Part I

Finite Abelian Groups

> It is unfortunate that so many scientists have been conditioned to believe that, say, 10^{30} particles can *always* be well approximated by an infinite number of points.
>
> D. Greenspan [1973]

In this age of computers, it is very natural to replace the continuous with the finite. One thinks nothing about replacing the real line $\mathbb{R}$ with a finite circle (i.e., a finite ring $\mathbb{Z}/n\mathbb{Z}$) and similarly one replaces the real Fourier transform with the fast Fourier transform (FFT). Then computers become happier about our computations. Moreover, the prerequisites for our book become much less formidable than they were for our earlier volumes on harmonic analysis on symmetric spaces (Terras [1985, 1988]). In fact, some (such as Greenspan [1973]) might arguethat, since the universe is finite, it is more appropriate to use finite models than infinite ones. Greenspan decides to "deny the concept of infinity" despite feeling "unmathematical" and "un-American" in doing so. Physicists have also begun considering dynamicalsystems over finite fields (see Nambu [1987]).

Here our goal is to consider finite analogues of the symmetric spaces such as $\mathbb{R}^n$ and the Poincaré upper half plane, which were studied in Terras [1985, 1988]. We will discover finite analogues of all the basic theorems in Fourier analysis, both commutative and noncommutative, including the Poisson summation formula and the Selberg trace formula. One motivation of this study is to develop an understanding of the continuous theory by developing the finite model. Here in finite-land, we will have no worries about convergence of integrals or interchange of summation and integration. Such worries often obscured the continuous theory in a myriad of analytic details.

In fact, finite Fourier "series" are quite analogous to the classical series that Fourier used to analyze periodic functions such as that describing the

temperature on a circular ring. Instead we must think of a finite set of points arranged on a circle and a discrete diffusion process.

It appears that mathematicians actually considered the Fourier transform (DFT) on the finite circle (defined in Chapter 1) before Fourier's work on Fourier series. See Heideman et al. [1984] who discuss the history. They have found that Clairaut considered the discrete Fourier transform in 1754, while Gauss found the fast version (FFT) in 1805 (two years before Fourier's paper and 160 years before Cooley and Tukey [1965]). Clairaut was applying the discrete Fourier transform to the determination of orbits. Gauss applied the DFT to number theory, that is, the quadratic reciprocity law via Gauss sums. Dirichlet also made use of this theory in his proof that there are infinitely many primes in any arithmetic progression.

By the early 1900s certain mathematicians knew how to do Fourier "series" on finite groups (e.g., Frobenius, Schur) and, later, on compact groups and locally compact groups (Cartan, Weyl, Weil, Pontryagin,...). The classical Fourier series are series of sines and cosines (or complex exponentials). In the analogue for a finite group G, the sines and cosines are replaced by the matrix entries of irreducible unitary representations π of G, that is, $\pi : G \to U(n)$ such that $\pi(gh) = \pi(g)\pi(h)$, where $U(n)$ is the group of unitary $n \times n$ matrices. When the group G is abelian, as in Part 1, we have $n = 1$.

Engineers and applied mathematicians (as late as the 1960s) have preferred to develop the subject independently using their own vocabulary, for example, saying "Hadamard transform" instead of Fourier transform on the additive group $(\mathbb{Z}/2\mathbb{Z})^k$ of vectors of 0s and 1s. That this transform has applications or recreations associated with it could come as a surprise to the pure mathematician working on representations of finite groups. For example, Figure I.1 is a picture of a code associated to the Fourier transform on $(\mathbb{Z}/2\mathbb{Z})^5$. This code was used in the transmission of data from the 1969 *Mariner* Mars probe (see Posner's article in Mann [1968] and our discussion of codes below). For the recreational aspects of this transform, see Ball and Coxeter [1987].

I have tried to make this book accessible to nonexperts such as advanced undergraduates, beginning graduate students, and scientists outside of mathematics. The book does mix up subjects that are most often kept in sterile separate compartments – number theory, group theory, graph theory, Fourier analysis, statistics, and coding theory. We have used it in undergraduate and graduate number theory courses at U.C.S.D. The undergraduates found it challenging. Any reader must be willing to do the exercises.

