

HARMONIC ANALYSIS ON FINITE ABELIAN GROUPS

PAUL H. KOESTER

ABSTRACT. We give a discussion of harmonic analysis on finite abelian groups, emphasizing various ways in which the structure of the group is encoded on various spaces of functions, ways in which the Fourier transform detects and preserves these structures. We discuss the major tools, like convolutions and Fourier transforms, along with some fundamental theorems, like the Plancherel, Parseval, Fourier inversion, and Poisson summation formulas, and fundamental heuristic principles, like the uncertainty principle. We originally intended to cover some applications of Fourier analysis on finite abelian groups to number theory, and to cover the Fast Fourier transform, but did not get a chance to include these yet.

1. INTRODUCTION

We feel the setting of a finite abelian group is the best place to begin a study of harmonic analysis. One often begins with one of the three classical groups, \mathbb{T} , \mathbb{Z} , or \mathbb{R} . However, it is necessary to burden oneself with many technicalities. A seemingly obvious formula may only be valid for functions satisfying an appropriate integrability or smoothness condition, or the formula may hold as an equality only interpreted in various weak senses, such as convergence in a certain norm, or in measure, or almost everywhere, or in a weak- $*$ sense, or interpreted in terms of measures, distributions, or tempered distributions. Even seemingly simple formulae involving integrals are more complicated than first sight indicates. Harmonic analysis *requires* Lebesgue integration¹, as many theorems are false if integrals are confined to Riemann integrals.

The setting of finite abelian groups avoids many technicalities associated with convergence and measure theory which appear in the setting of *locally compact abelian groups* which are not necessarily finite. In particular, measures, functions, and distributions all coincide, Fubini is always valid, and all of the L^p spaces, as well as other natural normed spaces, coincide as vector spaces. Also, we need not worry about abstract results on existence and uniqueness of Haar measures. A different set of technicalities are avoided which appear in the setting of *finite groups* which are not necessarily abelian. A certain amount of machinery from *representation theory* is needed in the nonabelian setting, but is trivialized by the fact that all representations are 1-dimensional in the abelian setting.

Aside from avoiding technicalities from the general case, harmonic analysis on finite abelian groups is interesting in its own right. First, some of the most significant features of harmonic analysis on more general groups already surface in the finite abelian setting. Second, many of the important applications of harmonic analysis to number theory and combinatorics involve finite abelian groups. Third, finite abelian groups, particularly the cyclic groups, provide discretizations of more classical groups, like \mathbb{T} , \mathbb{Z} , and \mathbb{R} . Many computations are then done on finite models of these groups.

The finite abelian setting does have a few drawbacks. First, there is no notion of differentiability in this setting. Some of the most important reasons why harmonic analysis is useful is its connection with differentiation. The Fourier transform has the affect of diagonalizing many important partial differential operators. Second, the connections between harmonic analysis and function theory, via Hardy spaces don't appear to have finite analogues. Third, the finite abelian setting may lead the reader to expect *self-duality*, which in fact fails in general but holds for all

Date: January 2, 2006.

¹In fact, a case can be made for studying some of the basic properties of harmonic analysis on these infinite groups using Riemann integrals, realize the shortcomings of these integrals, and then introduce Lebesgue integration to fix these shortcomings. [3].

finite abelian groups. Thus, it is not always apparent which phenomena are occurring on the *physical side* and which are on the *Fourier side*. We will go to pains to avoid carelessly identify a group and its dual, as well as distinguish between certain Lebesgue spaces, even though they all coincide in the finite setting. Fourth, special groups like \mathbb{R}^n have a very rich harmonic analysis due to the fact that many groups are represented on \mathbb{R}^n . In particular various groups of rotations and dilations are represented on \mathbb{R}^n , and thus appear in the harmonic analysis of \mathbb{R}^n . See [4]. We don't know of a finite abelian group which possesses as rich of a structure as \mathbb{R}^n .

We take as our basic definition of harmonic analysis on the group G to be *the study of complex valued functions defined on G , and the ways the group structure of G can be seen from these functions.*

2. HARMONIC ANALYSIS OF $\mathbb{Z}/N\mathbb{Z}$

In this section we give a cursory study of harmonic analysis limited to functions defined on a finite *cyclic* group. Our model for the cyclic group of order N will be the group of residues of \mathbb{Z} modulo N . Thus, we denote $\mathbb{Z}/N\mathbb{Z}$ additively, the identity element is denote as 0, and we denote the canonical generator of $\mathbb{Z}/N\mathbb{Z}$ by 1.

We will be most interested in $\mathfrak{X}(\mathbb{Z}/N\mathbb{Z})$, the vector space of all complex valued functions on $\mathbb{Z}/N\mathbb{Z}$. Let $\omega = e^{2\pi i/N}$. The set of functions

$$(1) \quad \{x \mapsto \omega^{rx}\}_{r \in \mathbb{Z}/N\mathbb{Z}}$$

will play a special role. Let $f \in \mathfrak{X}(\mathbb{Z}/N\mathbb{Z})$ and $r \in \mathbb{Z}/N\mathbb{Z}$. Then we define the r^{th} *Fourier coefficient* of f by

$$\hat{f}(r) = \frac{1}{N} \sum_{x \in \mathbb{Z}/N\mathbb{Z}} f(x) \omega^{-rx},$$

and the *Fourier inversion formula* is given by

$$f(x) = \sum_{r \in \mathbb{Z}/N\mathbb{Z}} \hat{f}(r) \omega^{rx}.$$

The inversion formula is a simple consequence of

$$\frac{1}{N} \sum_{x \in \mathbb{Z}/N\mathbb{Z}} \omega^{rx} = \begin{cases} 1; & \text{if } r = 0, \\ 0; & \text{else.} \end{cases}$$

Important relations involving various norms include *the Hausdorff-Young inequality*

$$\sum_{r \in \mathbb{Z}/N\mathbb{Z}} |\hat{f}(r)|^q \leq \frac{1}{N} \sum_{x \in \mathbb{Z}/N\mathbb{Z}} |f(x)|^p$$

for $1 \leq p \leq 2$ and $\frac{1}{p} + \frac{1}{q} = 1$, and *the Plancheral formula*

$$\sum_{r \in \mathbb{Z}/N\mathbb{Z}} |\hat{f}(r)|^2 = \frac{1}{N} \sum_{x \in \mathbb{Z}/N\mathbb{Z}} |f(x)|^2,$$

which is a special case of *Parseval's identity*

$$\sum_{r \in \mathbb{Z}/N\mathbb{Z}} \hat{f}(r) \overline{\hat{g}(r)} = \frac{1}{N} \sum_{x \in \mathbb{Z}/N\mathbb{Z}} f(x) \overline{g(x)}.$$

