CHARACTERS OF FINITE ABELIAN GROUPS

KEITH CONRAD

1. Introduction

The theme we will study is an analogue on finite abelian groups of Fourier analysis on $\mathbf{R}$. A Fourier series on the real line is the following type of series in sines and cosines:

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

This is 2π-periodic. Since $e^{inx} = \cos(nx) + i\sin(nx)$ and $e^{-inx} = \cos(nx) - i\sin(nx)$, a 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 $\chi\colon G \to S^1$.

We will usually write abstract groups multiplicatively, so $\chi(g_1g_2) = \chi(g_1)\chi(g_2)$ and $\chi(1) = 1$.

Example 1.2. The *trivial* character of G is the homomorphism $\mathbf{1}_G$ defined by $\mathbf{1}_G(g) = 1$ 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
$\mathbf{1}_G$	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 nth 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 of the group $(\mathbf{Z}/(m))^\times$ to prove that when $(a, m) = 1$ there are infinitely many primes $p \equiv a \bmod m$. The quadratic reciprocity law of elementary number theory is concerned with a deep property of a particular character, the Legendre symbol. Fourier series on finite abelian groups have applications in engineering: signal processing (the fast Fourier transform [2, Chap. 9]) and error-correcting codes [2, Chap. 11].

To provide a context against which our development of characters on 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. In particular, we will see that a finite abelian group is isomorphic to its dual group, but not naturally, and it is naturally isomorphic to its double-dual group (Pontryagin duality). 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 duality on group homomorphisms. 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 nth roots of unity in the unit circle S^1. It is a cyclic group of size n.

Exercises.

1. Make a character table for $\mathbf{Z}/(2) \times \mathbf{Z}/(2)$, with columns labeled by elements of the group and rows labeled by characters, as in Table 1.
2. Let G be a finite nonabelian simple group. (Examples include A_n for $n \geq 5$.) Show the only group homomorphism $\chi \colon G \to S^1$ 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 $f \colon \mathbf{R} \to \mathbf{C}$ that 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 nth Fourier coefficient c_n can be recovered as an integral:

$$c_n = \frac{1}{2\pi} \int_0^{2\pi} f(x) e^{-inx} \, \mathrm{d}x. \tag{2.1}$$

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

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

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

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

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

$$f(x) = \sum_{n\in\mathbf{Z}} c_n e^{2\pi inx}, \qquad c_n = \int_0^1 f(x)e^{-2\pi inx}\,\mathrm{d}x. \tag{2.2}$$

Parseval's formula becomes

$$\sum_{n\in\mathbf{Z}} |c_n|^2 = \int_0^1 |f(x)|^2\,\mathrm{d}x. \tag{2.3}$$

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

In addition to Fourier series there are Fourier integrals. The *Fourier transform* of a function f that decays rapidly at $\pm\infty$ is the function $\widehat{f}\colon \mathbf{R}\to\mathbf{C}$ defined by the integral formula

$$\widehat{f}(y) = \int_{\mathbf{R}} f(x)e^{-2\pi ixy}\,\mathrm{d}x.$$

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 $\widehat{f}$:

$$f(x) = \int_{\mathbf{R}} \widehat{f}(y)e^{2\pi ixy}\,\mathrm{d}y.$$

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

$$\langle f_1, f_2\rangle = \int_{\mathbf{R}} f_1(x)\overline{f}_2(x)\,\mathrm{d}x \in \mathbf{C},$$

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

$$\langle \widehat{f_1}, \widehat{f_2}\rangle = \langle f_1, f_2\rangle. \tag{2.4}$$

In particular, when $f_1 = f_2 = f$ the result is

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

which is called Parseval's formula since it 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

$$(f_1 * f_2)(x) = \int_{\mathbf{R}} f_1(t)f_2(x-t)\,\mathrm{d}t$$

and the Fourier transform turns this convolution into pointwise multiplication:

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

Example 2.1. A Gaussian is a function of the form ae^{-bx^2}, where $b > 0$. For example, the Gaussian $(1/\sqrt{2\pi})e^{-(1/2)x^2}$ is important in probability theory. The Fourier transform of a Gaussian is another Gaussian and the convolution of two Gaussians is another Gaussian:

$$\int_{\mathbf{R}} ae^{-bx^2}e^{-2\pi ixy}\,\mathrm{d}x = \sqrt{\frac{\pi}{b}}ae^{-\pi^2y^2/b} \tag{2.5}$$

and

$$f_1(x) = e^{-b_1x^2}, \quad f_2(x) = e^{-b_2x^2} \Longrightarrow (f_1 * f_2)(x) = \sqrt{\frac{\pi}{b_1+b_2}}e^{-(b_1b_2/(b_1+b_2))x^2}.$$

The formula (2.5) says that a highly peaked Gaussian (large b) has a Fourier transform that is a spread out Gaussian (small π^2/b) and *vice versa*. More generally, a function and its Fourier transform can't both be highly localized; this is a mathematical incarnation of Heisenberg's uncertainty principle from physics.

When $b = \pi$, (2.5) tells us that $ae^{-\pi x^2}$ is its own Fourier transform. Functions equal to their Fourier transform are called *self-dual*, and $e^{-\pi x^2}$ is the simplest nonzero example.

