Heisenberg's Uncertainty Principle

Daniel Penner

The principle, motivated by quantum mechanics, expresses the idea that a function and its Fourier transform cannot both be localized. Specificially, it states the following:

Main Theorem (Heisenberg's Inequality)**.** *If $f \in L^2$, and $\|f\| = 1$, then*

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

In the first section, I will introduce a few basic results of Fourier analysis on the class of Schwartz functions (which have very strong decay and smoothness assumptions), and prove the above inequality for Lebesgue square-integrable functions. The general idea of the proof is due to Dym and McKean [1]. In the second section, I will discuss analogues of the inequality for functions defined on finite abelian groups.

1 Heisenberg's Inequality on $L^2(\mathbb{R})$

1.1 Basic Fourier Analysis on $L^2(\mathbb{R})$

We define $L^2(\mathbb{R})$ (henceforth abbreviated as L^2) as the set of real-valued functions $f : \mathbb{R} \to \mathbb{R}$ which have finite L^2 norm, that is, for which

$$\|f\| = \|f\|_{L^2(\mathbb{R})} = \left(\int_{\mathbb{R}} |f(x)|^2 dx\right)^{1/2} < \infty.$$

A function $f \in L^2$ is called **Schwartz** if it is indefinitely differentiable, and if all its derivatives enjoy rapid decrease, that is, that $\sup_{x\in\mathbb{R}} |x|^k |f^l(x)| < \infty$ for every $k, l \geq 0$. If f is a Schwartz function, we can define its **Fourier transform** $\hat{f} : \mathbb{R} \to \mathbb{R}$ as

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

and note that the Fourier transform of a Schwartz function is itself a Schwartz function. As a consequence, the **Fourier inversion formula** holds for any Schwartz function, which states that a function can be recovered from its Fourier transform as follows:

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

It is easily verified that the set of Schwartz functions is a subspace of L^2, and we take for granted that the subspace of Schwartz functions is in fact dense in L^2. That is to say, for any $f \in L^2$ there is a sequence f_n of Schwartz functions such that $\|f_n - f\| \to 0$ as $n \to \infty$. The following theorem (whose proof we will not repeat, but is a quick application of convolutions) states that the Fourier transform is a unitary mapping on the subspace of Schwartz functions.

Theorem 1.1 (Plancherel's Formula)**.** *If f is Schwartz, then $\|f\| = \|\hat{f}\|$.*

The density of the Schwartz space in L^2 gives us a natural extension of the Fourier transform, as follows. Given $f \in L^2$, let f_n be a sequence of Schwartz functions converging to f in L^2. Theorem 1.1 gives us that

$$\|\hat{f}_n - \hat{f}_m\| = \|\widehat{f_n - f_m}\| = \|f_n - f_m\| \leq \|f_n - f\| + \|f - f_m\|,$$

and taking $m, n \to \infty$ shows that $\hat{f}_n$ is a Cauchy sequence in L^2. Since L^2 is complete, this implies that $\hat{f}_n$ converges to some limit which we call $\hat{f}$ and *define* as the Fourier transform of f. The Fourier inversion and Plancherel formulae for this Fourier transform follow immediately from limiting arguments with Schwartz approximations, and we take for granted that other familiar and necessary properties of the Fourier transform (linearity, uniqueness of the limit for any sequence f_n, etc) carry over from the Schwartz case.

1.2 Two Approximation Lemmas

Before approaching Heisenberg's inequality, we require two lemmas, both of which make the assumption that one of the terms on the left-hand side of the desired inequality, $\|\xi\hat{f}(\xi)\|$ and $\|xf(x)\|$, is finite. This assumption is natural, since in the case that either fails, the inequality is trivial.

