Fourier Analysis on Finite Abelian Groups With an Emphasis on Uncertainty Principles

Cameron LaVigne

December 18, 2013

Contents

Acknowledgments

I would like to thank the National Science Foundation for its support through the Summer and Fall 2013 "Mentoring through Critical Transition Points" (MCTP) grant DMS 1148801. I would also like to thank the Undergraduate Committee, especially Professor Monika Nitsche in her dual role as Chair of the Undergraduate Committee and PI of the MCTP grant. Finally, I would like to thank Professor Cristina Pereyra for her support and encouragement.

Chapter 1

Introduction

Most people are familiar with the Heisenberg Uncertainty Principle, which states that it is impossible to know for certain both a particle's momentum and its position. This uncertainty principle is actually just the most well-known of numerous uncertainty principles, including an uncertainty principle for supports of functions on groups.

The proof of the Heisenberg Uncertainty Principle involves Fourier analysis on the real number line, or classical Fourier analysis as we will refer to it. We will first review basic concepts from classical Fourier theory before we develop analogs to those same principles for Fourier analysis on finite abelian groups. When developing a Fourier theory on groups, we will begin with the very basics: first, we will develop analogs to integration and an inner-product vector space of functions from our group into the complex numbers. After that, we will develop a dual group, which will contain elements that play the same role as trigonometric functions do in classical Fourier analysis. We will then define the Fourier transform of elements in our dual group. From there, we will be free to find analogs to classical results in traditional Fourier theory such as Plancherel's identity, the Fourier inversion formula, and a partial time-frequency dictionary.

After we have developed a thorough theory for Fourier analysis on our groups, we will them provide proofs for both the classical and group versions of the uncertainty principles. The discrete uncertainty principle states $|\text{supp}f||\text{supp}\widehat{f}| \geq |G|$, where $\text{supp}f$ denotes the set of elements in our group for which our function is nonzero. We will also prove that the only functions that make those inequalities sharp are the Gaussians in $\mathbb{R}$ and translations, modulations, or scalar multiples of indicator or characteristic functions of subgroups in groups.

We will then take a small detour from the uncertainty principle to prove another inequality, the entropy uncertainty principle. This inequality can actually be used to prove the uncertainty principle for groups, although that result is beyond the scope of this paper. As with most of the ideas presented in this paper, we will look at the analog to the group version of the entropy uncertainty principle, the Shannon Entropy Inequality over the real line.

After that, we will return to the idea of the uncertainty principle and prove a refinement of the group version by Terence Tao. This refinement applies to cyclic groups of prime order. Tao's refinement states $|\text{supp}f| + |\text{supp}\widehat{f}| \geq p$, where p is the order of our group, which must be a prime number for this refinement.

Finally, we will look briefly at a couple of the applications of the idea of Fourier analysis on groups. The first application is the Green-Tao theorem, which says that for any positive integer k, there exists an arithmetic progression of primes of length k. This result, along with other work, earned Terence Tao the Fields Medal in 2006. While proving the Green-Tao theorem is far beyond the scope of this text, we mention it as an application to Tao's refinement because the refinement is used in the proof of the theorem.

The second application is the idea of compressed sensing, which allows comprehensive images to be constructed from limited data. Compressed sensing is a very popular area of research today, and its applications are wide-spread. The methods of compressed sensing are used in medical imaging and image compression, and the United States military has even used it. Again, going into detail of compressed sensing is beyond this text, but we will prove a theorem that gives us certain conditions where we can reconstruct a function from partial frequency information.

To begin, we will review classical Fourier analysis on the real line.

Chapter 2

Fourier Analysis on $\mathbb{R}$

Before we begin to develop our Fourier theory on finite abelian groups, let us first review some main ideas from classical Fourier analysis. These ideas and theorems will also play a role when we prove the Heisenberg Uncertainty Principle later on in this paper. The following definitions and theorems can be found in most Fourier analysis books.

2.1 The Schwartz Class

In order to develop the idea of Fourier analysis, we must first have a space of functions to work in. The space we will work in is called the Schwartz class, which is an inner-product vector space.

Definition 1. The **Schwartz class** $\mathcal{S}(\mathbb{R})$ is the collection of infinitely differentiable functions $f : \mathbb{R} \to \mathbb{C}$ that decrease faster than any polynomial increases, as do all of their derivatives. That is, for all non-negative integers k and l,

$$\lim_{|x|\to\infty} |x^k||f^{(l)}(x)| = 0$$

Lemma 2. *The Schwartz class is a vector space.*

Proof. To be a vector space, $\mathcal{S}(\mathbb{R})$ must be closed, be associative under addition and scalar multiplication, be commutative under addition, have an additive identity as well as additive inverses for every element, have a scalar multiplicative identity, and have a distributive law.

Since we are dealing with functions in $\mathbb{C}$, we know that addition of functions is commutative and associative, and the scalar multiplication is associative. We also know that for all $c_1, c_2 \in \mathbb{C}$ and functions $f, g : \mathbb{R} \to \mathbb{C}$, $c_1(f+g) = c_1f + c_2g$ and $(c_1+c_2)f = c_1f + c_2f$. So we need only check that $\mathcal{S}(\mathbb{R})$ is closed under addition and scalar multiplication, has an identity element, and has an inverse for each element. Let $f, g \in \mathcal{S}(\mathbb{R})$, then let $h(x) = f(x) + g(x)$. The n^{th} derivative $h^{(n)}(x) = f^{(n)}(x) + g^{(n)}(x)$. Then by limit laws and the triangle inequality, $0 \leq \lim_{|x|\to\infty} |x|^k|h^{(l)}(x)| \leq \lim_{|x|\to\infty} |x|^k|f^{(l)}(x)| + \lim_{|x|\to\infty} |x|^k|g^{(l)}(x)| = 0 + 0 = 0$. Thus, $\lim_{|x|\to\infty} |x|^k|h^{(l)}(x)| = 0$, so the Schwartz class is closed under addition.

If $c \in \mathbb{C}$, then $|cf(x)| = |c||f(x)|$ and any n^{th}derivative of $cf(x)$ will be equal to $c \times f^{(n)}(x)$. Again using limit laws, $\lim_{|x|\to\infty} |x|^k|cf^{(l)}(x)| = c \times \lim_{|x|\to\infty} |x|^k|f^{(l)}(x)| = |c| \times 0 = 0$, so the Schwartz class is closed under scalar multiplication as well.

Let $b : \mathbb{R} \to \mathbb{C}$ be defined as $b(x) := 0$ for all $x \in \mathbb{R}$. This function is in $\mathcal{S}(\mathbb{R})$ since $\lim_{|x|\to\infty} |x|^k |b^{(l)}(x)| = \lim_{|x|\to\infty} |x|^k \times 0 = 0$. Then for all $f \in \mathcal{S}(\mathbb{R})$, $f(x)+b(x) = f(x)+0 = f(x)$ for all $x \in \mathbb{R}$. Thus, $b(x)$ is the zero element of $\mathcal{S}(\mathbb{R})$. The scalar 1 is the multiplicative identity since $1 \times f(x) = f(x)$ for all f in $\mathcal{S}(\mathbb{R})$ and x in $\mathbb{R}$.

For every $g \in \mathcal{S}(\mathbb{R})$, consider the function $-g$, where $-g(x) = (-1) \times g(x)\ \forall x \in \mathbb{R}$. Then $g(x) + (-g(x)) = 0$ for all $g \in \mathcal{S}(\mathbb{R})$, so each element has an additive inverse. We can thus conclude that $\mathcal{S}(\mathbb{R})$ is indeed a vector space. □

Lemma 3. *The Schwartz class has an inner product. For all $f, g \in \mathcal{S}(\mathbb{R})$,*

$$\langle f, g\rangle := \int_{\mathbb{R}} f(x)\overline{g(x)}dx \tag{2.1.1}$$

Proof. First, it is clear that, because f, g are in $\mathcal{S}(\mathbb{R})$, that the inner product as defined in equation 2.1.1 is convergent. To prove that equation 2.1.1 defines an inner product, we must show four things for all $f, g, h \in \mathcal{S}(\mathbb{R})$ and $c \in \mathbb{R}$: $1)\langle f, g\rangle = \overline{\langle g, f\rangle}$, $2)\langle f, f\rangle \geq 0$ with equality only when $f := 0$, $3)\langle cf, g\rangle = c\langle f, g\rangle$, and $4)\langle f + g, h\rangle = \langle f, h\rangle + \langle g, h\rangle$.

To start with, $\int_{\mathbb{R}} f(x)\overline{g(x)}dx = \int_{\mathbb{R}} f(x)\overline{\overline{g(x)}dx} = \int_{\mathbb{R}} g(x)\overline{f(x)}dx$. So $\langle g, f\rangle = \overline{\langle f, g\rangle}$.

Second, we can see that $\langle f, f\rangle = \int_{\mathbb{R}} f(x)\overline{f(x)}dx = \int_{\mathbb{R}} |f(x)|^2 dx$. Hence $|f(x)|^2 \geq 0$ for all x in $\mathbb{R}$, so $\int_{\mathbb{R}} |f(x)|^2 dx \geq 0$. Since f is an element of the Schwartz class, we know that f is continuous. If f is not identically equal to zero, there must exist an x_0 in $\mathbb{R}$ such that $f(x_0) \neq 0$. By the definition of continuity, there exists a $\delta > 0$ so that, for all $|x - x_0| < \delta$, f is bounded away from zero, thus $|f(x)| > \frac{|f(x_0)|}{2}$. We can now write

$$\int_{\mathbb{R}} |f(x)|^2 dx \geq \int_{x_0-\delta}^{x_0+\delta} |f(x)|^2 dx \geq \frac{|f(x_0)|^2}{4} \times 2\delta > 0.$$

Thus, if f is not identically equal to zero, then $\langle f, f\rangle \neq 0$. Also, we know that $\int_{\mathbb{R}} 0dx = 0$, so we can now say that $\langle f, f\rangle = 0$ if and only if f is identically equal to zero.

Third, $\langle cf, g\rangle = \int_{\mathbb{R}} cf(x)\overline{g(x)}dx = c\int_{\mathbb{R}} f(x)\overline{g(x)}dx = c\langle f, g\rangle$.

Finally, $\langle f + g, h\rangle = \int_{\mathbb{R}}(f(x) + g(x))\overline{h(x)}dx = \int_{\mathbb{R}} f(x)\overline{h(x)}dx + \int_{\mathbb{R}} g(x)\overline{h(x)}dx = \langle f, h\rangle + \langle g, h\rangle$.

Thus, equation 2.1.1 defines an inner product on $\mathcal{S}(\mathbb{R})$. □

Definition 4. The **induced norm** of $\mathcal{S}(\mathbb{R})$ is defined as:

$$\| f \|_2 := \sqrt{\int_{\mathbb{R}} |f(x)|^2 dx} \tag{2.1.2}$$

Remark. The 2 subscript of the induced norm of $\mathcal{S}(\mathbb{R})$ refers to the fact that this induced norm coincides with the norm in $L^2(\mathbb{R})$, which is the space of square-integrable functions. $L^2(\mathbb{R})$ is a complete inner-product vector space, also known as a Hilbert space. The inner-product is defined as in equation 2.1.1, where the integral is the Lebesgue integral, which is beyond the scope of this thesis.

All inner-product vector spaces, including $\mathcal{S}(\mathbb{R})$ with the $L^2 - norm$, obey the Cauchy-Schwarz inequality.

Lemma 5. *(Cauchy-Schwarz Inequality): For $f, g \in L^2(\mathbb{R})$,*

$$| \langle f, g \rangle | \leq \| f \|_2 \| g \|_2 .$$

Lemma 6. *The Schwartz class is closed under multiplication.*

Proof. Let f and g be functions in $\mathcal{S}(\mathbb{R})$.

Consider the function $h : \mathbb{R} \to \mathbb{C}$ such that $h(x) = f(x)g(x)$ for all x in $\mathbb{R}$. We can then write the l^{th} derivative of $h(x)$ as

$$h^{(l)}(x) = \sum_{m=0}^{l} \binom{l}{m} f^{(m)}(x) g^{(l-m)}(x) \tag{2.1.3}$$

Then, using the limit laws and the triangle inequality,

$$\begin{aligned} \lim_{|x|\to\infty} |x|^k |h^{(l)}(x)| &\leq \lim_{|x|\to\infty} \sum_{m=0}^{l} |x|^k \binom{l}{m} |f^{(m)}(x) g^{(l-m)}(x)| \\ &= \sum_{m=0}^{l} \left[\left(\lim_{|x|\to\infty} |x|^k |f^{(m)}(x)| \right) \left(\binom{l}{m} \lim_{|x|\to\infty} |g^{(l-m)}(x)| \right) \right] \end{aligned}$$

Since $f, g \in \mathcal{S}(\mathbb{R})$, $\lim_{|x|\to\infty} |x|^k f^{(m)}(x)| = 0$ for all $k, m \geq 0$, $k, m \in \mathbb{Z}$. Similarly, $\lim_{|x|\to\infty} |g^{(n)}(x)| = 0$ for all $n \geq 0$, $n \in \mathbb{Z}$. Thus, $\lim_{|x|\to\infty} |x|^k |h^{(l)}(x)| = 0$, so $h \in \mathcal{S}(\mathbb{R})$. Thus, the Schwartz class is closed under multiplication. □

Lemma 7. *The Schwartz class is closed under multiplication by trigonometric functions.*

Proof. Let a function $f \in \mathcal{S}(\mathbb{R})$, and let $h(x) := e^{2\pi i x} f(x)$ $\forall x \in \mathbb{R}$. The l^{th} derivative of $h(x)$ will be given by equation 2.1.3, with $g^{(l-m)}(x) = (2\pi i)^{l-m} e^{2\pi i x}$. So by limit laws and the triangle inequality,

$$\begin{aligned} \lim_{|x|\to\infty} |x|^k |h^{(l)}(x)| &\leq \sum_{m=0}^{l} \left[\left(\lim_{|x|\to\infty} |x|^k |f^{(m)}(x)| \right) \binom{l}{m} \lim_{|x|\to\infty} |(2\pi i)^{l-m} |e^{2\pi i x}| \right] \\ &\leq \sum_{m=0}^{l} \left[\left(\lim_{|x|\to\infty} |x|^k |f^{(m)}(x)| \right) \binom{l}{m} \lim_{|x|\to\infty} (2\pi)^{l-m} \right] \\ &= \sum_{m=0}^{l} \left[0 \times \binom{l}{m} (2\pi)^{l-m} \right] \\ &= 0 \end{aligned}$$

Thus, $h(x) \in \mathcal{S}(\mathbb{R})$, so the Schwartz class is closed under multiplication by trigonometric functions. □

2.2 The Fourier Transform

We will now go over a few basic definitions and theorems from classical Fourier analysis that we will later find analogs to in the group setting.

Definition 8. The **Fourier transform** $\widehat{f} : \mathbb{R} \to \mathbb{C}$ of a Schwartz function for $\xi \in \mathbb{R}$ is defined by

$$\widehat{f}(\xi) := \int_{\mathbb{R}} f(x) e^{-2\pi i \xi x} dx.$$

The Riemann-Lebesgue Lemma tells us that $\lim_{|\xi| \to \infty} \widehat{f}(\xi) = 0$, so using that and Lemma 7, we know that the Fourier transform of a Schwartz function is also a Schwartz function.

The next few lemmas are part of the time-frequency dictionary, which relates the convolution, translation, derivative, and many other operations of functions and their Fourier transforms.

Lemma 9. *For $f \in \mathcal{S}(\mathbb{R})$, $\widehat{f'}(\xi) = 2\pi i \xi \widehat{f}(\xi)$.*

Proof. Consider the Fourier transform of the derivative of f, $\widehat{f'}(\xi) = \int_{\mathbb{R}} f'(x) e^{-2\pi i \xi x} dx$. We will use integration by parts, letting $u = e^{-2\pi i \xi x}$ and $dv = f'(x)dx$. We know that $du = -2\pi i \xi e^{-2\pi i \xi x} dx$ and $v = f(x)$. Using the integration by parts formula, $\widehat{f'}(\xi) = f(x)e^{-2\pi i \xi x}|_{-\infty}^{\infty} - \int_{\mathbb{R}} -2\pi i \xi e^{-2\pi i \xi x} f(x) dx$. Since $f \in \mathcal{S}(\mathbb{R})$, $f(x)e^{-2\pi i \xi x}|_{-\infty}^{\infty} = 0$. Thus, $\widehat{f'}(\xi) = \int_{\mathbb{R}} 2\pi i \xi e^{-2\pi i \xi x} f(x) dx = 2\pi i \xi \widehat{f}(\xi)$. □

Definition 10. The convolution of two functions, f and g, is defined as

$$f * g(x) = \int_{\mathbb{R}} f(x-y) g(y) dy$$

Lemma 11. *For $f, g \in \mathcal{S}(\mathbb{R})$, $\widehat{f * g}(\xi) = \widehat{f}(\xi)\widehat{g}(\xi)$.*

Proof. By definition of the Fourier transform and convolution, $\widehat{f * g}(\xi) = \int_{\mathbb{R}} (\int_{\mathbb{R}} f(x-y)g(y)dy) e^{-2\pi i \xi x} dx$. Let $u = x - y$, so $du = dx$ and $x = u + y$. Then after interchanging the order of integration, we get the desired result:

$$\begin{aligned} \widehat{f * g}(\xi) = \int_{\mathbb{R}} \big(\int f(u)g(y)dy \big) e^{-2\pi i \xi (u+y)} du &= \int_{\mathbb{R}} f(u) e^{-2\pi i \xi u} du \int_{\mathbb{R}} g(y) e^{-2\pi i \xi y} dy \\ &= \widehat{f}(\xi)\widehat{g}(\xi). \end{aligned}$$

□

Definition 12. The **translation** of a function f by a scalar h is defined as $\tau_h f(x) := f(x-h)$.

Definition 13. The **modulation** of a function f by a scalar h is defined as $M_h f(x) := e^{2\pi i h x} f(x)$.

Lemma 14. *For $f \in \mathcal{S}(\mathbb{R})$, $\widehat{M_h f}(\xi) = \tau_h \widehat{f}(\xi)$.*

Proof. Consider the function $\widehat{M_h f}(\xi) = \int_{\mathbb{R}} e^{2\pi i h x} f(x) e^{-2\pi i x \xi} dx = \int_{\mathbb{R}} f(x) e^{-2\pi i x(\xi - h)} dx = \widehat{f}(\xi - h) = \tau_h \widehat{f}(\xi)$. □

The Fourier transform creates a bijective map from $\mathcal{S}(\mathbb{R})$ onto itself. Because of this fact, we can recover the original function from its Fourier transform using the Fourier Inversion Formula.

