Problemas resueltos (Estructuras Algebraicas Abril 2018, UMA)

Alicia Tocino Sánchez

1. Sobre el intervalo $G = (-1, 1)$ de la recta real se define la siguiente operación $x * y = \frac{x+y}{1+xy}$ Demostrad que $(G, *)$ es un grupo abeliano.

Solución. Hay que comprobar que **la operación es interna**, es decir, hay que probar que $-1 < \frac{x+y}{1+xy} < 1$. Esto es lo mismo que $-1 - xy < x + y < 1 + xy$.

Empezamos con la desigualdad de la izquierda. Queremos ver que $0 < x + y + 1 + xy$, o equivalentemente

$$-1 < x + y + xy \tag{1}$$

Sabemos que $-1 < x < 1$ y $-1 < y < 1$. Por tanto, sumando tenemos $-2 < x + y < 2$ y multiplicando tenemos $-1 < xy < 1$. Sumando las dos desigualdades de la izquierdq quedaría $-3 < x + y + xy$. Por lo tanto la desigualdad (1) se verifica.

Veamos ahora que la desigualdad de la derecha se cumple. Queremos ver que

$$0 < 1 + xy - x - y \tag{2}$$

Sabemos que $1 > -x > -1$, $1 > -y > -1$ y $1 > -xy > -1$. Sumando las tres desigualdades tenemos $xy - x - y > -3$, entonces $1 + xy - x - y > -2$. Por lo tanto la desigualdad (2) se cumple.

Para ver que es un grupo abeliano se deben verificar las siguientes condiciones.
Asociativa: Sean $a, b, c \in G$, veamos que $(a * b) * c = a * (b * c)$:

$$(a * b) * c = \frac{a+b}{1+ab} * c = \frac{\frac{a+b}{1+ab} + c}{1 + \frac{a+b}{1+ab}c} = \frac{\frac{a+b+c+abc}{1+ab}}{\frac{1+ab+ac+bc}{1+ab}} = \frac{a+b+c+abc}{1+ab+ac+bc}$$

$$a * (b * c) = a * \frac{b+c}{1+bc} = \frac{a + \frac{b+c}{1+bc}}{1 + a\frac{b+c}{1+bc}} = \frac{\frac{a+abc+b+c}{1+bc}}{\frac{1+bc+ab+ac}{1+ab}} = \frac{a+b+c+abc}{1+ab+ac+bc}$$

Neutro: Si tomamos $e = 0$ entonces $x * e = e * x = x$ para cada $x \in G$.
Inverso: Sea $a \in G$, consideramos el inverso de a como $a' = -a$. Se verifica $a * a' = a * (-a) = \frac{a-a}{1+a(-a)} = e$ y $a' * a = e$.
Conmutativa: Sean $a, b \in G$. Entonces $a * b = \frac{a+b}{1+ab} = \frac{b+a}{1+ba} = b * a$.

2. Sea $n \in \mathbb{Z}$ y consideramos el conjunto

$$G_n = \{\cos\frac{2\pi k}{n} + i \sin\frac{2\pi k}{n} \ : \ k \in \mathbb{Z}\} \subseteq \mathbb{C}$$

equipado con la multiplicación de números complejos. Entonces:

- Probad que $(G_n, \cdot)$ es un grupo.
- Probad que G_n tiene un número finito de elementos.
- Probad que G_n es cíclico.

Solución: Para realizarlo tendremos en cuenta la siguiente igualdad $\cos(\frac{2\pi k}{n}) + i\sin(\frac{2\pi k}{n}) = 1_{\frac{2\pi k}{n}}$.
i: Veamos que es un grupo:

- La operación es interna.
- Asociativa: $(1_{\frac{2\pi k}{n}} 1_{\frac{2\pi l}{n}}) 1_{\frac{2\pi m}{n}} = 1_{\frac{2\pi k}{n}} (1_{\frac{2\pi l}{n}} 1_{\frac{2\pi m}{n}})$
- Neutro: $e = 1_{\frac{2\pi 0}{n}} = 1$
- Inverso: El inverso de $1_{\frac{2\pi k}{n}}$ es $1_{\frac{-2\pi k}{n}}$

ii: Veamos que G_n tiene un número finito de elementos. Los elementos de G_n dependen del valor de $k \in \mathbb{Z}$. Sabemos que:

$$1_{\frac{2\pi 0}{n}} = 1_{\frac{2\pi n}{n}},\ \ 1_{\frac{2\pi 1}{n}} = 1_{\frac{2\pi(n+1)}{n}},\ \ \ldots 1_{\frac{2\pi(-n)}{n}} = 1_{\frac{2\pi 0}{n}},\ \ 1_{\frac{2\pi(-n+1)}{n}} = 1_{\frac{2\pi(-1)}{n}}$$

Por tanto, los valores de k pueden variar entre $-(n-1) \leq k \leq n-1$ concluyendo que hay un número finito de elementos en G_n.
iii: Para ver que G_n es cíclico tenemos que encontrar un elementos $a \in G_n$ tal que $ord(a) = |G_n|$, es decir, $G =< a >= \{a^n | n \in \mathbb{Z}\}$. Tomando $a = 1_{\frac{2\pi 1}{n}}$ tenemos que cualquier $x \in G_n$ se puede escribir como a^k:

$$x = 1_{\frac{2\pi k}{n}} = 1^k_{\frac{2\pi k}{n}} = (1_{\frac{2\pi n}{n}})^k = a^k$$

3. Estudiad las isometrías del plano que dejan invariante un rectángulo. Si se define en este conjunto la operación composición de movimientos, comprobad que tiene estructura de grupo. (Este grupo se llama grupo de KLEIN)

Solución: Visto en clase. Llamamos $K = \{id, \sigma, \theta, \sigma\theta\}$ donde σ es un giro a la izquierda de 180º y θ es una simetría respecto al eje horizontal que divide el rectángulo por la mitad. Se verifica que $\sigma^2 = id$, $\theta^2 = id$ y $(\sigma\theta)^2 = id$.

4. Sea $f : (\mathbb{R}, +) \to (GL_2(\mathbb{R}), \cdot)$ aplicación dada por $f(x) = \begin{pmatrix} \cos x & \sin x \\ -\sin x & \cos x \end{pmatrix}$. Probad que f es un morfismo y calculad su núcleo.

Solución: Veamos que f es un morfismo. Se tiene que verificar que $f(0) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = id$ Veamos ahora que $f(a+b) = f(a)f(b)$. Para comprobar la igualdad será necesario usar las igualdades:

$$\cos(a+b) = \cos(a)\cos(b) - \sin(a)\sin(b), \quad \sin(a+b) = \sin(a)\cos(b) - \sin(b)\cos(a)$$

Entonces,

$$f(a)f(b) = \begin{pmatrix} \cos a & \sin a \\ -\sin a & \cos a \end{pmatrix} \begin{pmatrix} \cos b & \sin b \\ -\sin b & \cos b \end{pmatrix} = \begin{pmatrix} \cos(a+b) & \sin(a+b) \\ -\sin(a+b) & \cos(a+b) \end{pmatrix} = f(a+b)$$

Calculamos el núcleo de f:

$$ker(f) = \{x \in \mathbb{R} \mid \begin{pmatrix} \cos x & \sin x \\ -\sin x & \cos x \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\} = \{2\pi k \mid k \in \mathbb{Z}\}$$

5. Si G es un grupo cíclico, generado por un elemento $a \in G$, probad que cualquier morfismo $f : G \to H$ está unívocamente determinado por $f(a)$.

Solución: Como G es cíclico, está generado por un elementos$a \in G$.

$$G =< a >= \{a^k \ \ \forall k \in \mathbb{Z}\}$$

Entonces $f(x) = f(a^k) = f(a)^k$ por ser f un morfismo.

