_n \to \mathbb{C}$ is called *symmetric* if $F(-x) = F(x)$ and *antisymmetric* if $F(-x) = -F(x)$, where $-x$ is the inverse of x in $\mathbb{Z}_n$. By this definition, it is necessary that $F(0) = 0$ for every antisymmetric function F. Note that since $x = -x$ for $x \in \mathbb{Z}_2$ every function in $V_{\mathbb{Z}_2}$ is symmetric.

Symmetric and antisymmetric functions defined on $\mathbb{Z}_n$ are similar to even and odd real-valued functions defined on the interval $[-c, c]$ (or on $\mathbb{R}$), where $c \in \mathbb{R}$ and $c > 0$. For $n = 2k + 1$, an odd positive integer, we can consider $\mathbb{Z}_n = \{-k, \ldots, 0, \ldots, k\}$. Then

B. Luong, *Fourier Analysis on Finite Abelian Groups*, Applied and Numerical Harmonic Analysis, DOI 10.1007/978-0-8176-4916-6_7,

symmetric functions have equal values when their arguments are symmetric about zero.

Geometrically, the values of an antisymmetric function defined on $\mathbb{Z}_n$ are symmetric about the origin in the complex plane $\mathbb{C}$, while its nonzero arguments (i.e., $x \neq 0$) are "symmetric about the point $n/2$."

A linear combination of a finite number of symmetric functions is a symmetric function; that is, if $f_1, \dots, f_k$ are symmetric functions, then the sum $c_1 f_1 + \cdots + c_k f_k$ is symmetric for any constants $c_1, \dots, c_k$. Thus, symmetric functions on $\mathbb{Z}_n$ form a subspace of the vector space $V_{\mathbb{Z}_n}$. Similarly, antisymmetric functions on $\mathbb{Z}_n$ form a subspace of $V_{\mathbb{Z}_n}$. In general, without indication of the dependency on n, we denote the vector spaces of symmetric and antisymmetric functions by V_s and V_a, respectively.

Suppose that f is a complex-valued function on $\mathbb{Z}_n$. We define two functions f^s and f^a on $\mathbb{Z}_n$ in terms of f by setting

$$f^s(x) = \frac{f(x) + f(-x)}{2} \quad \text{and} \quad f^a(x) = \frac{f(x) - f(-x)}{2}.$$

Then it is clear that f^s is symmetric, f^a is antisymmetric, and $f = f^s + f^a$. Thus, we have decomposed f into a sum of symmetric and antisymmetric functions. Further, this decomposition is unique (Exercise 39). It follows that the vector space $V_{\mathbb{Z}_n}$ equals the direct sum of the vector spaces of symmetric and antisymmetric functions, that is, $V_{\mathbb{Z}_n} = V_s \oplus V_a$.

The functions f^s and f^a are called the *symmetric* and *antisymmetric parts of* f, respectively.

Next, we show that V_s and V_a are invariant subspaces of the FT; that is, $\widehat{V_s} \subset V_s$ and $\widehat{V_a} \subset V_a$, where$\widehat{V_s} = \{\hat{f} \mid f \in V_s\}$ and similarly for $\widehat{V_a}$.[1]

Theorem 7.1.1. *A function $f\colon \mathbb{Z}_n \to \mathbb{C}$ is symmetric (resp. antisymmetric) if and only if $\hat{f}$ is symmetric (resp. antisymmetric).*

[1] A note on notation: when V is a vector space of complex-valued functions, we use the notation $\widehat{V}$ to denote the set $\{\hat{f} \mid f \in V\}$. This notation is not to be confused with the character group of V. Being a vector space, V is not a finite set; on the other hand, except for the definition of characters, we consider the character groups only for finite groups. Thus, there should be no confusion.

Proof. Since

$$\hat{f}(-x) = \frac{1}{\sqrt{n}} \sum_{y \in \mathbb{Z}_n} e^{-\frac{2\pi i}{n} x(-y)} f(y) = \frac{1}{\sqrt{n}} \sum_{z \in \mathbb{Z}_n} e^{-\frac{2\pi i}{n} xz} f(-z),$$

where $z = -y$, we have

$$\hat{f}(-x) = \begin{cases} \hat{f}(x) & \text{if } f \text{ is symmetric,} \\ -\hat{f}(x) & \text{if } f \text{ is antisymmetric.} \end{cases}$$

That is, the FT of symmetric (resp. antisymmetric) functions are symmetric (resp. antisymmetric).

The converse follows from the equation $\hat{\hat{f}}(x) = f(-x)$, which was proved earlier in Theorem 4.1.2. ■

Since the FT is an isometry, we have $\widehat{V_s} = V_s$ and $\widehat{V_a} = V_a$; therefore, $\widehat{V_{\mathbb{Z}_n}} = \widehat{V_s} \oplus \widehat{V_a}$.

In the remainder of this section, we show that the dimension of V_s is $\lfloor n/2 \rfloor + 1$, where, for a real number x, $\lfloor x \rfloor$ denotes the greatest integer less than or equal to x. Since the dimension of $V_{\mathbb{Z}_n}$ equals n, it follows that the dimension of V_a equals $\lceil n/2 \rceil - 1$, where, for a real number x, $\lceil x \rceil$ denotes the least integer greater than or equal to x. That is,

$$\begin{aligned} \dim V_s &= \lfloor n/2 \rfloor + 1, \\ \dim V_a &= \lceil n/2 \rceil - 1. \end{aligned} \tag{7.1}$$

We prove the first equation in (7.1) by constructing an explicit basis for V_s. To make preparation for a proof we decompose each function B_j in the character basis $B_{\mathbb{Z}_n} = \{B_j \mid j \in \mathbb{Z}_n\}$ for the space $V_{\mathbb{Z}_n}$ into a unique sum of symmetric and antisymmetric functions as

$$B_j(x) = \frac{B_j(x) + B_j(-x)}{2} + \frac{B_j(x) - B_j(-x)}{2},$$

where $x \in \mathbb{Z}_n$. Since $B_j(-x) = B_{-j}(x)$, the previous equation becomes

$$B_j(x) = \frac{B_j(x) + B_{-j}(x)}{2} + \frac{B_j(x) - B_{-j}(x)}{2}.$$

Similarly, we have

$$B_{-j}(x) = \frac{B_j(x) + B_{-j}(x)}{2} - \frac{B_j(x) - B_{-j}(x)}{2}.$$

Notice the functions B_j and B_{-j} have the same symmetric parts. Thus, among the symmetric parts of the functions B_j, for $j = 0, \ldots, n-1$, there are at most $\lfloor n/2 \rfloor + 1$ distinct functions, namely, $(B_j + B_{-j})/2$ for $j = 0, \ldots, \lfloor n/2 \rfloor$. In fact, these functions are pairwise distinct. The truth of the last sentence is settled once we prove our objective that the set

$$\mathcal{S} = \left\{ \frac{B_j + B_{-j}}{2} \;\middle|\; j = 0, \ldots, \lfloor n/2 \rfloor \right\}$$

is an orthogonal basis for V_s (hence $\dim V_s = \lfloor n/2 \rfloor + 1$). We prove this in two steps:

(i) The functions in $\mathcal{S}$ are pairwise orthogonal (hence they are linearly independent); i.e., for each fixed pair of indices j and k, the number $\langle B_j + B_{-j}, B_k + B_{-k} \rangle$ is zero if $j \neq k$, and is nonzero if $j = k$.

(ii) The set $\mathcal{S}$ spans V_s, i.e., every symmetric function on $\mathbb{Z}_n$ can be written as a linear combination of functions in $\mathcal{S}$.

The two equations

$$\langle B_p, B_q \rangle = \begin{cases} 1 & \text{if } p = q, \\ 0 & \text{if } p \neq q, \end{cases}$$

for all p, $q \in \mathbb{Z}_n$, and

$$\begin{aligned} &\langle B_j + B_{-j}, B_k + B_{-k} \rangle \\ &\qquad = \langle B_j, B_k \rangle + \langle B_j, B_{-k} \rangle + \langle B_{-j}, B_k \rangle + \langle B_{-j}, B_{-k} \rangle \end{aligned}$$

imply (i). To prove (ii) we note that any $f \in V_{\mathbb{Z}_n}$ can be expressed uniquely as a linear combination of elements in the basis $\{B_j \mid j \in \mathbb{Z}_n\}$ as

$$f = \sum_{j \in \mathbb{Z}_n} \langle f, B_j \rangle B_j.$$

The decomposition $B_j = B_j^s + B_j^a$, where

$$B_j^s = \frac{B_j + B_{-j}}{2} \quad \text{and} \quad B_j^a = \frac{B_j - B_{-j}}{2}$$

are the symmetric and antisymmetric parts of B_j, respectively, leads to

$$f = \sum_{j \in \mathbb{Z}_n} \langle f, B_j \rangle B_j^s + \sum_{j \in \mathbb{Z}_n} \langle f, B_j \rangle B_j^a.$$

If f is symmetric, then the antisymmetric part of f is zero, i.e.,

$$\sum_{j \in \mathbb{Z}_n} \langle f, B_j \rangle B_j^a = 0,$$

whence

$$f = \sum_{j \in \mathbb{Z}_n} \langle f, B_j \rangle B_j^s. \tag{7.2}$$

Since f is an arbitrary element of V_s and, for $j > \lfloor n/2 \rfloor$, B_j^s is one of the functions in $\mathcal{S}$, equation (7.2) shows that $\mathcal{S}$ spans V_s.

To obtain an orthonormal basis for V_s, we normalize the orthogonal basis $\mathcal{S}$. If

$$\epsilon_j = \begin{cases} 2 & \text{if } j = 0 \text{ or if } n \text{ is even and } j = n/2, \\ \sqrt{2} & \text{otherwise,} \end{cases}$$

i.e., ϵ_j is the norm of the function $B_j + B_{-j}$, then the set

$$B_{\text{sym}} = \left\{ \frac{B_j + B_{-j}}{\epsilon_j} \;\middle|\; j = 0, \ldots, \lfloor n/2 \rfloor \right\} \tag{7.3}$$

obtained from $\mathcal{S}$ by scaling its elements, the jth element by the factor $2/\epsilon_j$, is an orthonormal basis for V_s. Thus (7.1) is proved.

Similarly, the set

$$B_{\text{antisym}} = \left\{ \frac{B_j - B_{-j}}{\sqrt{2}} \;\middle|\; j = 1, \ldots, \lceil n/2 \rceil - 1 \right\}$$

is an orthonormal basis of the vector space V_a of antisymmetric functions on $\mathbb{Z}_n$ for $n > 2$.

Since the FT preserves the norm of vectors and is invariant on V_s and V_a, it follows from the definition of the FT that the sets

$$\Delta_{\mathrm{sym}} = \left\{ \frac{\delta_j + \delta_{-j}}{\epsilon_j} \;\middle|\; j = 0, \ldots, \lfloor n/2 \rfloor \right\}$$

and

$$\Delta_{\mathrm{antisym}} = \left\{ \frac{\delta_j - \delta_{-j}}{\sqrt{2}} \;\middle|\; j = 1, \ldots, \lceil n/2 \rceil - 1 \right\}$$

are also orthonormal bases of the vector spaces V_s and V_a of symmetric and antisymmetric functions on $\mathbb{Z}_n$, respectively. We note that the sets (i.e., bases) B_{antisym} and $\Delta_{\mathrm{antisym}}$ make sense only when $n > 2$, for otherwise, i.e., if $n = 2$, they are empty since there are no antisymmetric functions on $\mathbb{Z}_2$.

Remark. Since $B_j(k) = \frac{1}{\sqrt{n}} e^{\frac{2\pi i}{n} jk}$ for j, $k \in \mathbb{Z}_n$, we have

$$\frac{B_j(k) + B_{-j}(k)}{2} = \frac{1}{\sqrt{n}} \cos\left(\frac{2\pi}{n} jk\right)$$

and

$$\frac{B_j(k) - B_{-j}(k)}{2} = \frac{1}{\sqrt{n}} i \sin\left(\frac{2\pi}{n} jk\right).$$

Exercises.

39. Suppose that $n > 2$ and $f \in V_{\mathbb{Z}_n}$. Show that the decomposition $f = f^s + f^a$ is unique.

40. Suppose that $n > 2$ and $f \in V_{\mathbb{Z}_n}$. Show that f is symmetric (resp. antisymmetric) if and only if $\check{f}$ is symmetric (resp. antisymmetric).

7.2 Eigenvalues and Eigenvectors

As a linear operator on finite-dimensional vector spaces over the field of complex numbers, which is algebraically closed, the FT has eigenvalues and eigenvectors. The purpose of this section is to determine the form of its eigenvectors and to show that the set of eigenvalues of the FT on $\mathbb{Z}_n$ is $\{\pm 1\}$ if $n = 2$, and is $U_4 = \{\pm 1, \pm i\}$, the set of the 4th roots of unity, if $n > 2$.

It follows from Theorem 4.1.2 that the FT composed with itself four times is the identity operator on V_{Z_n}, that is, $\mathcal{F}^4 = \mathcal{F}\mathcal{F}\mathcal{F}\mathcal{F} = I$. Thus, if λ is an eigenvalue of the FT and f is a corresponding eigenvector (hence, f is not identically zero), then $f = \mathcal{F}^4(f) = \lambda^4 f$. Hence, we have $\lambda^4 = 1$. Therefore, the set of eigenvalues of the FT is a subset of the set of 4th roots of unity.

If $n = 2$, then $x = -x$ for every $x \in \mathbb{Z}_2$. It follows that the FT composed with itself once is the identity operator on $V_{\mathbb{Z}_2}$, that is, $\mathcal{F}^2 = I$.

Theorem 7.2.1. *Suppose that f is a complex-valued function defined on $\mathbb{Z}_n$. Then*

(i) *f is symmetric if and only if $\hat{\hat{f}} = f$;*

(ii) *f is antisymmetric if and only if $\hat{\hat{f}} = -f$;*

(iii) *f is a non-identically zero symmetric function if and only if $\hat{f} \pm f$ is an eigenvector of the FT corresponding to the eigenvalue ± 1, respectively;*

(iv) *f is a non-identically zero antisymmetric function if and only if $\hat{f} \pm if$ is an eigenvector of the FT corresponding to the eigenvalue $\pm i$, respectively.*

Proof. Statements (i) and (ii) follow directly from Theorem 4.1.2. Statements (iii) and (iv) have similar proofs, and as an illustration we prove only part of (iv). If f is a non-identically zero antisymmetric function, then by (ii) the function $\hat{f} + if$ is an eigenvector of the FT corresponding to the eigenvalue i. Conversely, if $\hat{f} + if$ is an eigenvector of the FT corresponding to the eigenvalue i, then f is not identically zero (since $\hat{f} + if$ is not identically zero) and

$$i(\hat{f} + if) = (\hat{f} + if)\hat{} = \hat{\hat{f}} + i\hat{f},$$

whence $-f = \hat{\hat{f}}$. Hence, by (ii), f is antisymmetric. ■

Corollary 7.2.1. *The set of eigenvalues of the FT on $\mathbb{Z}_n$ is $\{1, -1\}$ if $n = 2$ and is $\{1, -1, i, -i\}$ if $n > 2$.*

In general, if a function defined on $\mathbb{Z}_n$ is an eigenvector of the FT, then it is either symmetric or antisymmetric. This fact is a consequence of the following theorem.

Theorem 7.2.2. *Suppose that a complex-valued function f defined on $\mathbb{Z}_n$ is an eigenvector of the FT corresponding to the eigenvalue λ. Then*

(i) *f is symmetric if and only if $\lambda = \pm 1$,*
(ii) *f is antisymmetric if and only if $\lambda = \pm i$.*

Proof. Assume that f is an eigenvector of the FT corresponding to the eigenvalue λ. Then (i) and (ii) follow from the equations $f(-x) = \hat{\hat{f}}(x) = \lambda^2 f(x)$. ■

The following theorem states that eigenvectors of the FT must have either the form $\hat{\alpha} \pm \alpha$ for some symmetric function α or $\hat{\beta} \pm i\beta$ for some antisymmetric function β.

Theorem 7.2.3. *Suppose that f is a complex-valued function defined on $\mathbb{Z}_n$. Then the following statements are true*:

(i) *f is an eigenvector of the FT corresponding to the eigenvalue ± 1 if and only if $f = \hat{\alpha} \pm \alpha$, respectively, for some non-identically zero symmetric function α.*
(ii) *f is an eigenvector of the FT corresponding to the eigenvalue $\pm i$ if and only if $f = \hat{\beta} \pm i\beta$, respectively, for some non-identically zero antisymmetric function β.*

Proof. Suppose that f is an eigenvector of the FT corresponding to the eigenvalue λ.

(i) If $\lambda = \pm 1$, then, according to Theorem 7.2.2, f is symmetric. Thus the function α defined by

$$\alpha = \begin{cases} f/2 & \text{if } \lambda = 1, \\ -f/2 & \text{if } \lambda = -1, \end{cases}$$

is non-identically zero and symmetric. It is clear that

$$f = \begin{cases} \hat{\alpha} + \alpha & \text{if } \lambda = 1, \\ \hat{\alpha} - \alpha & \text{if } \lambda = -1. \end{cases}$$

The converse follows from (iii) of Theorem 7.2.1.

(ii) Similar to the proof of (i) given above with

$$\beta = \begin{cases} -if/2 & \text{if } \lambda = i, \\ if/2 & \text{if } \lambda = -i. \end{cases} \qquad \blacksquare$$

Since symmetric and antisymmetric functions on $\mathbb{Z}_n$ are easy to construct, by Theorem 7.2.3, we can construct eigenvectors corresponding to any given eigenvalue $\lambda \in \{\pm 1, \pm i\}$. For later purposes, we present familiar functions in number theory that serve as eigenvectors with eigenvalue 1 or $-i$. First, we define a special kind of summation.