Theorem 15. *(Fourier Inversion Formula): If $f \in \mathcal{S}(\mathbb{R})$, then for all $x \in \mathbb{R}$,*

$$f(x) = \int_{\mathbb{R}} \widehat{f}(\xi) e^{2\pi i \xi x} d\xi.$$

Remark. For a proof of the above formula, see [14], pg. 180.

Theorem 16. *(Plancherel's Identity): If $f \in \mathcal{S}(\mathbb{R})$, then*

$$\| f \|_2 = \| \hat{f} \|_2 .$$

Remark. The proof to this identity involves the time-frequency dictionary, the Fourier Inversion Formula, and the multiplication formula, which states that $\int_{\mathbb{R}} f(x)\widehat{g}(x)dx = \int_{\mathbb{R}} \widehat{f}(x) g(x) dx$ for all $f, g \in \mathcal{S}(\mathbb{R})$.

Chapter 3

Fourier Analysis on Finite Abelian Groups

In this chapter, we will develop a Fourier theory on finite abelian groups. In order to have a well-developed theory, we will need analogs to key ideas in classical Fourier analysis, like integration, induced norms, and trigonometric functions. Before we do this though, we will need to review some key concepts of group theory.

3.1 Group Theory

Definition 17. A **finite abelian group**, denoted $\langle G, * \rangle$, is a set G closed under a binary operation $*$ such that the following properties are satisfied:

- $\forall a, b, c \in G, (a * b) * c = a * (b * c)$, associativity of $*$
- $\exists e \in G$ such that $a * e = e * a = a \ \forall a \in G$, identity element
- $\forall a \in G$, $\exists a' \in G$ such that $a * a' = a' * a = e$, inverse elements
- $\forall a, b \in G$, $a * b = b * a$, commutativity of $*$
- the set G has a finite number of elements

Definition 18. The **order** of a group G, denoted $|G|$, is the number of elements in the set G.

Example 19. Examples of finite abelian groups include the cyclic group $\langle \mathbb{Z}_n, + \rangle$, the integers modulo n under addition, and $\langle U_n, * \rangle$, the n^{th} roots of unity under multiplication. [10]

Example 20. An example of a finite abelian group that is not cyclic is the Klein 4-group. This group is isomorphic to $\langle \mathbb{Z}_2 \times \mathbb{Z}_2 \rangle$, with each nontrivial element having order 2. Its multiplication table is as follows:

*	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

We will remember that two groups are said to be isomorphic if there is a bijective function between the two groups that preserves the group operation.

Definition 21. [10]Let $\langle G, * \rangle$ and $\langle G', *' \rangle$ be two groups. G and G' are **isomorphic** if there exists a bijective function ϕ mapping G onto G' such that $\phi(a * b) = \phi(a) *' \phi(b)$ for all $a, b \in G$. We denote this as $G \simeq G'$.

Example 22. The previous example of the Klein 4-group is isomorphic to the group $\mathbb{Z}_2 \times \mathbb{Z}_2$, where the $\times$ denotes the direct product. Elements of this group are ordered pairs of the form (a, b), where $a, b \in \{0, 1\}$. This is just one particular case of groups of the form $\mathbb{Z}_2^n = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$. These groups are used in Boolean algebra, which is where the values of the variables can be only one of two things.

Remark 23. It can be shown that all finite abelian groups are isomorphic to the direct product of cyclic groups. A cyclic group is a group that can be generated by a single element, i.e. $G = \{a^n | n \in \mathbb{Z}\}$. Since every cyclic group of order n is isomorphic to $\langle \mathbb{Z}_n, + \rangle$, we can say that every finite abelian group is isomorphic to the group $\mathbb{Z}_{N_1} \times \mathbb{Z}_{N_2} \times \cdots \times \mathbb{Z}_{N_k}$, where $N_1, N_2, \ldots, N_k$ are positive integers, [12], Theorem 0.1.

Remark. Unless otherwise stated, $\langle G, * \rangle$ will be a finite abelian group of order n under addition.

3.2 $L^2(G)$

Since we are trying to create an analog to Fourier analysis on the real number line, we will need a space that takes the place of $L^2(\mathbb{R})$. We will call this space $L^2(G)$, which is the space of functions mapping elements of G into $\mathbb{C}$. Since we are only considering finite groups, we will always be dealing with finite groups; thus, we do not need a special, restricted space of functions like we did with the Schwartz class in $\mathbb{R}$. The analog to $\mathcal{S}(\mathbb{R})$ will therefore be the space of all functions from our group into the complex numbers, $L^2(G) = \{f : G \to \mathbb{C}\}$. Let $|G| = n$. For each $a \in G$ define a function $\delta_a : G \to \mathbb{C}$ by

$$\delta_a(x) = \begin{cases} 0 & x \neq a \\ \sqrt{n} & x = a \end{cases}$$

Normally it is customary to define $\delta_a(a) := 1$, but we make $\delta_a(a) = \sqrt{n}$ so that, when we later define an inner product for $L^2(G)$, the $\delta_a s$ can form an orthonormal basis for $L^2(G)$.

The next couple of lemmas will help us prove that the $\delta_a s$ do in fact form a basis for $L^2(G)$.

Lemma 24. *If $f \in L^2(G)$, then for all x in G*

$$f(x) = \frac{1}{\sqrt{n}} \sum_{a \in G} f(a)\delta_a(x) \tag{3.2.1}$$

Proof. Assume $G = \{a_1, a_2, \ldots, x, \ldots, a_{n-1}, a_n\}$.Then

$$\begin{aligned} \frac{1}{\sqrt{n}} \sum_{a \in G} f(a)\delta_a(x) &= \frac{1}{\sqrt{n}}[f(a_1) \times \delta_{a_1}(x) + \cdots + f(x) \times \delta_x(x) + \cdots + f(a_n) \times \delta_{a_n}(x)] \\ &= \frac{1}{\sqrt{n}}[f(a_1) \times 0 + \cdots + f(x) \times \sqrt{n} + \cdots + f(a_n) \times 0] \\ &= f(x) \end{aligned}$$

□

Lemma 25. *The functions $\{\delta_a\}_{a \in G}$ are linearly independent.*

Proof. Let $G = \{a_1, a_2, \ldots, a_n\}$ and $b_a \in \mathbb{C}$ for all a in G. Assume $\sum_{a \in G} b_a \delta_a(x) = 0$, for all $x \in G$. By equation 3.2.1, we know $\sum_{a \in G} b_a \delta_a(x) = \sqrt{n} b_x$ for all $x \in G$. This implies that $b_x = 0$ for all $x \in G$. By definition of linear independence, this implies $\{\delta_a\}_{a \in G}$ are linearly independent. □

Remark. Since $\{\delta_a\}_{a \in G}$ are linearly independent and are elements of $L^2(G)$, and since every element in $L^2(G)$ can be written as a linear combination of $\{\delta_a\}_{a \in G}$, then by definition, $\{\delta_a\}_{a \in G}$ form a basis for $L^2(G)$. The dimension of $L^2(G)$ is n, the order of G.

3.2.1 Integration on $L^2(G)$

Again, in the interest of creating an analog to classical Fourier analysis, we will need a form of integration of our functions over our group.

Definition 26. For $U \subset G$ and $f \in L^2(G)$, we define the **integral of f over U** to be:

$$\int_U f = \sum_{a \in U} f(a) \tag{3.2.2}$$

Lemma 27. *The integral as defined by equation 3.2.2 is linear.*

Proof. Let $\alpha, \beta \in \mathbb{C}$, $U \subset G$, and $f, g \in L^2(G)$. Then

$$\begin{aligned} \int_U \alpha f + \beta g &= \sum_{a \in U} \alpha f(a) + \beta g(a) \\ &= \sum_{a \in U} \alpha f(a) + \sum_{a \in U} \beta g(a) \\ &= \alpha \sum_{a \in U} f(a) + \beta \sum_{a \in U} g(a) \\ &= \alpha \int_U f + \beta \int_U g \end{aligned}$$

□

Lemma 28. *If U_1 and U_2 are disjoint subsets of G, then $\int_{U_1 \cup U_2} f = \int_{U_1} f + \int_{U_2} f$.*

Proof. Let $U_1 = \{a_1, a_2, \ldots, a_m\}$ and $U_2 = \{b_1, b_2, \ldots, b_k\}$.

$$\begin{aligned}\int_{U_1 \cup U_2} f &= \sum_{a \in U_1 \cup U_2} f(a) \\ &= f(a_1) + f(a_2) + \cdots + f(a_m) + f(b_1) + f(b_2) + \cdots + f(b_k) \\ &= \sum_{a \in U_1} f(a) + \sum_{a \in U_2} f(a) \\ &= \int_{U_1} f + \int_{U_2} f\end{aligned}$$

□

3.2.2 The Inner Product of $L^2(G)$

Since our goal is to develop a Fourier theory on groups, we obviously need to develop the idea of a Fourier transform on groups. To do this, we will need an inner product in our vector space, $L^2(G)$.

Define a mapping $\langle *, * \rangle : L^2(G) \times L^2(G) \to \mathbb{C}$ with the formula

$$\langle f, g \rangle = \frac{1}{|G|} \int_G f\overline{g} = \frac{1}{|G|} \sum_{a \in G} f(a)\overline{g(a)} \tag{3.2.3}$$

Lemma 29. *The mapping defined by equation 3.2.3 defines an inner product in $L^2(G)$.*

Proof. This time, there is no doubt that $\langle f, g \rangle$ is in $\mathbb{C}$ since we are dealing with finite sums. To be an inner product, $\langle *, * \rangle$ must satisfy these four properties for all $f, g, h \in L^2(G)$ and $\alpha, \beta \in \mathbb{C}$: 1)$\langle f, g \rangle = \overline{\langle g, f \rangle}$, 2) $\langle \alpha f + \beta g, h \rangle = \alpha \langle f, h \rangle + \beta \langle g, h \rangle$, 3) $\langle f, f \rangle \geq 0$, 4) $\langle f, f \rangle = 0 \iff f = 0$.

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

Second,

$$\begin{aligned}\langle \alpha f + \beta g, h \rangle &= \frac{1}{|G|} \sum_{a \in G} (\alpha f(a) + \beta g(a))\overline{h(a)} \\ &= \frac{1}{|G|} \sum_{a \in G} \alpha f(a)\overline{h(a)} + \beta g(a)\overline{h(a)} \\ &= \frac{1}{|G|} \sum_{a \in G} \alpha f(a)\overline{h(a)} + \frac{1}{|G|} \sum_{a \in G} \beta g(a)\overline{h(a)} \\ &= \frac{1}{|G|} \alpha \sum_{a \in G} f(a)\overline{h(a)} + \frac{1}{|G|} \beta \sum g(a)\overline{h(a)} \\ &= \alpha \langle f, h \rangle + \beta \langle g, h \rangle\end{aligned}$$

Third, $\langle f, f\rangle = \frac{1}{|G|}\sum_{a\in G} f(a)\overline{f(a)} \geq 0$

Fourth, assume $\langle f, f\rangle = 0$. Since $\frac{1}{|G|}\sum_{a\in G} f(a)\overline{f(a)}$ is simply adding up positive real numbers, if $\langle f, f\rangle = 0$, this has to imply that $|f(a)| = 0$ for all a in G. But this implies that $f(a) = 0$ for all a in G. Assume $f(a) = 0$ for all $a \in G$. Then $\frac{1}{|G|}\sum_{a\in G} f(a)\overline{f(a)} = 0 + 0 + \cdots + 0 = 0$. Thus, $\langle f, f\rangle = 0$ if and only if $f(a) = 0$ for all a in G.

Thus, $\langle *, *\rangle$ defines an inner product on $L^2(G)$. □

Definition 30. For any $f \in L^2(G)$, the **induced norm** is defined as

$$\| f \|_{L^2(G)} = \sqrt{\langle f, f\rangle} = \sqrt{\frac{1}{|G|}\sum_{a\in G} f(a)\overline{f(a)}} \tag{3.2.4}$$

Lemma 31. *The set $\{\delta_a\}_{a\in G}$ form an orthonormal basis for $L^2(G)$.*

Proof. We have already shown that $\{\delta_a\}_{a\in G}$ form a basis for $L^2(G)$. We need only show that $\{\delta_a\}_{a\in G}$ are orthonormal.

Let us first assume $a_j, a_k \in G$ and $j \neq k$. Then

$$\begin{aligned}
\langle \delta_{a_j}, \delta_{a_k}\rangle &= \frac{1}{|G|}\sum_{a\in G} \delta_{a_j}(a)\overline{\delta_{a_k}(a)} \\
&= 0 \times 0 + 0 \times 0 + \cdots + \delta_{a_j}(a_j) \times 0 + \cdots + 0 \times \overline{\delta_{a_k}(a_k)} + \cdots + 0 \times 0 \\
&= 0
\end{aligned}$$

Next, let us assume $a_j, a_k \in G$ and $j = k$. Then

$$\begin{aligned}
\langle \delta_{a_j}, \delta_{a_k}\rangle &= \frac{1}{|G|}\sum_{a\in G} \delta_{a_j}(a)\overline{\delta_{a_j}(a)} \\
&= \frac{1}{|G|}[0 \times 0 + 0 \times 0 + \cdots + \delta_{a_j}(a_j) \times \overline{\delta_{a_j}(a_j)} + \cdots + 0 \times 0] \\
&= \frac{1}{|G|} \times \sqrt{|G|} \times \overline{\sqrt{|G|}} \\
&= 1
\end{aligned}$$

Thus, by definition, $\{\delta_a\}_{a\in G}$ form an orthonormal basis for $L^2(G)$. □

Remark. The $L^2 - norm$ is not the only norm associated with our group. For any $p \geq 1$, we can define the $L^p - norm$ as

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

We have now built a group analog to the Schwarz class. The next step will be to find functions that can take the place of the trigonometric functions used in classical Fourier analysis.

3.3 Characters, Dual Group $\widehat{G}$, and $L^2(\widehat{G})$

In our Fourier analysis on groups, characters will play a role analogous to the role of trigonometric functions in classical Fourier analysis. The characters will map elements from G into the unit circle, just like the trigonometric functions take elements from $\mathbb{R}$ into the unit circle in $\mathbb{C}$. The characters form another group, the dual group, $\widehat{G}$. In this section, we will also define an inner product and an induced norm in the space $L^2(\widehat{G})$. Finally we will prove some additional lemmas for the characters needed to build the Fourier theory on groups.

Definition 32. A **character** of G is a group homomorphism $\chi : G \to S^1$, where S^1 denotes the unit circle, i.e. $S^1 = \{z \in \mathbb{C} : |z| = 1\}$.

Definition 33. χ is a **group homomorphism** if for all $a, b \in G$, $\chi(a+b) = \chi(a)\chi(b)$.

Lemma 34. *The set of characters, denoted by $\widehat{G}$, is a group with the binary operation $(\chi_1\chi_2)(a) = \chi_1(a)\chi_2(a)$ for all $\chi_1, \chi_2 \in \widehat{G}$ and $a \in G$.*

Proof. 1) We first need to show that $\widehat{G}$ is closed under our binary operation. Take any two elements $\chi_1, \chi_2 \in \widehat{G}$. Then $\chi_1\chi_2(a) = \chi_1(a)\chi_2(a)$, but $\chi_1(a)$ and $\chi_2(a)$ are in S^1, and any two elements in S^1, when multiplied together, produce another element in S^1. Furthermore, $\chi_1\chi_2$ is a character since $\chi_1\chi_2(a+b) = \chi_1(a+b)\chi_2(a+b)$ by the definition of our binary operation. Indeed, since χ_1 and χ_2 are group homomorphisms, $\chi_1(a+b)\chi_2(a+b) = \chi_1(a)\chi_1(b)\chi_2(a)\chi_2(b)$. Because $\chi_1(a)$ and $\chi_2(b)$ are elements of $\mathbb{C}$ for all a, b in G, and because we know that multiplication is commutative in $\mathbb{C}$, we can write $\chi_1(a)\chi_1(b)\chi_2(a)\chi_2(b) = \chi_1(a)\chi_2(a)\chi_1(b)\chi_2(b) = \chi_1\chi_2(a)\chi_1\chi_2(b)$. So $\chi_1\chi_2(a+b) = \chi_1\chi_2(a)\chi_1\chi_2(b)$, which implies that $\chi_1\chi_2$ is a group homomorphism. Thus, our group $\widehat{G}$ is closed under our binary operation.

2. We now must show that our binary operation is associative. Let $\chi_1, \chi_2, \chi_3 \in \widehat{G}$ and $a \in G$.

$$\begin{aligned}((\chi_1\chi_2)(\chi_3))(a) =& (\chi_1\chi_2)(a)\chi_3(a)\\ =& \chi_1(a)\chi_2(a)\chi_3(a)\\ =& \chi_1(a)(\chi_2\chi_3)(a)\\ =& (\chi_1(\chi_2\chi_3))(a)\end{aligned}$$

3. We now need an identity element in $\widehat{G}$. Let us define $\chi_0(a) = 1\ \forall a \in G$. This element is in S^1 since $1 \in S^1$. It is also a group homomorphism since $\chi_0(a+b) = 1 = 1\times 1 = \chi_0(a)\chi_0(b)$. For any $\chi \in G$, $(\chi\chi_0)(a) = \chi(a)\chi_0(a) = \chi(a) \times 1 = \chi(a)$. Similarly $(\chi_0\chi)(a) = \chi(a)$. Thus, χ_0 is an identity element for $\widehat{G}$.

4. We will note that, for any $\chi \in \widehat{G}$, $\chi(0) = 1$: Note that $\chi(a) \neq 0$ for any a in G since χ maps elements onto the unit circle. Therefore, for any a in G, $\chi(a)\chi(0) = \chi(a+0) = \chi(a)$. Since we know $\chi(a) \neq 0$, we can use the cancellation law, and we get that $\chi(0) = 1$.

5. We also need an inverse for each element in $\widehat{G}$. Define $\chi^{-1}(a) = \chi(-a)$, for all $a \in G$. Since $-a \in G$, our new element χ^{-1} will be in S^1 since $\chi : G \to S^1$. This element is also a group homomorphism: if we consider $\chi^{-1}(a+b) = \chi((a+b)^{-1}) = \chi(-a-b)$. But

$\chi(-a-b) = \chi(-a)\chi(-b) = \chi^{-1}(a)\chi^{-1}(b)$. So χ^{-1} is in fact a group homomorphism. We now need to show that χ^{-1} is actually an inverse element. Consider $(\chi^{-1}\chi)(a) = \chi^{-1}(a)\chi(a) = \chi(-a)\chi(a) = \chi(-a+a) = \chi(0) = 1$. Similarly, we can show $(\chi\chi^{-1})(a) = 1$.

