Respuestas a los problemas impares del capítulo 9

Semigrupos y monoides

9.1 Es un monoide, con X como elemento identidad.

9.3 Es un monoide con $0 = 2 \cdot 0$ como elemento identidad.

$$a * b = \frac{ab}{2}$$

9.5 Es monoide con $e = 2$ como elemento identidad.

9.7 Por inducción sobre n, siendo m arbitrario pero fijo. El paso inductivo es $(a^m)^{n+1} = (a^m)^n * a^m = a^{mn} * a^m = a^{mn+m} = a^{m(n+1)}$.

Grupos

9.9 No es grupo porque $A \neq X$ no tiene inverso.

9.11 No es grupo porque 1 no tiene inverso.

9.13 Sí es grupo. El elemento identidad es 1 y el inverso de x es $1/x$.

Propiedades de grupos

9.15 $a*x = b \quad\Rightarrow\quad a^{-1}*(a*x) = a^{-1}*b \quad\Rightarrow\quad (a^{-1}*a)*x = a^{-1}*b \quad\Rightarrow\quad x = a^{-1} * b$.

9.17 $(ab)(ab) = e \;\Rightarrow\; (a^2b)(ab) = ae \;\Rightarrow\; b(ab) = a \;\Rightarrow\; b^2ab = ba \;\Rightarrow\; eab = ba \Rightarrow\; ab = ba$.

Subgrupos

9.19 $1 \in \mathbb{R}^+$. Si $x > 0$ y $y > 0$, entonces $xy > 0$, es decir, $x, y \in \mathbb{R}^+ \Rightarrow xy \in \mathbb{R}^+$. Si $x > 0$, entonces $1/x > 0$, es decir, $x \in \mathbb{R}^+ \Rightarrow x^{-1} \in \mathbb{R}^+$.

9.21 $x, y \in N(a) \Rightarrow xa = ax \quad \wedge \quad ya = ay \Rightarrow xay = axy \quad \wedge \quad xya = xay \Rightarrow a(xy) = (xy)a$. Por lo tanto $xy \in N(a)$. El elemento identidad e pertenece a $N(a)$ porque $ea = a = ae$. Por último, $x \in N(a) \Rightarrow xa = ax \Rightarrow x^{-1}(xa) = x^{-1}(ax) \Rightarrow a = x^{-1}ax \Rightarrow ax^{-1} = x^{-1}a$. Por lo tanto $x^{-1} \in N(a)$.

Códigos de grupo

9.23 $W(a) = 4$, $W(b) = 4$, $W(c) = 2$, $W(d) = 5$.

9.25 $H(a, b) = 3$.

9.27 (a) La distancia mínima es 3. (b) Puede detectar 2 errores o menos.

9.29 Sí es código de grupo.

Homomorfismos

9.31 Como el inverso es único, la función $f(a) = a^{-1}$ es biyectiva. $f(ab) = (ab)^{-1} = b^{-1}a^{-1}$. Por otra parte, $f(a)f(b) = a^{-1}b^{-1}$. Por lo tanto f es isomorfismo $\Leftrightarrow a^{-1}b^{-1} = b^{-1}a^{-1} \Leftrightarrow (a^{-1}b^{-1})^{-1} = (b^{-1}a^{-1})^{-1} \Leftrightarrow ba = ab \quad \forall\, a, b \in G \Leftrightarrow G$ es abeliano.

9.33 $f(xy) = a(xy)a^{-1} = (axa^{-1})(aya^{-1}) = f(x)f(y)$.

9.35 $f(n + m) = a^{n+m} = a^n * a^m = f(n) * f(m)$.

9.37 $(g \circ f)(ab) = g(f(ab)) = g(f(a)f(b)) = g(f(a))g(f(b)) = (g \circ f)(a)(g \circ f)(b)$.

9.39 $f(xy) = \log_a(xy) = \log_a x + \log_a y = f(x) + f(y)$. Además en cursos de Cálculo se prueba que $f(x) = \log_a x$ es una función biyectiva de $\mathbb{R}^+$ en $\mathbb{R}$.

9.41 $\hat{e} = f(e) \in Im(f)$. Si $f(a),\ f(b) \in Im(f)$, entonces $f(a)f(b) = f(ab) \in Im(f)$. Si $f(a) \in Im(f)$ entonces $f(a)^{-1} = f(a^{-1}) \in Im(f)$.

Grupos cíclicos

9.43
$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}$$

Por lo que el producto de una matrices es una operación binaria en G. El elemento identidad es la matriz identidad de orden 2, que corresponde a $a = 0$. Obsérvese que

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix} \in G.$$

Por lo tanto G es un grupo, generado por la matriz

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

El teorema de Lagrange

9.45 Por el ejercicio anterior existe m tal que $a^m = e$ y $m|n$, es decir, existe un entero q tal que $n = mq$, de ahí que $a^n = a^{mq} = (a^m)^q = e^q = e$.