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

$$\sum_{n\in\mathbf{Z}} f(n) = \sum_{n\in\mathbf{Z}} \widehat{f}(n), \tag{2.6}$$

where $\widehat{f}(y) = \int_{\mathbf{R}} f(x)e^{-2\pi ixy}\,\mathrm{d}x$. For example, when $f(x) = e^{-bx^2}$ (with $b > 0$), the Poisson summation formula says

$$\sum_{n\in\mathbf{Z}} e^{-bn^2} = \sum_{n\in\mathbf{Z}} \sqrt{\frac{\pi}{b}}e^{-\pi^2n^2/b}.$$

To prove the Poisson summation formula, we 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: $F(x) = \sum_{n\in\mathbf{Z}} c_ne^{2\pi inx}$. Then

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

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

$$\sum_{n\in\mathbf{Z}} f(x+n) = \sum_{n\in\mathbf{Z}} \widehat{f}(n)e^{2\pi inx}, \tag{2.7}$$

which becomes the Poisson summation formula (2.6) 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":

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

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

There are several conventions for the definition of the Fourier transform as well as the inner product and convolution of functions. Tables 2 and 3 collect a number of different 2π-conventions. The first two columns of Tables 2 and 3 are definitions and the other columns are theorems.

$\widehat{f}(y)$	$\langle f_1, f_2\rangle$	$f(x)$	$\langle \widehat{f_1}, \widehat{f_2}\rangle$
$\int_{\mathbf{R}} f(x)e^{-2\pi ixy}\,\mathrm{d}x$	$\int_{\mathbf{R}} f_1(x)\overline{f}_2(x)\,\mathrm{d}x$	$\int_{\mathbf{R}} \widehat{f}(y)e^{2\pi ixy}\,\mathrm{d}y$	$\langle f_1, f_2\rangle$
$\int_{\mathbf{R}} f(x)e^{-ixy}\,\mathrm{d}x$	$\int_{\mathbf{R}} f_1(x)\overline{f}_2(x)\,\mathrm{d}x$	$\frac{1}{2\pi}\int_{\mathbf{R}} \widehat{f}(y)e^{ixy}\,\mathrm{d}y$	$2\pi\langle f_1, f_2\rangle$
$\frac{1}{\sqrt{2\pi}}\int_{\mathbf{R}} f(x)e^{-ixy}\,\mathrm{d}x$	$\frac{1}{\sqrt{2\pi}}\int_{\mathbf{R}} f_1(x)\overline{f}_2(x)\,\mathrm{d}x$	$\frac{1}{\sqrt{2\pi}}\int_{\mathbf{R}} \widehat{f}(y)e^{ixy}\,\mathrm{d}y$	$\langle f_1, f_2\rangle$

Table 2.

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

Table 3.

When the Fourier transform is defined using $\widehat{f}(y) = \frac{1}{\sqrt{2\pi}}\int_{\mathbf{R}} f(x)e^{-ixy}\,\mathrm{d}x$, the function $e^{-\pi x^2}$ is no longer self-dual, but $e^{-(1/2)x^2}$ is self-dual. You need to know how the Fourier transform is defined to say that a particular function is self-dual.

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 $f \colon \mathbf{R} \to \mathbf{C}$ and $c \in \mathbf{R}$, let $g(x) = f(x+c)$. Define the Fourier transform of a function h by $\widehat{h}(y) = \int_{\mathbf{R}} h(x)e^{-2\pi ixy}\,\mathrm{d}x$. If f has a Fourier transform, show g has Fourier transform $\widehat{g}(y) = e^{2\pi icy}\widehat{f}(y)$.
4. The Poisson summation formula over $\mathbf{R}$ was obtained by setting $x = 0$ in (2.7). Conversely, show that (2.7) 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

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

for all x then

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

(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.

3. Finite Abelian Group 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 of 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 nth 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 nth root of unity (not necessarily of exact order n, *e.g.*, $\mathbf{1}_G(\gamma) = 1$), so there are at most n characters. We now write down n characters.

Let ζ be any nth 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 $j \equiv k \bmod n$ 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 of 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 $\chi \colon H \to S^1$ be a character of H. We will extend χ to a character $\widetilde{\chi}$ of $\langle H, a\rangle$ and count the number of possible $\widetilde{\chi}$. 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 $\widetilde{\chi}(a)$? Since $a \notin H$, $\widetilde{\chi}(a)$ is not initially defined. But some power a^k is in H for $k \geq 1$ (*e.g.*, $k = [G : H]$), and therefore $\widetilde{\chi}(a^k)$ *is* defined: $\widetilde{\chi}(a^k) = \chi(a^k)$.

