INTRODUCCIÓN A MÉTODOS DE ANÁLISIS DE FOURIER EN COMBINATORIA ARITMÉTICA

PABLO CANDELA

Contenido

Introducción

Desde sus comienzos hace aproximadamente dos siglos, el análisis de Fourier ha tenido siempre una importancia fundamental y creciente en diversas áreas matemáticas, tanto puras como aplicadas [5]. En teoría de números, varias de estas aplicaciones constituyen resultados clásicos; entre estas se encuentran, por ejemplo, las aplicaciones del método del círculo como el teorema de Vinográdov, que nos dice que todo entero impar suficientemente grande es la suma de tres números primos (resultado cuya reciente mejora por Helfgott resultó en una prueba de la conjetura débil de Goldbach [13]), o el problema de Waring, que consiste en determinar el número de representaciones de un entero como suma de un número dado de potencias k-ésimas [6].

Alrededor de la mitad del siglo pasado, empezaron a darse aplicaciones combinatorias del análisis de Fourier en teoría de números que formaron algunos de los primeros resultados principales del área hoy conocida como *combinatoria aritmética*. Hoy en día esta área conoce un desarrollo muy activo, dentro del cual el análisis de Fourier ha generado un amplio abanico de métodos y aplicaciones. En este curso estudiaremos algunos ejemplos

centrales de estos métodos y algunas de sus aplicaciones principales. Para ello nos concentraremos en el análisis de Fourier sobre grupos abelianos finitos (también llamado análisis de Fourier *discreto*).

Empezamos en la sección siguiente introduciendo los conceptos básicos. En la sección 2 estudiaremos algunas de las ideas centrales que dan a esta teoría su utilidad en combinatoria aritmética. En la última sección daremos ejemplos concretos del uso de estas ideas, demostrando algunos resultados centrales en el área, como el teorema de Roth y el lema de Bogolyubov.

1. Análisis de Fourier en grupos abelianos finitos – teoría básica

Para todo conjunto finito X y toda función $f : X \to \mathbb{C}$, denotamos por $|X|$ la cardinalidad de X y por $\mathbb{E}_{x\in X} f(x)$ el promedio de f sobre X, es decir

$$\mathbb{E}_{x\in X} f(x) = \frac{1}{|X|}\sum_{x\in X} f(x).$$

Las funciones de valores complejos $f : X \to \mathbb{C}$ forman un espacio vectorial, que denotamos por $\mathbb{C}^X$, de dimensión $N = |X|$. Se puede definir la operación de producto interno (o producto escalar) siguiente:

$$\langle\cdot,\cdot\rangle \;:\; \mathbb{C}^X \times \mathbb{C}^X \to \mathbb{C}, \quad (f,g) \;\mapsto\; \langle f,g\rangle = \mathbb{E}_{x\in X} f(x)\overline{g(x)},$$

obteniendo así el *espacio vectorial con producto interno*[1] $(\mathbb{C}^X, \langle\cdot,\cdot\rangle)$. Una noción muy útil relacionada con estos espacios es la de *base ortonormal*. Un conjunto de elementos $\{v_x : x \in X\}$ forman una base ortonormal en $\mathbb{C}^X$ si satisfacen la condición siguiente:

$$\text{para todo } x, y \in X, \text{ tenemos } \langle v_x, v_y\rangle = \delta_{xy} = \begin{cases} 1, & x = y \\ 0, & x \neq y \end{cases}. \tag{1.1}$$

De esta condición se deduce fácilmente que los N elementos v_x son linealmente independientes, luego forman en efecto una base para $\mathbb{C}^X$. Toda función en $\mathbb{C}^X$ se puede por lo tanto descomponer de manera única como combinación lineal de estos elementos. La relación (1.1) permite además expresar los coeficientes de esta descomposición simplemente.

Lema 1.1. *Sea $\{v_x : x \in X\}$ una base ortonormal de $\mathbb{C}^X$. Entonces para toda función $f : X \to \mathbb{C}$ tenemos $f = \sum_{x\in X} \langle f, v_x\rangle\, v_x$.*

Prueba. Existen coeficientes $c_x \in \mathbb{C}$ tales que $f = \sum_{x\in X} c_x\, v_x$. Dado cualquier $x_0 \in X$, tomando el producto interno con v_{x_0} de ambos lados de esta ecuación, y usando (1.1), deducimos que $c_{x_0} = \langle f, v_{x_0}\rangle$. □

[1] Más precisamente, es un espacio hilbertiano, pero no usaremos este hecho.

Sea G un grupo abeliano finito. En $\mathbb{C}^G$ (y en general en $\mathbb{C}^X$) existen muchas bases ortonormales. Entre estas, hay una base específica que tiene propiedades adicionales muy útiles, y que constituye una de las nociones fundamentales del análisis de Fourier discreto. Esta es la base de los *caracteres* sobre G.

Denotemos por $\mathbb{C}^\times$ el grupo de números complejos no-nulos con multiplicación.

Definición 1.2. Un *carácter* sobre G es un homomorfismo $G \to \mathbb{C}^\times$.

Podemos equipar el conjunto de caracteres sobre G con la operación de multiplicación punto a punto: si χ_1, χ_2 son caracteres, el carácter producto $\chi_1\chi_2$ se define por $\chi_1\chi_2(x) = \chi_1(x)\chi_2(x)$, $x \in G$. Obtenemos así un grupo abeliano, llamado el *dual* de G y denotado por $\widehat{G}$. El elemento neutro de $\widehat{G}$ es el caracter que manda todo $x \in G$ a 1, llamado el *caracter principal*. Tenemos también que el inverso de un caracter χ es el caracter $x \mapsto \overline{\chi(x)}$ (donde $\overline{z}$ denota el conjugado de $z \in \mathbb{C}$).

Vamos a estudiar el grupo dual en más detalle, en particular para demostrar que sus elementos forman en efecto una base ortonormal en $\mathbb{C}^G$. Empezamos con las observaciones siguientes.

Lema 1.3. *Sea G un grupo abeliano finito, y sea n el exponente*[2] *de G. Entonces*

(1) *Todo carácter $\chi \in \widehat{G}$ toma sus valores en $\{z \in \mathbb{C} : z^n = 1\}$.*
(2) *Si G es un grupo cíclico $\mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z}$, entonces*

$$\widehat{G} = \{x \mapsto \exp(2\pi i\, rx/N) : r \in \mathbb{Z}_N\}.$$

Dejamos la prueba como ejercicio. La parte (2) de este lema nos da una descripción explícita de los caracteres sobre $\mathbb{Z}_N$: a todo $\chi \in \widehat{\mathbb{Z}_N}$ le corresponde un único elemento $r \in \mathbb{Z}_N$ tal que $\chi(x) = \exp(2\pi i\, rx/N)$. Llamaremos este elemento r la *frecuencia* de χ. Denotando el carácter de frecuencia r por χ_r, tenemos que la función $r \mapsto \chi_r$ es un isomorfismo de grupos $\mathbb{Z}_N \to \widehat{\mathbb{Z}_N}$.

Resulta que esta descripción de los caracteres sobre $\mathbb{Z}_N$ tiene una generalización muy satisfactoria a todo grupo abeliano finito. Para dar esta descripción usaremos la notación $\mathbb{T}$ para el grupo circular $\mathbb{R}/\mathbb{Z}$, y la notación e para la función $\mathbb{T} \to \mathbb{C}$, $\theta \mapsto e(\theta) = \exp(2\pi i\, \theta)$. Podemos ahora reescribir todo carácter χ sobre $G = \mathbb{Z}_N$ de la forma $\chi(x) = e(rx/N)$.

Para nuestra descripción general de los caracteres, conviene primero generalizar la función $(r, x) \mapsto rx/N \mod 1$.

Definición 1.4. Sea G un grupo abeliano. Una *forma bilineal* de G^2 a $\mathbb{T}$ es una función $G \times G \to \mathbb{T}$, $(r, x) \mapsto r \cdot x$ con la propiedad siguiente: para todo $r \in G$, la función $x \mapsto r \cdot x$

[2]El exponente de G es el menor entero positivo m tal que para todo $g \in G$ se tiene $mg = 0$.

es un homomorfismo, y para todo $x \in G$ la función $r \mapsto r \cdot x$ es un homomorfismo. Decimos que la forma bilineal es *no degenerada* si para todo $r \in G \setminus \{0\}$ existe $x \in G$ tal que $r \cdot x \neq 0$, y para todo $x \in G \setminus \{0\}$ existe r tal que $r \cdot x \neq 0$. Decimos que la forma es *simétrica* si $r \cdot x = x \cdot r$ para todo $r, x \in G$.

El teorema fundamental de los grupos abelianos finitos nos dice que G es isomorfo a una suma directa de grupos cíclicos, $G \cong \mathbb{Z}_{N_1} \oplus \cdots \oplus \mathbb{Z}_{N_t}$. Usando este teorema, podemos completar la descripción general del grupo dual.

Proposición 1.5. *Sea G un grupo abeliano finito. Entonces $\widehat{G} \cong G$. Existe una forma bilineal de G a $\mathbb{T}$ simétrica y no degenerada $(r, x) \mapsto r \cdot x$. Para todo carácter $\chi \in \widehat{G}$ existe un único elemento $r \in G$ tal que $\chi(x) = e(r \cdot x)$.*

En particular, denotando el carácter $x \mapsto e(r \cdot x)$ de frecuencia r por e_r, tenemos que la función $r \mapsto e_r$ es un isomorfismo explícito de G a $\widehat{G}$.

Prueba. Empezamos observando los dos hechos siguientes, fácilmente demostrados (ejercicio 2): primero, si $G \cong H$ entonces $\widehat{G} \cong \widehat{H}$; segundo, para grupos abelianos finitos G_1, G_2 cualesquiera, el dual de $G_1 \oplus G_2$ es isomorfo a $\widehat{G_1} \oplus \widehat{G_2}$. Combinando esto con el teorema fundamental de los grupos abelianos finitos y el hecho que $\widehat{\mathbb{Z}_N} \cong \mathbb{Z}_N$, deducimos que $\widehat{G} \cong G$.

Para encontrar la forma bilineal deseada, podemos suponer que $G = \mathbb{Z}_{N_1} \oplus \cdots \oplus \mathbb{Z}_{N_t}$. Sobre cada grupo $\mathbb{Z}_{N_j}$ tenemos ya una forma bilineal con las propiedades deseadas, a saber la forma $(r, x) \mapsto rx/N_j \mod 1$. Por otro lado, se verifica fácilmente que si G_1, G_2 tienen cada uno una forma $\cdot$ con estas propiedades, entonces la función $G_1 \oplus G_2 \to \mathbb{R}/\mathbb{Z}$, $((r_1, r_2), (x_1, x_2)) \mapsto r_1 \cdot x_1 + r_2 \cdot x_2$ también es una forma bilineal adecuada. Razonando por inducción sobre j, encontramos la forma sobre G.

Para ver la última parte, nótese que, por un lado, cada función $x \mapsto e(r \cdot x)$, $r \in G$ es un carácter, y por otro lado no pueden haber más caracteres sobre G. □

De ahora en adelante, supondremos siempre que un grupo abeliano finito G viene equipado con una tal forma bilineal. [3]

Verificamos ahora que los caracteres forman efectivamente una base ortonormal en $\mathbb{C}^G$.

