

TEMat

Problemas directos e inversos en combinatoria aditiva: las desigualdades de Plünnecke

✉ Alberto Espuny Díaz
University of Birmingham
axe673@bham.ac.uk

Resumen: La combinatoria aditiva es una rama de las matemáticas que ha experimentado un gran crecimiento en el último medio siglo. En este artículo nos centramos en presentar la teoría de los problemas directos e inversos relacionados con los conjuntos suma, una pequeña parte de todos los resultados en este contexto. En particular, nos centramos en presentar y demostrar unas desigualdades tradicionales de esta área, conocidas como desigualdades de Plünnecke-Ruzsa, así como una de sus aplicaciones más directas en un problema inverso.

Palabras clave: combinatoria aditiva, conjuntos suma, desigualdades de Plünnecke.

MSC2010: 11P70, 11B13.

Recibido: 22 de enero de 2017.

Aceptado: 23 de abril de 2017.

Agradecimientos: Me gustaría agradecer a los profesores Oriol Serra y Juanjo Rué por introducirme al mundo de la combinatoria aditiva, así como por toda la ayuda que me brindaron durante la realización de este trabajo.

Referencia: ESPUNY DÍAZ, Alberto. «Problemas directos e inversos en combinatoria aditiva: las desigualdades de Plünnecke». En: *TEMat*, 1 (2017), págs. 79-89. ISSN: 2530-9633. URL: <http://temat.anemat.com/articulo/2017-p79/>.

© Este trabajo se distribuye bajo una licencia Creative Commons Reconocimiento 4.0 Internacional
<https://creativecommons.org/licenses/by/4.0/>

1. Introducción

La combinatoria aditiva es una rama de las matemáticas que se desarrolló especialmente a partir de mediados del siglo pasado. Aunque algunos resultados aislados se conocían desde tiempo antes, esta teoría tuvo un gran impulso a partir del intento de Schnirelmann de resolver la conjetura de Goldbach. Aunque los resultados dados por esta teoría fueron rápidamente mejorados con otros métodos, quedó un interés por los resultados propios de la teoría que hizo que se convirtiese en un área de investigación muy activa, en la que aún hoy quedan muchos problemas abiertos.

La combinatoria aditiva se puede entender como una parte de la combinatoria aritmética, que se especializa en conocer propiedades de conjuntos contenidos en grupos, con los que se puede operar, y de entender la interacción entre las operaciones. La combinatoria aditiva sería, entonces, aquella parte en la que se consideran solo sumas y restas, y el objetivo sería entender la estructura aditiva de los conjuntos. En esta área se combinan técnicas de teoría de números, análisis armónico, combinatoria, geometría y teoría ergódica para dar lugar a resultados muy diversos. A menudo se puede utilizar como ejemplo para mostrar cómo la interacción de técnicas muy diversas puede dar lugar a resultados cada vez más generales e interesantes. Para un lector más interesado en el tema que quiera conocer todas las ramas de la combinatoria aditiva recomendamos el libro de Tao y Vu [15]; nosotros nos vamos a concentrar en problemas de *conjuntos suma*, para los que las desigualdades de Plünnecke van a resultar esenciales. Para un estudio en mayor profundidad de las desigualdades de Plünnecke recomendamos la monografía de Espuny Díaz [1] o los capítulos de Ruzsa [13]; también se pueden leer las notas de Petridis [7].

Lo primero que necesitamos es explicar qué es un conjunto suma. En general, vamos a tratar con conjuntos finitos en cualquier grupo conmutativo, pero el lector puede pensar en conjuntos de números enteros para tener una primera idea.

Definición 1. Sea $(G, +)$ un grupo abeliano. Sea $A \subseteq G$ un conjunto no vacío cualquiera. El **conjunto suma** de A se define como

$$A + A = \{a + b : a, b \in A\}.$$

Si tenemos un segundo conjunto $B \subseteq G$, el conjunto suma de ambos se define como

$$A + B = \{a + b : a \in A, b \in B\}.$$

Se puede definir el inverso de un conjunto como «el conjunto de los elementos inversos», es decir,

$$-A = \{-a : a \in A\},$$

ya que los elementos inversos existen por ser G un grupo. Eso permite definir también el **conjunto diferencia**

$$A - A = \{a - b : a, b \in A\}.$$

En general, se define el conjunto suma iterado de manera inductiva, como

$$mA = A + (m - 1)A = \{a_1 + a_2 + \dots + a_m : a_i \in A\},$$

para $m \in \mathbb{N}$, y se pueden definir similarmente conjuntos de sumas y restas iteradas para $k, l \in \mathbb{N}$ como

$$kA - lB = \{a_1 + \dots + a_k - b_1 - \dots - b_l : a_i \in A, b_j \in B\}. \quad \blacktriangleleft$$

Nótese que estas definiciones no tienen sentido si uno de los conjuntos es vacío. Por lo tanto, aunque a veces no se indique explícitamente, todos los resultados de este artículo suponen que los conjuntos con que se trabaja tienen al menos un elemento.