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 $\widetilde{\chi}$ is going to be a character then $\widetilde{\chi}(a)$ *must* be an k-th root of $\chi(a^k)$. That is our clue: define $\widetilde{\chi}(a) \in S^1$ to be a solution to $z^k = \chi(a^k)$:

$$\widetilde{\chi}(a)^k = \chi(a^k). \tag{3.1}$$

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

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

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

This formula does cover all possible elements of $\langle H, a\rangle$, but is $\widetilde{\chi}$ 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 $\widetilde{\chi}$. Suppose $ha^i = h'a^{i'}$. Then $a^{i-i'} \in H$, so $i' \equiv i \bmod k$ 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

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

Therefore $\widetilde{\chi}\colon \langle H, a\rangle \to S^1$ 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 $\widetilde{\chi}$ extending χ is the number of choices for $\widetilde{\chi}(a)$, 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 $\widetilde{\chi}$ to a character of G, so the number of extensions of a character on H to a character on G is $[G : \langle H, a\rangle][\langle H, a\rangle : H] = [G : H]$. □

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. □

We have used two important features of S^1 as the target group for characters: for any $k \geq 1$ the kth 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).

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 that takes different values at g_1 and g_2.*

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

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 that is trivial on H and not equal to 1 at g.*

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

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

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

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 $\chi \colon G \to S^1$ 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 $G/[G, G] \to S^1$ that's nontrivial on $\overline{g}$. Composing this character with the reduction map $G \to G/[G, G]$ produces a homomorphism $G \to S^1$ that is nontrivial on g. Therefore $[G, G] = \bigcap_\chi \ker \chi$, where the intersection runs over all homomorphisms $\chi \colon G \to S^1$. 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 $\overline{\chi} \colon G \to S^1$ given by $\overline{\chi}(g) := \overline{\chi(g)}$.

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

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

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

Theorem 3.3 says in part that

$$|G| = |\widehat{G}|. \tag{3.3}$$

In fact, the groups G and $\widehat{G}$ are *isomorphic*. First let's check this on cyclic groups.

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

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

Let $n = |G|$ and γ be a generator of G. Set $\chi\colon G \to S^1$ 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 $\widehat{G}$. □

Lemma 3.10. *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 of 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

$$\widehat{A \times B} \to \widehat{A} \times \widehat{B} \tag{3.4}$$

by sending χ to (χ_A, χ_B). It is left to the reader to check (3.4) 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 (3.4) have the same size by (3.3), so (3.4) is an isomorphism. □

Theorem 3.11. *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 3.10 extends easily to several factors in a direct product:

$$(H_1 \times \cdots \times H_r)^{\widehat{}} \cong \widehat{H}_1 \times \cdots \times \widehat{H}_r. \tag{3.5}$$

When H_i is cyclic, $\widehat{H}_i \cong H_i$, so (3.5) tells us that that dual group of $H_1 \times \cdots \times H_r$ is isomorphic to $H_1 \times \cdots \times H_r$. Every finite abelian group is isomorphic to a direct product of cyclic groups, so the dual group of any finite abelian group is isomorphic to itself. □

Although G and $\widehat{G}$ are isomorphic, there is *not* any kind of natural isomorphism between them, even when G is cyclic. For instance, to prove $G \cong \widehat{G}$ when G is cyclic we had to *choose* a generator. If we change the generator, then the isomorphism changes.[1]

The double-dual group $\widehat{\widehat{G}}$ is the dual group of $\widehat{G}$. Since G and $\widehat{G}$ are isomorphic, G and $\widehat{\widehat{G}}$ are isomorphic. However, while there isn't a natural isomorphism from G to $\widehat{G}$, there *is* a natural isomorphism from G to $\widehat{\widehat{G}}$. The point is that there is a natural way to map G to its double-dual group: associate to each $g \in G$ the function "evaluate at g," which is the function $\widehat{G} \to S^1$ given by $\chi \mapsto \chi(g)$. Here g is fixed and χ varies. This is a character of $\widehat{G}$, since $(\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g)$ by definition.

[1] If G is trivial or of order 2, then it has a unique generator, so in that case we could say the isomorphism $G \cong \widehat{G}$ is canonical.

Theorem 3.12. *Let G be a finite abelian group. The homomorphism $G \to \widehat{\widehat{G}}$ 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 3.12 is called *Pontryagin duality*. This label actually applies to a more general result about characters of 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 G as a dual group (namely the dual group of $\widehat{G}$).

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

To illustrate Pontryagin duality, consider the following theorem.

Theorem 3.13. *Let G be a finite abelian group and $m \in \mathbf{Z}$.*

a) For $g \in G$, $g^m = 1$ if and only if $\chi(g) = 1$ for every $\chi \in \widehat{G}$ that is an mth power in $\widehat{G}$.

b) For $g \in G$, g is an mth power in G if and only if $\chi(g) = 1$ for every $\chi \in \widehat{G}$ satisfying $\chi^m = \mathbf{1}_G$.