Given functions f and g we may form their *convolution product*

$$f * g(x) = \frac{1}{N} \sum_{y \in \mathbb{Z}/N\mathbb{Z}} f(y) g(x - y).$$

One has

$$\widehat{f * g} = \hat{f} \hat{g}.$$

Finally, we define two operations on functions. Given $y \in \mathbb{Z}/N\mathbb{Z}$ we define *translation by y* ,

$$T_y f(x) = f(x - y).$$

Given $r \in \mathbb{Z}/N\mathbb{Z}$ we define *modulation by r* ,

$$M_r f(x) = \omega^{rx} f(x).$$

Quick computations show

$$\widehat{T_y f} = M_{-y} \hat{f}$$

and

$$\widehat{M_y f} = T_y \hat{f}.$$

3. GENERAL FINITE ABELIAN GROUPS

We now study harmonic analysis on arbitrary finite abelian groups. We will make a more careful study now, in particular, focusing on what mechanisms are at work in various formulas and theorems. We will denote our group operations on G multiplicatively. The main object of interest is the vector space of all functions from G into \mathbb{C} . We will consider various norms on this space of functions. Due to the finite dimensionality all norms will be equivalent, and in particular $L^1(G) = L^2(G) = L^\infty(G)$. However, certain operations on functions will be associated with structures more correctly associated with one of these spaces than the others², and we may then designate which structure is being exploited by which notation we use for the space of functions. If we are only using the vector space structure we will simply refer to this space as $\mathfrak{X}(G)$.

4. THE DUAL GROUP

The exponential functions (1) played an important role in the analysis of $\mathbb{Z}/N\mathbb{Z}$. Let us pause a second to try to understand their importance. Given $r \in \mathbb{Z}/N\mathbb{Z}$ let us denote the mapping $x \mapsto \omega^{rx}$ by ε_r . Now we observe that

$$\omega^{r(x+y)} = \omega^{rx} \omega^{ry},$$

and so for each r , the mapping ε_r is a group homomorphism from $\mathbb{Z}/N\mathbb{Z}$ into \mathbb{C} , and in fact, the range of this homomorphism is contained in \mathbb{T} . Symmetrically, we have

$$\omega^{(r+s)x} = \omega^{rx} \omega^{sx},$$

which gives that

$$\varepsilon_{r+s} = \varepsilon_r \varepsilon_s.$$

Thus, the association $r \mapsto \varepsilon_r$ is a homomorphism of $\mathbb{Z}/N\mathbb{Z}$ into the group of homomorphisms from $\mathbb{Z}/N\mathbb{Z}$ into \mathbb{T} . Furthermore, suppose $\chi : \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{T}$ is a group homomorphism. Then

$$1 = \chi(0) = \chi(N) = \chi(1)^N,$$

so $\chi(1)$ must be some N^{th} root of unity ω^r , from which it follows that $\chi = \varepsilon_r$.

Given a finite abelian group G , we need to find functions on G which are analogous to the exponentials (1). Thus, we define the *dual group*, or *character group*,

$$\widehat{G} = \{\chi : G \rightarrow \mathbb{T} : \chi \text{ is a group homomorphism}\}.$$

By a *character of G* , we mean a group homomorphism of G into \mathbb{T} . The set of all characters has the structure of an abelian group under pointwise multiplication of characters. Notice \widehat{G} is a subset $\mathfrak{X}(G)$, and thus we have a way of somehow encoding the group structure of G into the $\mathfrak{X}(G)$, via \widehat{G} . The fundamental principle of harmonic analysis is then that *everything* about the space of all complex valued functions on G can be understood from \widehat{G} . In our finite

² L^1 has a group algebra structure, L^2 a Hilbert space structure, L^∞ a C^* -algebra structure

dimensional setting this principle is particularly clean, for we will see that \widehat{G} gives a basis for $\mathfrak{X}(G)$. The Fourier transform is nothing more than the corresponding change of basis operator, intermediating between the standard basis of Kronecker delta functions, and the basis of characters.

4.1. The Dual of $\mathbb{Z}/N\mathbb{Z}$. The simplest dual group to compute is for the finite cyclic groups $\mathbb{Z}/N\mathbb{Z}$. In fact, we already computed the dual group above. We have

$$\widehat{\mathbb{Z}/N\mathbb{Z}} = \{\varepsilon_r\}_{r \in \mathbb{Z}/N\mathbb{Z}} \cong \mathbb{Z}/N\mathbb{Z},$$

and in particular

$$(2) \quad \widehat{\mathbb{Z}/N\mathbb{Z}} \cong \mathbb{Z}N.$$

Note, however, that this isomorphism is not canonical, as it depends on the choice of a particular primitive N^{th} root of unity.

4.2. From Old Duals to New. Given an abelian group G we may form its dual group. The process of forming dual groups behaves nicely with respect to direct sums, subgroups, and quotient groups.

First, let G_1 and G_2 be two finite abelian groups. We claim

$$(3) \quad \widehat{G_1 \oplus G_2} = \widehat{G_1} \oplus \widehat{G_2}.$$

This is easy to see. Given $\chi_1 \in \widehat{G_1}$ and $\chi_2 \in \widehat{G_2}$, we form a character $\chi \in \widehat{G_1 \oplus G_2}$ by

$$(4) \quad \chi : G_1 \oplus G_2 \rightarrow \mathbb{T}; \quad \chi(x, y) = \chi_1(x)\chi_2(y).$$

Likewise, given $\chi \in \widehat{G_1 \oplus G_2}$, we have

$$(5) \quad \chi(\cdot, 1) \in \widehat{G_1} \quad \text{and} \quad \chi(1, \cdot) \in \widehat{G_2}.$$

Thus, the dual preserves direct sums. Coupling (3) with the *fundamental theorem of finite abelian groups* shows that it is sufficient to study finite cyclic groups. We will, however, adopt a point of view which handles general finite abelian groups. One nice consequence of (3) and (2) is the self-duality of finite abelian groups,

$$(6) \quad \widehat{G} \cong G.$$

We do not know of a direct proof of this fact.

Next, let H be a subgroup of G . Certainly, each character of G restricts to a character on H . A bit more effort shows each character on H extends to a character on G . By induction on the index of H in G it suffices to show that if $\chi \in \widehat{H}$ and $x \in G \setminus H$, then χ extends to a character, call it φ , on the subgroup generated by H and x . Now, $x^{|G|} = 1 \in H$ so we let m be the smallest positive integer so that $x^m \in H$. By necessity,

$$\varphi(x)^m = \varphi(x^m) = \chi(x^m)$$

and $\chi(x^m)$ is a primitive n^{th} root of unity for some $n \mid |H|$. Thus, we may set $\varphi(x)$ to be a primitive mn^{th} root of unity. This gives a correspondence between duals of subgroups of G and subgroups of \widehat{G} . Thus, the dual preserves subgroups.

