7 Finite Fourier Analysis

> This past year has seen the birth, or rather the rebirth, of an exciting revolution in computing Fourier transforms. A class of algorithms known as the fast Fourier transform or FFT, is forcing a complete reassessment of many computational paths, not only in frequency analysis, but in any fields where problems can be reduced to Fourier transforms and/or convolutions...
>
> *C. Bingham and J. W. Tukey,* 1966

In the previous chapters we studied the Fourier series of functions on the circle and the Fourier transform of functions defined on the Euclidean space $\mathbb{R}^d$. The goal here is to introduce another version of Fourier analysis, now for functions defined on finite sets, and more precisely, on finite abelian groups. This theory is particularly elegant and simple since infinite sums and integrals are replaced by finite sums, and thus questions of convergence disappear.

In turning our attention to finite Fourier analysis, we begin with the simplest example, $\mathbb{Z}(N)$, where the underlying space is the (multiplicative) group of N^{th} roots of unity on the circle. This group can also be realized in additive form, as $\mathbb{Z}/N\mathbb{Z}$, the equivalence classes of integers modulo N. The group $\mathbb{Z}(N)$ arises as the natural approximation to the circle (as N tends to infinity) since in the first picture the points of $\mathbb{Z}(N)$ correspond to N points on the circle which are uniformly distributed. For this reason, in practical applications, the group $\mathbb{Z}(N)$ becomes a natural candidate for the storage of information of a function on the circle, and for the resulting numerical computations involving Fourier series. The situation is particularly nice when N is large and of the form $N = 2^n$. The computations of the Fourier coefficients now lead to the "fast Fourier transform," which exploits the fact that an induction in n requires only about $\log N$ steps to go from $N = 1$ to $N = 2^n$. This yields a substantial saving in time in practical applications.

In the second part of the chapter we undertake the more general theory of Fourier analysis on finite abelian groups. Here the fundamental example is the multiplicative group $\mathbb{Z}^*(q)$. The Fourier inversion formula

for $\mathbb{Z}^*(q)$ will be seen to be a key step in the proof of Dirichlet's theorem on primes in arithmetic progression, which we will take up in the next chapter.

1 Fourier analysis on $\mathbb{Z}(N)$

We turn to the group of N^{th} roots of unity. This group arises naturally as the simplest finite abelian group. It also gives a uniform partition of the circle, and is therefore a good choice if one wishes to sample appropriate functions on the circle. Moreover, this partition gets finer as N tends to infinity, and one might expect that the discrete Fourier theory that we discuss here tends to the continuous theory of Fourier series on the circle. In a broad sense, this is the case, although this aspect of the problem is not one that we develop.

1.1 The group $\mathbb{Z}(N)$

Let N be a positive integer. A complex number z is an N^{th} **root of unity** if $z^N = 1$. The set of N^{th} roots of unity is precisely

$$\left\{1, e^{2\pi i/N}, e^{2\pi i 2/N}, \ldots, e^{2\pi i(N-1)/N}\right\}.$$

Indeed, suppose that $z^N = 1$ with $z = re^{i\theta}$. Then we must have $r^N e^{iN\theta} = 1$, and taking absolute values yields $r = 1$. Therefore $e^{iN\theta} = 1$, and this means that $N\theta = 2\pi k$ where $k \in \mathbb{Z}$. So if $\zeta = e^{2\pi i/N}$ we find that ζ^k exhausts all the N^{th} roots of unity. However, notice that $\zeta^N = 1$ so if n and m differ by an integer multiple of N, then $\zeta^n = \zeta^m$. In fact, it is clear that

$$\zeta^n = \zeta^m \quad \text{if and only if} \quad n - m \text{ is divisible by } N.$$

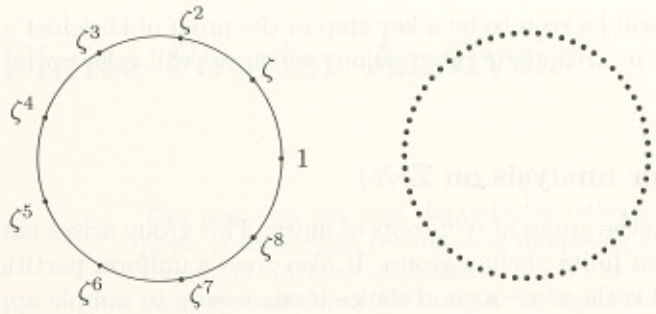
We denote the set of all N^{th} roots of unity by $\mathbb{Z}(N)$. The fact that this set gives a uniform partition of the circle is clear from its definition. Note that the set $\mathbb{Z}(N)$ satisfies the following properties:

(i) If $z, w \in \mathbb{Z}(N)$, then $zw \in \mathbb{Z}(N)$ and $zw = wz$.

(ii) $1 \in \mathbb{Z}(N)$.

(iii) If $z \in \mathbb{Z}(N)$, then $z^{-1} = 1/z \in \mathbb{Z}(N)$ and of course $zz^{-1} = 1$.

As a result we can conclude that $\mathbb{Z}(N)$ is an abelian group under complex multiplication. The appropriate definitions are set out in detail later in Section 2.1.



