

CHARACTERS OF FINITE ABELIAN GROUPS

KEITH CONRAD

1. INTRODUCTION

The theme we will study is an analogue for finite abelian groups of Fourier analysis on \mathbf{R} . Fourier series on the real line are expansions in terms of sines and cosines:

$$f(x) = \sum_{n \geq 0} a_n \cos(nx) + \sum_{n \geq 1} b_n \sin(nx).$$

Since $e^{inx} = \cos(nx) + i \sin(nx)$ and $e^{-inx} = \cos(nx) - i \sin(nx)$, Fourier series can also be written in terms of complex exponentials:

$$f(x) = \sum_{n \in \mathbf{Z}} c_n e^{inx},$$

where the summation runs over all integers ($c_0 = a_0$, $c_n = \frac{1}{2}(a_n - b_n i)$ for $n > 0$, and $c_n = \frac{1}{2}(a_{|n|} + b_{|n|} i)$ for $n < 0$). The convenient algebraic property of e^{inx} , which is not shared by sines and cosines, is that it is a group homomorphism from \mathbf{R} to the unit circle $S^1 = \{z \in \mathbf{C} : |z| = 1\}$:

$$e^{in(x+x')} = e^{inx} e^{inx'}.$$

We now replace the real line \mathbf{R} with a finite abelian group. Here is the analogue of the functions e^{inx} .

Definition 1.1. A *character* of a finite abelian group G is a homomorphism $\chi : G \rightarrow S^1$.

We will usually write abstract groups multiplicatively, with identity 1.

Example 1.2. The *trivial* character of G is the homomorphism ε defined by $\varepsilon(g) = 1$ for all $g \in G$.

Example 1.3. Let G be cyclic of order 4 with generator γ . Since $\gamma^4 = 1$, a character χ of G has $\chi(\gamma)^4 = 1$, so χ takes only four possible values at γ , namely 1, -1 , i , or $-i$. Once $\chi(\gamma)$ is known, the value of χ elsewhere is determined by multiplicativity: $\chi(\gamma^j) = \chi(\gamma)^j$. So we get four characters, whose values can be placed in a table. See Table 1.

	1	γ	γ^2	γ^3
ε	1	1	1	1
χ_1	1	-1	1	-1
χ_2	1	i	-1	$-i$
χ_3	1	$-i$	-1	i

TABLE 1

When G has size n and $g \in G$, for any character χ of G we have $\chi(g)^n = \chi(g^n) = \chi(1) = 1$, so the values of χ lie among the n th roots of unity in S^1 . More precisely, the order of $\chi(g)$ divides the order of g (which divides $\#G$).

Characters on finite abelian groups were first studied in number theory, since number theory is a source of many interesting finite abelian groups. For instance, Dirichlet used characters on the group $(\mathbf{Z}/(m))^\times$ to prove that when $(a, m) = 1$ there are infinitely many primes $p \equiv a \pmod{m}$. The quadratic reciprocity law of elementary number theory is concerned with a deep property of a particular character, the Legendre symbol.

To provide a context against which our development of characters over finite abelian groups can be compared, Section 2 discusses classical Fourier analysis on the real line. In Section 3 we will run through some properties of characters of finite abelian groups and introduce their dual groups. Section 4 uses characters of a finite abelian group to develop a finite analogue of Fourier series. In Section 5 we use characters to prove a structure theorem for finite abelian groups. In Section 6 we look at (finite) Pontryagin duality. Characters are used in Section 7 to factor the group determinant of any finite abelian group.

Our notation is completely standard, but we make two remarks about it. For a complex-valued function $f(x)$, the complex-conjugate function is usually denoted $\overline{f}(x)$ instead of $\overline{f(x)}$ to stress that conjugation creates a new function. (We sometimes use the overline notation also to mean the reduction \overline{g} into a quotient group.) For $n \geq 1$, we write μ_n for the group of n th roots of unity in the unit circle S^1 . It is a cyclic group of size n .

Exercises.

1. Make a character table for $\mathbf{Z}/(2) \times \mathbf{Z}/(2)$.
2. Let G be a finite nonabelian simple group. (Examples include A_n for $n \geq 5$.) Show the only group homomorphism $\chi: G \rightarrow S^1$ is the trivial map.

2. CLASSICAL FOURIER ANALYSIS

This section on Fourier analysis on \mathbf{R} serves as motivation for our later treatment of finite abelian groups, where there will be no delicate convergence issues (just finite sums!), so we take a soft approach and sidestep the analytic technicalities that a serious treatment of Fourier analysis on \mathbf{R} would demand.

Fourier analysis for periodic functions on \mathbf{R} is based on the functions e^{inx} for $n \in \mathbf{Z}$. Any “reasonably nice” function $f: \mathbf{R} \rightarrow \mathbf{C}$ which has period 2π can be expanded into a Fourier series

$$f(x) = \sum_{n \in \mathbf{Z}} c_n e^{inx},$$

where the sum runs over \mathbf{Z} and the n th Fourier coefficient c_n can be recovered as an integral:

$$(2.1) \quad c_n = \frac{1}{2\pi} \int_0^{2\pi} f(x) e^{-inx} dx.$$

This formula for c_n can be explained by replacing $f(x)$ in (2.1) by its Fourier series and integrating termwise (for “reasonably nice” functions this termwise integration is analytically justifiable), using the formula

$$\frac{1}{2\pi} \int_0^{2\pi} e^{imx} e^{-inx} dx = \begin{cases} 1, & \text{if } m = n, \\ 0, & \text{if } m \neq n. \end{cases}$$

An important link between a function $f(x)$ and its Fourier coefficients c_n is given by Parseval's formula

$$\sum_{n \in \mathbf{Z}} |c_n|^2 = \frac{1}{2\pi} \int_0^{2\pi} |f(x)|^2 dx.$$

Rather than working with functions $f: \mathbf{R} \rightarrow \mathbf{C}$ having period 2π , formulas look cleaner using functions $f: \mathbf{R} \rightarrow \mathbf{C}$ having period 1. The basic exponentials become $e^{2\pi i n x}$ and the Fourier series and coefficients for f are

$$(2.2) \quad f(x) = \sum_{n \in \mathbf{Z}} c_n e^{2\pi i n x}, \quad c_n = \int_0^1 f(x) e^{-2\pi i n x} dx.$$

Parseval's formula becomes

$$(2.3) \quad \sum_{n \in \mathbf{Z}} |c_n|^2 = \int_0^1 |f(x)|^2 dx.$$

Note c_n in (2.2) is not the same as c_n in (2.1).

We turn now from Fourier series to Fourier integrals. Periodic functions $f: \mathbf{R} \rightarrow \mathbf{C}$ are replaced by functions which decay to 0 at $\pm\infty$. The *Fourier transform* of such an f is the function $\widehat{f}: \mathbf{R} \rightarrow \mathbf{C}$ defined by the integral formula

$$\widehat{f}(x) = \int_{\mathbf{R}} f(y) e^{-2\pi i x y} dy.$$

The analogue of the expansion (2.2) of a periodic function into a Fourier series is the Fourier inversion formula, which expresses f in terms of its Fourier transform:

$$f(x) = \int_{\mathbf{R}} \widehat{f}(y) e^{2\pi i x y} dy.$$

Define a (Hermitian) inner product of two functions f_1 and f_2 from \mathbf{R} to \mathbf{C} by the integral

$$\langle f_1, f_2 \rangle = \int_{\mathbf{R}} f_1(x) \overline{f_2(x)} dx \in \mathbf{C},$$

Plancherel's theorem compares the inner product of two functions and the inner product of their Fourier transforms:

$$(2.4) \quad \langle \widehat{f_1}, \widehat{f_2} \rangle = \langle f_1, f_2 \rangle.$$

In particular, when $f_1 = f_2 = f$ this becomes Parseval's formula

$$\int_{\mathbf{R}} |\widehat{f}(x)|^2 dx = \int_{\mathbf{R}} |f(x)|^2 dx,$$

which is an analogue of (2.3).

The *convolution* of two functions f_1 and f_2 from \mathbf{R} to \mathbf{C} is a new function from \mathbf{R} to \mathbf{C} defined by

$$(f_1 * f_2)(x) = \int_{\mathbf{R}} f_1(y) f_2(x - y) dy$$

and the Fourier transform turns this convolution into pointwise multiplication:

$$\widehat{f_1 * f_2}(x) = \widehat{f_1}(x) \widehat{f_2}(x).$$

There are several conventions for the Fourier transform, the inner product, and the convolution. These conventions differ on how 2π appears (if at all) in the defining formulas and in the properties (*e.g.*, Fourier inversion, Plancherel theorem, Fourier transform of a

convolution). Tables 2 and 3 collect a number of different 2π -conventions found in analysis books. The first two columns of Table 2 are definitions and the last two columns are theorems (Fourier inversion and Plancherel's theorem). Table 3 describes the effect of the Fourier transform on convolutions using different 2π -conventions.

$\widehat{f}(x)$	$\langle f_1, f_2 \rangle$	$f(x)$	$\langle \widehat{f_1}, \widehat{f_2} \rangle$
$\frac{1}{\sqrt{2\pi}} \int_{\mathbf{R}} f(y) e^{-ixy} dy$	$\int_{\mathbf{R}} f_1(x) \overline{f_2(x)} dx$	$\frac{1}{\sqrt{2\pi}} \int_{\mathbf{R}} \widehat{f}(y) e^{ixy} dy$	$\langle f_1, f_2 \rangle$
$\frac{1}{\sqrt{2\pi}} \int_{\mathbf{R}} f(y) e^{-ixy} dy$	$\frac{1}{\sqrt{2\pi}} \int_{\mathbf{R}} f_1(x) \overline{f_2(x)} dx$	$\frac{1}{\sqrt{2\pi}} \int_{\mathbf{R}} \widehat{f}(y) e^{ixy} dy$	$\langle f_1, f_2 \rangle$
$\int_{\mathbf{R}} f(y) e^{-2\pi ixy} dy$	$\int_{\mathbf{R}} f_1(x) \overline{f_2(x)} dx$	$\int_{\mathbf{R}} \widehat{f}(y) e^{2\pi ixy} dy$	$\langle f_1, f_2 \rangle$

TABLE 2

$\widehat{f}(x)$	$(f_1 * f_2)(x)$	$\widehat{f_1 * f_2}(x)$
$\frac{1}{\sqrt{2\pi}} \int_{\mathbf{R}} f(y) e^{-ixy} dy$	$\int_{\mathbf{R}} f_1(y) f_2(x - y) dy$	$\sqrt{2\pi} \widehat{f_1}(x) \widehat{f_2}(x)$
$\frac{1}{\sqrt{2\pi}} \int_{\mathbf{R}} f(y) e^{-ixy} dy$	$\frac{1}{\sqrt{2\pi}} \int_{\mathbf{R}} f_1(t) f_2(x - t) dt$	$\widehat{f_1}(x) \widehat{f_2}(x)$
$\int_{\mathbf{R}} f(y) e^{-2\pi ixy} dy$	$\int_{\mathbf{R}} f_1(y) f_2(x - y) dy$	$\widehat{f_1}(x) \widehat{f_2}(x)$

TABLE 3

Functions which equal their Fourier transform are called *self-dual*. For instance, using complex analysis one can show

$$(2.5) \quad \int_{\mathbf{R}} e^{-\pi(y+ix)^2} dy = 1$$

for all $x \in \mathbf{R}$. Expanding the square in the exponent, this becomes

$$\int_{\mathbf{R}} e^{-\pi y^2} e^{-2\pi ixy} dy = e^{-\pi x^2},$$

which says $e^{-\pi x^2}$ is self-dual when the Fourier transform is set to $\widehat{f}(x) = \int_{\mathbf{R}} f(y) e^{-2\pi ixy} dy$. When the Fourier transform is defined using $\widehat{f}(x) = \frac{1}{\sqrt{2\pi}} \int_{\mathbf{R}} f(y) e^{-ixy} dy$, the function $e^{-(1/2)x^2}$ is self-dual.