Proposición 1.6. *Sea G un grupo abeliano finito. Entonces tenemos $\langle e_r, e_s \rangle = \delta_{rs}$ para todo $r, s \in G$.*

[3]Se puede verificar que para nuestro uso de esta teoría no tiene importancia qué forma particular escogemos. Si se quiere ser más explícito, se puede elegir la forma $r \cdot x = \sum_{r=1}^{t} \phi(r)_j \, \phi(x)_j / N_j \mod 1$, donde ϕ es un isomorfismo $G \to \mathbb{Z}_{N_1} \oplus \cdots \oplus \mathbb{Z}_{N_t}$.

Prueba. Tenemos $\langle e_r, e_s\rangle = \mathbb{E}_{x\in G}\, e((r-s)\cdot x)$. Este promedio tiene valor 1 cuando $r = s$, con lo cual solo nos queda por probar que tiene valor 0 cuando $r \neq s$. Sea $t = r - s \neq 0$. Siendo no degenerada la forma bilineal $\cdot$, existe $x_0 \in G$ tal que $t \cdot x_0 \neq 0$. Por otra parte, tenemos que $e(t\cdot x_0)\ \mathbb{E}_{x\in G}\ e(t\cdot x) = \mathbb{E}_{x\in G}\ e(t\cdot(x+x_0)) = \mathbb{E}_{x\in G}\ e(t\cdot x)$, luego $(e(t\cdot x_0)-1)\ \mathbb{E}_{x\in G}\ e(t\cdot x) = 0$. Como $e(t\cdot x_0) - 1 \neq 0$, deducimos que, efectivamente, $\mathbb{E}_{x\in G}\, e(t\cdot x) = 0$. □

Ha llegado el momento de definir la transformada de Fourier y describir sus primeras propiedades básicas.

Definición 1.7 (Transformada de Fourier discreta)**.** Para toda función $f \in \mathbb{C}^G$ y todo $\chi \in \widehat{G}$, la *transformada de Fourier* de f es la función $\widehat{f} : \widehat{G} \to \mathbb{C}$ definida por

$$\widehat{f}(\chi) = \langle f, \chi\rangle = \mathbb{E}_{x\in G} f(x)\overline{\chi(x)}.$$

Los valores $\widehat{f}(\chi)$ de la transformada se llaman los *coeficientes* de Fourier de f.

Proposición 1.8. *Sean $f, g \in \mathbb{C}^G$. Entonces tenemos*

- *Fórmula de inversión:*

$$f(x) = \sum_{\chi\in\widehat{G}} \widehat{f}(\chi)\ \chi(x). \tag{1.2}$$

- *Teorema de Plancherel:*

$$\langle f, g\rangle = \sum_{\chi\in\widehat{G}} \widehat{f}(\chi)\,\overline{\widehat{g}(\chi)}. \tag{1.3}$$

- *Identidad de Parseval:*

$$\mathbb{E}_{x\in G}|f(x)|^2 = \sum_{\chi\in\widehat{G}} |\widehat{f}(\chi)|^2. \tag{1.4}$$

Prueba. La fórmula de inversión es un caso especial del lema 1.1. El teorema de Plancherel se obtiene substituyendo las fórmulas de inversión para f y g dentro de $\langle f, g\rangle$ y usando la proposición 1.6. El caso especial $f = g$ nos da la identidad de Parseval. □

Nota 1.9. Formular los coeficientes de Fourier como lo hacemos, usando el promedio $\mathbb{E}_G$, supone que estamos usando la *medida de probabilidad uniforme* sobre G, es decir la medida que a cada conjunto $A \subset G$ asigna el valor $|A|/|G|$. La fórmula de inversión (1.2), compatible con esta definición de los coeficientes, supone en cambio que la medida que usamos sobre el grupo dual $\widehat{G}$ es la *medida de conteo*, que da a A el valor $|A|$. Siguiendo esta convención, es habitual definir la norma euclidiana sobre $\mathbb{C}^G$ usando la medida de probabilidad uniforme, escribiendo $\|f\|_{L^2(G)} = (\mathbb{E}_{x\in G}|f(x)|^2)^{1/2}$, y sobre $\mathbb{C}^{\widehat{G}}$ usando la

medida de conteo, escribiendo $\|g\|_{\ell^2(\widehat{G})} = \Big(\sum_\chi |g(\chi)|^2 \Big)^{1/2}$. La identidad de Parseval se puede entonces escribir $\|f\|_{L^2(G)} = \|\widehat{f}\|_{\ell^2(\widehat{G})}$.

La transformada de Fourier de f es una función $\widehat{f}$ definida sobre $\widehat{G}$. Sin embargo, en la práctica la trataremos a menudo como una función sobre G, usando el isomorfismo de la proposición 1.5, escribiendo $\widehat{f}(r)$ en vez de $\widehat{f}(e_r)$.

Usaremos también la famosa desigualdad siguiente.

Proposición 1.10 (Desigualdad de Cauchy-Schwarz)**.** *Para funciones $f, g \in \mathbb{C}^G$ cualesquiera,*

$$|\langle f, g\rangle| \ \leq \ \|f\|_{L^2(G)} \, \|g\|_{L^2(G)}. \tag{1.5}$$

(Nótese la versión equivalente: $\big| \sum_{x\in G} f(x)\overline{g(x)} \big| \leq \|f\|_{\ell^2(G)} \, \|g\|_{\ell^2(G)}$.)

A continuación empezamos a ilustrar la utilidad combinatoria de la transformada de Fourier.

2. Primeros usos en combinatoria aritmética

Uno de los temas centrales de la combinatoria aritmética, que se remonta a los orígenes de esta área, consiste en estudiar bajo qué condiciones (las más naturales y débiles posibles) un subconjunto A de un grupo abeliano debe contener configuraciones aritméticas de un tipo dado. Estas configuraciones consisten generalmente en tuplas de elementos de A que satisfacen ecuaciones lineales prescritas. En esta dirección, un resultado central en el área es el famoso teorema de Szemerédi, conjeturado por Erdős y Turán ya en 1936 [9]. Denotemos por $[N]$ el conjunto $\{1, 2, \dots, N\}$.

Teorema 2.1 (Szemerédi)**.** *Sea $\delta > 0$ y sea k un entero positivo. Entonces existe $N_0 > 0$ tal que para todo entero $N > N_0$ y todo conjunto de enteros $A \subset [N]$ de cardinalidad $|A| \geq \delta N$, existe una progresión aritmética de longitud k incluida en A.*

Nótese que una tal progresión es una k-tupla de elementos de A que satisfacen cierto sistema de $k-2$ ecuaciones lineales. Por ejemplo para $k = 3$ el sistema consiste en la única ecuación $x_1 - 2x_2 + x_3 = 0$.

Szemerédi dió la primera prueba de este teorema en 1975 usando argumentos complicados de teoría de grafos [18]. El caso no-trivial más simple del teorema, a saber el caso $k = 3$, había sido demostrado ya por Roth en 1953 [15]. La prueba de Roth usa el análisis de Fourier sobre grupos $\mathbb{Z}_N$, y las ideas principales que introdujo han pasado a formar parte importante del conjunto de herramientas en el área. Por ello, en la sección

siguiente estudiaremos el teorema de Roth como primera aplicación central. Con vistas a este objetivo, en esta sección presentaremos algunas ideas, en su mayoría relacionadas con la prueba del teorema de Roth, como principios generales del uso combinatorio de la transformada de Fourier. [4]

Dado un conjunto X y un subconjunto $A \subset X$, denotaremos por 1_A la *función indicadora* de A sobre X, definida como sigue: $1_A(x) = 1$ si $x \in A$, y $1_A(x) = 0$ si $x \in X \setminus A$.

Dada una ecuación lineal, y dado $A \subset G$, nos interesa contar cuantas soluciones de esta ecuación hay en A. Por ejemplo, en el caso del teorema de Roth, esto consiste esencialmente en analizar la cantidad siguiente:

$$\mathbb{E}_{\substack{x_1,x_2,x_3\in G:\\ x_1-2x_2+x_3=0}} 1_A(x_1)\,1_A(x_2)\,1_A(x_3). \tag{2.1}$$

Más generalmente, podemos considerar funciones $f_1, \dots, f_t : G \to \mathbb{C}$ arbitrarias (no necesariamente funciones indicadoras de conjuntos) y considerar promedios de tales funciones tomados sobre el conjunto de soluciones a una ecuación lineal $c_1x_1 + \cdots + c_tx_t = 0$ con coeficientes c_i enteros:

$$\mathbb{E}_{\substack{x_1,\dots,x_t\in G:\\ c_1x_1+\cdots+c_tx_t=0}} f_1(x_1)\cdots f_t(x_t). \tag{2.2}$$

El primer principio básico que vamos a estudiar es que la transformada de Fourier permite simplificar promedios de este tipo.

2.1. **Simplificación de promedios relativos a ecuaciones lineales.**

Empezamos con el promedio (2.1). Siempre y cuando el orden de G sea impar, usando la fórmula de inversión (1.2) para 1_A obtenemos la ecuación siguiente:

$$\mathbb{E}_{\substack{x_1,x_2,x_3\in G:\\ x_1-2x_2+x_3=0}} 1_A(x_1)\,1_A(x_2)\,1_A(x_3) = \sum_r \widehat{1_A}(r)^2\,\widehat{1_A}(-2r). \tag{2.3}$$

La suma a la derecha en (2.3) simplifica el promedio original, en el sentido que este promedio involucra más de una variable mientras que la suma es sobre la única variable r. [5] Este tipo de simplificación es muy útil, como veremos más adelante. Además, es bastante general.

Proposición 2.2. *Sea $c_1x_1 + \cdots + c_tx_t = 0$ una ecuación lineal con coeficientes enteros c_i. Sea G un grupo abeliano finito tal que la multiplicación $x \mapsto c_ix$ es sobreyectiva para*

[4] Nótese, no obstante, que los métodos de Roth no permiten demostrar el teorema de Szemerédi para $k > 3$. Más generalmente, los métodos Fourier-analíticos conciernen sobre todo a las configuraciones dadas por sistemas de ecuaciones lineales llamados *sistemas de complejidad 1.* (Véase el ejercicio 10.)

[5] Esta ecuación es un caso especial de la fórmula (2.4) probada a continuación, pero como primer ejemplo puede ser instructivo intentar demostrar la ecuación directamente.

todo $i \in [t]$, y sean $f_1, \dots, f_t$ funciones $G \to \mathbb{C}$ arbitrarias. Entonces tenemos la fórmula siguiente:

$$\mathbb{E}_{\substack{x_1,\dots,x_t \in G: \\ c_1x_1+\cdots+c_tx_t=0}} f_1(x_1) \cdots f_t(x_t) \;=\; \sum_{r\in G} \widehat{f_1}(c_1 r) \cdots \widehat{f_t}(c_t r). \tag{2.4}$$

Este es el resultado principal de esta subsección. Para demostrarlo, utilizaremos la operación de convolución, una operación que juega un papel crucial en esta área, sobre todo por su relación con la transformada de Fourier.

Definición 2.3 (Convolución)**.** Sean $f, g \in \mathbb{C}^G$. La *convolución* de f y g es la función $G \to \mathbb{C}$ denotada por $f * g$ y definida como sigue:

$$f * g(x) \;=\; \mathbb{E}_{y\in G}\, f(y)\, g(x-y).$$

La importancia de esta operación va mucho más allá de su utilidad en la prueba de la proposición 2.2. Por ejemplo, más adelante veremos que es muy útil para estudiar la estructura de conjuntos suma $A + B = \{a + b : a \in A, b \in B\}$, ya que tenemos la relación siguiente:

$$A + B = \operatorname{supp}(1_A * 1_B),$$

donde $\operatorname{supp}(f) = \{x \in G : f(x) \neq 0\}$ es el *soporte* de la función $f \in \mathbb{C}^G$.