$Z(9),\ \zeta = e^{2\pi i/9}$ $\qquad$ $Z(N),\ N = 2^6$

Figure 1. The group of N^{th} roots of unity when $N = 9$ and $N = 2^6 = 64$

There is another way to visualize the group $\mathbb{Z}(N)$. This consists of choosing the integer power of ζ that determines each root of unity. We observed above that this integer is not unique since $\zeta^n = \zeta^m$ whenever n and m differ by an integer multiple of N. Naturally, we might select the integer which satisfies $0 \le n \le N-1$. Although this choice is perfectly reasonable in terms of "sets," we ask what happens when we multiply roots of unity. Clearly, we must add the corresponding integers since $\zeta^n\zeta^m = \zeta^{n+m}$ but nothing guarantees that $0 \le n+m \le N-1$. In fact, if $\zeta^n\zeta^m = \zeta^k$ with $0 \le k \le N-1$, then $n+m$ and k differ by an integer multiple of N. So, to find the integer in $[0, N-1]$ corresponding to the root of unity $\zeta^n\zeta^m$, we see that after adding the integers n and m we must reduce modulo N, that is, find the unique integer $0 \le k \le N-1$ so that $(n+m)-k$ is an integer multiple of N.

An equivalent approach is to associate to each root of unity ω the class of integers n so that $\zeta^n = \omega$. Doing so for each root of unity we obtain a partition of the integers in N disjoint infinite classes. To add two of these classes, choose any integer in each one of them, say n and m, respectively, and define the sum of the classes to be the class which contains the integer $n+m$.

We formalize the above notions. Two integers x and y are **congruent modulo** N if the difference $x-y$ is divisible by N, and we write $x \equiv y \mod N$. In other words, this means that x and y differ by an integer multiple of N. It is an easy exercise to check the following three properties:

- $x \equiv x \mod N$ for all integers x.
- If $x \equiv y \mod N$, then $y \equiv x \mod N$.
- If $x \equiv y \mod N$ and $y \equiv z \mod N$, then $x \equiv z \mod N$.

The above defines an equivalence relation on $\mathbb{Z}$. Let $R(x)$ denote the equivalence class, or residue class, of the integer x. Any integer of the form $x + kN$ with $k \in \mathbb{Z}$ is an element (or "representative") of $R(x)$. In fact, there are precisely N equivalence classes, and each class has a unique representative between 0 and $N-1$. We may now add equivalence classes by defining

$$R(x) + R(y) = R(x+y).$$

This definition is of course independent of the representatives x and y because if $x' \in R(x)$ and $y' \in R(y)$, then one checks easily that $x'+y' \in R(x+y)$. This turns the set of equivalence classes into an abelian group called the **group of integers modulo** N, which is sometimes denoted by $\mathbb{Z}/N\mathbb{Z}$. The association

$$R(k) \longleftrightarrow e^{2\pi ik/N}$$

gives a correspondence between the two abelian groups, $\mathbb{Z}/N\mathbb{Z}$ and $\mathbb{Z}(N)$. Since the operations are respected, in the sense that addition of integers modulo N becomes multiplication of complex numbers, we shall also denote the group of integers modulo N by $\mathbb{Z}(N)$. Observe that $0 \in \mathbb{Z}/N\mathbb{Z}$ corresponds to 1 on the unit circle.

Let V and W denote the vector spaces of complex-valued functions on the group of integers modulo N and the N^{th} roots of unity, respectively. Then, the identification given above carries over to V and W as follows:

$$F(k) \longleftrightarrow f(e^{2\pi ik/N}),$$

where F is a function on the integers modulo N and f is a function on the N^{th} roots of unity.

From now on, we write $\mathbb{Z}(N)$ but think of either the group of integers modulo N or the group of N^{th} roots of unity.

1.2 Fourier inversion theorem and Plancherel identity on $\mathbb{Z}(N)$

The first and most crucial step in developing Fourier analysis on $\mathbb{Z}(N)$ is to find the functions which correspond to the exponentials $e_n(x) = e^{2\pi inx}$ in the case of the circle. Some important properties of these exponentials are:

(i) $\{e_n\}_{n\in\mathbb{Z}}$ is an orthonormal set for the inner product (1) (in Chapter 3) on the space of Riemann integrable functions on the circle.

(ii) Finite linear combinations of the e_n's (the trigonometric polynomials) are dense in the space of continuous functions on the circle.

(iii) $e_n(x+y) = e_n(x)e_n(y)$.

