Miscelánea Matemática **59** (2014) 1-17 SMM

Una nueva mirada a cuatro teoremas clásicos en teoría aditiva de números

Amanda Montejano
Facultad de Ciencias UMDI–Juriquilla
Universidad Nacional Autónoma de México
Querétaro, México.
amandamontejano@ciencias.unam.mx

Resumen

Dado un grupo abeliano G y dos subconjuntos finitos $A, B \subseteq G$, llamaremos a la pareja (A, B) *crítica* si su conjunto suma, $A + B = \{a + b : a \in A, b \in B\}$, satisface $|A + B| < |A| + |B|$. El teorema de Kemperman es un importante resultado dentro de la teoría aditiva de números, que caracteriza la estructura de las parejas críticas en grupos abelianos. Recientemente, en [1], se ha propuesto una reformulación al teorema de Kemperman que simplifica tanto su enunciado como su prueba. El objetivo de este artículo es, por un lado presentar las ideas propuestas en [1] así como la reformulación del teorema de Kemperman, y por otro, usar estas nuevas ideas para reformular a su vez los teoremas de Cauchy-Davenport, Vosper, y Kneser, con el fin de proporcionar al lector una manera original de estudiar estos teoremas clásicos en teoría aditiva de números.

1. Introducción

Dentro de la teoría de números, la teoría aditiva es la rama que se ocupa de estudiar la estructura o características del «conjunto suma» de dos o más conjuntos de números. Pero ¿qué significa sumar dos conjuntos de números? Como sucede con la mayoría de las buenas definiciones en matemáticas, la respuesta a esta pregunta resulta ser la más natural.

Consideremos un grupo aditivo abeliano G, y dos subconjuntos finitos A, B, (no necesariamente disjuntos) de G. El *conjunto suma* de A y B, denotado por $A+B$, se define como el conjunto de elementos en G que se pueden expresar como la suma de un elemento en A y un elemento en B, es decir:

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

Un *problema directo* en la teoría aditiva de números, es aquel que se propone estudiar características del conjunto suma $A+B$ teniendo información de los conjuntos A y B; mientras que un *problema inverso* en el área, es aquel que trata de inferir información de los conjuntos A y B a partir de cierto conocimiento del conjunto suma $A+B$.

En este artículo estudiaremos problemas directos e inversos referentes a la cardinalidad del conjunto suma $A+B$ en relación con las cardinalidades de los conjuntos sumandos A y B, así como con la propia estructura de tales conjuntos. Presentaremos cuatro bellos teoremas: Cauchy-Davenport y Vosper, cuyos enunciados se restringen a grupos de orden primo; y sus análogos (sus respectivas, profundas y complejas extensiones) Kneser y Kemperman, enunciados en grupos abelianos arbitrarios.

Partamos de la siguiente pregunta ¿dados A y B dos subconjuntos finitos de un grupo abeliano G, qué tan pequeño puede ser el conjunto suma $A+B$? Ciertamente, si G es un grupo libre de torsión, es decir, si todos sus elementos tienen orden infinito —pensemos por ejemplo en $\mathbb{Z}$— tendremos que para cualquier elección de A y B se cumple $|A+B| \geq |A|+|B|-1$. En 1813 el famoso matemático francés Augustin Louis Cauchy probó que tal aseveración permanece verdadera cuando G es un grupo cíclico de orden primo, siempre y cuando no suceda que $A+B=G$, [2]. Dicho resultado fue redescubierto por Davenport en 1935 y actualmente se conoce como el teorema de Cauchy-Davenport [3, 4, 14]. En la sección 3 daremos una prueba de este clásico teorema en la teoría aditiva de números.

El teorema de Kneser [10], publicado en 1953, es una profunda generalización al teorema de Cauchy-Davenport para grupos abelianos arbitrarios. Existen distintas maneras de enunciarlo y tanto sus corolarios más directos como sus aplicaciones más complejas resultan ser de gran inspiración en el área. En la sección 5 abundaremos al respecto presentando diversas vistas al teorema de Kneser, así como algunas de sus más simples —no por eso menos útiles— consecuencias.

Los teoremas de Cauchy-Davenport y Kneser ejemplifican resultados directos en la teoría aditiva de números. Sus respectivas contrapartes —en el sentido del resultado inverso— son los teoremas de Vosper y Kemperman. A grandes rasgos, dichos teoremas describen (cada uno en su contexto, uno en grupos de orden primo, y el otro en grupos abelianos arbitrarios) la estructura de aquellos subconjuntos finitos A y B para los cuales el conjunto suma $A+B$ es «pequeño».

Consideramos que un conjunto suma $A + B$ es un *conjunto suma pequeño* si se verifica que $|A + B| < |A| + |B|$. Una pareja (A, B) tal que su conjunto suma es pequeño se llama una *pareja crítica*. El problema inverso clásico en la teoría aditiva de números es entender —o mejor aún caracterizar— la estructura de aquellas parejas críticas. En 1956 Vosper resuelve por completo este problema para grupos de orden primo [13]. En 1960 Kemperman, complementando los trabajos de Kneser, hace lo propio para parejas críticas en grupos abelianos arbitrarios [9]. Estudiaremos ambos teoremas en las secciones 4 y 6 respectivamente.

El teorema de Kemperman, aún publicado cuatro escasos años después que el teorema de Vosper, permaneció largo tiempo sin recibir la atención y el reconocimiento que merecía. Esto sucedió principalmente por dos razones. La primera: que la estructura de las parejas críticas en grupos abelianos arbitrarios es ciertamente compleja. La segunda: que el artículo original de Kemperman resulta algo confuso y difícil de leer. De hecho, podemos advertir que años después de haber sido publicado y leído el trabajo de Kemperman, el problema de clasificar la estructura de las parejas críticas en grupos abelianos arbitrarios seguía considerándose —al menos en algún sector— un problema abierto. Tal aseveración se puede constatar en la página 130 (sección 4.5) del libro *Additive number theory: inverse problems and the geometry of sumsets*, de Melvyn B. Nathanson [12]. Excelente libro editado en 1991, que además ¡cita el trabajo de Kemperman!.