Lemma 1.2. *If $f \in L^2$, and $\|\xi\hat{f}(\xi)\| < \infty$, there is a sequence f_n of Schwartz functions such that*

$$\int_{\mathbb{R}} (1 + 4\pi^2\xi^2)|\hat{f}_n(\xi) - \hat{f}(\xi)|^2 d\xi \to 0.$$

Proof. We first notice that we can restrict our attention to the case in which $\hat{f}$ is compactly supported, since otherwise we can let

$$\hat{f}_n(\xi) = \begin{cases} \hat{f}(\xi) & |\xi| \leq n \\ 0 & \text{otherwise.} \end{cases}$$

to see that

$$\int_{\mathbb{R}} (1 + 4\pi^2\xi^2)|\hat{f}_n(\xi) - \hat{f}(\xi)|^2 d\xi = \int_{|x|>n} (1 + 4\pi^2\xi^2)|\hat{f}(\xi)|^2 d\xi$$

$$= \int_{|x|>n} |\hat{f}(\xi)|^2 d\xi + 4\pi^2 \int_{|x|>n} \xi^2 |\hat{f}(\xi)|^2 d\xi \to 0 \quad \text{as } n \to \infty,$$

the first term because $f \in L^2$ and therefore $\hat{f} \in L^2$, and the latter by our assumption that $\xi\hat{f}(\xi) \in L^2$ as well.

Now assuming that $\hat{f}$ is compactly supported and satisfies our hypotheses, we let φ be a non-negative Schwartz function supported in $[-1,1]$ for which $\int_{\mathbb{R}} \varphi(x)dx = 1$. Then if we let $\varphi_n(x) = n\varphi(nx)$, we see that the family $\{\varphi_n\}_{n=1}^{\infty}$ is an approximation to the identity, in the sense that for each n, the integral of φ_n on $\mathbb{R}$ is 1, $|\varphi_n(x)| \leq An$ everywhere, and $|\varphi_n(x)| \leq A/n|x|^2$, where A is a constant (the first two properties are immediate, and the third follows by examining small values of $|x|$ since φ_n is supported in $[-1,1]$).

Then [2, 112] the convolution $\hat{f}_n(\xi) = (\hat{f} * \varphi_n)(\xi)$ tends to $\hat{f}(\xi)$ as $n \to \infty$ for almost every $\xi \in \mathbb{R}$ (particularly, those in the Lebesgue set of $\hat{f}$). So what we see is that

$$\begin{aligned}\int_{\mathbb{R}} (1+4\pi^2\xi^2)|\hat{f}_n(\xi) - \hat{f}(\xi)|^2 d\xi &\leq (1+4\pi^2A^2)\int_{\mathbb{R}} |\hat{f}_n(\xi) - \hat{f}(\xi)|^2 d\xi \\ &= (1+4\pi^2A^2)\left(\int_L |\hat{f}_n(\xi) - \hat{f}(\xi)|^2 d\xi + \int_{L^c} |\hat{f}_n(\xi) - \hat{f}(\xi)|^2 d\xi\right) \\ &\leq (1+4\pi^2A^2)m(L)\sup_{\xi\in L} |\hat{f}_n(\xi) - \hat{f}(\xi)|^2 \to 0,\end{aligned}$$

as $n \to \infty$, where A is some finite bound for the support of $\hat{f}$ and the limit tends to zero by the pointwise convergence of $\hat{f}_n \to \hat{f}$, and since the integral on the complement of the Lebesgue set is zero (since it has measure zero). □

Lemma 1.3. *If $f \in L^2$, and $\|xf(x)\| < \infty$, then for each integer $n \in \mathbb{Z}$ there is a number $l_n \in (n, n+1)$ such that*

$$\lim_{n\to\infty} l_n(|f(l_n)|^2 + |f(-l_n)|^2) = 0.$$

Proof. First we can rewrite

$$\sum_{n=-\infty}^{\infty} \int_n^{n+1} x^2|f(x)|^2 dx = \int_{\mathbb{R}} x^2|f(x)|^2 dx < \infty,$$

for each n we can pick some $l_n \in (n, n+1)$ such that $|f(l_n)|^2$ is minimal in the given interval, and thus $\sum_{n=-\infty}^{\infty} n^2|f(l_n)|^2 < \int_{\mathbb{R}} x^2|f(x)|^2 dx < \infty$, so since $l_n \in (n, n+1)$, we must have that the limits $\lim_{n\to\infty} l_n^2|f(l_n)|^2 = 0$ and $\lim_{n\to\infty} |-l_n|^2|f(-l_n)|^2 = 0$. Finally, since for large n these terms dominate the terms $l_n|f(l_n)|^2$ and $l_n|f(l_n)|^2$, our claim is proved. □

1.3 The Proof

Theorem 1.4 (Heisenberg's Inequality)**.** *If $f \in L^2$, and $\|f\| = 1$, then*

$$\left(\int_{\mathbb{R}} x^2|f(x)|^2 dx\right)\left(\int_{\mathbb{R}} \xi^2|\hat{f}(\xi)|^2 d\xi\right) \geq \frac{1}{16\pi^2},$$

and equality holds if and only if $f(x) = Ae^{-Bx^2}$ where $B > 0$ and $|A|^2 = \sqrt{2B/\pi}$.