On $\mathbb{Z}(N)$, the appropriate analogues are the N functions $e_0, \dots, e_{N-1}$ defined by

$$e_\ell(k) = \zeta^{\ell k} = e^{2\pi i \ell k/N} \quad \text{for } \ell = 0, \dots, N-1 \text{ and } k = 0, \dots, N-1,$$

where $\zeta = e^{2\pi i/N}$. To understand the parallel with (i) and (ii), we can think of the complex-valued functions on $\mathbb{Z}(N)$ as a vector space V, endowed with the Hermitian inner product

$$(F, G) = \sum_{k=0}^{N-1} F(k)\overline{G(k)}$$

and associated norm

$$\|F\|^2 = \sum_{k=0}^{N-1} |F(k)|^2.$$

Lemma 1.1 *The family $\{e_0, \dots, e_{N-1}\}$ is orthogonal. In fact,*

$$(e_m, e_\ell) = \begin{cases} N & \text{if } m = \ell, \\ 0 & \text{if } m \neq \ell. \end{cases}$$

Proof. We have

$$(e_m, e_\ell) = \sum_{k=0}^{N-1} \zeta^{mk}\zeta^{-\ell k} = \sum_{k=0}^{N-1} \zeta^{(m-\ell)k}.$$

If $m = \ell$, each term in the sum is equal to 1, and the sum equals N. If $m \neq \ell$, then $q = \zeta^{m-\ell}$ is not equal to 1, and the usual formula

$$1 + q + q^2 + \cdots + q^{N-1} = \frac{1 - q^N}{1 - q}$$

shows that $(e_m, e_\ell) = 0$, because $q^N = 1$.

Since the N functions $e_0, \dots, e_{N-1}$ are orthogonal, they must be linearly independent, and since the vector space V is N-dimensional, we

conclude that $\{e_0, \dots, e_{N-1}\}$ is an orthogonal basis for V. Clearly, property (iii) also holds, that is, $e_\ell(k+m) = e_\ell(k)e_\ell(m)$ for all ℓ, and all $k, m \in \mathbb{Z}(N)$.

By the lemma each vector e_ℓ has norm $\sqrt{N}$, so if we define

$$e_\ell^* = \frac{1}{\sqrt{N}} e_\ell,$$

then $\{e_0^*, \dots, e_{N-1}^*\}$ is an orthonormal basis for V. Hence for any $F \in V$ we have

$$F = \sum_{n=0}^{N-1} (F, e_n^*)e_n^* \quad \text{as well as} \quad \|F\|^2 = \sum_{n=0}^{N-1} |(F, e_n^*)|^2. \tag{1}$$

If we define the n^{th} **Fourier coefficient** of F by

$$a_n = \frac{1}{N} \sum_{k=0}^{N-1} F(k)e^{-2\pi i k n/N},$$

the above observations give the following fundamental theorem which is the $\mathbb{Z}(N)$ version of the Fourier inversion and the Parseval-Plancherel formulas.

Theorem 1.2 *If F is a function on $\mathbb{Z}(N)$, then*

$$F(k) = \sum_{n=0}^{N-1} a_n e^{2\pi i n k/N}.$$

Moreover,

$$\sum_{n=0}^{N-1} |a_n|^2 = \frac{1}{N} \sum_{k=0}^{N-1} |F(k)|^2.$$

The proof follows directly from (1) once we observe that

$$a_n = \frac{1}{N}(F, e_n) = \frac{1}{\sqrt{N}}(F, e_n^*).$$

Remark. It is possible to recover the Fourier inversion on the circle for sufficiently smooth functions (say C^2) by letting $N \to \infty$ in the finite model $\mathbb{Z}(N)$ (see Exercise 3).

1.3 The fast Fourier transform

The fast Fourier transform is a method that was developed as a means of calculating efficiently the Fourier coefficients of a function F on $\mathbb{Z}(N)$.

The problem, which arises naturally in numerical analysis, is to determine an algorithm that minimizes the amount of time it takes a computer to calculate the Fourier coefficients of a given function on $\mathbb{Z}(N)$. Since this amount of time is roughly proportional to the number of operations the computer must perform, our problem becomes that of minimizing the number of operations necessary to obtain all the Fourier coefficients $\{a_n\}$ given the values of F on $\mathbb{Z}(N)$. By operations we mean either an addition or a multiplication of complex numbers.

We begin with a naive approach to the problem. Fix N, and suppose that we are given $F(0), \dots, F(N-1)$ and $\omega_N = e^{-2\pi i/N}$. If we denote by $a_k^N(F)$ the k^{th} Fourier coefficient of F on $\mathbb{Z}(N)$, then by definition

$$a_k^N(F) = \frac{1}{N} \sum_{r=0}^{N-1} F(r)\omega_N^{kr},$$

and crude estimates show that the number of operations needed to calculate all Fourier coefficients is $\leq 2N^2 + N$. Indeed, it takes at most $N-2$ multiplications to determine $\omega_N^2, \dots, \omega_N^{N-1}$, and each coefficient a_k^N requires $N+1$ multiplications and $N-1$ additions.

We now present the **fast Fourier transform**, an algorithm that improves the bound $O(N^2)$ obtained above. Such an improvement is possible if, for example, we restrict ourselves to the case where the partition of the circle is dyadic, that is, $N = 2^n$. (See also Exercise 9.)

Theorem 1.3 *Given $\omega_N = e^{-2\pi i/N}$ with $N = 2^n$, it is possible to calculate the Fourier coefficients of a function on $\mathbb{Z}(N)$ with at most*

$$4 \cdot 2^n n = 4N \log_2(N) = O(N \log N)$$

operations.

The proof of the theorem consists of using the calculations for M division points, to obtain the Fourier coefficients for $2M$ division points. Since we choose $N = 2^n$, we obtain the desired formula as a consequence of a recurrence which involves $n = O(\log N)$ steps.

