IIC3253

Repaso de teoría de grupos

Grupos

Un grupo es un par $(G, *)$, donde G es un conjunto y $*: G \times G \to G$ es una operación que satisface:

Neutro. Existe $e \in G$ tal que para todo $a \in G$

$$e * a = a * e = a$$

Inversos. Para todo $a \in G$ existe $a^{-1} \in G$ tal que

$$a * a^{-1} = a^{-1} * a = e$$

Asociatividad. Para todos $a, b, c \in G$ se tiene

$$(a * b) * c = a * (b * c)$$

Algunos ejemplos

$$(\mathbb{Z}, +)$$

$$(\mathbb{Q}, +)$$

$$(\mathbb{Q} \setminus \{0\}, \cdot)$$

Algunos ejemplos finitos

$$(\{0,1,2,3\}, + \mod 4)$$

$$(\mathbb{Z}_n, +)$$

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$$

Algunos ejemplos finitos

$$(\{1,2,3,4,5,6\}, \cdot \mod 7)$$

Algunos ejemplos finitos

$$(\{1,2,3,4,5,6\}, \cdot \bmod 7)$$

$$(\mathbb{Z}_n^*, \cdot)$$

$$\mathbb{Z}_n^* = \{a \in \{1, \ldots, n-1\} \mid MCD(a,n) = 1\}$$

Algunos ejemplos finitos

$$(\{1,3,7,9\}, \cdot \bmod 10)$$

$$(\{1,2,4,7,8,11,13,14\}, \cdot \bmod 15)$$

Subgrupos

Un subgrupo de $(G, *)$ es un conjunto $H \subseteq G$ tal que $(H, *)$ también es un grupo.

¿Qué subgrupos tiene $(\mathbb{Z}_{10}, +)$?

¿Qué subgrupos tiene $(\mathbb{Z}_{10}^*, \cdot)$?

Teorema de Lagrange

Si G es un grupo finito y H es un subgrupo de G, entonces $|H|$ divide a $|G|$

¿Cuáles son los tamaños de los subgrupos de $(\mathbb{Z}_{10}, +)$?

¿Cuáles son los tamaños de los subgrupos de $(\mathbb{Z}_{10}^{*}, \cdot)$?

Subgrupos generados

Sea $(G, *)$ un grupo y $a \in G$. Usando notación multiplicativa, definimos

$$a^n = \underbrace{a * \cdots * a}_{n \text{ veces}}$$

Además, definimos $\langle a \rangle = \{a^j \mid j \in \mathbb{N}\}$

Subgrupos generados

Considere $(\mathbb{Z}_{10}, +)$

$$\begin{aligned}
\langle 0 \rangle &= \{0\} \\
\langle 2 \rangle &= \{0, 2, 4, 6, 8\} \\
\langle 3 \rangle &= \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}
\end{aligned}$$

Subgrupos generados

Considere $(\mathbb{Z}_{10}^{*}, \cdot)$

Subgrupos generados

Considere $(\mathbb{Z}_{10}^{*}, \cdot)$

$$\begin{aligned}
\langle 1 \rangle &= \{1\} \\
\langle 3 \rangle &= \{1, 3, 7, 9\} \\
\langle 7 \rangle &= \{1, 3, 7, 9\} \\
\langle 9 \rangle &= \{1, 9\}
\end{aligned}$$

Subgrupos generados

Dado un grupo $(G, *)$ y $a \in G$, tenemos que $(\langle a \rangle, *)$ es un subgrupo de $(G, *)$

Grupos cíclicos

Un grupo $(G, *)$ es cíclico si existe $a \in G$ tal que

$$\langle a \rangle = G$$

$(\mathbb{Z}_{10}, +)$ es cíclico ya que $\langle 3 \rangle = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

$(\mathbb{Z}_{10}^{*}, \cdot)$ es cíclico ya que $\langle 7 \rangle = \{1, 3, 7, 9\}$

¿Son todos los grupos cíclicos?

Muestre que $(\mathbb{Z}_8^*, \cdot)$ no es cíclico

Los grupos $(\mathbb{Z}_p^*, \cdot)$ para p primo

Si p es un número primo, entonces $(\mathbb{Z}_p^*, \cdot)$ es un grupo cíclico

$(\mathbb{Z}_7^*, \cdot)$ es cíclico ya que $\langle 5 \rangle = \{1, 2, 3, 4, 5, 6\}$