La combinatoria aditiva se enfrenta principalmente a dos tipos de problemas: los problemas directos y los inversos. Los primeros son los que primero se plantearía uno: conociendo algo sobre la estructura del conjunto que tengo (y sobre el grupo en el que está, al que llamaremos el grupo ambiente), ¿qué podemos decir sobre la estructura de los conjuntos suma? En particular, ¿qué podemos decir sobre su tamaño? Y los problemas inversos funcionan exactamente al revés: dada cierta información sobre los conjuntos

suma (por ejemplo, su tamaño respecto al conjunto inicial), ¿qué podemos decir sobre la estructura del conjunto?

Una de las condiciones con las que vamos a trabajar es conocer el número de sumas de pares de elementos. Así, por ejemplo, uno de los problemas que nos interesan es, sabiendo cuántas sumas hay en $A + A$, ¿qué podemos decir sobre el número de diferencias? ¿Y sobre el número de triples sumas? Esto nos permitirá obtener información sobre la estructura de los conjuntos.

2. Cotas triviales

Se pueden dar ciertas cotas triviales sobre el tamaño de los conjuntos suma y diferencia que se aplican a cualquier conjunto. Si denotamos el tamaño de un conjunto A como $|A|$, refiriéndonos al número de elementos que tiene, para el conjunto suma básico tenemos las siguientes cotas.

Lema 1. *Sea A un conjunto finito no vacío en un grupo abeliano. Entonces,*

$$|A| \leq |A + A| \leq \binom{|A| + 1}{2}.$$

Demostración. La cota inferior es consecuencia del hecho de que $a + A \subseteq A + A$ para cualquier $a \in A$, y el conjunto $a + A$ es una traslación de A , que se puede entender como una permutación en el grupo ambiente, y por tanto tiene el mismo tamaño que A .

La cota superior es consecuencia de considerar el máximo número posible de sumas. El número de parejas de elementos que se pueden tomar es $\binom{|A|}{2}$ (consideramos parejas sin ordenar, ya que estamos en un grupo conmutativo); además, hay que considerar las parejas de la forma (a, a) , $a \in A$, de las que hay $|A|$ en total. La suma de las dos cantidades da el resultado. ■

Similarmente, se pueden establecer cotas triviales para las diferencias y las sumas iteradas.

Ejercicio 1. Encontrar las cotas triviales para el tamaño del conjunto diferencia $A - A$, donde A es un conjunto finito no vacío en un grupo abeliano. ◀

Ejercicio 2. Dados dos conjuntos finitos no vacíos A y B en un grupo abeliano G , demostrar que $|A + B| \leq |A||B|$. ◀

Ejercicio 3. Encontrar cotas triviales para el tamaño de conjuntos suma iterados nA y $A_1 + A_2 + \dots + A_n$ dados conjuntos finitos no vacíos A, A_1, \dots, A_n en un grupo abeliano. ◀

Nótese que, en general, podemos tener igualdad en las cotas triviales, para lo que basta con construir conjuntos adecuados. Entonces, para que el problema de encontrar cotas resulte interesante, debemos imponer restricciones sobre los conjuntos que consideramos.

3. Problemas directos e inversos

Para ilustrar mejor el tipo de problemas a los que nos enfrentamos, vamos a considerar un ejemplo: trabajamos con conjuntos finitos de números enteros.

Proposición 2. *Si $A \subseteq \mathbb{Z}$ es tal que $|A| = n > 0$, entonces $|A + A| \geq 2n - 1$.*

Demostración. Usando el orden normal de los números enteros, etiquetamos los elementos de A de manera que $A = \{a_1, a_2, \dots, a_n\}$ con $a_1 < a_2 < \dots < a_n$. Usando este orden, resulta evidente que

$$a_1 + a_1 < a_1 + a_2 < a_1 + a_3 < \dots < a_1 + a_n < a_2 + a_n < \dots < a_n + a_n,$$

y está claro que todos estos elementos están en $A + A$. Como en esa lista hay $2n - 1$ términos y todos ellos son diferentes, entonces $|A + A| \geq 2n - 1$. ■

Así, este resultado es un ejemplo en el que usamos la estructura del grupo ambiente (los enteros) para obtener una cota sobre el tamaño de los conjuntos suma que es mejor que la cota trivial. Se trata de una solución a un problema directo.

Proposición 3. Dado $A \subseteq \mathbb{Z}$ con $|A| = n > 0$, $|A + A| = 2n - 1$ si y solo si A es una progresión aritmética.

Demostración. Si A es una progresión aritmética el resultado es trivial, así que vamos a demostrar la otra implicación. Como hemos visto en la demostración de la proposición 2, podemos ordenar los elementos del conjunto suma como

$$a_1 + a_1 < a_1 + a_2 < a_1 + a_3 < a_1 + a_4 < \dots < a_1 + a_n < a_2 + a_n < \dots < a_n + a_n,$$

pero este no es el único orden posible. Por ejemplo, podemos considerar el orden dado por

$$a_1 + a_1 < a_2 + a_1 < a_2 + a_2 < a_2 + a_3 < \dots < a_2 + a_n < a_3 + a_n < \dots < a_n + a_n.$$

También podemos considerar

$$a_1 + a_1 < a_2 + a_1 < a_3 + a_1 < a_4 + a_1 < \dots < a_n + a_1 < a_n + a_2 < \dots < a_n + a_n$$