Let $\#(M)$ denote the minimum number of operations needed to calculate all the Fourier coefficients of any function on $\mathbb{Z}(M)$. The key to the proof of the theorem is contained in the following recursion step.

Lemma 1.4 *If we are given $\omega_{2M} = e^{-2\pi i/(2M)}$, then*

$$\#(2M) \leq 2\#(M) + 8M.$$

Proof. The calculation of $\omega_{2M}, \dots, \omega_{2M}^{2M}$ requires no more than $2M$ operations. Note that in particular we get $\omega_M = e^{-2\pi i/M} = \omega_{2M}^2$. The main idea is that for any given function F on $\mathbb{Z}(2M)$, we consider two functions F_0 and F_1 on $\mathbb{Z}(M)$ defined by

$$F_0(r) = F(2r) \quad \text{and} \quad F_1(r) = F(2r+1).$$

We assume that it is possible to calculate the Fourier coefficients of F_0 and F_1 in no more than $\#(M)$ operations each. If we denote the Fourier coefficients corresponding to the groups $\mathbb{Z}(2M)$ and $\mathbb{Z}(M)$ by a_k^{2M} and a_k^M, respectively, then we have

$$a_k^{2M}(F) = \frac{1}{2}\left(a_k^M(F_0) + a_k^M(F_1)\omega_{2M}^k\right).$$

To prove this, we sum over odd and even integers in the definition of the Fourier coefficient $a_k^{2M}(F)$, and find

$$\begin{aligned} a_k^{2M}(F) &= \frac{1}{2M} \sum_{r=0}^{2M-1} F(r)\omega_{2M}^{kr} \\ &= \frac{1}{2}\left(\frac{1}{M}\sum_{\ell=0}^{M-1} F(2\ell)\omega_{2M}^{k(2\ell)} + \frac{1}{M}\sum_{m=0}^{M-1} F(2m+1)\omega_{2M}^{k(2m+1)}\right) \\ &= \frac{1}{2}\left(\frac{1}{M}\sum_{\ell=0}^{M-1} F_0(\ell)\omega_M^{k\ell} + \frac{1}{M}\sum_{m=0}^{M-1} F_1(m)\omega_M^{km}\omega_{2M}^k\right), \end{aligned}$$

which establishes our assertion.

As a result, knowing $a_k^M(F_0)$, $a_k^M(F_1)$, and ω_{2M}^k, we see that each $a_k^{2M}(F)$ can be computed using no more than three operations (one addition and two multiplications). So

$$\#(2M) \leq 2M + 2\#(M) + 3 \times 2M = 2\#(M) + 8M,$$

and the proof of the lemma is complete.

An induction on n, where $N = 2^n$, will conclude the proof of the theorem. The initial step $n = 1$ is easy, since $N = 2$ and the two Fourier coefficients are

$$a_0^N(F) = \frac{1}{2}(F(1) + F(-1)) \quad \text{and} \quad a_1^N(F) = \frac{1}{2}(F(1) + (-1)F(-1)).$$

Calculating these Fourier coefficients requires no more than five operations, which is less than $4 \times 2 = 8$. Suppose the theorem is true up to $N = 2^{n-1}$ so that $\#(N) \leq 4 \cdot 2^{n-1}(n-1)$. By the lemma we must have

$$\#(2N) \leq 2 \cdot 4 \cdot 2^{n-1}(n-1) + 8 \cdot 2^{n-1} = 4 \cdot 2^n n,$$

which concludes the inductive step and the proof of the theorem.

2 Fourier analysis on finite abelian groups

The main goal in the rest of this chapter is to generalize the results about Fourier series expansions obtained in the special case of $\mathbb{Z}(N)$.

After a brief introduction to some notions related to finite abelian groups, we turn to the important concept of a character. In our setting, we find that characters play the same role as the exponentials $e_0, \ldots, e_{N-1}$ on the group $\mathbb{Z}(N)$, and thus provide the key ingredient in the development of the theory on arbitrary finite abelian groups. In fact, it suffices to prove that a finite abelian group has "enough" characters, and this leads automatically to the desired Fourier theory.

2.1 Abelian groups

An **abelian group** (or commutative group) is a set G together with a binary operation on pairs of elements of G, $(a, b) \mapsto a \cdot b$, that satisfies the following conditions:

(i) *Associativity*: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in G$.

(ii) *Identity*: There exists an element $u \in G$ (often written as either 1 or 0) such that $a \cdot u = u \cdot a = a$ for all $a \in G$.

(iii) *Inverses*: For every $a \in G$, there exists an element $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = u$.

(iv) *Commutativity*: For $a, b \in G$, we have $a \cdot b = b \cdot a$.

We leave as simple verifications the facts that the identity element and inverses are unique.

Warning. In the definition of an abelian group, we used the "multiplicative" notation for the operation in G. Sometimes, one uses the "additive" notation $a + b$ and $-a$, instead of $a \cdot b$ and a^{-1}. There are times when one notation may be more appropriate than the other, and the examples below illustrate this point. The same group may have different interpretations, one where the multiplicative notation is more suggestive, and another where it is natural to view the group with addition, as the operation.

Examples of abelian groups

- The set of real numbers $\mathbb{R}$ with the usual addition. The identity is 0 and the inverse of x is $-x$.