Por ahora nos concentramos en demostrar la proposición 2.2. El hecho principal que usaremos para ello es que la transformada de Fourier convierte una convolución de dos funciones en simple producto de sus coeficientes:

$$\text{para todo } \; r \in G \;\text{ y }\; f, g \in \mathbb{C}^G, \quad \text{tenemos} \quad \widehat{f * g}(r) \;=\; \widehat{f}(r)\, \widehat{g}(r). \tag{2.5}$$

Esta *fórmula de producto* se verifica aplicando la fórmula de inversión (1.2) para f y g, y la ortonormalidad de los caracteres (véase el ejercicio 3).

Prueba de la proposición 2.2. La idea es reescribir el promedio

$$\mathbb{E}_{\substack{x_1,\dots,x_t \in G: \\ c_1x_1+\cdots+c_tx_t=0}} f_1(x_1) \cdots f_t(x_t)$$

de una forma que revele que se trata de una convolución iterada. Hacemos primero el cambio de variables siguiente: $y_1 = c_1x_1, \dots, y_t = c_tx_t$. Nótese que, siendo cada función $x \mapsto c_i x$ sobreyectiva (luego biyectiva) de G a G, tiene una función inversa, que denotaremos por c_i^{-1}. El promedio original queda escrito de la forma siguiente:

$$\mathbb{E}_{\substack{y_1,\dots,y_t \in G: \\ y_1+\cdots+y_t=0}} \; f_1(c_1^{-1}y_1) \;\cdots\; f_t(c_t^{-1}y_t).$$

Definiendo las funciones $f_1'(y) = f_1(c_1^{-1}y), \dots, f_t'(y) = f_t(c_t^{-1}y)$, podemos reescribir el último promedio simplemente y ver que es efectivamente una convolución iterada:

$$\mathbb{E}_{\substack{y_1,\dots,y_t\in G:\\ y_1+\cdots+y_t=0}} \; f_1'(y_1) \; \cdots \; f_t'(y_t) = f_1' * \cdots * f_t'(0).$$

La fórmula de inversión nos dice que esto es igual a $\sum_r \widehat{f_1' * \cdots * f_t'}(r)$, y la fórmula de producto (aplicada $t-1$ veces) nos dice que esto es igual a $\sum_r \widehat{f_1'}(r)\widehat{f_2'}(r)\cdots\widehat{f_t'}(r)$. Finalmente, verificamos mediante un simple cálculo[6] que $\widehat{f_i'}(r) = \widehat{f_i}(c_i r)$. □

Nota 2.4. Esta proposición se puede demostrar de otra manera usando la fórmula de Poisson (véase el ejercicio 4).

¿Cómo se puede utilizar la simplificación de promedios dada en (2.4)? Para responder debemos estudiar, primero, cómo la estructura combinatoria de un conjunto A se puede ver reflejada en los coeficientes $\widehat{1_A}(r)$, y segundo, cómo una información sobre estos coeficientes se puede transformar a su vez en nueva información combinatoria provechosa.

2.2. **Transformar datos combinatorios en datos Fourier-analíticos, y viceversa.**

Empezamos con un conjunto $A \subset G$ dado. Denotamos por α la *densidad* de A en G, a saber $\alpha = |A|/|G|$. Una primera observación es que el llamado *coeficiente principal* $\widehat{1_A}(0)$ (correspondiente al carácter principal, a saber el carácter con valor constante igual a 1) es igual a α, independientemente de la estructura combinatoria de A:

$$\widehat{1_A}(0) = \mathbb{E}_{x\in G} 1_A(x) = \alpha.$$

Por lo tanto, para estudiar esta estructura hemos de concentrarnos en los coeficientes no-principales $\widehat{1_A}(r)$, $r \neq 0$. Para ello trabajaremos con la llamada *función nivelada* de A, denotada por f_A y definida como sigue:

$$f_A(x) = 1_A(x) - \alpha.$$

Nótese que tenemos $\widehat{f_A}(r) = \widehat{1_A}(r)$ para todo $r \neq 0$, y $\widehat{f_A}(0) = 0$.

Como mencionamos previamente, nuestro problema combinatorio general es el de analizar el promedio de 1_A relativo a una ecuación lineal dada. Para ser concretos tomemos de nuevo el promedio de progresiones aritméticas de longitud 3, que denotaremos de ahora en adelante por $T_3(A)$:

$$T_3(A) = \mathbb{E}_{\substack{x_1,x_2,x_3\in G:\\ x_1-2x_2+x_3=0}} \; 1_A(x_1)\, 1_A(x_2)\, 1_A(x_3).$$

[6]En el cálculo se usa el hecho que para todo entero n tenemos $r \cdot (nx) = (nr) \cdot x$.

La fórmula (2.3) nos dice que esto es igual a $\sum_r \widehat{1_A}(r)^2\ \widehat{1_A}(-2r)$. Aquí también es muy útil separar el carácter principal de los demás, como sigue:

$$T_3(A) = \alpha^3 + \sum_{r\neq 0} \widehat{1_A}(r)^2\ \widehat{1_A}(-2r) = \alpha^3 + \sum_r \widehat{f_A}(r)^2\ \widehat{f_A}(-2r). \tag{2.6}$$

Con esta ecuación se precisa nuestro problema: hemos de analizar la diferencia entre un promedio (aquí $T_3(A)$) y lo que podemos llamar su *valor principal* (aquí α^3, y para una ecuación más general en t variables, α^t). La ecuación también deja claro que en este análisis la *magnitud* de los coeficientes $\widehat{f_A}(r)$ va a jugar un papel importante.

Definición 2.5 (Uniformidad de Fourier)**.** Definimos la *norma de uniformidad de Fourier* para toda función $f : G \to \mathbb{C}$ como sigue:

$$\|f\|_u = \sup_r \ \big|\widehat{f}(r)\big|.$$

Como primer ejemplo de la utilidad de esta norma, tenemos el resultado siguiente.

Proposición 2.6. *Para todo conjunto $A \subset G$ de densidad α tenemos*

$$\big|\, T_3(A) - \alpha^3 \,\big| \ \leq\ \|f_A\|_u\ \alpha. \tag{2.7}$$

Este es un caso especial del resultado principal de esta sección, que nos dice esencialmente que la norma $\|\cdot\|_u$ controla la diferencia entre un promedio de tipo (2.2) y su valor principal:

Proposición 2.7. *Sea $c_1x_1 + \cdots + c_tx_t = 0$ una ecuación lineal con coeficientes enteros c_i, con $t \geq 3$. Sea G un grupo abeliano finito tal que la multiplicación $x \mapsto c_ix$ es sobreyectiva para todo $i \in [t]$, y sean $A_1, \ldots, A_t$ subconjuntos de G arbitrarios, de densidades $\alpha_1, \ldots, \alpha_t$ respectivamente. Entonces tenemos*

$$\big|\alpha_1 \cdots \alpha_t \ -\ \mathbb{E}_{\substack{x_1,\ldots,x_t\in G:\\ c_1x_1+\cdots+c_tx_t=0}}\ 1_{A_1}(x_1)\cdots 1_{A_t}(x_t)\big| \leq \|f_{A_1}\|_u \cdots \|f_{A_{t-2}}\|_u\ \alpha_{t-1}^{1/2}\ \alpha_t^{1/2}. \tag{2.8}$$

En particular tenemos $|\,\alpha^t - \mathbb{E}_{\substack{x_1,\ldots,x_t\in G:\\ c_1x_1+\cdots+c_tx_t=0}}\ 1_A(x_1)\cdots 1_A(x_t)\,| \leq \|f_A\|_u\ \alpha^{t-2}$.

Prueba. La fórmula (2.4) nos dice que el promedio $\mathbb{E}_{\substack{x_1,\ldots,x_t\in G:\\ c_1x_1+\cdots+c_tx_t=0}}\ 1_{A_1}(x_1)\cdots 1_{A_t}(x_t)$ es igual a

$$\alpha_1\cdots\alpha_t + \sum_{r\neq 0} \widehat{1_{A_1}}(c_1r)\cdots\widehat{1_{A_t}}(c_tr) = \alpha_1\cdots\alpha_t + \sum_r \widehat{f_{A_1}}(c_1r)\cdots\widehat{f_{A_t}}(c_tr).$$

Por lo tanto, el lado izquierdo de (2.8) vale como mucho

$$\begin{aligned}\sum_r \big|\widehat{f_{A_1}}(c_1r)\big|\cdots\big|\widehat{f_{A_t}}(c_tr)\big| \ &\leq\ \sup_r\big|\widehat{f_{A_1}}(c_1r)\big|\cdots\sup_r\big|\widehat{f_{A_{t-2}}}(c_{t-2}r)\big|\sum_r\big|\widehat{f_{A_{t-1}}}(c_{t-1}r)\big|\,\big|\widehat{f_{A_t}}(c_tr)\big| \\ &\leq\ \|f_{A_1}\|_u\cdots\|f_{A_{t-2}}\|_u\ \sum_r\ \big|\widehat{1_{A_{t-1}}}(c_{t-1}r)\big|\,\big|\widehat{1_{A_t}}(c_tr)\big|.\end{aligned}$$

Por la desigualdad de Cauchy-Schwarz y la identidad de Parseval, tenemos (usando también la biyectividad de las funciones $r \mapsto c_i r$)

$$\begin{aligned}\sum_r \left|\widehat{1_{A_{t-1}}}(c_{t-1}r)\right| \left|\widehat{1_{A_t}}(c_t r)\right| &\leq \Big(\sum_r \left|\widehat{1_{A_{t-1}}}(r)\right|^2\Big)^{1/2} \Big(\sum_r \left|\widehat{1_{A_t}}(r)\right|^2\Big)^{1/2} \\ &= \left(\mathbb{E}_{x\in G}\, 1_{A_{t-1}}(x)^2\right)^{1/2} \left(\mathbb{E}_{x\in G}\, 1_{A_t}(x)^2\right)^{1/2} \\ &= \alpha_{t-1}^{1/2}\ \alpha_t^{1/2}.\end{aligned}$$

□

Nota 2.8. Una norma estrechamente relacionada con $\|\cdot\|_u$ y de gran utilidad es la llamada *norma U^2 de Gowers*, definida para toda función $f : G \to \mathbb{C}$ por $\|f\|_{U^2} = \left(\mathbb{E}_{x,h,k\in G} f(x)\, \overline{f(x+h)}\, \overline{f(x+k)}\, f(x+h+k)\right)^{1/4}$. (Véase el ejercicio 5.)

Este resultado nos permite reducir gran parte de nuestro problema combinatorio inicial al de entender la relación entre la estructura de A y el valor de $\|f_A\|_u$. Empezamos a elucidar esta relación con la pregunta siguiente, un poco imprecisa:

> *¿Qué tipo de estructura del conjunto A garantiza que $\|f_A\|_u$ sea pequeña comparada con α?*

Podemos pensar en un coeficiente de Fourier no-principal $\widehat{1_A}(r)$ geométricamente como la suma en el plano complejo de los números $e_r(x)/|G|$, $x \in A$. Esta suma tendrá menor magnitud cuanto más haya cancelación entre estos números. Para que $\|f_A\|_u$ sea pequeña, tiene que haber una tal cancelación para todo $r \neq 0$, y un modo claro de garantizar esto es que para todo $r \neq 0$ los números $e_r(x)$, $x \in A$ se repartan de manera más o menos uniforme en el círculo unidad. Un momento de reflexión nos conduce a un tipo de estructura que garantiza esto de manera muy natural: un conjunto *A aleatorio de probabilidad α*, es decir un conjunto aleatorio tal que para cada $x \in G$ el evento $x \in A$ tiene probabilidad α, y estos eventos son independientes.