Numbers 1 through 5 imply that $\widehat{G}$ is indeed a group. $\widehat{G}$ is called the **dual group** of G. □

Example 35. If our group is equal to $\mathbb{Z}_n$, then the dual group can be identified with U_n, the n^{th} roots of unity. For $n = 3$, we can create multiplication tables for $\mathbb{Z}_3$ and U_3, as well as a character table:

For $\mathbb{Z}_3$, the multiplication table is as follows:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

A similar multiplication table is shown for U_3 :

*	1	$e^{2\pi i/3}$	$e^{4\pi i/3}$
1	1	$e^{2\pi i/3}$	$e^{4\pi i/3}$
$e^{2\pi i/3}$	$e^{2\pi i/3}$	$e^{4\pi i/3}$	1
$e^{4\pi i/3}$	$e^{4\pi i/3}$	1	$e^{2\pi i/3}$

Notice that the above group tables have the same structure. In fact, $\mathbb{Z}_3 \simeq U_3$. To see how the each character acts on each element of the group, we have a character table:

*	0	1	2
χ_0	1	1	1
χ_1	1	$e^{2\pi i/3}$	$e^{4\pi i/3}$
χ_2	1	$e^{4\pi i/3}$	$e^{2\pi i/3}$

The multiplication table for the characters of $\mathbb{Z}_3$ follows:

*	χ_0	χ_1	χ_2
χ_0	χ_0	χ_1	χ_2
χ_1	χ_1	χ_2	χ_0
χ_2	χ_2	χ_0	χ_1

Example 36. We can also create a character table for the Klein 4-group [1]:

*	e	a	b	ab
χ_0	1	1	1	1
χ_1	1	-1	1	-1
χ_2	1	-1	-1	1
χ_3	1	1	-1	-1

From this character table, we can build the multiplication table for the characters of the Klein 4-group as well:

$*$	χ_0	χ_1	χ_2	χ_3
χ_0	χ_0	χ_1	χ_2	χ_3
χ_1	χ_1	χ_0	χ_3	χ_2
χ_2	χ_2	χ_3	χ_0	χ_1
χ_3	χ_3	χ_2	χ_1	χ_0

Remark. In the two examples above, we observed that $G \simeq \widehat{G}$. This is not just a coincidence. For finite abelian groups, it is true that $G \simeq \widehat{G}$, [12, Theorem 1.4]. Because of this fact, we can then relate elements in G to elements in $\widehat{G}$. For every a in G, we can relate a to a χ_a in $\widehat{G}$. In general, there is no canonical isomorphism between the G and $\widehat{G}$.

Now that we have another group, we will need to define a similar space to $L^2(G)$, called $L^2(\widehat{G})$, which will be the space of functions from $\widehat{G}$ to $\mathbb{C}$. This space is called the dual space of $L^2(G)$. We can show in a similar way to what we did with $L^2(G)$ that $L^2(\widehat{G})$ is an inner-product vector space, so we will therefore need to define the inner product and induced norm of $L^2(\widehat{G})$.

Definition 37. We will also define an **inner product** in $L^2(\widehat{G})$, for $\widehat{f}, \widehat{g} \in \widehat{G}$, as:

$$\langle \widehat{f}, \widehat{g} \rangle := \sum_{\chi \in \widehat{G}} \widehat{f}(\chi)\overline{\widehat{g}(\chi)} \tag{3.3.1}$$

Definition 38. The **induced norm** in $L^2(\widehat{G})$ is defined as:

$$\| \widehat{f} \|_{L^2(\widehat{G})} := \sqrt{\sum_{\chi \in \widehat{G}} \widehat{f}(\chi)\overline{\widehat{f}(\chi)}} \tag{3.3.2}$$

Remark. We can similarly define an $L^p - norm$ for the space $L^p(\widehat{G})$ as

$$\| \widehat{f} \|_{L^p(\widehat{G})} = \left(\sum_{\xi \in \widehat{G}} |\widehat{f}(\xi)|^p \right)^{\frac{1}{p}}$$

Remark. Note that we do not normalize the inner product nor the L^p-norms.

Remark. We can define conjugation in $\widehat{G}$ by $\overline{\chi}(a) = \overline{\chi(a)}$. Since $\chi(a) \in S^1$, we know that $\chi^{-1}(a) = \overline{\chi(a)}$.

The next few lemmas will give us some building blocks so we can later define things like the Fourier transform and the Fourier Inversion Formula.

Lemma 39. *If* $\chi \in \widehat{G}$, *then* $\sum_{a\in G}\chi(a) = \begin{cases} 0 & \chi \neq \chi_0 \\ n & \chi = \chi_0 \end{cases}$ *where* $n = |G|$.

Proof. [6]: First, let us assume $\chi = \chi_0$. Then $\sum_{a\in G}\chi(a) = \sum_{a\in G}\chi_0(a) = \sum_{a\in G}(1) = n$. Next, let us assume $\chi \neq \chi_0$; hence, there exists $a_0 \in G$ such that $\chi(a_0) \neq 1$. If we let the b be the arbitrary element $b = a_0 + a$ for any a in G, then

$$\begin{aligned} \chi(a_0)\sum_{a\in G}\chi(a) &= \sum_{a\in G}\chi(a_0+a) \\ &= \sum_{b\in G}\chi(b) \end{aligned}$$

Since $\chi(a_0) \neq 1$, then $\sum_{a\in G}\chi(a) = 0$. □

Lemma 40. *If* $a \in G$, *then* $\sum_{\chi\in\widehat{G}}\chi(a) = \begin{cases} 0 & a \neq 0 \\ n & a = 0 \end{cases}$ *where* $n = |\widehat{G}|$.

Proof. First, let us assume $a = 0$. Then $\sum_{\chi\in\widehat{G}}\chi(a) = \sum_{\chi\in\widehat{G}}\chi(0) = \sum_{\chi\in\widehat{G}}1 = n$. Next, let us assume $a \neq 0$, then there exists $\chi_1 \in \widehat{G}$ such that $\chi_1(a) \neq 1$. Then

$$\begin{aligned} \chi_1(a)\sum_{\chi\in\widehat{G}}\chi(a) &= \sum\chi_1(a)\chi(a) \\ &= \sum_{\chi\in\widehat{G}}(\chi_1\chi)(a) \end{aligned}$$

Let β be the arbitrary element $\beta = \chi_1\chi$ for any $\chi \in \widehat{G}$. Then

$$\chi_1(a)\sum_{\chi\in\widehat{G}}\chi(a) = \sum_{\beta\in\widehat{G}}\beta(a)$$

Since $\chi_1(a) \neq 1$, this implies that$\sum_{\chi\in\widehat{G}}\chi(a) = 0$. □

Lemma 41. *If* $\chi_1, \chi_2 \in \widehat{G}$, *then* $\sum_{a\in G}\chi_1(a)\overline{\chi_2(a)} = \begin{cases} 0 & \chi_1 \neq \chi_2 \\ n & \chi_1 = \chi_2 \end{cases}$ *where* $n = |G|$.

Proof. [6]: First, let us assume $\chi_1 = \chi_2$. This implies $\chi_1\overline{\chi_2} = \chi_0$. We can then appeal to Lemma 39, which implies $\sum_{a\in G}\chi_1(a)\overline{\chi_2(a)} = n$. Now, we will assume $\chi_1 \neq \chi_2$. Since inverses in groups are unique, we know that $\chi_1\overline{\chi_2} \neq \chi_0$. Again, by Lemma 39, this implies $\sum_{a\in G}\chi_1(a)\overline{\chi_2(a)} = 0$. □

Lemma 42. *If* $a, b \in G$, *then* $\sum_{\chi\in\widehat{G}}\chi(a)\overline{\chi}(b) = \begin{cases} 0 & a \neq b \\ n & a = b \end{cases}$ *where* $n = |\widehat{G}|$.

Proof. First, let us note that $\chi(a)\overline{\chi}(b) = \chi(a)\chi(-b) = \chi(a-b)$. We will first consider the case where $a = b$. Then $\chi(a)\overline{\chi}(b) = \chi(a-b) = \chi(0)$. By Lemma 40, this implies $\sum_{\chi\in\widehat{G}}\chi(a)\overline{\chi}(b) = n$. Next, we will consider the case where $a \neq b$. Since inverses in groups are unique, $a - b \neq 0$, so by Lemma 40 again, $\sum_{\chi\in\widehat{G}}\chi(a)\overline{\chi}(b) = 0$. □

3.4 Fourier Transforms

We are now ready to actually define the Fourier transform on our group. In addition, we will prove the analogs to well-known theorems in classical Fourier analysis like the Fourier Inversion Formula and Plancherel's Identity.

Definition 43. The **Fourier transform** of $f \in L^2(G)$ is the function $\widehat{f} \in L^2(\widehat{G})$, defined as the inner product with a character in $\widehat{G}$, that is:

$$\widehat{f}(\chi) = \langle f, \chi \rangle = \frac{1}{|G|} \sum_{a \in G} f(a)\overline{\chi}(a) \tag{3.4.1}$$

Lemma 44. *The Fourier transform as defined by equation 3.4.1 is linear.*

Proof. For $\alpha, \beta \in \mathbb{C}$, $f, g \in G$, and $\chi \in \widehat{G}$,

$$\begin{aligned}
\widehat{\alpha f + \beta g}(\chi) &= \frac{1}{|G|} \sum_{a \in G} (\alpha f(a) + \beta g(a))\overline{\chi(a)} \\
&= \frac{1}{|G|} \sum_{a \in G} \alpha f(a)\overline{\chi(a)} + \frac{1}{|G|} \sum_{a \in G} \beta g(a)\overline{\chi(a)} \\
&= \alpha \frac{1}{|G|} \sum_{a \in G} f(a)\overline{\chi(a)} + \beta \frac{1}{|G|} \sum_{a \in G} g(a)\overline{\chi(a)} \\
&= \alpha \widehat{f}(\chi) + \beta \widehat{g}(\chi)
\end{aligned}$$

□

Just as in classical Fourier analysis, the Fourier transform forms a bijection from G to $\widehat{G}$. We can use this fact to prove the Fourier Inversion Formula.

Theorem 45. (Fourier Inversion Formula): *If $f \in L^2(G)$, then $f = \sum_{\chi \in \widehat{G}} \widehat{f}(\chi)\chi$.*

Proof. [6]: From Lemma 42, we can see that $\sum_{\chi \in \widehat{G}} \chi(b)\overline{\chi(a)} = \sqrt{n}\delta_a(b)$ for $a, b \in G$. By equation 3.2.1, we know

$$\begin{aligned}
f(x) =& \frac{1}{\sqrt{n}} \sum_{a \in G} f(a)\delta_a(x) \\
=& \frac{1}{\sqrt{n}} \sum_{a \in G} f(a) \frac{1}{\sqrt{n}} \sum_{\chi \in \widehat{G}} \chi(x)\overline{\chi(a)} \\
=& \frac{1}{n} \sum_{a \in G} \sum_{\chi \in \widehat{G}} f(a)\chi(x)\overline{\chi(a)} \\
=& \sum_{\chi \in \widehat{G}} \frac{1}{n} \sum_{a \in G} f(a)\overline{\chi(a)}\chi(x) \\
=& \sum_{\chi \in \widehat{G}} \widehat{f}(\chi)\chi(x)
\end{aligned}$$

□

Theorem 46. (Plancherel's Identity): *If $f \in L^2(G)$ and $|G| = n$, then* $\| f \|_{L^2(G)} = \| \widehat{f} \|_{L^2(\widehat{G})}$.

Proof. Consider

$$\begin{aligned}
\| \widehat{f} \|_{L^2(\widehat{G})} &= \sqrt{\sum_{\chi \in \widehat{G}} \widehat{f}(\chi)\overline{\widehat{f}(\chi)}} \\
&= \sqrt{\sum_{\chi \in \widehat{G}} (\frac{1}{n} \sum_{a \in G} f(a)\overline{\chi(a)})(\frac{1}{n} \sum_{b \in G} \overline{f(b)\overline{\chi(b)}})} \\
&= \sqrt{\sum_{\chi \in \widehat{G}} \frac{1}{n} \sum_{a \in G} f(a)\overline{\chi(a)} \frac{1}{n} \sum_{b \in G} \overline{f(b)}\chi(b)} \\
&= \frac{1}{n} \sqrt{\sum_{\chi \in \widehat{G}} \sum_{a \in G} \sum_{b \in G} f(a)\overline{f(b)\chi(a)}\chi(b)}
\end{aligned}$$

By Lemma 42, we know that $\sum_{\chi \in \widehat{G}} \overline{\chi(a)}\chi(b) = 0$ unless $a = b$, then it equals n. Thus

$$\begin{aligned}
\| \widehat{f} \|_{L^2(\widehat{G})} &= \frac{\sqrt{n}}{n} \sqrt{\sum f(a)\overline{f(a)}} \\
&= \| f \|_{L^2(G)}
\end{aligned}$$

□

In the next couple of subsections, we will partially build the time-frequency dictionary for our Fourier group theory.

3.4.1 Translation

Definition 47. We will define the **translation** by $a \in G$ of the function $f \in L^2(G)$ by

$$\tau_a f(x) = f(x - a) \tag{3.4.2}$$

Lemma 48. *For $a \in G$ and $f \in L^2(G)$, $\widehat{\tau_a f}(\chi) = \overline{\chi(a)}\widehat{f}(\chi)$.*

Proof. Consider

$$\begin{aligned}
\widehat{\tau_a f}(\chi) &= \sum_{x \in G} \tau_a f(x)\overline{\chi(x)} \\
&= \sum_{x \in G} f(x - a)\overline{\chi(x)}\chi(-a)\overline{\chi(-a)} \\
&= \big(\sum_{x \in G} f(x - a)\overline{\chi(x - a)} \big)\chi(-a) \\
&= \chi(-a)\widehat{f}(\chi) \\
&= \overline{\chi(a)}\widehat{f}(\chi)
\end{aligned}$$

□

3.4.2 Convolution

Definition 49. For $f, g \in L^2(G)$, we will define **convolution** as

$$(f * g)(x) = \sum_{a \in G} \tau_{-x} f(-a) g(a) \tag{3.4.3}$$

Lemma 50. *The convolution as defined in equation 3.4.3 is commutative.*

Proof. Consider

$$(f * g)(x) = \sum_{a \in G} f(x-a) g(a)$$

Let $x - a = b$, then $a = x - b$. Then

$$\begin{aligned}(f * g)(x) &= \sum_{b \in G} f(b) g(x-b) \\ &= (g * f)(x)\end{aligned}$$

□

Lemma 51. *For $f, g \in L^2(G)$ $\widehat{f * g} = \widehat{f}\widehat{g}$.*

Proof. Consider

$$\begin{aligned}\widehat{f * g}(\chi) &= \sum_{x \in G} (f * g)(x) \overline{\chi(x)} \\ &= \sum_{x \in G} \big(\sum_{a \in G} f(x-a) g(a) \big) \chi(x)\end{aligned}$$

Note that $\chi(x) = \chi(a)\chi(x-a)$. Let $b = x - a$. Then we get

$$\begin{aligned}\widehat{f * g}(\chi) &= \sum_{b \in G} \sum_{a \in G} f(b) g(a) \chi(a) \chi(b) \\ &= \big(\sum_{b \in G} f(b) \chi(b) \big) \big(\sum_{a \in G} g(a) \chi(a) \big) \\ &= \widehat{f}(\chi) \widehat{g}(\chi)\end{aligned}$$

□

3.4.3 Modulation

Definition 52. The **modulation** of a function $f \in L^2(G)$ by $\alpha \in \widehat{G}$ is defined as $M_\alpha f(x) = \alpha(x) f(x)$.

Lemma 53. *For $f \in L^2(G)$ and $\alpha \in \widehat{G}$, $\widehat{M_\alpha f}(\xi) = \widehat{f}(\alpha^{-1}\xi)$.*

Proof. Recall that for any $\xi, \alpha \in \widehat{G}$, $\xi^{-1} = \overline{\xi}$ and $(\alpha\xi)^{-1} = \alpha^{-1}\xi^{-1}$ since we are dealing with an abelian group. We will use these facts in the following list of equalities:

$$\begin{aligned}
\widehat{M_\alpha f}(\xi) &= \frac{1}{|G|}\sum_{x\in G}\alpha(x)f(x)\overline{\xi(x)} \\
&= \frac{1}{|G|}\sum_{x\in G}f(x)\alpha(x)\xi^{-1}(x) \\
&= \frac{1}{|G|}\sum_{x\in G}f(x)(\alpha\xi^{-1}(x)) \\
&= \frac{1}{|G|}\sum_{x\in G}f(x)\overline{(\alpha^{-1}\xi)(x)} \\
&= \widehat{f}(\alpha^{-1}\xi)
\end{aligned}$$

□

Remark. Note that, because the binary operation in $\widehat{G}$ is multiplication, we can define the translation by $\alpha \in \widehat{G}$ of $\widehat{f} \in L^2(\widehat{G})$ as $\tau_\alpha\widehat{f}(\xi) = \widehat{f}(\xi\alpha^{-1})$. With this definition, and the one for modulation, we can rewrite Lemma 48 as $\widehat{\tau_a f}(\xi) = M_{-a}\widehat{f}(\xi)$ and Lemma 53 as $\widehat{M_\alpha f}(\xi) = \tau_\alpha\widehat{f}(\xi)$.

Chapter 4

Uncertainty Principles

Now that we have the basic building blocks in both group and classical Fourier theory, we can prove both versions of the uncertainty principle. While the classical and discrete versions of the uncertainty principles look quite different, they actually both encode information about the supports of functions in space and frequency. In this section, we will also identify the extremal functions which change the inequalities to equalities in both settings.