6. Sea $\mathbb{R}^*$ el grupo multiplicativo de los números reales y sea f la siguiente aplicación

$$f : \mathbb{R}^* \to \mathbb{R}^* \quad x \mapsto x^2$$

- Demostrad que esta aplicación es un homomorfismo de grupos.
- Hallad $Ker(f)$ e $Im(f)$.
- Hallad el grupo cociente $\mathbb{R}^*/Ker(f)$ y la descomposición de f.

Solución: Comprobamos que f es homomorfismo,

$$f(xy) = (xy)^2 = x^2y^2 = f(x)f(y)$$

Calculamos ahora su núcleo y su imagen:

$$Ker(f) = \{x \in \mathbb{R}^* \mid f(x) = 1\} = \{x \in \mathbb{R}^* \mid x^2 = 1\} = \{-1, 1\}$$

$$Im(f) = \{y \in \mathbb{R}^* \mid \text{ existe } x \in \mathbb{R}^* \text{ con } f(x) = y\} = \mathbb{R}^*$$

Veamos cómo son los elementos de $\mathbb{R}^*/Ker(f)$. Sean $x, y \in \mathbb{R}^*$, entonces

$$x \equiv y \text{ si y solo si } xy^{-1} = \frac{x}{y} \in Ker(f) = \{-1, 1\}$$

Tenemos varias opciones: $\frac{x}{y} = 1$ o $\frac{x}{y} = -1$, en cuyos casos, $x = y$ o $x = -y$. Por lo tanto $[x] = [-x]$.

$$\mathbb{R}^*/Ker(f) = \{[x] \,|\, x \in \mathbb{R}^*,\ x \geq 0\}$$

Para dar la descomposición de f consideramos las aplicaciones:

$$\pi : \mathbb{R}^* \to \mathbb{R}^*/Ker(f) \text{ y } \bar{f} : \mathbb{R}^*/Ker(f) \to \mathbb{R}^*$$

De esta forma podemos descomponer f como composición de π y $\bar{f}$: $f = \bar{f} \circ \pi$.

7. Sean n y m enteros positivos. Probad que:

i: $Hom(\mathbb{Z}, \mathbb{Z}) = \{f_a \,|\, a \in \mathbb{Z} \text{ y } f_a(x) = xa \text{ para todo } x \in \mathbb{Z}\}$
ii: $Hom(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}) = \{0\}$
iii: $Hom(\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) = \{f_a \,|\, a \in \{0, 1, \ldots, n-1\} \text{ y } f_a(x) = \widetilde{xa} \text{ para todo } x \in \mathbb{Z}\}$
iv: $Hom(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) = \{f_a(\bar{x}) = \widetilde{ax},\ a = \frac{n}{d}a' \text{ para todo } \bar{x} \in \mathbb{Z}/m\mathbb{Z}\}$, siendo $d = mcd(n, m)$ y $a' \in \{0, 1, \ldots, d-1\}$.

Solución:

i. Veamos primero que $\{f_a \,|\, a \in \mathbb{Z} \text{ y } f_a(x) = xa \text{ para todo } x \in \mathbb{Z}\} \subseteq Hom(\mathbb{Z}, \mathbb{Z})$:

$$f_a(x + y) = a(x + y) = ax + ay = f_a(x) + f_a(y)$$

Veamos ahora que $Hom(\mathbb{Z}, \mathbb{Z}) \subseteq \{f_a \,|\, a \in \mathbb{Z} \text{ y } f_a(x) = xa \text{ para todo } x \in \mathbb{Z}\}$. Sea $g : \mathbb{Z} \to \mathbb{Z}$ un homomorfismo. Hay que ver que dado $g \in Hom(\mathbb{Z}, \mathbb{Z})$ existe $a \in \mathbb{Z}$ tal que $g = f_a$. Sabemos que $g(x + y) = g(x) + g(y)$. Como $\mathbb{Z}$ es cíclico, tiene un generador. Además $Im(f) \leq \mathbb{Z}$ también será ciclico, entonces existe $m \in \mathbb{Z}$ tal que $Im(g) = m\mathbb{Z}$ ya que los únicos subgrupos de $\mathbb{Z}$ son de la forma $n\mathbb{Z}$ para $n \in \mathbb{N}$. Como $\mathbb{Z}$ cíclico, por un ejercicio anterior está unívocamente determinado por f_m.