More generally, a change of variables in (2.5) shows the Fourier transform of a Gaussian exponential e^{-cx^2} is the scalar multiple of another Gaussian exponential:

$$(2.6) \quad \int_{\mathbf{R}} e^{-cy^2} e^{-2\pi ixy} dy = \sqrt{\frac{\pi}{c}} e^{-\pi^2 x^2 / c}.$$

This formula shows that a highly peaked Gaussian (large c) has a Fourier transform which is a spread out Gaussian (small π^2/c) and *vice versa*. More generally, there is a sense in which a function and its Fourier transform can't both be highly localized; this is a mathematical incarnation of Heisenberg's uncertainty principle from physics.

A link between Fourier series and Fourier integrals is the *Poisson summation formula*: for a “nice” function $f: \mathbf{R} \rightarrow \mathbf{C}$ that decays rapidly enough at $\pm\infty$,

$$(2.7) \quad \sum_{n \in \mathbf{Z}} f(n) = \sum_{n \in \mathbf{Z}} \widehat{f}(n),$$

where $\widehat{f}(x) = \int_{\mathbf{R}} f(y) e^{-2\pi i xy} dy$. To (nonrigorously) prove the Poisson summation formula, we will use Fourier series. Periodize $f(x)$ as

$$F(x) = \sum_{n \in \mathbf{Z}} f(x + n).$$

Since $F(x + 1) = F(x)$, write F as a Fourier series: $F(x) = \sum_{n \in \mathbf{Z}} c_n e^{2\pi i nx}$. The formula for c_n is

$$\begin{aligned} c_n &= \int_0^1 F(x) e^{-2\pi i nx} dx \\ &= \int_0^1 \left(\sum_{m \in \mathbf{Z}} f(x + m) \right) e^{-2\pi i nx} dx \\ &= \sum_{m \in \mathbf{Z}} \int_0^1 f(x + m) e^{-2\pi i nx} dx \\ &= \sum_{m \in \mathbf{Z}} \int_m^{m+1} f(x) e^{-2\pi i nx} dx \\ &= \int_{\mathbf{R}} f(x) e^{-2\pi i nx} dx \\ &= \widehat{f}(n). \end{aligned}$$

Therefore the expansion of $F(x)$ into a Fourier series is equivalent to

$$(2.8) \quad \sum_{n \in \mathbf{Z}} f(x + n) = \sum_{n \in \mathbf{Z}} \widehat{f}(n) e^{2\pi i nx},$$

which becomes the Poisson summation formula (2.7) by setting $x = 0$.

If we replace a sum over \mathbf{Z} with a sum over any one-dimensional lattice $L = a\mathbf{Z}$ in \mathbf{R} , where $a \neq 0$, the Poisson summation formula becomes

$$\sum_{\lambda \in L} f(\lambda) = \frac{1}{|a|} \sum_{\mu \in L^\perp} \widehat{f}(\mu),$$

where $L^\perp = (1/a)\mathbf{Z}$ is the “dual lattice”:

$$L^\perp = \{x : e^{2\pi i x \lambda} = 1 \text{ for all } \lambda \in L\}.$$

For example, $\mathbf{Z}^\perp = \mathbf{Z}$.

Exercises.

1. Without dwelling on analytic subtleties, check from Fourier inversion that $\widehat{\widehat{f}}(x) = f(-x)$ (if the Fourier transform is defined suitably).
2. If f is a real-valued even function, show its Fourier transform is also real-valued and even (assuming the Fourier transform of f is meaningful).
3. For a function $f: \mathbf{R} \rightarrow \mathbf{C}$ and $c \in \mathbf{R}$, let $g(x) = f(x + c)$. Define the Fourier transform of a function h by $\widehat{h}(x) = \int_{\mathbf{R}} h(y) e^{-2\pi i xy} dy$. If f has a Fourier transform, show g has Fourier transform $\widehat{g}(x) = e^{2\pi i cx} \widehat{f}(x)$.

4. The Poisson summation formula over \mathbf{R} was obtained by setting $x = 0$ in (2.8). Conversely, show that (2.8) for the function f follows from the Poisson summation formula for the function $g(t) = f(t + x)$.
5. Assuming the Fourier inversion formula holds for a definition of the Fourier transform as in Table 2, check that for all α and β in \mathbf{R}^\times that if we set

$$(\mathcal{F}f)(x) = \alpha \int_{\mathbf{R}} f(y) e^{-i\beta xy} dy$$

for all x then

$$f(x) = \frac{\beta}{2\pi\alpha} \int_{\mathbf{R}} (\mathcal{F}f)(y) e^{i\beta xy} dy.$$

(If $\beta = 2\pi\alpha^2$ then these two equations are symmetric in the roles of f and $\mathcal{F}f$ except for a sign in the exponential term.) Considering $\mathcal{F}f$ to be the Fourier transform of f , show $e^{-(1/2)\beta x^2}$ is self-dual in this sense.

3. FINITE CHARACTERS

We leave the real line and turn to the setting of finite abelian groups G . Our interest shifts from the functions e^{inx} to characters: homomorphisms from G to S^1 . The construction of characters on these groups begins with the case of cyclic groups.

Theorem 3.1. *Let G be a finite cyclic group of size n with a chosen generator γ . There are exactly n characters of G , each determined by sending γ to the different n th roots of unity in \mathbf{C} .*

Proof. We mimic Example 1.3, where G is cyclic of size 4. Since γ generates G , a character is determined by its value on γ and that value must be an n th root of unity (not necessarily of exact order n , e.g., $\varepsilon(\gamma) = 1$), so there are at most n characters. We now write down n characters.

Let ζ be any n th root of unity in \mathbf{C} . Set $\chi(\gamma^j) = \zeta^j$ for $j \in \mathbf{Z}$. This formula is well-defined (if $\gamma^j = \gamma^k$ for two different integer exponents j and k , we have $j \equiv k \pmod{n}$ so $\zeta^j = \zeta^k$), and χ is a homomorphism. Of course χ depends on ζ . As ζ changes, we get different characters (their values at γ are changing), so in total we have n characters. \square

To handle characters on non-cyclic groups, the following lemma is critical.

Lemma 3.2. *Let G be a finite abelian group and $H \subset G$ be a subgroup. Any character of H can be extended to a character of G in $[G : H]$ ways.*

Proof. We will induct on the index $[G : H]$ and we may suppose $H \neq G$. Pick $a \in G$ with $a \notin H$, so

$$H \subset \langle H, a \rangle \subset G.$$

Let $\chi : H \rightarrow S^1$ be a character of H . We will extend χ to a character $\tilde{\chi}$ of $\langle H, a \rangle$ and count the number of possible $\tilde{\chi}$. Then we will use induction to lift characters further from $\langle H, a \rangle$ all the way up to G .

What is a viable choice for $\tilde{\chi}(a)$? Since $a \notin H$, $\tilde{\chi}(a)$ is not initially defined. But some power a^k is in H for $k \geq 1$ (e.g., $k = [G : H]$), and therefore $\tilde{\chi}(a^k)$ is defined: $\tilde{\chi}(a^k) = \chi(a^k)$. Pick $k \geq 1$ minimal with $a^k \in H$. That is, k is the order of a in G/H , so $k = [\langle H, a \rangle : H]$. If $\tilde{\chi}$ is going to be a character then $\tilde{\chi}(a)$ must be an k -th root of $\chi(a^k)$. That is our clue: define $\tilde{\chi}(a) \in S^1$ to be a solution to $z^k = \chi(a^k)$:

$$(3.1) \quad \tilde{\chi}(a)^k = \chi(a^k).$$

Every number in S^1 has k different k -th roots in S^1 , so there are k potential choices for $\tilde{\chi}(a)$. We will show they all work.

Once we have chosen $\tilde{\chi}(a)$ to satisfy (3.1), define $\tilde{\chi}$ on $\langle H, a \rangle$ by

$$\tilde{\chi}(ha^i) := \chi(h)\tilde{\chi}(a)^i.$$

This formula does cover all possible elements of $\langle H, a \rangle$, but is $\tilde{\chi}$ well-defined? Perhaps H and $\langle a \rangle$ overlap nontrivially, so the expression of an element of $\langle H, a \rangle$ in the form ha^i is not unique. We have to show this doesn't lead to an inconsistency in the value of $\tilde{\chi}$. Suppose $ha^i = h'a^{i'}$. Then $a^{i-i'} \in H$, so $i' \equiv i \pmod k$ since k is denoting the order of a in G/H . Write $i' = i + kq$, so $h = h'a^{i'-i} = h'a^{kq}$. The terms h, h' , and a^k are in H , so

$$\begin{aligned} \chi(h')\tilde{\chi}(a)^{i'} &= \chi(h')\tilde{\chi}(a)^i\tilde{\chi}(a)^{kq} \\ &= \chi(h')\tilde{\chi}(a)^i\chi(a^k)^q \text{ since } \tilde{\chi}(a)^k = \chi(a^k) \\ &= \chi(h'a^{kq})\tilde{\chi}(a)^i \\ &= \chi(h)\tilde{\chi}(a)^i. \end{aligned}$$

Therefore $\tilde{\chi}: \langle H, a \rangle \rightarrow S^1$ is a well-defined function and it is easily checked to be a homomorphism. It restricts to χ on H . The number of choices of $\tilde{\chi}$ extending χ is the number of choices for $\tilde{\chi}(a)$, which is $k = [\langle H, a \rangle : H]$. Since $[G : \langle H, a \rangle] < [G : H]$, by induction on the index there are $[G : \langle H, a \rangle]$ extensions of each $\tilde{\chi}$ to a character of G , so the number of extensions of a character on H to a character on G is $[G : \langle H, a \rangle][\langle H, a \rangle : H] = [G : H]$. \square

Theorem 3.3. *If $g \neq 1$ in a finite abelian group G then $\chi(g) \neq 1$ for some character χ of G . The number of characters of G is $\#G$.*

Proof. The cyclic group $\langle g \rangle$ is nontrivial, say of size n , so $n > 1$. The group μ_n of n -th roots of unity in S^1 is also cyclic of order n , so there is an isomorphism $\langle g \rangle \cong \mu_n$. This isomorphism can be viewed as a character of the group $\langle g \rangle$. By Lemma 3.2 it extends to a character of G and does not send g to 1.

To show G has $\#G$ characters, apply Lemma 3.2 with H the trivial subgroup. \square

Corollary 3.4. *If G is a finite abelian group and $g_1 \neq g_2$ in G then there is a character of G which takes different values at g_1 and g_2 .*

Proof. Apply Theorem 3.3 to $g = g_1g_2^{-1}$. \square

Corollary 3.4 shows the characters of G “separate” the elements of G : different elements of the group admit a character taking different values on them.

Corollary 3.5. *If G is a finite abelian group and $H \subset G$ is a subgroup and $g \in G$ with $g \notin H$ then there is a character of G which is trivial on H and not equal to 1 at g .*

Proof. We work in the group G/H , where $\bar{g} \neq \bar{1}$. By Theorem 3.3 there is a character of G/H which is not 1 at \bar{g} . Composing this character with the reduction map $G \rightarrow G/H$ yields a character of G which is trivial on H and not equal to 1 at g . \square

It is easy to find functions on G which separate elements without using characters. For $g \in G$, define $\delta_g: G \rightarrow \{0, 1\}$ by

$$(3.2) \quad \delta_g(x) = \begin{cases} 1, & \text{if } x = g, \\ 0, & \text{if } x \neq g. \end{cases}$$

These functions separate elements of the group, but characters do this too and have better algebraic properties: they are group homomorphisms.