4.1 Uncertainty Principle in $\mathbb{R}$

The Heisenberg Uncertainty Principle was proved by Werner Heisenberg, a German theoretical physicist, in 1927. The uncertainty principle says that it is impossible to know a subatomic particle's position and momentum at the same time. The more precisely the position of a particle is known, the less precisely the momentum can be known, and vice versa. Here is the mathematical statement of Heisenberg's Uncertainty Principle:

Theorem 54. *(Heisenberg Uncertainty Principle): Suppose that $\psi \in \mathcal{S}(\mathbb{R})$ and that ψ is normalized in $L^2(\mathbb{R})$, i.e. $\| \psi \|_2 = 1$. Then*

$$\left(\int_{\mathbb{R}} x^2 |\psi(x)|^2 dx \right) \left(\int_{\mathbb{R}} \xi^2 |\hat{\psi}(\xi)|^2 d\xi \right) \geq 1/(16\pi^2).$$

Proof. [14]: We know that $\| \psi \|_2 = 1$. By the definition of the L^2-norm, this implies $\int_{\mathbb{R}} |\psi(x)|^2 dx = 1$. If we use integration by parts, with $u = |\psi(x)|^2$ and $dv = dx$, we get that $v = x$ and

$$\begin{aligned} du &= \frac{d}{dx}(|\psi(x)|^2) \\ &= \frac{d}{dx}(\psi(x)\overline{\psi(x)}) \\ &= \psi'(x)\overline{\psi(x)} + \psi(x)\overline{\psi'(x)} \\ &= \psi'(x)\overline{\psi(x)} + \overline{\psi'(x)\overline{\psi(x)}} \\ &= 2Re(\psi'(x)\overline{\psi(x)}) \end{aligned}$$

Using the formula for integration by parts, we get that

$$1 = (|\psi(x)|^2 x)|_{-\infty}^{\infty} - \int_{\mathbb{R}} 2xRe\big(\psi'(x)\overline{\psi(x)}\big)dx.$$

Since $\psi \in \mathcal{S}(\mathbb{R})$, $(|\psi(x)|^2 x)|_{-\infty}^{\infty} = 0$, so we are left with

$$1 = -\int_{\mathbb{R}} 2xRe(\psi'(x)\overline{\psi(x)}dx \tag{4.1.1}$$

Since $|\ z\ | \geq |Re(z)|$ and since $|\int f| \leq \int |f|$, we can rewrite equation (4.1.1) as

$$1 \leq 2\int_{\mathbb{R}} |x||\psi(x)||\psi'(x)|dx \tag{4.1.2}$$

By the Cauchy-Schwarz Inequality, Lemma 5, equation 4.1.2 becomes

$$1 \leq 2\left(\int_{\mathbb{R}} x^2|\psi(x)|^2dx\right)^{\frac{1}{2}}\left(\int_{\mathbb{R}} |\psi'(x)|^2dx\right)^{\frac{1}{2}}$$

By Plancherel's Identity, Theorem 16, we get

$$1 \leq 2\left(\int_{\mathbb{R}} |x\psi(x)|^2dx\right)^{\frac{1}{2}}\left(\int_{\mathbb{R}} |\widehat{\psi'}(\xi)|^2d\xi\right)^{\frac{1}{2}} \tag{4.1.3}$$

From Lemma 9, we know that $\widehat{M'}(\xi) = (2\pi i\xi)\widehat{M}(\xi)$. Thus, equation 4.1.3 becomes

$$1 \leq 2\left(\int_{\mathbb{R}} |x\psi(x)|^2dx\right)^{\frac{1}{2}}\left(\int_{\mathbb{R}} |4\pi^2\xi^2||\widehat{\psi}(\xi)|^2d\xi\right)^{\frac{1}{2}} \tag{4.1.4}$$

Squaring both sides of equation 4.1.4 yields

$$1 \leq 4\left(\int_{\mathbb{R}} |x\psi(x)|^2dx\right)4\pi^2\left(\int_{\mathbb{R}} |\xi\widehat{\psi}(\xi)|^2d\xi\right)$$

This implies

$$\frac{1}{16\pi^2} \leq \left(\int_{\mathbb{R}} |x\psi(x)|^2dx\right)\left(\int_{\mathbb{R}} |\xi\widehat{\psi}(\xi)|^2d\xi\right)$$

□

4.2 Uncertainty Principle in G

We will now present an analog to the Heisenberg Uncertainty Principle for finite abelian groups. Before we do that, though, we must first define the support of a function.

Definition 55. For a function f in $L^2(G)$, the **support** of f, denoted supp$f$, is the set of all a in G such that $f(a) \neq 0$. We denote the cardinality of the support by $|\text{supp}f|$. We can similarly define the support of a function $\widehat{f}$ in $\widehat{G}$ as the set of all $\chi \in \widehat{G}$ such that $\widehat{f}(\chi) \neq 0$.

Theorem 56. *(Discrete Uncertainty Principle): For $f \in L^2(G)$, $|suppf|\ |supp\widehat{f}| \geq |G|$.*

Proof. [6]: By the Fourier Inversion Formula, Theorem 45, we know that for all $a \in G$

$$f(a) = \sum_{\chi \in \widehat{G}} \widehat{f}(\chi)\chi(a)$$

This implies that

$$|f(a)| = |\sum_{\chi \in \widehat{G}} \widehat{f}(\chi)\chi(a)|$$

Since $\chi(a)$ is an element of S^1 for all $a \in G$ and $\chi \in \widehat{G}$, then $|\chi(a)| = 1$. Using this fact and the triangle inequality, we get that

$$|f(a)| \leq \sum_{\chi \in \widehat{G}} |\widehat{f}(\chi)||\chi(a)| = \sum_{\chi \in \widehat{G}} |\widehat{f}(\chi)| \tag{4.2.1}$$

By the definition of the Fourier transform, equation 3.4.1, and the triangle inequality, we know

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

Let $N = \max_{a \in G} |f(a)|$. We can then say

$$\sum_{a \in G} |f(a)| \leq |\text{supp}f| \times N \tag{4.2.2}$$

Thus, for all $\chi \in \widehat{G}$,

$$|\widehat{f}(\chi)| \leq \frac{1}{|G|} |\text{supp}f| \times N$$

Substituting this into equation 4.2.1, we get

$$|f(a)| \leq \sum_{\chi \in \widehat{G}} \frac{1}{|G|} |\text{supp}f| \times N = \frac{1}{|G|} \times |\text{supp}\widehat{f}| \times |\text{supp}f| \times N \tag{4.2.3}$$

Since equation 4.2.1 applied to every $a \in G$, it will apply to $a' \in G$ such that $f(a') = N$. Combining equation 4.2.1 and equation 4.2.3, we get

$$N \leq \frac{1}{|G|} \times |\text{supp}\widehat{f}| \times |\text{supp}f| \times N$$

Rearranging and canceling, we get

$$|\text{supp}\widehat{f}| \times |\text{supp}f| \geq |G|$$

□

In this context, it is clear that both the supports of f and $\widehat{f}$ cannot be too small since the product of their cardinalities must be greater than or equal to the order of the group G.

4.3 The "Gaussians"

In Fourier analysis in both $\mathbb{R}$ and G, there are specific functions that give us sharpness in the uncertainty principle. In classical Fourier analysis, these functions are Gaussians, while in the group setting, they are the translations, modulations, and scalar multiples of the indicator functions of subgroups of G. These are the functions for which equality is attained in the inequalities; these functions are also called extremal functions.

4.3.1 The Gaussians in $\mathbb{R}$

Recall that a Gaussian is a function of the form $G_a(x) = e^{-ax^2}$. Before we prove that the classical version of the uncertainty principle is an equality if and only if our function is a Gaussian, we first need to recall some preliminary calculations.

Lemma 57. *The integral* $\int_{\mathbb{R}} e^{-ax^2}dx = \sqrt{\frac{\pi}{a}}$.

Proof. Consider $\left(\int_{\mathbb{R}} e^{-ax^2}dx\right)^2 = \left(\int_{\mathbb{R}} e^{-ax^2}dx\right)\left(\int_{\mathbb{R}} e^{-ay^2}dy\right) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} e^{-a(x^2+y^2)}dxdy$. Changing this integral to polar coordinates, we get

$$\begin{aligned}\left(\int_{\mathbb{R}} e^{-ax^2}dx\right)^2 &= \int_0^{2\pi}\int_0^{\infty} e^{-ar^2}rdrd\theta \\ &= \int_0^{2\pi}\left(-\frac{1}{2a}[e^{-\infty}-e^0]\right) \\ &= \frac{\pi}{a}\end{aligned}$$

Thus, $\int_{\mathbb{R}} e^{-ax^2}dx = \sqrt{\frac{\pi}{a}}$.

In particular, this calculation shows that $\| G_a \|_{L^2(\mathbb{R})} = \left(\int_{\mathbb{R}} e^{-ax^2}dx\right)^{\frac{1}{2}} = (\frac{\pi}{a})^{\frac{1}{4}}$. If $a = \pi$, then $\| G_\pi \|_{L^2(\mathbb{R})} = 1$. □

Lemma 58. *The integral* $\int_{\mathbb{R}} x^2e^{-ax^2}dx = \frac{\sqrt{\pi}}{2a^{3/2}}$.

Proof. Let us evaluate the above integral using integration by parts, letting $u = x$ and $dv = xe^{-ax^2}dx$. We then get that $du = dx$ and $v = -\frac{1}{2a}e^{-ax^2}$. Using the formula for integration by parts, we get $\int_{\mathbb{R}} x^2e^{-ax^2}dx = -\frac{1}{2a}xe^{-ax^2}|_{-\infty}^{\infty} + \frac{1}{2a}\int_{\mathbb{R}} e^{-ax^2}dx$. Using L'Hopital's rule, $\lim_{x\to\pm\infty} -xe^{-ax^2} = \lim_{x\to\pm\infty}\frac{1}{xe^{ax^2}} = 0$. Thus, $-\frac{1}{2a}xe^{-ax^2}|_{-\infty}^{\infty} = 0$. We know from Lemma 57 that $\int_{\mathbb{R}} e^{-ax^2} = \sqrt{\frac{\pi}{a}}$, so $\int_{\mathbb{R}} x^2e^{-x^2}dx = \frac{\sqrt{\pi}}{2a^{3/2}}$. □

Lemma 59. *The Fourier transform of a Gaussian is another Gaussian.*

Proof. Consider the Gaussian function $G_B(x) = e^{-Bx^2}$. Then

$$\begin{aligned}\widehat{G_B}(\xi) &= \int_{\mathbb{R}} \sqrt{2B/\pi}e^{-Bx^2}e^{-2\pi ix\xi}dx \\ &= \int_{\mathbb{R}} \sqrt{2B/\pi}e^{-B(x^2+2\pi ix\xi/B)}dx\end{aligned}$$

Completing the square of $x^2 + 2\pi ix\xi/B$ gives us $(x + \frac{\pi i\xi}{B})^2 + (\frac{\pi\xi}{B})^2$. Our integral then becomes

$$\begin{aligned}\widehat{G_B}(\xi) &= \int_{\mathbb{R}} e^{-\pi^2\xi^2/B} e^{-B(x+\pi i\xi/B)^2} dx \\ &= e^{-\pi^2\xi^2/B} \int_{\mathbb{R}} e^{-B(x+\pi i\xi/B)^2} dx\end{aligned}$$

By Lemma 57, we can conclude that $\int_{\mathbb{R}} e^{-B(x+\pi i\xi/B)^2} dx = \frac{1}{\sqrt{B}}\sqrt{\pi}$. Thus, $\widehat{G_B}(\xi) = e^{-\pi^2\xi^2/B}\sqrt{\frac{\pi}{B}}$. But this is simply another Gaussian with a constant in front of it. Thus, the Fourier transform of a Gaussian is a Gaussian. □

Theorem 60. *The uncertainty principle, Theorem 54, is sharp if and only if* $\psi(x) = \sqrt{2B/\pi}e^{-Bx^2}$ *for some* $B > 0$.

Proof. ($\Longleftarrow$) Assume $\psi(x) = \sqrt{2B/\pi}G_B(x)$. From Lemma 59, we know that

$$\begin{aligned}\widehat{\psi}(\xi) &= \sqrt{2B/\pi}e^{-\pi^2\xi^2/B}\sqrt{\pi/B} \\ &= \sqrt{2}e^{-\pi^2\xi^2/B}\end{aligned}$$

Plugging our values of $\psi(x)$ and $\widehat{\psi}(\xi)$ into the left hand side of Theorem 54 and using Lemma 58, we get

$$\left(\int_{\mathbb{R}} \frac{2B}{\pi} x^2 e^{-2Bx^2} dx\right)\left(\int_{\mathbb{R}} 2\xi^2 e^{-2\pi^2\xi^2/B} d\xi\right) = \frac{2B}{\pi}\frac{\sqrt{\pi}}{2(2B)^{3/2}}\frac{2\sqrt{\pi}B^{3/2}}{2(2\pi^2)^{3/2}} \tag{4.3.1}$$

Simplifying the right hand side of equation 4.3.1, we get $\frac{B}{8\pi^3}$. Setting this equal to $\frac{1}{16\pi^2}$,we see that $B = \frac{1}{2}\pi$. Thus, the Gaussian $G_{\pi/2}(x) = e^{-\frac{1}{2}\pi x^2}$ is an extremal function for the uncertainty principle.

($\Longrightarrow$) Let us now assume that there exists some function $\psi(x)$ that makes Theorem 54 sharp. We will go through the proof of the Heisenberg Uncertainty Principle, making sure that each inequality is sharp. From the hypothesis, we know that $1 = \int_{\mathbb{R}} |\psi(x)|^2 dx$. Using integration by parts, we get $1 = 2\int_{\mathbb{R}} xRe[\overline{\psi(x)}\psi'(x)]dx$. $Re(z) = z$ if and only if $z \in \mathbb{R}$, so let us assume that $\overline{\psi(x)}\psi'(x)$ is real for all $x \in \mathbb{R}$. Since $1 > 0$, we can say that

$$1 = 2|\int_{\mathbb{R}} x\overline{\psi(x)}\psi'(x)dx| \tag{4.3.2}$$

Since $|\int f| = \int |f|$ only if f is always positive or always negative, let us assume $x\overline{\psi(x)}\psi'(x) \geq 0$ for all $x \in \mathbb{R}$ or $x\overline{\psi(x)}\psi'(x) \leq 0$ for all $x \in \mathbb{R}$. Then equation 4.3.2 becomes

$$1 = 2\int_{\mathbb{R}} |x\psi(x)||\psi'(x)|dx \tag{4.3.3}$$

The next step in the proof of the Uncertainty Principle was to apply the Cauchy-Schwarz inequality, which is only an equality if the two functions are multiples of each other. So let us assume that $x\psi(x) = C\psi'(x)$ for some $C \in \mathbb{C}$. This implies that $\psi(x) = C_1 e^{-ax^2}$ for some $a, C_1 \in \mathbb{C}$. Note that $x\overline{\psi(x)}\psi'(x) = -2ax^2 e^{-2ax^2}$, so it does in fact satisfy the requirement that $x\overline{\psi(x)}\psi'(x) \leq 0$ for all $x \in \mathbb{R}$. From the proof in the other direction, we know that in order to achieve equality, we need $a = \frac{1}{2}\pi$ and $|C_1| = 1$. But $|C_1| = 1$ implies that C_1 is on the unit circle. Thus, $\psi(x) = |C_1|e^{-\frac{\pi}{2}x^2}$ for $C_1 \in S_1$. □

4.3.2 The Gaussians in G

In this section, we will prove that, for cyclic groups, $|G| = |\text{supp}f||\text{supp}\widehat{f}|$ if and only if f is the translation, modulation, and/or scalar multiple of the indicator function, 1_H, where H is a subgroup of G.

To prove that the translations, modulations, and scalar multiplies of the indicator functions of subgroups are the only functions that give us sharpness with our group uncertainty principle, we will first need some more definitions and lemmas from group theory.

Definition 61. An **indicator function** is defined, for $A \subseteq G$, as

$$1_A(a) = \begin{cases} 1 & a \in A \\ 0 & a \notin A \end{cases}$$

Definition 62. [12]: The **orthogonal complement** of a set $S \subseteq G$, denoted $S^\perp$, is defined as $S^\perp := \{\alpha \in \widehat{G} : \alpha(x) = 1 \ \forall x \in S\}$.

Remark. Note that the orthogonal complement is a subset of the dual group $\widehat{G}$ and consists of the characters of G that are trivial on S. If S is a subgroup of G, then $S^\perp$ will be a subgroup of $\widehat{G}$ that is isomorphic to $\frac{G}{S}$.

Lemma 63. *If H is a subgroup of G, then for every $\alpha \in \widehat{G}$,*

$$\widehat{1_H}(\alpha) = \begin{cases} \frac{|H|}{|G|} & \alpha \in H^\perp \\ 0 & \alpha \notin H^\perp \end{cases}$$

Proof. [12]: If $\alpha \in H^\perp$,

$$\begin{aligned} \widehat{1_H}(\alpha) &= \langle 1_H, \alpha \rangle \\ &= \frac{1}{|G|} \sum_{x \in G} 1_H(x)\overline{\alpha(x)} \\ &= \frac{1}{|G|} \sum_{x \in H} \overline{\alpha(x)} \end{aligned}$$

If $\alpha \in H^\perp$, then $\alpha(x) = 1$ for all $x \in H$. So,

$$\begin{aligned} \widehat{1_H}(\alpha) &= \frac{1}{|G|} \sum_{x \in H} 1 \\ &= \frac{|H|}{|G|} \end{aligned}$$

If $\alpha \notin H^\perp$, then there exists a $y \in H$ such that $\alpha(y) \neq 1$. Let $z = x - y$ for each $x \in H$. Then

$$\begin{aligned} \sum_{x \in H} \overline{\alpha(x)} &= \alpha(y) \sum_{x \in H} \overline{\alpha(x-y)} \\ &= \alpha(y) \sum_{z \in H} \overline{\alpha(z)} \end{aligned}$$

Since H is a subgroup, $\sum_{x\in H}\overline{\alpha(x-y)} = \sum_{z\in H}\overline{\alpha(z)}$ when $y \in H$. This implies that $\sum_{x\in H}\overline{\alpha(x)} = 0$.

So if $\alpha \notin H^{\perp}$, then

$$\begin{aligned}\widehat{1_H}(\alpha) &= \sum_{x\in G} 1_H(x)\overline{\alpha(x)} \\ &= \sum_{x\in H}\overline{\alpha(x)} \\ &= 0\end{aligned}$$

□

Lemma 64. *If $H \subseteq G$ is a subgroup, then*

$$|H||H^{\perp}| = |G|.$$

Proof. [12]:

We know that

$$\begin{aligned}|H| &= \sum_{x\in G} 1_H(x) \\ &= \sum_{x\in G} |1_H(x)|^2 \\ &= |G| \parallel 1_H \parallel_2^2\end{aligned}$$

From Plancherel's Identity, we know that $\parallel 1_H \parallel_2^2 = \parallel \widehat{1_H} \parallel_2^2$. Thus,

$$|H| = |G|\sum_{x\in G}|\widehat{1_H}(x)|^2.$$

From Lemma 63, we know that

$$\widehat{1_H}(\alpha) = \begin{cases}\frac{|H|}{|G|} & \alpha \in H^{\perp} \\ 0 & \alpha \notin H^{\perp}\end{cases}.$$

Thus,

$$\begin{aligned}|G|\sum_{x\in G}|\widehat{1_H}(x)|^2 &= |G|\sum_{\alpha\in H^{\perp}}\left(\frac{|H|}{|G|}\right)^2 \\ &= |G||H^{\perp}|\left(\frac{|H|}{|G|}\right)^2.\end{aligned}$$

Therefore, $|H| = |G||H^{\perp}|\left(\frac{|H|}{|G|}\right)^2$. Rearranging, we get $|H||H^{\perp}| = |G|$. □

The next lemma involves translations and modulations, which were introduced in sections 3.4.1 and 3.4.3. Recall that for $a \in G$ and $\alpha \in \widehat{G}$, and for $f \in L^2(G)$ and $\widehat{f} \in \widehat{G}$, that $\tau_a f(x) := f(x-a)$ and $M_\alpha f(x) := \alpha(x)f(x)$. Furthermore, $\tau_\alpha \widehat{f}(\xi) = \widehat{f}(\xi\alpha^{-1})$ and $M_a \widehat{f}(\xi) = \xi(a)\widehat{f}(\xi)$. Also, $\widehat{\tau_a f} = M_{-a}\widehat{f}$ and $\widehat{M_\alpha f} = \tau_\alpha \widehat{f}$. Now note that $|\text{supp}f| = |\text{supp}\tau_a f|$ for all $a \in G$. Also, $\text{supp}f = \text{supp}M_\alpha f$ for all $\alpha \in \widehat{G}$.