(en general, podemos pensar que tenemos elementos en un cuadrado de lado n , y hay tantas formas de ordenar de menor a mayor $2n - 1$ sumas como caminos desde la esquina inferior izquierda hasta la esquina opuesta moviéndonos solo hacia arriba o hacia la derecha). Como cada lista tiene $2n - 1$ elementos diferentes, los elementos de cada lista están en $A + A$ y estamos suponiendo que $|A + A| = 2n - 1$, esto quiere decir que todas las listas tienen que ser iguales. Comparando las dos primeras listas que hemos dado, tenemos que $a_1 + a_i = a_2 + a_{i-1}$ para $i \in \{2, 3, \dots, n\}$. Eso quiere decir que $a_i - a_{i-1} = a_2 - a_1$ para todo i , es decir, la diferencia entre cada dos elementos del conjunto es siempre la misma. Y esta es la caracterización de una progresión aritmética. ■

Este es un ejemplo perfecto de un problema inverso. Partiendo de una condición sobre el tamaño de los conjuntos suma, hemos llegado a una propiedad estructural muy fuerte sobre los conjuntos que consideramos. Se pueden obtener otros resultados similares e interesantes en muchos casos.

Ejercicio 4. Sean $A, B \subseteq \mathbb{Z}$ dos conjuntos finitos no vacíos de enteros, con $|A| = n$, $|B| = m$. Demostrar que $|A + B| \geq n + m - 1$, con igualdad si y solo si A y B son progresiones aritméticas con la misma diferencia. ◀

Ejercicio 5. Dado un conjunto no vacío A en un grupo abeliano, demostrar que $|A + A| = |A|$ si y solo si A es una clase lateral de un subgrupo del grupo. ◀

Ejercicio 6 (teorema de Cauchy-Davenport (ver [13, pág. 142])). Sea p un número primo y sean A y B conjuntos no vacíos en $\mathbb{Z}/p\mathbb{Z}$. Demostrar que $|A + B| \geq \min\{p, |A| + |B| - 1\}$. ¿Cuándo se da la igualdad? ◀

En general, la idea que se puede obtener de las proposiciones 2 y 3 y los ejercicios 4, 5 y 6 es que, cuanto más pequeña sea la suma, mayor es la estructura de los conjuntos. El siguiente paso es preguntarse qué ocurre (en el caso de los enteros) si no tenemos igualdad. El siguiente resultado, cuya demostración se puede encontrar en el libro de Nathanson [5], da una primera respuesta a esa pregunta.

Teorema 4 (Freïman). Sea $A \subseteq \mathbb{Z}$ un conjunto finito tal que $|A| \geq 3$ y $|A + A| = 2n - 1 + b \leq 3n - 4$, con n y b enteros. Entonces, A está contenido en una progresión aritmética de longitud $n + b$.

Vemos que se pierde un poco de estructura en el conjunto, pero aún tenemos una condición muy fuerte. Sin embargo, algo así deja de ser cierto si $|A + A| = 3n - 3$: ya se pueden encontrar ejemplos en los que el conjunto no está contenido en una progresión aritmética.

Estos resultados se pueden seguir generalizando. Uno puede definir progresiones d -dimensionales (que quiere decir que se trabaja con d diferencias, no que estemos en un espacio d -dimensional), y entonces se puede demostrar que si el conjunto suma es «pequeño» (es decir, lineal en el tamaño del conjunto original), entonces el conjunto tiene que estar contenido en una progresión aritmética generalizada, con dimensión y tamaño que dependen del factor lineal del conjunto suma (este también es un teorema de Freïman [3, theorem 2]).

Todos los resultados (que no ejercicios) de esta sección se aplican solo al caso particular en que el grupo ambiente es el de los números enteros. Obviamente, también funcionan en algunos otros grupos (en los racionales o los reales tenemos los mismos resultados), pero no funcionan en todos los grupos conmutativos. Sin embargo, sí se pueden generalizar a cualquier grupo abeliano: el resultado más general es el que presentamos a continuación.

Teorema 5 (Green-Ruzsa [4]). *Sea G un grupo abeliano y sea $A \subseteq G$ un conjunto finito tal que $|A + A| \leq \alpha|A|$ para algún $\alpha \in \mathbb{Q}$. Entonces, A está contenido en un conjunto de la forma $H + P$, donde H es un subgrupo de G y P es una progresión aritmética generalizada, tal que la dimensión de P es como máximo d y $|H||P| \leq \alpha'|A|$, donde d y α' son funciones solo de α .*

En este artículo no vamos a demostrar este teorema, pero sí una versión más débil que ya permite dar conclusiones muy interesantes. En cualquier caso, es un buen ejemplo del tipo de resultados inversos que se persiguen en combinatoria aditiva.

4. La desigualdad triangular de Ruzsa

En esta sección presentamos una de las desigualdades que más aplicación tiene para conseguir nuevas desigualdades de tamaños de conjuntos suma, y mostramos algunas de sus aplicaciones. El resultado se puede formular como sigue.