Finally, let H be a subgroup of G , and let

$$(7) \quad \widehat{G}^H = \{\chi \in \widehat{G} : \chi(xh^{-1}) = \chi(x) \text{ for all } h \in H, x \in G\}.$$

Then

$$(8) \quad \widehat{G/H} \cong \widehat{G}^H \cong \widehat{G}/\widehat{H},$$

and so there is a correspondence between duals of quotient groups of G and quotient groups of \widehat{G} .

4.3. The Double Dual. Given an abelian group G we may form its dual group \widehat{G} . The dual group is again an abelian group so we may take the dual of the dual group. The terminology of dual groups already suggests that the group of characters of the group of characters on G should just be G . Thus, given $y \in G$ we need to see how y can be interpreted as a homomorphism on \widehat{G} . The reader familiar with *double dual* arguments from linear algebra will then recognize that this is accomplished by defining

$$(9) \quad y(\chi) := \chi(y),$$

and helps show

$$(10) \quad \widehat{\widehat{G}} \cong G.$$

The equation (9) shows that G is naturally a subgroup of $\widehat{\widehat{G}}$. Above, we alluded to the fact that \widehat{G} is a basis for the $|G|$ -dimensional vector space $\mathfrak{X}(G)$, which then shows

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

Iterating this equality a second time shows that G must be all of the double dual. Of course, the double duality (10) follows from self duality (6), but double duality is canonical, whereas self duality requires one to make arbitrary choices. Furthermore, double duality holds in generality, whereas infinite groups need not be isomorphic to their dual groups.³

4.4. Functoriality of Dual Groups. The operation of forming a dual group starts with a finite abelian group and outputs another finite abelian group. The above shows that this process respects the natural constructions associated with finite abelian groups. This construction also preserves group homomorphisms between groups. That is, suppose we have finite abelian groups G and H and a group homomorphism $\psi : G \rightarrow H$. Given a character $\chi \in \widehat{H}$, define

$$\Psi(\chi) = \chi \circ \psi.$$

For each χ , $\Psi(\chi)$ is a character on G and in fact $\Psi : \widehat{H} \rightarrow \widehat{G}$ is a group homomorphism. Thus, the operation of forming dual groups is in fact a contravariant functor from the category of finite abelian groups with group homomorphisms to itself. (The reader familiar with category theory will notice that forming dual groups is a special case of the hom functor.) We will never have occasion to make use of this functoriality, and include it only for completeness.

5. HAAR MEASURE

G possesses a natural measure which interacts with its group structure, namely its *Haar measure*⁴. In this finite setting we may specify exactly (almost) what this measure is. First, the σ -algebra we use on G is the power set of G , i.e., all subsets of G will be measurable. A measure in this setting is then a nonnegative valued function μ whose domain is the set of all subsets of G and μ is additive, in the sense that if $\{A_j\}$ is a collection of disjoint subsets of G , then

$$(11) \quad \mu\left(\bigcup_j A_j\right) = \sum_j \mu(A_j).$$

In fact, each function on G gives rise to a measure by defining

$$\mu(\{x\}) := \mu(x)$$

³The Pontryagin duality theorem asserts that discrete groups always have compact duals and vice versa, so in fact says that groups that are infinite and either compact or discrete are *never* self dual.

⁴It is theorem that any locally compact group possesses a (left) Haar measure, and this Haar measure is unique up to scaling. This existence and uniqueness is easy in our finite case.

and extending by (11), and likewise each measure on G defines a function on G . A *Haar measure* on a group is a measure which is invariant by the action of the group. Since functions and measure coincide in our setting, this simply requires μ to satisfy

$$(12) \quad \mu(x) = \mu(xy^{-1})$$

for all x and $y \in G$. Thus, this requires μ to be a constant function on G , and so once we chose the value of this constant, the Haar measure is unique.

Let G be a finite abelian group and μ a Haar measure on G , which as we just saw is nothing more than a nonnegative constant. We wish to specify now certain structures on various L^p spaces. First, we define the p -norm on G with respect to μ by

$$\|f\|_{L^p(G;\mu)}^p = \int_G |f(x)|^p d\mu = \sum_{x \in G} |f(x)|^p \mu$$

for $1 \leq p < \infty$ and

$$\|f\|_{L^\infty(G;\mu)} = \max_{x \in G} |f(x)|.$$

The three special cases correspond to $p = 1, 2, \infty$.

Many theorems in Fourier analysis assert that some integral on G is related to some integral on \widehat{G} , where the integrals are with respect to Haar measures. These formulas may often appear particularly nice if the normalizations on the Haar measures on G and \widehat{G} are chosen *properly*. In the finite setting there are two particularly natural normalizations of the Haar measure. In the first, *counting measure*, each element of G receives a value of 1. In the second, *normalized counting measure*, each element of G receives a value of $\frac{1}{|G|}$, so that G has total mass 1. We find it useful to make use of both of these measures, and to consider L^p norms with respect to both of these measures, and thus adopt the following conventions:

$$\|f\|_{L^p(G)}^p = \frac{1}{|G|} \sum_{x \in G} |f(x)|^p$$

and

$$\|f\|_{\ell^p(G)}^p = \sum_{x \in G} |f(x)|^p.$$

That is, $\ell^p(G)$ is the L^p space with respect to *counting measure*, and $L^p(G)$ is the L^p space with respect to *normalized counting measure*. We will distinguish between the corresponding *inner products* on the L^2 spaces via subscripting:

$$\langle f, g \rangle_{L^2(G)} = \frac{1}{|G|} \sum_{x \in G} f(x) \overline{g(x)}$$

and

$$\langle f, g \rangle_{\ell^2(G)} = \sum_{x \in G} f(x) \overline{g(x)}.$$

While working with the normalized counting measure we may find it useful to use terminology from probability theory. Thus,

$$\mathbb{E}(f) = \frac{1}{N} \sum_{x \in \mathbb{Z}/N\mathbb{Z}} f(x)$$

and

$$\mathbb{P}(A) = \frac{|A|}{N}$$

where $A \subset \mathbb{Z}/N\mathbb{Z}$.

We will chose to *not* specify a particular normalization. The reader may want to pin down a particular normalization, in case we suggest equipping G with normalized counting measure. It then becomes natural to equip \widehat{G} with counting measure.