Lemma 65. *If $f \not\equiv 0$, then $0 \in supp\big(\tau_{-x_0}M_{\alpha_0^{-1}}f\big)$, and $1_G = \chi_0 \in supp\big(\tau_{-x_0}M_{\alpha_0^{-1}}f\big)\widehat{\ }$ for some $x_0 \in G$ and $\alpha_0 \in \widehat{G}$.*

Proof. If $f \not\equiv 0$, then there exists $x_0 \in G$ such that $f(x_0) \neq 0$ and $\exists \alpha_0 \in \widehat{G}$ such that $\widehat{f}(\alpha_0) \neq 0$.

Consider $\tau_{-x_0}M_{\alpha_0^{-1}}f(x) = \tau_{-x_0}(\alpha_0^{-1}(x)f(x)) = \alpha_0^{-1}(x+x_0)f(x+x_0)$.

Then $\tau_{-x_0}M_{\alpha_0^{-1}}f(0) = \alpha_0^{-1}(x_0)f(x_0) \neq 0$. Thus, $0 \in \text{supp}\big(\tau_{-x_0}M_{\alpha_0^{-1}}f\big)$.

Now consider $\xi \in \widehat{G}$

$$\begin{aligned}
\big(\tau_{-x_0}M_{\alpha_0^{-1}}f\big)\widehat{\ }(\xi) &= \frac{1}{|G|}\sum_{x\in G}\tau_{-x_0}M_{\alpha_0^{-1}}f(x)\overline{\xi(x)} \\
&= \frac{1}{|G|}\sum_{x\in G}\alpha_0^{-1}(x+x_0)f(x+x_0)\overline{\xi(x)} \\
&= \frac{1}{|G|}\sum_{x\in G}f(x+x_0)\overline{\alpha_0(x+x_0)\xi(x)} \\
&= \frac{1}{|G|}\sum_{x\in G}f(x)\overline{\alpha_0(x)\xi(x-x_0)} \\
&= \frac{1}{|G|}\xi(x_0)\sum_{x\in G}f(x)\overline{\alpha_0(x)\xi(x)} \\
&= \xi(x_0)\widehat{f}(\alpha_0\xi).
\end{aligned}$$

So $\big(\tau_{-x_0}M_{\alpha_0^{-1}}f\big)\widehat{\ }(\chi_0) = \chi_0(x_0)\widehat{f}(\chi_0\alpha_0) = \widehat{f}(\alpha_0) \neq 0$, so $\chi_0 \in \text{supp}\big(\tau_{-x_0}M_{\alpha_0^{-1}}f\big)\widehat{\ }$. □

We are now ready to prove the main theorem of this subsection.

Theorem 66. *If $0 \in suppf$ and $\chi_0 \in supp\widehat{f}$, then $|suppf||supp\widehat{f}| = |G|$ if and only if $f = c1_H$, where H is a subgroup of a cyclic group G and c is a nonzero constant.*

Proof. [2]: ($\Rightarrow$) Let us assume $|\text{supp}f||\text{supp}\widehat{f}| = |G|$, and that $N = |G|$. This assumption implies that f is not identically equal to zero. By our hypothesis, $0 \in \text{supp}f$ and $\chi_0 \in \text{supp}\widehat{f}$. We need only show that $\text{supp}f$ is a subgroup. If $\text{supp}f = B$ is a subgroup, we know from Lemma 64 that $|B||B^\perp| = |G|$, so $|\text{supp}\widehat{f}| = |B^\perp|$. Since $B^\perp = \{\alpha \in \widehat{G} : \alpha(x) = 1\ \forall x \in B\}$, we can show that for any $\alpha \in \widehat{G}$ and $\beta \in B^\perp$,

$$\widehat{f}(\alpha\beta) = \frac{1}{|G|}\sum_{x\in G}f(x)\overline{\alpha\beta(x)}$$

Since f is supported on B, we can write

$$\widehat{f}(\alpha\beta) = \frac{1}{|G|}\sum_{x\in B} f(x)\overline{\alpha(x)\beta(x)}$$

Also, since $\beta \in B^{\perp}$, $\beta(x) = 1$ for all $x \in B$, which would imply that $\overline{\beta(x)} = 1$ for all $x \in B$. Thus, $\widehat{f}(\alpha\beta) = \frac{1}{|G|}\sum_{x\in B} f(x)\overline{\alpha(x)}$. But since f is supported on B, we can sum over all elements in G since we would just be adding zeros for x not in B. Thus, $\widehat{f}(\alpha\beta) = \frac{1}{|G|}\sum_{x\in G} f(x)\overline{\alpha(x)} = \widehat{f}(\alpha)$. Note that $\chi_0(a) = 1$ for all $a \in B$, so χ_0 is in $B^{\perp}$. Thus, if we let $\alpha = \chi_0$ in the above equation, we would get that $\widehat{f}(\beta) = \widehat{f}(\chi_0)$ for all $\beta \in B^{\perp}$. This proves that $\widehat{f}$ is constant on $B^{\perp}$.

We know that $\alpha = \chi_0 \in \text{supp}\widehat{f}$, and this implies that $\widehat{f}(\chi_0) \neq 0$. This implies that $\widehat{f}$ is a nonzero constant on $B^{\perp}$, which implies that $B^{\perp} \subseteq \text{supp}\widehat{f}$. But from our assumption that B is a subgroup of G, we know that $|\text{supp}\widehat{f}| = |B^{\perp}|$, so $\text{supp}\widehat{f} = B^{\perp}$. Since $\widehat{f}$ is supported and constant on $B^{\perp}$ we can say that $\widehat{f} = C1_{B^{\perp}}$. By Lemma 63, we know that, for $g = 1_B$, then $\widehat{g} = 1_{B^{\perp}}$. The Fourier Inversion Formula tells us that the Fourier transform forms a bijection from G onto $\widehat{G}$; this implies that $f = c1_B$ for c$\in \mathbb{C}$ and $c \neq 0$. We now just need to prove that supp$f$ is a subgroup of G.

Let $|\text{supp}\widehat{f}| = M$. Let $r_1, r_2, \ldots, r_M \in G$ be such that $\alpha_{r_j} \in \text{supp}\widehat{f}$ for $1 \leq j \leq M$. Because we are assuming that G is cyclic, we can relate each element $\alpha_j \in \widehat{G}$ to an element in the group U_n, where $n = |G|$ and $\alpha_j(k) = e^{2\pi ijk/n}$. Let $0 \leq p \leq N - M$. Define $\omega_k^{(p)} = f(p + k)$, with $1 \leq k \leq M$. By the Fourier Inversion formula, we know that

$$\begin{aligned}
\omega_k^{(p)} &= \sum_{\xi\in\widehat{G}} \widehat{f}(\xi)\xi(p+k) \\
&= \sum_{\alpha_r\in\text{supp}\widehat{f}} \widehat{f}(\alpha_r)\alpha_r(p+k) \\
&= \sum_{j=1}^{M} \widehat{f}(\alpha_{r_j})\alpha_{r_j}(p+k)
\end{aligned}$$

Let $\alpha_{r_j} = z_j$, let $u = \left(\widehat{f}(z_1), \widehat{f}(z_2), \ldots, \widehat{f}(z_M)\right)$, and let $\omega^{(p)} = \left(\omega_1^{(p)}, \omega_2^{(p)}, \ldots, \omega_M^{(p)}\right)$. Then $\omega^{(p)} = Zu$, where Z is an MxM matrix where $z_{k,j} = z_j^{p+k}$. We want to show that $\omega^{(p)} \neq 0$, which will show that f does not have M consecutive zeros. Since $u = \left(\widehat{f}(z_1), \widehat{f}(z_2), \ldots, \widehat{f}(z_M)\right)$, and $z_j \in \text{supp}\widehat{f}$, we know $u \neq 0$. To show that $\omega^{(p)} \neq 0$, we just have to show that $detZ \neq 0$.

$$Z = \begin{bmatrix} z_1^{p+1} & z_2^{p+1} & \cdots & z_M^{p+1} \\ z_1^{p+2} & z_2^{p+2} & \cdots & z_M^{p+2} \\ \vdots & \vdots & \ddots & \vdots \\ z_1^{p+M} & z_2^{p+M} & \cdots & z_M^{p+M} \end{bmatrix}$$

$$detZ = z_1^{p+1} z_2^{p+1} \cdots z_M^{p+1} det \begin{bmatrix} 1 & 1 & \cdots & 1 \\ z_1 & z_2 & \cdots & z_M \\ \vdots & \vdots & \ddots & \vdots \\ z_1^{M-1} & z_2^{M-1} & \cdots & z_M^{M-1} \end{bmatrix} = z_1^{p+1} z_2^{p+1} \cdots z_M^{p+1} det(V).$$

But V is a Vandermonde matrix, so

$$detZ = z_1^{p+1} z_2^{p+1} \cdots z_M^{p+1} \prod_{1 \le j < k \le M} (z_j - z_k).$$

Since $z_j \neq z_k$ if $j \neq k$, $detZ \neq 0$, thus $\omega^{(p)} \neq 0$ for $0 \le p \le N - M$. This implies that f does not have M consecutive zeros, or in other words, there are no elements in supp$f$ that are M elements apart. Suppose there were elements in supp$f$ that were less than $M - 1$ elements apart. But since $|\text{supp}f| = N/M$, this implies that there are at least two elements in supp$f$ that are M or more elements apart. This is a contradiction. Hence, the elements in supp$f$ must be exactly $M - 1$ elements apart. By our assumption $0 \in \text{supp}f$, then supp$f = \{0, M, 2M, \ldots, N - M\}$, which is a subgroup of G. So $f = c1_H$ where H is a subgroup of G.

($\Leftarrow$) Now assume $f = 1_H$ where H is a subgroup of G. Obviously, $|\text{supp}f| = H$. By Lemma 63, we know

$$\widehat{1_H}(a) = \begin{cases} \frac{|H|}{|G|} & a \in H^\perp \\ 0 & a \notin H^\perp \end{cases}$$

Thus, $|\text{supp}\widehat{\chi_H}| = |H^\perp|$, and by Lemma 64, we know $|H||H^\perp| = |G|$. □

Remark. Note that Theorem 66 and Lemma 65 imply that, if $g \not\equiv 0$, then $|\text{supp}g| + |\text{supp}\widehat{f}| \ge |G|$ if and only if g is the modulation, translation, or nonzero scalar multiple of the indicator function 1_H, where H is a subgroup of G and G is cyclic.

This statement is actually true even if G is not cyclic. For a proof of the more general version, see [13], Proposition 2.2.

Chapter 5

The Entropy Uncertainty Principle

While the uncertainty principle is one of the most well-known inequalities in Fourier analysis on groups, there are other inequalities that can be very useful. One of them, the entropy uncertainty principle, can even be used to prove the uncertainty principle. However, in order to prove that inequality, we will need some more basic ideas, including the notion of tensor powers. We will use these ideas to prove a few analogs to classical inequalities on $\mathbb{R}$, like the Hausdorff-Young inequality, which will give us the tools we need to prove the entropy uncertainty principle.

5.1 Entropy Uncertainty Principle

The entropy uncertainty principle relates a function on the group, its Fourier transform on the dual group, and the logarithms of their absolute values. Mathematically, the statement is as follows:

Theorem 67. *Entropy Uncertainty Principle: Let $f \in L(G)$ such that $\| f \|_{L^2(G)} = 1$. Then*

$$\frac{1}{2|G|} \sum_{a \in G} |f(a)|^2 \log |f(a)| + \frac{1}{2} \sum_{\xi \in \widehat{G}} |\widehat{f}(\xi)|^2 \log |\widehat{f}(\xi)| \leq 0.$$

Remark. Note that $L(G)$ is the space of functions which map elements of G into $\mathbb{C}$. Depending on the norm one uses, this space becomes $L^2(G)$, or more generally, $L^p(G)$ for $p \geq 1$. If f is in $L(G)$, then it is also in $L^p(G)$ for $p \geq 1$.

To prove the Entropy Uncertainty Principle, we will need a number of lemmas which we will state, and then prove in the following section.

Lemma 68. *(Young's Inequality). Let $a, b > 0$ and $p, q \in [1, \infty]$ with $\frac{1}{p} + \frac{1}{q} = 1$. Then $ab \leq \frac{a^p}{p} + \frac{b^q}{q}$.*

Lemma 69. *(Hölder's Inequality). Let $\frac{1}{p} + \frac{1}{q} = 1$, $p, q \geq 1$, with $f \in L^p(G)$ and $g \in L^q(G)$. Then*

$$\| fg \|_{L^1(G)} \leq \| f \|_{L^p(G)} \| g \|_{L^q(G)} .$$

Lemma 70. *(Hausdorff-Young Inequality). Let* $\frac{1}{p}+\frac{1}{q}=1$, *with* $1\leq p\leq 2$, *and* $f\in L^p(G)$ *and* $\| f \|_{L^p(G)}=1$. *Then*

$$\| f \|_{L^p(G)}\geq \| \widehat{f} \|_{L^q(\widehat{G})}.$$

Proof. (Proof of Entropy Uncertainty Principle)[2]: If $\frac{1}{p}+\frac{1}{q}=1$, then $q=\frac{p}{p-1}$. By the Hausdorff-Young Inequality, we know for $f\in L(G)$, $1\leq p\leq 2$,

$$\| \widehat{f} \|_{L^q(\widehat{G})}\leq \| f \|_{L^p(G)}.$$

Let us define $A(p):=\| f \|_{L^p(G)} - \| \widehat{f} \|_{L^{p/(p-1)}(\widehat{G})}$, then $A(p)\geq 0$ for $1\leq p\leq 2$. Recall that $L^p(G)$ and $L^p(\widehat{G})$ have different normalizations: for the $L^p(G)$ space, we divide by $|G|^p$, but we do not in the $L^p(\widehat{G})$ space. By the definition of an L^p norm on $L(G)$, $\| f \|_{L^p(G)}=\frac{1}{|G|^{1/p}}\left(\sum_{a\in G}|f(a)|^p\right)^{1/p}$. Similarly, $\| \widehat{f} \|_{L^p(\widehat{G})}=\left(\sum_{\xi\in\widehat{G}}|\widehat{f}(\xi)|^p\right)^{1/p}$. Thus, we can rewrite $A(p)$:

$$A(p)=\frac{1}{|G|^{1/p}}\left(\sum_{a\in G}|f(a)|^p\right)^{1/p}-\left(\sum_{\xi\in\widehat{G}}|\widehat{f}(a)|^{p/(p-1)}\right)^{(p-1)/p}.$$

Let us define $B(p):=\frac{1}{|G|^{1/p}}\left(\sum_{a\in G}|f(a)|^p\right)^{1/p}$ and $C(p):=\left(\sum_{\xi\in\widehat{G}}|\widehat{f}(\xi)|^{p/(p-1)}\right)^{(p-1)/p}$. Then $A(p)=B(p)-C(p)$.

Consider

$$\begin{aligned}\log(B(p)) &= \log\left(\frac{1}{|G|^{1/p}}\left(\sum_{a\in G}|f(a)|^p\right)^{1/p}\right)\\ &= \log(|G|^{-1/p})+\log\left(\left(\sum_{a\in G}|f(a)|^p\right)^{1/p}\right)\\ &= \frac{-1}{p}\log(|G|)+\frac{1}{p}\log\left(\sum_{a\in G}|f(a)|^p\right).\end{aligned}$$

Now consider

$$\begin{aligned}\frac{B'(p)}{B(p)} &= \frac{d}{dp}(\log(B(p))\\ &= \frac{1}{p^2}\log(|G|)-\frac{1}{p^2}\log\left(\sum_{a\in G}|f(a)|^p\right)+\frac{1}{p}\frac{d}{dp}\log\left(\sum_{a\in G}|f(a)|^p\right)\\ &= \frac{1}{p^2}\log(|G|)-\frac{1}{p^2}\log\left(\sum_{a\in G}|f(a)|^p\right)+\frac{1}{p}\left(\frac{1}{\sum_{a\in G}|f(a)|^p}\sum_{a\in G}(|f(a)|^p\log|f(a)|)\right).\end{aligned}$$

Since $\| f \|_{L^2(G)} = 1$, then $B(2) = 1$ and $B'(2) = \frac{B'(2)}{B(2)}$. Also, since $\| f \|_{L^2(G)} = 1$, then $\sum |f(a)|^2 = |G|$. Therefore,

$$\begin{aligned} B'(2) &= \frac{\log(|G|)}{4} - \frac{1}{4}\log\left(\sum_{a\in G}|f(a)|^2\right) + \frac{1}{2}\left(\frac{1}{\sum_{a\in G}|f(a|^2}\sum_{a\in G}\left(|f(a)|^2\log(|f(a)|)\right)\right) \\ &= \frac{\log(|G|)}{4} - \frac{1}{4}\log(|G|) + \frac{1}{2}\left(\frac{1}{|G|}\sum_{a\in G}\left(|f(a)|^2\log(|f(a)|)\right)\right) \\ &= \frac{1}{2|G|}\sum_{a\in G}|f(a)|^2\log(|f(a)|). \end{aligned}$$

Similarly,

$$\log(C(p)) = \frac{p-1}{p}\log\left(\sum_{\xi\in\widehat{G}}|\widehat{f}(\xi)|^{p/(p-1)}\right)$$