Remark 3.6. Nowhere in the proof of Lemma 3.2 did we use the finiteness of G . What mattered was finiteness of $[G : H]$. Infinite abelian groups like \mathbf{Z} or \mathbf{Z}^n can contain finite-index subgroups, so it's worth noting that we really proved that for any abelian group G , a character on a finite-index subgroup H extends in $[G : H]$ ways to a character on G . Lemma 3.2 for finite-index subgroups of infinite G has applications to Hecke characters in algebraic number theory.

Using Zorn's lemma (the axiom of choice), not only the finiteness of $\#G$ but also the finiteness of $[G : H]$ can be removed from Lemma 3.2: a character of any subgroup H of any abelian group G can be extended to a character of G (but the counting aspect with $[G : H]$ is no longer meaningful). In particular, Corollaries 3.4 and 3.5 are true for all abelian groups G .

Our definition of a character makes sense on nonabelian groups, but there will not be enough such characters for Theorem 3.3 to hold if G is finite and nonabelian: any homomorphism $\chi: G \rightarrow S^1$ must equal 1 on the commutator subgroup $[G, G]$, which is a nontrivial subgroup, so such homomorphisms can't distinguish elements in $[G, G]$ from each other. If $g \notin [G, G]$ then in the finite abelian group $G/[G, G]$ the coset of g is nontrivial so there is a character $G/[G, G] \rightarrow S^1$ that's nontrivial on \bar{g} . Composing this character with the reduction map $G \rightarrow G/[G, G]$ produces a homomorphism $G \rightarrow S^1$ which is nontrivial on g . Therefore $[G, G] = \bigcap_{\chi} \ker \chi$, where the intersection runs over all homomorphisms $\chi: G \rightarrow S^1$. This gives a “natural” explanation of why the commutator subgroup is normal in terms of kernels of homomorphisms: kernels are normal and the intersection of normal subgroups is normal. We put the word natural in quotes because appealing to the group $G/[G, G]$ in part of the argument means we had to use the normality of $[G, G]$ anyway. (Using Zorn's lemma as in Remark 3.6, the intersection formula for $[G, G]$ applies to all groups, not just finite groups.)

Definition 3.7. For a character χ on a finite abelian group G , the *conjugate character* is the function $\bar{\chi}: G \rightarrow S^1$ given by $\bar{\chi}(g) := \overline{\chi(g)}$.

Since any complex number z with $|z| = 1$ has $\bar{z} = 1/z$, $\bar{\chi}(g) = \chi(g)^{-1}$.

Definition 3.8. The *dual group* of a finite abelian group G is the set of homomorphisms $G \rightarrow S^1$ with the group law of pointwise multiplication of functions: $(\chi\psi)(g) = \chi(g)\psi(g)$. The dual group of G is denoted \hat{G} .

The trivial character of G is the identity in \hat{G} and the inverse of a character is its conjugate character. Note \hat{G} is abelian since multiplication in \mathbf{C}^\times is commutative.

Theorem 3.3 says in part that

$$(3.3) \quad \#G = \#\hat{G}.$$

In Theorem 5.7 we'll obtain a stronger result: the groups G and \hat{G} are *isomorphic*. For now we check this on cyclic groups.

Theorem 3.9. *If G is cyclic then $G \cong \hat{G}$ as groups.*

Proof. We will show \hat{G} is cyclic. Then since G and \hat{G} have the same size they are isomorphic.

Let $n = \#G$ and γ be a generator of G . Set $\chi: G \rightarrow S^1$ by $\chi(\gamma^j) = e^{2\pi i j/n}$ for all j . For any other character $\psi \in \widehat{G}$, we have $\psi(\gamma) = e^{2\pi i k/n}$ for some integer k , so $\psi(\gamma) = \chi(\gamma)^k$. Then

$$\psi(\gamma^j) = \psi(\gamma)^j = \chi(\gamma)^{jk} = \chi(\gamma^j)^k,$$

which shows $\psi = \chi^k$. Therefore χ generates \widehat{G} . \square

We will see later (Theorem 5.7) that Theorem 3.9 is true for all finite abelian G , not just cyclic G .

The following simple calculation will play a crucial role in the next section.

Theorem 3.10. *Let G be a finite abelian group and H be a subgroup. For $\chi \in \widehat{G}$,*

$$\sum_{h \in H} \chi(h) = \begin{cases} \#H, & \text{if } \chi \text{ is trivial on } H, \\ 0, & \text{otherwise.} \end{cases}$$

In particular,

$$\sum_{g \in G} \chi(g) = \begin{cases} \#G, & \text{if } \chi = \varepsilon, \\ 0, & \text{if } \chi \neq \varepsilon. \end{cases}$$

Proof. Let $S = \sum_{h \in H} \chi(h)$. If χ is trivial on H then $S = \#H$. If χ is not trivial on H , choose $h_0 \in H$ such that $\chi(h_0) \neq 1$. Then $\chi(h_0)S = \sum_{h \in H} \chi(hh_0) = \sum_{h \in H} \chi(h) = S$, so $S = 0$. \square

Taking $H = G$, Theorem 3.10 says the sum of a nontrivial character over a group vanishes. In terms of the character table of G this means the sum of the elements in each row of a character table is zero except for the top row (corresponding to the trivial character). Check this in Table 1.

Corollary 3.11. *Let G be a finite abelian group and K be a subgroup of \widehat{G} . For $g \in G$,*

$$\sum_{\chi \in K} \chi(g) = \begin{cases} \#K, & \text{if } \chi(g) = 1 \text{ for all } \chi \in K, \\ 0, & \text{otherwise.} \end{cases}$$

In particular,

$$\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} \#G, & \text{if } g = 1, \\ 0, & \text{if } g \neq 1. \end{cases}$$

Proof. The map “evaluate at g ” gives a function $K \rightarrow S^1$, where $\chi \mapsto \chi(g)$. Here g is fixed and χ varies. This is a character of K , since $(\chi_1 \chi_2)(g) = \chi_1(g) \chi_2(g)$ by definition, so $\sum_{\chi \in K} \chi(g)$ can be viewed as the sum of a character over the group K . By Theorem 3.10 this sum vanishes unless the character is trivial on the group, which means $\chi(g) = 1$ for all $\chi \in K$. \square

Corollary 3.11 with $K = \widehat{G}$ tells us that the sum of the elements in each column of the character table is zero except for the first column (corresponding to the identity element of G). Check this in Table 1.

Characters reverse the roles of m th roots of the identity in a finite abelian group and m th powers in its dual group, as in the next two theorems.

Theorem 3.12. *Let G be a finite abelian group and $m \in \mathbf{Z}$. For $g \in G$, $g^m = 1$ if and only if $\chi(g) = 1$ for every $\chi \in \widehat{G}$ which is an m th power in \widehat{G} .*

Proof. If $g^m = 1$ and $\chi = \psi^m$ for some $\psi \in \widehat{G}$ then

$$\chi(g) = \psi^m(g) = \psi(g)^m = \psi(g^m) = \psi(1) = 1.$$

Conversely, suppose $\chi(g) = 1$ whenever $\chi = \psi^m$ for some $\psi \in \widehat{G}$. Then for all $\psi \in \widehat{G}$ we have $1 = \psi^m(g) = \psi(g^m)$, so $g^m = 1$ by Theorem 3.3. \square

Theorem 3.13. *Let G be a finite abelian group and $m \in \mathbf{Z}$. For $g \in G$, g is an m th power in G if and only if $\chi(g) = 1$ for every $\chi \in \widehat{G}$ satisfying $\chi^m = \varepsilon$.*

Proof. If $g = x^m$ for some $x \in G$ then for every $\chi \in \widehat{G}$ such that $\chi^m = \varepsilon$ we have

$$\chi(g) = \chi(x)^m = \chi^m(x) = 1.$$

Conversely, assume $\chi(g) = 1$ for all χ such that $\chi^m = \varepsilon$. Then such χ are identically 1 on the subgroup G^m of m th powers in G , and conversely every character of G which is trivial on this subgroup has m th power ε . Therefore g is in G^m by Corollary 3.5. \square

We have used in this section two important features of S^1 as the target group for characters: for any $k \geq 1$ the k th power map on S^1 is k -to-1 (proof of Lemma 3.2) and for each $k \geq 1$ there is a cyclic subgroup of order k in S^1 (proof of Theorem 3.3).

Exercises.

1. Let's find the characters of the additive group $(\mathbf{Z}/(m))^r$, an r -fold direct product.
 - (a) For $k \in \mathbf{Z}/(m)$, let $\chi_k: \mathbf{Z}/(m) \rightarrow S^1$ by

$$\chi_k(j) = e^{2\pi i j k / m},$$

so $\chi_k(1) = e^{2\pi i k / m}$. Show $\chi_0, \chi_1, \dots, \chi_{m-1}$ are all the characters of $\mathbf{Z}/(m)$ and $\chi_k \chi_l = \chi_{k+l}$.

- (b) Let $r \geq 1$. For r -tuples \mathbf{a}, \mathbf{b} in $(\mathbf{Z}/(m))^r$, let

$$\mathbf{a} \cdot \mathbf{b} = a_1 b_1 + \dots + a_r b_r \in \mathbf{Z}/(m)$$

be the usual dot product. For $\mathbf{k} \in (\mathbf{Z}/(m))^r$, let $\chi_{\mathbf{k}}(\mathbf{j}) = e^{2\pi i (\mathbf{j} \cdot \mathbf{k}) / m}$. Show the functions $\chi_{\mathbf{k}}$ are all the characters of $(\mathbf{Z}/(m))^r$ and $\chi_{\mathbf{k}} \chi_{\mathbf{l}} = \chi_{\mathbf{k}+\mathbf{l}}$.

2. Show the following are equivalent properties of a character χ : $\chi(g) = \pm 1$ for all g , $\overline{\chi}(g) = \chi(g)$ for all g , and $\chi^2 = \varepsilon$.
3. Describe the error in the following bogus proof of Lemma 3.2. Let $m = [G : H]$ and pick a set of coset representatives g_1, \dots, g_m for G/H . Given a character χ on H , define $\tilde{\chi}$ on G by first picking the m ($= [G : H]$) values $\tilde{\chi}(g_i)$ for $1 \leq i \leq m$ and then writing any $g \in G$ in the (unique) form $g_i h$ and setting $\tilde{\chi}(g) = \tilde{\chi}(g_i) \chi(h)$. (Can you find a condition on how H sits in G under which this proof would be valid?)
4. Let G be a finite abelian group of order n and $g \in G$ have order m . Show

$$\prod_{\chi \in \widehat{G}} (1 - \chi(g)T) = (1 - T^m)^{n/m}.$$

5. For finite nonabelian G , show the characters of G (that is, homomorphisms $G \rightarrow S^1$) separate elements modulo $[G, G]$: if $\chi(g_1) = \chi(g_2)$ for all χ then $g_1 = g_2$ in $G/[G, G]$.

4. FINITE FOURIER SERIES

We will introduce the analogue of Fourier series on finite abelian groups. Engineering applications of these ideas include signal processing (the fast Fourier transform [2, Chap. 9]) and error-correcting codes [2, Chap. 11].