Definition 7.2.1. *For each positive integer n, the quadratic Gaussian sum of order n is the function $G_n \colon \mathbb{Z} \to \mathbb{C}$ defined by the equation*

$$G_n(x) = \frac{1}{\sqrt{n}} \sum_{k \in \mathbb{Z}_n} e^{-\frac{2\pi i}{n} x k^2}.$$

It follows from this definition that

(i) $G_1(x) = 1$ for all $x \in \mathbb{Z}$,
(ii) for $n > 1$, $G_n(x) = \sqrt{n}$ if x is a multiple of n, and
(iii) $G_n(x) = G_n(x+mn)$ for any integer m. In fact, G_n has period n (Exercise 45). Thus G_n is completely determined once its values on the fundamental set $\{0, 1, \ldots, n-1\}$ are known.

We rephrase Theorem 1.2.3 and equation (1.4) in terms of the FT as follows: if p is an odd prime and ζ_p is the function on $\mathbb{Z}_p$ defined in terms of the Legendre symbol by $\zeta_p(x) = (x/p)$, then

$$\hat{\zeta}_p(x) = \begin{cases} G_p(x) & \text{if } x \neq 0, \\ 0 & \text{if } x = 0. \end{cases} \tag{7.4}$$

Theorem 7.2.4. *If p is an odd prime, then $\hat{\zeta}_p = G_p(1)\zeta_p$.*

Proof. Since $\hat{\zeta}_p(0) = 0$ and $\zeta(0) = 0$, the theorem holds for $x = 0$. For a fixed $x \in \mathbb{Z}_p$ and $x \neq 0$, we have

$$\hat{\zeta}_p(x) = \frac{1}{\sqrt{p}} \sum_{y \in \mathbb{Z}_p} e^{-\frac{2\pi i}{p} xy} \zeta_p(y) = \frac{1}{\sqrt{p}} \sum_{y \in \mathbb{Z}_p} e^{-\frac{2\pi i}{p} xy} (y/p).$$

The change of variable $\theta = xy$ leads to

$$\hat{\zeta}_p(x) = \frac{1}{\sqrt{p}} \sum_{\theta \in x\mathbb{Z}_p} e^{-\frac{2\pi i}{p}\theta} (\theta x^{-1}/p),$$

where x^{-1} is the multiplicative inverse of x in $\mathbb{Z}_p$. Since $x\mathbb{Z}_p = \{xy \,(\mathrm{mod}\, p) \mid y \in \mathbb{Z}_p\} = \mathbb{Z}_p$, it follows from (1.5), (ii) of Theorem 1.2.1, and equation (7.4) that

$$\hat{\zeta}_p(x) = (x^{-1}/p) \frac{1}{\sqrt{p}} \sum_{\theta \in \mathbb{Z}_p} e^{-\frac{2\pi i}{p}\theta} (\theta/p) = \zeta_p(x^{-1})\hat{\zeta}_p(1) = \zeta_p(x) G_p(1).$$

■

We will show later in Chapter 9 that

$$G_n(1) = \frac{1 + i^n}{1 + i}.$$

From this formula we obtain

$$G_p(1) = \begin{cases} 1 & \text{if and only if } p \equiv 1 \,(\mathrm{mod}\, 4), \\ -i & \text{if and only if } p \equiv 3 \,(\mathrm{mod}\, 4). \end{cases}$$

Thus 1 and $-i$ are the eigenvalues of the FT on $\mathbb{Z}_p$, the eigenvalue is 1 or $-i$ depending on whether $p \equiv 1 \,(\mathrm{mod}\, 4)$ or $p \equiv 3 \,(\mathrm{mod}\, 4)$, respectively. By Theorems 7.2.2 and 7.2.4, for an odd prime p, the function ζ_p is symmetric if and only if p is congruent to 1 modulo 4 or, equivalently, ζ_p is antisymmetric if and only if p is congruent to 3 modulo 4. Thus, for any integer a that is not divisible by p, we have

$$(a/p) = \begin{cases} (-a/p) & \text{if and only if } p \equiv 1 \,(\mathrm{mod}\, 4), \\ -(-a/p) & \text{if and only if } p \equiv 3 \,(\mathrm{mod}\, 4). \end{cases}$$

Consequently, if $p \equiv 3 \,(\mod\, 4)$, then (a/p) and $(-a/p)$ have opposite sign. That is, exactly one of the numbers a or $-a$ is a quadratic residue modulo p. Suppose that a is a quadratic residue modulo p. In this case, there is a nonzero integer x such that $x^2 \equiv a \,(\mod\, p)$ and there is no integer y that satisfies $y^2 \equiv -a \,(\mathrm{mod}\, p)$. Since a

is an arbitrary integer that is not divisible by p, one can verify that, for any nonzero integer k, there is no integer y such that $x^2 + y^2 = kp$. The same result is obtained if $-a$ is a quadratic residue. We record this result of number theory (in different wording) as a theorem.

Theorem 7.2.5. *If p is a prime congruent to 3 modulo 4, then no positive integral multiple of p can be written as a sum of two squares of integers, one of which is relatively prime to p.*

Said differently, if a positive integer m is divisible by a prime p and $p \equiv 3 \pmod 4$, then there are no integers x and y with properties that

(i) either $\gcd(x, p) = 1$ or $\gcd(y, p) = 1$, and
(ii) $x^2 + y^2 = m$.

The following corollary is a reformulation of Theorem 7.2.4 according to consequence (iii) of the definition and (7.4).

Corollary 7.2.2. *If p is an odd prime and a is an integer that is not divisible by p, then $G_p(a) = (a/p)G_p(1)$.*

Thus, for an odd prime p, we reduce the evaluation of the Gaussian sum $G_p(a)$ to the determination of the Legendre symbol (a/p) and the constant $G_p(1)$. Since the Legendre symbol (a/p) is well-understood, it remains only to determine the value of $G_p(1)$. This is one of the crucial points in the direction we take in the evaluation of general quadratic Gaussian sums (in Chapter 9).

Exercises.

41. Let A be a self-adjoint linear operator on a finite-dimensional complex inner product space. Show that the eigenvalues of A are real numbers. Conclude from this result and Corollary 7.2.1 (on page 99) that the FT is not self-adjoint if $n > 2$.

42. Prove that the trace of the FT on $\mathbb{Z}_n$ is $G_n(1)$.

43. Suppose that $p_1, \ldots, p_k$ are odd primes and $G = \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_k}$. Prove that if f is a complex-valued function defined on G by $f = \zeta_{p_1} \otimes \cdots \otimes \zeta_{p_k}$, then $\hat{f} = cf$, where $c = \prod_{j=1}^{k} G_{p_j}(1)$.

44. Let $n_1, \dots, n_k$ be positive integers greater than 1 and let $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$. Prove that on the space V_G the eigenvalues of the FT are ± 1 if $n_1 = \cdots = n_k = 2$, and are ± 1, $\pm i$ otherwise.

45. Show that G_n has period n.

7.3 Spectral Theorem

If λ is an eigenvalue of the FT, then the eigenvectors corresponding to λ are nonzero solutions of the equation $(\mathcal{F} - \lambda I)x = 0$, which are the nonzero elements of the kernel of the linear operator $\mathcal{F} - \lambda I$. So, these eigenvectors together with the zero vector form a vector subspace. This subspace, denoted by E_λ, is called *the eigenspace corresponding to* λ. Our goals in this section are: first, to show that $V_{\mathbb{Z}_n}$ is equal to the direct sum of the eigenspaces; second, to decompose the FT into a sum of simpler linear operators.

Suppose that f is a non-identically zero, complex-valued, symmetric function defined on $\mathbb{Z}_n$. From the identity

$$f = \frac{\hat{f} + f}{2} - \frac{\hat{f} - f}{2} \tag{7.5}$$

we have, by Theorem 7.2.1, that $(\hat{f} + f)/2$ is an eigenvector corresponding to the eigenvalue 1 and $(\hat{f} - f)/2$ is an eigenvector corresponding to the eigenvalue -1. Thus, every nonzero symmetric function can be decomposed as a sum of two functions, one is an eigenvector corresponding to the eigenvalue 1 and the other is an eigenvector corresponding to the eigenvalue -1. Furthermore, this decomposition is unique (Exercise 46). Consequently, the vector space of symmetric functions is the direct sum of the eigenspaces corresponding to the eigenvalues ± 1, that is, $V_s = E_1 \oplus E_{-1}$.

Similarly, if f is a non-identically zero, complex-valued, antisymmetric function defined on $\mathbb{Z}_n$, then we have the decomposition

$$f = \frac{\hat{f} + if}{2i} - \frac{\hat{f} - if}{2i}, \tag{7.6}$$

where, by Theorem 7.2.1, the functions $(\hat{f}+if)/2i$ and $(\hat{f}-if)/2i$ are eigenvectors corresponding to the eigenvalues i and $-i$, respectively. Moreover, the decomposition (7.6) is unique (Exercise 46), so $V_a = E_i \oplus E_{-i}$.

We treat the cases $n = 2$ and $n > 2$ separately. First, assume that $n > 2$. Since $V_{\mathbb{Z}_n} = V_s \oplus V_a$, in view of the results obtained from the previous two paragraphs, we have

$$V_{\mathbb{Z}_n} = E_1 \oplus E_{-1} \oplus E_i \oplus E_{-i}. \tag{7.7}$$

Moreover, the eigenspaces E_λ, for $\lambda = \pm 1$, $\pm i$, are pairwise orthogonal, that is, every vector in E_λ is orthogonal to every vector in $E_{\lambda'}$ whenever $\lambda \neq \lambda'$. This fact follows from the Plancherel theorem; for, if $f_\lambda \in E_\lambda$, $f_{\lambda'} \in E_{\lambda'}$, and $\lambda \neq \lambda'$, then

$$\langle f_\lambda, f_{\lambda'} \rangle = \langle \hat{f}_\lambda, \hat{f}_{\lambda'} \rangle = \lambda \overline{\lambda'} \langle f_\lambda, f_{\lambda'} \rangle = \frac{\lambda}{\lambda'} \langle f_\lambda, f_{\lambda'} \rangle.$$

The inequality $\langle f_\lambda, f_{\lambda'} \rangle \neq 0$ would imply that $\lambda = \lambda'$. So, we must have $\langle f_\lambda, f_{\lambda'} \rangle = 0$.

The pairwise orthogonality of the eigenspaces E_λ induces orthogonal projection operators defined as follows: by (7.7), every complex-valued function f on $\mathbb{Z}_n$ can be expressed uniquely as

$$f = f_1 + f_{-1} + f_i + f_{-i}, \tag{7.8}$$

where $f_\lambda \in E_\lambda$ for $\lambda = \pm 1$, $\pm i$. We define, for each λ, the *orthogonal projection operator* P_λ on $V_{\mathbb{Z}_n}$ by setting

$$P_\lambda f = f_\lambda. \tag{7.9}$$

It is obvious that P_λ is well-defined, linear, and that its range is the space E_λ. The orthogonal projection operators are pairwise orthogonal, idempotent, and self-adjoint; that is,

$$P_\lambda P_{\lambda'} = \begin{cases} 0 & \text{if } \lambda \neq \lambda', \\ P_\lambda & \text{if } \lambda = \lambda', \end{cases} \tag{7.10}$$

and $P_\lambda = P_\lambda^*$ for $\lambda, \lambda' = \pm 1, \pm i$ (Exercise 47). We can conclude from (7.8) and (7.9) that

$$I \;= P_1 + P_{-1} + P_i + P_{-i},$$

where the sum of operators is defined in an obvious way (i.e., pointwise) and I denotes the identity operator on $V_{\mathbb{Z}_n}$. Since $\mathcal{F}P_\lambda = \lambda P_\lambda$, we have

$$\mathcal{F} = \mathcal{F}I \;= \mathcal{F}P_1 + \mathcal{F}P_{-1} + \mathcal{F}P_i + \mathcal{F}P_{-i} = P_1 - P_{-1} + iP_i - iP_{-i}.$$

The analysis for the case $n = 2$ is similar to that given above for the case $n > 2$, except that, since $V_a = \varnothing$ (the empty set), there are no $\pm i$, E_i, E_{-i}, P_i, or P_{-i} involved. Thus, we have $V_{\mathbb{Z}_2} = E_1 \oplus E_{-1}$, $I = P_1 + P_{-1}$, and $\mathcal{F} = P_1 - P_{-1}$.

The expression $\mathcal{F} = P_1 - P_{-1}$ when $n = 2$ or $\mathcal{F} = P_1 - P_{-1} + iP_i - iP_{-i}$ when $n > 2$ is called the *spectral form* of $\mathcal{F}$. We have proved half of the spectral theorem for the FT.

Theorem 7.3.1 (Spectral Theorem). *As a linear operator on the inner product space $V_{\mathbb{Z}_n}$, the FT can be expressed uniquely as a linear combination of the orthogonal projections on the eigenspaces as follows*:

$$\mathcal{F} = \begin{cases} P_1 - P_{-1} & \text{if } n = 2, \\ P_1 - P_{-1} + iP_i - iP_{-i} & \text{if } n > 2. \end{cases}$$

Proof. It remains only to prove the uniqueness. Since proofs of the two cases $n = 2$ and $n > 2$ are similar, we give a proof for the case $n > 2$ only. Suppose that $n > 2$ and

$$\mathcal{F} = c_1 P_1 + c_{-1} P_{-1} + c_i P_i + c_{-i} P_{-i} \tag{7.11}$$

for some constants c_1, c_{-1}, c_i, and c_{-i}. What we must show is that $c_\lambda = \lambda$ for $\lambda = \pm 1, \pm i$.

For a fixed $\lambda \in \{\pm 1, \pm i\}$, since $E_\lambda \neq \{0\}$, there is a nonzero vector $f_\lambda \in E_\lambda$ such that

(a) $P_\lambda f_\lambda = f_\lambda$, and
(b) $\mathcal{F} f_\lambda = \lambda f_\lambda$.

Also, since the eigenspaces are pairwise orthogonal, we have

(c) $P_{\lambda'} f_\lambda = 0$ whenever $\lambda' \neq \lambda$.

It follows from (7.11), (c), and (a) that

$$\mathcal{F}f_\lambda = c_1P_1f_\lambda + c_{-1}P_{-1}f_\lambda + c_iP_if_\lambda + c_{-i}P_{-i}f_\lambda = c_\lambda P_\lambda f_\lambda = c_\lambda f_\lambda.$$

This result combines with (b) to give $(c_\lambda - \lambda)f_\lambda = 0$. Since $f_\lambda \neq 0$, we have $c_\lambda = \lambda$. ■

Remark. Theorem 4.7.1 is a simple consequence of the equation $(iP_\lambda)^* = -iP_\lambda$ and the spectral theorem.

Exercises.

46. Prove the uniqueness of the decompositions (7.5) and (7.6).

47. Prove that the orthogonal projections P_λ, where $\lambda = \pm1, \pm i$, satisfy the equations in (7.10) and that $P_\lambda = P_\lambda^*$.

48. Recall the space $V_{\mathbb{Z}_n} = V_s \oplus V_a$ and the bases B_{sym} and B_{antisym} of V_s and V_a, respectively, which were defined in Section 7.1.

(i) Consider the FT restricted to the subspace V_s. It is a linear operator on V_s. Show that its matrix with respect to the orthonormal basis B_{sym} is

$$\left(\frac{4}{\epsilon_s\epsilon_t\sqrt{n}}\cos\frac{2\pi}{n}st\right)_{m\times m},$$

where $m = \lfloor n/2\rfloor + 1$ and $s,\, t = 0, \ldots, \lfloor n/2\rfloor$.

(ii) Assume that $n > 2$ (so that V_a is nonempty). Consider the FT restricted to the subspace V_a. It is a linear operator on V_a. Show that its matrix with respect to the orthonormal basis B_{antisym} is

$$\left(-\frac{2i}{\sqrt{n}}\sin\frac{2\pi}{n}st\right)_{m\times m},$$

where $m = \lceil n/2\rceil - 1$ and $s,\, t = 1, \ldots, m$.

49. For each $\lambda = \pm1, \pm i$, let $\mathcal{M}_{P_\lambda}$ be the matrix of the orthogonal projection P_λ with respect to the standard basis $\mathit{\Delta}_{\mathbb{Z}_n} = \{\delta_j \mid j = 0, \ldots, n-1\}$. Prove that

$$\begin{aligned}
\mathcal{M}_{P_1} &= \frac{1}{4}(B_t(s) + B_{-t}(s) + \delta_t(s) + \delta_{-t}(s))_{n\times n},\\
\mathcal{M}_{P_{-1}} &= -\frac{1}{4}(B_t(s) + B_{-t}(s) - [\delta_t(s) + \delta_{-t}(s)])_{n\times n},\\
\mathcal{M}_{P_i} &= \frac{1}{4}(i[B_t(s) - B_{-t}(s)] + [\delta_t(s) - \delta_{-t}(s)])_{n\times n},\\
\mathcal{M}_{P_{-i}} &= -\frac{1}{4}(i[B_t(s) - B_{-t}(s)] - [\delta_t(s) - \delta_{-t}(s)])_{n\times n},
\end{aligned}$$

where in each case s, $t = 0, \ldots, n-1$ and $-t$ is the inverse of t in the cyclic group $\mathbb{Z}_n$. The notation for matrices means, for example, that the (s,t) entry of the matrix $\mathcal{M}_{P_1}$ is

$$\frac{1}{4}(B_t(s) + B_{-t}(s) + \delta_t(s) + \delta_{-t}(s)),$$

which, by the remark at the end of Section 7.1, is equal to

$$\frac{1}{2\sqrt{n}}\cos\left(\frac{2\pi}{n}st\right) + \frac{\delta_t(s) + \delta_{-t}(s)}{4}.$$

50. Since every element $f \in V_{\mathbb{Z}_n} = V_s \oplus V_a$ can be expressed uniquely as the sum of its symmetric and antisymmetric parts as $f = f^s + f^a$, where $f^s \in V_s$ and $f^a \in V_a$, the induced linear operator P defined by $Pf = f^s$, i.e., P projects $V_{\mathbb{Z}_n}$ onto V_s, is well-defined. P is called the *symmetric orthogonal projection*. Show that

(i) $P = P_1 + P_{-1}$,
(ii) $P\mathcal{F} = \mathcal{F}P = P\mathcal{F}P$, and
(iii) $P\mathcal{F}^{-1} = \mathcal{F}^{-1}P = P\mathcal{F}^{-1}P$,

where, as usual, the product of operators is defined to be their composition. Analogously, define the antisymmetric orthogonal projection (only when $n > 2$) and show that (ii) and (iii) still hold when P is replaced by the operator just defined. Prove also that the antisymmetric orthogonal projection satisfied a similar equation as in (i), where the sum $P_1 + P_{-1}$ is replaced by $P_i + P_{-i}$.

