OTRO SUBGRUPO DE UN GRUPO FINITAMENTE GENERADO QUE NO ES FINITAMENTE GENERADO

Sea G un grupo y $X \subset G$. Notamos $X^{-1} = \{x^{-1} : x \in X\}$. Decimos que G es *finitamente generado* si existe $X \subset G$ finito tal que

$$G = \langle X \rangle = \{x_1 \cdots x_n : n \in \mathbb{N}_0,\ x_1, \dots, x_n \in X \cup X^{-1}\}.$$

Ejemplo 1. Un grupo es cíclico si y sólo si es generado por un único elemento.

Ejemplo 2. El grupo diedral $\mathbb{D}_n$ está generado por dos elementos; a saber, la rotación r y la reflexión s.

Ejemplo 3. Todo grupo finito G es finitamente generado, tomando $X = G$ como conjunto de generadores. Hay grupos infinitos que son finitamente generados: para cada $n \in \mathbb{N}$ el grupo abeliano $\mathbb{Z}^n = \mathbb{Z} \times \cdots \times \mathbb{Z}$ está generado por el conjunto $\{e_1, \dots, e_n\}$; aquí

$$e_i := (0, \dots, 0, \overbrace{\ 1\ }^{i}, 0, \dots, 0).$$

Hay grupos que no son finitamente generados, como veremos a continuación. Consideremos $\mathbb{Z}^{\mathbb{Z}}$ el conjunto de sucesiones *bi-infinitas* de números enteros, visto como grupo abeliano con las suma coordenada a coordenada. Dada $a = (a_n)_{n \in \mathbb{Z}} \in \mathbb{Z}^{\mathbb{Z}}$, su *soporte* es

$$\operatorname{sop}(a) = \{n \in \mathbb{Z} : a_n \neq 0\} \subset \mathbb{Z}.$$

Notamos $\mathbb{Z}^{(\mathbb{Z})}$ al conjunto de sucesiones cuyo soporte es un conjunto finito. Equivalentemente, estas son las sucesiones que son eventualmente nulas hacia ambos extremos. Notamos $e_i \in \mathbb{Z}^{(\mathbb{Z})}$ a la sucesión que tiene un 1 en el lugar i y 0 en el resto de sus coordenadas.

Ejercicio 1. Verificar que $\mathbb{Z}^{(\mathbb{Z})}$ es un subgrupo de $\mathbb{Z}^{\mathbb{Z}}$.

Intuitivamente, si tenemos finitas sucesiones cada una con soporte finito, entonces hay un conjunto finito F en el cual alguna de ellas tiene una coordenada no nula. Las posibles sumas y restas entre tales sucesiones siguen teniendo su soporte dentro de F, por lo que el grupo generado por ellas no pueden comprender a toda otra sucesión de soporte finito. A continuación formalizamos esta idea.

Proposición 1. *El grupo $\mathbb{Z}^{(\mathbb{Z})}$ no es finitamente generado.*

Demostración. Observemos primero que para cada $k \in \mathbb{Z}$ la evaluación $\operatorname{ev}_k \colon \mathbb{Z}^{(\mathbb{Z})} \to \mathbb{Z}$, $\operatorname{ev}_k(a) = a_k$ es un morfismo de grupos. Supongamos que $\mathbb{Z}^{(\mathbb{Z})}$ admitiese un conjunto finito de generadores $\mathbb{Z}^{(\mathbb{Z})} = \langle a_1, \dots, a_n \rangle$, y sean $S_i = \operatorname{sop}(a_i)$ para cada $i \in \{1, \dots, n\}$ sus soportes. Como $S := S_1 \cup \cdots \cup S_n$ es finito, existe $k \in \mathbb{Z} \setminus S$, y en particular $\operatorname{ev}_k(a_i) = 0$ para cada i.

