(17) Sabemos que la relación $\{(m,n) : m,n \in \mathbb{Z}$ y $m \equiv n(mod\ 2)\}$ es una relación de equivalencia en $\mathbb{Z}$ y además que $\mathbb{Z}/2\mathbb{Z} = \{0+2\mathbb{Z}, 1+2\mathbb{Z}\}$. Usar lo anterior para demostrar que para todo $m \in \mathbb{Z}$ se cumple una y sólo una de las siguientes afirmaciones:
   (a) $2 \mid m$;
   (b) Existe $n \in \mathbb{Z}$ tal que $m = 2n+1$.

(18) Sea G un semigrupo con la operación $*$; demostrar que para todo $m,n \in \mathbb{N}$ y $a \in G$, se cumple: $a^n * a^m = a^m * a^n$.

(19) Sea G un semigrupo con la operación $*$ y sean $e_0, e_1 \in G$ tales que
   (a) para todo $a \in G$, $e_0 * a = a$ y
   (b) para todo $a \in G$, $a * e_1 = a$.
   Demostrar que G tiene un elemento neutro.

(20) Si e es un elemento neutro de un monoide, entonces para todo $n \in \mathbb{N}$, se tiene que $e^n = e$.

(21) Demostrar que $(\mathbb{N}, +)$ es un semigrupo que no es monoide.

(22) Demostrar que para todo conjunto no vacío A, $(F(A), \circ)$ es un monoide con elemento identidad la funcion $Id_A : A \to A$ definida como $Id_A(a) = a$ para cada $a \in A$.

(23) Sea $I = [0,1]$. Hallar una operación en I tal que I con esta operación sea un monoide.

(24) Sea $G = [0,1] \cap \mathbb{Q}$. Hallar una operación en G tal que G con esta operación sea un monoide.

(25) Hallar una operación en $I = [0,1]$ tal que $G = [0,1] \cap \mathbb{Q}$ sea un submonoide de I.

mismo. De ello se desprende que $T^{-1}\circ\overline{T}(0) = \mathbf{0}$. Debido a que $T^{-1}\circ\overline{T}$ es una traslación concluimos que $T^{-1}\circ\overline{T} = Id_{\mathbb{R}^2}$. En consecuencia $T = \overline{T}$ y la igualdad $T\circ C = \overline{T}\circ\overline{C}$ se convierte, al aplicar T^{-1}, en $C = \overline{C}$. □

Definición III.58. *Si $F = T\circ C$, donde C es una transformación ortogonal de $\mathbb{R}^2$ y T es una traslación de $\mathbb{R}^2$, entonces C se llama la parte ortogonal de la isometría F y T la parte de traslación de F.*

Ejercicios

(1) Sean $(G,*)$ un monoide y $a\in G$. Diremos que a es invertible a izquierda si existe $b\in G$ tal que $b*a = e$ (e es el elemento neutro en G). Diremos que a es invertible a derecha si existe $c\in G$ tal que $a*c = e$. Demostrar que si a es invertible a izquierda y es invertible a derecha, entonces es invertible.

(2) Demostrar que la operación definida en $\mathbb{Z}/n\mathbb{Z}$ como $(m + n\mathbb{Z})\times(r+n\mathbb{Z}) = mr + n\mathbb{Z}$, es asociativa y su elemento neutro es $1+n\mathbb{Z}$.

(3) Probar que cada una de las siguientes parejas es un grupo:

(a) La pareja $(\mathcal{A},\triangle)$. Donde $\mathcal{A} = \mathcal{P}(U)$, el conjunto potencia de un conjunto U y la operación $\triangle$, se define como: para todo $A, B\in\mathcal{A}$: $A\triangle B = ((U\setminus A)\cap B)\cup((U\setminus B)\cap A)$, donde $U\setminus A = \{x\in U : x\notin A\}$, $U\setminus B = \{x\in U : x\notin B\}$ y $\emptyset$ es el elemento neutro.