51. Find an orthonormal basis for V_G with respect to which the matrix of the FT is diagonal.

52. A nonempty subset S of a complex inner product space V is said to be *convex* if the straight line segment joining any two points in S lies entirely in S; i.e., if x, $y \in S$ and r is a real number such that $0 < r < 1$, then $[(1-r)x + ry] \in S$. A point in a convex set S is called an *extreme point* if it is not an interior point of any straight line segment in S; i.e., e is an extreme point of S if $e \in S$ and $e \neq (1-r)x + ry$ for any x, $y \in S$ and any r for which $0 < r < 1$. Consider the set $S = \big\{\langle \hat{f}, f\rangle \,:\, f \in V_{\mathbb{Z}_n} \text{ and } \|f\| = 1\big\}$. Is S a convex set? If S is convex, determine its extreme points.

53. (This exercise requires sufficient knowledge of linear algebra.) Show that there is a self-adjoint linear operator A on $V_{\mathbb{Z}_n}$ such that $\mathcal{F} = e^{iA}$.

7.4 Ergodic Theorem

The spectral theorem for the FT provides us a convenient way to illustrate the general theory by considering a very special (but important) type of convergence problem.

Definition 7.4.1. *Let A be a linear operator on a finite-dimensional complex inner product space V.*

(a) *A sequence $\{A_n\}_{n=1}^{\infty}$ of linear operators on V is said to converge to A if, for each fixed $x \in V$,*

$$\lim_{n\to\infty} \|A_n x - Ax\| = 0.$$

We indicate that $\{A_n\}$ converges to A by the expression $\lim_{n\to\infty} A_n = A$.

(b) *If c is a scalar (i.e., a complex number), then the scalar multiple of A by c is the linear operator cA defined by $cAx = c(Ax)$ for all $x \in V$.*

If $\{c_n\}$ is a sequence of scalars which converges to zero and x in a vector in V, then, since

$$\begin{aligned}\lim_{n\to\infty} \|c_n Ax\| &= \lim_{n\to\infty} \|c_n(Ax)\| \\ &= \lim_{n\to\infty} |c_n|\|Ax\| = \|Ax\| \lim_{n\to\infty} |c_n| = 0,\end{aligned}$$

we have

$$\lim_{n\to\infty} c_n A = 0, \tag{7.12}$$

where the zero operator is also denoted by 0.

The convergence (7.12) will be used shortly in the special case when A is an orthogonal projection operator. Let $V = V_{\mathbb{Z}_n}$, where $n > 2$. By the spectral theorem it is straightforward to show (by induction with the aid of (7.10)) that

$$\mathcal{F}^k = P_1 + (-1)^k P_{-1} + i^k P_i + (-i)^k P_{-i}$$

for every positive integer k. It follows that the average of the first N positive powers of $\mathcal{F}$ is

$$\begin{aligned}S_N = \frac{1}{N}\sum_{k=1}^{N} \mathcal{F}^k = P_1 &+ \left(\frac{1}{N}\sum_{k=1}^{N}(-1)^k\right) P_{-1} \\ &+ \left(\frac{1}{N}\sum_{k=1}^{N} i^k\right) P_i + \left(\frac{1}{N}\sum_{k=1}^{N}(-i)^k\right) P_{-i}.\end{aligned}$$

For $r = -1$, $\pm i$, the identity

$$\sum_{k=1}^{N} r^k = r\frac{1 - r^N}{1 - r}$$

implies that

$$\lim_{N\to\infty} \frac{1}{N}\sum_{k=1}^{N} r^k = 0,$$

hence, by (7.12),

$$\lim_{N\to\infty} S_N = P_1. \tag{7.13}$$

For the case $n = 2$, since there are no $\pm i$, P_i, and P_{-i} involved, we have

$$\mathcal{F}^k = P_1 + (-1)^k P_{-1} \quad \text{and} \quad S_N = P_1 + \left(\frac{1}{N}\sum_{k=1}^{N}(-1)^k\right) P_{-1}.$$

Thus, the same conclusion (7.13) holds. We have proved the following theorem.

Theorem 7.4.1. *The arithmetic mean of positive integral powers of the FT on $\mathbb{Z}_n$ converges to the orthogonal projection on the eigenspace E_1. In symbols,*

$$\lim_{N\to\infty} \frac{1}{N}\sum_{k=1}^{N} \mathcal{F}^k = P_1.$$

For a more general (but still elementary) theorem which includes this theorem as a special case, see p. 185 of [3].

We conclude this section by pointing out some facts about linear operators defined on complex inner product spaces (these facts are not needed in this exposition other than in the exercise at the end of this section). First, we need a definition: Let A be a linear operator on a complex inner product space V. We say that A is *bounded* if there is a positive constant α such that $\|Ax\| \le \alpha\|x\|$ for all $x \in V$; if A is bounded, the *norm* of A, denoted by $\|A\|$, is defined to be the infimum of all such values of α. Next, some facts: every linear operator on finite-dimensional inner product spaces is bounded. In particular, the projections P_λ, for $\lambda = \pm 1$, $\pm i$, are bounded, in fact, $\|P_\lambda\| = 1$ for every λ. By the definition just given, bounded linear operators are uniformly continuous. The converse of the latter statement is also true.

Exercise.

54. Let A be a linear operator on a finite-dimensional inner product space V. Suppose that a sequence $\{A_n\}_{n=1}^{\infty}$ of linear operators on V converges to A. Prove the following:

(i) $\lim_{n\to\infty} \|A_n - A\| = 0$;

(ii) $\lim_{n\to\infty}\langle A_n x, y\rangle = \langle Ax, y\rangle$ for every fixed pair of vectors x and y in V;

(iii) Let G be a finite Abelian group. Determine whether there is a sequence $\{A_n\}_{n=1}^{\infty}$ of invertible linear operators on V_G that converges to $\mathcal{F}$.

7.5 Multiplicities of Eigenvalues

Recall from (7.7) that $V_{\mathbb{Z}_n} = E_1 \oplus E_{-1} \oplus E_i \oplus E_{-i}$ and from Subsection 2.3 that $\dim V_{\mathbb{Z}_n} = n$. In this section, we determine the dimensions of the eigenspaces E_λ or, equivalently, the multiplicities of the eigenvalues λ for $\lambda = \pm 1$, $\pm i$ by constructing an explicit basis for each eigenspace E_λ.

We will use some results of Section 1.3 of Chapter 1 to show that certain finite sets of the form $\{\alpha_j\}$ or $\{i\beta_j\}$, where α_j and β_j are real-valued functions, are linearly independent over $\mathbb{C}$. For finite sets of the type described, linearly independent over $\mathbb{C}$ is equivalent to linearly independent over $\mathbb{R}$. This fact will be used freely in this section, for this reason we state it as a lemma and leave its proof to the readers.

Lemma 7.5.1. *Suppose that for $j = 1, \ldots, k$, α_j and β_j are real-valued functions (defined on some set). Let $\mathcal{S}$ denote either one of the sets $\{\alpha_j \mid j = 1, \ldots, k\}$ or $\{i\beta_j \mid j = 1, \ldots, k\}$. A necessary and sufficient condition for $\mathcal{S}$ to be linearly independent over $\mathbb{C}$ is that it is linearly independent over $\mathbb{R}$.*

Also, for convenience we recall from page 97 that the norm of the function $B_j + B_{-j}$ is

$$\epsilon_j = \begin{cases} 2 & \text{if } j = 0 \text{ or if } n \text{ is even and } j = n/2, \\ \sqrt{2} & \text{otherwise.} \end{cases}$$

Dimension of E_1 and E_{-1}. We consider two cases, $n \equiv 0 \pmod 4$ or $n \equiv 1 \pmod 4$ and $n \equiv 2 \pmod 4$ or $n \equiv 3 \pmod 4$.

Case 1. Either $n \equiv 0 \,(\mathrm{mod} 4)$ or $n \equiv 1 \,(\mathrm{mod} 4)$, that is, either $n = 4m$ or $n = 4m+1$ for some positive integer m. (The integer m is not necessarily the same in these two subcases.) In either case, we have $\lfloor n/2 \rfloor = 2m$. Recall from Section 7.1 that the vector space V_s of symmetric functions has an orthonormal basis

$$B_{\mathrm{sym}} = \left\{ \frac{B_j + B_{-j}}{\epsilon_j} \;\middle|\; j = 0, \ldots, 2m \right\}.$$

Since $V_s = E_1 \oplus E_{-1}$, each function $(B_j + B_{-j})/\epsilon_j$ in B_{sym} can be written uniquely as the sum of a function in E_1 and a function in E_{-1}, according to (7.5), as

$$\frac{B_j + B_{-j}}{\epsilon_j} = s_j + s'_j,$$

where

$$\begin{aligned} s_j &= \frac{B_j + B_{-j} + \delta_j + \delta_{-j}}{2\epsilon_j} \in E_1 \quad \text{and} \\ s'_j &= \frac{B_j + B_{-j} - \delta_j - \delta_{-j}}{2\epsilon_j} \in E_{-1}. \end{aligned}$$

By the remark at the end of Section 7.1, s_j and s'_j can be expressed in terms of the cosine function as

$$\begin{aligned} s_j(k) &= \frac{1}{\epsilon_j \sqrt{n}} \left(\frac{\sqrt{n}}{2} [\delta_j(k) + \delta_{-j}(k)] + \cos \frac{2\pi}{n} jk \right), \\ s'_j(k) &= \frac{-1}{\epsilon_j \sqrt{n}} \left(\frac{\sqrt{n}}{2} [\delta_j(k) + \delta_{-j}(k)] - \cos \frac{2\pi}{n} jk \right), \end{aligned} \tag{7.14}$$

where $k \in \mathbb{Z}_n$.

Subcase $n = 4m$. Recall from (7.1) that $\dim V_s = 2m + 1$. Since E_{-1} and E_1 are nontrivial proper subspaces of V_s, we have $0 < \dim E_{-1} < 2m + 1$ and $0 < \dim E_1 < 2m + 1$.

The space E_{-1}. Since $\dim E_{-1} < 2m+1$ and the $2m+1$ functions $s'_0, \ldots, s'_{2m}$ belong to E_{-1}, these functions are linearly dependent (over $\mathbb{C}$). We claim that the first m of these functions, i.e., $s'_0, \ldots, s'_{m-1}$, are linearly independent. Suppose that for some real numbers $c_0, \ldots, c_{m-1}$ the function $S' = c_0 s'_0 + \cdots + c_{m-1} s'_{m-1}$ is identically zero on the group $\mathbb{Z}_{4m}$. Then, in particular, $S'(k) = 0$ for $k = m, \ldots, 2m-1$ or, equivalently, $M_{-1}c = 0$, where

$$M_{-1} = \begin{pmatrix} 1 & \cos\frac{\pi}{2} & \cos 2\frac{\pi}{2} & \ldots & \cos(m-1)\frac{\pi}{2} \\ 1 & \cos\frac{m+1}{2m}\pi & \cos 2\frac{m+1}{2m}\pi & \ldots & \cos(m-1)\frac{m+1}{2m}\pi \\ 1 & \cos\frac{m+2}{2m}\pi & \cos 2\frac{m+2}{2m}\pi & \ldots & \cos(m-1)\frac{m+2}{2m}\pi \\ \vdots & & & \ddots & \vdots \\ 1 & \cos\frac{2m-1}{2m}\pi & \cos 2\frac{2m-1}{2m}\pi & \ldots & \cos(m-1)\frac{2m-1}{2m}\pi \end{pmatrix}_{m\times m}$$

and c is the column vector in $\mathbb{R}^m$ whose coordinates are c_0, $\sqrt{2}c_1, \ldots, \sqrt{2}c_{m-1}$. For $\ell = 0, \ldots, m-1$, let

$$x_\ell = \frac{m+\ell}{2m}\pi$$

and define the real-valued function ϕ_ℓ on the interval $[0, \pi]$ by $\phi_\ell(x) = \cos \ell x$. In terms of these functions $M_{-1} = (\phi_s(x_t))$, where s, $t = 0, \ldots, m-1$. By Theorems 1.3.2 and 1.3.3(i), the matrix M_{-1} is nonsingular. It follows that $c = 0$, so the functions $s'_0, \ldots, s'_{m-1}$ are linearly independent. Since these linearly independent functions are elements of E_{-1}, $\dim E_{-1} \geq m$.

The space E_1. The inequality $\dim E_1 < 2m+1$ implies that the functions $s_0, \ldots, s_{2m}$, all elements of E_1, are linearly dependent (over $\mathbb{C}$). We claim that $s_0, \ldots, s_{m-1}$, s_{2m} are linearly independent. To prove this, suppose that for some real numbers $c_0, \ldots, c_{m-1}$, c_{2m} the function $S = c_0 s_0 + \cdots + c_{m-1}s_{m-1} + c_{2m}s_{2m}$ is identically zero on $\mathbb{Z}_{4m}$. Then, in particular, $S(k) = 0$ for $k = m, \ldots, 2m$ or, equivalently, $M_1 c = 0$, where

$$M_1 = \begin{pmatrix} 1 & \cos\frac{\pi}{2} & \cos 2\frac{\pi}{2} & \dots & \cos(m-1)\frac{\pi}{2} & (-1)^m \\ 1 & \cos\frac{m+1}{2m}\pi & \cos 2\frac{m+1}{2m}\pi & \dots & \cos(m-1)\frac{m+1}{2m}\pi & (-1)^{m+1} \\ 1 & \cos\frac{m+2}{2m}\pi & \cos 2\frac{m+2}{2m}\pi & \dots & \cos(m-1)\frac{m+2}{2m}\pi & (-1)^{m+2} \\ \vdots & & & \ddots & & \vdots \\ 1 & \cos\frac{2m-1}{2m}\pi & \cos 2\frac{2m-1}{2m}\pi & \dots & \cos(m-1)\frac{2m-1}{2m}\pi & -1 \\ 1 & \cos\pi & \cos 2\pi & \dots & \cos(m-1)\pi & 1+2\sqrt{m} \end{pmatrix}_{(m+1)\times(m+1)}$$

and c is the column vector in $\mathbb{R}^{m+1}$ whose coordinates are c_0, $\sqrt{2}c_1, \dots, \sqrt{2}c_{m-1}, c_{2m}$. Alternatively, M_1 can also be constructed from M_{-1}. First, insert the row vector

$$(1, \cos\pi, \dots, \cos(m-1)\pi)$$

into M_{-1} in such a way that it is the last row of the resulting matrix, call it M_{result}. Second, insert the column vector

$$\begin{pmatrix} (-1)^m \\ (-1)^{m+1} \\ (-1)^{m+2} \\ \vdots \\ -1 \\ 1+2\sqrt{m} \end{pmatrix}_{(m+1)\times 1}$$

into M_{result} to obtain M_1. By Theorems 1.3.2 and 1.3.3, the matrix M_1 is nonsingular. It follows that $c = 0$. Thus the vector space E_1 contains $m+1$ linearly independent vectors; namely, the functions $s_0, \dots, s_{m-1}, s_{2m}$, so $\dim E_1 \geq m+1$.

Subcase $n = 4m+1$. For the space E_{-1}, we claim that the functions $s'_0, \dots, s'_{m-1}$ are linearly independent. Analogous to the subcase $n = 4m$ we have $M_{-1}c = 0$, where

$$M_{-1} = \begin{pmatrix} 1 & \cos\frac{2m}{4m+1}\pi & \cos 2\frac{2m}{4m+1}\pi & \dots & \cos(m-1)\frac{2m}{4m+1}\pi \\ 1 & \cos\frac{2(m+1)}{4m+1}\pi & \cos 2\frac{2(m+1)}{4m+1}\pi & \dots & \cos(m-1)\frac{2(m+1)}{4m+1}\pi \\ \vdots & & & \ddots & \vdots \\ 1 & \cos\frac{2(2m-1)}{4m+1}\pi & \cos 2\frac{2(2m-1)}{4m+1}\pi & \dots & \cos(m-1)\frac{2(2m-1)}{4m+1}\pi \end{pmatrix}_{m\times m}$$

and c is the column vector in $\mathbb{R}^m$ whose coordinates are c_0, $\sqrt{2}c_1, \dots, \sqrt{2}c_{m-1}$. For $\ell = 0, \dots, m-1$, let

$$x_\ell = \frac{2(m+\ell)}{4m+1}\pi$$

and define the real-valued function ϕ_ℓ on the interval $[0, \pi]$ by $\phi_\ell(x) = \cos \ell x$. In terms of these functions $M_{-1} = (\phi_s(x_t))$, where s, $t = 0, \dots, m-1$. By Theorems 1.3.2 and 1.3.3(i), the matrix M_{-1} is nonsingular. It follows that $c = 0$, so the functions $s'_0, \dots, s'_{m-1}$ are linearly independent. Since these linearly independent functions are elements of E_{-1}, $\dim E_{-1} \geq m$.