Note:
Consider $y = a^{p/(p-1)}$. Then $\log(y) = \frac{p}{p-1}\log(a)$. Then $\frac{1}{y}dy = \log(a) * \frac{p-1-p}{(p-1)^2}dp = \frac{-1}{(p-1)^2}\log(a)dp$. This then implies that $\frac{dy}{dp} = \frac{-y}{(p-1)^2}\log(a) = \frac{-a^{p/(p-1)}\log(a)}{(p-1)^2}$.
Also,

$$\begin{aligned} \frac{C'(p)}{C(p)} &= \frac{d}{dp}\log(C(p)) \\ &= \frac{1}{p^2}\log\left(\sum_{\xi\in\widehat{G}}|\widehat{f}(\xi)|^{p/(p-1)}\right) + \left(\frac{p-1}{p}\right)\frac{d}{dp}\log\left(\sum_{\xi\in\widehat{G}}|\widehat{f}(\xi)|^{p/(p-1)}\right) \\ &= \frac{1}{p^2}\log\left(\sum_{\xi\in\widehat{G}}|\widehat{f}(\xi)|^{p/(p-1)}\right) + \frac{p-1}{p}\frac{1}{\sum_{\xi\in\widehat{G}|}|\widehat{f}(\xi)|^{p/(p-1)}}\frac{-\sum_{\xi\in\widehat{G}}|\widehat{f}(\xi)|^{p/(p-1)}\log(|\widehat{f}(\xi)|)}{(p-1)^2} \\ &= \frac{1}{p^2}\log\left(\sum_{\xi\in\widehat{G}}|\widehat{f}(\xi)|^{p/(p-1)}\right) - \frac{1}{p(p-1)}\frac{\sum_{\xi\in\widehat{G}}|\widehat{f}(\xi)|^{p/(p-1)}\log(|\widehat{f}(\xi)|)}{\sum_{\xi\in\widehat{G}}|\widehat{f}(\xi)|^{p/(p-1)}}. \end{aligned}$$

We know that $\| f \|_{L^2(G)} = 1$, so by Plancherel's Identity, $\| f \|_{L^2(G)} = \| \widehat{f} \|_{L^2(\widehat{G})} = 1$. By definition, $C(2) = 1$. So $\frac{C'(2)}{C(2)} = C'(2)$.

$$C'(2) = \frac{1}{4}\log\left(\sum_{\xi\in\widehat{G}}|\widehat{f}(\xi)|^2\right) - \frac{1}{2}\frac{\sum_{\xi\in\widehat{G}}|\widehat{f}(\xi)|^2\log(|\widehat{f}(\xi)|)}{\sum_{\xi\in\widehat{G}}|\widehat{f}(\xi)|^2}$$

Since $\sqrt{\sum_{\xi\in\widehat{G}}|\widehat{f}(\xi)|^2} = 1$, then $\sum_{\xi\in\widehat{G}}|\widehat{f}(\xi)|^2 = 1$. Thus,

$$\begin{aligned} C'(2) &= \frac{1}{4}\log(1) - \frac{1}{2}\sum_{\xi\in\widehat{G}}|\widehat{f}(\xi)|^2\log(|\widehat{f}(\xi)| \\ &= \frac{-1}{2}\sum_{\xi\in\widehat{G}}|\widehat{f}(\xi)|^2\log(|\widehat{f}(\xi)|. \end{aligned}$$

So by definition, $A'(2) = B'(2) - C'(2)$. By Plancherel's Identity, $A(2) = 0$. Since $A(p) \geq 0$ for $1 \leq p \leq 2$ and $A(2) = 0$, then $A'(2) \leq 0$. Thus,

$$\frac{1}{2|G|} \sum_{a \in G} |f(a)|^2 \log |f(a)| + \frac{1}{2} \sum_{\xi \in \widehat{G}} |\widehat{f}(\xi)|^2 \log |\widehat{f}(\xi)| \leq 0.$$

□

One might wonder why the above inequality is called the entropy uncertainty principle. By definition [2], the entropy of $|f|^2$ is

$$h(|f|^2) := -\frac{1}{|G|} \sum_{x \in G} |f(x)|^2 \log |f(x)|^2.$$

Similarly, the entropy of $|\widehat{f}|^2$ is defined as

$$h(|\widehat{f}|^2) := -\sum_{\xi \in \widehat{G}} |\widehat{f}(\xi)|^2 \log |\widehat{f}(\xi)|^2.$$

With this notation, the discrete entropy uncertainty principle reads $h(|f|^2) + h(|\widehat{f}|^2) \geq 0$.

5.2 Shannon Entropy Inequality

The reader might wonder if there is an analog to the entropy uncertainty principle in classical Fourier analysis. There is, in fact, an analog, called the Shannon Entropy Inequality.

Definition 71. The definition of entropy for functions in $\mathcal{S}(\mathbb{R})$ is similar to that for functions in G.

$$H(|f|^2) = -\int_{-\infty}^{\infty} |f(x)|^2 \log |f(x)|^2 dx$$

Theorem 72. *(Shannon Entropy Bound) [9]: For $f \in \mathcal{S}(\mathbb{R})$ and $g = \widehat{f}$, then*

$$H(|f|^2) + H(|g|^2) \geq \log \frac{e}{2}.$$

In 1957, Isidore Hirschman proved that $H(|f|^2) + H(|g|^2) \geq 0$, yielding a very similar result to our discrete entropy uncertainty principle. In 1975, William Beckner proved the above tighter bound, and that equality holds when f and g are Gaussians. This result is very similar to the Heisenberg Uncertainty Principle, which also attains equality in the case that the functions are Gaussians.

5.3 Proofs of Lemmas

We will now provide the proofs of the lemmas we needed to obtain the entropy uncertainty principle.

Young's Inequality (Lemma 68)*: Let* $a, b > 0$ *and* $p, q \in [1, \infty]$ *with* $\frac{1}{p} + \frac{1}{q} = 1$*. Then* $ab \leq \frac{a^p}{p} + \frac{b^q}{q}$.

Proof. [7]: Consider the function $f : (0, \infty) \to \mathbb{R}$, where $f(x) = \ln(x)$. We know that $f''(x) = \frac{-1}{x^2}$. Since $f''(x) > 0 \ \forall x \in \mathbb{R}$, we know that $f(x)$ is concave. By definition [8], this implies that $\ln((1-\lambda)x + \lambda y) \geq (1-\lambda)\ln(x) + \lambda \ln(y)$ for $\lambda \in [0, 1]$ and $x, y \in (0, \infty)$.

Let $t = \frac{1}{p}$. Since $p \in [1, \infty]$, $t \in [0, 1]$. Note that $\frac{1}{q} = 1 - t$.

Consider

$$\begin{aligned} \ln(\frac{a^p}{p} + \frac{b^q}{q}) &= \ln(ta^p + (1-t)b^q) \\ &\geq t\ln(a^p) + (1-t)\ln(b^q) \\ &= tp\ln(a) + (1-t)q\ln(b) \\ &= \ln(a) + \ln(b) \\ &= \ln(ab) \end{aligned}$$

If we take each side of the inequality as powers of e, we conclude that $ab \leq \frac{a^p}{p} + \frac{b^q}{q}$. □

Hölder's Inequality (Lemma **69**): *Let* $\frac{1}{p} + \frac{1}{q} = 1$, $p, q \geq 1$, *with* $f \in L^p(G)$ *and* $g \in L^q(G)$*. Then*

$$\| fg \|_{L^1(G)} \leq \| f \|_{L^p(G)} \| g \|_{L^q(G)} .$$

Proof. By Lemma 68, we know that, for all $a \in G$,

$$|f(a)g(a)| \leq \frac{|f(a)|^p}{p} + \frac{|g(a)|^q}{q}$$

This implies

$$\begin{aligned} \frac{1}{|G|}\sum_{a\in G}|f(a)g(a)| &\leq \frac{1}{|G|}\sum_{a\in G}\frac{|f(a)|^p}{p} + \frac{1}{|G|}\sum_{a\in G}\frac{|g(a)|^q}{q} \\ &= \frac{1}{p|G|}\sum_{a\in G}|f(a)|^p + \frac{1}{|G|q}\sum_{a\in G}|g(a)|^q \end{aligned}$$

Taking the natural logarithm of both sides yields

$$\ln\left(\frac{1}{|G|}\sum_{a\in G}|f(a)g(a)|\right) \leq \ln\left(\frac{1}{|G|p}\sum_{a\in G}|f(a)|^p + \frac{1}{q|G|}\sum_{a\in G}|g(a)|^q\right).$$

By the concavity of the logarithm, we get

$$\begin{aligned}
\ln\left(\frac{1}{|G|}\sum_{a\in G}|f(a)g(a)|\right) &\leq \frac{1}{p}\ln\left(\frac{1}{|G|}\sum_{a\in G}|f(a)|^p\right)+\frac{1}{q}\ln\left(\frac{1}{|G|}\sum_{a\in G}|g(a)|^q\right)\\
&= \ln\left(\frac{1}{|G|}\sum_{a\in G}|f(a)|^p\right)^{1/p}+\ln\left(\frac{1}{|G|}\sum_{a\in G}|g(a)|^q\right)^{1/q}\\
&= \ln\left(\| f \|_{L^p(G)}\right)+\ln\left(\| g \|_{L^q(G)}\right)\\
&= \ln\left(\| f \|_{L^p(G)}\| g \|_{L^q(G)}\right)
\end{aligned}$$

By making both sides of the inequality powers of e, we get

$$\| fg \|_{L^1(G)} \leq \| f \|_{L^p(G)} \| g \|_{L^q(G)} .$$

□

Next we present a non-traditional proof of the Hausdorff-Young Inequality based on Tao's "tensor-power trick" instead of on the more traditional Marcinkiewicz Interpolation Theorem. We first need to define tensor powers and prove a lemma relating the tensor powers and their Fourier transforms.

Definition 73. Let $f : G \to \mathbb{C}$. Let us define the M^{th} **tensor power** of f, denoted $f^{\otimes M}$, as $f^{\otimes M} : G^M \to \mathbb{C}$, with $f^{\otimes M}(a_1, a_2, \ldots, a_M) = f(a_1)f(a_2)\cdots f(a_M)$.

We not that $\widehat{G^M} = \left(\widehat{G}\right)^M$. So, for $\xi \in \widehat{G^M}$ and $a \in G^M$, we define $\xi(a) := \xi_1(a_1)\xi_2(a_2)\cdots\xi_M(a_M)$ where $a = (a_1, a_2, \ldots, a_M)$.

Lemma 74. *The tensor power of the Fourier transform of f is equal to the Fourier transform of the tensor power of f.*

Proof. Consider the Fourier transform of $f^{\otimes M}$. By the definition of the Fourier transform, for every $\xi \in \widehat{G^M}$,

$$\begin{aligned}
\widehat{f^{\otimes M}}(\xi) &= \frac{1}{|G|^M}\sum_{a\in G^M} f^{\otimes M}(a)\xi(a)\\
&= \frac{1}{|G|^M}\sum_{a_1\in G}\sum_{a_2\in G}\cdots\sum_{a_M\in G} f(a_1)f(a_2)\cdots f(a_M)\xi_1(a_1)\xi_2(a_2)\cdots\xi_M(a_M)\\
&= \left(\frac{1}{|G|}\sum_{a_1\in G} f(a_1)\xi_1(a_1)\right)\left(\frac{1}{|G|}\sum_{a_2\in G} f(a_2)\xi_2(a_2)\right)\cdots\left(\frac{1}{|G|}\sum_{a_M\in G} f(a_M)\xi_M(a_M)\right)\\
&= \widehat{f}(\xi_1)\widehat{f}(\xi_2)\cdots\widehat{f}(\xi_M)
\end{aligned}$$

□

Hausdorff-Young Inequality(Lemma **70**): *Let* $\frac{1}{p}+\frac{1}{q}=1$, *with* $1\leq p\leq 2$, *and* $f\in L^p(G)$ *and* $\| f \|_{L^p(G)}=1$. *Then*

$$\| f \|_{L^p(G)}\geq \| \widehat{f} \|_{L^q(\widehat{G})} .$$

Proof. [17]: Note that, by the definition of the Fourier transform and the triangle inequality,

$$|\widehat{f}(\xi)| = |\frac{1}{|G|}\sum_{a\in G} f(a)\xi(a)| \leq \frac{1}{|G|}\sum_{a\in G}|f(a)\xi(a)| = \frac{1}{|G|}\sum_{a\in G}|f(a)| = \| f \|_{L^1(G)}$$

for all $\xi\in\widehat{G}$. Since $\| \widehat{f} \|_{L^\infty(\widehat{G})}=\sup_{\xi\in\widehat{G}}|\widehat{f}(\xi)|$, so $\| \widehat{f} \|_{L^\infty(\widehat{G})}\leq \| f \|_{L^1(G)}$.

Also, from Plancherel's Identity, , we know

$$\left(\sum_{\xi\in\widehat{G}}|\widehat{f}(\xi)|^2\right)^{\frac{1}{2}} = \left(\frac{1}{|G|}\sum_{a\in G}|f(a)|^2\right)^{\frac{1}{2}} .$$

Let us assume that f is supported on some subset $A\subset G$ and that for $a\in A=\text{supp}f$, $2^m\leq |f(a)|\leq 2^{m+1}$ for some $m\in\mathbb{Z}$.

Consider the inequality

$$\begin{aligned}\sup_{\xi\in\widehat{G}}|\widehat{f}(\xi)| &\leq \frac{1}{|G|}\sum_{a\in G}|f(a)| \\ &\leq \frac{1}{|G|}\sum_{a\in A}2^{m+1} \\ &= \frac{|A|}{|G|}2^{m+1}\end{aligned}$$

This implies

$$\sup_{\xi\in\widehat{G}}|\widehat{f}(\xi)|\leq\frac{|A|}{|G|}2^{m+1} \tag{5.3.1}$$

From Plancherel's identity, we know

$$\begin{aligned}\left(\sum_{\xi\in\widehat{G}}|\widehat{f}(\xi)|^2\right)^{\frac{1}{2}} &= \left(\frac{1}{|G|}\sum_{a\in G}|f(a)|^2\right)^{\frac{1}{2}} \\ &\leq \left(\frac{1}{|G|}\sum_{a\in A}(2^{m+1})^2\right)^{\frac{1}{2}} \\ &= \left(\frac{|A|}{|G|}(2^{m+1})^2\right)^{\frac{1}{2}} \\ &= \left(\frac{|A|}{|G|}\right)^{\frac{1}{2}}2^{m+1}\end{aligned}$$

Thus,

$$\left(\sum_{\xi\in\widehat{G}}|\widehat{f}(\xi)|^2\right)^{\frac{1}{2}} \leq \left(\frac{|A|}{|G|}\right)^{\frac{1}{2}} 2^{m+1} \tag{5.3.2}$$

Since $1 \leq p \leq 2$, we know that $q \geq 2$, and so $q-2 \geq 0$. Now consider

$$\left(\sum_{\xi\in\widehat{G}}|\widehat{f}(\xi)|^q\right)^{\frac{1}{q}} = \left(\sum_{\xi\in\widehat{G}}|\widehat{f}(\xi)|^2|\widehat{f}(\xi)|^{q-2}\right)^{\frac{1}{q}}$$

Using equation 5.3.1, we can say

$$\begin{aligned}\left(\sum_{\xi\in\widehat{G}}|\widehat{f}(\xi)|^q\right)^{\frac{1}{q}} &\leq \left(\sum_{\xi\in\widehat{G}}|\widehat{f}(\xi)|^2\left(\frac{|A|}{|G|}2^{m+1}\right)^{q-2}\right)^{\frac{1}{q}} \\ &= \left(\left(\frac{|A|}{|G|}2^{m+1}\right)^{q-2}\sum_{\xi\in\widehat{G}}|\widehat{f}(\xi)|^2\right)^{\frac{1}{q}} \\ &= \left(\frac{|A|}{|G|}2^{m+1}\right)^{\frac{q-2}{q}}\left(\left(\sum_{\xi\in\widehat{G}}|\widehat{f}(\xi)|^2\right)^{\frac{1}{2}}\right)^{\frac{2}{q}}\end{aligned}$$

Using equation 5.3.2, we know

$$\begin{aligned}\left(\sum_{\xi\in\widehat{G}}|\widehat{f}(\xi)|^q\right)^{\frac{1}{q}} &\leq \left(\frac{|A|}{|G|}2^{m+1}\right)^{1-\frac{2}{q}}\left(\left(\frac{|A|}{|G|}\right)^{\frac{1}{2}}2^{m+1}\right)^{\frac{2}{q}} \\ &= \left(\frac{|A|}{|G|}\right)^{1-\frac{1}{q}-\frac{1}{q}}\left(\frac{|A|}{|G|}\right)^{\frac{1}{q}}\left(2^{m+1}\right)^{1-\frac{2}{q}}\left(2^{m+1}\right)^{\frac{2}{q}} \\ &= \left(\frac{|A|}{|G|}\right)^{1-\frac{1}{q}}\left(2^{m+1}\right) \\ &= \left(\frac{|A|}{|G|}\right)^{\frac{1}{p}}2^{m+1}\end{aligned}$$

Since we are assuming that $2^m \leq |f(a)| \leq 2^{m+1}$, we know

$$\begin{aligned}\left(\frac{|A|}{|G|}\right)^{\frac{1}{p}}2^{m+1} &= 2\left(\frac{|A|}{|G|}\right)^{\frac{1}{p}}2^m \\ &\leq 2\left(\frac{1}{|G|}\sum_{a\in G}|f(a)|^p\right)^{\frac{1}{p}}\end{aligned}$$

We then get that

$$\| \widehat{f} \|_{L^q(\widehat{G})} \leq 2 \| f \|_{L^p(G)} \tag{5.3.3}$$

For the above inequalities, we have assumed that $2^m \leq |f(a)| < 2^{m+1}$ for all a in $\text{supp} f$.

Even though there are an infinite number of dyadic intervals, if we normalize the L^p norm so that $(\sum_{a \in G} |f(a)|^p)^{\frac{1}{p}} = 1$, we need only consider the intervals between $|G|^{-100}$ and $|G|^{100}$. Here's why:

Suppose there exists an $x \in G$ such that $|f(x)| \geq |G|^{100}$. Even if for all other $a \in G$, $|f(a)| = 0$, $\| f \|_{L^p(G)} \geq \left(\frac{1}{|G|} (|G|^{100})^p \right)^{\frac{1}{p}}$. This implies that $\| f \|_{L^p(G)} \geq (|G|^{100p-1})^{\frac{1}{p}} = \frac{|G|^{100}}{|G|^{\frac{1}{p}}}$. Unless $|G| = 1$, this implies that $\| f \|_{L^p(G)} > 1$, which is a contradiction. We still need an argument as to why we can assume $|G|^{-100} \leq |f(x)|$ for all $x \in G$. However, we will just accept this as fact for now.

Let $A = \text{supp} f$. If $a \in A$, then, from the above argument, we know that $|G|^{-100} \leq |f(a)| \leq |G|^{100}$ for all $a \in A$. But $|G|^{-100} = 2^{-100 \log_2 |G|}$ and $|G|^{100} = 2^{100 \log_2 |G|}$. This yields the new inequality

$$2^{-100 \log_2 |G|} \leq |f(a)| \leq 2^{100 \log_2 |G|} \tag{5.3.4}$$

By the Archimedian Principle, we know that there exists some $k, l \in \mathbb{Z}$ such that $k \leq -100 \log_2 |G| < k + 1$ and $l \leq 100 \log_2 |G| < l + 1$. We can then rewrite equation 5.3.4 as $2^k \leq |f(a)| < 2^{l+1}$ for all $a \in A$. It is obvious that $k < l + 1$, so subtracting k from $l + 1$ should give us a positive number. Furthermore, $l - k \approx 200 \log_2 |G|$. This is the number of dyadic intervals that our function can take values in.