What are the prerequisites? The main one is a familiarity with linear algebra. See, for example, Gilbert [1976], Herstein [1964], or Strang [1976]. You will

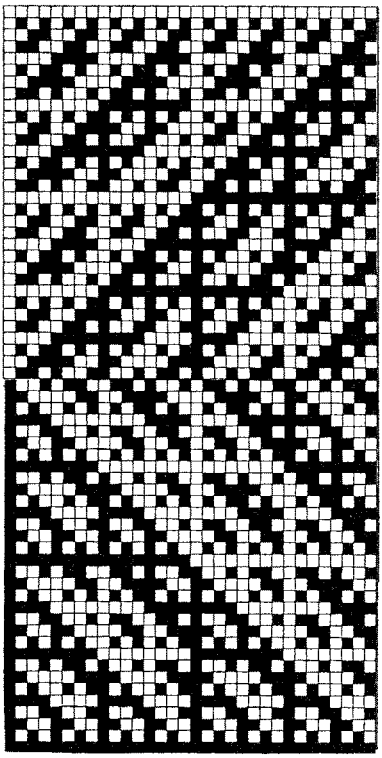

Figure I.1. The (32, 6) biorthogonal Reed–Muller code from Posner's article in Mann [1968, p. 23].

also need to know a tiny bit about finite groups, rings, and fields as in Gallian [1990], Gilbert [1976], and Herstein [1964]. We will give a brief treatment of the necessary number theory (congruences and the finite rings $\mathbb{Z}/n\mathbb{Z}$), but it might help to have a number theory book handy such as Hua [1982], Ireland and Rosen [1982], Rosen [1993], or Stark [1978]. You don't need to know anything about classical Fourier analysis. However, if you would like to compare with standard books on Fourier's world, look at Powers [1993, Chapter 1], Dym and McKean [1964], or Terras [1985, Chapter 1].

I will often make use of the rather costly computer packages Mathematica (see Wolfram [1996]) and Matlab (see MathWorks [1995]) to experiment, draw pictures, etc. If I were to write this book again, I would also use the computational group theory package GAP (see Schönert et al. [1995]) – a free program that can be found by surfing the net. GAP stands for groups, algorithms, and programming.

What sort of applications will we be considering? Here are a few examples:

1. construction of graphs that are good expanders,
2. reciprocity laws in number theory,
3. a study of graph analogues of Kac's question:
   "Can you hear the shape of a drum?" (see Kac [1966]),
4. error-correcting codes,
5. Ehrenfest model of diffusion,
6. switching functions,
7. random walks on graphs, and
8. vibrating systems and chemistry of molecules.

As I began to write this book I was inspired by the books of Diaconis [1988], Lubotzky [1994], and Sarnak [1990]. I also found the following papers inspirational, among others: Arthur [1989], showing an example of the trace formula on finite groups; Brooks [1991] and Buser [1988], giving connections between spectral theory on graphs and Riemannian manifolds; Chung and Sternberg [1992, 1993], on the spectra of buckyballs; and, finally, Lubotzky, Phillips, and Sarnak [1988], giving examples of Ramanujan graphs.

I have attempted to write a "user-friendly" book. To me, this means an abandonment of the style that starts with definition 1.1.1. and ends with corollary 10.66.5. However, I don't mean to say I will abandon proofs. Hardy [1940] notes that "all physicists, and a good many mathematicians, are contemptuous about proof." Then Hardy tells a story about some failures in analytic number theory where it is easy to make wrong guesses and where there are theorems "which have never been proved and which any fool could have guessed." Although finite Fourier analysis does not on the surface appear to be as difficult as analytic number theory, we will also stumble upon some "theorems" like those described by Hardy.

There are still not many books that attempt to do Fourier analysis both on abelian and nonabelian finite groups – with applications. The problem may be that the applied mathematician needs what Jessie MacWilliams calls "the antithesis of classical algebra" [see her coding theory survey article in Mann, 1968]. This means that one may well need explicit matrix entries rather than a coordinate-free approach. MacWilliams went on to write a limerick [see Mann, 1968]:

> Delight in your algebra dressy
> But take heed from a lady named Jessie
> Who spoke to us here
> of her primitive fear
> That good codes just might be messy.