For the space E_1, we claim that $s_0, \dots, s_{m-1}, s_{2m}$ are linearly independent. Analogous to the subcase $n = 4m$ we have $M_1 c = 0$, where M_1 is the $(m+1) \times (m+1)$ matrix

$$\begin{pmatrix}
1 \ \cos\frac{2m}{4m+1}\pi & \cos 2\frac{2m}{4m+1}\pi & \dots \cos(m-1)\frac{2m}{4m+1}\pi & \cos(2m)\frac{2m}{4m+1}\pi \\
1 \ \cos\frac{2(m+1)}{4m+1}\pi & \cos 2\frac{2(m+1)}{4m+1}\pi & \dots \cos(m-1)\frac{2(m+1)}{4m+1}\pi & \cos(2m)\frac{2(m+1)}{4m+1}\pi \\
\vdots & & \ddots & \vdots \\
1 \ \cos\frac{2(2m-1)}{4m+1}\pi & \cos 2\frac{2(2m-1)}{4m+1}\pi & \dots \cos(m-1)\frac{2(2m-1)}{4m+1}\pi & \cos(2m)\frac{2(2m-1)}{4m+1}\pi \\
1 \ \cos\frac{4m}{4m+1}\pi & \cos 2\frac{4m}{4m+1}\pi & \dots \cos(m-1)\frac{4m}{4m+1}\pi & \frac{\sqrt{4m+1}}{2} + \cos(2m)\frac{4m}{4m+1}\pi
\end{pmatrix}$$

and c is the column vector in $\mathbb{R}^{m+1}$ whose coordinates are c_0, $\sqrt{2}c_1, \dots, \sqrt{2}c_{m-1}, \sqrt{2}c_{2m}$. The cosine terms in the last column of M_1 are $\cos(2m)\frac{2(m+\ell)}{4m+1}\pi$ for $\ell = 0, \dots, m$. The inequalities

$$0 < \frac{m+\ell}{4m+1} < 1/2$$

and

$$(2m)\frac{2(m+\ell)}{4m+1}\pi = \left(1 - \frac{1}{4m+1}\right)(m+\ell)\pi$$

imply that

$$\cos\frac{m+\ell}{4m+1}\pi > 0$$

and

$$\begin{aligned}\cos(2m)\frac{2(m+\ell)}{4m+1}\pi &= \cos\left(1-\frac{1}{4m+1}\right)(m+\ell)\pi\\ &= [\cos(m+\ell)\pi]\cos\frac{m+\ell}{4m+1}\pi\\ &= (-1)^{m+\ell}\cos\frac{m+\ell}{4m+1}\pi.\end{aligned}$$

Thus, the entries in the last column of M_1 are alternating sign nonzero real numbers. Alternatively, M_1 can also be constructed from M_{-1}. First, insert the row vector

$$\left(1,\ \cos\frac{4m}{4m+1}\pi,\ \cos 2\frac{4m}{4m+1}\pi, \ldots,\ \cos(m-1)\frac{4m}{4m+1}\pi\right)$$

into M_{-1} in such a way that it is the last row of the resulting matrix, call it M_{result}. Second, insert the column vector

$$\begin{pmatrix}\cos(2m)\frac{2m}{4m+1}\pi\\ \cos(2m)\frac{2(m+1)}{4m+1}\pi\\ \vdots\\ \cos(2m)\frac{2(2m-1)}{4m+1}\pi\\ \frac{\sqrt{4m+1}}{2}+\cos(2m)\frac{4m}{4m+1}\pi\end{pmatrix}_{(m+1)\times 1}$$

into M_{result} to obtain M_1. Since the coordinates of this column vector are alternating sign nonzero real numbers, Theorems 1.3.2 and 1.3.3 imply that the matrix M_1 is nonsingular. It follows that $c = 0$, whence $\dim E_1 \geq m+1$.

Since $2m+1 = \dim V_s = \dim E_1 + \dim E_{-1}$, we conclude that

$$\begin{aligned}\dim E_1 &= m+1,\\ \dim E_{-1} &= m.\end{aligned}$$

The sets $\{s_0, \ldots, s_{m-1}, s_{2m}\}$ and $\{s'_0, \ldots, s'_{m-1}\}$ are bases for E_1 and E_{-1}, respectively.

Case 2. Either $n \equiv 2 \pmod 4$ or $n \equiv 3 \pmod 4$, that is, either $n = 4m+2$ or $n = 4m+3$ for some nonnegative integer m. (The integer m is not necessarily the same in these two subcases.) In either case, we have $\lfloor n/2 \rfloor = 2m+1$. The vector space V_s of symmetric functions has an orthonormal basis (see (7.3))

$$\begin{aligned} B_{\text{sym}} &= \left\{ \frac{B_j + B_{-j}}{\epsilon_j} \;\middle|\; j = 0, \ldots, 2m+1 \right\} \\ &= \{ s_j + s'_j \mid j = 0, \ldots, 2m+1 \}, \end{aligned}$$

where the functions s_j and s'_j are given by equations (7.14).

Subcase $n = 4m+2$. Recall from (7.1) that $\dim V_s = 2m+2$. Since E_{-1} and E_1 are nontrivial proper subspaces of V_s, we have $0 < \dim E_{-1} < 2m+2$ and $0 < \dim E_1 < 2m+2$.

The space E_{-1}. Since $\dim E_{-1} < 2m+2$ and the $2m+2$ functions $s'_0, \ldots, s'_{2m+1}$ belong to E_{-1}, they are linearly dependent. We claim that the first m of these functions, i.e., $s'_0, \ldots, s'_m$, are linearly independent. Suppose that for some real numbers $c_0, \ldots, c_m$ the function $S' = c_0 s'_0 + \cdots + c_m s'_m$ is identically zero on the group $\mathbb{Z}_{4m+2}$. Then, in particular, $S'(k) = 0$ for $k = m+1, \ldots, 2m+1$ or, equivalently, $M_{-1}c = 0$, where

$$M_{-1} = \begin{pmatrix} 1 & \cos \frac{m+1}{2m+1}\pi & \cos 2\frac{m+1}{2m+1}\pi & \ldots & \cos m\frac{m+1}{2m+1}\pi \\ 1 & \cos \frac{m+2}{2m+1}\pi & \cos 2\frac{m+2}{2m+1}\pi & \ldots & \cos m\frac{m+2}{2m+1}\pi \\ \vdots & & & \ddots & \vdots \\ 1 & \cos \frac{2m}{2m+1}\pi & \cos 2\frac{2m}{2m+1}\pi & \ldots & \cos m\frac{2m}{2m+1}\pi \\ 1 & \cos \pi & \cos 2\pi & \ldots & \cos m\pi \end{pmatrix}_{(m+1)\times(m+1)}$$

and c is the column vector in $\mathbb{R}^{m+1}$ whose coordinates are c_0, $\sqrt{2}c_1, \ldots, \sqrt{2}c_m$. For $\ell = 1, \ldots, m+1$, let

$$x_\ell = \frac{m+\ell}{2m+1}\pi$$

and define the real-valued function ϕ_ℓ on the interval $[0, \pi]$ by $\phi_\ell(x) = \cos(\ell - 1)x$. In terms of these functions $M_{-1} = (\phi_s(x_t))$, where $s, t = 1, \ldots, m+1$. By Theorems 1.3.2 and 1.3.3(i), the matrix M_{-1} is nonsingular. It follows that $c = 0$, whence the functions $s'_0, \ldots, s'_m$ are linearly independent. Since these linearly independent functions are elements of E_{-1}, $\dim E_{-1} \geq m+1$.

The space E_1. From the inequality $\dim E_1 < 2m+2$ we may conclude that the functions $s_0, \ldots, s_{2m+1}$, all elements of E_1, are linearly dependent. We claim that $s_0, \ldots, s_m$ are linearly independent. Suppose that for some real numbers $c_0, \ldots, c_m$ the function $S = c_0 s_0 + \cdots + c_m s_m$ is identically zero on $\mathbb{Z}_{4m+2}$. Then, in particular, $S(k) = 0$ for $k = m+1, \ldots, 2m+1$ or, equivalently, $M_1 c = 0$, where $M_1 = M_{-1}$ is a nonsingular matrix and c is the column vector in $\mathbb{R}^{m+1}$ whose coordinates are $c_0, \sqrt{2}c_1, \ldots, \sqrt{2}c_m$. Since M_1 is nonsingular, we have $c = 0$; i.e., the functions $s_0, \ldots, s_m$ are linearly independent, whence $\dim E_1 \geq m+1$.

Subcase $n = 4m+3$. For the space E_{-1} we claim that the functions $s'_0, \ldots, s'_m$ are linearly independent and for the space E_1 we claim that $s_0, \ldots, s_m$ are linearly independent. Analogous to the subcase $n = 4m+2$ we have $M_1 = M_{-1}$ and $M_{-1}c = 0$, where

$$M_{-1} = \begin{pmatrix} 1 & \cos \frac{m+1}{4m+3}2\pi & \cos 2\frac{m+1}{4m+3}2\pi & \ldots & \cos m\frac{m+1}{4m+3}2\pi \\ 1 & \cos \frac{m+2}{4m+3}2\pi & \cos 2\frac{m+2}{4m+3}2\pi & \ldots & \cos m\frac{m+2}{4m+3}2\pi \\ \vdots & & & \ddots & \vdots \\ 1 & \cos \frac{2m+1}{4m+3}2\pi & \cos 2\frac{2m+1}{4m+3}2\pi & \ldots & \cos m\frac{2m+1}{4m+3}2\pi \end{pmatrix}_{(m+1)\times(m+1)}$$

and c is the column vector in $\mathbb{R}^{m+1}$ whose coordinates are c_0, $\sqrt{2}c_1, \ldots, \sqrt{2}c_m$. For $\ell = 1, \ldots, m+1$, let

$$x_\ell = \frac{m+\ell}{4m+3}2\pi$$

and define the real-valued function ϕ_ℓ on the interval $[0, \pi]$ by $\phi_\ell(x) = \cos(\ell-1)x$. In terms of these functions $M_{-1} = (\phi_s(x_t))$, where $s, t = 1, \ldots, m+1$. By Theorems 1.3.2 and 1.3.3(i), the matrix M_{-1} is nonsingular. It follows that $c = 0$, whence $\dim E_{-1} \geq m+1$ and $\dim E_1 \geq m+1$.

Since $2m+2 = \dim V_s = \dim E_1 + \dim E_{-1}$, we conclude that

$$\dim E_1 = m+1,$$
$$\dim E_{-1} = m+1.$$

The sets $\{s_0, \ldots, s_m\}$ and $\{s'_0, \ldots, s'_m\}$ are bases for E_1 and E_{-1}, respectively.

Dimension of E_i and E_{-i}. We consider three cases, $n \equiv 0 \pmod 4$, $n \equiv 1 \pmod 4$ or $n \equiv 2 \pmod 4$, and $n \equiv 3 \pmod 4$.

Case 1. $n \equiv 0 \pmod 4$, that is, $n = 4m$ for some positive integer m. In this case we have $\lceil n/2 \rceil = 2m$. Recall from Section 7.1 that the vector space V_a of antisymmetric functions has an orthonormal basis

$$B_{\text{antisym}} = \left\{ \frac{B_j - B_{-j}}{\sqrt{2}} \;\middle|\; j = 1, \ldots, 2m-1 \right\}.$$

Since $V_a = E_i \oplus E_{-i}$, each function $(B_j - B_{-j})/\sqrt{2}$ in B_{antisym} can be written uniquely as the sum of a function in E_i and a function in E_{-i}, according to (7.6), as

$$\frac{B_j - B_{-j}}{\sqrt{2}} = a_j + a'_j,$$

where

$$a_j = \frac{i(B_j - B_{-j}) + (\delta_j - \delta_{-j})}{i2\sqrt{2}} \in E_i,$$
$$a'_j = \frac{i(B_j - B_{-j}) - (\delta_j - \delta_{-j})}{i2\sqrt{2}} \in E_{-i}.$$

By the remark at the end of Section 7.1, a_j and a'_j can be expressed in terms of the sine function as

$$\begin{aligned} a_j(k) &= \frac{-i}{\sqrt{2n}} \left(\frac{\sqrt{n}}{2}[\delta_j(k) - \delta_{-j}(k)] - \sin \frac{2\pi}{n} jk \right) \\ a'_j(k) &= \frac{i}{\sqrt{2n}} \left(\frac{\sqrt{n}}{2}[\delta_j(k) - \delta_{-j}(k)] + \sin \frac{2\pi}{n} jk \right), \end{aligned} \tag{7.15}$$

where $k \in \mathbb{Z}_n$.

By (7.1) $\dim V_a = 2m - 1$ and since E_i is a proper subspace of V_a, we have $\dim E_i < 2m - 1$. It follows that the functions $a_1, \ldots, a_{2m-1}$, all elements of E_i, are linearly dependent. We claim that the functions $a_1, \ldots, a_{m-1}$ are linearly independent. To prove this claim, suppose that for some real numbers $c_1, \ldots, c_{m-1}$ the function $A = c_1 a_1 + \cdots + c_{m-1} a_{m-1}$ is identically zero on $\mathbb{Z}_{4m}$. Then, in particular, $A(k) = 0$ for $k = m, \ldots, 2m - 2$ or, equivalently, $M_i c = 0$, where

$$M_i = \begin{pmatrix} \sin\frac{\pi}{2} & \sin 2\frac{\pi}{2} & \sin 3\frac{\pi}{2} & \ldots & \sin(m-1)\frac{\pi}{2} \\ \sin\frac{m+1}{2m}\pi & \sin 2\frac{m+1}{2m}\pi & \sin 3\frac{m+1}{2m}\pi & \ldots & \sin(m-1)\frac{m+1}{2m}\pi \\ \sin\frac{m+2}{2m}\pi & \sin 2\frac{m+2}{2m}\pi & \sin 3\frac{m+2}{2m}\pi & \ldots & \sin(m-1)\frac{m+2}{2m}\pi \\ \vdots & & & \ddots & \vdots \\ \sin\frac{2m-2}{2m}\pi & \sin 2\frac{2m-2}{2m}\pi & \sin 3\frac{2m-2}{2m}\pi & \ldots & \sin(m-1)\frac{2m-2}{2m}\pi \end{pmatrix}_{(m-1)\times(m-1)}$$

and c is the column vector in $\mathbb{R}^{m-1}$ whose coordinates are $c_1, \ldots, c_{m-1}$. Note that in the symbol M_i, just as in the symbol E_i, the subscript is the eigenvalue i. For $\ell = 1, \ldots, m - 1$, let

$$x_\ell = \frac{m - 1 + \ell}{2m}\pi$$

and define the real-valued function ϕ_ℓ on the interval $[0, \pi)$ by $\phi_\ell(x) = \sin \ell x$. In terms of these functions $M_i = (\phi_s(x_t))$, where s, $t = 1, \ldots, m-1$. By Theorems 1.3.2 and 1.3.3(i), the matrix M_i is nonsingular. It follows that $c = 0$, so the functions $a_1, \ldots, a_{m-1}$ are linearly independent. Since these linearly independent functions are elements of E_i, $\dim E_i \geq m - 1$.

Similarly, we have $\dim E_{-i} < 2m - 1$. It follows that the functions $a'_1, \ldots, a'_{2m-1}$, all elements of E_{-i}, are linearly dependent. We claim that $a'_1, \ldots, a'_{m-1}, a'_{2m-1}$ are linearly independent. Suppose that for some real numbers $c_1, \ldots, c_{m-1}, c_{2m-1}$ the function

$$A' = c_1 a'_1 + \cdots + c_{m-1} a'_{m-1} + c_{2m-1} a'_{2m-1}$$

is identically zero on $\mathbb{Z}_{4m}$. Then, in particular, $A'(k) = 0$ for $k = m, \ldots, 2m-1$ or, equivalently, $M_{-i} c = 0$, where M_{-i} is the matrix

$$\begin{pmatrix}
\sin\frac{\pi}{2} & \sin 2\frac{\pi}{2} & \dots & \sin(m-1)\frac{\pi}{2} & \sin(2m-1)\frac{\pi}{2} \\
\sin\frac{m+1}{2m}\pi & \sin 2\frac{m+1}{2m}\pi & \dots & \sin(m-1)\frac{m+1}{2m}\pi & \sin(2m-1)\frac{m+1}{2m}\pi \\
\sin\frac{m+2}{2m}\pi & \sin 2\frac{m+2}{2m}\pi & \dots & \sin(m-1)\frac{m+2}{2m}\pi & \sin(2m-1)\frac{m+2}{2m}\pi \\
\vdots & & \ddots & & \vdots \\
\sin\frac{2m-2}{2m}\pi & \sin 2\frac{2m-2}{2m}\pi & \dots & \sin(m-1)\frac{2m-2}{2m}\pi & \sin(2m-1)\frac{2m-2}{2m}\pi \\
\sin\frac{2m-1}{2m}\pi & \sin 2\frac{2m-1}{2m}\pi & \dots & \sin(m-1)\frac{2m-1}{2m}\pi & \sqrt{m}+\sin(2m-1)\frac{2m-1}{2m}\pi
\end{pmatrix}_{m\times m}$$

and c is the column vector in $\mathbb{R}^m$ whose coordinates are $c_1,\dots,c_{m-1},c_{2m-1}$. The sine terms in the last column of M_{-i} are $\sin(2m-1)\frac{m+\ell}{2m}\pi$ for $\ell=0,\dots,m-1$. The inequalities

$$0<\frac{m+\ell}{2m}<1$$

and

$$(2m-1)\frac{m+\ell}{2m}\pi=\left(1-\frac{1}{2m}\right)(m+\ell)\pi$$

imply that

$$\sin\frac{m+\ell}{2m}\pi>0$$

and

$$\begin{aligned}
\sin(2m-1)\frac{m+\ell}{2m}\pi &= -[\cos(m+\ell)\pi]\sin\frac{m+\ell}{2m}\pi \\
&= (-1)^{m+\ell+1}\sin\frac{m+\ell}{2m}\pi.
\end{aligned}$$

Thus, the entries in the last column of M_{-i} are alternating sign nonzero real numbers. Alternatively, M_{-i} can also be constructed from M_i. First, insert the row vector

$$\left(\sin\frac{2m-1}{2m}\pi,\ \sin 2\frac{2m-1}{2m}\pi,\dots,\ \sin(m-1)\frac{2m-1}{2m}\pi\right)$$

into M_i in such a way that it is the last row of the resulting matrix, call it M_{result}. Second, insert the column vector

$$\begin{pmatrix} \sin(2m-1)\frac{\pi}{2} \\ \sin(2m-1)\frac{m+1}{2m}\pi \\ \sin(2m-1)\frac{m+2}{2m}\pi \\ \vdots \\ \sin(2m-1)\frac{2m-2}{2m}\pi \\ \sqrt{m}+\sin(2m-1)\frac{2m-1}{2m}\pi \end{pmatrix}_{m\times 1}$$

into M_{result} to obtain M_{-i}. Since the coordinates of this column vector are alternating sign nonzero real numbers, Theorems 1.3.2 and 1.3.3 imply that the matrix M_{-i} is nonsingular. It follows that $c=0$, so $\dim E_{-i} \geq m$.