Proposición 6 (desigualdad triangular de Ruzsa [11]). *Sean X, Y y Z tres conjuntos finitos no vacíos en un grupo abeliano. Entonces,*

$$|X||Y - Z| \leq |X - Y||X - Z|.$$

Demostración. Fijemos un elemento $a = y - z \in Y - Z$. Este elemento se puede escribir de $|X|$ formas diferentes como $(x - z) - (x - y)$ (una forma para cada $x \in X$). Pero esto quiere decir que hay por lo menos $|X|$ formas de escribirlo como la diferencia de un elemento de $X - Z$ y un elemento de $X - Y$, de modo que

$$|Y - Z| \leq \frac{|(X - Y) - (X - Z)|}{|X|} \leq \frac{|X - Y||X - Z|}{|X|},$$

donde la última desigualdad es consecuencia de las cotas triviales (ejercicio 2). ■

La desigualdad triangular de Ruzsa se puede utilizar para obtener muchos otros resultados. También se pueden obtener resultados similares. Aquí presentamos algunos de ellos, y dejamos otros como ejercicios.

Corolario 7. *Sean A, B y C tres conjuntos finitos no vacíos en un grupo abeliano. Entonces,*

$$|A||B - C| \leq |A + B||A + C|.$$

Demostración. Basta con aplicar la proposición 6 tomando $X = A, Y = -B$ y $Z = -C$, y tener en cuenta que $|B - C| = |C - B|$ por la conmutatividad del grupo ambiente. ■

Corolario 8. *Sea A un conjunto finito en un grupo abeliano tal que $|A + A| \leq \alpha|A|$. Entonces,*

$$|A - A| \leq \alpha^2|A|.$$

Demostración. Aplicamos la proposición 6 tomando $X = A, Y = Z = -A$. Como $| -A + A| = |A - A|$, tenemos que

$$|A||A - A| \leq |A + A|^2,$$

y el resultado es consecuencia de aplicar la condición del enunciado. ■

Corolario 9. *Sea A un conjunto finito en un grupo abeliano tal que $|3A| \leq \alpha|A|$. Entonces,*

$$|2A - 2A| \leq \alpha^2|A|.$$

Demostración. Aplicamos la proposición 6 tomando $X = A, Y = Z = -2A$. ■

Ejercicio 7. Sea A un conjunto finito en un grupo abeliano tal que $|3A| \leq \alpha|A|$. Demostrar que

$$|4A| \leq \alpha^3|A|. \quad \blacktriangleleft$$

Ejercicio 8. Sea A un conjunto finito en un grupo abeliano tal que $|3A| \leq \alpha|A|$. Demostrar que

$$|nA| \leq \alpha^{2n-5}|A|, \quad |mA - A| \leq \alpha^{2m-2}|A| \quad \text{y} \quad |mA - lA| \leq \alpha^{2(l+m-3)}|A|$$

para todo $n \geq 3$ y $m, l \geq 2$. \blacktriangleleft

En general, observamos que la desigualdad triangular de Ruzsa nos permite obtener muchas desigualdades más generales, y la idea siempre es que si tenemos una cota (lineal, por ejemplo) para el tamaño de un determinado conjunto suma, entonces podemos conseguir cotas (también lineales) con parámetros que son una función (exponencial) de la constante conocida para distintos conjuntos suma.

Esta desigualdad se puede aplicar en casos muy diversos, pero hay algunas cosas que podemos preguntarnos y no puede responder. Por ejemplo, ¿hay un recíproco del corolario 8? Es decir, dada una cota sobre $|A - A|$, ¿podemos obtener cotas sobre $|A + A|$? Esta pregunta no se puede resolver con la desigualdad triangular de Ruzsa. De forma similar, la desigualdad triangular nunca nos permite obtener cotas para sumas de más de dos conjuntos si las cotas que conocemos son solo sobre la suma de dos. Así, aún no podemos responder otra de las preguntas principales de este artículo: dada una cota sobre el tamaño del conjunto suma, ¿qué cota podemos dar sobre el tamaño del conjunto suma de tres conjuntos? Para poder dar solución a estas dudas recurrimos a las desigualdades de Plünnecke.

5. Las desigualdades de Plünnecke

Las desigualdades de Plünnecke permiten dar cotas para la suma iterada de un conjunto una vez se conoce una cota para una suma de menos elementos. Así, si se conoce una cota para el tamaño del conjunto suma de un conjunto, se pueden dar cotas para el conjunto suma iterado tres, cuatro o, en general, k veces. Este resultado fue descubierto por Plünnecke a finales de los años sesenta [8], pero pasó desapercibido hasta que fue redescubierto por Ruzsa a finales de los ochenta [9, 10]. El teorema es en realidad más fuerte que estas cotas, y se puede escribir como sigue.

Teorema 10 (desigualdades de Plünnecke). *Sean A y B conjuntos finitos en un grupo abeliano tales que $|A + B| \leq \alpha|A|$. Entonces, existe un conjunto $X \subseteq A$ tal que para todo $k \geq 1$ se cumple que*

$$|X + kB| \leq \alpha^k|X|.$$

Esto permite obtener cotas para conjuntos suma de manera directa usando cotas triviales.