6. STRUCTURES ON $\mathfrak{X}(G)$.

6.1. General Structures. The space of all complex valued functions on G possesses two *involutions*. Recall an involution is an operator which is self invertible, i.e., $T \circ T = I$. The first is *complex conjugation*, and in fact does not involve the group structure of G :

$$(13) \quad \mathcal{C}f(x) = \overline{f(x)}.$$

Certainly \mathcal{C} is an involution. The other involution is *reflection*, denoted by \mathcal{R} .

$$(14) \quad \mathcal{R}f(x) = f(x^{-1}).$$

Again, this is an involution. Reflection does utilize the group structure of G .

6.2. $L^2(G; \mu)$; A Hilbert Space. $L^2(G; \mu)$ possesses the additional structure of a *Hilbert space*, which allows us to introduce notions of orthogonality. Recall that a Hilbert space is a complete normed space whose norm is derived from an inner product. The finite nature of our setting automatically guarantees all norms are complete. The inner product is defined by

$$\langle f, g \rangle_{L^2(G; \mu)} = \sum_{x \in G} f(x) \overline{g(x)} \mu.$$

The Hilbert space structure is naturally tied to $L^2(G; \mu)$ because of

$$\|f\|_{L^2(G; \mu)}^2 = \langle f, f \rangle_{L^2(G; \mu)}$$

and *the Cauchy-Schwarz inequality*

$$(15) \quad |\langle f, g \rangle_{L^2(G; \mu)}| \leq \|f\|_{L^2(G; \mu)} \|g\|_{L^2(G; \mu)}.$$

The Hilbert space structure does not utilize the group structure.

6.3. $L^\infty(G; \mu)$; A C^* -algebra. $L^\infty(G, \mu)$ possesses the additional structure of a C^* -algebra. This means $L^\infty(G, \mu)$ is equipped with an algebraic product, an involution, and the product, involution, and norm satisfy certain relations. The product is that of *pointwise multiplication*,

$$(16) \quad fg(x) = f(x)g(x).$$

This product is associative, commutative, and distributive over the vector space operations. The function identically 1 is the multiplicative identity. A function is invertible if and only if the function never vanishes. The involution is complex conjugation, (13). The C^* -algebra relations, which in particular link this product structure to $L^\infty(G; \mu)$ are

$$\|fg\|_{L^\infty(G; \mu)} \leq \|f\|_{L^\infty(G; \mu)} \|g\|_{L^\infty(G; \mu)}$$

and

$$\|f\mathcal{C}f\|_{L^\infty(G; \mu)} = \|f\|_{L^\infty(G; \mu)}^2.$$

The C^* -algebra structure does not utilize the group structure either. Nor does the particular choice of measure matter here.

6.4. $L^1(G; \mu)$; **A Group Algebra.** $L^1(G; \mu)$ possesses the additional structure of a *group algebra*. This means that $L^1(G; \mu)$ possesses an algebraic product, called *convolution*. Here the group structure is essential. The convolution product is defined by averaging one function against shifts of another function,

$$(17) \quad f * g(x) = \sum_{x \in G} f(y)g(xy^{-1})\mu.$$

This product is associative, commutative, and distributes over the vector space operations. The function

$$(18) \quad \delta(x) = \begin{cases} \frac{1}{\mu}; & \text{if } x = 1, \\ 0; & \text{if } x \neq 1, \end{cases}$$

is the convolution identity. The group algebra structure is naturally associated to $L^1(G; \mu)$ by

$$\|f * f\|_{L^1(G; \mu)} = \|f\|_{L^1(G; \mu)}^2$$

and *Young's inequality*

$$(19) \quad \|f * g\|_{L^1(G; \mu)} \leq \|f\|_{L^1(G; \mu)} \|g\|_{L^1(G; \mu)}.$$

7. SOME REPRESENTATIONS

Recall that a (unitary) representation of a group G on a *Hilbert space* \mathcal{H} is a group homomorphism of G into the space of *unitary operators* on \mathcal{H} . Equivalently, it is a mapping

$$\varphi : \mathcal{H} \times G \rightarrow \mathcal{H} \quad \varphi : (h, x) \mapsto \phi_x(h)$$

where $\phi_x : \mathcal{H} \rightarrow \mathcal{H}$ is unitary, and

$$\phi_{xy} = \phi_x \circ \phi_y.$$

We have already seen, though we did not use the language of representation theory, that $\mathbb{Z}/2\mathbb{Z}$ is represented on $L^2(G; \mu)$ in two different ways, through the involutions (13) and (14). We can also naturally represent both G and \widehat{G} on $L^2(G; \mu)$.

7.1. **Representation of G on $L^2(G; \mu)$; Translations.** Given a group G , we always have the *regular representation* of G on $L^2(G; \mu)$, which is given in terms of *translation operators*. We define the *translation operators* on $L^2(G; \mu)$ by

$$(20) \quad T_y f(x) = f(xy^{-1})$$

where $y \in G$. T_y is a unitary operator on $L^2(G; \mu)$ and our *regular representation* of G on $L^2(G; \mu)$ is then given by

$$(21) \quad \tau : L^2(G; \mu) \times G \rightarrow L^2(G; \mu); \quad \tau(f, y) = T_y f.$$

7.2. **Representation of \widehat{G} on $L^2(G; \mu)$; Modulations.** We can also represent the dual group \widehat{G} on $L^2(G; \mu)$. This representation is given in terms of the *modulation operators*. We define the *modulation operators* on $L^2(G; \mu)$ by

$$(22) \quad M_\chi f(x) = \chi(x)f(x)$$

where $\chi \in \widehat{G}$. M_χ is a unitary operator on $L^2(G; \mu)$ and our *dual representation* of \widehat{G} on $L^2(G; \mu)$ is then given by

$$(23) \quad \rho : L^2(G; \mu) \times G \rightarrow L^2(G; \mu); \quad \rho(f, \chi) = M_\chi f.$$

7.3. **A Commutation Relation.** The above shows that we have two groups of unitary operators acting on $L^2(G; \mu)$, the translations and the modulations. These two actions do not quite commute with each other. Let $y \in G$ and $\chi \in \widehat{G}$. We find that

$$(T_y \circ M_\chi - M_\chi \circ T_y)f(x) = \overline{(\chi(y) - 1)}\chi(x)f(xy^{-1}) = \overline{(\chi(y) - 1)}M_\chi \circ T_y f(x).$$

8. SUBSPACES OF $\mathfrak{X}(G)$.

The space of all functions on G is a $|G|$ -dimensional \mathbb{C} -vector space, and in particular possesses subspaces. Here we discuss some of the more natural subspaces.

