Apéndice B
Lema de Zorn

El lema de Zorn es una versión equivalente del **axioma de elección**[*] que se utiliza muy a menudo en álgebra. Aquí vamos a revisar el enunciado y un par de aplicaciones típicas.

B.1 Lema de Zorn

B.1.1. Definición. Se dice que un conjunto $\mathcal{P}$ es **parcialmente ordenado** si sobre los elementos de $\mathcal{P}$ está definida una relación $\preceq$ que satisface los siguientes axiomas.

1) **Reflexividad**: para todo $x \in \mathcal{P}$ se cumple $x \preceq x$.

2) **Antisimetría**: para cualesquiera $x, y \in \mathcal{P}$ si $x \preceq y$ e $y \preceq x$, entonces $x = y$.

3) **Transitividad**: para cualesquiera $x, y, z \in \mathcal{P}$ si $x \preceq y$ e $y \preceq z$, entonces $x \preceq z$.

Se dice que $m \in \mathcal{P}$ es un elemento **maximal** si no existe otro elemento $x \in \mathcal{P}$ tal que $m \preceq x$.
Se dice que un subconjunto $\mathcal{S} \subseteq \mathcal{P}$ es una **cadena** si para cualesquiera $s, s' \in \mathcal{S}$ se tiene $s \preceq s'$ o $s' \preceq s$.
Se dice que un subconjunto $\mathcal{S} \subseteq \mathcal{P}$ es **acotado** si existe $t \in \mathcal{P}$ (una **cota superior**) tal que $s \preceq t$ para todo $s \in \mathcal{S}$.

B.1.2. Lema de Zorn. *Sea $\mathcal{P}$ un conjunto parcialmente ordenado no vacío. Supongamos que toda cadena en $\mathcal{P}$ es acotada. Entonces, $\mathcal{P}$ posee un elemento maximal.*

B.2 Aplicación: bases de espacios vectoriales

La primera aplicación del lema de Zorn debe de ser conocida al lector. Recordemos primero algunas definiciones de álgebra lineal. Sea k un cuerpo. Para un espacio vectorial V sobre k y un subconjunto $S \subset V$ el subespacio vectorial **generado** por S es el subconjunto de las sumas finitas

$$\sum_{1 \leq i \leq n} \lambda_i v_i$$

donde $\lambda_i \in k$ y $v_i \in S$. Se dice que los elementos de S son **linealmente independientes** si para cualesquiera $\{v_1, \ldots, v_n\} \subseteq S$, si

$$\sum_{1 \leq i \leq n} \lambda_i v_i = 0,$$

[*] Esto no es un curso de lógica, así que no voy a probar la equivalencia; el lector puede consultar otras fuentes, por ejemplo [Lan2002, Appendix 2].

entonces $\lambda_1 = \cdots = \lambda_n = 0$. Se dice que S es una **base** de V si $\langle S \rangle = V$ y los elementos de S son linealmente independientes.

B.2.1. Teorema. *Sea V un espacio vectorial no nulo y sea $S \subset V$ un subconjunto linealmente independiente. Entonces, S puede ser completado a una base de V.*

Demostración. Sea $\mathcal{P}$ el conjunto de los subconjuntos linealmente independientes $T \subseteq V$ tales que $S \subseteq T$, parcialmente ordenado respecto a la inclusión. En particular, $S \in \mathcal{P}$, así que $\mathcal{P} \neq \emptyset$.

Sea $\{T_\alpha\}$ una cadena en $\mathcal{P}$; es decir, una colección de conjuntos linealmente independientes $T_\alpha \subset V$ tales que

1) $S \subseteq T_\alpha$ para todo α,

2) para cualesquiera α y β se tiene $T_\alpha \subseteq T_\beta$ o $T_\beta \subseteq T_\alpha$.

Tomemos la unión $T := \bigcup_\alpha T_\alpha$. Tenemos $S \subseteq T_\alpha \subseteq T$ para todo α. Además para una colección finita de vectores $\{v_1, \ldots, v_n\} \subseteq T$ tenemos $v_i \in T_{\alpha_i}$ para algunos α_i, y ya que $\{T_\alpha\}$ es una cadena, todos estos vectores pertenecen a algún conjunto T_α y por ende son linealmente independientes. Esto significa que $T \in \mathcal{P}$ y es una cota superior para la cadena.

