Estructuras algebraicas

Una **estructura algebraica** es un conjunto no vacío junto con operaciones. Las operaciones pueden ser, por ejemplo, binarias (cuando la operación es sobre dos elementos del conjunto) o unarias (cuando la operación es sobre un elemento del conjunto).

- Por ejemplo, el conjunto de los números reales con la operación binaria de suma es una estructura algebraica que escribimos $(\mathbb{R}, +)$.

$$3 + \sqrt{2}$$

$$-5 + 8 = 3$$

- Si en el conjunto de los enteros definimos la operación unaria op, que da el opuesto, es decir, $op(a) = -a$, entonces $(\mathbb{Z}, op)$ es una estructura algebraica.

$$op(-1) = 1$$
$$op(0) = 0$$

- El conjunto de los números naturales con las operaciones binarias de suma y producto es una estructura algebraica que escribimos $(\mathbb{N}, +, \cdot)$

$$4 + 7 = 11$$

$$23 \cdot 2 = 46$$

Grupos

Un **grupo** $(A,*)$ es una estructura algebraica en la cual $*$ es una operación binaria y se cumple que:

- A es **cerrado** con la operación $*$, es decir, que para todo $a, b \in A$, $a * b \in A$.
- La operación $*$ es **asociativa** en A, es decir, para todo $a, b, c \in A$, $(a * b) * c = a * (b * c)$.
- Existe un **neutro** $n \in A$, es decir, un elemento tal que $a * n = n * a = a$
- Para todo elemento $a \in A$, existe un **opuesto** $a' \in A$ tal que $a * a' = a' * a = n$

¿Es $(\mathbb{Z}, +)$ un grupo?

- Para todo $a, b \in \mathbb{Z}$, $a + x \in \mathbb{Z}$
- Para todo $a, b, c \in \mathbb{Z}$, vale que $(a + b) + c = a + (b + c)$
- Existe el neutro $0 \in \mathbb{Z}$ tal que $a + 0 = 0 + a = a$, para todo $a \in \mathbb{Z}$
- Para todo $a \in \mathbb{Z}$, existe $-a \in \mathbb{Z}$ tal que $a + (-a) = (-a) + a = 0$

¿Es $(\mathbb{Z},\cdot)$ un grupo?

- Para todo $a, b \in \mathbb{Z}$, $a \cdot x \in \mathbb{Z}$
- Para todo $a, b, c \in \mathbb{Z}$, vale que $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- Existe el neutro $1 \in \mathbb{Z}$ tal que $a \cdot 1 = 1 \cdot a = a$, para todo $a \in \mathbb{Z}$
- Para todo $a \in \mathbb{Z}$, ¿existe $a' \in \mathbb{Z}$ tal que $a \cdot a' = a' \cdot a = 1$?

Como la última propiedad no se cumple, no es un grupo.

Un **grupo abeliano/conmutativo** $(A,*)$ es una estructura algebraica en la cual $*$ es una operación binaria y se cumple que:

- A es **cerrado** con la operación $*$, es decir, que para todo $a, b \in A$, $a * b \in A$.
- La operación $*$ es **asociativa** en A, es decir, para todo $a, b, c \in A$, $(a * b) * c = a * (b * c)$.
- Existe un **neutro** $n \in A$, es decir, un elemento tal que $a * n = n * a = a$
- Para todo elemento $a \in A$, existe un **opuesto** $a' \in A$ tal que $a * a' = a' * a = n$
- La operación $*$ es **conmutativa** en A, es decir, para todo $a, b \in A$, $a * b = b * a$

Si definimos sobre $\mathbb{Z}$ la operación Δ como $a\Delta b = a + b + 2$, ¿es $(\mathbb{Z}, \Delta)$ un grupo abeliano?

- Para todo $a, b \in \mathbb{Z}$, $a\Delta b = a + b + 2 \in \mathbb{Z}$.
- Para todo $a, b, c \in \mathbb{Z}$, vale que $(a\Delta b)\Delta c = a\Delta(b\Delta c)$, ya que
$$(a + b + 2) + c + 2 = a + (b + c + 2) + 2$$
- Existe el neutro $-2 \in \mathbb{Z}$ tal que $a\Delta(-2) = a + (-2) + 2 = a$ y $(-2)\Delta a = -2 + a + 2 = a$ para todo $a \in \mathbb{Z}$
- Para todo $a \in \mathbb{Z}$, existe $-a - 4 \in \mathbb{Z}$ tal que $a\Delta(-a - 4) = a + (-a - 4) + 2 = -2$ y $(-a - 4)\Delta a = -a - 4 + a + 2 = -2$.
- Para todo $a, b \in \mathbb{Z}$ tenemos que $a\Delta b = a + b + 2 = b + a + 2 = b\Delta a$.