8.1. Subspaces of Localized Functions. Let Ω be any *subset* of G . The set of all functions on G which vanish off of Ω , $\mathfrak{X}(\Omega)$, forms a subspace of the set of all functions on G . In fact, we get a direct sum decomposition

$$\mathfrak{X}(G) = \mathfrak{X}(\Omega) \oplus \mathfrak{X}(G \setminus \Omega),$$

and an orthogonal decomposition of $L^2(G; \mu)$;

$$L^2(G; \mu) = L^2(\Omega; \mu|_{\Omega}) \oplus L^2(G \setminus \Omega; \mu|_{G \setminus \Omega}).$$

These subspaces are exactly the ideals under the multiplication algebra $L^\infty(G; \mu)$, and so the ideal structure of the C^* -algebra $L^\infty(G; \mu)$ is imprinted $\mathfrak{X}(G)$. Taking Ω to be a singleton gives rise to the standard basis of $\mathfrak{X}(G)$.

8.2. Subspaces of Periodic Functions. Let H be a *subgroup* of G . The set of functions invariant under H ,

$$\{f : G \rightarrow \mathbb{C} : T_y f = f \text{ for all } y \in H\},$$

defines a subspace of $\mathfrak{X}(G)$, and is in fact isomorphic to $\mathfrak{X}(G/H)$, the space of functions defined on the quotient group G/H . Thus, the subgroup structure of G is imprinted on $\mathfrak{X}(G)$. Functions invariant under a subgroup H will be referred to as H -periodic functions.

8.3. Subspaces of "Dually Periodic Functions". The previous family of subspaces arose from invariant subspaces under the regular representation. We may just as easily work with invariant subspaces for the modulation operators, though an explicit description of these spaces is not clear yet. To that affect, let Γ be a subgroup of \widehat{G} and consider the subspace of functions

$$\{f : G \rightarrow \mathbb{C} : M_\chi f = f \text{ for all } \chi \in \Gamma\}.$$

Thus, the subgroup structure of \widehat{G} is imprinted on $\mathfrak{X}(G)$.

8.4. Subspaces of "Band-Limited Functions". We don't have an explicit description of the ideals of the convolution algebra $L^1(G; \mu)$, but taking our cue from the spaces of localized functions, we see that these ideals also give rise to subspaces of $\mathfrak{X}(G)$ and should also be important. In the classical setting of analysis on \mathbb{R} one refers to such functions as being "band-limited".

9. THE FOURIER TRANSFORM

Above, we asserted that \widehat{G} gives a basis for $\mathfrak{X}(G)$ and that the Fourier transform is the change of basis operator from the standard basis to the basis of characters. We now wish to make this all precise.

9.1. Orthogonality of Characters. Suppose χ is a *non-trivial character*, meaning that χ is not the identity character. Therefore, there is some group element $y \in G$ so that $\chi(y) \neq 1$. Then

$$\begin{aligned} \langle 1, \chi \rangle_{L^2(G; \mu)} &= \frac{1}{\mu(G)} \sum_{x \in G} \overline{\chi(x)} = \frac{1}{\mu(G)} \sum_{x \in G} \overline{\chi(xy)} \\ &= \overline{\chi(y)} \frac{1}{\mu(G)} \sum_{x \in G} \overline{\chi(x)} = \overline{\chi(y)} \langle 1, \chi \rangle_{L^2(G; \mu)}, \end{aligned}$$

and so

$$\overline{(1 - \chi(y))} \langle 1, \chi \rangle_{L^2(G; \mu)} = 0.$$

Since $\chi(y) \neq 1$ it follows that

$$\langle 1, \chi \rangle_{L^2(G; \mu)} = 0.$$

Thus, we derive the *orthogonality of characters*;

$$(24) \quad \langle \varphi, \chi \rangle_{L^2(G; \mu)} = \begin{cases} 0; & \text{if } \varphi \neq \chi, \\ |G| \mu; & \text{if } \varphi = \chi. \end{cases}$$

In particular, using normalized counting measure the characters form an orthonormal subset of $L^2(G)$, and so

$$|\widehat{G}| \leq |G|.$$

Dually, we find that $\widehat{\widehat{G}}$ forms an orthogonal subset of $L^2(\widehat{G}; \mu)$ and so

$$|\widehat{\widehat{G}}| \leq |\widehat{G}|,$$

and so

$$|\widehat{\widehat{G}}| \leq |G|.$$

Coupled with the fact that G is a subgroup of $\widehat{\widehat{G}}$, via (9), we get the *double duality* relation (10). Our immediate interest in this is that it gives us

$$|G| = |\widehat{\widehat{G}}|,$$

and so $\widehat{\widehat{G}}$ gives us an orthogonal basis of $L^2(G; \mu)$.

9.2. Fourier Inversion. We define the Fourier coefficient of f with respect to the character χ by

$$(25) \quad \hat{f}(\chi) = \langle f, \chi \rangle_{L^2(G; \mu)} = \sum_{x \in G} f(x) \overline{\chi(x)} \mu.$$

From the orthogonality of characters, (24), we get

$$(26) \quad f(x) = \frac{1}{|G| \mu} \sum_{\chi \in \widehat{G}} \hat{f}(\chi) \chi(x).$$

Formula (26) is the *Fourier inversion formula*, which gives a recipe for reconstructing f from its *Fourier coefficients*.

Observe the meaning of $\hat{f}(\chi)$. f is a function defined on a group and we know that f is a superposition of basic group homomorphisms. So $\hat{f}(\chi)$ then tells us how much f resembles the particular homomorphism χ .

9.3. The Fourier Transform and L^2 : Parseval and Plancherel. We will see that the passing from a function to its Fourier coefficients preserves not only the vector space structure of functions on G , but also the Hilbert space structure. First, we deal with some technicalities involving the particular choice of Haar measure we use.

Our definition of the Fourier coefficients is dependent upon the particular normalization of the Haar measure on G . Let us fix Haar measures on G and \widehat{G} , assuming the chosen Haar measure is constantly ν . A straightforward calculation using (24) gives us the *Plancherel formula*

$$(27) \quad \|f\|_{L^2(G; \mu)}^2 = |G| \mu \nu \|\hat{f}\|_{L^2(\widehat{G}; \nu)}$$

and the *Parseval formula*

$$(28) \quad \langle f, g \rangle_{L^2(G; \mu)} = |G| \mu \nu \langle \hat{f}, \hat{g} \rangle_{L^2(\widehat{G}; \nu)}.$$

Now, given a group G there is no best choice for how to normalize its Haar measure, and we don't want to pin down any one choice as being superior to another. However, (27) and (28) suggest that once we have chosen a particular normalization for G then there is a best choice of normalization for the Haar measure on \widehat{G} , namely

$$(29) \quad \nu = \frac{1}{|G| \mu}.$$

We will always assume then that the dual group is equipped with Haar measure with this normalization. With this normalization we get normalized versions of Plancherel

$$(30) \quad \|f\|_{L^2(G;\mu)}^2 = \|\hat{f}\|_{L^2(\hat{G};\nu)}$$

and Parseval

$$(31) \quad \langle f, g \rangle_{L^2(G;\mu)} = \langle \hat{f}, \hat{g} \rangle_{L^2(\hat{G};\nu)}.$$

There is also a symmetry between (25) and (32), for the *Fourier inversion formula* now takes the form

$$(32) \quad f(x) = \langle \hat{f}, \bar{x} \rangle_{L^2(\hat{G};\nu)}.$$

The Fourier transform is now

$$(33) \quad \mathcal{F} : L^2(G; \mu) \rightarrow L^2(\hat{G}; \nu) \quad \mathcal{F}(f) = \hat{f}$$

where \hat{f} is defined with respect to μ by (25) and ν is given by (29).