Ahora, puesto que $e_k \in \mathbb{Z}^{(\mathbb{Z})} = \langle a_1, \dots, a_n \rangle$, deben existir $s_1, \dots, s_n \in \mathbb{Z}$ tales que

$$e_k = s_1 a_1 + \cdots + s_n a_n.$$

Evaluando en la coordenada k,

$$1 = \mathrm{ev}_k(e_k) = \mathrm{ev}_k(s_1 a_1 + \cdots + s_n a_n) = s_1 \,\mathrm{ev}_k(a_1) + \cdots + s_n \,\mathrm{ev}_k(a_n) = 0.$$

Lo anterior es absurdo, y la contradicción proviene de suponer que $\mathbb{Z}^{(\mathbb{Z})}$ es finitamente generado. Esto concluye la prueba. $\square$

El ejemplo anterior nos muestra que la finita generación no es una condición que podamos asumir siempre; en particular, es de interés saber qué construcciones entre grupos la preservan. Si bien cocientes de subgrupos finitamente generados vuelven a tener esta propiedad, no es cierto lo mismo en el caso de los subgrupos.

Definición 1. Definimos[1] el grupo $\mathbb{Z} \wr \mathbb{Z}$ que como conjunto es $\mathbb{Z}^{(\mathbb{Z})} \times \mathbb{Z}$ y cuya operación está dada por

$$((a_n)_{n\in\mathbb{Z}}, k) \cdot ((b_n)_{n\in\mathbb{Z}}, l) = ((a_n + b_{n+k})_{n\in\mathbb{Z}}, k + l).$$

Notar que tenemos $\mathbb{Z}^{(\mathbb{Z})} \times 0 \triangleleft \mathbb{Z} \wr \mathbb{Z}$, $0 \times \mathbb{Z} \leq \mathbb{Z} \wr \mathbb{Z}$ y que estos subgrupos de $\mathbb{Z} \wr \mathbb{Z}$ son isomorfos a $\mathbb{Z}^{(\mathbb{Z})}$ y $\mathbb{Z}$ respectivamente. En particular, como ya hemos visto que $\mathbb{Z}^{(\mathbb{Z})}$, para obtener nuestro contraejemplo será suficiente ver que $\mathbb{Z} \wr \mathbb{Z}$ es finitamente generado.

Proposición 2. $\mathbb{Z} \wr \mathbb{Z} = \langle (e_1, 0), (0, 1) \rangle$.

Demostración. Notemos en primer lugar que $(a, l) = (a, 0) \cdot (0, l)$, y que $(0, l) = (0, 1)^l$, donde aquí el exponente elevado a la l refiere a la multiplicación de l veces el elemento $(0, 1)$ en $\mathbb{Z} \wr \mathbb{Z}$. Similarmente tenemos $(a, 0)^s = (s \cdot a, 0)$.

Basta ver entonces que los elementos de la forma $((a_n)_{n\in\mathbb{Z}}, 0)$ pueden escribirse como productos de $(e_1, 0)$, $(0, 1)$ y sus inversos. Dado que $a = (a_n)_{n\in\mathbb{Z}}$ tiene soporte finito, existen $s_1, \ldots, s_k \in \mathbb{Z}$ e $i_1, \ldots, i_k \in \mathbb{Z}$ tales que

$$a = s_1 e_{i_1} + \cdots + s_k e_{i_k}$$

y entonces

$$(a, 0) = (e_{i_1}, 0)^{s_1} \cdots (e_{i_k}, 0)^{s_k}.$$

Esto permite reducir nuestro problema a ver que $(e_k, 0) \in \langle (e_1, 0), (0, 1) \rangle$ para todo $k \in \mathbb{N}$. Efectivamente,

$$(0, 1)^k (e_1, 0)(0, 1)^{-k} = (0, k)(e_1, 0)(0, -k) = (0, k)(e_1, -k) = (e_k, 0).$$

$\square$

[1] Este grupo es un producto semidirecto entre $\mathbb{Z}$ y $\mathbb{Z}^{(\mathbb{Z})}$; aquí el morfismo $\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}^{(\mathbb{Z})})$ está determinado por el automorfismo $R\colon \mathbb{Z}^{(\mathbb{Z})} \to \mathbb{Z}^{(\mathbb{Z})}$, $R(e_i) = e_{i-1}$.