Since $2m-1 = \dim V_a = \dim E_i + \dim E_{-i}$, we conclude that

$$\begin{aligned} \dim E_i &= m-1, \\ \dim E_{-i} &= m. \end{aligned}$$

The sets $\{a_1, \ldots, a_{m-1}\}$ and $\{a'_1, \ldots, a'_{m-1}, a'_{2m-1}\}$ are bases for E_i and E_{-i}, respectively.

Case 2. Either $n \equiv 1 \,(\text{mod} 4)$ or $n \equiv 2 \,(\text{mod} 4)$, that is, either $n = 4m+1$ for some positive integer m or $n = 4m+2$ for some nonnegative integer m. In either case, we have $\lceil n/2 \rceil = 2m+1$. The vector space V_a of antisymmetric functions has an orthonormal basis

$$\begin{aligned} B_{\text{antisym}} &= \left\{ \frac{B_j - B_{-j}}{\sqrt{2}} \;\middle|\; j = 1, \ldots, 2m \right\} \\ &= \{ a_j + a'_j \mid j = 1, \ldots, 2m \}, \end{aligned}$$

where the functions a_j and a'_j are given by equations (7.15).

Subcase $n = 4m+1$. Since E_i is a proper subspace of V_a and, by (7.1), $\dim V_a = 2m$, we have $\dim E_i < 2m$. It follows that the functions $a_1, \ldots, a_{2m}$, all elements of E_i, are linearly dependent. We claim that $a_1, \ldots, a_m$ are linearly independent. Suppose that for some real numbers $c_1, \ldots, c_m$ the function $A = c_1 a_1 + \cdots + c_m a_m$ is identically zero on the group $\mathbb{Z}_{4m+1}$. Then, in particular, $A(k) = 0$ for $k = m+1, \ldots, 2m$ or, equivalently, $M_i c = 0$, where

$$M_i = \begin{pmatrix} \sin\frac{2(m+1)}{4m+1}\pi & \sin 2\frac{2(m+1)}{4m+1}\pi & \sin 3\frac{2(m+1)}{4m+1}\pi & \dots & \sin m\frac{2(m+1)}{4m+1}\pi \\ \sin\frac{2(m+2)}{4m+1}\pi & \sin 2\frac{2(m+2)}{4m+1}\pi & \sin 3\frac{2(m+2)}{4m+1}\pi & \dots & \sin m\frac{2(m+2)}{4m+1}\pi \\ \vdots & & & \ddots & \vdots \\ \sin\frac{4m}{4m+1}\pi & \sin 2\frac{4m}{4m+1}\pi & \sin 3\frac{4m}{4m+1}\pi & \dots & \sin m\frac{4m}{4m+1}\pi \end{pmatrix}_{m\times m}$$

and c is the column vector in $\mathbb{R}^m$ whose coordinates are $c_1, \dots, c_m$. For $\ell = 1, \dots, m$, let

$$x_\ell = \frac{2(m+\ell)}{4m+1}\pi$$

and define the real-valued function ϕ_ℓ on the interval $[0,\pi)$ by $\phi_\ell(x) = \sin \ell x$. In terms of these functions $M_i = (\phi_s(x_t))$, where s, $t = 1, \dots, m$. By Theorems 1.3.2 and 1.3.3(i), the matrix M_i is nonsingular. It follows that $c = 0$, so the functions $a_1, \dots, a_m$ are linearly independent. Since these linearly independent functions are elements of E_i, $\dim E_i \geq m$.

For the space E_{-i}, we claim that $a'_1, \dots, a'_m$ are linearly independent. Suppose that for some real numbers $c_1, \dots, c_m$ the function $A' = c_1 a'_1 + \cdots + c_m a'_m$ is identically zero on $\mathbb{Z}_{4m+1}$. Then, in particular, $A'(k) = 0$ for $k = m+1, \dots, 2m$ or, equivalently, $M_{-i}c = 0$, where $M_{-i} = M_i$ is nonsingular and c is the column vector in $\mathbb{R}^m$ whose coordinates are $c_1, \dots, c_m$. Thus, $c = 0$ and the functions $a'_1, \dots, a'_m$ are linearly independent, whence $\dim E_{-i} \geq m$.

Subcase $n = 4m+2$. For the space E_i we claim that the functions $a_1, \dots, a_m$ are linearly independent and for the space E_{-i} we claim that $a'_1, \dots, a'_m$ are linearly independent. Analogous to the subcase $n = 4m+1$ we have $M_i = M_{-i}$ and $M_i c = 0$, where

$$M_i = \begin{pmatrix} \sin\frac{m+1}{2m+1}\pi & \sin 2\frac{m+1}{2m+1}\pi & \sin 3\frac{m+1}{2m+1}\pi & \dots & \sin m\frac{m+1}{2m+1}\pi \\ \sin\frac{m+2}{2m+1}\pi & \sin 2\frac{m+2}{2m+1}\pi & \sin 3\frac{m+2}{2m+1}\pi & \dots & \sin m\frac{m+2}{2m+1}\pi \\ \vdots & & & \ddots & \vdots \\ \sin\frac{2m}{2m+1}\pi & \sin 2\frac{2m}{2m+1}\pi & \sin 3\frac{2m}{2m+1}\pi & \dots & \sin m\frac{2m}{2m+1}\pi \end{pmatrix}_{m\times m}$$

and c is the column vector in $\mathbb{R}^m$ whose coordinates are $c_1, \dots, c_m$. For $\ell = 1, \dots, m$, let

$$x_\ell = \frac{m+\ell}{2m+1}\pi$$

and define the real-valued function ϕ_ℓ on the interval $[0,\pi)$ by $\phi_\ell(x) = \sin \ell x$. In terms of these functions $M_i = (\phi_s(x_t))$, where s, $t = 1, \ldots, m$. By Theorems 1.3.2 and 1.3.3(i), the matrix M_i is nonsingular. Thus $c = 0$, whence $\dim E_i \geq m$ and $\dim E_{-i} \geq m$.

Since $2m = \dim V_a = \dim E_i + \dim E_{-i}$, we conclude that

$$\begin{aligned} \dim E_i &= m, \\ \dim E_{-i} &= m. \end{aligned}$$

The sets $\{a_1, \ldots, a_m\}$ and $\{a'_1, \ldots, a'_m\}$ are bases for E_i and E_{-i}, respectively.

Case 3. $n \equiv 3 \pmod 4$, that is, $n = 4m+3$ for some nonnegative integer m. We have $\lceil n/2 \rceil = 2m+2$. The vector space V_a of antisymmetric functions has an orthonormal basis

$$\begin{aligned} B_{\text{antisym}} &= \left\{ \frac{B_j - B_{-j}}{\sqrt{2}} \;\middle|\; j = 1, \ldots, 2m+1 \right\} \\ &= \{ a_j + a'_j \mid j = 1, \ldots, 2m+1 \}, \end{aligned}$$

where the functions a_j and a'_j are given by equations (7.15).

Analogous to the subcase $n = 4m+1$ we have $M_i c = 0$, where

$$M_i = \begin{pmatrix} \sin \frac{2(m+1)}{4m+3}\pi & \sin 2\frac{2(m+1)}{4m+3}\pi & \sin 3\frac{2(m+1)}{4m+3}\pi & \ldots & \sin m\frac{2(m+1)}{4m+3}\pi \\ \sin \frac{2(m+2)}{4m+3}\pi & \sin 2\frac{2(m+2)}{4m+3}\pi & \sin 3\frac{2(m+2)}{4m+3}\pi & \ldots & \sin m\frac{2(m+2)}{4m+3}\pi \\ \vdots & & & \ddots & \vdots \\ \sin \frac{4m}{4m+3}\pi & \sin 2\frac{4m}{4m+3}\pi & \sin 3\frac{4m}{4m+3}\pi & \ldots & \sin m\frac{4m}{4m+3}\pi \end{pmatrix}_{m \times m}$$

and c is the column vector in $\mathbb{R}^m$ whose coordinates are $c_1, \ldots, c_m$. For $\ell = 1, \ldots, m$, let

$$x_\ell = \frac{2(m+\ell)}{4m+3}\pi$$

and define the real-valued function ϕ_ℓ on the interval $[0,\pi)$ by $\phi_\ell(x) = \sin \ell x$. In terms of these functions $M_i = (\phi_s(x_t))$, where

s, $t = 1, \ldots, m$. By Theorems 1.3.2 and 1.3.3(i), the matrix M_i is nonsingular, hence $c = 0$. It follows that $\dim E_i \geq m$.

For the space E_{-i}, we claim that $a'_1, \ldots, a'_m, a'_{2m+1}$ are linearly independent. Suppose that for some real numbers $c_1, \ldots, c_m, c_{2m+1}$ the function

$$A' = c_1 a'_1 + \cdots + c_m a'_m + c_{2m+1} a'_{2m+1}$$

is identically zero on $\mathbb{Z}_{4m+3}$. Then, in particular, $A'(k) = 0$ for $k = m+1, \ldots, 2m+1$ or, equivalently, $M_{-i} c = 0$, where M_{-i} is the $(m+1) \times (m+1)$ matrix

$$\begin{pmatrix} \sin \frac{2(m+1)}{4m+3}\pi & \sin 2\frac{2(m+1)}{4m+3}\pi & \ldots & \sin m\frac{2(m+1)}{4m+3}\pi & \sin(2m+1)\frac{2(m+1)}{4m+3}\pi \\ \sin \frac{2(m+2)}{4m+3}\pi & \sin 2\frac{2(m+2)}{4m+3}\pi & \ldots & \sin m\frac{2(m+2)}{4m+3}\pi & \sin(2m+1)\frac{2(m+2)}{4m+3}\pi \\ \vdots & & \ddots & & \vdots \\ \sin \frac{2(2m)}{4m+3}\pi & \sin 2\frac{2(2m)}{4m+3}\pi & \ldots & \sin m\frac{2(2m)}{4m+3}\pi & \sin(2m+1)\frac{2(2m)}{4m+3}\pi \\ \sin \frac{2(2m+1)}{4m+3}\pi & \sin 2\frac{2(2m+1)}{4m+3}\pi & \ldots & \sin m\frac{2(2m+1)}{4m+3}\pi & \frac{\sqrt{4m+3}}{2} + \sin(2m+1)\frac{2(2m+1)}{4m+3}\pi \end{pmatrix}$$

and c is the column vector in $\mathbb{R}^{m+1}$ whose coordinates are $c_1, \ldots, c_m, c_{2m+1}$. The sine terms in the last column of M_{-i} are $\sin(2m+1)\frac{2(m+\ell)}{4m+3}\pi$ for $\ell = 1, \ldots, m+1$. The inequalities

$$0 < \frac{m+\ell}{4m+3} < 1$$

and

$$(2m+1)\frac{2(m+\ell)}{4m+3}\pi = \left(1 - \frac{1}{4m+3}\right)(m+\ell)\pi$$

imply that

$$\sin \frac{m+\ell}{4m+3}\pi > 0$$

and

$$\begin{aligned} \sin(2m+1)\frac{2(m+\ell)}{4m+3}\pi &= -[\cos(m+\ell)\pi] \sin \frac{m+\ell}{4m+3}\pi \\ &= (-1)^{m+\ell+1} \sin \frac{m+\ell}{4m+3}\pi. \end{aligned}$$

Thus, the entries in the last column of M_{-i} are nonzero real numbers with alternating sign. Alternatively, M_{-i} can also be constructed from M_i. First, insert the row vector

$$\left(\sin \frac{2(2m+1)}{4m+3}\pi,\ \sin 2\frac{2(2m+1)}{4m+3}\pi, \ldots,\ \sin m\frac{2(2m+1)}{4m+3}\pi\right)$$

into M_i in such a way that it is the last row of the resulting matrix, call it M_{result}. Second, insert the column vector

$$\begin{pmatrix} \sin(2m+1)\frac{2(m+1)}{4m+3}\pi \\ \sin(2m+1)\frac{2(m+2)}{4m+3}\pi \\ \vdots \\ \sin(2m+1)\frac{2(2m)}{4m+3}\pi \\ \frac{\sqrt{4m+3}}{2} + \sin(2m+1)\frac{2(2m+1)}{4m+3}\pi \end{pmatrix}_{(m+1)\times 1}$$

into M_{result} to obtain M_{-i}. Since the coordinates of this column vector are alternating sign nonzero real numbers, Theorems 1.3.2 and 1.3.3 imply that the matrix M_{-i} is nonsingular. It follows that $c = 0$, so $\dim E_{-i} \geq m + 1$.

Since $2m + 1 = \dim V_a = \dim E_i + \dim E_{-i}$, we conclude that

$$\begin{aligned} \dim E_i &= m + 1, \\ \dim E_{-i} &= m. \end{aligned}$$

The sets $\{a_1, \ldots, a_m\}$ and $\{a'_1, \ldots, a'_m,\ a'_{2m+1}\}$ are bases for E_i and E_{-i}, respectively.

We summarize the results just proved in the theorem that follows, which is due to McClellan and Parks [13].

Theorem 7.5.1. *Let n be a positive integer and for $k = 0, \ldots, \lfloor n/2 \rfloor$ let*

$$\epsilon_k = \begin{cases} 2 & \text{if } k = 0 \text{ or if } n \text{ is even and } k = n/2, \\ \sqrt{2} & \text{otherwise;} \end{cases}$$

i.e., ϵ_k is the norm of the function $B_k + B_{-k}$.

(i) *The eigenvalues of the FT on $\mathbb{Z}_n$ are ± 1, $\pm i$. Further, if m_λ denotes the multiplicity of the eigenvalue λ, then the values of m_1, m_{-1}, m_i, and m_{-i} are given in the following table*:

n	m_1	m_{-1}	m_i	m_{-i}
$4m$	$m+1$	m	$m-1$	m
$4m+1$	$m+1$	m	m	m
$4m+2$	$m+1$	$m+1$	m	m
$4m+3$	$m+1$	$m+1$	m	$m+1$

(ii) *A basis for the eigenspace corresponding to the eigenvalue* 1: *If $n = 4m$, $4m+1$, then*

$$\left\{ \frac{B_j + B_{-j} + \delta_j + \delta_{-j}}{2\epsilon_j} \;\middle|\; j = 0, \ldots, m-1, 2m \right\}$$

is a basis. If $n = 4m+2$, $4m+3$, then

$$\left\{ \frac{B_j + B_{-j} + \delta_j + \delta_{-j}}{2\epsilon_j} \;\middle|\; j = 0, \ldots, m \right\}$$

is a basis.

(iii) *A basis for the eigenspace corresponding to the eigenvalue* -1: *If $n = 4m$, $4m+1$, then*

$$\left\{ \frac{B_j + B_{-j} - (\delta_j + \delta_{-j})}{2\epsilon_j} \;\middle|\; j = 0, \ldots, m-1 \right\}$$

is a basis. If $n = 4m+2$, $4m+3$, then

$$\left\{ \frac{B_j + B_{-j} - (\delta_j + \delta_{-j})}{2\epsilon_j} \;\middle|\; j = 0, \ldots, m \right\}$$

is a basis.

(iv) *A basis for the eigenspace corresponding to the eigenvalue i*: *If $n = 4m$, then*

$$\left\{ \frac{i(B_j - B_{-j}) + (\delta_j - \delta_{-j})}{i2\sqrt{2}} \;\middle|\; j = 1, \ldots, m-1 \right\}$$

is a basis. If $n = 4m+1$, $4m+2$, $4m+3$, then

$$\left\{ \frac{i(B_j - B_{-j}) + (\delta_j - \delta_{-j})}{i2\sqrt{2}} \;\middle|\; j = 1, \ldots, m \right\}$$

is a basis.

(v) *A basis for the eigenspace corresponding to the eigenvalue* $-i$: *If* $n = 4m$, *then*

$$\left\{ \frac{i(B_j - B_{-j}) - (\delta_j - \delta_{-j})}{i2\sqrt{2}} \;\middle|\; j = 1, \ldots, m-1, 2m-1 \right\}$$

is a basis. If $n = 4m+1$, $4m+2$, *then*

$$\left\{ \frac{i(B_j - B_{-j}) - (\delta_j - \delta_{-j})}{i2\sqrt{2}} \;\middle|\; j = 1, \ldots, m \right\}$$

is a basis. If $n = 4m+3$, *then*

$$\left\{ \frac{i(B_j - B_{-j}) - (\delta_j - \delta_{-j})}{i2\sqrt{2}} \;\middle|\; j = 1, \ldots, m, 2m+1 \right\}$$

is a basis.

In the table, for instance, if $n = 4m > 0$, then the eigenvalues 1, -1, i, and $-i$ have multiplicities $m+1$, m, $m-1$, and m, respectively. Also, the theorem says that for a fixed integer n, where $n > 2$, all 4th roots of unity are eigenvalues of the FT on $\mathbb{Z}_n$.

Corollary 7.5.1. *The trace and determinant of the FT on* $\mathbb{Z}_n$ *are given in the following table*:

n	$\mathrm{tr}(\mathcal{F})$	$\det \mathcal{F}$
$4m$	$1-i$	$i(-1)^{m+1}$
$4m+1$	1	$(-1)^m$
$4m+2$	0	$(-1)^{m+1}$
$4m+3$	$-i$	$i(-1)^m$

8

The Quantum Fourier Transform

The FT has many applications, particularly in the fields of quantum computation and quantum information. In these fields, the FT is often called the *quantum Fourier transform*. Traditionally, notation used in quantum physics (i.e., the Dirac notation) to denote vectors is different from that used in mathematics. In this chapter, we introduce the Dirac notation and describe the FT in terms of the new notation.