Let G be a finite abelian group. Set

$$L(G) = \{f: G \rightarrow \mathbf{C}\},$$

the \mathbf{C} -valued functions on G . This is a \mathbf{C} -vector space of functions. Every $f \in L(G)$ can be expressed as a linear combination of the delta-functions δ_g from (3.2):

$$(4.1) \quad f = \sum_{g \in G} f(g) \delta_g.$$

Indeed, evaluate both sides at each $x \in G$ and we get the same value. If the sum on the right side of (4.1) is zero, then $f(g) = 0$ for all g , so $f = 0$. Thus the functions δ_g are a basis of $L(G)$, so $\dim L(G) = \#G$.

The next theorem is the first step leading to an expression for each δ_g as a linear combination of characters of G .

Theorem 4.1. *Let G be a finite abelian group. Then*

$$\sum_{g \in G} \chi(g) = \begin{cases} \#G, & \text{if } \chi = \varepsilon, \\ 0, & \text{if } \chi \neq \varepsilon, \end{cases} \quad \sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} \#G, & \text{if } g = 1, \\ 0, & \text{if } g \neq 1. \end{cases}$$

Proof. This is a combination of Theorem 3.10 and Corollary 3.11. □

Corollary 4.2. *For characters χ_1 and χ_2 ,*

$$\sum_{g \in G} \chi_1(g) \overline{\chi_2}(g) = \begin{cases} \#G, & \text{if } \chi_1 = \chi_2, \\ 0, & \text{if } \chi_1 \neq \chi_2. \end{cases}$$

For $g_1, g_2 \in G$,

$$\sum_{\chi \in \widehat{G}} \chi(g_1) \overline{\chi}(g_2) = \begin{cases} \#G, & \text{if } g_1 = g_2, \\ 0, & \text{if } g_1 \neq g_2. \end{cases}$$

Proof. In the first equation of Theorem 4.1 let $\chi = \chi_1 \overline{\chi_2}$. In the second equation of Theorem 4.1 let $g = g_1 g_2^{-1}$. □

The equations in Corollary 4.2 say the character table of G has orthogonal rows and orthogonal columns when we measure orthogonality on row and column vectors over \mathbf{C} using the usual Hermitian inner product on vectors in \mathbf{C}^n .

Example 4.3. Let $G = (\mathbf{Z}/(m))^\times$. For $a \in (\mathbf{Z}/(m))^\times$ and p a prime not dividing m ,

$$\frac{1}{\varphi(m)} \sum_{\chi \bmod m} \overline{\chi}(a) \chi(p) = \begin{cases} 1, & \text{if } p \equiv a \bmod m, \\ 0, & \text{if } p \not\equiv a \bmod m, \end{cases}$$

where the sum runs over the characters of $(\mathbf{Z}/(m))^\times$. (Since p is prime, p not dividing m forces p to be in $(\mathbf{Z}/(m))^\times$.) This identity was used by Dirichlet in his proof that there are infinitely many primes $p \equiv a \bmod m$.

By the second equation in Corollary 4.2 we can express the delta-functions in terms of characters:

$$\delta_g(x) = \frac{1}{\#G} \sum_{\chi \in \widehat{G}} \bar{\chi}(g) \chi(x)$$

for every $x \in G$. Substituting this formula for δ_g into (4.1) gives

$$\begin{aligned} f(x) &= \sum_{g \in G} f(g) \left(\frac{1}{\#G} \sum_{\chi \in \widehat{G}} \bar{\chi}(g) \chi(x) \right) \\ &= \sum_{\chi \in \widehat{G}} \sum_{g \in G} \frac{1}{\#G} f(g) \bar{\chi}(g) \chi(x) \\ (4.2) \quad &= \sum_{\chi \in \widehat{G}} c_\chi \chi(x), \end{aligned}$$

where

$$(4.3) \quad c_\chi = \frac{1}{\#G} \sum_{g \in G} f(g) \bar{\chi}(g).$$

The expansion (4.2) is the Fourier series for f .

Equation (4.3) is similar to the formula for the coefficient c_n of e^{inx} in (2.1): an integral over $[0, 2\pi]$ divided by 2π is replaced by a sum over G divided by $\#G$ and $f(x)e^{-inx}$ is replaced by $f(g)\bar{\chi}(g)$. The number e^{-inx} is the conjugate of e^{inx} , which is also the relation between $\bar{\chi}(g)$ and $\chi(g)$. Equation (4.2) shows \widehat{G} is a spanning set for $L(G)$. Since $\#\widehat{G} = \#G = \dim L(G)$, \widehat{G} is a basis for $L(G)$.

Definition 4.4. Let G be a finite abelian group. If $f \in L(G)$ then its *Fourier transform* is the function $\widehat{f} \in L(\widehat{G})$ given by

$$\widehat{f}(\chi) = \sum_{g \in G} f(g) \bar{\chi}(g).$$

By (4.2) and (4.3),

$$(4.4) \quad f(x) = \frac{1}{\#G} \sum_{\chi \in \widehat{G}} \widehat{f}(\chi) \chi(x).$$

Equation (4.4) is called the *Fourier inversion formula* since it tells us how to recover f from its Fourier transform.

Remark 4.5. Classically the Fourier transform of a function $\mathbf{R} \rightarrow \mathbf{C}$ is another function $\mathbf{R} \rightarrow \mathbf{C}$. The finite Fourier transform, however, is defined on the dual group instead of on the original group. This is also happening classically, if one looks carefully. For $x \in \mathbf{R}$ let $\chi_x(y) = e^{ixy}$. Then $\chi_x: \mathbf{R} \rightarrow S^1$ is a character and $\widehat{f}(x)$ could be viewed as $\widehat{f}(\chi_x) = \int_{\mathbf{R}} f(y) \bar{\chi}_x(y) dy$, so \widehat{f} is a function of characters rather than of numbers.

Example 4.6. Let $f = \delta_g$. Then $\widehat{f}(\chi) = \bar{\chi}(g) = \chi(g^{-1})$. Notice f vanishes at all but one element of G while \widehat{f} is nonzero on all of \widehat{G} .

Example 4.7. Let $f = \psi$ be a character of G . Then $\widehat{f}(\chi) = \sum_g \psi(g) \bar{\chi}(g) = (\#G) \delta_\psi(\chi)$, so $\widehat{f} = (\#G) \delta_\psi$. Here f is nonzero on all of G and \widehat{f} is nonzero at only one element of \widehat{G} .

The Fourier transform on \mathbf{R} interchanges highly spread and highly peaked Gaussians. Examples 4.6 and 4.7 suggest a similar phenomenon in the finite case. Here is a general result in that direction (a finite version of Heisenberg uncertainty).

Theorem 4.8. *Let $f: G \rightarrow \mathbf{C}$ be a function on a finite abelian group G which is not identically zero. Then*

$$(4.5) \quad \#(\text{supp } f) \cdot \#(\text{supp } \hat{f}) \geq \#G,$$

where supp denotes the support of a function (the set of points where the function is nonzero).

Proof. We expand f into a Fourier series and make estimates. Since

$$f(x) = \sum_{\chi \in \hat{G}} \frac{1}{\#G} \hat{f}(\chi) \chi(x),$$

we have

$$(4.6) \quad |f(x)| \leq \sum_{\chi \in \hat{G}} \frac{1}{\#G} |\hat{f}(\chi)| \leq \frac{\#(\text{supp } \hat{f})}{\#G} \max_{\chi \in \hat{G}} |\hat{f}(\chi)|.$$

By the definition of $\hat{f}(\chi)$,

$$(4.7) \quad |\hat{f}(\chi)| \leq \sum_{g \in G} |f(g)|.$$

Let $m = \max_{g \in G} |f(g)|$, so $m > 0$ since f is not identically zero. Then (4.7) implies $|\hat{f}(\chi)| \leq m \#(\text{supp } f)$, and feeding this into (4.6) yields

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

Maximizing over all $x \in G$ implies $m \leq m \#(\text{supp } f) \#(\text{supp } \hat{f}) / \#G$. Divide both sides by m and the desired inequality drops out. \square

In Examples 4.6 and 4.7, inequality (4.5) is an equality, so Theorem 4.8 is sharp.

Since $L(G)$ is spanned by both the characters of G and the delta-functions, any linear identity in $L(G)$ can be verified by checking it on characters or on delta-functions. Let's look at an example.

Define a Hermitian inner product on $L(G)$ by the rule

$$(4.8) \quad \langle f_1, f_2 \rangle_G = \frac{1}{\#G} \sum_{x \in G} f_1(x) \overline{f_2(x)} \in \mathbf{C}.$$

We will prove Plancherel's theorem for G :

$$\langle f_1, f_2 \rangle_G = \frac{1}{\#G} \langle \hat{f}_1, \hat{f}_2 \rangle_{\hat{G}}$$

for all f_1 and f_2 in $L(G)$. (Compare to (2.4).) To check this identity, which is linear in both f_1 and f_2 , it suffices to check it when f_1 and f_2 are characters. By Corollary 4.2, for characters χ_1 and χ_2 of G we have

$$\langle \chi_1, \chi_2 \rangle_G = \begin{cases} 1, & \text{if } \chi_1 = \chi_2, \\ 0, & \text{if } \chi_1 \neq \chi_2. \end{cases}$$

Since $\widehat{\chi} = (\#G)\delta_\chi$ (Example 4.7),

$$\begin{aligned} \frac{1}{\#G} \langle \widehat{\chi_1}, \widehat{\chi_2} \rangle_{\widehat{G}} &= \#G \langle \delta_{\chi_1}, \delta_{\chi_2} \rangle_{\widehat{G}} \\ &= \sum_{\chi \in \widehat{G}} \delta_{\chi_1}(\chi) \overline{\delta_{\chi_2}(\chi)} \\ &= \begin{cases} 1, & \text{if } \chi_1 = \chi_2, \\ 0, & \text{if } \chi_1 \neq \chi_2. \end{cases} \end{aligned}$$

This verifies Plancherel's theorem for G . The special case where $f_1 = f_2 = f$ is a single function from G to \mathbf{C} gives us Parseval's formula for G :

$$(4.9) \quad \sum_{g \in G} |f(g)|^2 = \frac{1}{\#G} \sum_{\chi \in \widehat{G}} |\widehat{f}(\chi)|^2.$$

In Appendix B, we apply Parseval's formula for the group $G = \mathbf{Z}/(m)$ to prove a certain function of two variables is not a sum of products of functions of one variable.

Finite abelian analogues of Poisson summation and the relation between Fourier transforms and convolutions are in Exercises 4.6 and 4.10.

Let's look at some examples of Fourier transforms for functions on a cyclic group. By writing a cyclic group in the form $\mathbf{Z}/(m)$, we can make the isomorphism with the dual group explicit: every character of $\mathbf{Z}/(m)$ arises in the form $\chi_k: j \mapsto e^{2\pi i j k / m}$ for a unique $k \in \mathbf{Z}/(m)$ (Exercise 3.1). The character $\chi_1: j \mapsto e^{2\pi i j / m}$ is a generator of $\widehat{\mathbf{Z}/(m)}$. From this point of view the Fourier transform of a function $f: \mathbf{Z}/(m) \rightarrow \mathbf{C}$ is a second function $\widehat{f}: \mathbf{Z}/(m) \rightarrow \mathbf{C}$ also defined on $\mathbf{Z}/(m)$:

$$\widehat{f}(j) = \sum_{k \in \mathbf{Z}/(m)} f(k) e^{-2\pi i j k / m}.$$

Notice that j appears on the right side in the context of $e^{-2\pi i j k / m} = \overline{\chi_j(k)}$, showing the Fourier transform is still really a function of characters. But we can think of it as a function of integers modulo m since characters of $\mathbf{Z}/(m)$ are parametrized by $\mathbf{Z}/(m)$.