And so it goes with many applications of group representations. Thus we will avoid the methods which Curtis and Reiner [1966] call "the second stage in the development of representation theory." This stage was begun by Emmy Noether in 1929. According to Curtis and Reiner, Noether's approach "resulted in the absorption of the theory into the study of modules over rings and algebras."

Cast of Characters

The definitions below describe most of the characters needed from a basic algebra course. See Dornhoff and Hohn [1978], Dummit and Foote [1991], Gallian [1990], Gilbert [1976], Herstein [1964], Hungerford [1974], Lang [1984, 1987], Strang [1976], or van der Waerden [1991] for more details.

The Abstract

A group G is a set with a binary operation $(\cdot)$ which gives a unique $x \cdot y = xy \in G$ for every $x, y \in G$ such that

- the operation is associative (i.e., $(xy)z = x(yz)$);
- there is an element e (the identity) in G such that $ex = xe = x$ for all $x \in G$;
- for each $x \in G$ there is a $y \in G$ such that $xy = yx = e$.

A homomorphism mapping group G into group H is a function $f : G \to H$ such that for all $x, y \in G$, $f(xy) = f(x)f(y)$.

A set of generators S of a group G means that the smallest subgroup of G containing S is G itself. Write $G = \langle S \rangle$. In the case that S has one element we say that G is cyclic. If G is finite, the number of elements in $\langle a \rangle$, $a \in G$, is the order of a.

The quotient space G/H for a subgroup H of the group G consists of cosets $gH = \{gh | h \in H\}$. It forms a group iff (if and only if) H is a normal subgroup, that is, $Hg = gH$ for all $g \in G$.

A ring R is a set with two binary operations, addition $(+)$ and multiplication $(\cdot)$, such that

- R is a commutative group under $+$ with identity 0;
- multiplication is associative;
- distributive laws hold: $x(y + z) = xy + xz$ and $(x + y)z = xz + yz$, for all $x, y, z \in \mathbb{R}$.

A field F is a ring such that the set of nonzero elements forms a group under multiplication (with 1 as the identity).

A vector space V over a field F is an abelian group under $+$ such that there is an operation of scalar multiplication taking $a \in F$, $v \in V$ to $av \in V$

such that for all $x, y \in V, a, b \in F$:

- $a(x+y) = ax + ay$;
- $(a+b)x = ax + bx$;
- $a(bx) = (ab)x$;
- $1x = x$.

A linear map from vector space V to vector space W is a function $f : V \to W$ such that $f(x+y) = f(x) + f(y)$ and $f(ax) = af(x)$ for all $x, y \in V$ and $a \in F$.

A basis of an n-dimensional vector space V is a set of vectors $v_1, \ldots, v_n \in V$ such that every vector $v \in V$ can be expressed as a linear combination $v = \sum_{j=1}^{n} a_j v_j$, for unique scalars $a_j \in F$.

The matrix of a linear transformation or map $L : V \to V$, where V is an n-dimensional vector space with basis $v_1, \ldots, v_n$, is the $n \times n$ array of scalars $(m_{ij})_{1 \le i,j \le n}$, where

$$Lv_j = \sum_{i=1}^{n} m_{ij} v_i, \quad \text{where } m_{ij} \in F.$$

An eigenvalue of a linear transformation $L : V \to V$ is a scalar $\lambda \in F$ such that $Lx = \lambda x$ for some nonzero vector $x \in V$. And x is called an eigenvector.

A (simple, undirected) graph X is a set of vertices V and edges E connecting pairs of vertices. The edges are undirected and each pair x, y of vertices has at most one edge connecting it. Then we say x and y are adjacent. The degree of a vertex x is the number of edges coming out of that vertex.

The adjacency matrix A of a graph X with n vertices $x_1, \ldots, x_n$ is the $n \times n$ matrix A with entry $a_{ij} = 1$ if vertex i is adjacent to vertex j and $a_{ij} = 0$, otherwise.

The Concrete

$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ = the ring of integers.

$\mathbb{Q} = \{p/q \mid p, q \in \mathbb{Z}, q \neq 0\}$ = the field of rational numbers.