8.1 The Dirac Notation

Let V be a finite-dimensional complex inner product space. The Dirac notation is defined for nonzero vectors only; the zero vector of V is denoted by 0 (as usual). A nonzero vector $x \in V$ is denoted by $|x\rangle$, called the *ket-vector* x; the *bra-vector* x, denoted by $\langle x|$, is defined to be the dual of x. In terms of ket and bra vectors, for x, $y \in V$, the value of the linear functional y^* at x (recall (2.6)) is denoted by $\langle y|x\rangle$, i.e.,

$$\langle y|x\rangle = \langle x, y\rangle.$$

Because of this equation, we call $\langle y|x\rangle$ the inner product of x and y.

In particular, if $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ are nonzero vectors in $\mathbb{C}^n$, then

$$\langle y|x\rangle = \langle x, y\rangle = \sum_{j=1}^{n} x_j \bar{y}_j.$$

B. Luong, *Fourier Analysis on Finite Abelian Groups*, Applied and Numerical Harmonic Analysis, DOI 10.1007/978-0-8176-4916-6_8,

In practice, the ket-vector x, i.e., $|x\rangle$, is considered to be the column vector

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \tag{8.1}$$

and the bra-vector y, i.e., $\langle y|$, is considered to be the row vector $(\bar{y}_1, \ldots, \bar{y}_n)$. With that in mind, the inner product $\langle y|x\rangle$ can be thought of as multiplication of matrices. That is, if we consider the row vector $(\bar{y}_1, \ldots, \bar{y}_n)$ as a $1 \times n$ matrix and the column vector (8.1) as an $n \times 1$ matrix, then

$$\langle y|x\rangle = (\bar{y}_1 \,\cdots\, \bar{y}_n) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Let G be a finite Abelian group. Recall from Section 2.3 that the set $\Delta_G = \{\delta_g \mid g \in G\}$ is the standard orthonormal basis of the complex vector space V_G associated with G. In terms of the ket-vector notation, we denote δ_g simply by $|g\rangle$. With this notation, equation (4.10) becomes

$$|f\rangle = \sum_{g \in G} \langle g|f\rangle \, |g\rangle,$$

where f is any non-identically zero complex-valued function defined on G and $\langle g|f\rangle = \langle f, \delta_g\rangle = f(g)$.

The purpose of the following example is to emphasize that the symbol $|0\rangle$ does not denote the zero vector! (Recall that the ket and bra vector notation are not defined for the zero vector.)

Example 8.1.1. If $G = \mathbb{Z}_n$, then $|0\rangle$ is a unit vector in the basis $\Delta_{\mathbb{Z}_n}$ and $\langle 0|$ is a linear functional on $V_{\mathbb{Z}_n}$, which is the dual of $|0\rangle$.

In summary, for a finite Abelian group G, the set $\Delta_G = \{|g\rangle \mid g \in G\}$ is the standard orthonormal basis[1] for the inner

[1] Also called the *standard computational basis.*

product space V_G. The dual of $\varDelta_G$ is the set $\varDelta_G^* = \{\langle g| : g \in G\}$, which is an orthonormal basis of the dual space V_G^*.

The character basis $B_G = \big\{|B_g\rangle : g \in G\big\}$ is sometimes called the *Fourier basis* of V_G.

Example 8.1.2. Let V and W be finite-dimensional complex inner product spaces. If $|v\rangle \in V$ and $|w\rangle \in W$, then the symbols $|w\rangle\langle v|$ define a linear operator from V to W, which maps a vector $|v'\rangle$ in V to the vector $\langle v|v'\rangle|w\rangle$ in W. The operator $|w\rangle\langle v|$ is called an *outer product* of $|w\rangle$ and $|v\rangle$, (another outer product of $|w\rangle$ and $|v\rangle$ is $|v\rangle\langle w|$, a linear operator from W to V). In general, if $\{|v_1\rangle, \ldots, |v_n\rangle\}$ and $\{|w_1\rangle, \ldots, |w_n\rangle\}$ are finite sets of vectors in V and W, respectively, then the equation

$$\mathcal{L} = |w_1\rangle\langle v_1| + \cdots + |w_n\rangle\langle v_n|$$

defines a linear operator $\mathcal{L}$ from V to W. The image of a vector $|v\rangle \in V$ is given by the equation

$$\mathcal{L}|v\rangle = \langle v_1|v\rangle|w_1\rangle + \cdots + \langle v_n|v\rangle|w_n\rangle,$$

where $\mathcal{L}|v\rangle = \mathcal{L}(|v\rangle)$.

A special case of Example 8.1.2: let G be a finite Abelian group. For a fixed $g \in G$, the outer product $|g\rangle\langle g|$ is the orthogonal projection of V_G onto the one-dimensional subspace spanned by the unit vector $|g\rangle$. More general, if S is a nonempty subset of G, then the equation

$$\mathcal{L} = \sum_{g \in S} |g\rangle\langle g|$$

defines the orthogonal projection of V_G onto the subspace spanned by the orthonormal set of vectors $\{|g\rangle : g \in S\}$. In particular, if $S = G$, then $\mathcal{L}$ is the identity operator I on V_G, i.e.,

$$I = \sum_{g \in G} |g\rangle\langle g|. \tag{8.2}$$

Equation (8.2) is known as the *completeness relation* for the orthonormal vectors $|g\rangle$, $g \in G$.

8.2 The Fourier Transform in the Dirac Notation

For each non-identically zero complex-valued function f defined on G, i.e., $|f\rangle \in V_G$, we denote the FT of $|f\rangle$ by either $\mathcal{F}|f\rangle$ or $\widehat{|f\rangle}$. These notations shall be used interchangeably.

In the Dirac notation for vectors, equation (4.1) becomes

$$\mathcal{F} = \sum_{x,\, y \,\in\, G} \langle B_x|y\rangle\, |x\rangle\langle y|,$$

where $\langle B_x|y\rangle = \langle \delta_y, B_x\rangle = \bar{B}_x(y)$. Since $\mathcal{F}$ is linear, it is uniquely determined by its action on any basis of V_G. Often, we determine $\mathcal{F}$ by expressing its values at the vectors in the standard computational basis Δ_G; by the orthonormal property of the basis Δ_G, the image of $|y\rangle \in \Delta_G$ under $\mathcal{F}$ is

$$\widehat{|y\rangle} = \sum_{x \,\in\, G} \langle B_x|y\rangle\, |x\rangle.$$

Example 8.2.1. Let $x = (x_1, \ldots, x_m)$ and $y = (y_1, \ldots, y_m)$ be elements of the group $G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m}$. By (3.4), we have

$$\bar{B}_x(y) = \frac{1}{\sqrt{n_1 \ldots n_m}} e^{-2\pi i\left(\frac{x_1 y_1}{n_1} + \cdots + \frac{x_m y_m}{n_m}\right)},$$

whence

$$\widehat{|y\rangle} = \frac{1}{\sqrt{n_1 \ldots n_m}} \sum_{x \,\in\, G} e^{-2\pi i\left(\frac{x_1 y_1}{n_1} + \cdots + \frac{x_m y_m}{n_m}\right)}\, |x\rangle.$$

It follows from this formula (with $y = 0$) that

$$\widehat{|0\rangle} = \frac{1}{\sqrt{|G|}} \sum_{x \,\in\, G} |x\rangle.$$

Example 8.2.2. If $G = \mathbb{Z}_n^m$, then by the previous example (with $n_j = n$, for $j = 1, \ldots, m$) we have

$$\widehat{|y\rangle} = \frac{1}{\sqrt{n^m}} \sum_{x \,\in\, \mathbb{Z}_n^m} e^{-\frac{2\pi i}{n} x\cdot y}\, |x\rangle \tag{8.3}$$

for all $y \in \mathbb{Z}_n^m$, where $x \cdot y = x_1 y_1 + \cdots + x_m y_m$. In particular, if $n = 2$, then

$$\widehat{|y\rangle} = \frac{1}{\sqrt{2^m}} \sum_{x \,\in\, \mathbb{Z}_2^m} (-1)^{x \cdot y}\, |x\rangle. \tag{8.4}$$

For the group $\mathbb{Z}_n = \{j \mid j = 0, \ldots, n-1\}$, we have, by (8.3) with $m = 1$, that

$$\widehat{|j\rangle} = \frac{1}{\sqrt{n}} \sum_{k \,\in\, \mathbb{Z}_n} e^{-\frac{2\pi i}{n} jk}\, |k\rangle. \tag{8.5}$$

Setting $n = 2$ in equation (8.5) (or setting $m = 1$ in equation (8.4)) we obtain

$$\widehat{|0\rangle} = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad \text{and} \quad \widehat{|1\rangle} = \frac{|0\rangle - |1\rangle}{\sqrt{2}},$$

which can be combined into one formula as

$$\widehat{|k\rangle} = \frac{|0\rangle + (-1)^k |1\rangle}{\sqrt{2}}, \tag{8.6}$$

where $k = 0$, 1.

Notation conventions. There are notation conventions for the tensor product when the group in consideration (or the underlying group) is either $\mathbb{Z}_2^m$ or $\mathbb{Z}_{2^m}$. First, if the underlying group is $\mathbb{Z}_2^m$ and $y = (y_1, \ldots, y_m)$ is an element of this group, then by Exercise 15 (at the end of Chapter 3) and Theorem 6.2.1 we have

$$\delta_y = \delta_{y_1} \otimes \cdots \otimes \delta_{y_m} \quad \text{and} \quad \hat{\delta}_y = \hat{\delta}_{y_1} \otimes \cdots \otimes \hat{\delta}_{y_m}.$$

In the ket-vector notation, these equations become

$$|y\rangle = |y_1\rangle \otimes \cdots \otimes |y_m\rangle \quad \text{and} \quad \widehat{|y\rangle} = \widehat{|y_1\rangle} \otimes \cdots \otimes \widehat{|y_m\rangle}, \tag{8.7}$$

respectively.

Since there is a natural one-to-one correspondence between the set $\mathbb{Z}_2^m$ and the set of all bit-strings of length m given by

$$(y_1, \ldots, y_m) \leftrightarrow y_1 \ldots y_m,$$

we may identify y with the ordered bit-string $y_1 \dots y_m$ and write $y = y_1 \dots y_m$. Also, for simplicity we write the tensor product $|y_1\rangle \otimes \cdots \otimes |y_m\rangle$ simply as $|y_1\rangle \cdots |y_m\rangle$. With this simplification and the defined identification, equations (8.7) can be written as

$$|y\rangle = |y_1 \dots y_m\rangle = |y_1\rangle \cdots |y_m\rangle \quad \text{and} \quad \widehat{|y\rangle} = \widehat{|y_1\rangle} \dots \widehat{|y_m\rangle}. \tag{8.8}$$

Second, since the groups $\mathbb{Z}_{2^m}$ and $\mathbb{Z}_2^m$ have the same number of elements, namely, 2^m, there is a one-to-one correspondence between them. Moreover, there is a canonical one-to-one correspondence between the two groups, which may be described as follows: by the Euclidean division algorithm, each $y \in \mathbb{Z}_{2^m}$ can be expressed uniquely in base 2 as

$$y = y_1 2^{m-1} + y_2 2^{m-2} + \cdots + y_{m-1} 2 + y_m,$$

where, for each $j = 1, \dots, m$, y_j is either 0 or 1. Thus, the function $\omega\colon \mathbb{Z}_{2^m} \to \mathbb{Z}_2^m$ defined by

$$\omega(y) = y_1 \dots y_m$$

is bijective. The ordered bit-string $y_1 \dots y_m$ is the *binary representation* of y. Through the correspondence ω, we identify y with its binary representation $y_1 \dots y_m$ and write

$$y = y_1 \dots y_m.$$

Remarks.

1) Since ω is a one-to-one correspondence between the bases $\Delta_{\mathbb{Z}_{2^m}}$ and $\Delta_{\mathbb{Z}_2^m}$ of the inner product spaces $V_{\mathbb{Z}_{2^m}}$ and $V_{\mathbb{Z}_2^m}$, respectively, the linear extension of ω to the entire space $V_{\mathbb{Z}_{2^m}}$, also denoted by ω, is an isometry between $V_{\mathbb{Z}_{2^m}}$ and $V_{\mathbb{Z}_2^m}$.
2) For $y \in \mathbb{Z}_{2^m}$, we observe from (8.5) with $n = 2^m$, where $m > 1$, that some[2] coefficients of the vector $\mathcal{F}|y\rangle$ (in the basis $\Delta_{\mathbb{Z}_{2^m}}$) are complex numbers (which are not real), whereas by (8.4) all coefficients of the vector $\mathcal{F}|\omega(y)\rangle \in V_{\mathbb{Z}_2^m}$ (in the basis $\Delta_{\mathbb{Z}_2^m}$) are real numbers; in fact, they are either 1 or -1. Thus, the following diagram is not commutative:

[2] If m is large, then most of the coefficients are in $\mathbb{C}$ and not in $\mathbb{R}$.

$$\begin{tikzcd} V_{\mathbb{Z}_{2^m}} \arrow[r, "\mathcal{F}"] \arrow[d, "\omega"'] & V_{\mathbb{Z}_{2^m}} \arrow[d, "\omega"] \\ V_{\mathbb{Z}_2^m} \arrow[r, "\mathcal{F}"] & V_{\mathbb{Z}_2^m} \end{tikzcd}$$

3) In the field of quantum computation, often the space $V_{\mathbb{Z}_{2^m}}$ is used as a state space (i.e., an underlying space in which all mathematical representations of a quantum physical system under consideration take place). To compute the FT of basis vectors, i.e., to evaluate finite sums such as that in (8.5) with $n = 2^m$, it is convenient to identify the spaces $V_{\mathbb{Z}_{2^m}}$ and $V_{\mathbb{Z}_2^m}$ by the identification ω. Then, a quantum circuit (i.e., a composition of a finite number of tensor products of, not necessarily distinct, linear isometries on $V_{\mathbb{Z}_2}$) is used for the computation. That is, to compute the sum in (i) of Theorem 8.2.1 below, a quantum circuit is used to compute its identification, the tensor product. The point here is that the correspondence ω necessitates the construction of a quantum algorithm to evaluate the FT on $\mathbb{Z}_{2^m}$. For this reason, the product (or composition) $\omega\mathcal{F}$ is useful.

Theorem 8.2.1.

(i) *For each $j \in \mathbb{Z}_{2^m}$, we have the identity*

$$\sum_{k=0}^{2^m-1} e^{-\frac{2\pi i}{2^m} jk} \,|k\rangle = \bigotimes_{\nu=1}^{m} (|0\rangle + e^{-\frac{2\pi i}{2^\nu} j} |1\rangle).$$

(ii) *For each $y = (y_1, \dots, y_m) \in \mathbb{Z}_2^m$, we have the identity*

$$\sum_{x \in \mathbb{Z}_2^m} (-1)^{x \cdot y} \,|x\rangle = \bigotimes_{\nu=1}^{m} (|0\rangle + (-1)^{y_\nu} |1\rangle).$$

Notes.

(a) In this theorem the notation $\bigotimes$ has the following meaning:

$$\bigotimes_{\nu=1}^{m} |x_\nu\rangle = |x_1\rangle \dots |x_m\rangle.$$

(b) In (i), the sum is an element of the vector space $V_{\mathbb{Z}_{2^m}}$ while the tensor product is an element of the space $V_{\mathbb{Z}_2^m}$. The equality means that they are identified by the correspondence ω.

Proof of Theorem 8.2.1. To prove (i), for each $k = 0, \ldots, 2^m - 1$, we express k (in base 2) as

$$k = k_1 2^{m-1} + k_2 2^{m-2} + \cdots + k_{m-1} 2 + k_m,$$

where $k_\nu = 0$, 1. Upon dividing both sides by 2^m, we have

$$\frac{k}{2^m} = \frac{k_1}{2} + \frac{k_2}{2^2} + \cdots + \frac{k_{m-1}}{2^{m-1}} + \frac{k_m}{2^m}.$$

If we write $k = k_1 \ldots k_m$, then

$$\begin{aligned}
\sum_{k=0}^{2^m-1} e^{-\frac{2\pi i}{2^m} jk} \, |k\rangle &= \sum_{k_1, \ldots, k_m = 0}^{1} \quad e^{-2\pi i j \left(\sum_{\nu=1}^m \frac{k_\nu}{2^\nu}\right)} |k_1 \ldots k_m\rangle \\
&= \sum_{k_1, \ldots, k_m = 0}^{1} \bigotimes_{\nu=1}^{m} e^{-\frac{2\pi i}{2^\nu} j k_\nu} |k_\nu\rangle \\
&= \bigotimes_{\nu=1}^{m} \sum_{k_\nu = 0}^{1} e^{-\frac{2\pi i}{2^\nu} j k_\nu} |k_\nu\rangle \qquad \text{(bilinearity of } \otimes\text{)} \\
&= \bigotimes_{\nu=1}^{m} \Big(|0\rangle + e^{-\frac{2\pi i}{2^\nu} j} |1\rangle \Big).
\end{aligned}$$

(ii) Let $y = (y_1, \ldots, y_m)$ be an element of the group $\mathbb{Z}_2^m$ and identify y with the ordered bit-string $y_1 \ldots y_m$, i.e., write $y = y_1 \ldots y_m$. Since $|y\rangle = |y_1\rangle \ldots |y_m\rangle$, it follows from (8.8) and (8.6) that

$$\widehat{|y\rangle} = \bigotimes_{\nu=1}^{m} \widehat{|y_\nu\rangle} = \frac{1}{\sqrt{2^m}} \bigotimes_{\nu=1}^{m} \Big(|0\rangle + (-1)^{y_\nu} |1\rangle \Big).$$

On the other hand, we recall from (8.4) that

$$\widehat{|y\rangle} = \frac{1}{\sqrt{2^m}} \sum_{x \in \mathbb{Z}_2^m} (-1)^{x \cdot y} \, |x\rangle.$$

■

The FT plays an important role in the two well-known quantum algorithms, Shor's and Grover's algorithms. For readers who are interested in quantum computation and, in particular, the two mentioned quantum algorithms we recommend [18].