Proof. First we note that we may assume that $\|\xi\hat{f}(\xi)\|, \|xf(x)\| < \infty$, since otherwise the inequality is trivial.

Now, since f may be non-differentiable, we define $f'(x) = \int_{\mathbb{R}} 2\pi i\xi\hat{f}(\xi)e^{2\pi ix\xi}d\xi$ in line with what Fourier inversion would give us for the deriviatve of f, were f known to be differentiable. We know that $f' \in L^2$ and is well-defined by our assumption that $\|\xi\hat{f}\| < \infty$. Immediately from our definition we obtain that

$$4\pi^2\left(\int_{\mathbb{R}} x^2|f(x)|^2dx\right)\left(\int_{\mathbb{R}} \xi^2|\hat{f}(\xi)|^2d\xi\right) = \left(\int_{\mathbb{R}} |xf(x)|^2dx\right)\left(\int_{\mathbb{R}} |2\pi i\xi\hat{f}(\xi)|^2d\xi\right)$$

$$= \left(\int_{\mathbb{R}} |xf(x)|^2dx\right)\left(\int_{\mathbb{R}} |f'(x)|^2dx\right) \geq \left[\int_{\mathbb{R}} |xf'(x)\overline{f(x)}|dx\right]^2 = \left[\int_{\mathbb{R}} \frac{x}{2}(f'(x)\overline{f(x)} + \overline{f'(x)}f(x))dx\right]^2,$$

where the inequality is Cauchy-Schwarz.

Now by Lemma 1.2 we may pick a sequence of Schwartz functions f_n such that

$$\int_{\mathbb{R}} (1 + 4\pi^2\xi^2)|\hat{f}_n(\xi) - \hat{f}(\xi)|^2d\xi \to 0.$$

An application of the Plancherel formula (with the fact that since f_n is a Schwartz function, then $\widehat{f_n'} = \int_{\mathbb{R}} 2\pi i\xi f_n(x)dx$) gives us that

$$\|f_n - f\|^2 + \|f_n' - f'\|^2 = \|\hat{f}_n - \hat{f}\|^2 + \|2\pi i\xi(\hat{f}_n - \hat{f})\|^2 = \int_{\mathbb{R}} (1 + 4\pi^2\xi^2)|\hat{f}_n(\xi) - \hat{f}(\xi)|^2d\xi \to 0,$$

as $n \to \infty$, and therefore $f_n \to f$ and $f_n' \to f'$ in norm. Furthermore, for fixed $x \in \mathbb{R}$, the Plancherel formula gives us that

$$|f_n(x) - f(x)| \leq \|\hat{f}_n - \hat{f}\|_{L^1} \leq \left(\int_{\mathbb{R}} (1 + 4\pi^2\xi^2)^{-1}d\xi\right)^{1/2}\left(\int_{\mathbb{R}} (1 + 4\pi^2\xi^2)|\hat{f}_n(\xi) - \hat{f}(\xi)|^2d\xi\right)^{1/2},$$

which tends to zero as $n \to \infty$ by our approximation, so that $f_n(x) \to f(x)$ pointwise as $n \to \infty$. This approximation allows us to finish the proof as follows:

$$\int_{\mathbb{R}} x(f'(x)\overline{f(x)} + \overline{f'(x)}f(x))dx = \lim_{m,n\to\infty} \int_{|x|\leq m} x(f_n'(x)\overline{f_n(x)} + \overline{f_n'(x)}f_n(x))dx$$

$$= \lim_{m,n\to\infty} \int_{|x|\leq m} x(|f_n|^2)'dx = \lim_{m,n\to\infty} \left(x|f_n(x)|^2\Big|_{-m}^{m} - \int_{|x|\leq m} |f_n(x)|^2dx\right)$$

$$= \lim_{m\to\infty} m(|f(m)|^2 + |f(-m)|^2) - \|f\|^2 = -\|f\|^2 = -1,$$

where to cross from the first to second line we used the product rule for differentiation (since f_n is Schwartz) and subsequently used integration by parts to evaluate the integral, and in the last line we applied Lemma 1.3, which works since we assumed $\|xf(x)\| < \infty$.