Proof. a) 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.

b) If $g = x^m$ for some $x \in G$ then for every $\chi \in \widehat{G}$ such that $\chi^m = \mathbf{1}_G$ we have

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

Conversely, assume $\chi(g) = 1$ for all χ such that $\chi^m = \mathbf{1}_G$. Such χ are identically 1 on the subgroup G^m of mth powers in G. Conversely, every character of G that is trivial on the subgroup G^m has mth power $\mathbf{1}_G$ (why?). Therefore $\chi(g) = 1$ for all χ in $\widehat{G}$ that are trivial on G^m, so $g \in G^m$ by Corollary 3.5. $\square$

Since Theorem 3.13 is a theorem about *all* finite abelian groups, by Pontryagin duality we can swap the roles of G and $\widehat{G}$ in the theorem. Part a is equivalent to

$$\chi^m = \mathbf{1}_G \Longleftrightarrow \chi(g) = 1 \text{ for every } g \in G \text{ such that } g = x^m \text{ for some } x \in G$$

and part b is equivalent to

$$\chi \text{ is an } m\text{th power in } \widehat{G} \Longleftrightarrow \chi(g) = 1 \text{ for all } g \in G \text{ such that } g^m = 1.$$

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 $\chi_k \colon \mathbf{Z}/(m) \to S^1$ by
   $$\chi_k(j) = e^{2\pi i jk/m},$$
   so $\chi_k(1) = e^{2\pi i k/m}$. Show $\chi_0, \chi_1, \ldots, \chi_{m-1}$ 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

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

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 $\chi^2 = \mathbf{1}_G$.
3. Describe the error in the following bogus proof of Lemma 3.2. Let $m = [G : H]$ and pick a set of coset representatives $g_1, \ldots, g_m$ for G/H. Given a character χ on H, define $\widetilde{\chi}$ on G by first picking the m $(= [G : H])$ values $\widetilde{\chi}(g_i)$ for $1 \leq i \leq m$ and then writing any $g \in G$ in the (unique) form $g_i h$ and defining $\widetilde{\chi}(g) = \widetilde{\chi}(g_i)\chi(h)$. This defines $\widehat{\chi}$ on G, and since we had to make m choices there are m characters.
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 $G \to S^1$) separate elements modulo $[G, G]$: $\chi(g_1) = \chi(g_2)$ for all χ if and only if $g_1 = g_2$ in $G/[G, G]$.
6. This exercise will give an interpretation of characters as eigenvectors. For a finite abelian group G and $g \in G$, let $T_g \colon L(G) \to L(G)$ by $(T_g f)(x) = f(gx)$.

(a) Show the T_g's are commuting linear transformations and any character of G is an eigenvector of each T_g.

(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 characters of G are the simultaneous eigenvectors of the T_g's, suitably normalized.

(c) Show the T_g's are each diagonalizable. Deduce from this and parts (a) 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.)

7. 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, $G^\perp = \{\mathbf{1}_G\}$ 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, $|H|^\perp = [G : H]$.

8. 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 $n-d$.

9. 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 $(G^n)^\perp = \widehat{G}[n]$ in $\widehat{G}$.

4. Finite Fourier series

We will introduce the analogue of Fourier series on finite abelian groups.

Let G be a finite abelian group. Set

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

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):

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

Indeed, evaluate both sides at each $x \in G$ and we get the same value. The functions δ_g span $L(G)$ by (4.1) and they are linearly independent: if $\sum_g a_g\delta_g = 0$ then evaluating the sum at $x \in G$ shows $a_x = 0$. 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, which will lead to a Fourier series expansion of f. It is the first time we *add* character values.

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

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

Proof. Let $S = \sum_{g \in G} \chi(g)$. If χ is trivial on G then $S = |G|$. If χ is not trivial on G, say $\chi(g_0) \neq 1$. Then $\chi(g_0)S = \sum_{g \in G} \chi(gg_0) = \sum_{g \in G} \chi(g) = S$, so $S = 0$.

The second formula in the theorem can be viewed as an instance of the first formula via Pontryagin duality: the second sum is a sum of the character "evaluate at g" over the group $\widehat{G}$, and this character on $\widehat{G}$ is nontrivial when $g \neq 1$ by Pontryagin duality. $\square$

Theorem 4.1 says the sum of a nontrivial character over a group vanishes and the sum of all characters of a group evaluated at a nontrivial element vanishes, so the sum of the elements in each row and column of a character table of G is zero except the row for the trivial character and the column for the identity element. Check this in Table 1.

Corollary 4.2. *For characters χ_1 and χ_2 in $\widehat{G}$ and g_1 and g_2 in G,*

$$\sum_{g \in G} \chi_1(g)\overline{\chi}_2(g) = \begin{cases} |G|, & \text{if } \chi_1 = \chi_2, \\ 0, & \text{if } \chi_1 \neq \chi_2, \end{cases} \qquad \sum_{\chi \in \widehat{G}} \chi(g_1)\overline{\chi}(g_2) = \begin{cases} |G|, & \text{if } g_1 = g_2, \\ 0, & \text{if } g_1 \neq g_2. \end{cases}$$

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 $g = g_1g_2^{-1}$. (Alternatively, after proving the first equation for all G we observe that the second equation is a special case of the first by Pontryagin duality.) $\square$

The equations in Corollary 4.2 are called the *orthogonality relations*. They say that the character table of G has orthogonal rows and orthogonal columns when we define orthogonality of two n-tuples of complex numbers as vanishing of their Hermitian inner product: in $\mathbf{C}^n$: $\langle (z_1,\dots,z_n),(w_1,\dots,w_n)\rangle := \sum_{k=1}^n z_k\overline{w_k}$.

