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 $\mathbb{Z}$.

   Demostración. Debemos probar que la relación definida es reflexiva, simétrica y transitiva.

   a) Notemos que para todo $a \in \mathbb{Z}$ se verifica que $a - a = 0$, por lo que tomando $k = 0$ en la definición se tiene que $a\mathcal{R}a$.

   b) Sean $a, b \in \mathbb{Z}$ tales que $a\mathcal{R}b$. Esto significa que existe $k \in \mathbb{Z}$ tal que $a - b = nk$. Por lo tanto $b - a = n(-k)$ y así $b\mathcal{R}a$.

   c) Sean $a, b, c \in \mathbb{Z}$ tales que $a\mathcal{R}b, b\mathcal{R}c$, i.e., existen $k, k' \in \mathbb{Z}$ tales que $a - b = nk$ y $b - c = nk'$. Usando lo anterior vemos que $a - c = (a - b) + (b - c) = nk + nk' = n(k + k')$ y así $a\mathcal{R}c$.

   □

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 $0 \leq r < |b|$.

   Demostración. Consideremos $a \in \mathbb{Z}$ y $[a]_n \in \mathbb{Z}/n\mathbb{Z}$ su clase de equivalencia. Utilizando la indicación, se tiene la existencia de $q, r \in \mathbb{Z}$ tales que $a = nq + r$ con $0 \leq r < n$. Por lo tanto se tiene que $a - r = nq$ y así vemos que $a \equiv r \pmod{n}$. De las propiedades de equivalencia se tiene entonces que $[a]_n = [r]_n$ y así $[a]_n \in \{[0], [1]_n, \ldots, [n-1]_n\}$ pues $0 \leq r < n$. □

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 $[ab]_n = [a'b']_n$.

   Demostración. Verificaremos primero la suma y luego la multiplicación. Sean $a, a', b, b' \in \mathbb{Z}$ tales que $a \equiv a' \pmod{n}$ y $b \equiv b' \pmod{n}$. Por la hipótesis anterior existen $k, k' \in \mathbb{Z}$ de tal manera que $a - a' = nk$ y $b - b' = nk'$. Luego se verifica

   $$(a + b) - (a' + b') = (a - a') + (b - b') = nk + nk' = n(k + k') \Rightarrow a + b \equiv a' + b' \pmod{n}$$

   probando así que la suma en $\mathbb{Z}/n\mathbb{Z}$ está bien definida.
   De forma similar, notamos que

   $$ab = (a' + nk)(b' + nk') = a'b' + a'nk' + nkb' + n^2kk' \Rightarrow ab - a'b' = n(a'k' + kb' + nkk') \Rightarrow ab \equiv a'b' \pmod{n}$$

   □

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].

   Demostración. Probemos en primer lugar los axiomas de grupo para la suma.

   a) **Asociatividad:** Sean $a, b, c \in \mathbb{Z}$. Luego

   $$([a]_n + [b]_n) + [c]_n = [a+b]_n + [c]_n = [(a+b)+c]_n = [a+(b+c)]_n = [a]_n + ([b]_n + [c]_n)$$

   donde se ha utilizado la asociatividad de la suma de enteros.

   b) **Elemento neutro:** Claramente $[0]_n \in \mathbb{Z}/n\mathbb{Z}$ es neutro para la suma pues $[0]_n + [a]_n = [0+a]_n = [a]_n = [a+0]_n = [a]_n + [0]_n$ para todo $a \in \mathbb{Z}$.

   c) **Elemento inverso:** Notamos que para $[a]_n \in \mathbb{Z}/n\mathbb{Z}$ la clase $[-a]_n \in \mathbb{Z}/n\mathbb{Z}$ es un inverso pues

   $$[a]_n + [-a]_n = [a + (-a)]_n = [0]_n$$

   d) **Conmutatividad:** Sean $[a]_n, [b]_n \in \mathbb{Z}/n\mathbb{Z}$. Luego

   $$[a]_n + [b]_n = [a+b]_n = [b+a]_n = [b]_n + [a]_n$$

   en donde se ha utilizado el hecho de que la suma de enteros es conmutativa.