Con el paso de los años, en definitiva, dicha situación fue solventada. No podemos dejar de mencionar los trabajos de Lev [11], Hamidoune [8, 7] y Grynkiewicz [5, 6], que contribuyeron enormemente a resolver tal tesitura. Recientemente, en [1], los autores proponen una nueva versión del teorema de Kemperman, cuya descripción estructural se expone en términos de ternas (en vez de parejas) críticas, facilitando considerablemente tanto el enunciado como la prueba del teorema. En el presente trabajo exponemos esta nueva mirada al teorema de Kemperman, y tras presentar las herramientas necesarias aprovechamos para mirar y repasar también, bajo la luz que nos proporciona esta nueva lente, los teoremas de Cauchy-Davenport, Vosper y Kneser.

2. Deficiencia y tríos

Tal como se expresa en el título de este artículo, es nuestra meta presentar una nueva mirada a cuatro clásicos teoremas en teoría aditiva de números. En esta sección introducimos las nociones básicas que nos permitirán alcanzar nuestro objetivo.

Como es habitual, dado $A \subseteq G$, usamos $-A$ para denotar al conjunto $\{-a : a \in A\}$, así como $A + g$ para referirnos al conjunto $A + \{g\}$, que llamaremos una *translación* de A. Notemos que $|A| = |-A| = |A + g|$ para todo $A \subseteq G$ y $g \in G$. A continuación presentamos la definición de deficiencia, usada en [1].

Definición 2.1. Dados dos subconjuntos finitos no vacíos A y B de un grupo abeliano G, definimos la *deficiencia* de la pareja (A, B) como $\delta(A, B) = |A| + |B| - |A + B|$.

Observemos que una pareja (A, B) es crítica (es decir, su conjunto suma es pequeño) si su deficiencia $\delta(A, B)$ es un número positivo. De esta manera, entendemos que una pareja es tanto más crítica como más grande es su deficiencia.

Como hemos dicho antes, nos interesa entender y caracterizar la estructura de las parejas críticas. Comenzaremos por descartar un tipo trivial de parejas críticas. Observemos que si $A, B \subseteq G$ satisfacen $|A|+|B| > |G|$, entonces $A+B = G$, ya que para todo $g \in G$ se cumple $(g - A) \cap B \neq \emptyset$. Entonces, las parejas (A, B) tales que $|A| + |B| > |G|$ son trivialmente críticas. Así, llamaremos a una pareja (A, B) *trivial* si, o bien $|B|+|A| > |G|$, o bien alguno de los conjuntos es vacío. Diremos que una pareja es *no trivial* en caso contrario, y nos restringiremos a clasificar la estructura de las parejas críticas no triviales.

A lo largo de los años, el estudio de parejas críticas y su estructura en distintos contextos, ha llevado a diversos autores a reconocer la utilidad de un tercer conjunto $C \subseteq G$ asociado a la pareja (A, B), definido naturalmente como $C = G \setminus -(A + B)$. Este tercer conjunto posee propiedades muy interesantes que estudiaremos en esta sección. Supongamos por un momento que G es un grupo abeliano finito, no es difícil argumentar que si (A, B) es una pareja crítica no trivial en G y C se define como $C = G \setminus -(A + B)$, entonces todas las parejas de conjuntos en la terna $\{A, B, C\}$ son críticas no triviales (ver proposición 2.7). Esta observación (en apariencia inocente) nos sugiere el estudio de ciertas ternas de conjuntos a las cuales llamaremos tríos y definimos a continuación.

Consideremos un grupo abeliano G. Admitiremos que G sea de orden infinito, en cuyo caso pediremos que los conjuntos a estudiar, A, B y C, sean finitos o *cofinitos* (es decir, de complemento finito).

Definición 2.2. Sean A, B y C subconjuntos finitos o cofinitos de un grupo abeliano G. Decimos que (A, B, C) es un *trío* si se satisface que

$$0 \notin A + B + C.$$

Le llamamos a un trío (A, B, C) *no trivial* si ninguno de sus conjuntos es vacío.

Antes de continuar enfaticemos el hecho de que, por definición, en una pareja crítica no trivial (A, B) ambos conjuntos son finitos. En contraste, un trío admite conjuntos cofinitos. Sin embargo, es fundamental notar que de la propia definición de trío, se infiere que sólo uno de los tres conjuntos puede ser infinito. Este hecho es consecuencia inmediata de la siguiente útil observación.

Observación 2.3. Sea (A, B, C) un trío en G. Para todo $X \in \{A, B, C\}$, donde $\{Y, Z\} = \{A, B, C\} \setminus \{X\}$, se cumple $X \subseteq G \setminus -(Y + Z)$, equivalentemente $(Y + Z) \subseteq G \setminus -X$.

Ahora podemos definir de manera consistente la deficiencia para un trío, y a continuación la noción de criticidad. Posteriormente podremos extender la noción de pareja crítica a parejas en las cuales se permita que alguno de los conjuntos sea cofinito.

Definición 2.4. Sea (A, B, C) un trío no trivial en G. Definimos la *deficiencia* de (A, B, C) como

$$\delta(A, B, C) = |X| + |Y| - |G \setminus Z|$$

donde $\{A, B, C\} = \{X, Y, Z\}$ con $|X| \leq |Y| \leq |Z|$. Decimos que un trío (A, B, C) es *crítico* si se cumple

$$\delta(A, B, C) > 0.$$

Antes de continuar observemos que, en el caso en que G es un grupo abeliano finito, la deficiencia de un trío (A, B, C) resulta:

$$\delta(A, B, C) = |A| + |B| + |C| - |G|,$$

y el trío resulta crítico si $|A| + |B| + |C| > |G|$.