Proposición 2.9 (Uniformidad de un conjunto aleatorio)**.** *Sea $A \subset G$ un conjunto aleatorio de probabilidad $\alpha \leq 1/2$ y sea $t > 0$. Entonces, suponiendo que $\alpha \geq 8\log(4t|G|)/|G|$, tenemos, con probabilidad al menos $1 - 1/t$,*

$$\big|\, |A|/|G| - \alpha \,\big| \leq 4\sqrt{\log(4t|G|)/|G|} \quad y \quad \|f_A\|_u \leq 4\sqrt{\log(4t|G|)/|G|}.$$

Prueba. Usamos la desigualdad de Chernoff en su versión para variables aleatorias complejas. Este resultado dice lo siguiente (véase [19, teorema 1.8 y ejercicio 1.3.4]): sean $X_1, \ldots, X_n$ variables aleatorias complejas independientes tales que $|X_i - \mathbb{E}(X_i)| \leq 1$ para todo $i \in [n]$. Sea $X = X_1 + \cdots + X_n$ y sea $\sigma = \sqrt{\mathrm{Var}(X)}$ la desviación estándar de X.

Entonces para todo $\lambda > 0$ tenemos

$$\mathbb{P}(|X - \mathbb{E}(X)| \geq \lambda\sigma) \leq 4\max(e^{-\lambda^2/8}, e^{-\lambda\sigma/4}). \tag{2.9}$$

Dado un elemento no-nulo $r \in G$, aplicando (2.9) a las variables $X_x = e(-r \cdot x)1_A(x)$, $x \in G$ y usando que $X = |G|\,\widehat{1_A}(r)$, $\mathbb{E}(X) = 0$, y $\sigma = \sqrt{\sum_x \mathrm{Var}(X_x)} \in [\sqrt{\frac{\alpha}{2}|G|}, \sqrt{3\alpha|G|}]$, obtenemos $\mathbb{P}(|\widehat{1_A}(r)| \geq \lambda|G|^{-1/2}) \leq 4e^{-\lambda^2/8}$, suponiendo que $\lambda < 2\sigma$ (para lo cual es suficiente tener $\lambda^2 < \alpha|G|$). Eligiendo $\lambda = \sqrt{8\log(4t|G|)}$, completamos la prueba. □

Nótese que por la identidad de Parseval tenemos $\sqrt{\alpha(1-\alpha)} = \left(\sum_r |\widehat{f_A}|^2\right)^{1/2} \leq \|f_A\|_u |G|^{1/2}$, de modo que esta proposición nos dice que los conjuntos aleatorios son extremadamente uniformes (sus normas $\|f_A\|_u$ son muy pequeñas, casi tanto como el mínimo posible). Junto con la proposición 2.7, esto indica que la norma $\|f_A\|_u$ se puede usar para medir cuanto se parece el conjunto A, en sus propiedades combinatorias relativas a ecuaciones lineales, a un conjunto aleatorio de la misma densidad. Se dice que, cuanto más pequeño es el valor de $\|f_A\|_u$, más *quasi-aleatorio* es el conjunto. Nótese, no obstante, que los conjuntos aleatorios no son los únicos ejemplos de conjuntos con norma de uniformidad muy pequeña (este matiz conduce a temas muy interesantes; véase el ejercicio 8).

De todos modos, con la proposición 2.7 nuestro problema inicial queda resuelto en el caso de conjuntos suficientemente quasi-aleatorios: si $\|f_A\|_u$ es suficientemente pequeña como función de α, entonces cualquier promedio del tipo de (2.8) tiene que ser cercano a su valor principal (que es también aproximadamente el valor esperado de este promedio para un conjunto aleatorio de la misma densidad).

A continuación exploramos el caso no quasi-aleatorio, a partir de la pregunta siguiente:

Pregunta 2.10. ¿Suponiendo que $\|f_A\|_u$ es mayor que una función dada de α, qué información combinatoria podemos deducir acerca de A?

Empecemos buscando algunos ejemplos de conjuntos A que tengan $\|f_A\|_u$ grande (al menos una fracción fija de α). Dado que los conjuntos aleatorios fueron tan buenos ejemplos de la propiedad opuesta, es natural buscar ahora entre conjuntos con una estructura "ordenada". Para precisar esto, volvamos a la intuición geométrica que nos condujo al ejemplo del conjunto aleatorio. Vemos pronto que una manera natural de que el promedio $\mathbb{E}_{x\in G}1_A(x)e(r\cdot x)$ tenga la mayor magnitud posible es que para $x \in A$ los números complejos $e_r(x)$ apunten lo más posible en la misma dirección en el plano (minimizando así su cancelación mutua). La manera óptima de garantizar esto es que $x \mapsto r \cdot x$ sea constante sobre A. Esto se da, por ejemplo, si A es una clase lateral del llamado *conjunto anulador* de r.

Definición 2.11. Dado un conjunto $S \subset G$, el *anulador* de S es el subgrupo de G denotado $S^\perp$ y definido como sigue

$$S^\perp := \{x \in G : r \cdot x = 0 \text{ para todo } r \in S\}.$$

(Cuando S es un singleton $\{r\}$ escribiremos $r^\perp$ en vez de $\{r\}^\perp$.)

Tenemos que $r \cdot x$ es constante para todo $x \in A$ si y solo si A está contenido en una clase lateral de $r^\perp$. (En ámbitos del análisis de Fourier más generales, donde no se da el isomorfismo $G \cong \widehat{G}$, el conjunto anulador se define como subgrupo del grupo dual: $S^\perp := \{\chi \in \widehat{G} : \chi(r) = 1 \text{ para todo } r \in S\}$.)

Trabajar con estos conjuntos $r^\perp$ nos será de muy gran utilidad siempre y cuando se pueda garantizar que el tamaño de un tal subgrupo es comparable al orden de G. Ahora bien, esto no es el caso en cualquier grupo G, y por esta razón a partir de ahora es conveniente distinguir algunos tipos diferentes de grupos abelianos finitos.

Una familia de grupos G especialmente ricos en subgrupos anuladores de gran tamaño es la familia de espacios vectoriales finitos $G = \mathbb{F}_p^n$, donde p es un primo fijo y n es la dimensión (que típicamente se toma mucho más grande que p). Como veremos en la sección siguiente, esta familia es muy útil, por la riqueza de subgrupos (subespacios) de densidades variadas que contiene, y porque en estos grupos muchos cálculos de análisis de Fourier se reducen a simples argumentos de álgebra lineal. En estos grupos, los subespacios constituyen ejemplos óptimos de conjuntos densos con grandes coeficientes de Fourier no-principales.

Ejemplo 2.12 (Transformada de Fourier de un subespacio)**.** *Sea V un subespacio de $\mathbb{F}_p^n$, y sea $N = |\mathbb{F}_p^n| = p^n$. Entonces tenemos*[7]*, para toda frecuencia $r \in \mathbb{F}_p^n$,*

$$\widehat{1}_V(r) = \frac{|V|}{N} 1_{V^\perp}(r). \tag{2.10}$$

En particular, para todo $r \in V^\perp$ la transformada alcanza su valor máximo posible $\frac{|V|}{N}$.

En el otro extremo tenemos los grupos cíclicos $\mathbb{Z}_N$ con N primo, que no contienen ningún subgrupo no-trivial. En particular, en estos grupos un conjunto anulador $r^\perp$ con $r \neq 0$ no es más que el singleton $\{0\}$. ¿Qué noción podemos usar en este tipo de grupos para reemplazar los conjuntos anuladores? Como veremos, resulta sumamente útil trabajar con una familia de conjuntos que constituyen *anuladores aproximativos* de caracteres. Estos conjuntos son los llamados *conjuntos de Bohr*.

[7]Véase el ejercicio 4.

Definición 2.13. Sea $S \subset G$ y sea $\delta \geq 0$. El *conjunto de Bohr* con *frecuencias* en S y *radio* δ es el conjunto $B(S,\delta) = \{x \in G : \|r \cdot x\|_{\mathbb{T}} \leq \delta \text{ para todo } r \in S\}$.

Aquí, dado un elemento $\theta \in \mathbb{T}$, representado por un punto del intervalo $[-1/2, 1/2)$, denotamos por $\|\theta\|_{\mathbb{T}}$ la distancia entre θ y el conjunto $\mathbb{Z}$, es decir $\|\theta\|_{\mathbb{T}} = |\theta|$. Recordamos también las desigualdades básicas

$$4\|\theta\|_{\mathbb{T}} \leq |1 - e(\theta)| \leq 2\pi\|\theta\|_{\mathbb{T}}. \tag{2.11}$$

Los conjuntos de Bohr tienen varias propiedades que los hacen semejantes a subgrupos; veremos ejemplos de tales propiedades en la sección siguiente. Por ahora, confirmemos que los conjuntos de Bohr pueden ser de gran densidad y que tienen grandes coeficientes de Fourier.

Proposición 2.14. *Sea $\delta \leq 1/(4\pi)$, sea $S \subset G$, y denotemos por β la densidad $|B(S,\delta)| / |G|$. Entonces para todo $r \in S$ tenemos $|\widehat{1_{B(S,\delta)}}(r)| \geq \beta/2$. Tenemos también*

$$\delta^{|S|} \leq \beta \leq 4/|S|. \tag{2.12}$$

Prueba. Denotando $B(S,\delta)$ por B, tenemos

$$|G|\, |\widehat{1_B}(r)| = \Big|\sum_{x\in B} e_r(x)\Big| = \Big||B| - \sum_{x\in B}(1 - e_r(x))\Big| \geq |B| - \sum_{x\in B}\big|1 - e_r(x)\big|.$$

Si $r \in S$ entonces $\sum_{x\in B}\big|1 - e_r(x)\big| \leq |B|\, 2\pi \sup_{x\in B}\|r \cdot x\|_{\mathbb{T}} \leq |B|/2$, de donde sigue nuestra primera afirmación.

Combinando esta estimación con la identidad de Parseval obtenemos $\beta = \sum_r |\widehat{1_B}(r)|^2 \geq |S|\beta^2/4$, de donde sigue la segunda desigualdad de (2.12).

Para todo elemento fijo $z = (z_r)_{r\in S} \in \mathbb{T}^S$, tenemos

$$\sum_{x\in G}\prod_{r\in S} 1_{\|r\cdot x - z_r\| < \delta/2}(x,z) = |\{x \in G : \|r \cdot x - z_r\| < \delta/2,\ \forall\, r \in S\}|.$$

Si fijamos cualquier elemento x_0 que verifica $\|r \cdot x_0 - z_r\| < \delta/2$ para todo $r \in S$, entonces para todo otro elemento x con esta propiedad tenemos que $y = x - x_0$ verifica $\|r \cdot y\| \leq \|r \cdot x - z_r\| + \|r \cdot x_0 - z_r\| < \delta$. Deducimos que

$$\sum_{x\in G}\prod_{r\in S} 1_{\|r\cdot x - z_r\| < \delta/2}(x,z) \leq |\{y \in G : \|r \cdot y\| < \delta,\ \forall\, r \in S\}| = |B(S,\delta)|.$$

Integrando esto sobre $z \in \mathbb{T}^S$ deducimos que $\sum_{x\in G}\delta^{|S|} \leq |B(S,\delta)|$, de donde sigue la primera desigualdad en (2.12). □

Nótese que en grupos $\mathbb{F}_p^n$ un conjunto de Bohr $B(S,\delta)$ siempre contiene el subespacio anulador $S^\perp$ (de hecho es igual a este subespacio si $\delta < 1/p$). Esta propiedad tiene

una versión análoga en $\mathbb{Z}_N$, si reemplazamos los subespacios por progresiones aritméticas simétricas con respecto a 0.