(29) has a hidden importance, as it hints to the *uncertainty principle*. Heuristically, this principle asserts the more localized a function is, the more spread out its Fourier transform must be. We will say more of this principle in a later section.

9.4. The Fourier Transform on L^1 : The Riemann-Lebesgue Lemma. The Plancherel identity (30) asserts that the Fourier transform is an isometry between (suitably normalized) L^2 spaces, and thus, we may compute the 2-norm of a function by computing the 2-norm of its Fourier transform. In general, this is the only isometry. The *Riemann-Lebesgue lemma* asserts that there is an *inequality* between certain norms, however. We compute

$$\begin{aligned} \|\hat{f}\|_{L^\infty(\hat{G};\nu)} &= \max_{\chi \in \hat{G}} \left| \sum_{x \in G} f(x) \overline{\chi(x)} \mu \right| \\ &\leq \max_{\chi \in \hat{G}} \sum_{x \in G} |f(x)| |\overline{\chi(x)}| \mu = \sum_{x \in G} |f(x)| \mu = \|f\|_{L^1(G;\mu)}. \end{aligned}$$

The *Riemann-Lebesgue lemma* is the conclusion of this argument:

$$(34) \quad \|\hat{f}\|_{L^\infty(\hat{G};\nu)} \leq \sum_{x \in G} |f(x)| \mu = \|f\|_{L^1(G;\mu)},$$

and thus we have

$$(35) \quad \mathcal{F} : L^1(G; \mu) \rightarrow L^\infty(\hat{G}; \nu).$$

9.5. The Fourier Transform on L^p : Young's Inequality. Let $1 \leq p \leq 2$ and let q be the conjugate exponent,

$$(36) \quad \frac{1}{p} + \frac{1}{q} = 1.$$

Young's inequality is then

$$(37) \quad \|\hat{f}\|_{L^q(\hat{G};\nu)} \leq \|f\|_{L^p(G;\mu)},$$

and so

$$(38) \quad \mathcal{F} : L^p(G; \mu) \rightarrow L^q(\hat{G}; \nu).$$

The special cases for $p = 1$ and $p = 2$ are contained in the Riemann-Lebesgue lemma (34) and Plancherel's identity (30) respectively. The general case then follows from the theory of interpolation of operators. See [4], for instance. It is possible to derive this inequality for q a power of two by iterating Plancherel's identity and using

$$\|f\|_{2k}^{2k} = \|f\bar{f}\|_k^k.$$

We can extend (38) to all $1 \leq p \leq \infty$ by interpolating with the estimate

$$(39) \quad \|\hat{f}\|_{L^1(\hat{G};\nu)} \leq |G| \|f\|_{L^\infty(G;\mu)}.$$

Interpolation gives

$$(40) \quad \|\hat{f}\|_{L^q(\widehat{G};\nu)} \leq C_{p,|G|} \|f\|_{L^p(G;\mu)},$$

where $C_{p,|G|} = 1$ for $1 \leq p \leq 2$ and $C_{p,|G|} = |G|^{1-2/p}$. As far as I know, it is not possible to get this inequality with a constant independent of $|G|$ when $p > 2$.

10. INTERTWINING PROPERTIES OF THE FOURIER TRANSFORM

We saw that there are many structures present in $\mathfrak{X}(G)$. The Fourier transform is well behaved between most of these structures.

10.1. Intertwining the Involutions. Both $\mathfrak{X}(G)$ and $\mathfrak{X}(\widehat{G})$ are equipped with the two involutions of *complex conjugation* (13) and *reflection* (14). Easy computations show

$$(41) \quad \widehat{\mathcal{C} \circ \mathcal{R}f} = \mathcal{C}\hat{f}$$

and

$$(42) \quad \widehat{\mathcal{R}f} = \mathcal{R}\hat{f}.$$

Thus, reflection commutes with the Fourier transform, and though conjugation does not commute with the Fourier transform, it has a simple commutator.

10.2. Intertwining the Algebras. We have the algebra of pointwise multiplication and the algebra of convolution on $\mathfrak{X}(G)$. We saw the former algebra is tied in with $L^\infty(G;\mu)$ and the latter algebra is tied in with $L^1(G;\mu)$. Furthermore, we saw, via Riemann-Lebesgue (34) that $L^1(G;\mu)$ is tied in with $L^\infty(\widehat{G};\nu)$, and this latter space has its own algebra of pointwise multiplication. A simple calculation using (24) gives

$$(43) \quad \widehat{f * g} = \hat{f}\hat{g},$$

and so not only is (35) true as a mapping between normed spaces, but in fact \mathcal{F} is an homomorphism of normed algebras between the convolution algebra on $L^1(G;\mu)$ to the pointwise multiplication algebra on $L^\infty(\widehat{G};\nu)$, and the homomorphism preserves the multiplicative identities. For, recall δ is defined by (18). Then

$$\widehat{\delta}(\chi) = \sum_{x \in G} \delta(x) \overline{\chi(x)} \mu = \chi(1) = 1.$$

We mention one peculiarity here. In addition to being a normed algebra, the pointwise multiplication algebra on L^∞ is a C^* -algebra. The Fourier transform is well behaved with respect to the algebraic structure, but not the C^* -algebra structure.

The Fourier transform also gives a well defined vector space homomorphism from $L^\infty(G;\mu)$ into $L^1(\widehat{G};\nu)$. The former is an algebra under multiplication and the latter is an algebra under convolution, and again the Fourier transform is an unital algebra homomorphism;

$$(44) \quad \widehat{fg} = \hat{f} * \hat{g}.$$

Further more, the Fourier transform is a *normed* algebra homomorphism by (39), although the bound is dependent on $|G|$.