Substituting this sequence of equalities into our earlier work, we obtain that

$$4\pi^2\left(\int_{\mathbb{R}} x^2|f(x)|^2dx\right)\left(\int_{\mathbb{R}} \xi^2|\hat{f}(\xi)|^2d\xi\right) = \left[\int_{\mathbb{R}} \frac{x}{2}(f'(x)\overline{f(x)} + \overline{f'(x)}f(x))dx\right]^2 = \frac{1}{4}(-1)^2 = \frac{1}{4},$$

from which the result follows after dividing out by $4\pi^2$.

Examining the proof, we see that the equality case would require equality in the use of Cauchy-Schwarz, which means that $f'(x) = Cxf(x)$ for some constant C. Solving this equation gives us that $f(x) = Ae^{-Bx^2/2}$ for constants A, B, where the requirement that f be Schwartz forces $B > 0$. Finally, our normalizing assumption forces us to have that $|A|^2 \int_{\mathbb{R}} |e^{Bx^2}|dx = \int_{\mathbb{R}} |A|^2 |e^{Bx^2/2}|^2 dx = 1$, so that $|A|^2 = \sqrt{2B/\pi}$. However, in this solution we assumed that f' is actually the derivative of f. But the verification of this is actually fairly straightforward:

$$\int_0^x f'(y)dy = \lim_{n\to\infty} \int_0^x f_n'(y)dy = \lim_{n\to\infty} (f_n(x) - f_n(0)) = f(x) - f(0).$$

This completes the proof. □

2 Heisenberg's Inequality on Finite Abelian Groups

2.1 Basic Fourier Analysis on Finite Abelian Groups

Let G be a finite abelian group, written additively. We define a bi-character on G as a map $\varphi : G \times G \to S^1 = \{z \in \mathbb{C} : |z| = 1\}$ which is multiplicative in both coordinates: $e(x + x', \xi) = e(x, \xi)e(x', \xi)$ and $e(x, \xi + \xi') = e(x, \xi)e(x, \xi')$. Taking $e(x, \xi)$ to be any non-degenerate bi-character, in the sense that for each nonzero x (resp., ξ) there is some ξ (resp., x) such that $e(x, \xi) \neq 1$, we define the set of characters on G to be the maps $\varphi_\xi(x) = e(x, \xi)$, taken on all $\xi \in G$ (it is in fact a group isomorphic to G, which follows from the multiplicative property of the bi-character, and taking the inverses to be complex conjugates).

Consider the vector space V of complex-valued functions on G, which has dimension $|G|$, since we can write each function as a finite linear combination of characteristic functions. We define an inner product on this space as follows:

$$(f, g) = \frac{1}{|G|} \sum_{x\in G} f(x)\overline{g(x)}.$$

The next theorem is fundamental to the theory of Fourier transforms on finite abelian groups.

Theorem 2.1. *Let G be a finite abelian group, and let e be a non-degenerate bi-character on $G \times G$. The set $\{\varphi_\xi\}_{x\in G}$ of characters is an orthonormal basis for the complex vector space of functions $f : G \to \mathbb{C}$.*

Proof. The proof consists of two stages: showing that the characters are orthonormal, and showing that there are in fact $|G|$ of them (the dimension of the vector space). The first stage is straightforward, using the fact that our sums are finite and thus we can rearrange them. The second stage follows from considering concretely the case of cyclic groups, and reducing the general case to this case by way of the Structure Theorem for Finite Abelian Groups. □

Now that we have an orthonormal basis for this space V of functions on G, the basic Fourier theory follows very quickly. Let $f \in V$, and φ_ξ be a character on G. Then we define the **Fourier transform** of f for φ_ξ as

$$\hat{f}(\xi) = (f, \varphi_\xi) = \frac{1}{|G|} \sum_{x \in G} f(x)\overline{\varphi_\xi(x)}.$$