Ejemplo 2.15. *Un conjunto de Bohr $B(S,\delta)$ en $\mathbb{Z}_N$ contiene una progresión aritmética centrada en 0 y de cardinalidad al menos $\delta N^{1/|S|}$.*

Esto se demuestra usando el teorema de aproximación simultánea de Dirichlet (véase el ejercicio 6). Se dice que la progresión en este ejemplo es "larga" porque su cardinalidad es una función de N que tiende al infinito con N, si $|S|$ y δ están fijados.[8] (Si se quiere ser más preciso, se dice que la progresión tiene *tamaño polinomial* en N.) Como veremos, a menudo en $\mathbb{Z}_N$ es técnicamente más conveniente trabajar con tales progresiones aritméticas que con conjuntos de Bohr enteros.

Las progresiones aritméticas son nuestro tercer y último ejemplo de conjuntos con grandes coeficientes de Fourier.

Lema 2.16. *Sea P una progresión aritmética en $\mathbb{Z}_N$ (N primo), de cardinalidad $\ell \in (0, N/2)$ y diferencia común d. Entonces $|\widehat{1_P}(d^{-1})| \geq 2\ell/(\pi N)$. Tenemos también $|\widehat{1_P}(r)| \leq \min\{\frac{\ell}{N}, \frac{1}{2N\|rd/N\|_{\mathbb{T}}}\}$ para todo $r \neq 0$.*

Prueba. Nótese primero que la magnitud de los coeficientes de Fourier de un conjunto no cambia si se traslada el conjunto, de modo que podemos suponer que $P = \{0, d, 2d, \ldots, (\ell-1)d\}$. Usando (2.11), tenemos entonces $N\,|\widehat{1_P}(d^{-1})| = \left|\sum_{t=0}^{\ell-1} e(t/N)\right| = \frac{|1-e(\ell/N)|}{|1-e(1/N)|} \geq 2\ell/\pi$. Por otro lado, para todo $r \neq 0$ tenemos $N\,|\widehat{1_P}(r)| = \left|\sum_{t=0}^{\ell-1} e(trd/N)\right| = \frac{|1-e(\ell rd/N)|}{|1-e(rd/N)|} \leq \frac{1}{2\|rd/N\|_{\mathbb{T}}}$. □

Hemos visto algunos ejemplos principales de conjuntos A con gran norma $\|f_A\|_u$. Sin embargo, se ve fácilmente que estos ejemplos no son exhaustivos: si A es un tal conjunto y B es un conjunto suficientemente quasi-aleatorio disjunto de A, entonces (por la linealidad de la transformada de Fourier) el conjunto $C = A \cup B$ también tiene $\|f_C\|_u$ grande. Por lo tanto, aun no hemos dado una respuesta general satisfactoria a la pregunta 2.10.

El ejemplo del conjunto C que acabamos de ver sugiere una posible respuesta: si $\|f_A\|_u$ es grande, puede que A no sea uno de los conjuntos estructurados que hemos visto, pero a lo mejor es necesario que A tenga una intersección de gran tamaño con un tal conjunto.

Roth confirmó una idea de este tipo en [15] trabajando en grupos $\mathbb{Z}_N$, y la usó para demostrar su teorema sobre progresiones de longitud 3 (teorema que veremos en la sección siguiente). Más precisamente, la idea de Roth es que si $\|f_A\|_u$ es grande entonces existe una

[8] Se conoce un resultado más fuerte, a saber que un conjunto de Bohr $B(S,\delta)$ en $\mathbb{Z}_N$ siempre contiene una progresión aritmética generalizada (o multidimensional) de *densidad positiva* dependiente sólo de $|S|, \delta$ (véase [19, Proposición 4.22]).

progresión aritmética larga dentro de la cual el conjunto A tiene *mayor densidad* que en el grupo original. Terminaremos esta sección con este resultado, pero primero presentamos un resultado análogo en los grupos $\mathbb{F}_p^n$, donde el argumento se puede expresar más limpiamente usando subespacios de codimensión 1 en vez de progresiones aritméticas.

Lema 2.17 (Incremento de densidad en $\mathbb{F}_p^n$)**.** *Sea $A \subset \mathbb{F}_p^n$ de densidad α, y sean $r \in \mathbb{F}_p^n \backslash \{0\}$ y $c > 0$ tales que $|\widehat{1_A}(r)| \geq c\alpha$. Entonces existe un subespacio $V \leqslant \mathbb{F}_p^n$ de codimensión 1 tal que $|A \cap (x+V)| \,/\, |V| \geq \alpha(1 + c/2)$ para algún $x \in \mathbb{F}_p^n$.*

Prueba. Como es de esperar, el subespacio que tomaremos es el conjunto anulador $V = r^\perp$. Las clases laterales de este subgrupo son las preimágenes de los elementos de $\{0, \frac{1}{p}, \dots, \frac{p-1}{p}\}$ por la función $\mathbb{F}_p^n \to \mathbb{T}$, $x \mapsto r \cdot x$. Fijando un elemento x_j en cada una de estas preimágenes, tenemos $\mathbb{F}_p^n = \bigsqcup_{j=0}^{p-1} x_j + V$. Denotemos por α_j la densidad que tiene A dentro de $x_j + V$, es decir $\alpha_j = |A \cap (x_j + V)|/|V|$. Podemos multiplicar $\widehat{1}_A(r)$ por algún número $e(\theta)$ de modo que tengamos $\widehat{1}_A(r)e(\theta) > 0$. Entonces, usando el hecho que $\mathbb{E}_{x \in \mathbb{F}_p^n} f_A(x) = 0$, tenemos

$$c\alpha \leq \widehat{1}_A(r)e(\theta) = \widehat{f}_A(r)e(\theta) = \mathbb{E}_{x \in \mathbb{F}_p^n}\, f_A(x)\, (e(r \cdot x + \theta) + 1).$$

Tomando la parte real, tenemos $c\alpha \leq \mathbb{E}_{x \in \mathbb{F}_p^n}\, f_A(x)\, \mathrm{Re}(e(r \cdot x + \theta) + 1)$. La función $x \mapsto \mathrm{Re}(e(r \cdot x + \theta) + 1)$ toma un valor constante en el intervalo $[0, 2]$ sobre cada clase $x_j + V$, valor que denotaremos por λ_j. Tenemos entonces

$$c\alpha \leq \frac{1}{p^n} \sum_{j=0}^{p-1} \sum_{x \in x_j + V} (1_A(x) - \alpha)\, \lambda_j = \frac{|V|}{p^n} \sum_{j=0}^{p-1} \lambda_j\, \mathbb{E}_{x \in x_j + V}(1_A(x) - \alpha) = \mathbb{E}_{j \in [0, p-1]}\, \lambda_j(\alpha_j - \alpha).$$

Tiene por lo tanto que existir $j \in [0, p-1]$ tal que $c\alpha \leq \lambda_j(\alpha_j - \alpha)$, de lo cual se deduce que $\alpha_j \geq \alpha + c\alpha/2$. □

En este argumento hemos obtenido el incremento de densidad sobre una traslación del subespacio anulador de un carácter dominante de A (un carácter e_r para el cual $|\widehat{f_A}(r)| = \|f_A\|_u$).

Pasamos ahora a los grupos cíclicos de orden primo. Aquí, como ya mencionamos, no hay subgrupos anuladores no-triviales, pero podemos aun obtener un incremento de densidad sobre una traslación de una progresión aritmética larga que es *anuladora aproximativa* de un carácter dominante. Este aspecto aproximativo hace que este argumento sea un poco más técnico que el de $\mathbb{F}_p^n$, por dos razones principales.

Primero, en $\mathbb{Z}_N$ la partición del grupo en traslaciones de una misma progresión es solo aproximativa (es decir que no se da exactamente el análogo de la partición de $\mathbb{F}_p^n$ en clases laterales de V). Segundo, para las aplicaciones, a menudo querremos garantizar que, si empezamos con $A \subset \mathbb{Z}_N$ visto como un conjunto de enteros en $[N]$, entonces el incremento

de densidad tiene lugar en una progresión aritmética en $\mathbb{Z}_N$ que es también una progresión en $\mathbb{Z}$ (por ejemplo, el conjunto $\{4, 5, 1\}$ es una progresión en $\mathbb{Z}_5$ pero no lo es en $\mathbb{Z}$).

Estas dificultades se pueden resolver usando el resultado siguiente.

Lema 2.18. *Sea I un intervalo en $\mathbb{Z}_N$ de cardinalidad m, y sea r un elemento no-nulo de $\mathbb{Z}_N$. Para todo $\epsilon > 0$, existe una partición de I en progresiones aritméticas P_i en $\mathbb{Z}_N$ de cardinalidad al menos $\epsilon\sqrt{m}/2$, y tales que para todo $x, y \in P_i$ tenemos $\|(rx - ry)/N\|_{\mathbb{T}} \leq \epsilon$, para todo i.*

Aquí rx/N es nuestra forma bilineal favorita $r \cdot x$ sobre $\mathbb{Z}_N$.

Prueba. El resultado es invariante por traslación en $\mathbb{Z}_N$, con lo cual podemos suponer que I es un intervalo de enteros en $[N]$. Sea $u = \sqrt{m}$, y consideremos los números $0, r, 2r, \ldots, ur$. Por el principio del palomar, existen $v < w$ en $[0, u]$ tales que $\|r \cdot w - r \cdot v\|_{\mathbb{T}} = \|r \cdot (w - v)\|_{\mathbb{T}} \leq 1/u$. Denotando $w - v$ por s, dividimos I en clases módulo s, y observamos que cada clase tiene cardinalidad al menos $\lfloor m/s \rfloor \geq \lfloor m/u \rfloor$. Cada una de estas clases puede ser dividida en progresiones aritméticas de la forma $a, a + s, \ldots, a + \ell s$, con $\epsilon u/2 < \ell \leq \epsilon u$. Para cualquier tal progresión P_i, tenemos $\|r \cdot x - r \cdot y\|_{\mathbb{T}} \leq \ell \|r \cdot s\|_{\mathbb{T}} \leq \epsilon$ para todo $x, y \in P_i$. □

Dado un conjunto X y una función $\phi : X \to \mathbb{C}$, llamaremos la cantidad $\sup_{x,y \in X} |\phi(x) - \phi(y)|$ el *diámetro* de ϕ sobre X. Del último lema deducimos, usando (2.11), que el carácter e_r tiene diámetro como mucho $2\pi\epsilon$ sobre cada progresíon P_i. En otras palabras, cada progresión P_i es un *conjunto de nivel aproximado* para e_r (un conjunto sobre el cual e_r es casi constante).

Podemos ahora demostrar el incremento de densidad en grupos $\mathbb{Z}_N$, con la garantía adicional de que si identificamos el conjunto subyacente con $[N]$, entonces la progresión donde ocurre el incremento es una progresión en $\mathbb{Z}$ (y no solo en $\mathbb{Z}_N$).

Lema 2.19 (Incremento de densidad en $[N]$)**.** *Sea $B \subset [N]$ de densidad $|B|/N = \beta$ y sean $r \neq 0$ en $\mathbb{Z}_N$ y $c > 0$ tales que en $\mathbb{Z}_N$ tengamos $|\widehat{1_B}(r)| \geq c\beta$. Entonces existe una progresión aritmética $P \subset [N]$ de cardinalidad al menos $c_1\sqrt{N}$ tal que*

$$|B \cap P| / |P| \geq \beta(1 + c_2).$$

Podemos tomar $c_1 = c/60$, $c_2 = c/4$.