For $k \leq m \leq l$, let us define $A_m = \{a \in A | 2^m \leq |f(a)| < 2^{m+1}\}$. Notice that $A = \bigcup_{m=k}^{l} A_m$ and that all A_ms are disjoint. Let us also define $f_m = f \chi_{A_m}$. Then, since the A_ms are disjoint, $f = \sum_{m=k}^{l} f_m$. But since the Fourier transform is linear, we also get that $\widehat{f} = \sum_{m=k}^{l} \widehat{f}_m$. From equation 5.3.3, we know that $\| \widehat{f}_m \|_{L^q(\widehat{G})} \leq 2 \| f_m \|_{L^p(G)}$ for all m. Thus,

$$\| \widehat{f} \|_{L^q(\widehat{G})} = \| \sum_{m=k}^{l} \widehat{f}_m \|_{L^q(\widehat{G})}$$

By the triangle inequality, we get that

$$\begin{aligned}
\| \widehat{f} \|_{L^q(\widehat{G})} &\leq \sum_{m=k}^{l} \| \widehat{f}_m \|_{L^q(\widehat{G})} \\
&\leq \sum_{m=k}^{l} 2 \| f_m \|_{L^p(G)} \\
&\leq 2(l + 1 - k) \| f \|_{L^p(G)} \\
&= 2(1 + 200 \log_2 |G|) \| f \|_{L^p(G)} \\
&\leq 400(1 + \log_2 |G|) \| f \|_{L^p(G)}
\end{aligned}$$

So, for all finite abelian groups G and for all $f \in L^2(G)$, we have $\| \widehat{f} \|_{L^q(\widehat{G})} \leq 400(1 + \log_2 |G|) \| f \|_{L^p(G)}$. In particular, this is true for the group G^M, where $|G^M| = |G|^M$, and

for the function $F \in L^2(G^M)$ where $F = f^{\otimes M}$. Plugging these values into the inequality, we get

$$\| (f^{\otimes M})\widehat{\ } \|_{L^q(\widehat{G^M})} \leq 400(1 + \log_2 |G^M|) \| f^{\otimes M} \|_{L^p(G^M)}$$

Using the tensor power trick, we get

$$\| \widehat{f} \|^M_{L^q(\widehat{G})} \leq 400(1 + M \log_2 |G|) \| f \|^M_{L^p(G)}$$

Now taking the M^{th} root,

$$\| \widehat{f} \|_{L^q(\widehat{G})} \leq \sqrt[M]{400(1 + M \log_2 |G|} \| f \|_{L^p(G)}$$

Finally, taking the limit as M goes to infinity yields

$$\| \widehat{f} \|_{L^q(\widehat{G})} \leq \| f \|_{L^p(G)}$$

□

Chapter 6

Tao's Refinement

6.1 Tao's Refinement

Terence Tao has proved a refinement to Theorem 56. We will prove his result, but we will need a number of preliminary lemmas to do so. Again, we will first state these lemmas and then provide proofs for them in a later section. Notice that this refinement applies to cyclic groups.

Theorem 75. *(Tao's Refinement): Let p be a prime number. If $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ is a nonzero function, then*

$$|suppf| + |supp\widehat{f}| \geq p + 1.$$

Conversely, if A and B are two non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$ such that $|A| + |B| \geq p + 1$, then there exists a function f such that $suppf = A$ and $supp\widehat{f} = B$.

6.1.1 Why is this a Refinement?

Before we provide the lemmas and proofs, let us first examine why this result is an improvement of the uncertainty principle. To do this, we will show that, from Tao's refinement, we can recover our original uncertainty principle.

Lemma 76. *If $a + b \geq p + 1$ for a, b, p positive integers, then $a \times b \geq p$.*

Proof. We know that $a + b \geq p + 1$. We will obtain our result by contradiction, so let us assume that $ab < p$. Let us consider two cases: $b = 1$ and $b > 1$.

Case 1: Assume $b = 1$, then $ab < p$ implies that $a < p$, but $a + b \geq p + 1$ implies that $a = ab \geq p$. So we have a contradiction.

Case 2: Assume $b > 1$. Then $ab < p$ implies that $a < \frac{p}{b}$. But $a + b \geq p + 1$ implies that $a \geq p + 1 - b$. Combining the two inequalities, we get that $p + 1 - b < \frac{p}{b}$. Multiplying through by b, we get $bp + b - b^2 < p$. Subtracting bp from both sides and factoring, we get that $b(1 - b) < p(1 - b)$. Since $b > 1$, we know $1 - b < 0$, so our inequality reduces to $b > p$. Since a is a positive integer, $ab \geq b$, so we get that $ab > p$, which is a contradiction.

Thus, if $a+b \geq p+1$, this implies that $ab \geq p$. Tao's refinement is indeed an improvement on the uncertainty principle. □

6.1.2 Lemmas for the Refinement

Lemma 77. *[19]: Let p be a prime, let n be a positive integer, and let $P(z_1, z_2, \ldots, z_n)$ be a polynomial with integer coefficients. If $\omega_1, \omega_2, \ldots, \omega_n$ are p^{th} roots of unity, not necessarily distinct, and $P(\omega_1, \omega_2, \ldots, \omega_n) = 0$, then $P(1, 1, \ldots, 1)$ is a multiple of p.*

Lemma 78. *The n^{th} derivative of the polynomial $\prod_{1\leq i<j\leq n}(z_j - z_i)$ yields:*

$$\frac{d^{(n-1)}}{dz_n^{(n-1)}} \prod_{1\leq i<j\leq n} (z_j - z_i) = (n-1)! \prod_{1\leq i<j\leq n-1} (z_j - z_i).$$

The following Lemma says that all minors of the Fourier matrix are invertible.

Lemma 79. *Let p be a prime and let $1 \leq n \leq p$. Let $x_1, x_2, \ldots, x_n$ be distinct elements of $\mathbb{Z}/p\mathbb{Z}$ and let $y_1, y_2, \ldots, y_n$ also be distinct elements of $\mathbb{Z}/p\mathbb{Z}$. Then the matrix $\left(e^{2\pi i x_j y_k/p}\right)_{1\leq j,k\leq n}$ has a non-zero determinant.*

Corollary 80. *If p is a prime, and $A, \tilde{A}$ are non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$ such that $|A| = |\tilde{A}|$, then the linear transformation $T : l^2(A) \to l^2(\tilde{A})$ defined by $Tf = \widehat{f}|_{\tilde{A}}$ (the restriction of the Fourier transform of f to $\tilde{A}$) is invertible. Here, $l^2(A)$ denotes the functions $f : G \to \mathbb{C}$ which are equal to zero outside of A.*

6.1.3 Proof of the Refinement

Tao's Refinement (Theorem 75): *Let p be a prime number. If $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ is a nonzero function, then*

$$|supp f| + |supp \widehat{f}| \geq p + 1.$$

Conversely, if A and B are two non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$ such that $|A| + |B| \geq p + 1$, then there exists a function f such that $supp f = A$ and $supp \widehat{f} = B$.

Proof. [16]: Let us prove the first statement by contradiction. Assume$|\text{supp} f| + |\text{supp}\widehat{f}| \leq p$. Let $A := \text{supp}(f)$. We can then find a set $\tilde{A} \subseteq \mathbb{Z}/p\mathbb{Z}$ such that $\tilde{A} \cap \text{supp}(\widehat{f}) = \emptyset$ with $|\tilde{A}| = |A|$. If $Tf|_A = \widehat{f}|_{\tilde{A}}$, then by Corollary 80 we know that T is invertible. Since $\tilde{A}$ is disjoint from $\text{supp}(\widehat{f})$, we know $\widehat{f}|_{\tilde{A}} = 0$. Because T is invertible, this implies that $f|_A = 0$. But $f|_A \neq 0$ by definition, so this is a contradiction. Therefore, $|\text{supp} f| + |\text{supp}\widehat{f}| \geq p + 1$.

To prove the second statement, let us assume A and B are two non-empty subsets of $\mathbb{Z}/p\mathbb{Z}$ such that $|A| + |B| \geq p + 1$. First, let us assume that $|A| + |B| = p + 1$. Let us pick a subset $\tilde{A} \in \mathbb{Z}/p\mathbb{Z}$ such that $|\tilde{A}| = |A| = n$ and let the intersection of $\tilde{A}$ and B contain just one element, say ξ. Because the linear map T defined in Corollary 80 is invertible, we can find a non-zero function $f \in l^2(A)$ such that $\widehat{f}$ is zero on $\tilde{A} \backslash \{\xi\}$ but $\widehat{f}(\xi) \neq 0$. But since

$\tilde{A} \cap B = \{\xi\}$ and $\widehat{f}$ is zero on $\tilde{A}\backslash\{\xi\}$, this implies that $\text{supp}\widehat{f} \subseteq B$. Also, since $f \in l^2(A)$, $\text{supp}f \subseteq A$. But by the first part of the theorem, $\text{supp}f = A$ and $\text{supp}\widehat{f} = B$.

When we consider the case where $|A|+|B| > p+1$, we can find subsets A' and B' of A and B respectively, such that $|A'| + |B'| = p + 1$. We can then take generic linear combinations as A' and B' vary. We will eventually conclude that for all $A' \subseteq A$, if $x \in A'$ then $x \in \text{supp}f$ for some $f \in l^2(A)$. Similarly, for all $B' \subseteq B$, if $y \in B'$ then $y \in \text{supp}\widehat{f}$. Thus, $A = \text{supp}f$ and $B = \text{supp}\widehat{f}$. □

Remark. Note that if our group did not have prime order, then this result would not be true. For example, consider the group $\mathbb{Z}_6$. If our function was the indicator function of the subgroup $H = \{0, 2, 4\}$, then $|\text{supp}f| = 3$. From Lemma 63 and Lemma 64, we know that $|\text{supp}\widehat{f}| = \frac{|G|}{|H|} = 2$. Then $|\text{supp}f| + |\text{supp}\widehat{f}| = 5 < 7$. We could also consider our repeating example of the Klein 4-group. Obviously, $|G| = 4$, and we have a subgroup of order 2, $H = \{e, a\}$. Then $|\text{supp}f| = 2$, and again by the two lemmas mentioned above, $|\text{supp}\widehat{f}| = 2$. So $|\text{supp}f| + |\text{supp}\widehat{f}| = 4 < 5$, so our refinement cannot be applied to groups without prime order.

6.2 Proofs of Lemmas

Here we prove the three lemmas we used to prove Tao's Refinement of the uncertainty principle.

Proof. (Proof of Lemma 77): Let p be a prime, let n be a positive integer, and let $P(z_1, z_2, \ldots, z_n)$ be a polynomial with integer coefficients. Our goal is to show that if $\omega_1, \omega_2, \ldots, \omega_n$ are p^{th} roots of unity, not necessarily distinct, and $P(\omega_1, \omega_2, \ldots, \omega_n) = 0$, then $P(1, 1, \ldots, 1)$ is a multiple of p. Consider

$$P(z_1, z_2, \ldots, z_n) := \sum_{1 \leq i_1, i_2, \ldots, i_n \leq r} a_{i_1 i_2 \cdots i_n} z_1^{i_1} z_2^{i_2} \cdots z_n^{i_n},$$

where $a_{i_1 i_2 \cdots i_n} \in \mathbb{Z}$.

Then

$$P(z^{k_1}, z^{k_2}, \ldots, z^{k_n}) = \sum_{1 \leq i_1, i_2 \ldots, i_n \leq r} a_{i_1 i_2 \cdots i_n} z^{(k_1 i_1 + k_2 i_2 + \cdots + k_n i_n)}.$$

Let us divide $P(z^{k_1}, z^{k_2}, \ldots, z^{k_n})$ by $z^p - 1$. Then $P(z^{k_1}, z^{k_2}, \ldots, z^{k_n}) = Q(z)(z^p - 1) + R(z)$, where $deg(R(z)) \leq p - 1$. The $Q(z)$ and $R(z)$ depend on our choice of k_is, so let use choose the k_is so that $R(z)$ will be of the form $R(z) = \sum_{i=0}^{p-1} \alpha_i z^i$ with $\alpha_i \in \mathbb{Z}$.

Let $\omega = e^{2\pi i/p}$, and $\omega_j(k) = \omega^{k_j}$. We know $P(\omega_1, \omega_2, \ldots, \omega_n) = 0$, and $\omega^p - 1 = 0$. This implies that $R(\omega) = 0$. Consider $f(x) = 1 + x + x^2 + \cdots + x^{p-1}$, then $f(x)$ is irreducible over $\mathbb{Q}$ ([10], pg.216, Corollary 23.17). But since ω is a root of $f(x)$ and $f(x)$ is irreducible, $f(x) = qR(x)$, $q \in \mathbb{Q}$ since irreducible polynomials for α over $\mathbb{C}$ are unique up to a constant factor, ([10], pg. 269, Theorem 29.13). But since $R(x)$ has integer coefficients, and so does $f(x)$, this implies that the constant multiple $k = \frac{1}{q} \in \mathbb{Z}$, since $\frac{1}{q} f(x) = R(x)$.

Consider $P(1,1,\ldots,1) = P(1^{k_1}, 1^{k_2}, \ldots, 1^{k_n}) = Q(1)(1^p - 1) + R(1)$. Since $1^p - 1 = 0$, this implies that $P(1,1,\ldots,1) = R(1)$. But $R(1) = k(1 + 1 + 1^2 + \cdots + 1^{p-1}) = pk$, some $k \in \mathbb{Z}$. Thus, $P(1,1,\ldots,1) = pk$, and $P(1,1,\ldots,1)$ is a multiple of p. □

Proof. (Proof of Lemma 78): Consider

$$\prod_{1\le i<j\le n}(z_j - z_i) = (z_n - z_{n-1})(z_n - z_{n-2})\cdots(z_n - z_1)\prod_{1\le i<j\le n-1}(z_j - z_i).$$

Then we want to calculate its n^{th} derivative:

$$\frac{d^{(n-1)}}{dz_n^{(n-1)}}\prod_{1\le i<j\le n}(z_j - z_i) = \frac{d^{(n-1)}}{dz_n^{(n-1)}}\left((z_n - z_{n-1})(z_n - z_{n-2})\cdots(z_n - z_1)\prod_{1\le i<j\le n-1}(z_j - z_i)\right)$$

Since $\prod_{1\le i<j\le n-1}(z_j - z_i)$ does not depend on z_n, we can pull it out front. Using the product rule, we get

$$\begin{aligned} &= \frac{d^{(n-1)}}{dz_n^{(n-1)}}\prod_{1\le i<j\le n}(z_j - z_i) \\ &= \left(\prod_{1\le i<j\le n-1}(z_j - z_i)\right)\frac{d^{(n-1)}}{dz_n^{(n-2)}}[(z_n - z_{n-2})(z_n - z_{n-3})\cdots(z_n - z_1) + \cdots \\ &\quad \cdots + (z_n - z_{n-1})(z_n - z_{n-2})\cdots(z_n - z_2)] \end{aligned}$$

Since we started with $n-1$ linear terms multiplied together, we get $n-1$ terms, each with $n-2$ linear terms once we apply the product rule. Since we are taking the $(n-1)th$ derivative, we will eventually end up taking the first derivative of $(n-1)!$ linear terms. Thus,

$$\frac{d}{dz_n}^{(n-1)}\prod_{1\le i<j\le n}(z_j - z_i) = (n-1)!\prod_{1\le i<j\le n-1}(z_j - z_i).$$

□

Proof. (Proof of Lemma 79) [16]: Let p be a prime and let $1 \le n \le p$. Let $x_1, x_2, \ldots, x_n$ be distinct elements of $\mathbb{Z}/p\mathbb{Z}$ and let $y_1, y_2, \ldots, y_n$ also be distinct elements of $\mathbb{Z}/p\mathbb{Z}$. Our goal is to show that the matrix $\left(e^{2\pi i x_j y_k/p}\right)_{1\le j,k\le n}$ has a non-zero determinant. Define $\omega_j := e^{2\pi i x_j/p}$. Each ω_j is a distinct root of unity, and we need to show that

$$det(\omega_j^{y_k})_{1\le j,k\le n} \neq 0,$$

where $y_1, y_2, \ldots, y_n$ are also distinct elements of $\mathbb{Z}_p$.

Let us define a polynomial $D(z_1, z_2, \ldots, z_n)$ of n variables as

$$D(z_1, z_2, \ldots, z_n) := det(z_j^{y_k})_{1\le j,k\le n}.$$

$D(z_1, z_2, \ldots, z_n)$ is obviously a polynomial with integer coefficients.

If $z_j = z_{j'}$, we would have two identical rows of our matrix, so $D(z_1, z_2, \ldots, z_n) = 0$. Thus, we can factorize D to get

$$D(z_1, z_2, \ldots, z_n) = P(z_1, z_2, \ldots, z_n) \prod_{1 \le j < j' \le n} (z_j - z_{j'})$$

where $P(z_1, z_2, \ldots, z_n)$ is some polynomial with n variables and integer coefficients. Note that there are $\binom{n}{2} = \frac{n!}{(n-2)!2!} = \frac{n(n-1)}{2}$ linear factors in D in the product.

We will try to show that $P(1, 1, \ldots, 1)$ is not a multiple of p, which Lemma 77 will then tell us that $P(\omega_1, \omega_2, \ldots, \omega_n)$ is non-zero. This will prove our claim, since $\prod_{1 \le j < j' \le n}(\omega_j - \omega_{j'}) \neq 0$, since ω_js are all distinct.

In order to compute $P(1, 1, \ldots, 1)$, we will differentiate D a number of times.

Consider the expression

$$\left(z_1 \frac{d}{dz_1}\right)^0 \left(z_2 \frac{d}{dz_2}\right)^1 \left(z_3 \frac{d}{dz_3}\right)^2 \cdots \left(z_n \frac{d}{dz_n}\right)^{n-1} D(z_1, z_2, \ldots, z_n) \tag{6.2.1}$$

Now note that there are $0+1+2+\cdots+(n-1) = \frac{n(n-1)}{2}$ differentiation operators applied to D, which is the same as the number of linear factors in D. Moreover, there are $n-k$ linear factors involving z_{n-k+1}.