Exercise.

55. In this exercise we assume that V is a finite-dimensional complex inner product space and every vector belongs to V. Also, we denote the adjoint of a linear operator A (on V) by A^*. Prove the following:

(i) $(|x\rangle\langle y|)^* = |y\rangle\langle x|$; in particular, $|x\rangle\langle x|$ is self-adjoint.

(ii) $|x\rangle\langle y||u\rangle\langle v| = \langle y|u\rangle|x\rangle\langle v|$.

(iii) $\||x\rangle\langle y|\| = \||x\rangle\|\||y\rangle\|$.

(iv) P is a 1-dimensional orthogonal projection (i.e., projection of rank 1) if and only if $P = |x\rangle\langle x|$ for some unit vector $|x\rangle$.

(v) $A|x\rangle\langle y| = |Ax\rangle\langle y|$ and $|x\rangle\langle y|A = |x\rangle\langle A^*y|$. It follows that if $V = V_G$ and $A = \mathcal{F}$, then we have

$$\mathcal{F}|f\rangle\langle g| = |\hat{f}\rangle\langle g|$$

for every f and g in V_G.

9

Quadratic Gaussian Sums

Recall that the quadratic Gaussian sum of order n is the complex-valued function G_n defined on the set of integers by the equation

$$G_n(x) = \frac{1}{\sqrt{n}} \sum_{k \in \mathbb{Z}_n} e^{-\frac{2\pi i}{n} k^2 x}.$$

If n is prime, then one may use the expression on the left of the equation in Theorem 1.2.3 as a definition for $G_n(x)$ (see page 71 of [7]).

9.1 The Number $G_n(1)$

For an odd prime p, we showed that $G_p(1)$ is an eigenvalue of the FT on $\mathbb{Z}_p$ (Theorem 7.2.4 on page 101). Also, Corollary 7.2.2 on page 103 reduces the determination of $G_p(a)$ to the evaluation of $G_p(1)$. Presently, we evaluate $G_p(1)$. We can do more by giving a general formula for $G_n(1)$.

Theorem 9.1.1. *If n is a positive integer, then*

$$G_n(1) = \frac{1 + i^n}{1 + i}.$$

Proof. Consider the function $f\colon [0,1] \to \mathbb{C}$ defined by

$$f(x) = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} e^{-\frac{2\pi i}{n}(k+x)^2}.$$

B. Luong, *Fourier Analysis on Finite Abelian Groups*, Applied and Numerical Harmonic Analysis, DOI 10.1007/978-0-8176-4916-6_9,

Since $f(0) = f(1)$ (by Theorem 1.1 on page 2), we can extend f periodically (with period 1) to a piecewise smooth continuous function on $\mathbb{R}$. If we denote this extension also by f, then the Fourier series of f converges (uniformly) to f at every point $x \in \mathbb{R}$, that is,

$$f(x) = \sum_{m=-\infty}^{\infty} a_m e^{2\pi imx},$$

where

$$a_m = \int_0^1 f(x) e^{-2\pi imx}\,\mathrm{d}x. \tag{9.1}$$

Since $G_n(1) = f(0) = \sum_{m=-\infty}^{\infty} a_m$, our aim is to evaluate this infinite series. First, we express the general term a_m in a form that can be added without much difficulty. Using the defining sum of f in the integrand of (9.1) we have

$$\begin{aligned} a_m &= \frac{1}{\sqrt{n}} \int_0^1 \sum_{k=0}^{n-1} e^{-\frac{2\pi i}{n}(k+x)^2} e^{-2\pi imx}\,\mathrm{d}x \\ &= \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} \int_0^1 e^{-2\pi i\frac{(k+x)^2+mnx}{n}}\,\mathrm{d}x. \end{aligned}$$

Now the exponent of e in the last integral can be rewritten as follows:

$$\begin{aligned} &-2\pi i\frac{(k+x)^2+mnx}{n} \\ &\quad = -2\pi i\left(\frac{\left(k+x+\frac{1}{2}mn\right)^2 - kmn - \frac{1}{4}m^2n^2}{n}\right) \\ &\quad = -2\pi i\left(\frac{\left(k+x+\frac{1}{2}mn\right)^2}{n} - km - \frac{1}{4}m^2 n\right) \\ &\quad = -2\pi i\frac{\left(k+x+\frac{1}{2}mn\right)^2}{n} + 2\pi ikm + \frac{\pi i}{2}m^2 n. \end{aligned}$$

It follows that

$$e^{-2\pi i\frac{(k+x)^2+mnx}{n}} = e^{\frac{\pi i}{2}m^2 n} e^{-2\pi i\frac{(k+x+\frac{1}{2}mn)^2}{n}} = i^{m^2 n} e^{-2\pi i\frac{(k+x+\frac{1}{2}mn)^2}{n}},$$

whence

$$a_m = \frac{i^{m^2n}}{\sqrt{n}} \sum_{k=0}^{n-1} \int_0^1 e^{-2\pi i \frac{(k+x+\frac{1}{2}mn)^2}{n}} \, \mathrm{d}x.$$

The change of variable $u = k + x + \frac{1}{2}mn$ leads to

$$a_m = \frac{i^{m^2n}}{\sqrt{n}} \sum_{k=0}^{n-1} \int_{k+\frac{1}{2}mn}^{k+1+\frac{1}{2}mn} e^{-2\pi i \frac{u^2}{n}} \, \mathrm{d}u = \frac{i^{m^2n}}{\sqrt{n}} \int_{\frac{1}{2}mn}^{n+\frac{1}{2}mn} e^{-2\pi i \frac{u^2}{n}} \, \mathrm{d}u.$$

Using the last equation for a_m we have

$$G_n(1) = \sum_{m=-\infty}^{\infty} a_m = \frac{1}{\sqrt{n}} \sum_{m=-\infty}^{\infty} i^{m^2n} \int_{\frac{1}{2}mn}^{n+\frac{1}{2}mn} e^{-2\pi i \frac{u^2}{n}} \, \mathrm{d}u.$$

Next, since

$$m^2 \equiv \begin{cases} 0 \pmod 4 & \text{if } m \text{ is even,} \\ 1 \pmod 4 & \text{if } m \text{ is odd,} \end{cases}$$

we have

$$i^{m^2n} = \begin{cases} 1 & \text{if } m \text{ is even,} \\ i^n & \text{if } m \text{ is odd.} \end{cases}$$

Consequently,

$$\begin{aligned} G_n(1) & \\ &= \frac{1}{\sqrt{n}} \left\{ \sum_{m \text{ even}} \int_{\frac{1}{2}mn}^{n+\frac{1}{2}mn} e^{-2\pi i \frac{u^2}{n}} \, \mathrm{d}u + i^n \sum_{m \text{ odd}} \int_{\frac{1}{2}mn}^{n+\frac{1}{2}mn} e^{-2\pi i \frac{u^2}{n}} \, \mathrm{d}u \right\} \\ &= \frac{1+i^n}{\sqrt{n}} \int_{-\infty}^{\infty} e^{-2\pi i \frac{u^2}{n}} \, \mathrm{d}u \\ &= (1+i^n) 2 \int_0^{\infty} e^{-2\pi i t^2} \, \mathrm{d}t \qquad (t = u/\sqrt{n}). \end{aligned}$$

To evaluate the last integral, we observe that

$$1 = G_1(1) = (1+i) 2 \int_0^{\infty} e^{-2\pi i t^2} \, \mathrm{d}t,$$

from which we may conclude that

$$2\int_0^\infty e^{-2\pi i t^2}\,\mathrm{d}t = \frac{1}{1+i}. \tag{9.2}$$

Therefore, we have

$$G_n(1) = \frac{1+i^n}{1+i}. \qquad \blacksquare$$

The proof of Theorem 9.1.1 contains the following results (which is normally seen in advanced calculus):

$$\int_0^\infty \cos(x^2)\,\mathrm{d}x = \int_0^\infty \sin(x^2)\,\mathrm{d}x = \frac{1}{2}\sqrt{\frac{\pi}{2}}.$$

These equations follow from (9.2) by equating the real and imaginary parts of the two sides.

9.2 Reduction Formulas

After we found a simple formula for $G_n(1)$, we concentrate on evaluating (or simplifying) $G_n(a)$ for arbitrary integers a and n with $n > 0$. We need the following lemma.

Lemma 9.2.1.

(i) *If m and n are relatively prime positive integers, then*

$$\begin{aligned}\mathbb{Z}_{mn} &= n\mathbb{Z}_m + m\mathbb{Z}_n \pmod{mn}\\ &= \big\{(nx+my) \pmod{mn} \mid x \in \mathbb{Z}_m \text{ and } y \in \mathbb{Z}_n\big\}.\end{aligned}$$

(ii) *If j and n are positive integers, then*

$$\mathbb{Z}_{n^\nu} = n^{\nu-j}\mathbb{Z}_{n^j} + \mathbb{Z}_{n^{\nu-j}} = \big\{n^{\nu-j}\alpha + \beta \mid \alpha \in \mathbb{Z}_{n^j} \text{ and } \beta \in \mathbb{Z}_{n^{\nu-j}}\big\}$$

for any integer $\nu \geq j$.

Proof. (i) It is clear that $n\mathbb{Z}_m + m\mathbb{Z}_n \pmod{mn} \subset \mathbb{Z}_{mn}$. For the reverse inclusion let $k \in \mathbb{Z}_{mn}$. If m and n are relatively prime, then $c_1 n + c_2 m = 1$ for some integers c_1 and c_2, so $k = kc_1 n + kc_2 m$. Now observe that there are integers j and j' such that $x \overset{\text{def}}{=} (jm+kc_1) \in \mathbb{Z}_m$ and $y \overset{\text{def}}{=} (j'n+kc_2) \in \mathbb{Z}_n$. Then we have

$$k = nx + my \pmod{mn},$$

whence $\mathbb{Z}_{mn} \subset n\mathbb{Z}_m + m\mathbb{Z}_n \pmod{mn}$.

(ii) Fix a positive integer j and assume that $\nu \geq j$. Since $0 \leq n^{\nu-j}\alpha + \beta \leq n^{\nu} - 1$ for any $\alpha \in \mathbb{Z}_{n^j}$ and $\beta \in \mathbb{Z}_{n^{\nu-j}}$, we have $n^{\nu-j}\mathbb{Z}_{n^j} + \mathbb{Z}_{n^{\nu-j}} \subset \mathbb{Z}_{n^\nu}$. Conversely, the Euclidean division algorithm implies that every $m \in \mathbb{Z}_{n^\nu}$ can be written as $m = \alpha n^{\nu-j} + \beta$ for some $\alpha \in \mathbb{Z}_{n^j}$ and $\beta \in \mathbb{Z}_{n^{\nu-j}}$. Thus $\mathbb{Z}_{n^\nu} \subset n^{\nu-j}\mathbb{Z}_n + \mathbb{Z}_{n^{\nu-j}}$. ■

The following theorem enables us to evaluate $G_n(a)$.

Theorem 9.2.1. *Let a, m, n, and ν be integers. Suppose that $m, n > 0$, p is a prime, and $p \nmid a$.*

(i) *If m and n are relatively prime, then $G_{mn}(a) = G_m(an)$ $G_n(am)$.*
(ii) *If $k \in \mathbb{Z}$ and $\nu \geq 1$, then $G_{n^\nu}(kn) = \sqrt{n}\, G_{n^{\nu-1}}(k)$.*
(iii) *If either $\nu \geq 2$ and $p > 2$ or $\nu \geq 4$ and $p = 2$, then $G_{p^\nu}(a) = G_{p^{\nu-2}}(a)$.*

Proof. (i) Assume that m and n are relatively prime. We have

$$\begin{aligned}
G_m(an)G_n(am) &= \frac{1}{\sqrt{m}} \sum_{\alpha \in \mathbb{Z}_m} e^{-2\pi i \frac{an\alpha^2}{m}} \frac{1}{\sqrt{n}} \sum_{\beta \in \mathbb{Z}_n} e^{-2\pi i \frac{am\beta^2}{n}} \\
&= \frac{1}{\sqrt{mn}} \sum_{\substack{\alpha \in \mathbb{Z}_m \\ \beta \in \mathbb{Z}_n}} e^{-2\pi i a \frac{\alpha^2 n^2 + \beta^2 m^2}{mn}} \\
&= \frac{1}{\sqrt{mn}} \sum_{\substack{\alpha \in \mathbb{Z}_m \\ \beta \in \mathbb{Z}_n}} e^{-2\pi i a \frac{(\alpha n + \beta m)^2}{mn}} \\
&= \frac{1}{\sqrt{mn}} \sum_{k \in \mathbb{Z}_{mn}} e^{-\frac{2\pi i a k^2}{mn}} \qquad \big(\text{Lemma 9.2.1(i)}\big) \\
&= G_{mn}(a).
\end{aligned}$$

(ii) Assume that $\nu \geq 1$. For $a \in \mathbb{Z}$ we have

$$G_{n^\nu}(a) = \frac{1}{\sqrt{n^\nu}} \sum_{m \in \mathbb{Z}_{n^\nu}} e^{-\frac{2\pi i a m^2}{n^\nu}} = \frac{1}{\sqrt{n^\nu}} \sum_{\substack{\alpha \in \mathbb{Z}_n \\ \beta \in \mathbb{Z}_{n^{\nu-1}}}} e^{-\frac{2\pi i a(\beta+\alpha n^{\nu-1})^2}{n^\nu}},$$

where the last equality is assured by Lemma 9.2.1(ii) (with $j = 1$). It follows from the following equation for the exponent

$$-\frac{2\pi i a(\beta + \alpha n^{\nu-1})^2}{n^\nu} = -\frac{2\pi i a \beta^2}{n^\nu} - 4\pi i a \alpha \frac{\beta}{n} - 2\pi i a \alpha^2 n^{\nu-2},$$

that

$$G_{n^\nu}(a) = \frac{1}{\sqrt{n^\nu}} \sum_{\beta \in \mathbb{Z}_{n^{\nu-1}}} e^{-\frac{2\pi i a \beta^2}{n^\nu}} \sum_{\alpha \in \mathbb{Z}_n} e^{-4\pi i a \alpha \frac{\beta}{n}}\, e^{-2\pi i a \alpha^2 n^{\nu-2}}. \quad (9.3)$$

Thus, for $a = kn$ we have $e^{-4\pi i a \alpha \beta / n} = 1$ and equation (9.3) becomes

$$G_{n^\nu}(kn) = \frac{1}{\sqrt{n^\nu}} \sum_{\beta \in \mathbb{Z}_{n^{\nu-1}}} e^{-\frac{2\pi i k \beta^2}{n^{\nu-1}}} \sum_{\alpha \in \mathbb{Z}_n} e^{-2\pi i k \alpha^2 n^{\nu-1}}.$$

The assumption $\nu \geq 1$ assures that $e^{-2\pi i k \alpha^2 n^{\nu-1}} = 1$, hence

$$\begin{aligned} G_{n^\nu}(kn) &= \frac{n}{\sqrt{n^\nu}} \sum_{\beta \in \mathbb{Z}_{n^{\nu-1}}} e^{-\frac{2\pi i k \beta^2}{n^{\nu-1}}} \\ &= \frac{n}{\sqrt{n^\nu}} \sqrt{n^{\nu-1}}\, G_{n^{\nu-1}}(k) = \sqrt{n} G_{n^{\nu-1}}(k). \end{aligned}$$

(iii) First, assume that $\nu \geq 2$ and p is odd. The assumption $\nu \geq 2$ implies that $e^{-2\pi i a \alpha^2 p^{\nu-2}} = 1$, thus equation (9.3) (with $n = p$) is simplified to

$$G_{p^\nu}(a) = \frac{1}{\sqrt{p^\nu}} \sum_{\beta \in \mathbb{Z}_{p^{\nu-1}}} e^{-\frac{2\pi i a \beta^2}{p^\nu}} \sum_{\alpha \in \mathbb{Z}_p} e^{-4\pi i a \alpha \frac{\beta}{p}}.$$

By the geometric progression formula (in the case $p \nmid \beta$)

$$\sum_{\alpha \in \mathbb{Z}_p} e^{-4\pi i a \alpha \frac{\beta}{p}} = \begin{cases} p & \text{if } p \mid \beta, \\ 0 & \text{if } p \nmid \beta, \end{cases}$$

whence

$$G_{p^\nu}(a) = \frac{p}{\sqrt{p^\nu}} \sum_{\substack{\beta\,\in\,\mathbb{Z}_{p^{\nu-1}}\\ p\,|\,\beta}} e^{-\frac{2\pi i a\beta^2}{p^\nu}} = \frac{1}{\sqrt{p^{\nu-2}}} \sum_{\substack{\beta\,\in\,\mathbb{Z}_{p^{\nu-1}}\\ p\,|\,\beta}} e^{-\frac{2\pi i a}{p^{\nu-2}}\left(\frac{\beta}{p}\right)^2}.$$

Since the subset of $\mathbb{Z}_{p^{\nu-1}}$ that consists of multiples of p is $p\mathbb{Z}_{p^{\nu-2}}$, we have

$$G_{p^\nu}(a) = \frac{1}{\sqrt{p^{\nu-2}}} \sum_{k\,\in\,\mathbb{Z}_{p^{\nu-2}}} e^{-\frac{2\pi i a k^2}{p^{\nu-2}}} = G_{p^{\nu-2}}(a).$$