Prueba. Fijando $\epsilon = c/(8\pi)$, usando el lema 2.18 dividimos $[N]$ en progresiones aritméticas de longitud al menos $\epsilon\sqrt{N}/2$, sobre cada una de las cuales el carácter e_r tiene diámetro como mucho $2\pi\epsilon$. Fijando un elemento x_i arbitrario en cada progresión P_i, deducimos lo

siguiente:

$$\begin{aligned}|\widehat{f_B}(r)|\,N \leq \sum_i \Big|\sum_{x\in P_i} f_B(x)e(r\cdot x)\Big| &= \sum_i \Big|\sum_{x\in P_i} f_B(x)e_r(x_i) + \sum_{x\in P_i} f_B(x)\big(e_r(x)-e_r(x_i)\big)\Big| \\ &\leq \sum_i \left[\Big|\sum_{x\in P_i} f_B(x)\Big| + \sum_{x\in P_i}|f_B(x)|2\pi\epsilon\right] \\ &\leq 4\beta\pi\epsilon N + \sum_i \Big|\sum_{x\in P_i} f_B(x)\Big|.\end{aligned}$$

Usando el valor elegido para ϵ, el hecho que $\mathbb{E}_{\mathbb{Z}_N} f_B = 0$, y la suposición $|\widehat{f_B}(r)| \geq c\beta$, deducimos que $\sum_i \big[\big|\sum_{x\in P_i} f_B(x)\big| + \sum_{x\in P_i} f_B(x)\big] \geq c\beta N/2 = \sum_i c\beta|P_i|/2$.

Existe por lo tanto un valor de i tal que

$$\Big|\sum_{x\in P_i} f_B(x)\Big| + \sum_{x\in P_i} f_B(x) \geq c\beta|P_i|/2,$$

de donde sigue que $\sum_{x\in P_i} f_B(x) \geq c\beta|P_i|/4$, lo cual implica el resultado. □

Existen también argumentos de incremento de densidad con respecto a conjuntos de Bohr. Estos argumentos pueden ser mucho más eficientes que los lemas 2.17 y 2.19 de un punto de vista cuantitativo (dando mayores incrementos de densidad); son también bastante más técnicos (ver por ejemplo [16]).

3. Aplicaciones

En esta sección combinamos las ideas vistas en la sección 2 para demostrar algunos resultados clásicos de combinatoria aritmética.

3.1. **Teoremas de Roth y Meshulam.**

¿Cuán grande puede ser un subconjunto de un grupo abeliano finito si el conjunto no contiene progresiones aritméticas de longitud 3? Los teoremas de Roth y de Meshulam dan respuestas no-triviales a esta pregunta, en los grupos $\mathbb{Z}_N$ y $\mathbb{F}_p^n$ respectivamente.

Históricamente el teorema de Roth [15] es anterior al de Meshulam [14], pero la demostración de este último es más sencilla (gracias a la ya mencionada riqueza algebraica de $\mathbb{F}_p^n$), de modo que empezaremos con este resultado. Para esto, no se pierde generalidad con trabajar en $\mathbb{F}_3^n$ en vez de $\mathbb{F}_p^n$.

Teorema 3.1 (Meshulam). *Sea $A \subset G = \mathbb{F}_3^n$, sea $\alpha = |A|/|G|$, y supongamos que A no contiene ninguna progresión aritmética no-trivial de longitud 3. Entonces*[9]

$$\alpha = O(1/\log|G|). \tag{3.1}$$

Prueba. De la suposición inicial deducimos que $T_3(A) = \alpha/|G|$ (contando las progresiones $(x, x+d, x+2d)$ con $d = 0$). La Proposición 2.6 implica entonces que $\|f_A\|_u \geq \alpha^{-1}(\alpha^3 - \alpha/|G|)$. Si $|G| \geq 2\alpha^{-2}$, obtenemos que $\|f_A\|_u \geq \alpha^2/2$.

Podemos entonces obtener un incremento de densidad: el Lema 2.17 nos da un subespacio V_1 y un elemento x_1 tal que $|A \cap (x_1 + V_1)|/|V_1| \geq \alpha(1+\alpha/4)$. Denotemos el conjunto $A \cap (x_1 + V_1)$ por A_1, y su densidad en V_1 por α_1. Observemos que este A_1, siendo un subconjunto de A, tampoco contiene progresiones. Como una traslación de una progresión sigue siendo una progresión, podemos trasladar A por $-x_1$ para suponer que A_1 es un subconjunto de $V_1 \cong \mathbb{F}_3^{n-1}$. La idea ahora es repetir este argumento en A_1. Obtenemos así otro subconjunto A_2, dentro de un nuevo subespacio $V_2 \cong \mathbb{F}_3^{n-2}$, con aun mayor densidad $\alpha_2 \geq \alpha_1(1 + \alpha_1/4) \geq \alpha + 2\,\alpha^2/4$.

Cada vez que repetimos el argumento, perdemos una dimensión. Por otro lado, incrementamos la densidad de $\alpha^2/4$. En particular, pasamos de densidad α a 2α en $\alpha/(\alpha^2/4) = 4\alpha^{-1}$ repeticiones, pasamos de 2α a 4α en $2\alpha/((2\alpha)^2/4) = \frac{1}{2}4\alpha^{-1}$ repeticiones, y en general de $2^j\alpha$ a $2^{j+1}\alpha$ en $\frac{1}{2^j}4\alpha^{-1}$ repeticiones. Como la densidad de un conjunto es como mucho 1, no podemos repetir este argumento más de $t = (1 + \frac{1}{2} + \frac{1}{4} + \dots)4\alpha^{-1} = 8\alpha^{-1}$ veces. En particular, después de estas t repeticiones es necesario que $|V_t|$ sea menor que $2\alpha^{-2}$ (de lo contrario sería posible repetir el argumento). Por lo tanto tenemos $|V_t| = 3^{n-8\alpha^{-1}} \leq 2\alpha^{-2}$, de donde sigue la cota (3.1). □

Encontrar el valor óptimo de la cota (3.1) es un problema central en esta área. Por un lado, se intenta reducir la cota, y en este sentido el mejor resultado actualmente conocido es el de Bateman y Katz [1], quienes obtuvieron la cota $\alpha = O\big(1/(\log|G|)^{1+\epsilon}\big)$, para algún $\epsilon > 0$. Por otro lado, se intenta encontrar ejemplos de grandes conjuntos en $\mathbb{F}_3^n$ sin progresiones. El conjunto $\{0,1\}^n$ nos da un primer ejemplo, de cardinalidad 2^n. El ejemplo de mayor cardinalidad actualmente conocido es el que dió Edel en [8], demostrando lo siguiente.

Teorema 3.2 (Edel). *Existe un conjunto $A \subset \mathbb{F}_3^n$ sin progresiones de longitud 3 y de cardinalidad al menos 2.217^n.*

¡La diferencia entre la cota superior de Bateman y Katz y la inferior de Edel es enorme! Sería muy interesante demostrar, por ejemplo, que existe $\epsilon > 0$ tal que si $A \subset \mathbb{F}_3^n$ no

[9]Recuerden la notación de Landau: dos funciones $f(N), g(N)$ satisfacen $f = O(g)$ si y solo si existe una constante absoluta $C > 0$ y un N_0 tal que $|f(N)| \leq C|g(N)|$ para todo $N \geq N_0$.

contiene progresiones de longitud 3 entonces $|A| \leq (3-\epsilon)^n$.

Pasamos ahora al teorema de Roth.

Teorema 3.3 (Roth)**.** *Sea $A \subset [N]$, sea $\alpha = |A|\,/\,N$, y supongamos que A no contiene ninguna progresión aritmética no-trivial de longitud 3. Entonces*

$$\alpha = O(1/\log\log N). \tag{3.2}$$

La prueba usa las mismas ideas que la prueba anterior, pero técnicamente es un poco más compleja. Uno de los problemas aquí es que el intervalo de enteros $[N]$ no tiene estructura de grupo con la cual hacer análisis de Fourier, de modo que primero tendremos que trasladar el problema a un grupo cíclico. Además, tendremos que hacer esto sin perder de vista que estamos buscando progresiones en los enteros y no solo en grupos cíclicos.

Prueba. Denotemos por α la densidad de A en $[N]$, y supongamos que $N > 50/\alpha^2$. Sea p un número primo entre $N/3$ y $2N/3$ (cuya existencia está garantizada por el postulado de Bertrand).

Nótese primero que, denotando por B el conjunto $A \cap [p]$ y por β la densidad de B en $[p]$, podemos suponer que $\beta \geq \alpha(1-\alpha/200)$, pues de lo contrario tendríamos $|A \cap [p+1, N]| \geq \alpha(N-p) + \alpha^2 p/200 \geq \alpha(1+\alpha/400)(N-p)$, lo cual implicaría que ya tendríamos un incremento de densidad apropiado en la progresión aritmética $[p+1, N]$. Trabajemos por lo tanto con este conjunto B, usando la transformada de Fourier en $\mathbb{Z}_p$.

De nuestra suposición combinatoria sobre A deduciremos primero una cota inferior no-trivial para $\|f_B\|_u$. Sea $B' = B \cap [p/3, 2p/3]$, con densidad en $[p]$ denotada β', y nótese que una progresión aritmética en $B \times B' \times B'$ modulo p es siempre una progresión en los enteros (y contenida en A, por supuesto). Por lo tanto, tenemos

$$\big|\beta\beta'^2 - \mathbb{E}_{\substack{x_1,x_2,x_3 \in \mathbb{Z}_p \\ x_1 - 2x_2 + x_3 = 0}} 1_B(x_1) 1_{B'}(x_2) 1_{B'}(x_3)\big| = |\beta\beta'^2 - \beta'/p\,|.$$

La proposición 2.7 nos dice que esto es como mucho $\|f_B\|_u \beta'$. Por otro lado, podemos suponer que $\beta' \geq \beta/5$. En efecto, de lo contrario tendríamos $|B \cap [p/3]| \geq 2\beta p/5$ o bien $|B \cap [2p/3, p]| \geq 2\beta p/5$, y entonces B tendría una densidad al menos $(2\beta p/5)/(p/3) = 6\beta/5$ en una de las progresiones $[p/3]$, $[2p/3, p]$. Concluimos que $\|f_B\|_u \geq \beta^2/5 - 1/p \geq \beta^2/10$.

Podemos ahora deducir el incremento de densidad deseado. El lema 2.19 nos dice que existe una progresión $P \subset [p]$ de longitud al menos $(\beta/600)\sqrt{p} \geq \alpha\sqrt{N}/2^{10}$ en la cual la densidad de B (y por lo tanto de A) se incrementa de $\beta^2/40 \geq \alpha^2/80$.