Definición 2.5. Sean $A, B \subseteq G$ dos subconjuntos no vacíos, uno de ellos finito, y el otro finito o cofinito. Definimos la *deficiencia* de la pareja (A, B) como $\delta(A, B) = \delta(A, B, C)$, donde $C = G \setminus -(A + B)$. Diremos que la pareja (A, B) es *crítica* si $\delta(A, B) > 0$.

Es importante notar que para una pareja (A, B) de subconjuntos finitos no vacíos la definición 2.5 coincide con la definición 2.1. Además, de la observación 2.3 se infiere que para todo trío se satisface que la deficiencia de cada pareja es mayor o igual a la deficiencia del trío. Justificar la siguiente observación es un buen ejercicio para que el lector repase las definiciones dadas en esta sección.

Observación 2.6. Sea (A, B, C) un trío en G, entonces

$$\delta(A, B, C) \leq \text{mín}\{\delta(A, B), \delta(B, C), \delta(C, A)\}.$$

La siguiente proposisión justifica la noción de trío crítico no trivial presentada como extensión del concepto de pareja crítica no trivial.

Proposición 2.7. *Toda pareja crítica no trivial (A, B) de subconjuntos finitos de G, se puede extender a un trío crítico no trivial (A, B, C). Mas aún, todo trío crítico no trivial (A, B, C) de G, satisface que (A, B), (B, C) y (C, A) son parejas críticas no triviales de G.*

Demostración. Dada (A, B) una pareja crítica no trivial definimos $C = G \setminus -(A + B)$. Resulta inmediato observar que $0 \notin A + B + C$, luego (A, B, C) es un trío. Siendo (A, B) no trivial tenemos que $A \neq \emptyset$, $B \neq \emptyset$, y $A+B \neq G$, por lo tanto $C \neq \emptyset$. El trío es crítico ya que, por definición, $\delta(A, B) = \delta(A, B, C)$.

Ahora consideremos (A, B, C) un trío crítico no trivial. Verificar que las tres parejas son no triviales es inmediato con el uso de la observación 2.3. El hecho de que cada pareja es crítica, se sigue de la observación 2.6. □

De la proposición 2.7 concluimos que para clasificar la estructura de las parejas críticas no triviales, es suficiente estudiar y clasificar la estructura de los tríos críticos no triviales.

3. Cauchy-Davenport

En lo sucesivo p denota un número primo y $\mathbb{Z}/p\mathbb{Z}$ es el grupo cíclico de orden p. El clásico teorema de Cauchy-Davenport nos proporciona una cota inferior natural para la cardinalidad de un conjunto suma en $\mathbb{Z}/p\mathbb{Z}$. Excelentes referencias con respecto a este teorema son [4, 14].

Teorema 3.1 (Cauchy-Davenport)**.** *Sean $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$ conjuntos no vacíos, entonces*

$$|A + B| \geq \text{mín}\{p, |A| + |B| - 1\}.$$

En otras palabras el teorema 3.1 nos dice que en grupos abelianos de orden primo, excepto cuando $A + B = G$, toda pareja de subconjuntos (A, B) satisface $\delta(A, B) \leq 1$. Es decir, las únicas parejas críticas no triviales que existen en estos grupos son aquellas con deficiencia uno, la menor deficiencia posible para una pareja crítica. A continuación, usando los conceptos de trío y deficiencia, proponemos una nueva versión del teorema de Cauchy-Davenport, cuya demostración también presentamos en el contexto de los tríos. No es difícil probar la equivalencia entre la versión clásica y la versión tríos del teorema de Cauchy-Davenport.

Teorema 3.2 (Cauchy-Davenport, versión tríos)**.** *Sea (A, B, C) un trío crítico no trivial en $\mathbb{Z}/p\mathbb{Z}$, entonces $\delta(A, B, C) = 1$.*

Demostración. Procederemos por inducción sobre $|A|$, suponiendo sin pérdida de generalidad que $|A| \leq |B| \leq |C|$. Si $|A| = 1$, dado que el trío es crítico, sabemos que $|B| + |C| > p - 1$. Por otro lado, de la observación 2.3 obtenemos $|C| \leq p - |A + B| = p - |B|$, de donde se infiere que $|B|+|C| = p$, y por lo tanto $\delta(A, B, C) = |A|+|B|+|C|-p = 1$.

Supongamos ahora que $|A| \geq 2$. En primer lugar notemos que para cualesquiera $g_1, g_2 \in \mathbb{Z}/p\mathbb{Z}$, la terna $(A + g_1, B + g_2, C - g_1 - g_2)$ es un trío con deficiencia $\delta(A + g_1, B + g_2, C - g_1 - g_2) = \delta(A, B, C)$. Supongamos entonces, sin pérdida de generalidad, que para $a \neq 0$, $\{0, a\} \subseteq A$, $0 \in B$ y $a \notin B$ (esto se puede lograr ya que $B \neq \mathbb{Z}/p\mathbb{Z}$, y $\mathbb{Z}/p\mathbb{Z}$ no tiene subgrupos propios no triviales). Consideremos ahora los conjuntos $(A \cap B)$ y $(A \cup B)$. Notemos que $\emptyset \neq (A \cap B) \subset A$, y que $(A \cap B, A \cup B, C)$ es un trío. Entonces, por hipótesis de inducción $\delta(A \cap B, A \cup B, C) = 1$, lo cual concluye la prueba ya que es inmediato notar que $\delta(A \cap B, A \cup B, C) = \delta(A, B, C)$. $\square$

En otras palabras, el teorema 3.2 nos dice que todo trío (A, B, C) crítico no trivial en $\mathbb{Z}/p\mathbb{Z}$ satisface $|A| + |B| + |C| = p + 1$.

4. Vosper

Como se ha dicho anteriormente, el problema inverso clásico en la teoría aditiva de números es el de clasificar la estructura de las parejas críticas no triviales. Este problema fue resuelto por completo para grupos de orden primo en 1956 por Vosper.