Next, assume that $\nu \geq 4$ and $p = 2$. We have

$$\begin{aligned} G_{2^\nu}(a) &= \frac{1}{\sqrt{2^\nu}} \sum_{k\,\in\,\mathbb{Z}_{2^\nu}} e^{-\frac{2\pi i a k^2}{2^\nu}} \\ &= \frac{1}{\sqrt{2^\nu}} \sum_{\substack{\alpha\,\in\,\mathbb{Z}_{2^2}\\ \beta\,\in\,\mathbb{Z}_{2^{\nu-2}}}} e^{-\frac{2\pi i a(\beta+\alpha 2^{\nu-2})^2}{2^\nu}} \qquad \begin{pmatrix}\text{Lemma 9.2.1(ii)}\\ \text{with } j = 2 \text{ and } n = 2\end{pmatrix} \\ &= \frac{1}{\sqrt{2^\nu}} \sum_{\beta\,\in\,\mathbb{Z}_{2^{\nu-2}}} e^{-\frac{2\pi i a\beta^2}{2^\nu}} \sum_{\alpha\,\in\,\mathbb{Z}_{2^2}} e^{-\pi i a\alpha\beta}. \end{aligned}$$

It is easy to verify that

$$\sum_{\alpha\,\in\,\mathbb{Z}_4} e^{-\pi i a\alpha\beta} = 2\left(1 + e^{-\pi i a\beta}\right) = \begin{cases} 4 & \text{if } 2 \mid \beta, \\ 0 & \text{if } 2 \nmid \beta, \end{cases}$$

whence

$$G_{2^\nu}(a) = \frac{4}{\sqrt{2^\nu}} \sum_{\substack{\beta\,\in\,\mathbb{Z}_{2^{\nu-2}}\\ 2\,|\,\beta}} e^{-\frac{2\pi i a\beta^2}{2^\nu}} = \frac{2}{\sqrt{2^{\nu-2}}} \sum_{\substack{\beta\,\in\,\mathbb{Z}_{2^{\nu-2}}\\ 2\,|\,\beta}} e^{-\frac{2\pi i a}{2^{\nu-2}}\left(\frac{\beta}{2}\right)^2}.$$

Since the subset of $\mathbb{Z}_{2^{\nu-2}}$ that consists of multiples of 2 is $2\mathbb{Z}_{2^{\nu-3}}$, we have

$$G_{2^\nu}(a) = \frac{2}{\sqrt{2^{\nu-2}}} \sum_{k\,\in\,\mathbb{Z}_{2^{\nu-3}}} e^{-\frac{2\pi i a k^2}{2^{\nu-2}}}.$$

Finally, equation (1.7) on page 15 implies that

$$G_{2^\nu}(a) = \frac{1}{\sqrt{2^{\nu-2}}} \sum_{k\,\in\,\mathbb{Z}_{2^{\nu-2}}} e^{-\frac{2\pi i a k^2}{2^{\nu-2}}} = G_{2^{\nu-2}}(a). \qquad \blacksquare$$

Statement (i) of Theorem 9.2.1 reduces the study of $G_m(n)$ to a special case $G_{p^\nu}(n)$, where p is a prime. Statement (ii) reduces the determination of $G_{p^\nu}(n)$ to the case $G_{p^\nu}(n)$, where $p \nmid n$. Statement (iii) reduces the power ν to its smallest permissible value. When $p = 2$ and n is odd, the determination of $G_{p^\nu}(n)$ rests on the evaluation of either $G_4(n)$ or $G_8(n)$ depending on whether ν is even or odd, respectively. The evaluations of $G_4(n)$ and $G_8(n)$ are trivial; their values are given in the following corollary.

Corollary 9.2.1. *Suppose that k, n, ν are integers.*

(i)

$$G_2(n) = \begin{cases} 0 & \textit{if } n \textit{ is odd,} \\ \sqrt{2} & \textit{if } n \textit{ is even.} \end{cases}$$

$$G_4(n) = 1 + (-i)^n.$$

$$G_8(n) = \frac{1}{\sqrt{2}}\left(1 + (-1)^n + 2e^{-\frac{n\pi i}{4}}\right).$$

(ii) *If $\nu > 0$, p is an odd prime, and a is an integer that is not divisible by p, then*

$$G_{p^\nu}(a) = \begin{cases} 1 & \textit{if } \nu \textit{ is even,} \\ (a/p)G_p(1) & \textit{if } \nu \textit{ is odd.} \end{cases}$$

(iii) *If $\nu \geq 4$ and n is odd, then*

$$G_{2^\nu}(n) = \begin{cases} 1 - i^n & \textit{if } \nu \textit{ is even,} \\ \sqrt{2}e^{-\frac{n\pi i}{4}} & \textit{if } \nu \textit{ is odd.} \end{cases}$$

(iv) *If $\nu > n \geq 0$ and k is odd, then $G_{2^\nu}(k2^n) = (\sqrt{2})^n G_{2^{\nu-n}}(k)$.*

Example 9.2.1. Suppose that $n = 1139062500$ and $a = 7882875$. This example illustrates the use of various results obtained to evaluate $G_n(a)$. First, it is necessary to find the prime power decomposition of n. We find that $n = (2^2)(3^6)(5^8)$. Then by (i) of Theorem 9.2.1 we have

$$\begin{aligned} G_n(a) &= G_{2^2}(3^6 5^8 a) G_{3^6 5^8}(2^2 a) \\ &= G_{2^2}(3^6 5^8 a) G_{3^6}(2^2 5^8 a) G_{5^8}(2^2 3^6 a). \end{aligned}$$

Next, we evaluate each term in the product on the right-hand side of the last equality separately. For that, it is necessary to find the prime power decomposition of a. We find that $a = (3^2)(5^3)(7^2)(11)(13)$.

Evaluation of $G_{2^2}(3^6 5^8 a)$: By (iii) of the previous corollary, $G_{2^2}(3^6 5^8 a) = 1 - i^{3^6 5^8 a}$. Since $3^6 5^8 a \equiv 3 \pmod 4$ we have $i^{3^6 5^8 a} = -i$, whence

$$G_{2^2}(3^6 5^8 a) = 1 + i. \tag{9.4}$$

Evaluation of $G_{3^6}(2^2 5^8 a)$: By (ii) of Theorem 9.2.1 and (ii) of the previous corollary, we have

$$G_{3^6}(2^2 5^8 a) = G_{3^6}(2^2 3^2 b) = 3 G_{3^4}(2^2 b) = 3, \tag{9.5}$$

where $b = 5^{11} 7^2 (11)(13)$.

Evaluation of $G_{5^8}(2^2 3^6 a)$: We have $G_{5^8}(2^2 3^6 a) = G_{5^8}(5^3 c)$ with $c = 2^2 3^8 7^2 (11)(13)$. Part (ii) of Theorem 9.2.1 implies that $G_{5^8}(2^2 3^6 a) = 5\sqrt{5} G_{5^5}(c)$. By (ii) of the previous corollary and (i) of Theorem 1.2.1,

$$G_{5^8}(2^2 3^6 a) = 5\sqrt{5}(2^2/5)(3^8/5)(7^2/5)(11/5)(13/5) G_5(1).$$

Again, by (i) of Theorem 1.2.1, we have

$$G_{5^8}(2^2 3^6 a) = 5\sqrt{5}(2/5)^2(3/5)^8(7/5)^2(11/5)(13/5) G_5(1).$$

Since the value of each of the Legendre symbols (2/5), (3/5), and (7/5) is either 1 or -1, the square of each has value 1. Also, since $(11/5) = 1$ and $(13/5) = -1$, it follows that

$$G_{5^8}(2^2 3^6 a) = -5\sqrt{5} G_5(1) = -5\sqrt{5}\frac{1 + i^5}{1 + i} = -5\sqrt{5}. \tag{9.6}$$

We gather the results from (9.4)–(9.6) and obtain

$$G_n(a) = -15\sqrt{5}(1 + i).$$

As an application of some of the results about Gaussian sums, we give a short proof of the Quadratic Reciprocity Law for the Legendre symbol.

Theorem 9.2.2 (Quadratic Reciprocity Law). *If p and q are distinct odd primes, then*

$$(p/q)(q/p) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Proof. By Corollary 7.2.2 (on page 103), (i) of Theorem 9.2.1, and Theorem 9.1.1 we have

$$(p/q)(q/p) = \frac{G_p(q)G_q(p)}{G_p(1)G_q(1)} = \frac{G_{pq}(1)}{G_p(1)G_q(1)} = \frac{(1+i^{pq})(1+i)}{(1+i^p)(1+i^q)}.$$

It is easy to verify that

$$\frac{(1+i^{pq})(1+i)}{(1+i^p)(1+i^q)} = \begin{cases} 1 & \text{if either } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4, \\ -1 & \text{otherwise,} \end{cases}$$

therefore $(p/q)(q/p) = (-1)^{(p-1)(q-1)/4}$. ■

An equivalent statement of the Quadratic Reciprocity Law: if p and q are distinct odd primes, then $(p/q) = (q/p)$ unless $p \equiv q \equiv 3 \pmod 4$, in which case $(p/q) = -(q/p)$.

For readers who are interested in learning more about Gauss sums we recommend [7], which has a good chapter on the subject. A more comprehensive treatment may be found in [1].

Exercise.

56. (Formulas for Gaussian sums) Suppose that n is an odd positive integer greater than 1 whose prime decomposition is given by the equation

$$n = \prod_{j=1}^{k} p_j^{\nu_j},$$

where each integral exponent ν_j is positive. For an integer a, the *Jacobi symbol* (a/n) is defined by the equation

$$(a/n) = \prod_{j=1}^{k} (a/p_j)^{\nu_j},$$

where (a/p_j) is the Legendre symbol. Thus, the possible values of (a/n) are -1, 0, 1, with $(a/n) = 0$ if and only if a and n have a common factor greater than one. Prove that if a and n are relatively prime, then

$$G_n(a) = \begin{cases} (a/n) & \text{if } n \equiv 1 \pmod 4, \\ -i(a/n) & \text{if } n \equiv 3 \pmod 4. \end{cases}$$

References

1. Berndt, C. Bruce, Evans, Ronald J., and Williams, Kenneth S., *Gauss and Jacobi Sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, Vol. 21, Wiley-Interscience, 1998.
2. Dudley, Underwood, *Elementary Number Theory*, 2nd edition, W.H. Freeman and Company, 1978.
3. Halmos, P. R., *Finite-Dimensional Vector Spaces*, UTM, Springer-Verlag, 1987.
4. Halmos, P. R., *Introduction to Hilbert Space*, 2nd edition, Chelsea Publishing Company, 1957.
5. Hardy, G. H. and Wright, E. M., *An Introduction to the Theory of Numbers*, 4th edition, Clarendon Press, 1960.
6. Herstein, I.N., *Topics in Algebra*, 2nd edition, Wiley & Sons, Inc., 1975.
7. Ireland, K. and Rosen, M., *A Classical Introduction to Modern Number Theory*, 2nd edition, GTM, Vol. 24, Springer-Verlag, 1990.
8. Isaacs, Martin I., *Character Theory of Finite Groups*, Academic Press 1976, (reprinted by AMS, Chelsea, 2006).
9. Jones, G. A. and Jones, M. J., *Elementary Number Theory*, UTM, Springer-Verlag, 1998 (reprinted 2002).
10. Karlin, Samuel and Studden, William J., *Tchebycheff Systems*: *With Applications in Analysis and Statistics*, Wiley & Sons, Inc., 1966.
11. Keng, H. L., *Introduction to Number Theory*, Springer-Verlag, 1982.
12. Koch, Helmut, *Number Theory*, Graduate Studies in Mathematics, Vol. 24, AMS, 2000.
13. McClellan, H. James and Parks, W. Thomas, *Eigenvalue and Eigenvector Decomposition of the Discrete Fourier Transform*, IEEE Transactions on Audio and Electroacoustics, Vol. Au-20, No. 1, pp 66-74, 1972.
14. McCoy, N. H., *Introduction to Modern Algebra*, 3rd edition, Allyn and Bacon, 1975.
15. Mollin, Richard A., *An Introduction to Cryptography*, Chapman & Hall/CRC, 2001.
16. Munkres, J., *Topology*, 2nd edition, Prentice Hall, 2000.
17. Newman, M., *Integral Matrices*, Academic Press, Inc., 1972.
18. Nielsen, M. A. and Chuang, I. L., *Quantum Computation and Quantum Information*, Cambridge University Press, 2000 (reprinted 2003).
19. Rice, John, *The Approximation of Functions*, Vol. 1, Addison-Wesley, 1964.
20. Tolimieri, R., An, M., and Lu, Chao, *Algorithms for Discrete Fourier Transform and Convolution*, Springer-Verlag, 1989.

Index

Applied and Numerical Harmonic Analysis

J.M. Cooper: *Introduction to Partial Differential Equations with MATLAB*
(ISBN 978-0-8176-3967-9)

C.E. D'Attellis and E.M. Fernández-Berdaguer: *Wavelet Theory and Harmonic Analysis in Applied Sciences* (ISBN 978-0-8176-3953-2)

H.G. Feichtinger and T. Strohmer: *Gabor Analysis and Algorithms* (ISBN 978-0-8176-3959-4)

T.M. Peters, J.H.T. Bates, G.B. Pike, P. Munger, and J.C. Williams: *The Fourier Transform in Biomedical Engineering* (ISBN 978-0-8176-3941-9)

A.I. Saichev and W.A. Woyczyński: *Distributions in the Physical and Engineering Sciences*
(ISBN 978-0-8176-3924-2)

R. Tolimieri and M. An: *Time-Frequency Representations* (ISBN 978-0-8176-3918-1)

G.T. Herman: *Geometry of Digital Spaces* (ISBN 978-0-8176-3897-9)

A. Procházka, J. Uhlĩř, P.J.W. Rayner, and N.G. Kingsbury: *Signal Analysis and Prediction*
(ISBN 978-0-8176-4042-2)

J. Ramanathan: *Methods of Applied Fourier Analysis* (ISBN 978-0-8176-3963-1)

A. Teolis: *Computational Signal Processing with Wavelets* (ISBN 978-0-8176-3909-9)

W.O. Bray and Č.V. Stanojević: *Analysis of Divergence* (ISBN 978-0-8176-4058-3)

G.T Herman and A. Kuba: *Discrete Tomography* (ISBN 978-0-8176-4101-6)

J.J. Benedetto and P.J.S.G. Ferreira: *Modern Sampling Theory* (ISBN 978-0-8176-4023-1)

A. Abbate, C.M. DeCusatis, and P.K. Das: *Wavelets and Subbands*
(ISBN 978-0-8176-4136-8)

L. Debnath: *Wavelet Transforms and Time-Frequency Signal Analysis*
(ISBN 978-0-8176-4104-7)

K. Gröchenig: *Foundations of Time-Frequency Analysis* (ISBN 978-0-8176-4022-4)

D.F. Walnut: *An Introduction to Wavelet Analysis* (ISBN 978-0-8176-3962-4)

O. Bratteli and P. Jorgensen: *Wavelets through a Looking Glass* (ISBN 978-0-8176-4280-8)

H.G. Feichtinger and T. Strohmer: *Advances in Gabor Analysis* (ISBN 978-0-8176-4239-6)

O. Christensen: *An Introduction to Frames and Riesz Bases* (ISBN 978-0-8176-4295-2)

L. Debnath: *Wavelets and Signal Processing* (ISBN 978-0-8176-4235-8)

J. Davis: *Methods of Applied Mathematics with a MATLAB Overview*
(ISBN 978-0-8176-4331-7)

G. Bi and Y. Zeng: *Transforms and Fast Algorithms for Signal Analysis and Representations*
(ISBN 978-0-8176-4279-2)

J.J. Benedetto and A. Zayed: *Sampling, Wavelets, and Tomography*
(ISBN 978-0-8176-4304-1)

E. Prestini: *The Evolution of Applied Harmonic Analysis* (ISBN 978-0-8176-4125-2)

O. Christensen and K.L. Christensen: *Approximation Theory* (ISBN 978-0-8176-3600-5)

L. Brandolini, L. Colzani, A. Iosevich, and G. Travaglini: *Fourier Analysis and Convexity*
(ISBN 978-0-8176-3263-2)

W. Freeden and V. Michel: *Multiscale Potential Theory* (ISBN 978-0-8176-4105-4)

O. Calin and D.-C. Chang: *Geometric Mechanics on Riemannian Manifolds*
(ISBN 978-0-8176-4354-6)

Applied and Numerical Harmonic Analysis (Cont'd)

J.A. Hogan and J.D. Lakey: *Time-Frequency and Time-Scale Methods*
(ISBN 978-0-8176-4276-1)

C. Heil: *Harmonic Analysis and Applications* (ISBN 978-0-8176-3778-1)

K. Borre, D.M. Akos, N. Bertelsen, P. Rinder, and S.H. Jensen: *A Software-Defined GPS and Galileo Receiver* (ISBN 978-0-8176-4390-4)

T. Qian, V. Mang I, and Y. Xu: *Wavelet Analysis and Applications* (ISBN 978-3-7643-7777-9)

G.T. Herman and A. Kuba: *Advances in Discrete Tomography and Its Applications*
(ISBN 978-0-8176-3614-2)

M.C. Fu, R.A. Jarrow, J.-Y. J. Yen, and R.J. Elliott: *Advances in Mathematical Finance*
(ISBN 978-0-8176-4544-1)

O. Christensen: *Frames and Bases* (ISBN 978-0-8176-4677-6)

P.E.T. Jorgensen, K.D. Merrill, and J.A. Packer: *Representations, Wavelets, and Frames*
(ISBN 978-0-8176-4682-0)

M. An, A.K. Brodzik, and R. Tolimieri: *Ideal Sequence Design in Time-Frequency Space*
(ISBN 978-0-8176-4737-7)

S.G. Krantz: *Explorations in Harmonic Analysis* (ISBN 978-0-8176-4668-4)

G.S. Chirikjian: *Stochastic Models, Information Theory, and Lie Groups*, Volume I
(ISBN 978-0-8176-4802-2)

C. Cabrelli and J.L. Torrea: *Recent Developments in Real and Harmonic Analysis*
(ISBN 978-0-8176-4531-1)

B. Luong: *Fourier Analysis on Finite Abelian Groups* (ISBN 978-0-8176-4915-9)