A partir de aquí, la prueba consiste en una iteración muy similar a la que ya vimos para el teorema de Meshulam. Repetimos el argumento como mucho $80/\alpha$ veces para

que la densidad suba de α a 2α, y siguiendo así se llegaría a una densidad 1 después de $t \leq 80\alpha^{-1}(1 + \frac{1}{2} + \frac{1}{4} + \cdots) \leq 160\alpha^{-1}$ repeticiones. En cada repetición pasamos de una progresión de longitud m a una de longitud $(\alpha/2^{10})\sqrt{m}$, con lo cual la longitud de la progresión después de t repeticiones es $(\alpha/2^{10})^{1+1/2+1/4+\cdots} N^{1/2^t} \geq (\alpha^2/2^{20}) N^{1/2^{160\alpha^{-1}}}$. Para que no haya contradicción (es decir que no se pueda repetir más el incremento) es necesario que $(\alpha^2/2^{20}) N^{1/2^{160\alpha^{-1}}} \leq 50\alpha^{-2}$, de donde se deduce la cota (3.2). □

El problema de mejorar (reducir) la cota (3.2) es tan famoso como en el caso del teorema de Meshulam. De hecho lo es quizás aun más, por sus consecuencias directas en teoría de números. Por ejemplo, una cota de tipo $\alpha \leq 1 / (\log N)^{1+c}$, para alguna constante absoluta $c > 0$, implicaría el *teorema de Roth en los números primos*, a saber que todo subconjunto de los números primos de densidad positiva contiene una progresión de longitud 3. Este resultado ya fue demostrado por Green en [11], pero la idea aquí es que con la cota mencionada el resultado se deduciría mucho más fácilmente, usando sólo el teorema de los números primos. La mejor cota actualmente conocida para el teorema de Roth se debe principalmente a Sanders, quien demostró en [16], combinando varias herramientas recientes en un argumento bastante técnico de incremento de densidad sobre conjuntos de Bohr, que la cota superior en (3.2) se puede reducir a $(\log\log N)^6 / \log N$; véase también la mejora de Bloom en [3] que reduce la potencia 6 a 4.

En cuanto a ejemplos de grandes subconjuntos de $[N]$ sin progresiones, la construcción principal conocida se debe a Behrend [2] ¡ y no se ha mejorado significativamente desde 1946 ! (Para una exposición clara de una cota algo más fuerte, siguiendo la idea original de Behrend, véase [12].)

Teorema 3.4 (Behrend)**.** *Existe un conjunto $A \subset [N]$ sin progresiones aritméticas de longitud 3 que verifica*

$$\alpha \geq c\ \exp\big(-c\sqrt{\log N}\big),$$

donde $c > 0$ es una constante absoluta.

3.2. **Lema de Bogolyubov.**

Recordemos que, dados dos subconjuntos A, B de un grupo abeliano, su *conjunto suma* es $A + B = \{a + b : a \in A, b \in B\}$. Como ya mencionamos, este conjunto es precisamente el soporte de la convolución $1_A * 1_B$.

El resultado del que trataremos aquí es un ejemplo central de cómo la transformada de Fourier permite estudiar la estructura de conjuntos suma, gracias a su interacción con la operación de convolución. Hay un principio general en análisis relativo a la operación de

convolución, según el cual esta operación "suaviza" las funciones[10]. En particular cuanto más se repite esta operación (tomando $f * f$, después $f * f * f$, etc.) más regular se hace la función. Este principio tiene una versión análoga de gran utilidad en combinatoria aritmética, a saber que tomar sumas (o diferencias) iteradas de un conjunto produce conjuntos con estructura aritmética cada vez más rica. El resultado principal de esta sección ilustra esto con el conjunto de suma y diferencia siguiente:

$$2A - 2A = \{a_1 + a_2 - a_3 - a_4 : a_1, a_2, a_3, a_4 \in A\}.$$

Usando la transformada de Fourier, se puede demostrar que un tal conjunto siempre contiene un conjunto de Bohr de gran densidad (densidad que depende sólo de $\alpha = |A|/|G|$). Este resultado, llamado comúnmente *lema de Bogolyubov*, se origina en [4] y juega un papel importante en el área (como indicamos más adelante).

Lema 3.5 (Bogolyubov)**.** *Sea A un subconjunto de densidad α en un grupo abeliano finito G. Entonces existe $S \subset G$ con $|S| \leq 2\alpha^{-2}$ y tal que $2A - 2A \supset B(S, \frac{1}{4})$.*

Antes de dar la prueba, motivaremos este resultado describiendo unas propiedades básicas de los conjuntos de Bohr que los hacen semejantes a subgrupos; de modo que, efectivamente, el lema nos dice que $2A - 2A$ tiene una rica estructura aditiva. Nótese también que si tomamos menos sumandos, considerando por ejemplo $A - A$ en vez de $2A - 2A$, entonces el lema falla (véase el ejercicio 7).

Definición 3.6 (Grupo aproximado)**.** Sea K un entero positivo. Un subconjunto finito S de un grupo abeliano es un *grupo K-aproximado* si contiene el elemento 0, es simétrico respecto a 0 (es decir que $S = -S$) y existe un cubrimiento de $S + S$ por K traslaciones de S.

Esta noción aparece en [19, Definición 2.25].

Lema 3.7. *Un conjunto de Bohr $B(S, \delta)$ es un grupo $11^{|S|}$-aproximado.*

Para demostrar esto usamos un resultado muy útil llamado *lema de cubrimiento*, introducido por Ruzsa.

Lema 3.8 (Ruzsa)**.** *Sean A, B subconjuntos finitos de un grupo abeliano tales que $|A + B| \leq K|A|$. Entonces existe un subconjunto $X \subset B$ de cardinalidad $|X| \leq K$ tal que $B \subset A - A + X$.*

[10]Una instancia precisa de este principio es que para funciones integrables $f, g : \mathbb{R} \to \mathbb{R}$, si f y g se pueden derivar m y n veces respectivamente, entonces la convolución $f * g$ se puede derivar $m + n$ veces.

Prueba. Sea $\mathcal{X}$ la familia de conjuntos $Y \subset B$ tales que los conjuntos $y + A$, $y \in Y$ son disjuntos dos a dos. Sea X un miembro de $\mathcal{X}$ de cardinalidad máxima. Entonces, por un lado, tenemos $|X|\,|A| = |X + A| \leq |B + A| \leq K\,|A|$, de donde sigue que $|X| \leq K$, y por otro lado, siendo X máximo, para todo $b \in B$ existe $x \in X$ tal que $(b + A) \cap (x + A) \neq \emptyset$, luego $b \in x + A - A$. □

Prueba del lema 3.7. Arguyendo como en la prueba de la proposición 2.14 tenemos, para todo $z \in \mathbb{T}^S$,

$$\sum_{x \in G} \prod_{r \in S} 1_{\|r \cdot x - z_r\| < \frac{\delta}{2}}(x, z) \leq |B(S, \delta)|.$$

Sea $\lambda > 0$. Definimos el conjunto $Z = \{z \in \mathbb{T}^S : \sup_{r \in S} \|z_r\| \leq (\lambda + \frac{1}{2})\,\delta\}$. Tenemos entonces

$$\begin{aligned}
\delta^{|S|}\,|B(S, \lambda\delta)| &= \sum_{x \in B(S, \lambda\delta)} \int_{\mathbb{T}^S} \prod_{r \in S} 1_{\|r \cdot x - z_r\| < \frac{\delta}{2}}(x, z)\, \mathrm{d}\mu_{\mathbb{T}^S}(z) \\
&= \int_{\mathbb{T}^S} \sum_{x \in B(S, \lambda\delta)} \prod_{r \in S} 1_{\|r \cdot x - z_r\| < \frac{\delta}{2}}(x, z)\ \ 1_Z(z)\, \mathrm{d}\mu_{\mathbb{T}^S}(z) \\
&\leq \int_Z \sum_{x \in G} \prod_{r \in S} 1_{\|r \cdot x - z_r\| < \frac{\delta}{2}}(x, z)\, \mathrm{d}\mu_{\mathbb{T}^S}(z) \ \leq\ |B(S, \delta)|\ \mu_{\mathbb{T}^S}(Z).
\end{aligned}$$

Como $\mu_{\mathbb{T}^S}(Z) = ((2\lambda + 1)\delta)^{|S|}$, deducimos que

$$\forall\, \lambda > 0, \qquad |B(S, \lambda\delta)| \leq (2\lambda + 1)^{|S|} |B(S, \delta)|. \tag{3.3}$$

Denotemos $B(S, \lambda\delta)$ por B_λ. Aplicando (3.3) tenemos $|B_{1/2} + B_2| \leq |B_{5/2}| \leq 11^{|S|} B_{1/2}$. Por lo tanto el lema de cubrimiento de Ruzsa nos da un conjunto $X \subset B_2$ de cardinalidad como mucho $|B_{5/2}|/|B_{1/2}| \leq 11^{|S|}$, tal que $B_2 \subset X + B_{1/2} - B_{1/2} \subset X + B_1$. Por lo tanto, el conjunto $B(S, \delta) + B(S, \delta) \subset B_2$ se puede cubrir con $11^{|S|}$ traslaciones de $B(S, \delta)$, a saber las traslaciones $x + B_1$, $x \in X$. □

Para demostrar el lema 3.5, introducimos la noción Fourier-analítica siguiente.

Definición 3.9. Sea $\epsilon > 0$ y sea $f : G \to \mathbb{C}$ con $\|f\|_{L^\infty} \leq 1$. El *ϵ-espectro* de f es el conjunto de frecuencias

$$\mathrm{Spec}_\epsilon(f) = \{r \in \widehat{G} : |\widehat{f}(r)| \geq \epsilon\}.$$

La identidad de Parseval nos da una primera cota superior general para la cardinalidad de este conjunto. En efecto, tenemos

$$\|f\|_{L^2}^2 = \|\widehat{f}\|_{\ell^2}^2 \geq \sum_{r \in \mathrm{Spec}_\epsilon(f)} |\widehat{f}(r)|^2 \geq \epsilon^2\, |\mathrm{Spec}_\epsilon(f)|,$$

luego $|\mathrm{Spec}_\epsilon(f)| \leq \epsilon^{-2}\|f\|_{L^2}^2 \leq \epsilon^{-2}\|f\|_{L^\infty}^2$.

Podemos ahora demostrar el lema de Bogolyubov.

Prueba del lema 3.5.
La primera observación clave es que $2A - 2A = \mathrm{supp}(1_A * 1_A * 1_{-A} * 1_{-A})$. Por otra parte, tenemos para todo $x \in G$

$$1_A * 1_A * 1_{-A} * 1_{-A}(x) = \sum_{r \in \widehat{G}} |\widehat{1}_A(r)|^4 \, e_r(x). \tag{3.4}$$

Fijemos $S = \mathrm{Spec}_\lambda(1_A)$, donde $\lambda > 0$ es un parámetro que escogeremos más tarde. La idea es que para probar que $B(S, \frac{1}{4}) \subset 2A - 2A$, basta con demostrar que para todo $x \in B(S, \frac{1}{4})$ la convolución en (3.4) es positiva en x. Esta convolución es igual a

$$\mathrm{Re} \sum_r |\widehat{1}_A(r)|^4 e_r(x) = \sum_{r \in S} |\widehat{1_A}(r)|^4 \cos(2\pi \, r \cdot x) + \sum_{r \notin S} |\widehat{1_A}(r)|^4 \cos(2\pi \, r \cdot x).$$

Como $\cos(2\pi \, r \cdot x) > 0$ para todo $x \in B(S, \frac{1}{4})$ y todo $r \in S$, deducimos que

$$1_A * 1_A * 1_{-A} * 1_{-A}(x) \ \geq \ |\widehat{1}_A(0)|^4 - \sum_{r \notin S} |\widehat{1}_A(r)|^4 \ = \ \alpha^4 - \sum_{r \notin S} |\widehat{1}_A(r)|^4.$$

La identidad de Parseval nos da que $\sum_{r \notin S} |\widehat{1_A}(r)|^4 \leq \lambda^2 \alpha$. Fijando $\lambda = \alpha^{3/2}/\sqrt{2}$, deducimos que la convolución es positiva como deseado. □

Mejorar la cota $2\alpha^{-2}$ en el lema de Bogolyubov es un problema de gran importancia actualmente en combinatoria aritmética, en particular por su relación con la *conjetura polynomial de Freiman-Ruzsa* (para más información sobre esta conjetura, véase los apuntes de Julia Wolf en este curso). La mejor cota actualmente conocida fue obtenida por Sanders [17], y esencialmente reduce $2\alpha^{-2}$ a $O(\log^4(1/\alpha))$. Para una prueba alternativa (y bastante clara) de esta mejora, véase [7, Teorema 7.5].