(b) $(A,+)$, donde $A = \{a+b\sqrt{5} : a,b\in\mathbb{Q}\}$, $+$ es la suma en $\mathbb{R}$ y el neutro es el cero de los reales.

(c) $(A,\circ)$ donde la pareja se define de la siguiente manera. $A = \{E,F,G,H,I,J\}$, donde E,F,G,H,I,J son funciones de $\mathbb{R}\setminus\{0,1\}$ en $\mathbb{R}\setminus\{0,1\}$ tales que $E = Id_{\mathbb{R}\setminus\{0,1\}}$ y para todo $c\in\mathbb{R}\setminus\{0,1\}$: $F(c) = \frac{1}{c}$, $G(c) = 1-c$, $H(c) = \frac{1}{1-c}$, $I(c) = \frac{c-1}{c}$, $J(c) = \frac{c}{c-1}$. En este caso E es el neutro de $(A,\circ)$.

(d) La pareja $(\mathcal{A},\circ)$, donde $\mathcal{A} = \{Id_{\mathbb{R}^3}, T_1, T_2, T_3\}$ con
T_1 gira $\mathbb{R}^3$ 180° alrededor del eje X,
T_2 gira $\mathbb{R}^3$ 180° alrededor del eje Y y
T_3 gira $\mathbb{R}^3$ 180° alrededor del eje Z. Aquí el neutro es $Id_{\mathbb{R}^3}$.

(e) La pareja $(D_4,\circ)$, donde
$D_4 = \{Id_{\mathbb{R}^2}, R_1, R_2, R_3, H, V, D, D'\}$ con
R_1 es la rotación de $\mathbb{R}^2$ en 90°,
R_2 es la rotación de $\mathbb{R}^2$ en 180°,

Todos los ejercicios seleccionados

R_3 es la rotación de $\mathbb{R}^2$ en 270^o,
H es la reflexión respecto al eje X,
V es la reflexión respecto al eje Y,
D es la reflexión respecto a la diagonal $\{(x,x) : x \in \mathbb{R}\}$ y
D' es la reflexión respecto a la diagonal $\{(x,-x) : x \in \mathbb{R}\}$.
Donde el neutro es $Id_{\mathbb{R}^2}$.

(f) $(\mathcal{A}, *)$, donde
$\mathcal{A} = \{I_2, \left(\begin{smallmatrix}-1 & 0\\ 0 & 1\end{smallmatrix}\right), \} \left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right), \left(\begin{smallmatrix}-1 & 0\\ 0 & -1\end{smallmatrix}\right)\}$ y $*$ es el producto de matrices. El neutro es la matriz I_2.

(4) Si U es un conjunto, $\mathcal{P}(U)$ es el conjunto potencia de U, pruebe que $(\mathcal{P}(U), \cup)$, $(\mathcal{P}(U), \cap)$ son monoides pero no son grupos.

(5) Demostrar que $T \subset G$ es un subgrupo de $(G, *)$ si y sólo si
  (a) Para todo $a, b \in T$, se tiene que $a * b \in T$ y
  (b) para todo $a \in T$, se tiene que $a^{-1} \in T$.

(6) Sean $(G_1, *_1)$ y $(G_2, *_2)$ dos grupos, demostrar que la operación $*$ definida en $G_1 \times G_2$ como $(g_1, g_2) * (h_1, h_2) = (g_1 *_1 h_1, g_2 *_2 h_2)$ define en $G_1 \times G_2$ una estrucutra de grupo, es decir $(G_1 \times G_2, *)$ es un grupo.

(7) Considere la matriz $R = \left(\begin{smallmatrix}0 & 1\\ -1 & 0\end{smallmatrix}\right)$. Vea que R tiene orden 4 bajo la multiplicación de matrices, asi que $\{R, R^2, R^3, R^4\}$ es un grupo cíclico. Observe que $R\left(\begin{smallmatrix}x\\ y\end{smallmatrix}\right) = \left(\begin{smallmatrix}y\\ -x\end{smallmatrix}\right)$ e interprete geométricamente el efecto de R.