Exploremos primero algunos ejemplos naturales de parejas críticas no triviales. Sean $A, B \subseteq G$ conjuntos no vacíos tales que $A + B \neq G$. La primera condición que nos viene a la mente para satisfacer que (A, B) sea una pareja crítica es que alguno de los dos conjuntos, digamos A, tenga cardinalidad uno. Así, el conjunto suma $A+B$ es en realidad una translación de B, y por tanto $|A + B| = |B| = |B| + |A| - 1$.

Otra condición, quizás un poco menos directa, que se nos puede ocurrir para satisfacer que el conjunto $A + B$ sea pequeño, es que ambos conjuntos A y B sean progresiones aritméticas con la misma diferencia. Recordemos que un subconjunto $A \subseteq G$ es una *progresión aritmética* si es de la forma $A = \{a+id : 0 \leq i \leq t-1\}$; en tal caso decimos que A es una progresión aritmética con t términos, $|A| = t$, y *diferencia* d. Consideremos dos progresiones aritméticas $A, B \subseteq G$ con la misma diferencia d. Sean $A = \{a + id : 0 \leq i \leq t_1 - 1\}$ y $B = \{b + id : 0 \leq i \leq t_2 - 1\}$, entonces $A + B = \{(a + b) + id : 0 \leq i \leq t_1 + t_2 - 2\}$ es otra progresión aritmética de diferencia d con $(t_1 + t_2 - 1)$ términos, y por lo tanto $|A + B| = |A| + |B| - 1$.

Lo que nos dice el teorema de Vosper es que, en esencia, estas son las únicas formas de conseguir que el conjunto suma sea pequeño en un grupo abeliano de orden primo. A continuación presentamos el teorema de Vosper tal como se encuentra redactado en [12].

Teorema 4.1 (Vosper)**.** *Sea p un número primo, y sean A, B, dos subconjuntos no vacíos del grupo $G = \mathbb{Z}/p\mathbb{Z}$ tales que $A + B \neq G$. Entonces, $|A + B| = |A| + |B| - 1$ si y sólo si al menos una de las siguientes condiciones se satisface:*

(i) $\min\{|A|, |B|\} = 1$,
(ii) $|A + B| = p - 1$ *y* $B = G \setminus (c - A)$ *donde* $\{c\} = G \setminus (A + B)$,
(iii) *A y B son progresiones aritméticas con la misma diferencia.*

Como se explicó en la sección 2, para clasificar la estructura de las parejas críticas no triviales es suficiente clasificar la estructura de los tríos críticos no triviales. En este sentido, podemos reformular el teorema de Vosper de la siguiente manera.

Teorema 4.2 (Vosper, versión tríos)**.** *Si (A, B, C) es un trío crítico no trivial en $\mathbb{Z}_p$ entonces alguna de las siguientes condiciones se satisface:*

(i) $\min\{|A|, |B|, |C|\} = 1$,
(ii) *A, B y C son progresiones aritméticas con la misma diferencia.*

A continuación probaremos la equivalencia entre ambas versiones del teorema de Vosper. Antes de continuar, sin embargo, observemos que en su versión clásica (teorema 4.1) el teorema de Vosper es un «si y sólo si» mientras que en su versión tríos (teorema 4.2) dicho teorema establece sólo una implicación (la «ida») y de hecho el «regreso» no es verdad. Es importante remarcar que la fuerza del teorema original de Vosper lo comprende precisamente la «ida». Por este motivo, para probar la equivalencia, nos enfocaremos en analizar únicamente tal implicación.

Proposición 4.3. *Los teoremas 4.1 y 4.2 son equivalentes.*

Demostración. En primer lugar asumamos la veracidad del teorema 4.1 y demostremos el teorema 4.2. Sea (A, B, C) un trío crítico no trivial en $\mathbb{Z}/p\mathbb{Z}$. Luego A y B son dos subconjuntos no vacíos de $G = \mathbb{Z}/p\mathbb{Z}$ tales que $A+B \neq G$ (pues de la observación 2.3 se sigue que $A+B \subseteq G\setminus -C$ y por hipótesis $C \neq \emptyset$). El hecho de que (A, B, C) sea un trío crítico nos indica que $\delta(A, B, C) = 1$. Entonces, por la observación 2.6, $\delta(A, B) \geq 1$, de lo cual obtenemos (por el teorema de Cauchy-Davenport) que $|A+B| = |A|+|B|-1$. Una vez obtenidas las hipótesis del teorema 4.1, sabemos que alguna de las tres condiciones descritas en él se satisface:

- si se cumple (i), entonces $\min\{|A|, |B|, |C|\} = 1$.
- si se cumple (ii), usando nuevamente la observación 2.3, se sigue que $|C| = \min\{|A|, |B|, |C|\} = 1$.

- si se cumple (iii), entonces C también es una progresión aritmética con la misma diferencia que las progresiones A y B, pues del hecho de que (A, B, C) sea un trío crítico se infiere que $C = G \setminus -(A+B)$.

Ahora, demostremos el teorema 4.1 asumiendo la veracidad del teorema 4.2. Sean A y B dos subconjuntos no vacíos de $G = \mathbb{Z}/p\mathbb{Z}$ tales que $A + B \neq G$. Definamos $C := G \setminus -(A + B)$, obteniendo así un trío no trivial (A, B, C) tal que $\delta(A, B, C) = \delta(A, B)$. Notemos que si la pareja (A, B) satisface $|A + B| = |A| + |B| - 1$, entonces $\delta(A, B) = 1$, por lo que (A, B, C) es un trío crítico. Una vez obtenidas las hipótesis del teorema 4.2, sabemos que alguna de las dos condiciones descritas en él se satisface:

- si se cumple (i), entonces, o bien $\min\{|A|, |B|\} = 1$ o bien $|C| = 1$, en cuyo caso $|A + B| = p - 1$, luego $A + B = G \setminus \{c\}$ para algún $c \in G$, de donde $B = G \setminus (c - A)$.
- si se cumple (ii), en particular A y B son progresiones aritméticas con la misma diferencia. $\square$

La demostración del teorema de Vosper requiere un poco más de esfuerzo y no la incluimos en este trabajo.