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:

$$\sum_{\chi\in\widehat{G}}\chi(g)\overline{\chi}(x) = |G|\delta_g(x) \Longrightarrow \delta_g(x) = \frac{1}{|G|}\sum_{\chi\in\widehat{G}}\overline{\chi}(g)\chi(x).$$

Substituting this formula for δ_g into (4.1) gives

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

where

$$c_\chi = \frac{1}{|G|}\sum_{g\in G} f(g)\overline{\chi}(g). \tag{4.3}$$

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 $f(g)\overline{\chi}(g)$. The number e^{-inx} is the conjugate of e^{inx}, which is also the relation between $\overline{\chi}(g)$ 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

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

By (4.2) and (4.3),

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

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 $\mathbf{R} \to \mathbf{C}$ is another function $\mathbf{R} \to \mathbf{C}$. The finite Fourier transform, however, is defined on the dual group instead of on the original group. We can also interpret the classical Fourier transform to be a function of characters. For $y \in \mathbf{R}$ let $\chi_y(x) = e^{ixy}$. Then $\chi_y \colon \mathbf{R} \to S^1$ is a character and $\widehat{f}(y)$ could be viewed as $\widehat{f}(\chi_y) = \int_{\mathbf{R}} f(x)\overline{\chi}_y(x)\,\mathrm{d}x$, so $\widehat{f}$ is a function of characters rather than of numbers.

Example 4.6. Let $f = \delta_g$. Then $\widehat{f}(\chi) = \overline{\chi}(g) = \chi(g^{-1})$. 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 $\widehat{f}(\chi) = \sum_g \psi(g)\overline{\chi}(g) = |G|\delta_\psi(\chi)$, 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). This will be the only time (outside Appendix B) when we will use inequalities with characters of finite abelian groups.

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

$$|\operatorname{supp} f| \cdot |\operatorname{supp} \widehat{f}| \geq |G|, \tag{4.5}$$

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

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

we have

$$|f(x)| \leq \sum_{\chi \in \widehat{G}} \frac{1}{|G|}|\widehat{f}(\chi)| \leq \frac{|\operatorname{supp} \widehat{f}|}{|G|} \max_{\chi \in \widehat{G}} |\widehat{f}(\chi)|. \tag{4.6}$$

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

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

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

$$|f(x)| \leq \frac{m|\operatorname{supp} f||\operatorname{supp} \widehat{f}|}{|G|}.$$

Maximizing over all $x \in G$ implies $m \leq m|\operatorname{supp} f||\operatorname{supp} \widehat{f}|/|G|$. Divide both sides by m and the desired inequality drops out. ∎

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

$$\langle f_1, f_2\rangle_G = \frac{1}{|G|}\sum_{g\in G} f_1(g)\overline{f}_2(g) \in \mathbf{C}. \tag{4.8}$$

We will prove Plancherel's theorem for G:

$$\langle f_1, f_2\rangle_G = \frac{1}{|G|}\langle \widehat{f_1}, \widehat{f_2}\rangle_{\widehat{G}}$$

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:

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

Let's look at Fourier transforms for functions on a cyclic group. By writing a cyclic group in the form $\mathbf{Z}/(m)$, we can make an isomorphism with the dual group explicit: every character of $\mathbf{Z}/(m)$ has the form $\chi_k\colon j \mapsto e^{2\pi ijk/m}$ for a unique $k \in \mathbf{Z}/(m)$ (Exercise 3.1). The Fourier transform of a function $f\colon \mathbf{Z}/(m) \to \mathbf{C}$ can be regarded as a function not on $\widehat{\mathbf{Z}/(m)}$, but on $\mathbf{Z}/(m)$:

$$\widehat{f}(k) := \sum_{j\in\mathbf{Z}/(m)} f(j)\overline{\chi_k}(j) = \sum_{j\in\mathbf{Z}/(m)} f(j)e^{-2\pi ijk/m}. \tag{4.10}$$

This is similar to the classical viewpoint of the Fourier transform of a function on $\mathbf{R}$ as another function of $\mathbf{R}$.

Example 4.9. Let $f\colon \mathbf{Z}/(8) \to \mathbf{C}$ 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

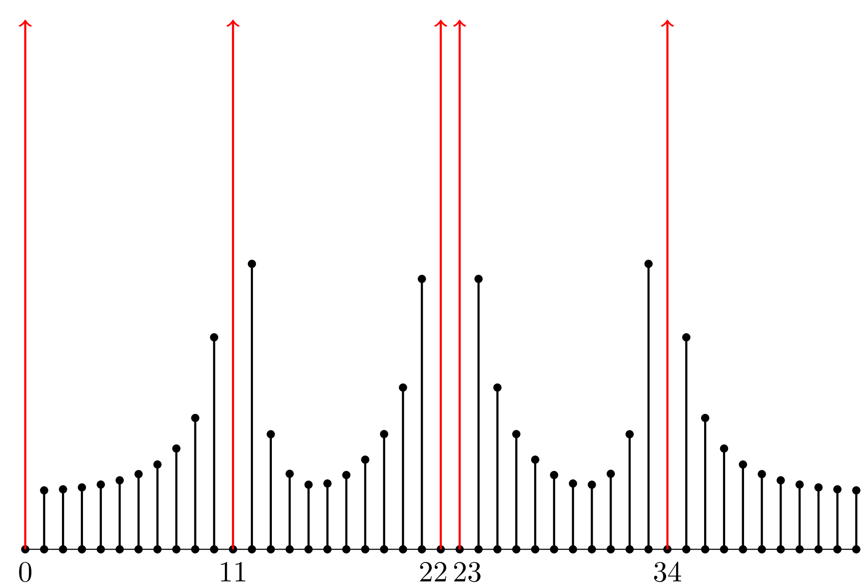
Table 4.