   Se verifican a continuación las propiedades del producto

   a) **Asociatividad:** Sean $a, b, c \in \mathbb{Z}$. Entonces

   $$([a]_n \cdot [b]_n) \cdot [c]_n = [a \cdot b]_n \cdot [c]_n = [(a \cdot b) \cdot c]_n = [a \cdot (b \cdot c)] = [a]_n \cdot [b \cdot c]_n$$

   b) **Elemento neutro:** El elemento $[1]_n \in \mathbb{Z}/n\mathbb{Z}$ es neutro para el producto pues

   $$[a]_n \cdot [1]_n = [a \cdot 1]_n = [a]_n = [1 \cdot a]_n = [1]_n \cdot [a]_n \quad \forall a \in \mathbb{Z}$$

   c) **Conmutatividad:** Para $[a]_n, [b]_n \in \mathbb{Z}/n\mathbb{Z}$ se cumple que

   $$[a]_n \cdot [b]_n = [a \cdot b]_n = [b \cdot a]_n = [b]_n \cdot [a]_n$$

   gracias a la conmutatividad del producto de enteros.

   Para finalizar, verificamos la distributividad del producto con respecto a la suma. Para ello consideremos $[a]_n, [b]_n, [c]_n \in \mathbb{Z}/n\mathbb{Z}$ y notemos que

   $$[a]_n \cdot ([b]_n + [c]_n) = [a]_n[b+c]_n = [a \cdot (b+c)]_n = [a \cdot b + a \cdot c]_n = [a \cdot b]_n + [a \cdot c]_n = [a]_n \cdot [b]_n + [a]_n \cdot [c]_n$$

   gracias a la propiedad de distributividad de los enteros. □

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 máximo común divisor entre a y b.*

   Demostración. Sea $a \in \mathbb{Z}$ y $d = \text{mcd}(a, n)$. Supongamos en primer lugar que existe $b \in \mathbb{Z}$ verificando que $[a]_n \cdot [b]_n = [1]_n$ en $\mathbb{Z}/n\mathbb{Z}$. Por lo tanto $ab \equiv 1 \pmod{n}$ y existe $k \in \mathbb{Z}$ tal que $ab = 1 + nk$. Esto implica que $ab - kn = 1$ y como d divide a a y también divide a n por definición, entonces d divide a 1, deduciendo entonces que $d = 1$.
   Recíprocamente, suponemos que $d = 1$ y veamos que $[a]_n$ posee inverso multiplicativo en $\mathbb{Z}/n\mathbb{Z}$. Por el lema de Bézout existen $x, y \in \mathbb{Z}$ cumpliendo que $ax + ny = 1$ de donde $ax - 1 = n(-y)$ deduciendo que $ax \equiv 1 \pmod{n}$. □

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

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

   Demostración. Sea $p \in \mathbb{Z}$ primo y $[a]_p \in \mathbb{Z}/p\mathbb{Z}$ es no nulo. Entonces se cumple que $\text{mcd}(a, p) = 1$ pues $a \in \{1, 2, \ldots, p-1\}$, y por la parte anterior $[a]_n$ posee inverso multiplicativo en $\mathbb{Z}/p\mathbb{Z}$.
   Ahora, suponiendo por contradicción que $\mathbb{Z}/p\mathbb{Z}$ es cuerpo pero $p \in \mathbb{Z}$ no es primo, entonces $n = ab$ con $1 < b \leq a < n$. Notar entonces que $\text{mcd}(a, n) = a \neq 1$ y por la parte anterior $[a]_n$ no es invertible, lo cual contradice el hecho de que $\mathbb{Z}/p\mathbb{Z}$ sea cuerpo.

   □

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.

   Demostración. Dado que $G \subseteq \mathbb{C}$ y el producto en G es simplemente el producto en $\mathbb{C}$, este hereda sus propiedades y es por lo tanto asociativo y conmutativo. Por otro lado, $1 \in G$ pues $1^1 = 1$, y así G posee identidad. Además, notar que si $z \in G$, i.e., $z^n = z \cdot z^{n-1} = 1$ y así z^{n-1} es un elemento inverso para z, el cual se encuentra en G pues
   $$(z^{n-1})^n = z^{n(n-1)} = (z^n)^{n-1} = 1^{n-1} = 1$$
   de donde deducimos que G posee sus elementos inversos. Finalmente, si $z_1, z_2 \in G$ existen $n_1, n_2 \in \mathbb{N}$ tal que $z_1^{n_1} = z_2^{n_2} = 1$, y comprobamos que $z_1 z_2 \in G$ como sigue
   $$(z_1 z_2)^{n_1 n_2} = (z_1)^{n_1 n_2} (z_2)^{n_1 n_2} = (z_1^{n_1})^{n_2} (z_2^{n_2})^{n_1} = 1^{n_2} 1^{n_1} = 1$$
   Dado que G es cerrado bajo el producto, todo elemento en G posee un inverso en G, $1 \in G$ es un elemento neutro, y el producto es asociativo y conmutativo, concluimos que G es un grupo abeliano. □

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

   Demostración. Basta con notar que $1 \in G$ pero $1 + 1 = 2 \notin G$ por lo que G no es cerrado bajo la suma y en consecuencia no puede ser un grupo con esta operación. □

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.