(8) Demostrar que si $(G, *)$ es un grupo cíclico entonces es un grupo abeliano.

(9) Sea $(G, *)$ un grupo y $a \in G$. Si $aGa^{-1} = \{a * g * a^{-1} : g \in G\}$, demostrar que $(aGa^{-1}, *)$ es un subgrupo de G.

(10) Sea $(G, *)$ un grupo abeliano. Probar que $aGa^{-1} = G$, para todo $a \in G$.

(11) Dar un ejemplo de un grupo $(G, *)$ y elementos $a, b, g \in G$ tales que $b = a * g * a^{-1}$ y $b \neq g$.

(12) Demostrar que $(\mathbb{Z}/n\mathbb{Z}, \oplus)$ es un grupo cíclico. ¡Cuidado con la notación aditiva!

(13) Sea $M_2(\mathbb{Q}) \subset M_2(\mathbb{R})$ donde $A \in M_2(\mathbb{Q})$ si y sólo si

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},$$

y $a_{ij} \in \mathbb{Q}$ para todo $i, j \in \{1, 2\}$. Demostrar que $M_2(\mathbb{Q})$ es un subgrupo de $(M_2(\mathbb{R}), +)$.

(14) Sea $A \in (M_2(\mathbb{R}), +)$ con

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}.$$

Demostrar que para todo $n \in \mathbb{Z}$,

$$nA = \begin{pmatrix} na_{11} & na_{12} \\ na_{21} & na_{22} \end{pmatrix}.$$

(15) Demostrar que en $(In_2(\mathbb{R}), \cdot)$ no se cumple que, para todo $A, B \in In_2(\mathbb{R})$ y $n \in \mathbb{Z}$: $(AB)^n = A^n B^n$ (ver Lema III.12).

(16) Demostrar que si $A \in In_2(\mathbb{R})$, entonces $det(A^{-1}) = \frac{1}{detA}$.

(17) Probar que si

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},$$

entonces $detA^t = detA$ (ver la Definición III.46).

(18) Demostrar que si A es ortogonal entonces $detA = \pm 1$. Además probar el Corolario III.56.

(19) Demostrar que en general si $(G, *)$ es un monoide y $In(G) = \{g \in G : g \text{ es invertible en } (G, *)\}$, entonces $(In(G), *)$ es un grupo.

(20) Si $N_2(\mathbb{R}) = \{A \in In_2(\mathbb{R}) : detA = 1\}$, demostrar que $(N_2(\mathbb{R}), \cdot)$ es un subgrupo de $(In_2(\mathbb{R}), \cdot)$.

(21) Para todo $n \in \mathbb{N}$, se cumple que

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

(22) Sea $D_2(\mathbb{R})$ el conjunto de matrices de la forma

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix},$$

donde $ab \neq 0$. Demostrar que $(D_2(\mathbb{R}), \cdot)$ es un subgrupo de $(In_2(\mathbb{R}), \cdot)$.

(23) Sea $(G, *)$ un grupo finito, es decir, G tiene sólo un número finito de elementos, entonces todo elemento de G tiene orden finito.

(24) Sea $(G, *)$ un grupo finito, denotaremos por $|G|$ la cardinalidad de G, es decir, el número de elementos del conjunto G. Si G es infinito entonces $|G| = \infty$. Demostrar que $|S_n| = n!$.

(25) En general, si $w \in \mathbb{R}^2$, definimos $Tras_w : \mathbb{R}^2 \to \mathbb{R}^2$ como $Tras_w(x) = x + w$, para todo $x \in \mathbb{R}^2$. Demostrar que $Tras_w$ es una isometría.

(26) Demuestre que si $u, v \in \mathbb{R}^2$, entonces
- (a) $Tras_u \circ Tras_v = Tras_{u+v}$,
- (b) $(Tras_u)^{-1} = Tras_{-u}$,
- (c) $Id_{\mathbb{R}^2} = Tras_0$,