10.3. Intertwining the Representations. We mentioned that our two involutions of complex conjugation and reflection arose from representations of $\mathbb{Z}/2\mathbb{Z}$ on $L^2(G; \mu)$, and then (41) and (42) are statements that the Fourier transform intertwines these two representations. The representations (21) and (23) likewise behave nicely under Fourier transformation. First, we have that modulations are sent to translations,

$$(45) \quad \widehat{M_y f} = T_y \hat{f}.$$

Likewise, translations are sent to modulations, but with a reflection in the modulation,

$$(46) \quad \widehat{T_y f} = M_{-y} \hat{f}.$$

10.4. A Missing Intertwining Relation. One of the most important intertwining relation for the Fourier transform on \mathbb{R} is that it intertwines the two operators

$$f \mapsto \frac{d}{dx} f(x)$$

and

$$f \mapsto x f(x),$$

and thus becomes a powerful tool in differential equations. There appears to be no analogue of this in the finite abelian group setting. In fact, recall that a *derivation* on a \mathbb{C} -algebra is a linear transformation D of the algebra into itself which satisfies the Leibnitz rule

$$D(fg) = f(Dg) + (Df)g.$$

We show that $L^\infty(G; \mu)$, under pointwise multiplication, does not have any nontrivial derivations. To that end, let V be a finite dimensional vector space which has a product structure of pointwise multiplication. Let $\{e_j\}$ be a basis of V . Let $f = \sum_j a_j e_j$ and $g = \sum_j b_j e_j$ be elements of V . Then

$$fg = \sum_j a_j b_j e_j.$$

By linearity, we have

$$D\left(\sum_j a_j e_j\right) = \sum_j a_j D(e_j)$$

and likewise for g . Then

$$D(fg) = \sum_j a_j b_j (D(e_j)) = f(Dg) = (Df)g$$

and so the Leibnitz rule cannot hold unless $D = 0$.

11. THE FOURIER TRANSFORM ON DERIVED GROUPS

We saw that the operation of forming dual groups behaves nicely with respect to various ways of building new groups from old groups. It is thus natural to believe the Fourier transform theory behaves nicely with respect to the operations as well.

11.1. The Fourier Transform on \widehat{G} . As an abelian group, \widehat{G} has its own Fourier transform. Let us denote the Fourier transform on G by \mathcal{F}_G and the Fourier transform on \widehat{G} by $\mathcal{F}_{\widehat{G}}$. Given a function $F \in L^2(\widehat{G}; \nu)$ and a character $x \in \widehat{\widehat{G}}$ and applying (25) to this data, we get

$$\mathcal{F}_{\widehat{G}} F(x) = \langle F, x \rangle_{L^2(\widehat{G}; \nu)}.$$

In particular, if $F = \hat{f} = \mathcal{F}_G f$ where $f \in L^2(G; \mu)$, then

$$\mathcal{F}_{\widehat{G}} \circ \mathcal{F}_G f(x) = \langle \hat{f}, x \rangle_{L^2(\widehat{G}; \nu)}.$$

This is only off from (32) by a reflection in the character. Therefore,

$$(47) \quad \mathcal{F}_{\widehat{G}} \circ \mathcal{F}_G = \mathcal{R}.$$

Notice that even though G is canonically isomorphic to its double dual, that

$$\mathcal{F}_{\widehat{\widehat{G}}} = \mathcal{R} \circ \mathcal{F}_G,$$

and so we have to dualize four times to get back to our exact starting point. In many ways, one may think applying the Fourier transform as analogous to multiplying a complex number by i .

11.2. The Fourier Transform on $G_1 \oplus G_2$. Let us begin by recalling *tensor products of vector spaces*. The treatment is particularly simple, and natural, when the vector spaces are spaces of functions on some set. Let X and Y be two finite sets, and $\mathfrak{X}(X)$ and $\mathfrak{X}(Y)$ the vector spaces of all complex valued functions defined on X and Y . The tensor product $\mathfrak{X}(X) \otimes \mathfrak{X}(Y)$ is then formed as follows. Given $f \in \mathfrak{X}(X)$ and $g \in \mathfrak{X}(Y)$, we form the *elementary tensor* $f \otimes g : X \times Y \rightarrow \mathbb{C}$ by

$$f \otimes g(x, y) = f(x)g(y).$$

The tensor product $\mathfrak{X}(X) \otimes \mathfrak{X}(Y)$ is then the linear span of all of the elementary tensors. The identity

$$\mathfrak{X}(X) \otimes \mathfrak{X}(Y) = \mathfrak{X}(X \times Y)$$

suggests that the tensor product is the natural category theoretic product. Likewise we may form tensor products of spaces with additional structure, and for instance

$$L^p(X) \otimes L^p(Y) = L^p(X \times Y)$$

where X and Y are measure spaces.

Let G_1 and G_2 be finite abelian groups. Let \mathcal{F}_{G_1} and \mathcal{F}_{G_2} denote the Fourier transforms on the groups G_1 and G_2 . Let $\mathcal{F}_{G_1 \oplus G_2}$ denote the Fourier transform on the direct sum $G_1 \oplus G_2$. Then

$$(48) \quad \mathcal{F}_{G_1 \oplus G_2} = \mathcal{F}_{G_1} \otimes \mathcal{F}_{G_2};$$

that is,

$$\mathcal{F}_{G_1 \oplus G_2}(f_1 \otimes f_2)(\chi_1 \otimes \chi_2) = \mathcal{F}_{G_1}(f_1)(\chi_1)\mathcal{F}_{G_2}(f_2)(\chi_2).$$

11.3. Interaction with Subgroups: The Poisson Summation Formula. We want to adopt a point of view which will place (32) and (25) on equal footing. First, (32) expresses f evaluated at a point as a suitable average over \widehat{G} of the Fourier coefficients of f , whereas (25) expresses \hat{f} evaluated at a point as a suitable average over G of the values of f . In the first case, let us think of $f(x)$ as being a suitable average of f over a coset of the trivial subgroup of G . In the second case, let us think of $\hat{f}(\chi)$ as a suitable average of \hat{f} over a coset of the trivial subgroup of \widehat{G} . Thus, both (25) and (32) asserts that a certain average of f over a coset of a subgroup of G coincides with a certain average of \hat{f} over a coset of a subgroup of \widehat{G} .

Now let H be any subgroup of G . Then using inversion and recalling (7), we have

$$\begin{aligned} \sum_{x \in H} f(x)\mu &= \frac{1}{|G|} \sum_{x \in H} \sum_{\chi \in \widehat{G}} \hat{f}(\chi)\chi(x) \\ &= \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \hat{f}(\chi) \sum_{x \in H} \chi(x) = \frac{|H|}{|G|} \sum_{\chi \in \widehat{G}^H} \hat{f}(\chi). \end{aligned}$$

The *Poisson summation formula* is the result of this computation:

$$(49) \quad \sum_{x \in H} f(x)\mu = \frac{|H|}{|G|} \sum_{\chi \in \widehat{G}^H} \hat{f}(\chi).$$

This asserts that certain averages of f over subgroups of G correspond to certain averages of \hat{f} over subgroups of \hat{G} . This can be extended to cosets of subgroups,

$$(50) \quad \sum_{x \in H} f(xy) \overline{\varphi(x)} \mu = \frac{|H|}{|G|} \varphi(y) \sum_{\chi \in \hat{G}^H} \hat{f}(\chi \varphi) \chi(y)$$

where $\varphi \in \hat{G}$ and $y \in G$. Taking $H = \{1\}$ and $\varphi = 1$ recovers (32). Taking $H = G$ and $y = 1$ gives $\hat{f}(\varphi)$. This formula foreshadows the *uncertainty principle*: Averaging f over a large subgroup of G corresponds to averaging \hat{f} over a small subgroup of \hat{G} and vice versa.