Corolario 11. *Sea A un conjunto finito en un grupo abeliano tal que $|A + A| \leq \alpha|A|$. Entonces, para todo $k \geq 1$,*

$$|kA| \leq \alpha^k|A|.$$

Demostración. Tomamos $B = A$ en el teorema 10. Así, para cada $k \geq 1$ podemos escribir

$$|kA| \leq |X + kA| \leq \alpha^k|X| \leq \alpha^k|A|,$$

para algún $X \subseteq A$. \blacksquare

La demostración original de las desigualdades de Plünnecke aplica técnicas de teoría de grafos. Plünnecke construyó lo que él llamó *grafos conmutativos*, que crecían de acuerdo a las propiedades conmutativas de los grupos ambiente, y dando cotas sobre el crecimiento en estos grafos logró demostrar su resultado¹. Esta es una demostración larga y laboriosa, para la que se deben tener en cuenta muchos detalles, y para escribirla hacen falta conocimientos básicos de teoría de grafos. Sin embargo, recientemente Petridis presentó una nueva demostración elemental de este resultado [6], que es la que presentamos aquí. Toda su demostración se basa en el siguiente lema.

¹En realidad, el resultado demostrado por Plünnecke, aunque equivalente para casi todas las aplicaciones, es ligeramente diferente al teorema 10, dando un resultado más débil en lo que se refiere al conjunto X para el que las cotas se cumplen pero permitiendo cotas ligeramente mejores si la hipótesis es sobre un conjunto de la forma $A + jB$ para algún $j > 1$.

Lema 12 (Petridis [6, proposition 2.1]). Sean X y B dos conjuntos finitos en un grupo tales que

$$\lambda := \frac{|X+B|}{|X|} \leq \frac{|Z+B|}{|Z|}$$

para todo $Z \subseteq X$. Entonces, para cualquier conjunto C finito en el mismo grupo ambiente,

$$|C+X+B| \leq \lambda|C+X|.$$

Demostración. La demostración la vamos a hacer por inducción sobre el tamaño del conjunto C . Para preparar lo que vamos a necesitar, démosle un orden a los elementos de C (nos vale cualquier orden), $C = \{c_1, c_2, \dots, c_r\}$. Definimos entonces los conjuntos X_1, \dots, X_r como $X_1 := X$ y $X_i := \{x \in X : c_i + x \notin \{c_1, \dots, c_{i-1}\} + X\}$ para todo $2 \leq i \leq r$ (es decir, cada X_i es el conjunto de elementos de X que al sumarles c_i dan lugar a sumas que no habíamos conseguido con los anteriores elementos de C). Esta definición de los conjuntos X_i nos permite escribir $C+X$ como una unión disjunta de conjuntos,

$$C+X = \bigsqcup_{i=1}^r (c_i + X_i).$$

De hecho, para cada subconjunto de C con los primeros j elementos de nuestro orden podemos escribir la misma igualdad como unión disjunta,

$$\{c_1, \dots, c_j\} + X = \bigsqcup_{i=1}^j (c_i + X) = \bigsqcup_{i=1}^j (c_i + X_i),$$

de modo que al considerar cardinales tenemos que

$$(1) \quad |\{c_1, \dots, c_j\} + X| = \sum_{i=1}^j |c_i + X_i| = \sum_{i=1}^j |X_i|.$$

El caso base de la inducción es fácil: cuando C tiene solo un elemento, $C = \{c\}$, tenemos que

$$|C+X+B| = |c+X+B| = |X+B| = \lambda|X| = \lambda|c+X| = \lambda|C+X|,$$

donde la tercera igualdad es consecuencia de la definición de λ . Para demostrar el caso general, supongamos que ya conocemos la desigualdad hasta conjuntos de tamaño $r-1$, y demostrémosla para conjuntos de tamaño r . Para ello, definimos el complemento de X_r en X , $X_r^c = X \setminus X_r$. Por definición de los conjuntos X_i tenemos que $c_r + X_r^c \subseteq \{c_1, \dots, c_{r-1}\} + X$, de modo que $c_r + X_r^c + B \subseteq \{c_1, \dots, c_{r-1}\} + X + B$ y

$$C+X+B \subseteq (\{c_1, \dots, c_{r-1}\} + X + B) \cup ((c_r + X + B) \setminus (c_r + X_r^c + B)).$$

Podemos observar que $(c_r + X + B) \setminus (c_r + X_r^c + B) = c_r + ((X+B) \setminus (X_r^c + B))$, ya que se trata de una traslación de los conjuntos. De este modo, tomando cardinales obtenemos las cotas

$$\begin{aligned} |C+X+B| &\leq |(\{c_1, \dots, c_{r-1}\} + X + B) \cup ((c_r + X + B) \setminus (c_r + X_r^c + B))| \\ &\leq |\{c_1, \dots, c_{r-1}\} + X + B| + |(c_r + X + B) \setminus (c_r + X_r^c + B)| \\ &= |\{c_1, \dots, c_{r-1}\} + X + B| + |X+B| - |X_r^c + B|, \end{aligned}$$

ya que $X_r^c + B \subseteq X + B$. En la última expresión, podemos acotar el término de la izquierda por la hipótesis de inducción, de modo que

$$|\{c_1, \dots, c_{r-1}\} + X + B| \leq \lambda |\{c_1, \dots, c_{r-1}\} + X| = \lambda \sum_{i=1}^{r-1} |X_i|,$$

donde la igualdad viene de la expresión (1). Para acotar el término de la derecha, la hipótesis del enunciado establece que $|X_r^c + B| \geq \lambda |X_r^c|$ y que $|X+B| = \lambda |X|$, de modo que

$$|X+B| - |X_r^c + B| \leq \lambda(|X| - |X_r^c|) = \lambda |X_r|.$$

Juntando ambas expresiones y aplicando (1) otra vez, concluimos que

$$|C + X + B| \leq \lambda \sum_{i=1}^r |X_i| = \lambda |C + X|. \quad \blacksquare$$