Example 4.9. Let $f: \mathbf{Z}/(8) \rightarrow \mathbf{C}$ be a function with period 2 having values 1 and 2. See Table 4. The Fourier transform of f vanishes except at 0 and 4, which are the multiples of the frequency of f (how often the period repeats).

n	0	1	2	3	4	5	6	7
$f(n)$	1	2	1	2	1	2	1	2
$\widehat{f}(n)$	12	0	0	0	-4	0	0	0

TABLE 4

Example 4.10. Now let $f: \mathbf{Z}/(8) \rightarrow \mathbf{C}$ have the periodic values 5, 3, 1, and 1. Both f and its Fourier transform are listed in Table 5. Now f has frequency 2 (its period repeats twice) and the Fourier transform vanishes except at 0, 2, 4, and 6, which are multiples of the frequency.

n	0	1	2	3	4	5	6	7
$f(n)$	5	3	1	1	5	3	1	1
$\widehat{f}(n)$	20	0	$8 + 4i$	0	4	0	$8 - 4i$	0

TABLE 5

Example 4.11. Consider a function $f: \mathbf{Z}/(45) \rightarrow \mathbf{C}$ with the four successive repeating values 1, 8, 19, 17. It is not a periodic function on $\mathbf{Z}/(45)$ since 4 does not divide 45, but the sequence 1, 8, 19, 17 repeats nearly 11 times. A calculation of the Fourier transform of f shows there are sharp peaks in $|\widehat{f}(n)|$ at $n = 0, 11, 22, 23$, and 34. (For example, $|\widehat{f}(11)|$ is between 3 and 4 times larger than the adjacent values $|\widehat{f}(10)|$ and $|\widehat{f}(12)|$.) The peaks in $|\widehat{f}(n)|$ occur approximately at multiples of the approximate frequency.

The Fourier transform of a periodic function on $\mathbf{Z}/(m)$ knows the frequency of the original function by the positions where the Fourier transform takes on its nonzero values, and for nearly periodic functions the approximate frequency is reflected in where the Fourier transform takes on its largest values. This is used in Shor's quantum algorithm for integer factorization [3, Chap. 17].

Exercises.

1. Let $f: \mathbf{Z}/(8) \rightarrow \mathbf{C}$ take the four values a, b, c , and d twice in this order. Compute $\widehat{f}(n)$ explicitly and determine some values for a, b, c , and d such that $\widehat{f}(n)$ is nonzero for $n = 0, 2$, and 6, but $\widehat{f}(4) = 0$.
2. For a subgroup H of a finite abelian group G , let

$$H^\perp = \{\chi \in \widehat{G} : \chi = 1 \text{ on } H\}.$$

These are the characters of G that are trivial on H . For example, $G^\perp = \{\varepsilon\}$ and $\{1\}^\perp = \widehat{G}$. Note $H^\perp \subset \widehat{G}$ and H^\perp depends on H and G .

Show H^\perp is a subgroup of \widehat{G} , it is isomorphic to $\widehat{G/H}$, and $\widehat{G}/(H^\perp) \cong \widehat{H}$. In particular, $\#H^\perp = [G : H]$.

3. For any subgroup H of a finite abelian group G , let δ_H be the function which is 1 on H and 0 off of H . Show the Fourier transform of δ_H is $\widehat{\delta_H} = (\#H)\delta_{H^\perp}$. How do the supports of δ_H and its Fourier transform compare with the inequality (4.5)?
4. Let H be a subgroup of a finite abelian group G .
 - (a) Suppose $f: G \rightarrow \mathbf{C}$ is constant on H -cosets (it is H -periodic). For $\chi \in \widehat{G}$ with $\chi \notin H^\perp$, show $\widehat{f}(\chi) = 0$. Thus the Fourier transform of an H -periodic function on G is supported on H^\perp .
 - (b) If $f: \mathbf{Z}/(m) \rightarrow \mathbf{C}$ has period d where $d|m$, show $\widehat{f}: \mathbf{Z}/(m) \rightarrow \mathbf{C}$ is supported on the multiples of m/d . (See Examples 4.9 and 4.10.)

5. Find the analogue of Exercise 2.3 for functions on a finite abelian group.
6. Let G be a finite abelian group and H be a subgroup. For any function $f: G \rightarrow \mathbf{C}$, Poisson summation on G says

$$\frac{1}{\#H} \sum_{h \in H} f(h) = \frac{1}{\#G} \sum_{\chi \in H^\perp} \widehat{f}(\chi),$$

where H^\perp is as in Exercise 4.2. Prove this formula in two ways:

a) Copy the classical proof sketched in Section 2 (start with the function $F(x) = \sum_{h \in H} f(xh)$, which is H -periodic so it defines a function on G/H) to obtain

$$(4.10) \quad \frac{1}{\#H} \sum_{h \in H} f(xh) = \frac{1}{\#G} \sum_{\chi \in H^\perp} \widehat{f}(\chi) \chi(x)$$

for any $x \in G$ and then set $x = 1$.

b) By linearity in f of both sides of the desired identity, verify Poisson summation directly on the delta-functions of G . (Corollary 3.5 and Example 4.6 will be useful.)

7. Let p be prime and χ be a *nontrivial* character of the multiplicative group $(\mathbf{Z}/(p))^\times$. Extend χ to a function on $\mathbf{Z}/(p)$ by setting $\chi(0) = 0$. This extended function is not a character of the additive group $\mathbf{Z}/(p)$, but the formula $\chi(xy) = \chi(x)\chi(y)$ holds even if one of x or y is 0. The Fourier transform $\widehat{\chi}: \mathbf{Z}/(p) \rightarrow \mathbf{C}$ is

$$\widehat{\chi}(x) = \sum_{y \in \mathbf{Z}/(p)} \chi(y) e^{-2\pi i xy/p} = \sum_{y \in (\mathbf{Z}/(p))^\times} \chi(y) e^{-2\pi i xy/p}.$$

(Don't confuse the Fourier transform for a function on $\mathbf{Z}/(p)$ with the Fourier transform for a function on $(\mathbf{Z}/(p))^\times$.)

(a) Show $\widehat{\chi}(x) = \chi(-1)G(\chi)\overline{\chi}(x)$, where $G(\chi) = \sum_y \chi(y)e^{2\pi i y/p}$. The sum $G(\chi)$ is called a *Gauss sum*.

(b) Show $\overline{G(\chi)} = \chi(-1)G(\overline{\chi})$.

(c) Although $G(\chi)$ is a sum of $p-1$ roots of unity, its magnitude is much smaller than the naive upper bound $p-1$: $|G(\chi)| = \sqrt{p}$. Show this by computing the Fourier expansion for χ as a function on $\mathbf{Z}/(p)$ to find $G(\chi)G(\overline{\chi}) = \chi(-1)p$ and then use (b).

(d) Derive the formula $|G(\chi)| = \sqrt{p}$ in a second way by computing both sides of Parseval's formula (4.9) for the function $\chi: \mathbf{Z}/(p) \rightarrow \mathbf{C}$ where $\chi(0) = 0$.

8. For a finite abelian group G and $g \in G$, let $T_g: L(G) \rightarrow L(G)$ by $(T_g f)(x) = f(gx)$.

(a) Show the T_g 's are commuting linear transformations.

(b) If f is a simultaneous eigenvector of all the T_g 's, show $f(1) \neq 0$ (if $f(1) = 0$ conclude f is identically zero, but the zero vector is not an eigenvector) and then after rescaling f so $f(1) = 1$ deduce that f is a character of G . Thus the simultaneous eigenvectors of the T_g 's, suitably normalized, are the characters of G .

(c) Show the T_g 's are simultaneously diagonalizable. Deduce from this and (b) that \widehat{G} is a basis of $L(G)$, so $\#\widehat{G} = \dim L(G) = \#G$. (This gives a different proof that G and \widehat{G} have the same size.)

9. Let $T_g: L(G) \rightarrow L(G)$ be as in the previous exercise.

(a) Show $\widehat{T_g f} = \chi(g)\widehat{f}$ for any $f \in L(G)$.

(b) Show for any f_1 and f_2 in $L(G)$ that $\langle T_g f_1, T_g f_2 \rangle_G = \langle f_1, f_2 \rangle_G$.

10. Let G be a finite abelian group. For f_1 and f_2 in $L(G)$, define their *convolution* $f_1 * f_2: G \rightarrow \mathbf{C}$ by

$$(f_1 * f_2)(x) = \sum_{y \in G} f_1(y) f_2(xy^{-1}).$$

(a) Show $\delta_g * \delta_h = \delta_{gh}$, so $L(G)$ under convolution is a commutative \mathbf{C} -algebra isomorphic to the group ring $\mathbf{C}[G]$.

(b) Show $\widehat{f_1 * f_2}(\chi) = \widehat{f_1}(\chi)\widehat{f_2}(\chi)$, so the Fourier transform turns convolution into pointwise multiplication.

(c) Show $\delta_g * f = T_{g^{-1}}(f)$ and $\chi * f = \widehat{f}(\chi)\chi$ in two ways: by a direct calculation or by computing the Fourier transform of both sides and using (b).

(d) For each $\chi \in \widehat{G}$, the function $h_\chi: L(G) \rightarrow \mathbf{C}$ given by $h_\chi(f) = \widehat{f}(\chi)$ is a \mathbf{C} -algebra homomorphism by (b). Does every \mathbf{C} -algebra homomorphism from $L(G)$ to \mathbf{C} arise in this way?

11. Formulate the Fourier inversion formula and Plancherel's theorem for functions on a finite abelian group G using the rescaled definitions

$$\widehat{f}(\chi) = \frac{1}{\sqrt{\#G}} \sum_{g \in G} f(g) \overline{\chi}(g), \quad \langle f_1, f_2 \rangle_G = \frac{1}{\sqrt{\#G}} \sum_{g \in G} f_1(g) \overline{f_2}(g).$$

Does this modified Fourier transform send convolution to multiplication if we use the definition

$$(f_1 * f_2)(g) = \frac{1}{\sqrt{\#G}} \sum_{h \in G} f_1(h) f_2(gh^{-1})?$$

5. STRUCTURE OF FINITE ABELIAN GROUPS

We will now put characters to work by using them to prove a structure theorem: every finite abelian group is a direct product of cyclic groups. We begin with a lemma having nothing to do with characters.

Lemma 5.1. *Let G be a finite abelian group. The order of any element in G divides the maximal order of the elements of G .*

Proof. We will show if G contains an element g_1 of order n_1 and an element g_2 of order n_2 then it contains some product $g_1^{a_1} g_2^{a_2}$ whose order is the least common multiple $[n_1, n_2]$. The reason this idea is helpful is the following. Let m be the maximal order among all the elements of G , and n be any order of the elements of G . We want to show $n|m$. If $[m, n]$ is the order of an element of G , then $[m, n] \leq m$ by maximality of m . Also $m|[m, n]$, so $[m, n] = m$. Therefore m is a multiple of n (a least common multiple is a multiple), which is what the lemma is claiming.

Returning to the construction of an element of order $[n_1, n_2]$, the basic idea is to write $[n_1, n_2]$ as a product $k_1 k_2$ of two relatively prime factors and then find exponents a_1 and a_2 such that $g_1^{a_1}$ and $g_2^{a_2}$ have orders equal to those factors k_1 and k_2 , and then their product $g_1^{a_1} g_2^{a_2}$ will have order equal to $k_1 k_2$ (the order of a product is the product of the orders for commuting elements with relatively prime order), which is $[n_1, n_2]$ by design.