Bibliografía

[1] M. Bateman, N. H. Katz, *New bounds on cap sets*, J. Amer. Math. Soc. **25** (2012), no. 2, 585–613.

[2] F. A. Behrend, *On sets of integers which contain no three terms in arithmetical progression*, Proc. Nat. Acad. Sci. U. S. A. **32** (1946). 331–332.

[3] T. Bloom, *A quantitative improvement for Roth's theorem on arithmetic progressions*, prepublicación. arXiv:1405.5800

[4] N. Bogolioùboff, *Sur quelques propriétés arithmétiques des presque-périodes*, Ann. Chaire Phys. Math. Kiev **4** (1939), 185–205.

[5] F. Chamizo, *Aplicaciones del análisis armónico*, disponible en www.uam.es/personal_pdi/ciencias/fchamizo/libreria/fich/APcavan.pdf

[6] F. Chamizo, E. Cristóbal, A. Ubis, *El método del círculo*, La gaceta de la RSME, vol. 9.2 (2006), 465–481. www.uam.es/personal_pdi/ciencias/cillerue/Curso/Curso/el metodo del circulo.pdf

[7] E. Croot, I. Laba, O. Sisask, *Arithmetic progressions in sumsets and L^p-almost-periodicity*, Combin. Probab. Comput. **22** (2013), no. 3, 351–365.

[8] Y. Edel, *Extensions of generalized product caps*, Des. Codes Cryptogr. **31** (2004), no. 1, 5–14.

[9] P. Erdős, P. Turán, *On some sequences of integers*, J. London Math. Soc. S1-**11** (1936), no. 4, 261–264.

[10] W. T. Gowers, *A new proof of Szemerédi's theorem*, GAFA **11** (2001), 465–588.

[11] B. Green, *Roth's Theorem in the primes*, Annals of Math. **161** (2005), no. 3, 1609–1636.

[12] B. Green, J. Wolf, *A note on Elkin's improvement of Behrend's construction*, Additive number theory: festschrift in honor of the sixtieth birthday of Melvyn B. Nathanson, Springer, 2010.

[13] H. A. Helfgott, *The ternary Golbach conjecture is true*, prepublicación. arxiv:1312.7748

[14] R. Meshulam, *On subsets of finite abelian groups with no 3-term arithmetic progressions*, J. Combin. Theory Ser. A **71** (1995), 168–172.

[15] K. F. Roth, *On certain sets of integers*, Jour. London Math. Soc. **28** (1953), 245-252.

[16] T. Sanders, *On Roth's theorem on progressions*, Ann. of Math. **174** (2011) (2) , no. 1, 619–636.

[17] T. Sanders, *On the Bogolyubov-Ruzsa lemma*, Anal. PDE **5** (2012), no. 3, 627–655.

[18] E. Szemerédi, *On sets of integers containing no k elements in arithmetic progressions*, Acta Arith. **27** (1975), 299-345.

[19] T. Tao, V. Vu, *Additive combinatorics*, Cambridge University Press, 2006.

[20] P. Varnavides, *On certain sets of positive density*, J. London Math. Soc. **34** (1959), 358–360.

Ejercicios

Ejercicio 1. Demostrar el lema 1.3, a saber que si G es un grupo abeliano finito de exponente n, entonces

(1) Todo carácter $\chi \in \widehat{G}$ toma sus valores en $\{z \in \mathbb{C} : z^n = 1\}$.
(2) Si G es un grupo cíclico $\mathbb{Z}_N$, entonces $\widehat{G} = \{x \mapsto \exp(2\pi i\, rx/N) : r \in \mathbb{Z}_N\}$.

(pista: para la parte (2), usar (1) y el hecho que cada $\chi \in \widehat{\mathbb{Z}_N}$ está determinado por su valor en $x = 1$.)

Ejercicio 2. Demostrar que para todo grupo abeliano finito G y H, tenemos $G \cong H \Rightarrow \widehat{G} \cong \widehat{H}$ y $\widehat{G \oplus H} \cong \widehat{G} \oplus \widehat{H}$.

Ejercicio 3. Demostrar la fórmula de producto para la convolución:

$$\text{para cualquier } \ r \in G \ \text{ y } \ f, g \in \mathbb{C}^G, \quad \widehat{f * g}(r) \ = \ \widehat{f}(r)\, \widehat{g}(r).$$

Ejercicio 4. Sea Z un grupo abeliano finito, sea $F : Z \to \mathbb{C}$, sea H un subgrupo de Z, y sea $g(x) = F(x)1_H(x)$. Demostrar que $\widehat{1_H} = \frac{|H|}{|G|} 1_{H^\perp}$. Usando esto, demostrar que $\widehat{g}(s) = \frac{|H|}{|G|} \sum_{r \in H^\perp} \widehat{F}(s + r)$ para todo $s \in \widehat{G}$. Deducir la *fórmula de Poisson*:

$$\mathbb{E}_{x \in H} F(x) = \sum_{r \in H^\perp} \widehat{F}(r). \tag{1.5}$$

Usando (1.5), demostrar la fórmula (2.4):

$$\mathbb{E}_{\substack{x_1,\dots,x_t \in G: \\ c_1x_1 + \cdots + c_tx_t = 0}} \ f_1(x_1)\, f_2(x_2) \cdots f_t(x_t) \ = \ \sum_{r \in G} \widehat{f_1}(c_1 r)\, \widehat{f_2}(c_2 r) \cdots \widehat{f_t}(c_t r).$$

(pista: aplicar (1.5) con $Z = G^t$ y $H = \{x \in G^t : c_1x_1 + \cdots + c_tx_t = 0\}$.)

Ejercicio 5. Demostrar que la norma U^2 de Gowers,

$$\|f\|_{U^2(G)} = \big(\mathbb{E}_{x,h_1,h_2 \in G}\ f(x)\, \overline{f(x + h_1)}\, \overline{f(x + h_2)}\, f(x + h_1 + h_2)\big)^{1/4},$$

satisface la fórmula $\|f\|_{U^2(G)} = \|\widehat{f}\|_{\ell^4(\widehat{G})}$. Demostrar que $\|f\|_u \le \|f\|_{U^2(G)} \le \|f\|_u^{1/2}\, \|f\|_{L^2(G)}^{1/2}$.

Ejercicio 6. El teorema de aproximación de Dirichlet nos dice que dados unos elementos $\theta_1, \dots, \theta_d \in \mathbb{T}$ cualesquiera y un entero N, existe $n \in [N - 1]$ tal que $\|n\theta_i\|_{\mathbb{T}} \le N^{-1/d}$ para todo $i \in [d]$.

Demostrar que un conjunto de Bohr $B(S, \delta)$ en $\mathbb{Z}_N$ contiene una progresión aritmética

centrada en 0 y de cardinalidad al menos $\delta N^{1/|S|}$.

Sea A un subconjunto de $\mathbb{Z}_N$ de cardinalidad $|A| \leq \frac{1}{10}\log N$. Demostrar que existe $r \neq 0$ tal que $|\widehat{1_A}(r)| \geq \alpha/2$. (Este ejemplo indica que el análisis de Fourier pierde su utilidad combinatoria cuando la densidad del conjunto es demasiado pequeña.)

Ejercicio 7. Demostrar que existe un conjunto $A \subset \mathbb{F}_2^n$ de densidad $1/4$ tal que $A + A$ no contiene ninguna clase lateral de subespacio de codimensión $\sqrt{n}$.
(Pista: considérese $A = \{x \in \mathbb{F}_2^n : x$ tiene al menos $n/2 + \sqrt{n}/2$ coordenadas igual a $1\}$.)

Ejercicio 8 (Construcción explícita de un conjunto extremadamente quasi-aleatorio)**.**
1) Sea $f_s : \mathbb{Z}_p \to \mathbb{C}$, $x \mapsto e(sx^2/p)$, donde $s \in \mathbb{Z}_p \setminus \{0\}$. Usando el hecho que $|\widehat{f_s}(r)|^2 = \mathbb{E}_h \mathbb{E}_x f_s(x+h)\overline{f_s(x)}e(-rh/p)$, demostrar que $\|f_s\|_u \leq p^{-1/2}$.
2) Usando el lema 2.16, demostrar que si P es un intervalo de densidad $1/2$ en $\mathbb{Z}_p$ entonces $\sum_{r\in\mathbb{Z}_p} |\widehat{1_P}(r)| \leq 10 \log p$.
3) Sea $A = \{x \in \mathbb{Z}_p : x^2 \in P\}$. Demostrar que $\widehat{1_A}(r) = \sum_s \widehat{1_P}(s)\widehat{f_s}(r)$, y combinar esto con 1) y 2) para deducir que $\sup_{r\neq 0} |\widehat{1_A}(r)| \leq 10p^{-1/2}\log p$.
4) La norma U^3 de Gowers se define sobre $\mathbb{C}^G$ por

$$\begin{aligned}\|f\|_{U^3(G)} \;=\; \Big(&\mathbb{E}_{x,h_1,h_2,h_3\in G}\, f(x)\,\overline{f(x+h_1)}\,\overline{f(x+h_2)}\,f(x+h_1+h_2)\\ &\overline{f(x+h_3)}f(x+h_1+h_3)f(x+h_2+h_3)\overline{f(x+h_1+h_2+h_3)}\Big)^{1/8}.\end{aligned}$$

Demostrar que $\|f_s\|_{U^3(\mathbb{Z}_p)} = 1$ y $\|1_A\|_{U^3(\mathbb{Z}_p)} \gg 1$.

Ejercicio 9. † A partir del teorema de Roth, deducir la versión siguiente demostrada por Varnavides [20]: para todo $\alpha > 0$ existe $c > 0$ tal que todo conjunto $A \subset [N]$ de densidad α verifica $\mathbb{E}_{x,d\in[N]} 1_A(x)1_A(x+d)1_A(x+2d) \geq c$. (Un resultado análogo se da para el teorema de Meshulam.)

Ejercicio 10. † Una ecuación lineal $c_1x_1 + \cdots + c_tx_t = 0$ es *invariante por traslación* (o simplemente *invariante*) si $c_1 + \cdots + c_t = 0$. Verificar que la prueba del teorema 3.3 se puede adaptar para obtener un resultado análogo para cualquier tal ecuación con $t \geq 3$. Se dice de un sistema de ecuaciones $Mx = 0$ con $M \in \mathbb{Z}^{r\times m}$ que es *invariante* si $M(1,\ldots,1) = 0$, y que tiene *complejidad 1* si, para funciones $f : \mathbb{Z}_p \to \mathbb{C}$ con $\|f\|_\infty \leq 1$, el promedio $\mathbb{E}_{x\in\mathbb{Z}_p^m : Mx=0} f(x_1)\cdots f(x_m)$ tiende a 0 cuando $\|f\|_u \to 0$. (Por ejemplo, los sistemas de una sola ecuación lineal con al menos tres variables son de complejidad 1; esto se ve siguiendo la prueba de la proposición 2.7.) Verificar que la prueba del teorema 3.3 se puede generalizar a todo sistema invariante de complejidad 1.

(Los ejercicios marcados con † son más difíciles.)