Example 4.10. Let $f\colon \mathbf{Z}/(8) \to \mathbf{C}$ have the periodic values 5, 3, 1, and 1. Both f and its Fourier transform are 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 $f\colon \mathbf{Z}/(45) \to \mathbf{C}$ with the four successive repeating values 1, 8, 19, 17 starting with $f(0) = 1$. 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. (The value of $f(44)$ is 1.) A calculation of $|\widehat{f}(n)|$, the *absolute value* of the Fourier transform of f, reveals sharp peaks at $n = 0, 11, 22, 23$, and 34. A plot of $|\widehat{f}(n)|$ is below. The red peaks are cut off because the lowest red bar would be around three times as tall as the highest black bar. Peaks in $|\widehat{f}(n)|$ occur approximately at multiples of the approximate frequency!



As Examples 4.9 and 4.10 suggest, 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 has nonzero values (Exercise 4.4). For *nearly* periodic functions on $\mathbf{Z}/(m)$, the approximate frequency is reflected in where the Fourier transform takes on its largest values. This idea is used in Shor's quantum algorithm for integer factorization [3], [4, Chap. 17], where it is convenient to redefine the Fourier transform (4.10) by dividing the sum by $\sqrt{m}$, which has the effect of making the Fourier transform a unitary operator on the functions $\mathbf{Z}/(m) \to \mathbf{C}$. See Exercise 4.10.

Exercises.

1. Let G be a finite abelian group, H be a subgroup of G, and K be a subgroup of $\widehat{G}$. Show

$$\sum_{h \in H} \chi(h) = \begin{cases} |H|, & \text{if } \chi \text{ is trivial on } H, \\ 0, & \text{otherwise,} \end{cases} \qquad \sum_{\chi \in K} \chi(g) = \begin{cases} |K|, & \text{if } \chi(g) = 1 \text{ for all } \chi \in K, \\ 0, & \text{otherwise.} \end{cases}$$

2. Let $f \colon \mathbf{Z}/(8) \to \mathbf{C}$ 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 $\widehat{f}(4) = 0$.
3. For any subgroup H of a finite abelian group G, let δ_H be the function that 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 $f \colon G \to \mathbf{C}$ 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 $f \colon \mathbf{Z}/(m) \to \mathbf{C}$ has period d where $d|m$, show $\widehat{f} \colon \mathbf{Z}/(m) \to \mathbf{C}$ 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 $f \colon G \to \mathbf{C}$, 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 3.7. 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

$$\frac{1}{|H|} \sum_{h \in H} f(xh) = \frac{1}{|G|} \sum_{\chi \in H^\perp} \widehat{f}(\chi)\chi(x) \tag{4.11}$$

   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 $T_g \colon L(G) \to L(G)$ be as in Exercise 3.6.
   (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 $\langle T_g f_1, T_g f_2 \rangle_G = \langle f_1, f_2 \rangle_G$.
8. 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:

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

Check the identity $\widehat{\mathrm{Avg}_H(f)} = \mathrm{Cut}_{H^\perp}(\widehat{f})$ 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 (4.11) 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 $\mathrm{Cut}_{H^\perp}$ on $L(\widehat{G})$, or equivalently Cut_H on $L(G)$ and $\mathrm{Avg}_{H^\perp}$ on $L(\widehat{G})$.)

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

$$(f_1 * f_2)(g) = \sum_{h\in G} f_1(h)f_2(gh^{-1}).$$

(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 $h_\chi \colon L(G) \to \mathbf{C}$ 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?

10. On every finite abelian group G, rescale the definition of the Fourier transform by dividing by $\sqrt{|G|}$:

$$\widehat{f}(\chi) := \frac{1}{\sqrt{|G|}}\sum_{g\in G} f(g)\overline{\chi}(g).$$

Verify the following new versions of Fourier inversion and Plancherel's theorem: $f(g) = \frac{1}{\sqrt{|G|}}\sum_\chi \widehat{f}(\chi)\chi(g)$ and $\langle f_1, f_2\rangle_G = \langle \widehat{f_1}, \widehat{f_2}\rangle_{\widehat{G}}$.

Check that this new Fourier transform sends convolution on $L(G)$ (Exercise 4.9) to multiplication only if we redefine convolution using division by $\sqrt{|G|}$:

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

5. Structure of finite abelian groups

We will now put characters to work by using them to prove that every finite abelian group is a direct product of cyclic groups. This result was already used in the proof of Theorem 3.11, that $G \cong \widehat{G}$, but that work will not be used here, so no circular reasoning will occur.