Here are the details. Factor n_1 and n_2 into primes:

$$n_1 = p_1^{e_1} \cdots p_r^{e_r}, \quad n_2 = p_1^{f_1} \cdots p_r^{f_r}.$$

We use the same list of (distinct) primes in these factorizations, but use an exponent 0 on a prime that is not a factor of one of the integers. The least common multiple is

$$[n_1, n_2] = p_1^{\max(e_1, f_1)} \cdots p_r^{\max(e_r, f_r)}.$$

Break this into a product of two factors, one being a product of the prime powers where $e_i \geq f_i$ and the other using prime powers where $e_i < f_i$. Call these two numbers k_1 and k_2 :

$$k_1 = \prod_{e_i \geq f_i} p_i^{e_i}, \quad k_2 = \prod_{e_i < f_i} p_i^{f_i}.$$

Then $[n_1, n_2] = k_1 k_2$ and $(k_1, k_2) = 1$ (since k_1 and k_2 have no common prime factors). By construction, $k_1 | n_1$ and $k_2 | n_2$. Then $g_1^{n_1/k_1}$ has order k_1 and $g_2^{n_2/k_2}$ has order k_2 . Since these orders are relatively prime and the two powers of g_1 and g_2 commute with each other, $g_1^{n_1/k_1} g_2^{n_2/k_2}$ has order $k_1 k_2 = [n_1, n_2]$. \square

Example 5.2. Suppose g_1 has order $n_1 = 60 = 2^2 \cdot 3 \cdot 5$ and g_2 has order $n_2 = 630 = 2 \cdot 3^2 \cdot 5 \cdot 7$. Then $[n_1, n_2] = 2^2 \cdot 3^2 \cdot 5 \cdot 7$. We can write this as $(2^2 \cdot 5) \cdot (3^2 \cdot 7)$, where the first factor appears in n_1 , the second in n_2 , and the factors are relatively prime. Then g_1^3 has order $2^2 \cdot 5$ and g_2^{10} has order $3^2 \cdot 7$. These orders are relatively prime, so $g_1^3 g_2^{10}$ has order $2^2 \cdot 5 \cdot 3^2 \cdot 7 = [n_1, n_2]$.

Since the same power of 5 appears in both n_1 and n_2 , there is another factorization of $[n_1, n_2]$ we can use: placing the 5 in the second factor, we have $[n_1, n_2] = (2^2)(3^2 \cdot 5 \cdot 7)$. Then g_1^{15} has order 2^2 and g_2^2 has order $3^2 \cdot 5 \cdot 7$. These orders are relatively prime, so $g_1^{15} g_2^2$ has order $2^2 \cdot 3^2 \cdot 5 \cdot 7 = [n_1, n_2]$.

Lemma 5.1 is usually false for nonabelian groups, *e.g.*, the orders of the elements of S_3 are 1, 2, and 3, so the maximal order is not divisible by all other orders.

Since all orders of elements in a finite abelian group G divide the size of the group, every character of G has values in μ_N , where $N = \#G$. Lemma 5.1 leads to a sharper result:

Theorem 5.3. *Let G be a finite abelian group and let n be the maximum order of any element of G . Every character of G has values in μ_n .*

Proof. By Lemma 5.1, every $g \in G$ satisfies $g^n = 1$, so $\chi(g)^n = 1$ for any $\chi \in \widehat{G}$. \square

The following theorem shows that any cyclic subgroup of maximal size in a finite abelian group can always be split off as a direct factor. Characters get used in an essential way in the proof.

Theorem 5.4. *Let G be a finite abelian group and let $g \in G$ have maximal order in G . Then there is a subgroup $H \subset G$ such that $G \cong H \times \langle g \rangle$.*

Proof. Let n be the order of g . The subgroup $\langle g \rangle$ is cyclic of size n , so it is isomorphic to μ_n . Pick an isomorphism of $\langle g \rangle$ with μ_n . This isomorphism is an example of a character of $\langle g \rangle$. Extend this to a character of G (Lemma 3.2), so we get a character $\chi: G \rightarrow S^1$ such that $\chi(g)$ has order n . The image of χ is μ_n (Theorem 5.3) since $\chi(g)$ was chosen to generate μ_n .

Set $H = \ker \chi$. Then $H \cap \langle g \rangle = \{1\}$ since χ is one-to-one on $\langle g \rangle$ by construction. For any $x \in G$, $\chi(x)$ is in $\mu_n = \chi(\langle g \rangle)$ so $\chi(x) = \chi(g^k)$ for some k . Therefore $x = hg^k$, so $h \in H$. This proves $G \cong H \times \langle g \rangle$. \square

Theorem 5.5. *Every nontrivial finite abelian group G is isomorphic to a product of cyclic groups. More precisely, we can write*

$$G \cong \mathbf{Z}/(n_1) \times \mathbf{Z}/(n_2) \times \cdots \times \mathbf{Z}/(n_k),$$

where $n_1 | n_2 | \cdots | n_k$ and $n_1 > 1$.

Proof. Induct on $\#G$. The result is clear when $\#G$ is prime, *e.g.*, when $\#G = 2$. Let n be the maximal order of the elements of G , so $G \cong H \times \mathbf{Z}/(n)$ by Theorem 5.4. Since $\#H < \#G$, by induction

$$(5.1) \quad H \cong \mathbf{Z}/(n_1) \times \mathbf{Z}/(n_2) \times \cdots \times \mathbf{Z}/(n_r)$$

where $n_1|n_2|\cdots|n_r$. From (5.1) n_r is the order of an element of H (in fact it is the maximal order of an element of H), so $n_r|n$ by Lemma 5.1. Thus we can tack $\mathbf{Z}/(n)$ onto the end of (5.1) and we're done. \square

Theorem 5.5 not only expresses G as a direct product of cyclic groups, but does so with the extra feature that successive cyclic factors have size divisible by the previous cyclic factor. When written this way, the n_i 's are uniquely determined by G , but we will not prove this more precise result.

As an application of Theorem 5.5 we compare the group structure of G and \widehat{G} .

Lemma 5.6. *If A and B are finite abelian groups, there is an isomorphism $\widehat{A \times B} \cong \widehat{A} \times \widehat{B}$.*

Proof. Let χ be a character on $A \times B$. Identify the subgroups $A \times \{1\}$ and $\{1\} \times B$ of $A \times B$ with A and B in the obvious way. Let χ_A and χ_B be the restrictions of χ to A and B respectively, i.e., $\chi_A(a) = \chi(a, 1)$ and $\chi_B(b) = \chi(1, b)$. Then χ_A and χ_B are characters on A and B and $\chi(a, b) = \chi((a, 1)(1, b)) = \chi(a, 1)\chi(1, b) = \chi_A(a)\chi_B(b)$. So we get a map

$$(5.2) \quad \widehat{A \times B} \rightarrow \widehat{A} \times \widehat{B}$$

by sending χ to (χ_A, χ_B) . It is left to the reader to check (5.2) is a group homomorphism. Its kernel is trivial since if χ_A and χ_B are trivial characters then $\chi(a, b) = \chi_A(a)\chi_B(b) = 1$, so χ is trivial. Both sides of (5.2) have the same size by (3.3), so (5.2) is an isomorphism. \square

Theorem 5.7. *If G is a finite abelian group then G is isomorphic to \widehat{G} .*

Proof. The case when G is cyclic was Theorem 3.9. Lemma 5.6 extends easily to several factors in a direct product:

$$(H_1 \times \cdots \times H_r)^\wedge \cong \widehat{H}_1 \times \cdots \times \widehat{H}_r.$$

In particular, applying this to a cyclic decomposition of G from Theorem 5.5, each H_j is isomorphic to \widehat{H}_j so we obtain $G \cong \widehat{G}$. \square

Corollary 5.8. *If G is a finite abelian group and H is a subgroup then there is a subgroup of G which is isomorphic to G/H .*

Proof. Every character of G/H lifts in a natural way to a character of G which is trivial on H and this is an embedding $\widehat{G/H} \hookrightarrow \widehat{G}$. Since the dual group is isomorphic to the group, this embedding can be converted (non-canonically) into an embedding of G/H into G . \square

This corollary is not true for all finite groups, for instance $Q_8/\{\pm 1\} \cong \mathbf{Z}/(2) \times \mathbf{Z}/(2)$ but there is no subgroup of Q_8 which is isomorphic to this quotient group (there is only one element of order 2 in Q_8).

Exercises.

1. What is the structure (as a direct product of cyclic groups) of the finite abelian groups whose nontrivial characters all have order 2?
2. Mimic the proof of Theorem 5.4 to decompose $(\mathbf{Z}/(20))^\times$ (of size 8) and $(\mathbf{Z}/(45))^\times$ (of size 24) into a direct product of cyclic groups as in Theorem 5.5.
3. Show by an explicit counterexample that the following is false: if two subgroups H and K of a finite abelian group G are isomorphic then there is an automorphism of G which restricts to an isomorphism from H to K .

6. PONTRYAGIN DUALITY

While G and \widehat{G} are isomorphic groups, there is no “natural” isomorphism between them. For instance, when G is cyclic the isomorphism we wrote down between G and \widehat{G} in the proof of Theorem 3.9 depends on a choice of generator, and there is not a unique generator for G (if $\#G > 2$). Another indication that the isomorphism between G and \widehat{G} is not “natural” is that it breaks down for infinite G , *e.g.*, the characters of \mathbf{Z} (homomorphisms $\mathbf{Z} \rightarrow S^1$) are parametrized by points on the unit circle as functions χ_z , where $\chi_z(n) = z^n$, so $\widehat{\mathbf{Z}} \cong S^1$ if dual groups for infinite abelian groups are defined in the right way. In particular, $\widehat{\mathbf{Z}} \not\cong \mathbf{Z}$.

We can map any finite abelian group G to its double-dual group $\widehat{\widehat{G}}$ (the dual group of \widehat{G}) by sending each $g \in G$ to the function “evaluate at g ,” which associates to each $\chi \in \widehat{G}$ the number $\chi(g)$. Viewing evaluation at g as a character on \widehat{G} was met already in the proof of Corollary 3.11.

Theorem 6.1. *Let G be a finite abelian group. The homomorphism $G \rightarrow \widehat{\widehat{G}}$ associating to $g \in G$ the function “evaluate at g ” is an isomorphism.*

Proof. Since a finite abelian group and its dual group have the same size, a group and its double-dual group have the same size, so it suffices to show this homomorphism is injective. If $g \in G$ is in the kernel then every element of \widehat{G} is 1 at g , so $g = 1$ by Theorem 3.3. \square

Theorem 6.1 is called *Pontryagin duality*. This label actually applies to a more general result about characters on locally compact abelian groups. Finite abelian groups are a special case, where difficult analytic techniques can be replaced by counting arguments. The isomorphism between G and its double-dual group given by Pontryagin duality lets us think about any finite abelian group as a dual group (namely the dual group of \widehat{G}). For instance we can now say that the two parts of Corollary 4.2, as statements about all finite abelian groups G , are logically equivalent to each other since we can view G as a dual group by viewing its elements as the different characters of \widehat{G} .

The isomorphism in Pontryagin duality is natural, *i.e.*, it does not depend on any *ad hoc* choices along the way (unlike the isomorphism between a finite abelian group and its dual group).

As an application of Pontryagin duality, recall that in Theorem 3.12 we saw in any finite abelian group G that

$$g^m = 1 \iff \chi(g) = 1 \text{ for every } \chi \in \widehat{G} \text{ such that } \chi = \psi^m \text{ for some } \psi \in \widehat{G}.$$

By Pontryagin duality this implies (in fact, it is equivalent to) the result

$$\chi^m = \varepsilon \iff \chi(g) = 1 \text{ for every } g \in G \text{ such that } g = x^m \text{ for some } x \in G.$$

Similarly, the dual version of Theorem 3.13 says that a character χ of G is an m th power of another character if and only if χ is trivial on every $g \in G$ such that $g^m = 1$.