Let us point out a consequence of the Poisson summation formula (49). Suppose H is a subgroup of G and $f = \mathbf{1}_H$. Let $\varphi \in \hat{G}$. Then

$$\hat{f}(\varphi) = \sum_{x \in G} f(x) \overline{\varphi(x)} \mu = \sum_{x \in H} \overline{\varphi(x)} \mu,$$

and so

$$(51) \quad \widehat{\mathbf{1}_H}(\varphi) = \begin{cases} \mu |H|; & \text{if } \varphi \in \hat{G}^H, \\ 0; & \text{else.} \end{cases}$$

Thus, in view of (8), the Fourier transform effectively maps subgroups of G to quotient groups of \hat{G} . Together with the self-duality (6) of finite abelian groups the Fourier transform is thus seen to pass from H to G/H . Along with (46) and (45), we can see that the Fourier transform takes cosets of subgroups to cosets of quotient groups. This is particularly exploited in the study of linear equations over finite fields, in which case the Fourier transform gives an analytic apparatus which moves back and forth between the null space and the row space of a system of equations.

12. THE UNCERTAINTY PRINCIPLE

A heuristic principle in Fourier analysis is that if one wants to localize a function, one must be willing to concede a loss in the localization of the functions Fourier transform. There are numerous ways to quantify what we mean by *localize*.

12.1. Heisenberg Tiles. A particularly nice form of the uncertainty principle exists for finite abelian groups in which the degree of localization is measured in terms of the cardinality of the supports of the f and \hat{f} . Let $A = \text{supp } f$ and $B = \text{supp } \hat{f}$ and consider thus

$$\begin{aligned} \|\hat{f}\|_{L^\infty(\hat{G}; \nu)} &= \max_{\chi \in \hat{G}} |\hat{f}(\chi)| = \max_{\chi \in \hat{G}} \left| \sum_{x \in G} f(x) \overline{\chi(x)} \mu \right| \\ &= \max_{\chi \in \hat{G}} \left| \sum_{x \in G} \mathbf{1}_A(x) f(x) \overline{\chi(x)} \mu \right| \leq \sqrt{|A| \mu} \|f\|_{L^2(G; \mu)} = \sqrt{|A| \mu} \|\hat{f}\|_{L^2(\hat{G}; \nu)} \\ &= \sqrt{|A| \mu} \left(\sum_{\chi \in \hat{G}} \mathbf{1}_B(\chi) |\hat{f}(\chi)|^2 \nu \right)^{1/2} \leq \sqrt{|A| |B| \mu \nu} \|\hat{f}\|_{L^\infty(\hat{G}; \nu)}. \end{aligned}$$

Rearranging this computation and recalling (29), we get the uncertainty principle

$$(52) \quad |\text{supp } f| |\text{supp } \hat{f}| \geq |G|,$$

provided f is not identically 0. Thus, if f is supported on a very small set then \hat{f} is supported on a very large set.

We saw that the Fourier transform of the characteristic function of a subgroup is effectively the characteristic function of the corresponding quotient group, and so equality in (52) holds whenever f is the characteristic function of a subgroup. Translations and modulation (or equivalently taking cosets of subgroups) don't affect the uncertainty relation, and one can show that if equality holds in (52) then f must be a scalar multiple of a translation and

modulation of the characteristic function of a subgroup of G .

The name "Heisenberg tiles" refers to the fact that if we draw the Cartesian product of the support of f and the support of \hat{f} in the *phase space* $G \oplus \widehat{G}$, then we get a rectangle whose size is at least $|G|$. A lot of intuition⁵ can be developed by studying the phase space, but we will not do so here. The interested reader is referred to [5].

12.2. A Heuristic Explanation for the Uncertainty Principle. We reproduce an argument from [5] which indicates why one might suspect the uncertainty principle to hold. Let our group be $G = \mathbb{Z}/2\mathbb{Z}$ and suppose we could find a function $f_{(0,0)}$ with $\text{supp } f_{(0,0)} = \{0\}$ and $\text{supp } \widehat{f_{(0,0)}} = \{0\}$. Then by translating and modulating $f_{(0,0)}$ we may find functions $f_{(n,m)}$ with $\text{supp } f_{(n,m)} = \{n\}$ and $\text{supp } \widehat{f_{(n,m)}} = \{m\}$ for each $(n, m) \in \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. These four functions are then mutually orthogonal, and in particular they are linearly independent. But now we have a set of four linearly independent functions in the two dimensional vector space $L^2(\mathbb{Z}/2\mathbb{Z})$, a contradiction.

REFERENCES

- [1] Nathanson, M.B., *Elementary Methods in Number Theory*, Graduate Texts in Mathematics 195, Springer-Verlag, (2000)
- [2] Serre, J.P., *A Course in Arithmetic*, Graduate Texts in Mathematics 7, Springer-Verlag, New York, (1973)
- [3] Stein, E. M., Shakarchi, R., *Fourier Analysis: An Introduction* Princeton Lectures in Analysis 1, Princeton University Press, Princeton, (2003)
- [4] Stein, E. M., Weiss, G., *Introduction to Fourier Analysis on Euclidean Spaces* Princeton Mathematical Series, No. 32, Princeton University Press, Princeton, (1971)
- [5] Tao, T., *Harmonic Analysis in the phase plane*, Lecture Notes, UCLA, Math 254A, <http://www.math.ucla.edu/>
- [6] Tao, T., *Technical survey of harmonic analysis*, Expository Note, available <http://www.math.ucla.edu/tao/preprints/harmonic.html>
- [7] Terras, A., *Fourier Analysis on Finite Groups and Applications*, London Mathematical Society Student Texts 43, Cambridge University Press, Cambridge, (1999)

DEPARTMENT OF MATHEMATICS, WASHINGTON UNIVERSITY, ST. LOUIS, MO 63130, U. S. A.
E-mail address: paul@math.wustl.edu

⁵In particular, many important decompositions in Fourier analysis can be represented on phase space, and many formulas and estimates are encoded in the geometry and combinatorics of how Heisenberg tiles overlap.