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_1k_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_1k_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 $[n_1, n_2] = k_1k_2$ 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 $k_1k_2 = [n_1, n_2]$. □

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 $\chi \in \widehat{G}$. □

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 $\chi \colon G \to S^1$ 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 $h := xg^{-k}$ is in H and $x = hg^k$. This proves that multiplication $H \times \langle g \rangle \to G$ is surjective. It is a homomorphism and its kernel is trivial, so this is an isomorphism. $\square$

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 $|G| = 2$. 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

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

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.

Exercises.

1. Write the groups $\mathbf{Z}/(2) \times \mathbf{Z}/(3) \times \mathbf{Z}/(4)$ and $\mathbf{Z}/(4) \times \mathbf{Z}/(10)$ in the form of Theorem 5.5, where the successive moduli n_i divide each other.
2. What is the structure (as a direct product of cyclic groups) of the finite abelian groups whose nontrivial characters all have order 2?
3. 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.
4. 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 that restricts to an isomorphism from H to K.
5. For any finite abelian group G, show the maximum order of the elements of G and the number $|G|$ have the same prime factors. (This is false in general for nonabelian G, *e.g.*, $G = S_3$.)

6. Let G be a finite abelian group and F be a field containing a full set of $|G|$th roots of unity. (That is, the equation $x^{|G|} = 1$ has $|G|$ solutions in F.) Define characters of G to be group homomorphisms $\chi\colon G \to F^\times$ and write the set of all such characters as $\widehat{G}$.
   a) Construct a character table for $\mathbf{Z}/(4)$ and $(\mathbf{Z}/(2))^2$ when F is the field $\mathbf{Z}/(5)$.
   b) Prove every lemma, theorem, and corollary from Section 3 for the new meaning of $\widehat{G}$. There is no longer complex conjugation on character values, but the inverse of χ is still the function $g \mapsto \chi(g^{-1}) = \chi(g)^{-1}$. (Hint: For each d dividing $|G|$, $x^d = 1$ has d distinct solutions in $F^\times$, which form a cyclic group.)
   c) Prove Theorem 4.1 and Corollary 4.2 for F-valued characters of G.
   d) Set $L(G, F)$ to be the functions $G \to F$. This is an F-vector space in the same way that $L(G)$ is a complex vector space. For any function $f \in L(G, F)$, define its Fourier transform $\widehat{f} \in L(\widehat{G}, F)$ by $\widehat{f}(\chi) = \sum_{g\in G} f(g)\chi(g^{-1})$. Prove the Fourier inversion formula and Plancherel's theorem in this context. (Note: If the field F has characteristic p then $1/|G|$ in the Fourier inversion formula makes sense in F since p doesn't divide $|G|$ – why?)
   e) Check everything you have done goes through if the assumption that $x^{|G|} = 1$ has a full set of solutions in F is weakened to $x^m = 1$ having a full set of solutions in F, where m is the maximal order of the elements of G. For example, if $G = (\mathbf{Z}/(2))^d$ then $m = 2$ and we can use $F = \mathbf{Z}/(3)$.

6. Dual Homomorphisms

The set $\mathrm{Hom}(G_1, G_2)$ of all homomorphisms from the abelian group G_1 to the abelian group G_2 forms an abelian group under pointwise multiplication

Theorem 6.1. *Let G_1 and G_2 be finite abelian groups. For any homomorphism $f\colon G_1 \to G_2$, set $f^*\colon \widehat{G}_2 \to \widehat{G}_1$ by $f^*(\chi) = \chi \circ f$. Then f^* is a group homomorphism and the map sending f to f^* gives a group isomorphism*

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

Proof. If $f\colon G_1 \to G_2$ 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 $\mathrm{Hom}(G_1, G_2) \to \mathrm{Hom}(\widehat{G}_2, \widehat{G}_1)$ as advertised. Check $(ff')^* = f^*(f')^*$, so $f \mapsto f^*$ is a homomorphism.

Repeating this idea leads to a group homomorphism $\mathrm{Hom}(\widehat{G}_2, \widehat{G}_1) \to \mathrm{Hom}(\widehat{\widehat{G}}_1, \widehat{\widehat{G}}_2)$. By Pontryagin duality it is a homomorphism $\mathrm{Hom}(\widehat{G}_2, \widehat{G}_1) \to \mathrm{Hom}(G_1, G_2)$ and the composite

$$\mathrm{Hom}(G_1, G_2) \to \mathrm{Hom}(\widehat{G}_2, \widehat{G}_1) \to \mathrm{Hom}(G_1, G_2)$$

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

The homomorphism $f^*\colon \widehat{G}_2 \to \widehat{G}_1$ is called the *dual homomorphism* to f.

Exercises.

1. For a homomorphism $f\colon G_1 \to G_2$, show $(\ker f)^\perp = \mathrm{im}\, f^*$ in $\widehat{G}_1$ and $(\mathrm{im}\, f)^\perp = \ker f^*$ in $\widehat{G}_2$.