$\mathbb{R}$ = {all decimals} = {limits of Cauchy sequences of rational numbers} = the field of real numbers.

$\mathbb{C} = \{x + iy \mid x, y \in \mathbb{R}\}$ = the field of complex numbers; $i = \sqrt{-1}$.

$\mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$ = the unit circle = the 1-torus.

$\mathbb{F}_q$ = the finite field with $q = p^r$ elements; p = prime.

$K^n = \{v = {}^t(v_1, \ldots, v_n) \mid v_j \in K, \text{ all } j = 1, \ldots, n\}$ = n-dimensional vector space over a field K, vectors v being column vectors and ${}^t v$ denoting transpose of v.

$GL(n, K) = \{g \in K^{n\times n} \mid \det g \neq 0\}$ = the general linear group of all invertible $n \times n$ matrices over the field K.

$\mathbb{Z}/n\mathbb{Z}$ = the finite circle = the quotient group of integers modulo n consisting of equivalence classes of integers where $a, b \in \mathbb{Z}$ are equivalent if n divides $b - a$ and we write $a \equiv b (\text{mod } n)$.

$U(n) = \{g \in GL(n, \mathbb{C}) \mid {}^t\bar{g}g = I\}$ = unitary group, where I = identity matrix and ${}^t\bar{g}$ is the matrix obtained from g by transposing and then replacing each entry by its complex conjugate.

$O(n) = \{g \in GL(n, \mathbb{R}) \mid {}^tgg = I\}$ = orthogonal group.

$K[x]$ = the ring of polynomials with coefficients in a field K.

$K[x]/(g(x))$ = the quotient ring of polynomials modulo $g(x)$.

R^* = the multiplicative group of units in a ring R ($a \in R$ is a unit if $a^{-1} \in R$).

$L^2(X)$ = vector space or Hilbert space of all complex-valued functions on a finite set $X = \{f : X \to \mathbb{C}\}$, considered as a vector space over $\mathbb{C}$ of dimension $|X|$ and inner product

$$\langle f, g\rangle = \sum_{x\in X} f(x)\overline{g(x)}.$$

S_n = the symmetric group of permutations of the set $\{1, 2, 3, \ldots, n\}$.

A_n = the alterating group of even permutations in S_n.

Chapter 1

Congruences and the Quotient Ring of the Integers mod n

> Monitor to Tegan: "Their language is the language of numbers and they have no need to smile."
> Monitor to the Doctor: "Yes, Doctor, you were right. Our numbers were holding the fabric of the universe together."
> Dr. Who in Logopolis

Congruences

In this first section, we review a little elementary number theory. We consider congruences mod n and the ring $\mathbb{Z}/n\mathbb{Z}$. We assume that the reader is familiar with some notions from elementary number theory, for example, divisibility of integers and unique factorization into primes. For more information, see Hua [1982], Ireland and Rosen [1982], Rosen [1993], or Stark [1978]. Some references for algebra are Dornhoff and Hohn [1971], Gallian [1990], Gilbert [1976], and Herstein [1964].

Definition. Suppose that n is a positive integer. Then for any integers a, b we say *a is congruent to b modulo n*, written

$$\begin{aligned} a \equiv b \pmod{n} &\Leftrightarrow n \text{ divides } (a-b) \\ &\Leftrightarrow a - b \in n\mathbb{Z} = \text{the ideal of integer multiples of } n \\ &\Leftrightarrow a \text{ and } b \text{ have the same remainder upon division by } n. \end{aligned} \tag{1}$$

Gauss introduced the congruence notation [in *Disquisitiones Arithmeticae*, 1799]. Consider two integers to be the same if they are congruent modulo n. We will fix n throughout this paragraph. The elements of the quotient ring $\mathbb{Z}/n\mathbb{Z}$ are defined to be the equivalence classes you get upon making this identification. Thus $\mathbb{Z}/n\mathbb{Z}$ is in 1-1 correspondence with the set $\{0, 1, 2, \ldots, n-1\}$. Note

