Ayudantía 2 Álgebra Lineal

31 de marzo de 2022

Problema 1. Sea $n \in \mathbb{N}^{\geq 2}$, y $\mathbb{Z}$ el conjunto de los números enteros. Se define sobre este conjunto la relación de **congruencia módulo** n como sigue

$$a\mathcal{R}b \iff \exists k \in \mathbb{Z} \text{ tal que } a - b = nk$$

1. Pruebe que la relación anterior define una relación de equivalencia sobre $\mathbb{Z}$.

2. De ahora en adelante, denotaremos $a\mathcal{R}b$ como $a \equiv b \pmod{n}$ y la clase de equivalencia de $a \in \mathbb{Z}$ como $[a]_n = \{b \in \mathbb{Z} : a \equiv b \pmod{n}\}$. Sea $\mathbb{Z}/n\mathbb{Z}$ el conjunto cociente de $\mathbb{Z}$ por la relación de equivalencia congruencia módulo n. Pruebe que
$$\mathbb{Z}/n\mathbb{Z} = \{[0],[1]_n, \ldots, \{n-1\}_n\}$$
Indicación: Recuerde que para $a, b \in \mathbb{Z}$ con $b \neq 0$ siempre existen únicos enteros $q, r \in \mathbb{Z}$ tales que $a = bq + r$ con $0 \leq r < |b|$,

3. A continuación defina las siguientes operaciones sobre $\mathbb{Z}/n\mathbb{Z}$
$$[a]_n + [b]_n := [a+b]_n \qquad [a]_n \cdot [b]_n := [a \cdot b]_n \qquad \forall a, b \in \mathbb{Z}$$
Pruebe que las operaciones anteriores están bien definidas, i.e., si $a \equiv a' \pmod{n}$ y $b \equiv b' \pmod{n}$ entonces $[a+b]_n = [a'+b']_n$ y $[ab]_n = [a'b']_n$.

4. Demuestre que $(\mathbb{Z}/n\mathbb{Z}, +)$ es un grupo abeliano, i.e., la suma módulo n definida anteriormente es asociativa y conmutativa, posee elemento neutro e inversos. Asimismo, note que $\cdot$ es asociativo, conmutativo y posee neutro. Finalmente, pruebe que $\cdot$ verifica la propiedad distributiva respecto de $+$[1].

5. Demuestre que $a \in \mathbb{Z}$ posee un inverso multiplicativo en $\mathbb{Z}/n\mathbb{Z}$, i.e., existe $b \in \mathbb{Z}$ tal que $[a]_n \cdot [b]_n = 1$ si y solo si $\text{mcd}(a, n) = 1$ en $\mathbb{Z}$, donde mcd denota el máximo común divisor.
Indicación: Tenga presente el siguiente resultado sobre números enteros conocido como Lema de Bézout:

Lema 0.1 (Bézout)**.** *Sean $a, b \in \mathbb{Z}$ no nulos. Entonces existen $x, y \in \mathbb{Z}$ tales que $ax + by = \text{mcd}(a, b)$ donde $\text{mcd}(a, b)$ denota el maáximo común divisor entre a y b.*

6. Concluya que $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ es un cuerpo si y solo si $p \in \mathbb{Z}$ es primo.

Problema 2. Considere el conjunto de **raíces enésimas de la unidad**

$$G = \{z \in \mathbb{C} : z^n = 1 \text{ para algún } n \in \mathbb{N}\}$$

1. Demuestre que G es un grupo junto con la multiplicación usual de números complejos.

2. Pruebe que G no es un grupo con la suma.

Considere ahora el conjunto

$$H = \{a + b\sqrt{2} \in \mathbb{R} : a, b \in \mathbb{Q}\}$$

3. Demuestre que H es un grupo con la suma.

4. Demuestre que H es también un grupo junto con la multiplicación.

[1] Todas estas propiedades se resumen en el hecho de que $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ es un anillo abeliano.

Problema 3. Sea K un cuerpo, $\mathbf{V}$ un espacio vectorial sobre K y S un conjunto.

1. Pruebe que si se tiene una función $f : \mathbf{V} \to S$ biyectiva con inversa $f^{-1} : S \to \mathbf{V}$, entonces el conjunto S posee estructura de espacio vectorial sobre K dada por las operaciones

$$v \oplus w = f(f^{-1}(v) + f^{-1}(w)) \qquad \alpha \odot v = f(\alpha f^{-1}(v)), \qquad \forall \alpha \in K, v, w \in S$$

2. Considere $S = \mathbb{R}^+$. Pruebe que S es un espacio vectorial con las operaciones

$$v \oplus w = vw \qquad \alpha \otimes v = v^\alpha, \qquad \forall \alpha \in K, v, w \in S$$

3. Demuestre que $S = \mathbb{R}$ es un espacio vectorial junto con las operaciones

$$v \oplus w = v + w + 1 \qquad \alpha \otimes v = \alpha v + \alpha - 1, \qquad \forall \alpha \in K, v, w \in S$$