2. Show the isomorphism $\mathrm{Hom}(G,G) \cong \mathrm{Hom}(\widehat{G},\widehat{G})$ in Theorem 6.1 coming from the identity map on G associates $g \mapsto g^m$ in $\mathrm{Hom}(G,G)$ with $\chi \mapsto \chi^m$ in $\mathrm{Hom}(\widehat{G},\widehat{G})$.

7. Abelian group determinants

Consider a square $n \times n$ matrix where each row is a cyclic shift of the previous row:

$$\begin{pmatrix} X_0 & X_1 & X_2 & \dots & X_{n-1} \\ X_{n-1} & X_0 & X_1 & \dots & X_{n-2} \\ X_{n-2} & X_{n-1} & X_0 & \dots & X_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ X_1 & X_2 & X_3 & \dots & X_0 \end{pmatrix}. \tag{7.1}$$

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

$$\begin{vmatrix} X_0 & X_1 \\ X_1 & X_0 \end{vmatrix} = X_0^2 - X_1^2 \quad \text{and} \quad \begin{vmatrix} X_0 & X_1 & X_2 \\ X_2 & X_0 & X_1 \\ X_1 & X_2 & X_0 \end{vmatrix} = X_0^3 + X_1^3 + X_2^3 - 3X_0X_1X_2.$$

These factor as

$$(X_0 + X_1)(X_0 - X_1) \quad \text{and} \quad (X_0 + X_1 + X_2)(X_0 + \omega X_1 + \omega^2 X_2)(X_0 + \omega^2 X_1 + \omega X_2),$$

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:

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

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

Circulants of order 2 and 3 are products of linear factors with roots of unity as coefficients. Dedekind and Burnside each proved the same property 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 (Dedekind)**.** *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 linear transformation and then find its 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 $L_v \colon V \to V$ 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: 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,

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

If we interchange the roles of χ and $\overline{\chi}$ 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 $\zeta_n=e^{2\pi i/n}$,

$$\begin{aligned}
\begin{vmatrix}
X_0 & X_1 & \dots & X_{n-1}\\
X_{n-1} & X_0 & \dots & X_{n-2}\\
\vdots & \vdots & \ddots & \vdots\\
X_1 & X_2 & \dots & X_0
\end{vmatrix}
&= \prod_{j=0}^{n-1}\left(\sum_{k=0}^{n-1}\zeta_n^{jk}X_k\right)\\
&= \prod_{j=0}^{n-1}(X_0+\zeta_n^jX_1+\cdots+\zeta_n^{(n-1)j}X_{n-1}).
\end{aligned}$$

Applications of the factorization of the group determinant for abelian (not necessarily cyclic) groups can be found in [5, §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 $\chi\colon G \to S^1$.

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 $(\mathbf{Z}/(m))^\times \to (\mathbf{Z}/(d))^\times$ is onto: when $(a, d) = 1$, there is b such that $b \equiv a \bmod d$ and $(b, m) = 1$.*

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

$$b \equiv a \bmod \widetilde{d}, \quad b \equiv 1 \bmod n.$$

Then $b \equiv a \bmod d$ and b is relatively prime to m since it is relatively prime to d (a factor of $\widetilde{d}$) and to n. □

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 $\chi\colon G \to S^1$ 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 $\chi\colon \langle x\rangle \cong \mu_m$. 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 $\ell' \equiv \ell \bmod n/k$ such that $(\ell', n) = 1$. Since $\ell' k \equiv \ell k \bmod n$, $\chi(y^k) = e^{2\pi i\ell' k/n}$. Set $z = e^{2\pi i\ell'/n}$, which has order n. Since $z^k = \chi(y^k)$, we can set $\chi(y) = z$. □

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 $\chi(g) = e^{2\pi ia/m}$ and $\chi(h) = e^{2\pi ib/n}$, 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 $aa' \equiv 1 \bmod m$, $\chi(g^{a'}) = \chi(g)^{a'} = e^{2\pi i aa'/m} = e^{2\pi i/m}$. The argument for $e^{2\pi i/n}$ is similar. Write $mu + nv = (m, n)$ for some integers u and v, so the equation $mn = [m, n](m, n)$ 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 characters, and in particular Parseval's formula, we will give an example of a function of two variables that is provably not a sum of products of functions of one variable.

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

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

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

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

where $f\colon \mathbf{Z}/(N) \to \mathbf{C}$ 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 dual group as in 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 $\mathbf{Z}/(N)$, $\sum_{j=1}^{N}|\widehat{f}(j)|^2 = N\sum_{k=1}^{N}|f(k)|^2 = N\sum_{k=1}^{N}|w_k|^2$. □

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

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

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

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

Then

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

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

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

Now set $x_j = j/N$:

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

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

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). Could there be such a series representation of $e^{2\pi i x k}$ that is 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] P. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, http://arxiv.org/abs/quant-ph/9508027v2.

[4] W. Trappe and L. Washington, "Introduction to Cryptography with Coding Theory," Prentice-Hall, Upper Saddle River, NJ 2002.

[5] L. Washington, "Introduction to Cyclotomic Fields," 2nd ed., Springer-Verlag, New York, 2000.