5. Kneser

Recordemos que una pareja (A, B) se dice crítica si su deficiencia $\delta(A, B)$ es positiva, y esto quiere decir que su conjunto suma es pequeño: $|A+B| < |A|+|B|$. Como vimos en la sección 3, el teorema de Cauchy-Davenport afirma que todas las parejas críticas no triviales (A, B) en $\mathbb{Z}_p$ tienen deficiencia $\delta(A, B) = 1$, es decir, cumplen $|A+B| = |A|+|B|-1$. Para grupos abelianos arbitrarios no podemos tener esperanza de que algo así siempre suceda (consideremos por ejemplo H, un subgrupo no trivial de G, y $A = B = H$, entonces $A + B = H$). No obstante, el teorema de Kneser nos dice que si bien no toda pareja crítica (A, B) tiene deficiencia uno, es verdad que para toda pareja crítica no trivial (A, B) de G existe un subgrupo H de G tal que en el cociente G/H las imágenes naturales de A y B forman una pareja crítica con deficiencia uno. En esta sección presentaremos las dos formulaciones más clásicas del teorema de Kneser así como la versión tríos presentada en [1].

5.1 Versiones clásicas

Para enunciar de manera precisa el teorema de Kneser es necesario introducir la importante noción de estabilizador o periodo de un subconjunto en un grupo. Sea A un subconjunto no vacío de un grupo abeliano G, el *estabilizador* de A, denotado por G_A, es el conjunto definido por $G_A = \{g \in G : g + A = A\}$. Con respecto al estabilizador de un subconjunto cualquiera $A \subseteq G$ debemos notar las siguientes características:

(a) G_A es un subgrupo de G;
(b) el conjunto A es unión de clases laterales de G_A;
(c) G_A es el máximo subgrupo de G que satisface la propiedad (2).

Teorema 5.1 (Kneser, versión 1)**.** *Sean A y B dos subconjuntos finitos no vacíos de un grupo abeliano G, y sea $H = G_{A+B}$, entonces*

$$|A + B| \geq |A + H| + |B + H| - |H|. \tag{1}$$

Para entender y analizar lo que nos dice el teorema de Kneser, debemos introducir un poco más de notación. Como es usual, dado un subgrupo $H < G$, denotamos por G/H al grupo cociente. Usaremos $\varphi_{G/H} : G \to G/H$ para referirnos al homomorfismo canónico, así como $\tilde{A} = \varphi_{G/H}(A)$ y $\tilde{B} = \varphi_{G/H}(B)$ para referirnos a las imágenes correspondientes en el cociente de nuestros conjuntos A y B.

Observemos que la conclusión del teorema de Kneser, desigualdad (1), nos remite a la cota inferior natural (Cauchy-Davenport) para el conjunto suma de una pareja de conjuntos (A, B), siempre que $G_{A+B} = \{0\}$ o $G_{A+B} = G$. Más aún, notemos que por definición se satisfacen las siguientes igualdades:

(i) $|A + B| = |\tilde{A} + \tilde{B}||H|$.
(ii) $|A + H| = |\tilde{A}||H|$ y $|B + H| = |\tilde{B}||H|$.

Usando (i) y (ii) deducimos que la desigualdad en (1) se puede expresar de la siguiente manera, adquiriendo la apariencia de Cauchy-Davenport en el cociente:

$$|\tilde{A} + \tilde{B}| \geq |\tilde{A}| + |\tilde{B}| - 1. \tag{2}$$

No resulta difícil argumentar que una pareja crítica no trivial (A, B) en G induce una pareja crítica no trivial $(\tilde{A}, \tilde{B})$ en G/H. De hecho, en ocasiones, el teorema de Kneser se encuentra enunciado de la siguiente manera.

Teorema 5.2 (Kneser, versión 2)**.** *Sea (A, B) una pareja crítica no trivial de subconjuntos en G, y sea $H = G_{A+B}$, entonces*

$$|A + B| = |A + H| + |B + H| - |H|. \tag{3}$$

A continuación, a modo de ejercicio, probaremos la equivalencia de ambas versiones del teorema de Kneser.

Proposición 5.3. *Los teoremas 5.1 y 5.2 son equivalentes.*

Demostración. En primer lugar asumamos la veracidad del teorema 5.1 y demostremos el teorema 5.2. Sea (A, B) una pareja crítica no trivial en G. Concatenando (1) y el hecho de que (A,B) es crítica obtenemos:

$$|A+H|+|B+H|-|H| \leq |A+B| < |A|+|B| \leq |A+H|+|B+H|,$$

de donde se infiere, usando las identidades (i) y (ii), y dividiendo por $|H|$, que: $|\tilde{A}|+|\tilde{B}|-1 \leq |\tilde{A}+\tilde{B}| < |\tilde{A}|+|\tilde{B}|$, es decir, $|\tilde{A}+\tilde{B}| = |\tilde{A}|+|\tilde{B}|-1$, que al volver a multiplicar por $|H|$, resulta ser (3).

Ahora, demostremos el teorema 5.1 asumiendo el teorema 5.2. Sean A y B dos subconjuntos finitos, no vacíos de G, y sea $H = G_{A+B}$. Consideremos los conjuntos $A+H$ y $B+H$. Si $(A+H, B+H)$ es una pareja crítica entonces, aplicando el teorema 5.2, obtenemos $|A+B| = |(A+H)+(B+H)| = |A+H|+|B+H|-|H|$. Si $(A+H, B+H)$ no es una pareja crítica, entonces $|A+B| = |(A+H)+(B+H)| \geq |A+H|+|B+H|$. En ambos casos se satisface la desigualdad (1). □

5.2 Versión tríos

En esta sección presentaremos una nueva versión del teorema de Kneser consistente con la reformulación del teorema de Kemperman que se expone en [1]. En dicho artículo los autores proponen estudiar ciertas parejas críticas llamadas maximales.