The set $\text{Hom}(G_1, G_2)$ of all homomorphisms from the abelian group G_1 to the abelian group G_2 forms an abelian group under pointwise multiplication (exercise). Pontryagin duality gives the following relation between two such Hom groups.

Theorem 6.2. *Let G_1 and G_2 be finite abelian groups. For any homomorphism $f: G_1 \rightarrow G_2$, set $f^*: \widehat{G}_2 \rightarrow \widehat{G}_1$ by $f^*(\chi) = \chi \circ f$. Then f^* is a group homomorphism and the map*

sending f to f^* gives a group isomorphism

$$\text{Hom}(G_1, G_2) \cong \text{Hom}(\widehat{G}_2, \widehat{G}_1).$$

Proof. If $f: G_1 \rightarrow G_2$ is a homomorphism and $\chi \in \widehat{G}_2$, then for g and g' in G_1 we have

$$\chi(f(gg')) = \chi(f(g)f(g')) = \chi(f(g))\chi(f(g')),$$

so $f^*(\chi) := \chi \circ f$ lies in \widehat{G}_1 . Thus we get the map from $\text{Hom}(G_1, G_2)$ to $\text{Hom}(\widehat{G}_2, \widehat{G}_1)$ as advertised. The reader can check $(ff')^* = f^*(f')^*$ in $\text{Hom}(\widehat{G}_2, \widehat{G}_1)$, so the map between Hom-groups is a homomorphism.

The same construction gives a group homomorphism $\text{Hom}(\widehat{G}_2, \widehat{G}_1) \rightarrow \text{Hom}(\widehat{\widehat{G}}_1, \widehat{\widehat{G}}_2)$. By Pontryagin duality this can be viewed as a homomorphism $\text{Hom}(\widehat{G}_2, \widehat{G}_1) \rightarrow \text{Hom}(G_1, G_2)$ and the composite map

$$\text{Hom}(G_1, G_2) \rightarrow \text{Hom}(\widehat{G}_2, \widehat{G}_1) \rightarrow \text{Hom}(G_1, G_2)$$

turns out (after unwinding definitions, which is left to the reader) to be the identity function. Therefore our original map $\text{Hom}(G_1, G_2) \rightarrow \text{Hom}(\widehat{G}_2, \widehat{G}_1)$ is a group isomorphism. \square

More applications of Pontryagin duality are in the exercises.

Exercises.

1. Let G be finite abelian and $H \subset G$ be a subgroup.
 - (a) Viewing $H^{\perp\perp} = (H^\perp)^\perp$ in G using Pontryagin duality, show $H^{\perp\perp} = H$. (Hint: The inclusion in one direction is easy. Count sizes for the other inclusion.)
 - (b) Show for each m dividing $\#G$ that

$$\#\{H \subset G : \#H = m\} = \#\{H \subset G : [G : H] = m\}$$

by associating H to H^\perp and using a (fixed) isomorphism of G with \widehat{G} .

(c) For a finite abelian group G , part b says the number of subgroups of G with index 2 is equal to the number of elements of G with order 2. Use this idea to count the number of subgroups of $(\mathbf{Z}/(m))^\times$ with index 2. (The answer depends on the number of odd prime factors of m and the highest power of 2 dividing m .)

(d) Show, for a prime p , that the number of subspaces of $(\mathbf{Z}/(p))^n$ with dimension d equals the number of subspaces with dimension $n - d$.

2. For a finite abelian group G , let $G[n] = \{g \in G : g^n = 1\}$ and $G^n = \{g^n : g \in G\}$. Both are subgroups of G . Prove $G[n]^\perp = \widehat{G}^n$ and $(G^n)^\perp = \widehat{G}[n]$.
3. Let $f \in L(G)$, so \widehat{f} is in $L(\widehat{G})$ and $\widehat{\widehat{f}}$ is in $L(\widehat{\widehat{G}})$.

(a) Viewing $\widehat{\widehat{G}}$ as G by Pontryagin duality, show $\widehat{\widehat{f}}(g) = (\#G)f(g^{-1})$.

(b) For any subgroup H in G , define the H -average of f and the H -cutoff of f to be the following functions on G :

$$\text{Avg}_H(f)(g) = \frac{1}{\#H} \sum_{h \in H} f(gh), \quad \text{Cut}_H(f)(g) = \begin{cases} f(g), & \text{if } g \in H, \\ 0, & \text{if } g \notin H. \end{cases}$$

Check the identity $\widehat{\widehat{\text{Avg}_H(f)}} = \widehat{\widehat{\text{Cut}_H(f)}}$ of functions on \widehat{G} and then take the Fourier transform of both sides to get an identity of functions on G , which will be (4.10) as x varies. (This shows that Poisson summation is essentially equivalent

to the fact that the Fourier transform exchanges the operators Avg_H on $L(G)$ and Cut_{H^\perp} on $L(\widehat{G})$, or equivalently Cut_H on $L(G)$ and Avg_{H^\perp} on $L(\widehat{G})$.)

4. For a homomorphism $f: G_1 \rightarrow G_2$, show $(\ker f)^\perp = \text{im } f^*$ in \widehat{G}_1 and $(\text{im } f)^\perp = \ker f^*$ in \widehat{G}_2 .
5. Show the isomorphism $\text{Hom}(G, G) \cong \text{Hom}(\widehat{G}, \widehat{G})$ in Theorem 6.2 coming from the identity map on G associates $g \mapsto g^m$ in $\text{Hom}(G, G)$ with $\chi \mapsto \chi^m$ in $\text{Hom}(\widehat{G}, \widehat{G})$.

7. ABELIAN GROUP DETERMINANTS

Consider a square $n \times n$ matrix where each row is obtained from the previous one by a cyclic shift:

$$(7.1) \quad \begin{pmatrix} X_0 & X_1 & X_2 & \cdots & X_{n-1} \\ X_{n-1} & X_0 & X_1 & \cdots & X_{n-2} \\ X_{n-2} & X_{n-1} & X_0 & \cdots & X_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ X_1 & X_2 & X_3 & \cdots & X_0 \end{pmatrix}.$$

Its determinant is called a *circulant*. When n is 2 and 3, the circulants are

$$\begin{vmatrix} X_0 & X_1 \\ X_1 & X_0 \end{vmatrix} = X_0^2 - X_1^2$$

and

$$\begin{vmatrix} X_0 & X_1 & X_2 \\ X_2 & X_0 & X_1 \\ X_1 & X_2 & X_0 \end{vmatrix} = X_0^3 + X_1^3 + X_2^3 - 3X_0X_1X_2$$

These factor as

$$(X_0 + X_1)(X_0 - X_1), \quad (X_0 + X_1 + X_2)(X_0 + \omega X_1 + \omega^2 X_2)(X_0 + \omega^2 X_1 + \omega X_2),$$

where $\omega = e^{2\pi i/3}$.

If we think about the variables X_i as being indexed by $\mathbf{Z}/(n)$ then the (i, j) entry of (7.1) is X_{j-i} . More generally, for any finite group G index a set of variables X_g by G and form the matrix indexed by $G \times G$ where the (g, h) entry is $X_{gh^{-1}}$. (The circulant is the determinant of the matrix $(X_{j-i}) = (X_{i-j})^\top$.) The determinant is called the *group determinant* of G :

$$(7.2) \quad \Delta(G) = \det(X_{gh^{-1}}).$$

This is a homogeneous polynomial of degree $\#G$ with integer coefficients. A circulant is the group determinant of a cyclic group.

The circulants of order 2 and 3 decompose into a product of linear factors, with roots of unity as coefficients. Dedekind and Burnside each discovered that the same property holds for the group determinant of any finite abelian group, but Dedekind's approach revealed more structure in the factors: the roots of unity in a given linear factor are the values of one of the characters of the group.

Theorem 7.1. *If G is a finite abelian group then its group determinant factors into linear factors over the complex numbers:*

$$\det(X_{gh^{-1}}) = \prod_{\chi \in \widehat{G}} \left(\sum_{g \in G} \chi(g) X_g \right).$$

Proof. We will realize $(X_{gh^{-1}})$ as the matrix for a certain linear transformation and then find a diagonalization to compute its determinant.

Let $V = \mathbf{C}[G]$ be the group ring of G . For each $v \in V$, define the linear map $L_v: V \rightarrow V$ to be (left) multiplication by v : $L_v(x) = vx$. We will compute the matrix for L_v with respect to the basis G of V . Writing $v = \sum_{g \in G} a_g g$ we have for each $h \in G$

$$L_v(h) = \sum_{g \in G} a_g gh = \sum_{g \in G} a_{gh^{-1}} g,$$

so the matrix for L_v with respect to the basis G is $(a_{gh^{-1}})$.

Another basis for $\mathbf{C}[G]$ is the set of formal sums $\sum_{g \in G} \chi(g)g$, one for each character χ of G . Indeed, the number of such sums has the right size to be a basis, and for any linear relation

$$\sum_{\chi} c_{\chi} \left(\sum_{g \in G} \chi(g)g \right) = 0$$

in $\mathbf{C}[G]$ we get $\sum_{\chi} c_{\chi} \chi(g) = 0$ for all g (the coefficient of each g is 0), so every c_{χ} is 0 by Fourier inversion.

This new basis of $\mathbf{C}[G]$, indexed by the characters, consists of eigenvectors for L_v :

$$\begin{aligned} L_v \left(\sum_{h \in G} \chi(h)h \right) &= \left(\sum_{g \in G} a_g g \right) \left(\sum_{h \in G} \chi(h)h \right) \\ &= \sum_{k \in G} \left(\sum_{gh=k} a_g \chi(h) \right) k \\ &= \sum_{k \in G} \left(\sum_{g \in G} a_g \chi(g^{-1}) \chi(k) \right) k \\ &= \left(\sum_{g \in G} a_g \chi(g^{-1}) \right) \left(\sum_{k \in G} \chi(k)k \right). \end{aligned}$$

Since $\det(L_v)$ is the product of the eigenvalues of L_v for an eigenbasis,

$$\det(a_{gh^{-1}}) = \prod_{\chi \in \widehat{G}} \left(\sum_{g \in G} a_g \bar{\chi}(g) \right).$$

If we interchange the roles of χ and $\bar{\chi}$ in this product then we obtain

$$\det(a_{gh^{-1}}) = \prod_{\chi \in \widehat{G}} \left(\sum_{g \in G} a_g \chi(g) \right).$$

Thus the multivariable polynomials $\det(X_{gh^{-1}})$ and $\prod_{\chi \in \widehat{G}} \sum_{g \in G} \chi(g) X_g$ are equal on all of \mathbf{C}^n , so they must be the same polynomial. \square

Example 7.2. Taking $G = \mathbf{Z}/(n)$ and $\zeta_n = e^{2\pi i/n}$,

$$\begin{aligned} \begin{vmatrix} X_0 & X_1 & \cdots & X_{n-1} \\ X_{n-1} & X_0 & \cdots & X_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ X_1 & X_2 & \cdots & X_0 \end{vmatrix} &= \prod_{j=0}^{n-1} \left(\sum_{k=0}^{n-1} \zeta_n^{jk} X_k \right) \\ &= \prod_{j=0}^{n-1} (X_0 + \zeta_n^j X_1 + \cdots + \zeta_n^{(n-1)j} X_{n-1}). \end{aligned}$$

Applications of the factorization of the group determinant for abelian (not necessarily cyclic) groups can be found in [4, §5.5].