ii. La aplicación $0 : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}$ que manda $[1] \mapsto 0$ es un morfismo ya que $f([a]) = f([1][a]) = f([1]) + f([a]) = 0 + f([a])$. Además, $< [1] >= \mathbb{Z}/m\mathbb{Z}$ por ser cíclico. Para cada $[x] \in \mathbb{Z}/m\mathbb{Z}$, $[x] = k[1]$. Entonces $f([x]) = f(k[1]) = kf([1]) = k \cdot 0 = 0$ es el único morfismo que existe.

iii. Veamos primero que f_a definido por $f_a(x) = [xa]$ es un homomorfismo. Sea $f_a : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. Entonces $f_a(x + y) = [(x + y)a] = [xa + ya] = [xa] + [ya] = f_a(x) + f_a(y)$. Veamos ahora que cualquier homomorfismo se define como $f_a(x) = [xa]$ para algún $a \in \mathbb{Z}$. Sea $g : \mathbb{Z} \to \mathbb{Z}/nZ$ que

manda $1 \mapsto [a]$. Como $\mathbb{Z}$ cíclico, $x = x \cdot 1 = 1 + \ldots + 1 \Rightarrow g(x) = g(x \cdot 1) = g(1 + \ldots + 1) = g(1) + \ldots + g(1) = [a] + \ldots + [a] = x[a] = [xa = f_a(x)]$.

8. Sean $m, n \in \mathbb{Z}^+ - \{0\}$.

i: Probad que si existe un homomorfismo inyectivo de $\mathbb{Z}/m\mathbb{Z}$ en $\mathbb{Z}/n\mathbb{Z}$ entonces $m|n$.

ii: Si $m|n$ y para cada $a' \in \{0, 1, \ldots, m-1\}$ consideramos $f_a \in Hom(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ definido por $f_a(\bar{x}) = \widetilde{\frac{n}{m}xa'}$ probad que f_a es inyectivo si y sólo si $mcd(a', m) = 1$.

Solución:

i: Como $f$es inyectivo, entonces $ord(Im(f)) = m$. Como $Im(f) \leq \mathbb{Z}/n\mathbb{Z}$ entonces $m = ord(Im(f))|ord(\mathbb{Z}/n\mathbb{Z})$ n por el Teorema de Lagrange.

ii: Veamos una serie de datos equivalentes: $[x] \in Ker(f_a)$ si y solo si $[\frac{n}{m}a'x] = [0]$ en $Z/n\mathbb{Z}$ si y solo si $\frac{n}{m}a'x = tn$ para cierto $t \in \mathbb{Z}$ si y solo si $na'x = mnt$ si y solo si $a'x = mt$ si y solo si $m|a'x$ si y solo si $m|x$. Por tanto:

$$f_a \text{ es inyectivo si y solo si } m|x$$

Veamos primero la implicación de izquierda a derecha de (**ii**). Supongamos $mcd(a', m) = 1$ y $m|a'x$. Entonces $m|x$ si y sólo si $[x] = [0]$ en $\mathbb{Z}/n\mathbb{Z}$. Esto es equivalente a que f_a sea inyectiva.

Veamos ahora la implicación de izquierda a derecha de (**ii**). Los probamos por el contrarecíproco. Sea $1 \neq d = mcd(a', m)$, entonces existe $0 < m' < m$ y $a'' < a'$ tal que $m = dm'$ y $a' = da''$. De aquí,

$$f_a([m']) = [\frac{n}{m}a'm'] = [\frac{n}{m}a''dm'] = [\frac{n}{m}a''m] = [na''] = [0]$$

Entonces, $[m'] \neq [0]$ en $\mathbb{Z}/n\mathbb{Z}$ y por lo tanto f_a no es inyectiva.