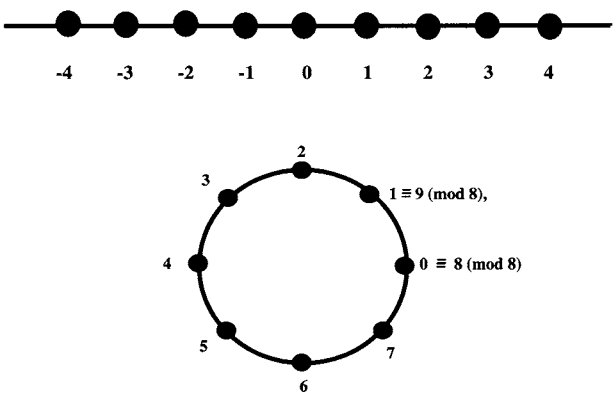

Figure I.2. Rolling up the line of integers into a finite circle.

that here we identify 0 with n. Thus we are taking the integers usually thought of as in a line and rolling that line up into a circle. See Figure I.2.

So we may view $\mathbb{Z}/n\mathbb{Z}$ as the finite circle. Note that we can use other sets of representatives for $\mathbb{Z}/n\mathbb{Z}$ (e.g., $\{1, 2, \ldots, n\}$). In fact we can replace any number j by $j + an$ for some $a \in \mathbb{Z}$.

Define addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$ by using $+$ and $\times$ in $\mathbb{Z}$ and then taking the remainder of the result upon division by n. Since $\mathbb{Z}/n\mathbb{Z}$ is finite, it is easy to write tables for addition and multiplication. The entry in the ith row and jth column stands for $i + j \pmod 7$ in the addition table (Table I.1) and $i * j \pmod 7$ in the multiplication table (Table I.2).

Exercise. Complete Tables I.1 and I.2. Then the tables for $\mathbb{Z}/12\mathbb{Z}$.

Clearly the addition tables are pretty predictable. Each row is obtained from the one above it by moving everything over 1 and then moving the stuff hanging out at the end back to the beginning.

Table I.1. *Addition mod 7*

+ mod 7	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3					0		
4				0			
5			0				
6		0					

Table I.2. *Multiplication mod 7*

$*$ mod 7	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3			5		
4	0	4		5			
5	0	5	3				
6	0	6					

It is not hard to see that $\mathbb{Z}/n\mathbb{Z}$ forms a commutative group under addition. It is closed under $+$ and $-$, contains 0, and $+$ is associative and commutative. In fact, it is a cyclic group generated by 1, since any element $a \pmod n$ is a sum of a ones.

Moreover, there is a way to visualize this additive group $G = \mathbb{Z}/n\mathbb{Z}$ as the *Cayley graph* obtained as follows. Let $S = \{1, -1 \pmod n\}$. This is a set of generators of G. Take the vertices of the graph to be the elements of G. Draw an edge between two vertices v and w if $w \equiv v + s \pmod n$, $s \equiv \pm 1 \pmod n$. For $n = 8$, we get the graph shown in Fig. I.3, which is just the finite circle graph.

Cayley graphs should actually be directed graphs having edges labeled with the appropriate generator of the group. Since we are taking a symmetric set S of generators of G (i.e., $s \in S$ implies $-s \in S$), we will leave off the directions and draw only one edge between each pair of vertices. We will say more about Cayley graphs in Chapter 3 and elsewhere. References for Cayley graphs are Biggs [1974], Bollobás [1979], and Gallian [1990]. There are connections with finite-state machines or automata [see Dornhoff and Hohn, 1978].

The main application of congruences that we will consider is to Fourier analysis. Replace the real line $\mathbb{R}$ or the circle $\mathbb{T} \cong \mathbb{R}/\mathbb{Z}$ with the finite circle.

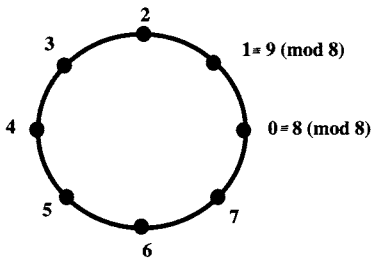

Figure I.3. Cayley graph for additive group $\mathbb{Z}/8\mathbb{Z}$ with generating set $S = \{\pm 1 \pmod 8\}$.