Theorem 2.2 (Fourier Inversion and Plancherel Formula)**.** *Let G be a finite abelian group, and V be the vector space of complex-valued functions on G. Then the Fourier inversion formula holds for all $f \in V$:*

$$f = \sum_{\xi \in G} \hat{f}(\xi)\varphi_\xi,$$

and the Plancherel formula holds:

$$\|f\|^2 = \sum_{\xi \in G} |\hat{f}(\xi)|^2.$$

Proof. Since the characters form a basis for V, there are constants a_ξ such that $f = \sum_{\xi \in G} a_\xi \varphi_\xi$. But since the φ_ξ are orthogonal, we have that $(f, \varphi_\xi) = a_\xi$, and therefore

$$f = \sum_{\xi \in G} a_\xi \varphi_\xi = \sum_{\xi \in G} (f, \varphi_\xi)\varphi_\xi = \sum_{\xi \in G} \hat{f}(\xi)\varphi_\xi.$$

For the Plancherel formula note that by Fourier inversion we have

$$\|f\|^2 = (f, f) = \sum_{\xi \in G} (f, \varphi_x)\overline{\hat{f}(\xi)} = \sum_{\xi \in G} \hat{f}(\xi)\overline{\hat{f}(\xi)} = \sum_{\xi \in G} |\hat{f}(\xi)|^2.$$

□

With the tools in place, we can easily prove the analogue of Heisenberg's inequality.

Theorem 2.3 (Heisenberg Inequality on Finite Abelian Groups)**.** *Let G be a finite abelian group, and let $f \in V$, the space of complex-valued functions on G, such that f is not identically zero. Then if $supp(f) = \{x \in G : f(x) \neq 0\}$ denotes the support of f, we have*

$$supp(f) \cdot supp(\hat{f}) \geq |G|.$$

Proof. The Fourier inversion formula and the triangle inequality give us that

$$|f(x)| = \left| \frac{1}{|G|} \sum_{\xi \in G} \hat{f}(\xi)\varphi_\xi(x) \right| \leq \frac{1}{|G|} \sum_{\xi \in G} |\hat{f}(\xi)| \leq \frac{\text{supp}(\hat{f})}{|G|} \max_{\xi \in G} |\hat{f}(\xi)|.$$

But similarly we have that for any $\xi \in G$,

$$|\hat{f}(\xi)| = \left| \frac{1}{|G|} \sum_{x \in G} f(x)\overline{\varphi_\xi(x)} \right| \leq \sum_{x \in G} |f(x)| \leq \text{supp}(f) \max_{x \in G} |f(x)|.$$

Combining the two and taking the maximum of f on $x \in G$ from below gives us that

$$\max_{x \in G} |f(x)| \leq \frac{\text{supp}(\hat{f}) \cdot \text{supp}(f)}{|G|} \max_{x \in G} |f(x)|.$$

□

2.2 The Case of Cyclic Groups of Prime Order

To see that the inequality is sharp, consider the case in which f is the characteristic function of a subgroup $H \subset G$. Here $|\text{supp}(f)| = |H|$ by definition and $|\text{supp}(\hat{f})| = |G|/|H|$, since

$$\hat{f}(\xi) = \frac{1}{|G|} \sum_{x \in G} f(x)\overline{\varphi_\xi(x)} = \frac{1}{|G|} \sum_{x \in H} \varphi_\xi(x^{-1}) = \frac{1}{|G|} \sum_{x \in H} \varphi_\xi(x)$$

which is zero if and only if $\xi \in H$, so that the support of $\hat{f}$ has size $|G|/|H|$.

It can be shown that this is essentially the only equality case possible (that is, up to symmetries of the Fourier transform). Thus we might expect that for cyclic groups of prime order, which have no proper subgroups, Theorem 2.3 is strict and thus could be improved. In a paper [3] published in 2005 , Terence Tao made the following improvement:

Theorem 2.4. *Let p be a prime number. If $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ is a non-zero function, then*

$$|supp(f)| + |supp(\hat{f})| \geq p + 1.$$

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 $supp(\hat{f}) = B$.

The proof's main engine is the following fact:

Lemma 2.5. *If p is a prime, and $A, \tilde{A}$ be 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 $Tf = \hat{f}|_{\tilde{A}}$ is invertible. Here $l^2(A)$ denotes the functions $f : G \to \mathbb{C}$ whose support is a subset of A.*

We proceed with the proof of the theorem.