   Demostración. Como en el caso anterior, ya que $H \subseteq \mathbb{R}$ y la operación considerada es la suma usual, se heredan las propiedades de asociatividad y conmutatividad. Además, es claro que $0 = 0 + 0\sqrt{2} \in G$ es identidad para la suma.
   Considerar ahora $a + b\sqrt{2}, c + d\sqrt{2} \in G$ y notar que
   $$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \in G$$
   y así G es cerrado bajo la suma. Por último, notar que para $a + b\sqrt{2} \in G$, el elemento $(-a) + (-b)\sqrt{2} \in G$ es un inverso pues $(a + b\sqrt{2}) + ((-a) + (-b)\sqrt{2}) = 0$. Así G resulta ser un grupo con la suma. □

4. Demuestre que $H \setminus \{0\}$ es también un grupo junto con la multiplicación.

Demostración. Nuevamente, la operación resulta ser asociativa y conmutativa pues $H\setminus\{0\} \subseteq \mathbb{R}\setminus\{0\}$. Además posee elemento neutro pues $1 = 1 + 0\sqrt{2} \in H \setminus \{0\}$ claramente verifica la propiedad.
Ahora, si $a + b\sqrt{2}, c + d\sqrt{2} \in H \setminus \{0\}$ entonces

$$(a + b\sqrt{2})(c + d\sqrt{2}) = ac + ad\sqrt{2} + bc\sqrt{2} + 2bd = (ac + 2bd) + (ad + bc)\sqrt{2} \in H \setminus \{0\}$$

Resta ver entonces que $H\setminus\{0\}$ posee elementos inversos para la multiplicación. Sea entonces $a+b\sqrt{2} \in H\setminus\{0\}$. Entonces vemos que

$$(a + b\sqrt{2})\frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a^2 - 2b^2}{a^2 - 2b^2} = 1 \Rightarrow (a + b\sqrt{2})^{-1} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \left(\frac{a}{a^2 - 2b^2}\right) + \left(\frac{-b}{a^2 - 2b^2}\right)\sqrt{2} \in H \setminus \{0\}$$

□

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

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

Demostración. Debemos probar en primer lugar que $(S, \oplus)$ es un grupo abeliano.

a) **Asociatividad:** Sean $u, v, w \in S$. Entonces

$$\begin{aligned}(u \oplus v) \oplus w &= f(f^{-1}(u \oplus v) + f^{-1}(w)) \\ &= f[f^{-1}(f[f^{-1}(u) + f^{-1}(v)]) + f^{-1}(w)] \\ &= f([f^{-1}(u) + f^{-1}(v)] + f^{-1}(w)] \\ &\overset{(*)}{=} f(f^{-1}(u) + [f^{-1}(v) + f^{-1}(w)]) \\ &= f(f^{-1}(u) + f^{-1}(f[f^{-1}(v) + f^{-1}(w)]) \\ &= f(f^{-1}(u) + f^{-1}(v \oplus w)) \\ &= u \oplus (v \oplus w)\end{aligned}$$

($*$) La suma en $\mathbf{V}$ es asociativa.

b) **Neutro:** Sea $\mathbf{0} \in \mathbf{V}$ su elemento neutro. Notamos entonces que

$$v \oplus f(\mathbf{0}) = f(f^{-1}(u) + f^{-1}(f(\mathbf{0}))) = f(f^{-1}(u) + \mathbf{0}) = f(f^{-1}(u)) = u \qquad \forall v \in S$$

y de manera similar se observa que $f(\mathbf{0}) \oplus v = v$.