9. Sean $m, n \in \mathbb{Z}^+ - \{0\}$ y $d = mcd(m, n)$.

i: Probad que si existe un homomorfismo sobreyectivo de $\mathbb{Z}/m\mathbb{Z}$ en $\mathbb{Z}/n\mathbb{Z}$ entonces $n|m$.

ii: Si $n|m$ y para todo $a \in \{0, 1, \ldots, d-1\}$ consideramos $f_a \in Hom(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})$ definido por $f_a(\bar{x}) = \widetilde{ax}$, probad que f_a es sobreyectiva si y sólo si $mcd(a, n) = 1$.

Solución:

i: Supongamos $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ sobreyectiva. Entonces $< f([1]) >= Im(f) = \mathbb{Z}/n\mathbb{Z}$. Entonces $ord(f([1])) = ord(\mathbb{Z}/n\mathbb{Z}) = n$. Como $n = ord(f([1]))$ divide a $ord([1]) = m$ tenemos que $n|m$.

ii: Sea $f : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ que manda $[1] \mapsto [a]$. Sabemos que f es un epimorfismo si y sólo si existe $[x] \in \mathbb{Z}/m\mathbb{Z}$ tal que $[ax] = [1]$. Pero $[ax] + [nt] = 1$ para algún $t \in \mathbb{Z}$ (donde $[nt] = [0]$) si y sólo si $mcd(a, n) = 1$ por la identidad de Bezout.

10. Sea G un grupo y H un subgrupo de G definido por $H = \{x^2 \,|\, x \in G\}$. Probar que H es un subgrupo normal de G y que G/H es abeliano.

Solución: Queremos ver que $H = a^{-1}Ha$ para todo $a \in G$. Trivialmente tenemos que $H \subseteq a^{-1}Ha$. Hay que ver que $a^{-1}Ha \subseteq H$. Sea $x \in H$, entonces $x = y^2$. Veamos que $a^{-1}xa \in H$.

$$a^{-1}xa = a^{-1}y^2a = a^{-1}y1ya = a^{-1}yaa^{-1}ya = (a^{-1}ya)(a^{-1}ya) = (a^{-1}ya)^2 \in H \text{ ya que } a^{-1}ya \in G.$$

Como H es un subgrupo normal G/H tiene orden 2. Todo grupo de orden 2 es abeliano.

11. Sea G grupo, y H un subgrupo de G. Se define el conjunto $N = \cap_{x\in G} xHx^{-1}$. Probar que N es un subgrupo normal de G.

Solución: Queremos ver que $N = aNa^{-1}$. Sabemos que $N \subseteq aNa^{-1}$. Veamos la otra contención ($aNa^{-1} \subseteq N$).

$$aNa^{-1} = a(\cap_{x\in G} xHx^{-1})a^{-1} * = * \cap_{x\in G} axHx^{-1}a^{-1} = \cap_{x\in G}(ax)H(ax)^{-1} = \cap_{y\in G} yHy^{-1} = N$$

El único paso dudoso es la igualdad entre asteriscos ($* = *$). Tenemos que tener en mente que sólo queremos la contención, no la igualdad. Entonces, sea $t \in a(\cap_{x\in G} xHx^{-1})a^{-1}$ donde $t = asa^{-1}$ con $s \in \cap_{x\in G} xHx^{-1}$. Por tanto $t = asa^{-1}$ donde $s \in xHx^{-1}$ para cada $x \in G$. De ahí que, $t = asa^{-1}$ con $s = xhx^{-1}$ para algún $h \in H$ y para cada $x \in G$. Luego,

$$t = asa^{-1} = a(xhx^{-1})a^{-1} = (ax)h(x^{-1}a^{-1}) = (ax)h(ax)^{-1}$$

donde h depende de x y no de a. Por tanto, $t \in (ax)H(ax)^{-1}$ para cada $x \in G$, de ahí que $t \in \cap_{x\in G}(ax)H(ax)^{-1}$ como queríamos ver.