Demostración del teorema 10. Sea $X \subseteq A$ un subconjunto que minimice el cociente $\frac{|Z + B|}{|Z|}$, para $Z \subseteq A$, y sea λ el valor de este mínimo. En particular, $\lambda \leq \alpha$. La demostración se hace por inducción sobre k . El caso base vendría dado para $k = 1$, cuando tenemos que $|X + B| = \lambda |X| \leq \alpha |X|$.

Supongamos que el resultado está demostrado para $k - 1$. Entonces tenemos que

$$|X + kB| = |(k - 1)B + X + B| \leq \lambda |(k - 1)B + X| \leq \alpha |(k - 1)B + X| \leq \alpha^k |X|,$$

donde la primera desigualdad es consecuencia del lema 12 y la tercera, de la hipótesis de inducción. \blacksquare

Ahora ya hemos conseguido contestar la pregunta de cómo acotar el número de triples sumas dada una cota sobre el número de dobles sumas (las desigualdades de Plünnecke nos dicen que si $|A + A| \leq \alpha |A|$ entonces $|A + A + A| \leq \alpha^3 |A|$). También tenemos respuesta a la pregunta de cómo acotar $|A + A|$ si lo que conocemos es una cota sobre $|A - A|$: basta con tomar $B = -A$ en el enunciado del teorema 10 y aplicar cotas triviales de la misma forma que en el corolario 11 para obtener que $|2A| = |2B| \leq \alpha^2 |A|$. Más en general, nos podemos preguntar cómo acotar el tamaño de sumas y diferencias iteradas de conjuntos dadas cotas sobre conjuntos suma. Una combinación de algunos resultados previos da respuesta a esta pregunta.

Teorema 13 (desigualdades de Plünnecke-Ruzsa [10]). *Sean A y B dos conjuntos finitos en un grupo abeliano tales que $|A + B| \leq \alpha |A|$. Entonces, para $l, m \geq 1$ enteros cualesquiera,*

$$|lB - mB| \leq \alpha^{l+m} |A|.$$

Demostración. El teorema 10 nos garantiza la existencia de un conjunto $T \subseteq A$ tal que $|T + kB| \leq \alpha^k |T|$, para todo $k \geq 1$. Ahora basta con aplicar la proposición 6 tomando $X = T$, $Y = -mB$ y $Z = -lB$. Entonces,

$$|T||lB - mB| \leq |T + lB||T + mB| \leq \alpha^l |T| \alpha^m |T| \leq \alpha^{l+m} |T||A|.$$

El resultado se obtiene dividiendo por $|T|$. \blacksquare

El nuevo método de Petridis, además de permitir demostrar los teoremas 10 y 13 de manera sencilla, tiene aplicación en otros muchos problemas. Por ejemplo, permite demostrar la siguiente desigualdad, análoga a la desigualdad triangular de Ruzsa pero que no se deduce de esta.

Proposición 14 ([7, lemma 1.7]). *Sean A, B y C tres conjuntos no vacíos en un grupo abeliano. Entonces,*

$$|A||B + C| \leq |A + B||A + C|.$$

Demostración. Sea X el conjunto que minimiza el cociente $\frac{|Z + B|}{|Z|}$ para todo $Z \subseteq A$. Por el lema 12, tenemos que

$$|C + B| \leq |C + X + B| \leq |C + X| \frac{|X + B|}{|X|} \leq |C + A| \frac{|A + B|}{|A|},$$

por definición de X y por las cotas triviales. El enunciado se obtiene multiplicando ambos lados de la desigualdad por $|A|$ y reordenando los términos (ya que el grupo ambiente es conmutativo). \blacksquare

Ejercicio 9. Mejorar las cotas del ejercicio 8 en vista de la proposición 14: si $|3A| \leq \alpha |A|$, entonces

$$|nA| \leq \alpha^{n-2} |A|, \quad |mA - A| \leq \alpha^m |A| \quad \text{y} \quad |mA - lA| \leq \alpha^{l+m-2} |A|$$

para todo $n \geq 3$ y $m, l \geq 2$. \blacktriangleleft

Además de esto, el lema 12 también tiene muchas aplicaciones para el caso en que se consideran conjuntos en grupos no abelianos. El estudio de este caso es más complejo que el del caso conmutativo, pero muchas de las técnicas y resultados expuestos aquí se pueden extender. Además, un lector cuidadoso podrá darse cuenta de que en la demostración del lema 12 no hemos utilizado en ningún momento la conmutatividad del grupo ambiente, lo cual quiere decir que el mismo resultado es cierto en grupos no conmutativos, y utilizando esto se pueden obtener otros resultados en este contexto.