  Also, $\mathbb{R} - \{0\}$ and $\mathbb{R}^+ = \{x \in \mathbb{R} : x > 0\}$ equipped, with the standard multiplication, are abelian groups. In both cases the unit is 1 and the inverse of x is $1/x$.

- With the usual addition, the set of integers $\mathbb{Z}$ is an abelian group. However, $\mathbb{Z} - \{0\}$ is not an abelian group with the standard multiplication, since, for example, 2 does not have a multiplicative inverse in $\mathbb{Z}$. In contrast, $\mathbb{Q} - \{0\}$ is an abelian group with the standard multiplication.

- The unit circle S^1 in the complex plane. If we view the circle as the set of points $\{e^{i\theta} : \theta \in \mathbb{R}\}$, the group operation is the standard multiplication of complex numbers. However, if we identify points on S^1 with their angle θ, then S^1 becomes $\mathbb{R}$ modulo 2π, where the operation is addition modulo 2π.

- $\mathbb{Z}(N)$ is an abelian group. Viewed as the N^{th} roots of unity on the circle, $\mathbb{Z}(N)$ is a group under multiplication of complex numbers. However, if $\mathbb{Z}(N)$ is interpreted as $\mathbb{Z}/N\mathbb{Z}$, the integers modulo N, then it is an abelian group where the operation is addition modulo N.

- The last example consists of $\mathbb{Z}^*(q)$. This group is defined as the set of all integers modulo q that have *multiplicative* inverses, with the group operation being multiplication modulo q. This important example is discussed in more detail below.

A **homomorphism** between two abelian groups G and H is a map $f : G \to H$ which satisfies the property

$$f(a \cdot b) = f(a) \cdot f(b),$$

where the dot on the left-hand side is the operation in G, and the dot on the right-hand side the operation in H.

We say that two groups G and H are **isomorphic**, and write $G \approx H$, if there is a bijective homomorphism from G to H. Equivalently, G and H are isomorphic if there exists another homomorphism $\tilde{f} : H \to G$, so that for all $a \in G$ and $b \in H$

$$(\tilde{f} \circ f)(a) = a \quad \text{and} \quad (f \circ \tilde{f})(b) = b.$$

Roughly speaking, isomorphic groups describe the "same" object because they have the same underlying group structure (which is really all that matters); however, their particular notational representations might be different.

EXAMPLE 1. A pair of isomorphic abelian groups arose already when we considered the group $\mathbb{Z}(N)$. In one representation it was given as the multiplicative group of N^{th} roots of unity in $\mathbb{C}$. In a second representation it was the additive group $\mathbb{Z}/N\mathbb{Z}$ of residue classes of integers modulo N. The mapping $n \mapsto R(n)$, which associates to a root of unity $z = e^{2\pi in/N} = \zeta^n$ the residue class in $\mathbb{Z}/N\mathbb{Z}$ determined by n, provides an isomorphism between the two different representations.

EXAMPLE 2. In parallel with the previous example, we see that the circle (with multiplication) is isomorphic to the real numbers modulo 2π (with addition).

EXAMPLE 3. The properties of the exponential and logarithm guarantee that

$$\exp : \mathbb{R} \to \mathbb{R}^+ \quad \text{and} \quad \log : \mathbb{R}^+ \to \mathbb{R}$$

are two homomorphisms that are inverses of each other. Thus $\mathbb{R}$ (with addition) and $\mathbb{R}^+$ (with multiplication) are isomorphic.

In what follows, we are primarily interested in abelian groups that are finite. In this case, we denote by $|G|$ the number of elements in G, and call $|G|$ the **order** of the group. For example, the order of $\mathbb{Z}(N)$ is N.

A few additional remarks are in order:

- If G_1 and G_2 are two finite abelian groups, their **direct product** $G_1 \times G_2$ is the group whose elements are pairs (g_1, g_2) with $g_1 \in G_1$ and $g_2 \in G_2$. The operation in $G_1 \times G_2$ is then defined by

$$(g_1, g_2) \cdot (g_1', g_2') = (g_1 \cdot g_1', g_2 \cdot g_2').$$

  Clearly, if G_1 and G_2 are finite abelian groups, then so is $G_1 \times G_2$. The definition of direct product generalizes immediately to the case of finitely many factors $G_1 \times G_2 \times \cdots \times G_n$.

- The structure theorem for finite abelian groups states that such a group is isomorphic to a direct product of groups of the type $\mathbb{Z}(N)$; see Problem 2. This is a nice result which gives us an overview of the class of all finite abelian groups. However, since we shall not use this theorem below, we omit its proof.

We now discuss briefly the examples of abelian groups that play a central role in the proof of Dirichlet's theorem in the next chapter.