If G is a nonabelian group then its group determinant has an irreducible factor with degree greater than 1. Studying irreducible factors of the group determinant for nonabelian G led Frobenius to discover representation theory and the correct extension of the notion of a character to (finite) nonabelian groups.

Exercises.

1. Check the factorization of the group determinant for $\mathbf{Z}/(4)$.
2. Compute and factor the group determinant of $\mathbf{Z}/(2) \times \mathbf{Z}/(2)$.
3. If G is nonabelian, show the polynomial $\Delta(G)$ in (7.2) is divisible by $\sum_{g \in G} X_g$, and more generally by $\sum \chi(g) X_g$ for any homomorphism $\chi: G \rightarrow S^1$.

APPENDIX A. ALTERNATE PROOF OF LEMMA 5.1

We will use characters of finite abelian groups to give another proof of Lemma 5.1: in a finite abelian group G , the order of any element in G divides the maximal order of the elements of G . Although this alternate proof is longer than the one in the main text, the point is just to see characters used again.

Lemma A.1. *For positive d and m with $d|m$, the natural reduction $(\mathbf{Z}/(m))^\times \rightarrow (\mathbf{Z}/(d))^\times$ is onto: when $(a, d) = 1$, there is b such that $b \equiv a \pmod{d}$ and $(b, m) = 1$.*

Proof. Let \tilde{d} be the product of the prime powers in m whose primes divide d , so $m = \tilde{d}n$ with $(\tilde{d}, n) = 1$. (For example, if $m = 90$ and $d = 6$ then $\tilde{d} = 18$ and $n = 5$.) Then $\tilde{d}|d$. By the Chinese remainder theorem we can find $b \in \mathbf{Z}$ satisfying

$$b \equiv a \pmod{\tilde{d}}, \quad b \equiv 1 \pmod{n}.$$

Then $b \equiv a \pmod{d}$ and b is relatively prime to m since it is relatively prime to d (a factor of \tilde{d}) and to n . \square

Lemma A.2. *Let G be a finite abelian group. If $x \in G$ has order m and $y \in G$ has order n then there is a character $\chi: G \rightarrow S^1$ such that $\chi(x)$ has order m and $\chi(y)$ has order n .*

Proof. The subgroup $\langle x \rangle$ is cyclic of order m , so there is an isomorphism $\chi: \langle x \rangle \cong \mu_m$. In particular, $\chi(x)$ has order m . Following the proof of Lemma 3.2, we can extend χ to a character on $\langle x, y \rangle$ (and then all the way up to G) by sending y to any solution $z \in S^1$ of the equation $z^k = \chi(y^k)$, where $k \geq 1$ is minimal such that $y^k \in \langle x \rangle$. We will show z can be picked to have order n in S^1 .

Since $y^n = 1 \in \langle x \rangle$, k divides n . Then y^k has order n/k , so $\chi(y^k)$ has order n/k because χ is one-to-one on $\langle x \rangle$. Write $\chi(y^k) = e^{2\pi i \ell / (n/k)} = e^{2\pi i \ell k / n}$, where $(\ell, n/k) = 1$. By Lemma A.1, there is an $\ell' \equiv \ell \pmod{n/k}$ such that $(\ell', n) = 1$. Since $\ell' k \equiv \ell k \pmod{n}$, $\chi(y^k) = e^{2\pi i \ell' k / n}$. Set $z = e^{2\pi i \ell' / n}$, which has order n . Since $z^k = \chi(y^k)$, we can set $\chi(y) = z$. \square

Lemma A.2 does not extend to more than two arbitrary elements in G . For instance, if $G = \mu_2 \times \mu_2$ then no character on G sends all three non-identity elements in G to -1 . (Why?)

Now we are ready to prove Lemma 5.1. As explained at the start of the first proof of Lemma 5.1, it suffices to construct from elements of two orders m and n an element of order $[m, n]$. By Lemma A.2, there is a character χ on G such that $\chi(g)$ has order m and $\chi(h)$ has order n . Write $\chi(g) = e^{2\pi i a / m}$ and $\chi(h) = e^{2\pi i b / n}$, where $(a, m) = 1$ and $(b, n) = 1$.

The roots of unity $e^{2\pi i / m}$ and $e^{2\pi i / n}$ are in $\chi(G)$. For instance, letting $aa' \equiv 1 \pmod{m}$, $\chi(g^{a'}) = \chi(g)^{a'} = e^{2\pi i aa' / m} = e^{2\pi i / m}$. The argument for $e^{2\pi i / n}$ is similar. Write $mu + nv = (m, n)$ for some integers u and v , so the equation $mn = m, n$ can be rewritten as

$$\frac{1}{[m, n]} = \frac{(m, n)}{mn} = \frac{mu + nv}{mn} = u \frac{1}{n} + v \frac{1}{m}.$$

Thus

$$e^{2\pi i / [m, n]} = (e^{2\pi i / n})^u (e^{2\pi i / m})^v \in \chi(G),$$

say $e^{2\pi i / [m, n]} = \chi(t)$. The order of t in G is divisible by the order of $\chi(t)$ in S^1 , so t has order divisible by $[m, n]$. Thus, raising t to a suitable power we obtain an element of G with order $[m, n]$.

APPENDIX B. FUNCTIONS OF TWO VARIABLES

When analyzing a function of several variables, it is a common theme to decompose it into a sum of products of functions of one variable. For instance, to solve a PDE like the heat equation $\partial_t u - c \partial_x^2 u = 0$, first separable solutions of the form $u(x, t) = g(x)h(t)$ are classified. It is too much to hope that a general solution is separable, but in nice situations there are theorems guaranteeing that a general solution can be written as an infinite series of separable solutions: $u(x, t) = \sum_{n \geq 1} g_n(x)h_n(t)$. This is where expansions in Fourier series first appeared in mathematics.

Using character theory, and in particular Parseval's formula, we will give an example of a function of two variables which is provably not equal to a series of products of functions of one variable.

Lemma B.1. *Fix a positive integer N . For vectors (z_1, \dots, z_N) and (w_1, \dots, w_N) in \mathbf{C}^N ,*

$$\left| \sum_{j,k=1}^N e^{-2\pi i jk/N} z_j w_k \right| \leq \sqrt{N} \left(\sum_{j=1}^N |z_j|^2 \right)^{1/2} \left(\sum_{k=1}^N |w_k|^2 \right)^{1/2}.$$

Proof. Write the double sum as an iterated single sum:

$$\sum_{j,k=1}^N e^{-2\pi i jk/N} z_j w_k = \sum_{j=1}^N \left(\sum_{k=1}^N e^{-2\pi i jk/N} w_k \right) z_j = \sum_{j=1}^N \widehat{f}(j) z_j,$$

where $f: \mathbf{Z}/(N) \rightarrow \mathbf{C}$ by $f(k) = w_k$. The right side brings in the Fourier transform of f , where we think about \widehat{f} as a function on $\mathbf{Z}/(N)$ by identifying $\mathbf{Z}/(N)$ with its own character group in the natural way (Exercise 3.1).

Using the Cauchy–Schwarz inequality,

$$\left| \sum_{j=1}^N \widehat{f}(j) z_j \right| \leq \left(\sum_{j=1}^N |\widehat{f}(j)|^2 \right)^{1/2} \left(\sum_{j=1}^N |z_j|^2 \right)^{1/2}.$$

By Parseval's formula on $\mathbf{Z}/(N)$, $\sum_{j=1}^N |\widehat{f}(j)|^2 = N \sum_{k=1}^N |f(k)|^2 = N \sum_{k=1}^N |w_k|^2$. \square

Theorem B.2. *It is impossible to write*

$$e^{2\pi i x k} = \sum_{n \geq 1} g_n(x) h_n(k),$$

where $x \in [0, 1]$, $k \in \mathbf{Z}$, the functions $g_n: [0, 1] \rightarrow \mathbf{C}$ and $h_n: \mathbf{Z} \rightarrow \mathbf{C}$ are each bounded, and $\sum_{n \geq 1} \|g_n\|_{\sup} \|h_n\|_{\sup} < \infty$, where $\|\cdot\|_{\sup}$ is the sup-norm on bounded functions.

Proof. Assume there is a series expansion

$$e^{2\pi i x k} = \sum_{n \geq 1} g_n(x) h_n(k)$$

for all $x \in [0, 1]$ and $k \in \mathbf{Z}$, where $c := \sum_{n \geq 1} \|g_n\|_{\sup} \|h_n\|_{\sup} < \infty$. That means the series representation is absolutely convergent for all x and k . Pick $N \geq 1$ and $x_1, \dots, x_N \in [0, 1]$. Then

$$\sum_{j,k=1}^N e^{-2\pi i j k / N} e^{2\pi i x_j k} = \sum_{j,k=1}^N e^{-2\pi i j k / N} \left(\sum_{n \geq 1} g_n(x_j) h_n(k) \right) = \sum_{n \geq 1} \sum_{j,k=1}^N e^{-2\pi i j k / N} g_n(x_j) h_n(k).$$

Then

$$\begin{aligned} \left| \sum_{j,k=1}^N e^{-2\pi i j k / N} e^{2\pi i x_j k} \right| &= \left| \sum_{n \geq 1} \sum_{j,k=1}^N e^{-2\pi i j k / N} g_n(x_j) h_n(k) \right| \\ &\leq \sum_{n \geq 1} \left| \sum_{j,k=1}^N e^{-2\pi i j k / N} g_n(x_j) h_n(k) \right| \\ &\leq \sum_{n \geq 1} \sqrt{N} \left(\sum_{j=1}^N |g_n(x_j)|^2 \right)^{1/2} \left(\sum_{k=1}^N |h_n(k)|^2 \right)^{1/2} \end{aligned}$$

by Lemma B.1. Since $\sum_{j=1}^N |g_n(x_j)|^2 \leq N \|g_n\|_{\sup}^2$ and $\sum_{k=1}^N |h_n(k)|^2 \leq N \|h_n\|_{\sup}^2$,

$$\left| \sum_{j,k=1}^N e^{-2\pi i j k / N} e^{2\pi i x_j k} \right| \leq \sum_{n \geq 1} \sqrt{N} \sqrt{N} \|g_n\|_{\sup} \sqrt{N} \|h_n\|_{\sup} \leq N^{3/2} c.$$

Now set $x_j = j/N$:

$$\sum_{j,k=1}^N e^{-2\pi i j k / N} e^{2\pi i x_j k} = \sum_{j,k=1}^N e^{-2\pi i j k / N} e^{2\pi i j k / N} = N^2,$$

so $N^2 \leq N^{3/2}c$ for all $N \geq 1$. This is false when N is large enough ($N > c^2$). \square

This theorem says we can't write $e^{2\pi i x k} = \sum_{n \geq 1} g_n(x) h_n(k)$ where the functions g_n and h_n are bounded and the series converges absolutely (since convergence of $\sum_{n \geq 1} \|g_n\|_{\sup} \|h_n\|_{\sup}$ implies absolute convergence). I don't know if there could be such a series representation of $e^{2\pi i x k}$ which is only conditionally convergent.

REFERENCES

- [1] K. Ireland and M. Rosen, "A Classical Introduction to Modern Number Theory," 2nd ed., Springer-Verlag, New York, 1990.
- [2] A. Terras, "Fourier Analysis on Finite Groups and Applications," Cambridge Univ. Press, Cambridge, 1999.
- [3] W. Trappe and L. Washington, "Introduction to Cryptography with Coding Theory," Prentice-Hall, Upper Saddle River, NJ 2002.
- [4] L. Washington, "Introduction to Cyclotomic Fields," 2nd ed., Springer-Verlag, New York, 2000.