Proof of Theorem 2.4. Suppose $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ is not identically zero and $|\text{supp}(f)| + |\text{supp}(\hat{f})| \leq p$. Letting $A = \text{supp}(f)$, we see that our assumption allows us to pick a set $\tilde{A}$ disjoint from $\text{supp}(\hat{f})$ such that $|A| = |\tilde{A}|$. But then $Tf = 0$, where T is the linear transformation from Lemma 2.5, but $f \neq 0$. This is a contradiction, since T is invertible.

For the converse, it suffices to prove the case where $|A| + |B| = p + 1$, since if $|A| + |B| > p + 1$, we can take subsets A', B' such that $|A'| + |B'| = p + 1$, apply the theorem in this case, and then take linear combinations of the functions we obtain.

So if $|A| + |B| = p + 1$, we can choose some set $\tilde{A}$ such that $|A| = |\tilde{A}|$ and $\tilde{A} \cap B = \{x\}$, where $x \in \mathbb{Z}/p\mathbb{Z}$. Lemma 2.5 gives us that the transformation T which sends $f \mapsto \hat{f}|_{\tilde{A}}$ is invertible, so that we can find a function $f \in l^2(A)$ such that $\hat{f}$ is zero on $\tilde{A} \setminus \{x\}$, but doesn't vanish at x. But then since $|\text{supp}(f)| \leq |A| = p + 1 - |B|$, to satisfy the inequality proved above we must have $\text{supp}(f) = A$ and $\text{supp}(\hat{f}) = B$, as desired. □

Finally, we outline the proof of Lemma 2.5. In fact, the statement follows immediately from the following proposition, since the matrix of T takes precisely the form described below:

Proposition 2.6. *Let p be prime and $1 \leq n \leq p$. Let $x_1 \ldots, x_n$ be distinct elements of $\mathbb{Z}/p\mathbb{Z}$, and $\xi_1, \ldots, \xi_n$ also be distinct elements of $\mathbb{Z}/p\mathbb{Z}$. The matrix $(e^{2\pi i x_i \xi_k/p})_{1\leq j,k\leq n}$ has nonzero determinant.*

Proof. We only sketch the proof. If $\omega_j = e^{2\pi i x_j/p}$, we wish to show that $\det(\omega_j^{\xi_k})_{1\leq j,k\leq n} \neq 0$. So we define a polynomial $D(z_1, \ldots, z_n) = \det(z_j^{\xi_k})_{1\leq j,k\leq n}$, which has integer coefficients. Since $D = 0$ if $z_j = z_{j'}$ for any $j \neq j'$, we can factor D as

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

where P still has integer coefficients.

Now we claim that $P(1, \ldots, 1)$ is not divisible by p. To prove this, we differentiate D $\frac{n(n-1)}{2}$ times, and note that when $z_i = 1$ for all $i = 1, \ldots, n$, the only terms that do not vanish are those that do not have a derivative of P as a factor. The remaining terms are equal to ξ_k^{j-1} for $1 \leq j, k \leq n$, and this polynomial is a Vandermonde determinant, which is not a multiple of p. The following algebraic lemma, which we do not prove, allows us to finish the proof.

Lemma 2.7. *Let p be prime, n be a positive integer, and $P(z_1, \ldots, z_n)$ be a polynomial with integer coefficients. suppose we have n p^{th} roots of unity $\omega_1, \ldots, \omega_n$ for which $P(\omega_1, \ldots, \omega_n) = 0$. Then $P(1, \ldots, 1)$ is a multiple of p.*

Now since $P(1, \ldots, 1)$ is not divisible by p, Lemma 2.7 gives us that $P(\omega_1, \ldots, \omega_n) \neq 0$. Since the ω_i are distinct, this means that $D(\omega_1, \ldots, \omega_n) \neq 0$, so that the determinant is indeed nonzero. □

References

[1] H. Dym and H.P. McKean. *Fourier Series and Integrals*. Academic Press, Inc. (1972)

[2] E. Stein and R. Shakarchi. *Real Analysis*. Princeton University Press. (2005)

[3] T. Tao. "An Uncertainty Principle for Cyclic Groups of Prime Order." *Mathematical Research Letters* 12, 121-127. (2005)