Ahora el lema de Zorn implica que existe un elemento maximal en $\mathcal{P}$; es decir, un conjunto linealmente independiente B tal que $S \subseteq B$ y B no está contenido en ningún otro conjunto linealmente independiente. Vamos a probar que los elementos de B generan a V.

Supongamos que $\langle B \rangle \subsetneq V$. En este caso existe un vector $v \in V$, $v \notin \langle B \rangle$. Vamos a ver que esto implica que el conjunto $B \cup \{v\}$ es linealmente independiente. Si $B \cup \{v\}$ fuera linealmente dependiente, entonces existiría una combinación lineal

$$\lambda\, v + \lambda_1\, v_1 + \cdots + \lambda_n\, v_n = 0$$

donde $\lambda, \lambda_i \in k$ son escalares, no todos nulos, y $v_1, \ldots, v_n \in B$. Dado que los elementos de B son linealmente independientes, tenemos necesariamente $\lambda \neq 0$. Sin embargo, en este caso

$$v = -\left(\frac{\lambda_1}{\lambda}\, v_1 + \cdots + \frac{\lambda_n}{\lambda}\, v_n\right),$$

lo que implica que $v \in \langle B \rangle$. Entonces, el conjunto $B \cup \{v\}$ debe ser linealmente independiente.

Esto contradice el hecho de que B sea un conjunto linealmente independiente maximal, y por lo tanto $\langle B \rangle = V$. ■

B.2.2. Corolario. *Todo espacio vectorial no nulo posee una base.*

Demostración. En el resultado anterior, basta tomar $S = \{v\}$ donde v es cualquier vector no nulo en V. ■

B.2.3. Corolario. *Sea V un espacio vectorial no nulo. Para todo subespacio $U \subset V$ existe otro espacio $W \subset V$ tal que $V = U \oplus W$.*

Demostración. Según el teorema, podemos escoger una base S de U, y luego completarla a una base B de V. Sea W el subespacio generado por $B \setminus S$. Se puede verificar que $V = U + W$ y $U \cap W = \{0\}$. ■

B.3 Aplicación: grupos abelianos divisibles (*)

Recordemos que un grupo abeliano D es **divisible** si para cualesquiera $x \in D$ y $n = 1, 2, 3, \ldots$ existe $y \in D$ tal que $ny = x$. Hemos encontrado estos grupos en los ejercicios. Por ejemplo, los grupos $\mathbb{Q}, \mathbb{R}, \mathbb{Q}/\mathbb{Z}, \mathbb{R}/\mathbb{Z}$ son divisibles. He aquí una caracterización importante de grupos divisibles.

B.3.1. Teorema (Reinhold Baer, 1940). *Sea D un grupo abeliano. Las siguientes condiciones son equivalentes.*

1) *Para todo grupo abeliano A y un subgrupo $B \subseteq A$ cualquier homomorfismo $f\colon B \to D$ se extiende a un homomorfismo $\widetilde{f}\colon A \to D$:*

$$\begin{array}{ccc} B & \hookrightarrow & A \\ {\scriptstyle f}\downarrow & \swarrow_{\exists \widetilde{f}} & \\ D & & \end{array}$$

$$\widetilde{f}\big|_B = f.$$

2) *D es divisible.*

Demostración. La implicación fácil es 1) $\Rightarrow$ 2). Para $n = 1, 2, 3, \ldots$ consideremos el subgrupo $n\mathbb{Z} \subseteq \mathbb{Z}$. Un elemento $x \in D$ corresponde a un homomorfismo

$$f\colon n\mathbb{Z} \to D, \quad an \mapsto ax.$$

Luego, si D cumple la propiedad 1), entonces f se extiende a $\widetilde{f}$:

$$\begin{array}{ccc} n\mathbb{Z} & \hookrightarrow & \mathbb{Z} \\ {\scriptstyle f}\downarrow & \swarrow_{\exists \widetilde{f}} & \\ D & & \end{array}$$

Tenemos

$$n \cdot \widetilde{f}(1) = \widetilde{f}(n \cdot 1) = f(n) = x.$$

Esto demuestra que x es divisible por n.