The group $\mathbb{Z}^*(q)$

Let q be a positive integer. We see that multiplication in $\mathbb{Z}(q)$ can be unambiguously defined, because if n is congruent to n' and m is congruent to m' (both modulo q), then nm is congruent to $n'm'$ modulo q. An integer $n \in \mathbb{Z}(q)$ is a **unit** if there exists an integer $m \in \mathbb{Z}(q)$ so that

$$nm \equiv 1 \mod q.$$

The set of all units in $\mathbb{Z}(q)$ is denoted by $\mathbb{Z}^*(q)$, and it is clear from our definition that $\mathbb{Z}^*(q)$ is an abelian group under *multiplication* modulo q. Thus within the additive group $\mathbb{Z}(q)$ lies a set $\mathbb{Z}^*(q)$ that is a group under multiplication. An alternative characterization of $\mathbb{Z}^*(q)$ will be given in the next chapter, as those elements in $\mathbb{Z}(q)$ that are relatively prime to q.

EXAMPLE 4. The group of units in $\mathbb{Z}(4) = \{0, 1, 2, 3\}$ is

$$\mathbb{Z}^*(4) = \{1, 3\}.$$

This reflects the fact that odd integers are divided into two classes depending on whether they are of the form $4k + 1$ or $4k + 3$. In fact, $\mathbb{Z}^*(4)$ is isomorphic to $\mathbb{Z}(2)$. Indeed, we can make the following association:

$\mathbb{Z}^*(4)$		$\mathbb{Z}(2)$
1	$\longleftrightarrow$	0
3	$\longleftrightarrow$	1

and then notice that multiplication in $\mathbb{Z}^*(4)$ corresponds to addition in $\mathbb{Z}(2)$.

EXAMPLE 5. The units in $\mathbb{Z}(5)$ are

$$\mathbb{Z}^*(5) = \{1, 2, 3, 4\}.$$

Moreover, $\mathbb{Z}^*(5)$ is isomorphic to $\mathbb{Z}(4)$ with the following identification:

$\mathbb{Z}^*(5)$		$\mathbb{Z}(4)$
1	$\longleftrightarrow$	0
2	$\longleftrightarrow$	1
3	$\longleftrightarrow$	3
4	$\longleftrightarrow$	2

EXAMPLE 6. The units in $\mathbb{Z}(8) = \{0,1,2,3,4,5,6,7\}$ are given by

$$\mathbb{Z}^*(8) = \{1,3,5,7\}.$$

In fact, $\mathbb{Z}^*(8)$ is isomorphic to the direct product $\mathbb{Z}(2) \times \mathbb{Z}(2)$. In this case, an isomorphism between the groups is given by the identification

$$\begin{array}{ccc} \mathbb{Z}^*(8) & & \mathbb{Z}(2) \times \mathbb{Z}(2) \\ 1 & \longleftrightarrow & (0,0) \\ 3 & \longleftrightarrow & (1,0) \\ 5 & \longleftrightarrow & (0,1) \\ 7 & \longleftrightarrow & (1,1) \end{array}$$

2.2 Characters

Let G be a finite abelian group (with the multiplicative notation) and S^1 the unit circle in the complex plane. A **character** on G is a complex-valued function $e : G \to S^1$ which satisfies the following condition:

$$e(a \cdot b) = e(a)e(b) \quad \text{for all } a, b \in G. \tag{2}$$

In other words, a character is a homomorphism from G to the circle group. The **trivial** or **unit character** is defined by $e(a) = 1$ for all $a \in G$.

Characters play an important role in the context of finite Fourier series, primarily because the multiplicative property (2) generalizes the analogous identity for the exponential functions on the circle and the law

$$e_\ell(k+m) = e_\ell(k)e_\ell(m),$$

which held for the exponentials $e_0, \ldots, e_{N-1}$ used in the Fourier theory on $\mathbb{Z}(N)$. There we had $e_\ell(k) = \zeta^{\ell k} = e^{2\pi i \ell k/N}$, with $0 \le \ell \le N-1$ and $k \in \mathbb{Z}(N)$, and in fact, the functions $e_0, \ldots, e_{N-1}$ are precisely all the characters of the group $\mathbb{Z}(N)$.

If G is a finite abelian group, we denote by $\hat{G}$ the set of all characters of G, and observe next that this set inherits the structure of an abelian group.

Lemma 2.1 *The set $\hat{G}$ is an abelian group under multiplication defined by*

$$(e_1 \cdot e_2)(a) = e_1(a)e_2(a) \quad \text{for all } a \in G.$$

The proof of this assertion is straightforward if one observes that the trivial character plays the role of the unit. We call $\hat{G}$ the **dual group** of G.

In light of the above analogy between characters for a general abelian group and the exponentials on $\mathbb{Z}(N)$, we gather several more examples of groups and their duals. This provides further evidence of the central role played by characters. (See Exercises 4, 5, and 6.)

EXAMPLE 1. If $G = \mathbb{Z}(N)$, all characters of G take the form $e_\ell(k) = \zeta^{\ell k} = e^{2\pi i \ell k/N}$ for some $0 \le \ell \le N-1$, and it is easy to check that $e_\ell \mapsto \ell$ gives an isomorphism from $\widehat{\mathbb{Z}(N)}$ to $\mathbb{Z}(N)$.

EXAMPLE 2. The dual group of the circle[1] is precisely $\{e_n\}_{n \in \mathbb{Z}}$ (where $e_n(x) = e^{2\pi i n x}$). Moreover, $e_n \mapsto n$ gives an isomorphism between $\widehat{S^1}$ and the integers $\mathbb{Z}$.