Si A es un conjunto, definimos el **conjunto de partes de A,** que escribimos $P(A)$, como $P(A) = \{X: X \subseteq A\}$, es decir el conjunto cuyos elementos son los subconjuntos de A.

Si $A = \{1,2,3\}$, entonces $P(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$

Sea A un conjunto, ¿es $(P(A),\cup)$ un grupo abeliano?

- Para todo $B, C \in P(A)$, $B \cup C \in P(A)$

  Si $B, C \in P(A)$, entonces veamos que $B \cup C \in P(A)$, es decir, que $B \cup C \subseteq A$.

  Sea $x \in B \cup C$. Luego, $x \in B \vee x \in C$.

  Como $B \in P(A)$, entonces $B \subseteq A$ y como $C \in P(A)$, entonces $C \subseteq A$.

  Teníamos entonces que $x \in B \vee x \in C$, pero entonces tenemos que $x \in A \vee x \in A$. Por lo tanto, vimos que $B \cup C \subseteq A$.
- Para todo $B, C, D \in P(A)$, $(B \cup C) \cup D = B \cup (C \cup D)$
- Para todo $B \in P(A)$, existe $\emptyset \in P(A)$ tal que $B \cup \emptyset = \emptyset \cup B = B$
- ¿Para todo $B \in P(A)$ existe un opuesto?

Como la última propiedad no se cumple, no es un grupo.

Anillos

Un anillo $(A, +, \cdot)$ es una estructura algebraica en la cual $+$ y $\cdot$ son operaciones binarias que cumplen que:

- $(A, +)$ es un grupo conmutativo/abeliano.
- Para todo $a, b \in A$, $a \cdot b \in A$
- Para todo $a, b, c \in A$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- Para todo $a, b, c \in A$, $a \cdot (b + c) = a \cdot b + a \cdot c$ y $(a + b) \cdot c = a \cdot c + b \cdot c$

¿Es $(\mathbb{R}, +, \cdot)$ un anillo?

- Para todo $a, b \in \mathbb{R}$, $a + b \in \mathbb{R}$
- Para todo $a, b, c \in \mathbb{R}$, $(a + b) + c = a + (b + c)$
- Existe $0 \in \mathbb{R}$ tal que $a + 0 = 0 + a = a$, para todo $a \in \mathbb{R}$
- Para todo $a \in \mathbb{R}$, existe $-a \in \mathbb{R}$ tal que $a + (-a) = -a + a = 0$
- Para todo $a, b \in \mathbb{R}$, $a + b = b + a$
- Para todo $a, b \in \mathbb{R}$, $a \cdot b \in \mathbb{R}$
- Para todo $a, b, c \in \mathbb{R}$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- Para todo $a, b, c \in \mathbb{R}$, $a \cdot (b + c) = a \cdot b + a \cdot c$ y $(a + b) \cdot c = a \cdot c + b \cdot c$

Sea # la operación binaria definida sobre $\mathbb{Q}$ como $a\#b = \frac{a.b}{2}$

¿Es $(\mathbb{Q}, +, \#)$ un anillo?

- Para todo $a, b \in \mathbb{Q}$, $a + b \in \mathbb{Q}$
- Para todo $a, b, c \in \mathbb{Q}$, $(a + b) + c = a + (b + c)$
- Existe $0 \in \mathbb{Q}$ tal que $a + 0 = 0 + a = a$, para todo $a \in \mathbb{Q}$
- Para todo $a \in \mathbb{Q}$, existe $-a \in \mathbb{Q}$ tal que $a + (-a) = -a + a = 0$
- Para todo $a, b \in \mathbb{Q}$, $a + b = b + a$
- Para todo $a, b \in \mathbb{Q}$, $a\#b \in \mathbb{Q}$

$$a\#b = \frac{a.b}{2} \in \mathbb{Q}$$

- Para todo $a, b, c \in \mathbb{Q}$, $(a\#b)\#c = a\#(b\#c)$

$$(a\#b)\#c = \frac{a.b}{2}\#c = \frac{\left(\frac{a.b}{2}\right).c}{2} = \frac{\frac{a.b.c}{2}}{2} = \frac{a.b.c}{4}$$

$$a\#(b\#c) = a\#\frac{b.c}{2} = \frac{a.\frac{b.c}{2}}{2} = \frac{\frac{a.b.c}{2}}{2} = \frac{a.b.c}{4}$$

- Para todo $a, b, c \in \mathbb{Q}$, $a\#(a + c) = a\#b + a\#c$ y $(a + b)\#c = a\#c + b\#c$

$$a\#(b + c) = \frac{a.(b + c)}{2} = \frac{a.b + a.c}{2} = \frac{a.b}{2} + \frac{a.c}{2} = a\#b + a\#c$$

$$(a + b)\#c = \frac{(a + b).c}{2} = \frac{a.c + b.c}{2} = \frac{a.c}{2} + \frac{b.c}{2} = a\#c + b\#c$$