Ejercicio 10. Encontrar las versiones no conmutativas de las proposiciones 6 y 14, así como las cotas del ejercicio 8 (en el caso no abeliano queremos cotas sobre $|\varepsilon_1 A + \varepsilon_2 A + \dots + \varepsilon_n A|$ para $n \geq 3$, con $\varepsilon_i \in \{-1, 1\}$ para todo i). ◀

Las desigualdades de Plünnecke, sin embargo, dejan de ser ciertas en el caso no conmutativo. El motivo de esto es que se pueden construir conjuntos en grupos no abelianos tales que su conjunto suma es «pequeño» (lineal en el tamaño del conjunto), pero cuyo conjunto triple suma es «grande» (cuadrático). Se puede encontrar un ejemplo detallado de este fenómeno en la monografía de Espuny Díaz [1, example 5.2].

De este modo, el estudio de las propiedades de los conjuntos suma se vuelve más complejo y queda fuera de los objetivos de este artículo. Se puede leer una discusión sobre los problemas del caso no conmutativo en el libro de Ruzsa [13]. Para sortear estos problemas, se han buscado otras condiciones que sí permitan establecer cotas del estilo de las desigualdades de Plünnecke. Se pueden encontrar resultados positivos en los artículos de Tao [14], Petridis [6] y Espuny Díaz [2].

6. Aplicación: un problema inverso

Para cerrar este artículo, vamos a demostrar un resultado inverso muy importante. Se trata de un caso particular del teorema 5 que se puede demostrar utilizando las desigualdades de Plünnecke-Ruzsa. Este caso particular no cubre todas las posibilidades que hay en los grupos abelianos, pero sí sirve para ver, de nuevo, el tipo de resultados que se buscan en combinatoria aditiva, y para ver lo útiles que resultan las desigualdades de Plünnecke. Su demostración se debe a Ruzsa [12], quien combinó todas las técnicas anteriores de manera elegante y sencilla.

Teorema 15 (Freiman-Ruzsa). *Sea G un grupo abeliano tal que todos sus elementos tienen orden acotado. Sea r una cota superior para el orden de todos los elementos. Sea $A \subseteq G$ un conjunto finito tal que $|A + A| \leq \alpha|A|$. Entonces, A está contenido en un subgrupo H de G tal que*

$$|H| \leq \alpha^2 r^{\alpha^4} |A|.$$

Demostración. Definimos un conjunto $X \subseteq 2A - A$ que sea maximal sujeto a la condición de que para cada $x \in X$, los conjuntos $x + A$ sean disjuntos; este conjunto existe porque $2A - A$ es finito. Eso quiere decir que podemos escribir

$$X + A = \bigcup_{x \in X} (x + A),$$

siendo la unión disjunta, de modo que $|X + A| = |X||A|$. Por otra parte, ya que $X \subseteq 2A - A$, entonces $X + A \subseteq 3A - A$. Aplicando el teorema 13, tenemos que

$$|X||A| = |X + A| \leq |3A - A| \leq \alpha^4 |A|,$$

de modo que $|X| \leq \alpha^4$.

Sea $t \in 2A - A$ un elemento cualquiera. Por la maximalidad de X , tenemos que $(t + A) \cap (X + A) \neq \emptyset$: de ser esta intersección vacía, habríamos encontrado un elemento t que podríamos añadir a X sin romper la condición, de modo que X no sería maximal y llegaríamos a una contradicción. Esto quiere decir que $t \in X + A - A$. Como podemos hacer lo mismo para cualquier elemento t , tenemos que $2A - A \subseteq X + A - A$. Ahora podemos demostrar por inducción que $jA - A \subseteq (j - 1)X + A - A$. En efecto, tenemos que

$$jA - A = (j - 1)A - A + A \subseteq (j - 2)X + A - A + A = (j - 2)X + 2A - A \subseteq (j - 2)X + X + A - A = (j - 1)X + A - A,$$

donde las inclusiones vienen dadas por la hipótesis de inducción y el caso base, respectivamente.

Sea H el subgrupo de G generado por A , y sea I el subgrupo generado por X . Dado que el orden de todos los elementos de G está acotado, tenemos que $H = \bigcup_{j \geq 2} (jA - A)$, ya que $H = \bigcup_{j \geq 1} (jA)$, y sumar y restar A no puede hacer que nos salgamos del subgrupo. También podemos escribir $I = \bigcup_{j \geq 1} (jX)$. Así, teniendo en cuenta el resultado que acabamos de demostrar por inducción,

$$H = \bigcup_{j \geq 2} (jA - A) \subseteq \bigcup_{j \geq 2} ((j-1)X + A - A) = \bigcup_{j \geq 1} (jX) + A - A = I + A - A.$$