Definición 5.4. Decimos que una pareja de conjuntos (A,B) es *maximal* si los únicos conjuntos $A^* \supseteq A$ y $B^* \supseteq B$ tales que $A^*+B^* = A+B$ son exactamente $A^* = A$ y $B^* = B$.

No es difícil observar que si una pareja (A,B) es maximal entonces satisface $G_A = G_B = G_{A+B}$, siendo falso en general el converso. Sin embargo, es consecuencia del teorema de Kneser, que al restringirnos a parejas críticas la máximalidad es equivalente a la condición anterior.

Proposición 5.5. *Sea (A,B) una pareja crítica en un grupo abeliano G. Entonces, (A,B) es maximal si y sólo si $G_A = G_B = G_{A+B}$.*

Demostración. Supongamos que (A,B) es maximal y que $G_A \neq G_{A+B}$. Notemos entonces que $G_A < G_{A+B}$, y definamos $A^* = A + G_{A+B}$. Así, $A^* \supset A$ satisface $A^*+B = A+B$, contradiciendo la maximalidad de (A,B).

Supongamos ahora que $H = G_A = G_B = G_{A+B}$ y consideremos conjuntos $A^* \supseteq A$ y $B^* \supseteq B$ tales que $A^*+B^* = A+B$. Aplicando el teorema de Kneser a ambas parejas (A^*,B^*) y (A,B) obtenemos

$$|A^*+H|+|B^*+H|-|H| \leq |A^*+B^*| = |A+B| = |A|+|B|-|H|$$

de lo cual se deduce que $A^* = A$ y $B^* = B$, por lo que (A,B) es maximal. □

La siguiente proposición (consecuencia también del teorema de Kneser) justifica el estudio de parejas críticas maximales.

Proposición 5.6. *Para una pareja (A,B) no trivial de conjuntos finitos en G, donde $H = G_{A+B}$, son equivalentes las siguientes condiciones.*

(i) *(A,B) es crítica,*

(ii) *$(A+H,B+H)$ es crítica maximal y $|(A+H)\setminus A|+|(B+H)\setminus B| < |H|$.*

Demostración. Supongamos primero que (A,B) es una pareja crítica. La pareja $(A+H,B+H)$ resulta ser crítica por definición ya que $A+B = (A+H)+(B+H)$. Además $(A+H,B+H)$ es maximal en virtud de la proposición 5.5. Más aún, concatenando la desigualdad (1) con el hecho de que (A,B) es crítica obtenemos $|A+H|-|A|+|B+H|-|B| < |H|$, de donde se sigue lo deseado.

Ahora supongamos que (ii) se satisface. En vista de que $A+B = (A+H)+(B+H)$, $(A+H)+H = A+H$ y $(B+H)+H = B+H$, el siguiente renglón es consecuencia de aplicar el teorema de Kneser a la pareja $(A+H,B+H)$,

$$|A+B| = |(A+H)+(B+H)| = |A+H|+|B+H|-|H|.$$

De lo cual se concluye que (A,B) es crítica ya que $|A+H|+|B+H|-|H| < |A|+|B|$ es consecuencia directa de $|(A+H)\setminus A|+|(B+H)\setminus B| < |H|$. □

Así pues, toda pareja crítica (A,B) se obtiene de una pareja crítica maximal (A^*,B^*), donde $A^* \supseteq A$ y $B^* \supseteq B$ cumplen $|A^*\setminus A|+|B^*\setminus B| < |H|$, siendo $H = G_{A^*} = G_{B^*} = G_{A^*+B^*} = G_{A+B}$. Por este motivo, con el fin de estudiar la estructura de las parejas críticas, nos permitimos restringir nuestra atención al estudio de parejas críticas maximales. Más aún, podemos extender la noción de maximalidad para tríos, y ocuparnos de estudiar tríos críticos maximales.

Definición 5.7. Decimos que un trío (A,B,C) en G es *maximal* si los únicos conjuntos $A^* \supseteq A$, $B^* \supseteq B$ y $C^* \supseteq C$ tales que (A^*,B^*,C^*) es un trío son exactamente $A^* = A$, $B^* = B$ y $C^* = C$.

Observación 5.8. Una pareja (A,B) en G es maximal si y sólo si el trío (A,B,C) es maximal, donde $C = G \setminus -(A+B)$.

Recordemos además las observaciones 2.3 y 2.6 enunciadas para tríos. No es difícil observar que para tríos maximales obtenemos lo siguiente.

Observación 5.9. Sea (A,B,C) un trío maximal en G, entonces

- $C = G\setminus -(A+B)$, $B = G\setminus -(A+C)$ y $A = G\setminus -(C+B)$
- $\delta(A,B,C) = \delta(A,B) = \delta(B,C) = \delta(C,A)$.

Ahora estamos listos para enunciar el teorema de Kneser en su versión tríos.

Teorema 5.10 (Kneser, versión tríos). *Si (A,B,C) es un trío no trivial, crítico y maximal en G, entonces $G_A = G_B = G_C$ y $\delta(A,B,C) = |G_A|$.*

Nuevamente, a modo de ejercicio probaremos la equivalencia entre la versión 2 y la versión tríos del teorema de Kneser.

Proposición 5.11. *Los teoremas 5.2 y 5.10 son equivalentes.*

Demostración. En primer lugar asumamos la veracidad del teorema 5.2 y demostremos el teorema 5.10. Sea (A,B,C) un trío no trivial, crítico y maximal en G. Supongamos sin pérdida de generalidad que A y B son conjuntos finitos. Por la proposición 2.7 y la observación 5.8, sabemos que (A,B) es una pareja crítica maximal. De la proposición 5.5 concluimos que $G_A = G_B = G_{A+B} = G_C$. Usando lo anterior junto con el teorema 5.2 obtenemos $|A+B| = |A+G_A|+|B+G_B|-|G_A| = |A|+|B|-|G_A|$. En otras palabras $\delta(A,B) = |G_A|$ y por la observación 5.9 concluímos $\delta(A,B,C) = |G_A|$.