c) **Inverso:** Sea $v \in S$ y denotemos $-v = f(-f^{-1}(v))$. Entonces se cumple

$$\begin{aligned}v \oplus (-v) = f(f^{-1}(v) + f^{-1}(-v)) &= f[f^{-1}(v) + f^{-1}(f(-f^{-1}(v)))] \\ &= f[f^{-1}(v) - f^{-1}(v)] = f(\mathbf{0})\end{aligned}$$

y similarmente $(-v) \oplus v = f(\mathbf{0})$

d) **Conmutatividad:** Basta utilizar la conmutatividad de la suma en $\mathbf{V}$

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

Así, se tiene que $(S, \oplus)$ es un grupo abeliano. Se verifican ahora las propiedades de $\odot$

a) Sean $\alpha \in K, v, w \in S$. Entonces

$$\begin{aligned}\alpha \odot (v \oplus w) = f(\alpha f^{-1}(v \oplus w)) &= f[\alpha f^{-1}(f[f^{-1}(v) + f^{-1}(w)])] \\ &= f[\alpha f^{-1}(v) + \alpha f^{-1}(w)] \\ &= f[f^{-1}(f(\alpha f^{-1}(v))) + f^{-1}(f(\alpha f^{-1}(w)))] \\ &= f[f^{-1}(\alpha \odot u) + f^{-1}(\alpha \odot v)] \\ &= (\alpha \odot u) \oplus (\alpha \odot v)\end{aligned}$$

b) Sean $\alpha, \beta \in K, v \in S$. Verificamos entonces que

$$\begin{aligned}(\alpha + \beta) \odot v = f[(\alpha + \beta) f^{-1}(v)] &= f(\alpha f^{-1}(v) + \beta f^{-1}(v)) \\ &= f[f^{-1}(f[\alpha f^{-1}(v)]) + f^{-1}(f[\beta f^{-1}(v)]))] \\ &= f[f^{-1}(\alpha \odot v) + f^{-1}(\beta \odot v)] \\ &= (\alpha \odot v) \oplus (\beta \odot v)\end{aligned}$$

c) Sean $\alpha, \beta \in K, v \in S$. Entonces

$$\begin{aligned}(\alpha\beta) \odot v = f((\alpha\beta) f^{-1}(v)) &= f(\alpha(\beta f^{-1}(v))) \\ &= f(\alpha f^{-1}[f(\beta f^{-1}(v))]) \\ &= f(\alpha f^{-1}[\beta \odot v]) \\ &= \alpha \odot (\beta \odot v)\end{aligned}$$

d) Sea $1 \in K$ el elemento neutro de $(K \setminus \{0\}, \cdot)$. Entonces se tiene que

$$1 \odot v = f(1 f^{-1}(v)) = f(f^{-1}(v)) = v \qquad \forall v \in S$$

Hemos probado así todas las propiedades que debe satisfacer un espacio vectorial, por lo que se concluye la demostración. □

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

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

Demostración. Consideremos la función $f : \mathbb{R} \to \mathbb{R}^+, x \mapsto e^x$, la cual es biyectiva. Verifiquemos entonces que dicha función induce las operaciones deseadas. En efecto,

$$v \oplus w = f(f^{-1}(v) + f^{-1}(w)) = \exp(\ln(v) + \ln(w)) = \exp(\ln(v)) \exp(\ln(w)) = uv \qquad \forall v, w \in S$$

y además

$$\alpha \odot v = f(\alpha f^{-1}(v)) = \exp(\alpha \ln(v)) = \exp(\ln(v^\alpha)) = v^\alpha$$

Así, por el ejercicio anterior se tiene que las operaciones definidas dotan a $\mathbb{R}^+$ de estructura de espacio vectorial pues encontramos una función que induce dichas operaciones. □

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

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

Demostración. Consideremos ahora la función biyectiva $g : \mathbb{R} \to \mathbb{R}, x \mapsto x - 1$, cuya inversa es claramente $g^{-1} : \mathbb{R} \to \mathbb{R}, x \mapsto x + 1$. Entonces se observa que

$$v \oplus w = g(g^{-1}(u) + g^{-1}(v)) = g((u + 1) + (v + 1)) = g(u + v + 2) = u + v + 1 \qquad \forall v, w \in \mathbb{R}$$

Por otro lado, se tiene que

$$\alpha \odot v = g(\alpha g^{-1}(v)) = g(\alpha(v + 1)) = g(\alpha v + \alpha) = \alpha v + \alpha - 1 \qquad \forall \alpha \in K, v \in \mathbb{R}$$

Se concluye entonces por la parte 1. □