Así, basta con acotar el tamaño de $I + A - A$ para obtener una cota para el tamaño del subgrupo H en el que A está contenido. Podemos acotar $|I|$ considerando que cualquier elemento g de I se tiene que poder escribir como $n_1 x_1 + n_2 x_2 + \dots + n_{|X|} x_{|X|}$, donde x_i son los elementos de X escritos en un orden arbitrario y $0 \leq n_i < r$. El tamaño de I es como mucho el número de estas expresiones, que es $r^{|X|}$. Finalmente, usamos la cota que hemos obtenido para el tamaño de X , una de las desigualdades triviales (ejercicio 2) y el corolario 8 (que también se puede obtener usando el teorema 13) para obtener la cota

$$|H| \leq |I + A - A| \leq |I||A - A| \leq \alpha^2 r^{\alpha^4} |A|. \quad \blacksquare$$

Nota. Se pueden encontrar soluciones a los ejercicios 4, 5 y 8 (y, por tanto, al ejercicio 7), así como a la primera parte del ejercicio 10, en la monografía de Espuny Díaz [1, proposition 1.2, proposition 1.1, corollary 4.7, theorem 5.18 y lemma 6.6, respectivamente], algunas de ellas escritas de manera más general que en este artículo pero pudiéndose obtener estas de manera inmediata. La solución del ejercicio 9 sigue las mismas líneas que la del ejercicio 8. Finalmente, la solución de la segunda parte del ejercicio 10 se puede encontrar en un artículo de Espuny Díaz [2], en la demostración del teorema 1.7; también sigue las líneas del ejercicio 8. ◀

Referencias

- [1] ESPUNY DÍAZ, Alberto. *Classical and modern approaches for Plünnecke-type inequalities*. Trabajo Final de Grado. Universitat Politècnica de Catalunya, 2015. URL: <http://hdl.handle.net/2117/77022>.
- [2] ESPUNY DÍAZ, Alberto. «Explicit bounds for growth of sets in non-abelian groups». En: *Reports@SCM* 3.1 (2017). Preprint, págs. 17-26. ISSN: 2385-4227. URL: <http://revistes.iec.cat/index.php/reports/article/view/142624>.
- [3] FREĪMAN, Gregory A. *Foundations of a structural theory of set addition*. Traducido del ruso, Translations of Mathematical Monographs, Vol 37. American Mathematical Society, Providence, R. I., 1973, págs. vii+108.
- [4] GREEN, Ben y RUZSA, Imre Z. «FreĪman's theorem in an arbitrary abelian group». En: *J. Lond. Math. Soc. (2)* 75.1 (2007), págs. 163-175. ISSN: 0024-6107. <https://doi.org/10.1112/jlms/jdl021>.
- [5] NATHANSON, Melvyn B. *Additive number theory*. Vol. 165. Graduate Texts in Mathematics. Inverse problems and the geometry of sumsets. Springer-Verlag, New York, 1996, págs. xiv+293. ISBN: 0-387-94655-1. <https://doi.org/10.1007/978-1-4757-3845-2>.
- [6] PETRIDIS, Giorgis. «New proofs of Plünnecke-type estimates for product sets in groups». En: *Combinatorica* 32.6 (2012), págs. 721-733. ISSN: 0209-9683. <https://doi.org/10.1007/s00493-012-2818-5>.
- [7] PETRIDIS, Giorgis. *Introduction to the Theory of Set Addition*. Notas para el Block Course Towards the Polynomial Freiman-Ruzsa Conjecture. Oct. de 2014. URL: https://mat-web.upc.edu/people/juan.jose.rue/BlockCourse-FUBerlin-Week1/Berlin_notes.pdf.
- [8] PLÜNNECKE, Helmut. «Eine zahlentheoretische Anwendung der Graphentheorie». En: *J. Reine Angew. Math.* 243 (1970), págs. 171-183. ISSN: 0075-4102.
- [9] RUZSA, Imre Z. «Addendum to: An application of graph theory to additive number theory». En: *Sci. Ser. A Math. Sci. (N.S.)* 4 (1990/1991), págs. 93-94.

-
- [10] RUZSA, Imre Z. «An application of graph theory to additive number theory». En: *Sci. Ser. A Math. Sci. (N.S.)* 3 (1989), págs. 97-109. ISSN: 0716-8446.
- [11] RUZSA, Imre Z. «Sums of finite sets». En: *Number theory (New York, 1991–1995)*. Springer, New York, 1996, págs. 281-293. https://doi.org/10.1007/978-1-4612-2418-1_21.
- [12] RUZSA, Imre Z. «An analog of Freiman's theorem in groups». En: *Astérisque* 258 (1999). Structure theory of set addition, págs. xv, 323-326. ISSN: 0303-1179.
- [13] RUZSA, Imre Z. «Sumsets and structure». En: *Combinatorial number theory and additive group theory*. Adv. Courses Math. CRM Barcelona. Birkhäuser Verlag, Basel, 2009, págs. 87-210. <https://doi.org/10.1007/978-3-7643-8962-8>.
- [14] TAO, Terence. «Product set estimates for non-commutative groups». En: *Combinatorica* 28.5 (2008), págs. 547-594. ISSN: 0209-9683. <https://doi.org/10.1007/s00493-008-2271-7>.
- [15] TAO, Terence y VU, Van H. *Additive combinatorics*. Vol. 105. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 2006, págs. xviii+512. ISBN: 978-0-521-85386-6; 0-521-85386-9. <https://doi.org/10.1017/CB09780511755149>.