Prueba de Furstenberg de la infinitud de los primos

David Cardozo

28 de enero de 2015

Definición 1. *Para cada* $a \in \mathbb{Z}^+$ *y* $b \in \mathbb{Z}$ *definimos el conjunto* $S(a,b) := \{an + b : n \in \mathbb{Z}\} \subseteq \mathbb{Z}$

1. Pruebe que la colección $\{S(a,b) : (a,b) \in \mathbb{Z}^+ \times \mathbb{Z}\}$ es base para una topología.

Solución. Usando la ayuda de la definición, queremos observar que pasan dos cosas:

1. Para cada $x \in \mathbb{Z}$, existe por lo menos un elemento básico B que contiene a x

   Nótese entonces que $b \in S(a,b)$ para todo $a \in \mathbb{Z}^+$. Por lo tanto esta condición es cumplida.

2. Si a pertenece a a intersección de dos elementos básicos B_1 y B_2, entonces existe un elemento básico B_3 que contiene a x tal que $B_3 \subseteq B_1 \cap B_2$

   En general, obsérvese que sea a un elemento que pertenece a ambos $S(b,a)$ y $S(c,a)$, tenemos que:

   $$S(b,a) = \{bn + a : n \in \mathbb{Z}\}$$
   $$S(c,a) = \{cn + a : n \in \mathbb{Z}\}$$

   y podemos entonces que para que un elemento este en los dos, también esta en el conjunto(m.cm denota el mínimo común múltiplo):

   $$S(\text{ m.c.m } (b,c), a) = \{a + n \text{ m.c.m } (b,c) : n \in \mathbb{Z}\}$$

   y claramente $a \in S(a, \text{ m.c.m } (b,c))$ Por lo tanto observamos que en general, la intersección de elementos base, es base. O lo que se quería observar: Si a pertenece a a intersección de dos elementos básicos B_1 y B_2, entonces existe un elemento básico B_3 que contiene a x tal que $B_3 \subseteq B_1 \cap B_2$.

2. Muéstrese que la topología discreta sobre τ_f no es la usual topología discreta sobre $\mathbb{Z}$. Mas aún, muestre que ningún conjunto finito $A \subseteq Z$ es abierto.

Solución Para resolver esta pregunta, la reformularemos en el siguiente lema:

Lema 1. *Sea $A \subseteq \mathbb{Z}$ y $A \neq \varnothing$ un conjunto finito, en la topología τ_f, A no es abierto.*

Demostración. (*Peligro: Una línea.*) Observamos que como cualquier abierto diferente de $\varnothing$ contiene una secuencia de números enteros infinitos, para un A finito, es decir, A que contiene finitos números enteros no va tener una secuencia infinita de números enteros, por lo tanto concluimos que ningún subconjunto finito es un abierto en $(\mathbb{Z}, \tau_f)$ $\square$

3. Muestre que $(\mathbb{Z}, \tau_f)$ es un espacio de Hausdorff.

Solución (*Peligro: Una línea.*) Observar que para $b, c \in \mathbb{Z}$ y suponer que $n \nmid (b - c)$ tenemos que:

$$\{an + b | n \in \mathbb{Z}\} \cap \{kn + c | n \in \mathbb{Z}\} = \varnothing$$

Por lo tanto, tenemos que para cada par de elementos b, c, existen entornos $S(a, b)$ y $S(k, c)$ que son disjuntos.

4. Pruebe que cada $S(a, b)$ es un **conjunto cerrado** (i.e. complemento de un abierto).

Solución. Observemos dos cosas, uno es que $S(a, b)$ es un abierto por definición, por lo tanto, queremos ver que $S(a, b)$ es complemento de un abierto. Esto ultimo, lo podemos ver ya que:

$$S(a, b) = \left(\bigcup_{i=1}^{a-1} S(a, b + i) \right)^c$$

Y esto es visto con argumento de conteo: Observar que $S(a, b)$ es una colección de números enteros con origen de una progresión aritmética (*i.e.* la diferencia de dos términos es múltiplo de una constante), y el complemento de este conjunto son elementos de otras progresiones aritméticas con la misma constante de separación, pero con un origen diferente (*i.e.* $S(a, b)$ con b variando hasta cierto numero, en concreto, variando hasta la constante de la progresión menos 1), entonces podemos describir el complemento como unión de finitas progresiones aritméticas.

5. Muestre que:

$$\mathbb{Z} \setminus \{-1, 1\} = \bigcup_{p \text{ primo}} S(p, 0)$$

concluya que existen infinitos números primos.

Solución Para esta parte del problema, utilizamos el *Teorema fundamental de la Aritmética* probado en Estructural, citando:

> " Todo número natural $n > 1$ tiene una única factorización en números primos."

Por lo tanto todo numero a excepción de 1 y -1 tiene una factorización única en primos y por lo tanto esta contenido a lo sumo en un $S(p, 0)$ para p

primo. Por lo tanto el conjunto de los enteros salvo 1 y -1, se puede escribir como la unión de :

$$\mathbb{Z}\setminus\{-1,1\} = \bigcup_{p \text{ primo}} S(p,0)$$

Observación: Con este resultado, concluimos que existen infinitos primos, razonando de la siguiente manera:

Suponga que no hay infinitos primos, entonces la colección de números primos es finita, pero según el problema 2, la unión de $\cup_{p \text{ primo}} S(p,0)$ sería cerrada, y tendríamos entonces que concluir con que el conjunto $\{1,-1\}$ es abierto porque es el complemento a un cerrado, lo cual es absurdo.

Concluimos entonces que deben existir infinitos primos.

Aclaración: El autor conocía de esta prueba antes de ver la tarea, debido a la aparición de esta en el libro: *Proofs from THE BOOK* escrito por Aigner y Ziegler. Es por ello, que esta tarea sigue en similitud la misma idea escrita en tal libro.