EXAMPLE 3. Characters on $\mathbb{R}$ are described by

$$e_\xi(x) = e^{2\pi i \xi x} \quad \text{where } \xi \in \mathbb{R}.$$

Thus $e_\xi \mapsto \xi$ is an isomorphism from $\hat{\mathbb{R}}$ to $\mathbb{R}$.

EXAMPLE 4. Since $\exp : \mathbb{R} \to \mathbb{R}^+$ is an isomorphism, we deduce from the previous example that the characters on $\mathbb{R}^+$ are given by

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

and $\widehat{\mathbb{R}^+}$ is isomorphic to $\mathbb{R}$ (or $\mathbb{R}^+$).

The following lemma says that a nowhere vanishing multiplicative function is a character, a result that will be useful later.

Lemma 2.2 *Let G be a finite abelian group, and $e : G \to \mathbb{C} - \{0\}$ a multiplicative function, namely $e(a \cdot b) = e(a)e(b)$ for all $a, b \in G$. Then e is a character.*

[1] In addition to (2), the definition of a character on an infinite abelian group requires continuity. When G is the circle, $\mathbb{R}$, or $\mathbb{R}^+$, the meaning of "continuous" refers to the standard notion of limit.

Proof. The group G being finite, the absolute value of $e(a)$ is bounded above and below as a ranges over G. Since $|e(b^n)| = |e(b)|^n$, we conclude that $|e(b)| = 1$ for all $b \in G$.

The next step is to verify that the characters form an orthonormal basis of the vector space V of functions over the group G. This fact was obtained directly in the special case $G = \mathbb{Z}(N)$ from the explicit description of the characters $e_0, \ldots, e_{N-1}$.

In the general case, we begin with the orthogonality relations; then we prove that there are "enough" characters by showing that there are as many as the order of the group.

2.3 The orthogonality relations

Let V denote the vector space of complex-valued functions defined on the finite abelian group G. Note that the dimension of V is $|G|$, the order of G. We define a Hermitian inner product on V by

$$(f, g) = \frac{1}{|G|} \sum_{a \in G} f(a)\overline{g(a)}, \qquad \text{whenever } f, g \in V. \tag{3}$$

Here the sum is taken over the group and is therefore finite.

Theorem 2.3 *The characters of G form an orthonormal family with respect to the inner product defined above.*

Since $|e(a)| = 1$ for any character, we find that

$$(e, e) = \frac{1}{|G|} \sum_{a \in G} e(a)\overline{e(a)} = \frac{1}{|G|} \sum_{a \in G} |e(a)|^2 = 1.$$

If $e \neq e'$ and both are characters, we must prove that $(e, e') = 0$; we isolate the key step in a lemma.

Lemma 2.4 *If e is a non-trivial character of the group G, then $\sum_{a \in G} e(a) = 0$.*

Proof. Choose $b \in G$ such that $e(b) \neq 1$. Then we have

$$e(b) \sum_{a \in G} e(a) = \sum_{a \in G} e(b)e(a) = \sum_{a \in G} e(ab) = \sum_{a \in G} e(a).$$

The last equality follows because as a ranges over the group, ab ranges over G as well. Therefore $\sum_{a \in G} e(a) = 0$.

We can now conclude the proof of the theorem. Suppose e' is a character distinct from e. Because $e(e')^{-1}$ is non-trivial, the lemma implies that

$$\sum_{a \in G} e(a)(e'(a))^{-1} = 0.$$

Since $(e'(a))^{-1} = \overline{e'(a)}$, the theorem is proved.

As a consequence of the theorem, we see that distinct characters are linearly independent. Since the dimension of V over $\mathbb{C}$ is $|G|$, we conclude that the order of $\hat{G}$ is finite and $\leq |G|$. The main result to which we now turn is that, in fact, $|\hat{G}| = |G|$.

2.4 Characters as a total family

The following completes the analogy between characters and the complex exponentials.

Theorem 2.5 *The characters of a finite abelian group G form a basis for the vector space of functions on G.*

There are several proofs of this theorem. One consists of using the structure theorem for finite abelian groups we have mentioned earlier, which states that any such group is the direct product of cyclic groups, that is, groups of the type $\mathbb{Z}(N)$. Since cyclic groups are self-dual, using this fact we would conclude that $|\hat{G}| = |G|$, and therefore the characters form a basis for G. (See Problem 3.)

Here we shall prove the theorem directly without these considerations.

Suppose V is a vector space of dimension d with inner product $(\cdot, \cdot)$. A linear transformation $T : V \to V$ is **unitary** if it preserves the inner product, $(Tv, Tw) = (v, w)$ for all $v, w \in V$. The spectral theorem from linear algebra asserts that any unitary transformation is diagonalizable. In other words, there exists a basis $\{v_1, \ldots, v_d\}$ (eigenvectors) of V such that $T(v_i) = \lambda_i v_i$, where $\lambda_i \in \mathbb{C}$ is the eigenvalue attached to v_i.

The proof of Theorem 2.5 is based on the following extension of the spectral theorem.

