Estructuras Álgebraicas

Alejandro Zubiri

Mon Oct 14 2024

1 Grupos

Se define un grupo siguiente la siguiente notación

$$(\mathbb{K}, +) \tag{1}$$

Donde $\mathbb{K}$ es un conjunto y $+$ es una operación entre elementos de dicho conjunto (no necesáriamente la suma). Estos elementos forman un grupo sí:

- La operación es asociativa: $(a + b) + c = a + (b + c)$.
- Existe el elemento neutro con respecto a dicha operación en el conjunto: $\exists e \in \mathbb{K} : x + e = x \forall x \in \mathbb{K}$.
- Existe el inverso para todo elemento: $\forall x \in \mathbb{K} \exists x^{-1} : x + x^{-1} = e$

Además, este grupo puede ser **abeliano** si la operación es **conmutativa**: $a+b = b + a$.

2 Anillos

Un anillo está formado por un conjunto $\mathbb{K}$ y dos operaciones $+, \cdot$. Las condiciones para ser un anillo son:

- $(\mathbb{K}, +)$ forman un grupo abeliano.
- $\cdot$ es una operación asociativa.
- $\cdot$ es distributiva con respecto a $+$.

Además, este anillo puede ser:

- Conmutativo si $\cdot$ es conmutativa.
- Unitario si existe el elemento unitario respecto a $\cdot$: $\exists u \in \mathbb{K} : u \cdot x = x \cdot u = x \forall x \in \mathbb{K}$.

3 Cuerpos

Un anillo $(\mathbb{K};+,\cdot)$ será un cuerpo si:

- Es un anillo unitario.
- Existe un único elemento inverso respecto a $\cdot$ para cada elemento: $\forall x \in \mathbb{K} \exists x^{-1} \in \mathbb{K} : x \cdot x^{-1} = u$

Sin embargo, podemos resumir estas condiciones en:

- $(\mathbb{K};+)$ es un grupo abeliano.
- $(\mathbb{K} \setminus \{0\};\cdot)$ es un grupo abeliano (sin el 0 porque no tiene inverso).
- $\cdot$ es distributivo respecto a $+$.

4 Cuerpos de módulo n

Estos cuerpos se caracterizan por la siguiente notación:

$$\mathbb{K}_n \tag{2}$$

Donde n es el número de elementos del cuerpo. Hablando vulgarmente, estos cuerpos se comportan como un reloj respecto a sus operaciones. Por ejemplo, para $\mathbb{K}_2$, teniendo los elementos $\{0,1\}$, la suma de $1+1 \neq 2$, sino que $1+1=0$. Sería el equivalente a "dar la vuelta".

Definición 1. *Si $\exists n \in \mathbb{Z} : n \cdot 1 = 0$, se dice que tiene característica, m, siendo m el menor entero $/m \cdot 1 = 0$.*

Teorema 1. *Si el subíndice n no es primo, entonces no es un cuerpo.*

Demostración. Supongamos que $n = p \cdot q / p, q \neq 1 \wedge p, q < n$. Entonces

$$n \cdot 1 = (p \cdot q) \cdot 1 = (p \cdot 1)(q \cdot 1) = 0 \implies p \cdot 1 = 0 \vee q \cdot 1 = 0 \tag{3}$$

Lo que implica que la característica es p o q. #
Por tanto n debe ser primo.
QED □