Ahora demostremos el teorema 5.2 asumiendo el teorema 5.10. Sea (A,B) una pareja crítica no trivial de subconjuntos en G, y sea $H = G_{A+B}$. De la proposición 2.7 sabemos que $(A,B,C = G \setminus -(A+B))$ es un trío crítico no trivial. Para obtener un trío maximal consideremos $(A+H, B+H, C)$. Así, del teorema 5.10 concluímos $\delta(A+H, B+H, C) = |H|$. Equivalentemente, $|A+H| + |B+H| + |C| - |G| = |H|$, de donde se infiere la conclusión del teorema 5.2. □

6. Kemperman, versión tríos

En esta sección presentaremos únicamente la formulación del teorema estructural de Kemperman en su versión tríos. Para ello, es preciso dar algunas definiciones que describen los diferentes tipos de comportamiento presentes en la estructura de tríos no triviales, críticos, y maximales en un grupo abeliano arbitrario.

En primer lugar, observemos que de cualquier permutación de los conjuntos en un trío (A,B,C) resulta un nuevo trío. Además, para todo $g \in G$ tenemos que $(A+g, B-g, C)$ es un trío también.

Definición 6.1. Dos tríos (A,B,C) y (A',B',C') son *equivalentes* si uno se puede obtener del otro por una secuencia de las operaciones descritas en el párrafo anterior.

Observación 6.2. Sea (A,B,C) un trío no trivial, crítico, y maximal. Si (A',B',C') es un trío equivalente a (A,B,C), entonces (A',B',C') es no trivial, crítico, y maximal. Más aún, $\delta(A,B,C) = \delta(A',B',C')$.

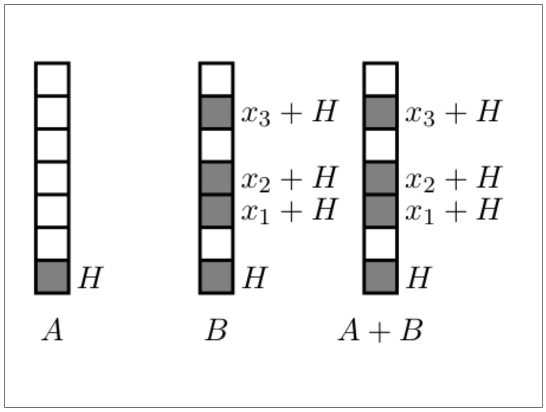

Figura 1. Compás puro relativo a H.

Comenzaremos por describir la estructura de los dos tipos de tríos que generalizan las dos estructuras presentes en el teorema de Vosper versión tríos (teorema 4.2). En adelante G denotará un grupo abeliano, y usaremos Υ para referirnos a un trío en G.

Definición 6.3. Sea $H < G$ finito. Un trío Υ es un *compás puro relativo a* H, si Υ es equivalente a un trío (A, B, C) que satisface lo siguiente:

(1) $A = H$,
(2) $G_B = H$,
(3) $C = G \setminus -(A + B) \neq \emptyset$.

Sea $H < G$ un subgrupo finito, y sean $A, R \in G/H$. Asumamos que G/H es un grupo cíclico generado por R. A un conjunto de la forma $\{A+iR : 0 \leq i \leq t-1\}$ le llamamos una R*–secuencia* de longitud t. Una R–secuencia es *no trivial* si tiene longitud al menos 2. Una R–secuencia es *básica* si es de la forma $\{H + iR : 0 \leq i \leq t - 1\}$.

Definición 6.4. Sea $H < G$ finito. Un trío Υ es un *acorde puro relativo a* H, si G/H es un grupo cíclico generado por $R \in G/H$, y Υ es equivalente a un trío (A, B, C) que satisface lo siguiente:

(1) A y B son ambos R–secuencias no triviales,
(2) $C = G \setminus -(A + B)$ no está contenido en una clase lateral de H.

Se puede verificar que todo compás o acorde puro relativo a H es un trío no trivial, crítico, maximal, con deficiencia $|H|$. En las figuras 1 y 2 se ilustran las estructuras de un compás puro y de un acorde puro respectivamente.

A continuación definiremos dos variantes a las estructuras antes descritas, que nos permitirán dar una descripción recursiva de la estructura de un trío no trivial, crítico, y maximal, en un grupo abeliano arbitrario.

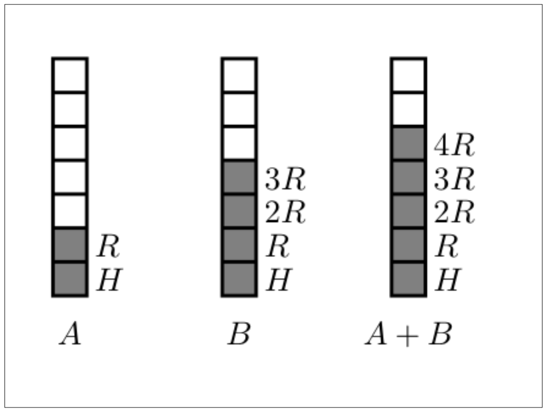

Figura 2. Acorde puro relativo a H.

Para un subgrupo $H \leq G$, diremos que un subconjunto $A \subseteq G$ es H–*periódico* si $A + H = A$ (equivalentemente, $H \leq G_A$). Dado un subconjunto $A \subseteq G$ existe un subgrupo minimal, $H \leq G$, tal que A está contenido en una sola clase lateral de H. A dicha clase lateral la denotaremos por $[A]$ y la llamaremos la *cerradura* de A.

Definición 6.5. Un trío Υ es un *compás impuro relativo a* $H \leq G$, si es equivalente a un trío (A, B, C) que satisface lo siguiente:

(1) $[A] = H$, $B \cap H \neq \emptyset$ y $C \cap H \neq \emptyset$,
(2) $B \setminus H$ es H–periódico,
(3) $C \setminus H = (G \setminus -(A + B)) \setminus H$.