When we take the derivative of D, we will need to use the product rule $\frac{n(n-1)}{2}$ times. We will end up adding numerous terms together, with each term having a combination of linear factors multiplied by various derivatives of $P(z_1, z_2, \ldots, z_n)$. The only term that will have no linear factors will be $P(z_1, z_2, \ldots, z_n)$, multiplied by $z_1 z_2 \cdots z_n$ and $\left(z_1 \frac{d}{dz_1}\right)^0 \left(z_2 \frac{d}{dz_2}\right)^1 \left(z_2 \frac{d}{dz_3}\right)^2 \cdots \left(z_n \frac{d}{dz_n}\right)^{n-1} \prod_{1 \le j < j' \le n}(z_j - z_{j'})$, which we can calculate using Lemma 78. This will be the only term that matters, since when we plug in 1 for all the z_i, that will be the only term that doesn't equal zero because all other terms will have at least one linear factor. We can see this if we just consider taking the first few derivatives. To begin with, let's compute $z_n \frac{d}{dz_n}\big(D(z_1, z_2, \ldots, z_n)\big)$. Let's call $P(z_1, z_2, \ldots, z_n) = f$ and $\prod_{1 \le j < j' \le n}(z_j - z_{j'}) = g$. Then $D(z_1, z_2, \ldots, z_n) = fg$, and

$$z_n \frac{d}{dz_n}\big(D(z_1, z_2, \ldots, z_n)\big) = z_n\big(f \frac{dg}{dz_n} + g \frac{df}{dz_n}\big).$$

Now consider

$$z_n \frac{d}{dz_n}\left(z_n \frac{d}{dz_n}(fg)\right) = z_n \left(f \frac{dg}{dz_n} + z_n \frac{dg}{dz_n}\frac{df}{dz_n} + z_n f \frac{d^2 g}{dz_n^2} + g \frac{df}{dz_n} + z_n \frac{dg}{dz_n}\frac{df}{dz_n} + z_n g \frac{d^2 f}{dz_n^2}\right)$$

If we continue until we take the n^{th} derivative, we will end up with a term $z_n^n f \frac{d^n g}{dz_n^n}$. All of the other terms will be of the form

$$z_n^k \frac{d^j f}{dz_n^j} \frac{d^i g}{dz_n^i}$$

where $0 \le k \le n$, $0 \le j \le n$, and $0 \le i \le n-1$. We can write $\frac{d^n g}{dz_n^n}$ as $(n-1)! \prod_{1 \le i < j \le n-1}(z_j - z_i)$ by Lemma 78. We can do the same process for $z_{n-1}, \ldots, z_1$. We will eventually be left

with a very large sum of terms that each contain something of the form $\frac{d^k g}{dz_j}$ where $k < g$, except one term, which will be $z_n^n z_{n-1}^{n-1} \cdots z_1 f(n-1)!(n-2)! \cdots 1$. In the first type of term mentioned, there will always be some sort of linear factor of the form $(z_i - z_k)$. When we plug in 1 for all of the $z_j s$, these terms will all vanish. Thus,

$$\left(z_1\frac{d}{dz_1}\right)^0\left(z_2\frac{d}{dz_2}\right)^1\cdots\left(z_n\frac{d}{dz_n}\right)^{n-1} D(z_1,z_2,\ldots,z_n)|_{z_1=\cdots=z_n=1} \;=\; (n-1)!\cdots 1!P(1,1,\ldots,1).$$

Since $n < p$, $(n-1)!(n-2)!\cdots 1!$ is not divisible by the prime number p, we need only show that the above formula is not a multiple of p to show that $P(1,1,\ldots,1)$ is not divisible by p.

Let S_n denote the group of permutations on n objects. By the definition of the determinant[2],

$$D(z_1,z_2,\ldots,z_n) = \sum_{\sigma\in S_n} sgn(\sigma)\prod_{j=1}^{n} z_j^{y_{\sigma(j)}}$$

So we can write equation 6.2.1 as

$$\begin{aligned}
&\left(z_1\frac{d}{dz_1}\right)^0\left(z_2\frac{d}{dz_2}\right)^1\left(z_2\frac{d}{dz_3}\right)^2\cdots\left(z_n\frac{d}{dz_n}\right)^{n-1}\sum_{\sigma\in S_n} sgn(\sigma)\prod_{j=1}^{n} z_j^{y_{\sigma(j)}}\\
=\;&\sum_{\sigma\in S_n} sgn(\sigma)\left(z_1\frac{d}{dz_1}\right)^0\left(z_2\frac{d}{dz_2}\right)^1\left(z_2\frac{d}{dz_3}\right)^2\cdots\left(z_n\frac{d}{dz_n}\right)^{n-1}\prod_{j=1}^{n} z_j^{y_{\sigma(j)}}\\
&\sum_{\sigma\in S_n} sgn(\sigma)\left(z_1\frac{d}{dz_1}\right)^0\left(z_2\frac{d}{dz_2}\right)^1\left(z_2\frac{d}{dz_3}\right)^2\cdots\left(z_{n-1}\frac{d}{dz_{n-1}}\right)^{n-2} y_{\sigma(n)}^{n-1}\prod_{j=1}^{n} z_j^{y_{\sigma(j)}}\\
=\;&\sum_{\sigma\in S_n} sgn(\sigma)\left(z_1\frac{d}{dz_1}\right)^0\left(z_2\frac{d}{dz_2}\right)^1\left(z_2\frac{d}{dz_3}\right)^2\cdots\left(z_{n-2}\frac{d}{dz_{n-2}}\right)^{n-3} y_{\sigma(n)}^{n-1}y_{\sigma(n-1)}{}^{n-2}\prod_{j=1}^{n} z_j^{y_{\sigma(j)}}\\
&\vdots\\
=\;&\sum_{\sigma\in S_n} sgn(\sigma) y_{\sigma(n)}^{n-1}y_{\sigma(n-1)}^{n-2}\cdots y_{\sigma(2)}1\prod_{j=1}^{n} z_j^{y_{\sigma(j)}}
\end{aligned}$$

Since we are concerned only when $z_1 = z_2 = \cdots = z_n = 1$,

$$\begin{aligned}
&\left(z_1\frac{d}{dz_1}\right)^0\left(z_2\frac{d}{dz_2}\right)^1\left(z_2\frac{d}{dz_3}\right)^2\cdots\left(z_n\frac{d}{dz_n}\right)^{n-1} D(1,1,\ldots,1)\\
=\;&\sum_{\sigma\in S_n} sgn(\sigma) y_{\sigma(n)}^{n-1}y_{\sigma(n-1)}^{n-2}\cdots y_{\sigma(2)}1\\
=\;&\sum_{\sigma\in S_n} sgn(\sigma)\prod_{j=1}^{n} y_{\sigma(j)}^{j-1}
\end{aligned}$$

But this is the Vandermonde determinant, which we know to be $\prod_{1\le i<j\le n}(y_j - y_i)$. Since $y_i \in \mathbb{Z}/p\mathbb{Z}$ and all y_i are distinct, we know that $\prod_{1\le i<j\le n}(y_j - y_i)$ is not a multiple of p. Thus, $P(1,1,\ldots,1)$ is not a multiple of p. By Lemma 77, this implies that $P(\omega_1,\omega_2,\ldots,\omega_n) \neq 0$, and furthermore that $D(\omega_1,\omega_2,\ldots,\omega_n) = det(\left(e^{2\pi i x_j y_k/p}\right) \neq 0$. □

Proof. (Proof of Corollary 80): Let p be a prime, and let $A, \tilde{A}$ be non-empty subsets of $\mathbb{Z}_p$ such that $|A| = |\tilde{A}|$. We want to prove that the linear transformation $T : l^2(A) \to l^2(\tilde{A})$ defined by $Tf|_A = \widehat{f}|_{\tilde{A}}$. Define $\omega := e^{2\pi i/p}$. By the definition of the Fourier transform equation 3.4.1, $\widehat{f}(\tilde{a}) = \sum_{a \in G} f(a)\omega^{\tilde{a}a}$. Since $f \in l^2(A)$, we can rewrite the Fourier transform as $\widehat{f}(\tilde{a}) = \sum_{a \in A} f(a)\omega^{\tilde{a}a}$. Let $|A| = n$ and let $A = \{a_1, a_2, \ldots, a_n\}$. Similarly, let $\tilde{A} = \{\tilde{a_1}, \tilde{a_2}, \ldots, \tilde{a_n}\}$.Consider the column vector

$$\begin{pmatrix} f(a_1) \\ f(a_2) \\ \vdots \\ f(a_n) \end{pmatrix} \tag{6.2.2}$$

We must apply a linear transformation, T, to equation 6.2.2 to get

$$\begin{pmatrix} \widehat{f}(\tilde{a_1}) \\ \widehat{f}(\tilde{a_2}) \\ \vdots \\ \widehat{f}(\tilde{a_n}) \end{pmatrix}.$$

By the definition of the Fourier transform,

$$T = \begin{pmatrix} \omega^{\tilde{a_1}a_1} & \omega^{\tilde{a_1}a_2} & \cdots & \omega^{\tilde{a_1}a_n} \\ \omega^{\tilde{a_2}a_1} & \omega^{\tilde{a_2}a_2} & \cdots & \omega^{\tilde{a_2}a_n} \\ \vdots & \vdots & \ddots & \vdots \\ \omega^{\tilde{a_n}a_1} & \omega^{\tilde{a_n}a_2} & \cdots & \omega^{\tilde{a_n}a_n} \end{pmatrix}$$

But we know from Lemma 79 that det(T) is non-zero, and so T is invertible. □

Chapter 7

Applications

After developing this new version of Fourier analysis, one might wonder, why have we done this? It turns out there are many applications of Fourier analysis on groups, two of which we will discuss in this section. First is a theoretical application of Tao's refinement of the uncertainty principle to the distribution of primes, and the second is a more practical application to the field of compressed sensing.

7.1 Arithmetic Progression of Primes

Tao's refinement has been used to prove a very impressive theorem by Tao and Ben Green, the Green-Tao Theorem. This result, along with other works, earned Terence Tao the prestigious Fields Medal in 2006.

Theorem 81. *(The Green-Tao Theorem): The prime numbers contain infinitely many arithmetic progressions of length k for all k.[11]*

Remark. The proof of this groundbreaking theorem is far beyond the scope of this text. However, it is mentioned because the ideas developed in Tao's refinement play a role in proving the above result.

We can see a simple example, where $k = 5 : 5, 11, 17, 23, 29$. This is only the first of an infinite list of arithmetic progressions of length 5 of prime numbers.

The longest known arithmetic progression is of length 26 and starts with the number 43142746595714191 with a difference of 5283234035979900. This was discovered in 2010 by Perichon [15].

7.2 Compressed Sensing

While we have created a comprehensive theory for Fourier analysis of groups, one might wonder if there is any practical application to such notions. In fact, compressed sensing, a very popular area of interest and research, relies heavily on the concepts we have just developed. Compressed sensing has applications to medical imaging and image compression. The military would like to implement this technique, using small, inexpensive cameras to

record small amounts of data that can later be reconstructed using compressed sensing to give a comprehensive view [5].

Lemma 82. *[16]: Let N be a prime number and T, Ω be subsets of $\mathbb{Z}_N$. Let $l_2(T)$ and $l_2(\Omega)$ be the spaces of signals that are zero outside of T and Ω respectively. The restricted Fourier transform $\mathcal{F}_{T\to\Omega} : l_2(T) \to l_2(\Omega)$ is defined as*

$$\mathcal{F}_{T\to\Omega} f := \widehat{f}|_\Omega \quad \text{for all } f \in l_2(T)$$

If $|T| = |\Omega|$, then $\mathcal{F}_{T\to\Omega}$ is a bijection. If $|T| \leq |\Omega|$, $\mathcal{F}_{T\to\Omega}$ is an injection, and if $|T| \geq |\Omega|$, then $\mathcal{F}_{T\to\Omega}$ is a surjection.

Proof. In Corollary 80, we proved that if $|T| = |\Omega|$, then the linear transformation $A : l_2(T) \to l_2(\Omega)$ defined as $Af = \widehat{f}|_\Omega$ is invertible. This implies that, if $|T| = |\Omega|$, then $\mathcal{F}_{T\to\Omega}$ is a bijection. Therefore, if $|T| \leq |\Omega|$, then $\mathcal{F}_{T\to\Omega}$ is an injection. Similarly, if $|T| \geq |\Omega|$, then $\mathcal{F}_{T\to\Omega}$ is a surjection. The theorem holds if the Fourier transform is replaced by the inverse Fourier transform. □

Theorem 83. *Let $f : \mathbb{Z}_\mathbb{N} \to \mathbb{C}$, with N being a prime number. Let Ω be a subset of $\{0, 1, 2, \ldots, N-1\}$ and f be a vector supported on T such that $|T| \leq \frac{1}{2}|\Omega|$. Then f can be constructed uniquely from Ω and $\widehat{f}|_\Omega$. Conversely, if Ω is not the set of all N frequencies, then there exist distinct vectors f, g such that $|supp(f)|, |supp(g)| \leq \frac{1}{2}|\Omega| + 1$ and $\widehat{f}|_\Omega = \widehat{g}|_\Omega$.*

Proof. [3]: Let us start with the first claim of the theorem. Assume that f is a vector supported on T such that $|T| \leq \frac{1}{2}|\Omega|$. Since $|T| \leq |\Omega|$, we know from Lemma 82 that $\mathcal{F}_{T\to\Omega}$ is injective. By the definition of injective, each element of $\widehat{f}|_\Omega$ in the range of $\mathcal{F}_{T\to\Omega}$ is the image of a unique element $f \in l_2(T)$. Equivalently, if $\mathcal{F}_{T\to\Omega} f_1 = \mathcal{F}_{T\to\Omega} f_2$ then $f_1 = f_2$. Therefore, we can reconstruct f. To prove uniqueness, assume there exists $f, g \in l_2(T)$ such that $|\text{supp}(f)|, |\text{supp}(g)| \leq \frac{1}{2}|\Omega|$ and $\widehat{f}|_\Omega = \widehat{g}|_\Omega$. Consider the function $f - g$. Since $\widehat{f-g} = \widehat{f} - \widehat{g}$, we know that the Fourier transform of $f - g$ vanishes on Ω. Also, $|\text{supp}(f-g)| \leq |\Omega|$. Again by Lemma 82, we know that $\mathcal{F}_{\text{supp}(f-g)\to\Omega}$ is injective. But since $\widehat{f-g}|_\Omega = 0$, this implies that $f - g = 0$. Thus, $f = g$.

Now, consider the second statement of the theorem. Assume that $|\Omega| < N$. We can find disjoint subsets S, T such that $|S|, |T| \leq \frac{1}{2}|\Omega| + 1$ and $|T| + |S| = |\Omega| + 1$. Let a_0 be a frequency which is not in Ω. By Lemma 82, we know that $\mathcal{F}_{T\cup S\to\Omega\cup\{a_0\}}$ is a bijection. This implies that we can find a vector h that's supported on $T \cup S$ that vanishes on Ω but is non-zero at a_0. Thus, h is non-zero. If we then define $f := h|_T$ and $g := h|_S$, we have that $\widehat{f}|_\Omega = \widehat{g}|_\Omega$ and $|\text{supp}(f)|, |\text{supp}(g)| \leq \frac{1}{2}|\Omega|$. □

While there is much, much more involved in the quickly-developing field of compressed sensing, the above theorems show how closely compressed sensing is related to Tao's refinement.

Bibliography

[1] "Abstract Algebra, Exam II." Math.harvard.edu. Harvard University, n.d. Web. 17 Nov. 2013.

[2] Bell, Jordan. "Uncertainty Principles and Compressed Sensing." Math.toronto.edu. N.p., n.d. Web. 28 June 2013.

[3] Candes, E.J., J. Romberg, and T. Tao. "Robust Uncertainty Principles: Exact Signal Reconstruction from Highly Incomplete Frequency Information." IEEE Transactions on Information Theory 52.2 (2006): 489-509. Print.

[4] Candes, Emmanuel, and Terence Tao. "Near Optimal Signal Recovery From Random Projections: Universal Encoding Strategies?" Arxiv.org. N.p., 4 Apr. 2006. Web. 30 Nov. 2013.

[5] Chang, Kenneth. "SCIENTIST AT WORK: Terence Tao; Journeys to the Distant Fields of Prime." The New York Times. The New York Times, 13 Mar. 2007. Web. 17 Nov. 2013.

[6] Conrad, Keith. "Characters of Finite Abelian Groups." Math.uconn.edu. N.p., n.d. Web. 8 Dec. 2012. <http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/charthy.pdf>.

[7] "Convexity, Inequalities, and Norms." Math.bard.edu. N.p., n.d. Web. 25 July 2013.

[8] "Dyadic Decomposition." Tricki. N.p., n.d. Web. 09 Aug. 2013. <http://www.tricki.org/article/Dyadic_decomposition>.

[9] "Entropic Uncertainty." Wikipedia. Wikimedia Foundation, 10 Oct. 2013. Web. 17 Nov. 2013.

[10] Fraleigh, John B. A First Course in Abstract Algebra. Reading, MA: Addison-Wesley Pub., 1967. Print.

[11] Green, Ben, and Terence Tao. "The Primes Contain Arbitrarily Long Arithmetic Progressions." Arxiv.org. N.p., 23 Sept. 2007. Web. 17 Nov. 2013.

[12] Hatami, Hamed. "COMP760, Lectures 2,3: Fourier Analysis of Finite Abelian Groups."Cs.mcgill.ca. N.p., n.d. Web. 19 June 2013.

[13] Matusiak, Ewa, Murad Ozaydın, and Tomasz Przebinda. "The Donoho-Stark Uncertainty Principle for a Finite Abelian Group." University of Oklahoma, n.d. Web. 7 Dec. 2013.

[14] Pereyra, María Cristina., and Lesley A. Ward. Harmonic Analysis: From Fourier to Wavelets. Providence, RI: American Mathematical Society, 2012. Print.

[15] "Primes in Arithmetic Progression Records." Primes in Arithmetic Progression Records. N.p., n.d. Web. 30 Nov. 2013. <http://users.cybercity.dk/~dsl522332/math/aprecords.htm>.

[16] Tao, Terence. "An Uncertainty Principle for Cyclic Groups of Prime Order." Math.Res.Lett.12, 121-127 (2005).

[17] Tao, Terence. "The Tensor Power Trick." What's New. Wordpress, 25 Aug. 2008. Web. 31 July 2013.

[18] "Triangle Inequality for Complex Numbers." Math.ucdavis.edu. University of California, Davis, n.d. Web. 14 Nov. 2013.

[19] Vasanth, L. "An Uncertainty Principle for Finite Abelian Groups and Cyclic Groups of Prime Orders." International Journal of Emerging Trends in Engineering and Development 3.1 (2011): 247. Web. 2 July 2013.

[20] "Young's Inequality for Products." - ProofWiki. N.p., n.d. Web. 25 July 2013.