Lemma 2.6 *Suppose $\{T_1, \ldots, T_k\}$ is a commuting family of unitary transformations on the finite-dimensional inner product space V; that is,*

$$T_i T_j = T_j T_i \quad \text{for all } i, j.$$

Then $T_1, \ldots, T_k$ are simultaneously diagonalizable. In other words, there exists a basis for V which consists of eigenvectors for every T_i, $i = 1, \ldots, k$.

Proof. We use induction on k. The case $k = 1$ is simply the spectral theorem. Suppose that the lemma is true for any family of $k-1$ commuting unitary transformations. The spectral theorem applied to T_k says that V is the direct sum of its eigenspaces

$$V = V_{\lambda_1} \oplus \cdots \oplus V_{\lambda_s},$$

where V_{λ_i} denotes the subspace of all eigenvectors with eigenvalue λ_i. We claim that each one of the $T_1, \ldots, T_{k-1}$ maps each eigenspace V_{λ_i} to itself. Indeed, if $v \in V_{\lambda_i}$ and $1 \le j \le k-1$, then

$$T_k T_j(v) = T_j T_k(v) = T_j(\lambda_i v) = \lambda_i T_j(v)$$

so $T_j(v) \in V_{\lambda_i}$, and the claim is proved.

Since the restrictions to V_{λ_i} of $T_1, \ldots, T_{k-1}$ form a family of commuting unitary linear transformations, the induction hypothesis guarantees that these are simultaneously diagonalizable on each subspace V_{λ_i}. This diagonalization provides us with the desired basis for each V_{λ_i}, and thus for V.

We can now prove Theorem 2.5. Recall that the vector space V of complex-valued functions defined on G has dimension $|G|$. For each $a \in G$ we define a linear transformation $T_a : V \to V$ by

$$(T_a f)(x) = f(a \cdot x) \quad \text{for } x \in G.$$

Since G is abelian it is clear that $T_a T_b = T_b T_a$ for all $a, b \in G$, and one checks easily that T_a is unitary for the Hermitian inner product (3) defined on V. By Lemma 2.6 the family $\{T_a\}_{a \in G}$ is simultaneously diagonalizable. This means there is a basis $\{v_b(x)\}_{b \in G}$ for V such that each $v_b(x)$ is an eigenfunction for T_a, for every a. Let v be one of these basis elements and 1 the unit element in G. We must have $v(1) \neq 0$ for otherwise

$$v(a) = v(a \cdot 1) = (T_a v)(1) = \lambda_a v(1) = 0,$$

where λ_a is the eigenvalue of v for T_a. Hence $v = 0$, and this is a contradiction. We claim that the function defined by $w(x) = \lambda_x = v(x)/v(1)$ is a character of G. Arguing as above we find that $w(x) \neq 0$ for every x, and

$$w(a \cdot b) = \frac{v(a \cdot b)}{v(1)} = \frac{\lambda_a v(b)}{v(1)} = \lambda_a \lambda_b \frac{v(1)}{v(1)} = \lambda_a \lambda_b = w(a) w(b).$$

We now invoke Lemma 2.2 to conclude the proof.

2.5 Fourier inversion and Plancherel formula

We now put together the results obtained in the previous sections to discuss the Fourier expansion of a function on a finite abelian group G. Given a function f on G and character e of G, we define the **Fourier coefficient** of f with respect to e, by

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

and the **Fourier series** of f as

$$f \sim \sum_{e \in \hat{G}} \hat{f}(e) e.$$

Since the characters form a basis, we know that

$$f = \sum_{e \in \hat{G}} c_e e$$

for some set of constants c_e. By the orthogonality relations satisfied by the characters, we find that

$$(f, e) = c_e,$$

so f is indeed equal to its Fourier series, namely,

$$f = \sum_{e \in \hat{G}} \hat{f}(e) e.$$

We summarize our results.

Theorem 2.7 *Let G be a finite abelian group. The characters of G form an orthonormal basis for the vector space V of functions on G equipped with the inner product*

$$(f, g) = \frac{1}{|G|} \sum_{a \in G} f(a) \overline{g(a)}.$$

In particular, any function f on G is equal to its Fourier series

$$f = \sum_{e \in \hat{G}} \hat{f}(e) e.$$

Finally, we have the Parseval-Plancherel formula for finite abelian groups.

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

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

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

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

3 Exercises

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

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

We also let

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

denote the ordinary Fourier coefficients of f.

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

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

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

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

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

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

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

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

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

from its finite version.
[Hint: For the first part, use the second symmetric difference

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

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

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

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

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

Conversely, every function of this type is a character on $\mathbb{Z}(N)$. Deduce that $e_\ell \mapsto \ell$ defines an isomorphism from $\hat{G}$ to G.
[Hint: Show that $e(1)$ is an N^{th} root of unity.]

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

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

and check that $e_n \mapsto n$ defines an isomorphism from $\widehat{S^1}$ to $\mathbb{Z}$.
[Hint: If F is continuous and $F(x+y) = F(x)F(y)$, then F is differentiable. To see this, note that if $F(0) \neq 0$, then for appropriate δ, $c = \int_0^\delta F(y)\,dy \neq 0$, and $cF(x) = \int_x^{\delta+x} F(y)\,dy$. Differentiate to conclude that $F(x) = e^{Ax}$ for some A.]

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

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

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

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

(a) Show that M is unitary.