AMPLIACIÓN DE MATEMÁTICAS

SUBGRUPOS.

Toda estructura algebraica suele contener subconjuntos que heredan la estructura. Así los espacios vectoriales contienen subespacio vectoriales. También los grupos, de forma análoga, contienen **subgrupos**.

Definición 1. *Sea* $(\mathbb{G}, *)$ *un grupo y se* S *un subconjunto de* $\mathbb{G}$ *(* $S \subset \mathbb{G}$ *). Decimos que* S *con la operación de* $\mathbb{G}$*,* $(S, *)$*, es un* ***subgrupo*** *de* $\mathbb{G}$ *si* $(S, *)$ *es un grupo.*

Observación 1. *Escribiremos* $S \trianglelefteq \mathbb{G}$ *para indicar que* S *es un subgrupo de* $\mathbb{G}$*. Si* $S \subsetneq \mathbb{G}$ *escribimos* $S \triangleleft \mathbb{G}$*.*

Obviamente, siempre se tiene que el orden del subgrupo es menor o igual que el del grupo:

$$\text{si } S \trianglelefteq \mathbb{G}, \text{ entonces } |S| \leq |\mathbb{G}|.$$

Ejemplos 1.
1. $\mathbb{G} \trianglelefteq \mathbb{G}$.
2. $(\{e\}, *) \trianglelefteq (\mathbb{G}, *)$, *donde* e *es el elemento neutro de* $\mathbb{G}$.
3. $(n\mathbb{Z}_n, +) \triangleleft (\mathbb{Z}, +) \triangleleft (\mathbb{Q}, +) \triangleleft (\mathbb{R}, +) \triangleleft (\mathbb{C}, +)$.
4. $(\mathbb{Q}\backslash\{0\}, \times) \triangleleft (\mathbb{R}\backslash\{0\}, \times) \triangleleft (\mathbb{C}\backslash\{0\}, \times)$.
5. *Si* $X \subsetneq Y$*, entonces* $(P(X), \triangle) \triangleleft (P(Y), \triangle)$.
6. *Si* $X = \mathbb{R}^n$*, entonces el grupo general lineal es un subgrupo del grupo de biyecciones sobre* $\mathbb{R}^n$*, es decir*

$$GL(n, \mathbb{R}) \triangleleft S_X.$$

Es fácil caracterizar a los subgrupos, como en el caso de espacios vectoriales.

Teorema 1. *(**Caracterización de subgrupos**). Sea* $(\mathbb{G}, *)$ *un grupo y sea* $S \subseteq \mathbb{G}$ *un subconjunto no vacío. Entonces* S *es un subgrupo de* $\mathbb{G}$ *si y solo si*

$$g_1 * g_2^{-1} \in S \qquad \text{para todo} \qquad g_1, g_2 \in S.$$

Demostración:

- Si $(S, *)$ es un grupo, entonces para todo $g_1, g_2 \in S$ existe el inverso de g_2 (de cualquier elemento de S), $g_2^{-1} \in S$, y además si operamos $g_1 * g_2^{-1}$ esta operación no se sale de S.
- Si ahora tenemos que $g_1 * g_2^{-1} \in S \qquad$ para todo $\qquad g_1, g_2 \in S$, entonces

$$\text{para} \qquad g \in S \Rightarrow g * g^{-1} = e \in S;$$

$$\text{para} \qquad e, g \in S \Rightarrow e * g^{-1} = g^{-1} \in S;$$

$$\text{para} \qquad g_1, g_2 \in S, \text{como} \qquad g_2^{-1} \in S \Rightarrow g_1 * g_2 = g_1 * (g_2^{-1})^{-1} \in S.$$

  Así la operación $*$ sobre S es cerrada, tiene elemento neutro e, cada elemento de S tiene inverso y la operación es asociativa ya que lo es en todo $(\mathbb{G}, *)\square$

Proposición 1. *Sea $(\mathbb{G}, *)$ un grupo y sea $(S_i)_{i \in I}$ una familia de subgrupos de $\mathbb{G}$, es decir $S_i \trianglelefteq \mathbb{G}$ para todo $\ i \in I$, $\ $ donde I es un conjunto de índices. Entonces*

$$S = \bigcap_{i \in I} S_i$$

es un subgrupo de $\mathbb{G}$.

Demostración: Sea $g_1, g_2 \in S$, en particular son elementos de S_i para todo $i \in I$. Por tanto como los S_i son subgrupos se tiene que

$$g_1 * g_2^{-1} \in S_i \qquad \text{para todo} \qquad i \in I.$$

Luego también $g_1 * g_2^{-1} \in S$. Por la caracterización de subgrupo, S lo es$\square$

Definición 2. *Sea $(\mathbb{G}, *)$ un grupo y sea $X \subseteq \mathbb{G}$ un **subconjunto** de $\mathbb{G}$. Se define el **subgrupo generado por** X, escribimos $< X >$, como el menor subgrupo de $\mathbb{G}$ que contiene a X, es decir*

$$< X >= \bigcap_{X \subseteq S \trianglelefteq \mathbb{G}} S.$$

En el caso de que X sea finito, $\ X = \{g_1, g_2, ..., g_n\}$, escribimos también $< X >=< g_1, g_2, ..., g_n >$.

Esta definición es correcta ya que por la Proposición anterior la intersección de subgrupos es de nuevo un subgrupo y además al menos el subgrupo total $\mathbb{G}$ contiene a X.

Ejemplos 2. 1. $\{1\} \subset (\mathbb{Q}, +) \quad \Rightarrow \quad <1>= \mathbb{Z}$.

2. $\{2\} \subset (\mathbb{Q}\backslash\{0\}, \times) \quad \Rightarrow \quad <2>= \{2^m \ : \ m \in \mathbb{Z}\}$.
3. *En* $(\mathbb{Z}, +)$ *se tiene que* $<14, 16, 20>=<2>= 2\mathbb{Z}$.

El caso 3) merece una explicación, los otros son bastante más claros. Primero $<2>= 2\mathbb{Z}$, esto es claro ya que $(2\mathbb{Z}, +)$ es un subgrupo de $(\mathbb{Z}, +)$ que contine al 2 y por tanto tiene que contener a todos sus múltiplos. Luego no hay otro subgrupo más pequeño que contenga al 2.

Ahora, por otro lado, $14, 16, 20 \in 2\mathbb{Z}$, luego $<14, 16, 20>\subseteq<2>$. Y como $2 = 16 - 14 \in<14, 16, 20>$, así $<2>\subseteq<14, 16, 20>$. Ambas inclusiones prueban la igualdad buscada $\Box$

Referencias

Departamento de Análisis Matemático, Facultad de Matemáticas, Universidad Complutense, 28040 Madrid, Spain

E-mail address: Cesar_Ruiz@mat.ucm.es