Para probar 2) $\Rightarrow$ 1), primero notamos que si D es divisible, entonces la propiedad 1) se cumple para los subgrupos de $\mathbb{Z}$: como arriba, todo homomorfismo $f\colon n\mathbb{Z} \to D$ se extiende a $\widetilde{f}\colon \mathbb{Z} \to D$. De hecho, f está definido por la imagen $f(n) = x \in D$, y por la divisibilidad existe $y \in D$ tal que $n \cdot y = x$. Podemos definir

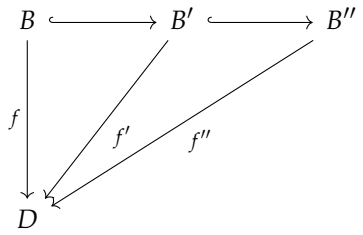
$$\widetilde{f}\colon \mathbb{Z} \to D, \quad 1 \mapsto y.$$

Ahora para todo $an \in n\mathbb{Z}$ se cumple

$$\widetilde{f}(an) = an\,\widetilde{f}(1) = any = ax = a\,f(n) = f(an).$$

Procedamos con la prueba. Sean A un grupo abeliano, $B \subseteq A$ un subgrupo y $f\colon B \to D$ un homomorfismo. Sea $\mathcal{P}$ un conjunto de los pares (B', f') donde $B \subseteq B' \subseteq A$ es un subgrupo que contiene a B y $f'\colon B' \to D$ es un homomorfismo tal que $f = f'|_B$. En particular, $(B, f) \in \mathcal{P}$, así que $\mathcal{P} \neq \emptyset$. Consideremos la siguiente relación sobre $\mathcal{P}$:

$$(B', f') \preceq (B'', f'') \iff B' \subseteq B'' \text{ y } f''\big|_{B'} = f'.$$



El conjunto $\mathcal{P}$ es parcialmente ordenado respecto a esta relación. Para una cadena $\{(B_\alpha, f_\alpha)\}$ podemos considerar la unión $\bigcup_\alpha B_\alpha$. Puesto que $\{(B_\alpha, f_\alpha)\}$ es una cadena, se ve que $\bigcup_\alpha B_\alpha$ es un subgrupo abeliano de A tal que $B_\alpha \subseteq \bigcup_\alpha B_\alpha$ para todo α. Podemos definir un homomorfismo $\phi\colon \bigcup_\alpha B_\alpha \to D$ de la siguiente manera: para todo $x \in \bigcup_\alpha B_\alpha$ tenemos $x \in B_\alpha$ para algún α, y pongamos $\phi(x) := f_\alpha(x)$. Dado que $\{(B_\alpha, f_\alpha)\}$ es una cadena en $\mathcal{P}$, esto nos da un homomorfismo bien definido. Por la definición, $\phi|_{B_\alpha} = f_\alpha$ para todo α. Entonces, $(\bigcup_\alpha B_\alpha, \phi)$ es una cota superior para la cadena.

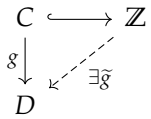
El lema de Zorn implica que $\mathcal{P}$ posee un elemento maximal (B', f'). Necesitamos probar que $B' = A$. Supongamos que $B' \subsetneq A$. Entonces, existe algún elemento $x \in A \setminus B'$, y podemos considerar el conjunto

$$C := \{a \in \mathbb{Z} \mid a \cdot x \in B'\} \subseteq \mathbb{Z}.$$

Se ve que esto es un subgrupo de $\mathbb{Z}$. Consideremos el homomorfismo de grupos abelianos

$$g\colon C \to D, \quad a \mapsto f'(a \cdot x).$$

Como hemos notado, dado que D es divisible, el homomorfismo g se extiende a un homomorfismo $\widetilde{g}\colon \mathbb{Z} \to D$:



Consideremos ahora el subgrupo $B'' := \langle B' \cup \{x\}\rangle$. Sus elementos son sumas $y + nx$ donde $y \in B'$ y $n \in \mathbb{Z}$. Por nuestra hipótesis que $x \notin B'$, se tiene $B' \subsetneq B'' \subseteq A$. Consideramos la aplicación

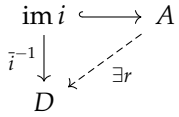
$$\begin{aligned} &f''\colon B'' \to A, \\ &y + nx \mapsto \widetilde{g}(n) + f'(y). \end{aligned}$$

Se ve que esto es un homomorfismo de grupos abelianos y $f''|_{B'} = f'$. Entonces, $(B', f') \preceq (B'', f'')$. Pero esto contradice la maximalidad de (B', f'). Podemos concluir que $B' = A$. ■

De aquí podemos deducir otra caracterización de grupos divisibles.

B.3.2. Corolario. *D es un grupo abeliano divisible si y solamente si todo monomorfismo de grupos abelianos $i\colon D \rightarrowtail A$ admite un homomorfismo $r\colon A \to D$ tal que $r \circ i = \mathrm{id}_D$.*

Demostración. Supongamos que D es divisible. Un monomorfismo $i\colon D \rightarrowtail A$ induce un isomorfismo $\overline{i}\colon D \xrightarrow{\cong} \operatorname{im} i$. El teorema anterior nos dice que $\overline{i}^{-1}\colon \operatorname{im} i \xrightarrow{\cong} D$ se extiende al grupo A:



Tenemos $r|_{\operatorname{im} i} = \bar{i}^{-1}$, así que $r \circ i = \bar{i}^{-1} \circ \bar{i} = \mathrm{id}_D$.

Viceversa, supongamos que todo monomorfismo $i\colon D \rightarrowtail A$ admite un homomorfismo $r\colon A \to D$ tal que $r \circ i = \mathrm{id}_D$. Para un elemento $x \in D$ y $n = 1, 2, 3, \ldots$ consideremos el conjunto

$$C := \{(a \cdot x, -an) \mid a \in \mathbb{Z}\} \subseteq D \times \mathbb{Z}.$$

Esto es un subgrupo de $D \times \mathbb{Z}$: tenemos $(0,0) = (0 \cdot x, -0 \cdot n) \in C$, y luego para cualesquiera $a, b \in \mathbb{Z}$

$$(a \cdot x, -an) \pm (b \cdot x, -bn) = ((a \pm b) \cdot x, -(a \pm b)\, n).$$

Podemos pasar al grupo cociente $(D \times \mathbb{Z})/C$ y considerar el homomorfismo

$$\begin{aligned} i\colon D &\to (D \times \mathbb{Z})/C, \\ z &\mapsto (z, 0) + C \end{aligned}$$

(esto es la composición de la inclusión de D como un subgrupo de $D \times \mathbb{Z}$ con la proyección sobre el grupo cociente). Notamos que

$$(x, 0) - (0, n) = (x, -n) = (1 \cdot x, -1 \cdot n) \in C,$$

así que

$$i(x) = (0, n) + C \quad \text{en } (D \times \mathbb{Z})/C.$$

Verifiquemos que i es un monomorfismo: si tenemos

$$(z, 0) - (z', 0) \in C,$$

entonces

$$(z - z', 0) = (a \cdot x, -an)$$

para algún $a \in \mathbb{Z}$. Sin embargo, $n \neq 0$, así que esto significa que $a = 0$ y luego $z - z' = 0 \cdot x = 0$, y por ende $z = z'$. Entonces, por nuestra hipótesis, existe un homomorfismo $r\colon (D \times \mathbb{Z})/C \to D$ tal que $r \circ i = \mathrm{id}_D$. En particular,

$$x = r \circ i(x) = r((0, n) + C) = n \cdot r((0, 1) + C).$$

Esto establece la divisibilidad de x por n. ■

Bibliografía

[Lan2002] Serge Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. MR1878556
http://dx.doi.org/10.1007/978-1-4613-0041-0