Definición 6.6. Un trío Υ es un *acorde impuro relativo a* $H \leq G$, si G/H es un grupo cíclico generado por $R \in G/H$, y Υ es equivalente a un trío (A, B, C) que satisface lo siguiente:

(1) $A \cup H$ y $B \cup H$ son ambos R–secuencias básicas no triviales,
(2) $A \cap H \neq \emptyset$, $B \cap H \neq \emptyset$ y $C \cap H \neq \emptyset$,
(3) $\emptyset \neq (C \setminus H) = (G \setminus -(A + B)) \setminus H$.

Notemos que por definición, si $\Upsilon = (A, B, C)$ es un compás o acorde impuro relativo a H, entonces $(A \cap H, B \cap H, C \cap H)$ es un trío no trivial, maximal siempre que Υ sea maximal, y $\delta(A, B, C) = \delta(A \cap H, B \cap H, C \cap H)$. Al nuevo trío $(A \cap H, B \cap H, C \cap H)$ le llamaremos una *continuación* de Υ. En las figuras 3 y 4 se ilustran las estructuras de un compás impuro, y de un acorde impuro respectivamente.

Ahora si estamos listos para enunciar el teorema estructural de Kemperman en su versión tríos.

Teorema 6.7 (Kemperman, versión tríos)**.** *Sea Υ un trío no trivial, crítico, y maximal. Entonces existe una secuencia de tríos $\Upsilon = \Upsilon_1, \Upsilon_2, \ldots, \Upsilon_m$, que satisfacen lo siguiente:*

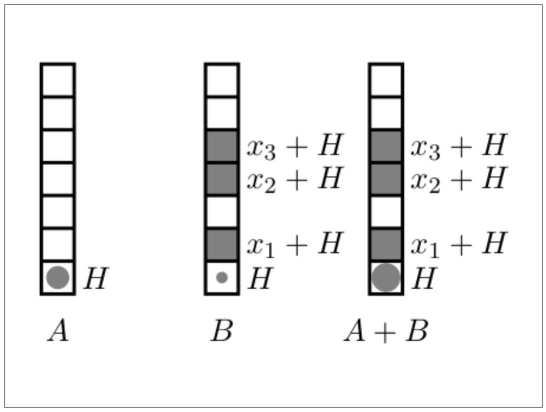

Figura 3. Compás impuro relativo a H.

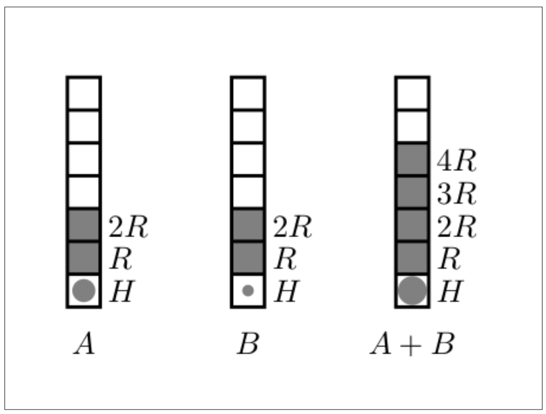

Figura 4. Acorde impuro relativo a H.

(i) Υ_i *es un compás o acorde impuro con continuación* Υ_{i+1}*, para* $1 \leq i \leq m-1$,
(ii) Υ_m *es un compás o acorde puro.*

La prueba de este teorema se puede consultar en [1].

Agradecimientos. Este trabajo se realizó con el apoyo del proyecto PAPIIT IA102013. Agradezco al *Centro de Innovación Matemática A. C.* y a todos los alumnos de la *Tercera Escuela de Verano de Matemáticas en Querétaro* a quienes impartí un curso con el material comprendido en este trabajo. Muy en especial agradezco también a Leonardo Martínez por leer cuidadosamente el primer borrador de este escrito, y por hacerme sugerencias siempre pertinentes para mejorar la exposición del material.

Bibliografía

[1] T. Boothby, M. DeVos y A. Montejano, «A new proof of kemperman's theorem», *Integers: The Electronic Journal of Combinatorial Number Theory*, vol. #A15, 2015, 1–20.

[2] A. Cauchy, «Recherches sur les nombres», *J. Ecole polytechnique*, vol. 9, 1813, 99–116.

[3] H. Davenport, «On the addition of residue classes», *J. London Math. Soc.*, vol. 10, 1935, 30–32.

[4] S. Eliahou y M. Kervaire, «Some extensions of the cauchy-davenport theorem», *Electronic Notes in Discrete Mathematics*, vol. 28, 2007, 557–564.

[5] D. J. Grynkiewicz, «Quasi-periodic decompositions and the kemperman structure theorem», *European J. Combin.*, vol. 26, núm. 5, 2005, 559–575.

[6] ———, «A step beyond kemperman's structure theorem», *Mathematika*, vol. 55, núm. 1-2, 2009, 67–114.

[7] Y. O. Hamidoune, «Hyper-atoms and the kemperman's critical pair theory», arXiv:0708.3581.

[8] ———, «A structure theory for small sum subsets», *Acta Arith.*, vol. 147, núm. 4, 2011, 303–327.

[9] J. H. B. Kemperman, «On small sumsets in an abelian group», *Acta Mathematica*, vol. 103, 1960, 63–88.

[10] M. Kneser, «Abschätzungen der asymptotischen dichte von summenmengen», *Math. Z*, vol. 58, 1953, 459–484.

[11] V. Lev, «Critical pairs in abelian groups and kemperman's structure theorem», *Int. J. Number Theory*, vol. 2, núm. 3, 2006, 379–396.

[12] M. B. Nathanson, *Additive number theory: Inverse problems and the geometry of sumsets*, Graduate Texts in Mathematics, 165, Springer-Verlag, New York, 1996.

[13] A. G. Vosper, «The critical pairs of subsets of a group of prime order», *J. London Math. Soc.*, vol. 31, 1956, 200–205.

[14] J. P. Wheeler, «The cauchy-davenport theorem for finite groups», 2012, arXiv:1202.1816v1.