ESTRUCTURAS ALGEBRAICAS. Problemas. 14 de Septiembre.

Ejercicio 1. Hoja 1. Se consideran en $\mathbb{R}^2$ los dos ejes OX y OY. Sea

$$V = \{\iota,\, \sigma_0,\, \sigma_X,\, \sigma_Y\},$$

donde ι es la aplicación identidad en $\mathbb{R}^2$; σ_0, σ_X y σ_Y son las simetrías respecto al origen, y respecto a los ejes OX y OY, respectivamente. Demostrad que $(V, \circ)$ es un grupo, donde $\circ$ es la composición de aplicaciones. Hallad la tabla de $(V, \circ)$, llamado el *grupo de Klein*.

Solución:

Recordamos que los elementos de V, como aplicaciones de $\mathbb{R}^2$ en $\mathbb{R}^2$, vienen dados por:

$$\iota(x,y) = (x,y), \quad \sigma_0(x,y) = (-x,-y), \quad \sigma_X(x,y) = (x,-y), \quad \sigma_Y(x,y) = (-x,y) \quad \text{para cada } (x,y) \in \mathbb{R}^2$$

Describimos la tabla de la operación composición al aplicarla sobre V:

$\circ$	ι	σ_0	σ_X	σ_Y
ι	ι	σ_0	σ_X	σ_Y
σ_0	σ_0	ι	σ_Y	σ_X
σ_X	σ_X	σ_Y	ι	σ_0
σ_Y	σ_Y	σ_X	σ_0	ι

Finalmente, comprobamos que $(V, \circ)$ satisface las propiedades de grupo:

(G0) V es un conjunto cerrado para la composición de funciones.

(G1) La asociatividad se hereda de la asociatividad para la composición de funciones de $\mathbb{R}^2$ en $\mathbb{R}^2$.

(G2) El elemento identidad es ι.

(G3) Todo elemento de V tiene inverso en V:

$$\iota^{-1} = \iota, \quad \sigma_0^{-1} = \sigma_0, \quad \sigma_X^{-1} = \sigma_X, \quad \sigma_Y^{-1} = \sigma_Y$$

(C) Además, como comprobamos en la tabla, la composición es conmutativa en V.

Por tanto, el grupo de Klein $(V, \circ)$ es un grupo abeliano.

Ejercicio 2. Hoja 1. En el intervalo $G = (-1, 1)$ de la recta real se define la siguiente operación:

$$x * y = \frac{x+y}{1+xy} \quad \text{para } x, y \in G.$$

¿Es $(G, *)$ un grupo?

Solución:

Comprobamos que la operación $*$ está bien definida en G, es decir, que para todo $x, y \in G$

$$1 + xy \neq 0 \quad \text{y} \quad \left|\frac{x+y}{1+xy}\right| < 1$$

Para todo $x, y \in G$, tenemos que $|xy| < 1$. Por lo que, $1 + xy > 0$. Falta ver que $|x+y| < 1+xy$. Supongamos que no fuera así, es decir, $|x+y| \geq 1+xy$, entonces:

- O bien, $x+y \geq 1+xy$. Lo que implicaría que $y(1-x) \geq (1-x)$ y, en consecuencia, tendríamos $y \geq 1$, una contradicción.
- O bien, $x+y \leq -1-xy$. Lo que implicaría que $y(1+x) \leq -(1+x)$ y, en consecuencia, tendríamos $y \geq -1$, una contradicción.

Por tanto, se tiene que $|x+y| < 1+xy$ para todo $x, y \in G$. Veamos si $(G, *)$ cumple las propiedades de grupo:

(G1) Asociatividad. Sean $x, y, z \in G$:

$$(x*y)*z = \left(\frac{x+y}{1+xy}\right)*z = \frac{\frac{x+y}{1+xy}+z}{1+\frac{x+y}{1+xy}z} = \frac{x+y+z+xyz}{1+xy+xz+yz} = \frac{x+\frac{y+z}{1+yz}}{1+\frac{y+z}{1+yz}x} = x*\left(\frac{y+z}{1+yz}\right) = x*(y*z)$$

(G2) Elemento identidad. Sean $x, y \in G$:

$$x*y = x \implies \frac{x+y}{1+xy} = x \implies x^2y - y = 0 \implies y(x^2-1) = 0 \underset{|x|<1}{\implies} y = 0$$

Como $0*x = x = x*0$, 0 es el elemento identidad.

(G3) Elemento inverso. Sean $x, y \in G$:

$$x*y = 0 \implies \frac{x+y}{1+xy} = 0 \implies x+y = 0 \implies y = -x$$

Como $x*(-x) = 0 = (-x)*x$, entonces $x^{-1} = -x$ para cada $x \in G$.

(C) Además, de la simetría en la expresión de $x*y$, deducimos que $x*y = y*x$ para todo $x, y \in G$.

Por tanto, $(G, *)$ es un grupo abeliano.

Ejercicio 3. Hoja 1. Sea G un grupo. Demostrad que las siguientes condiciones son equivalentes.

(a) G es abeliano.

(b) $(ab)^2 = a^2b^2$ para todo $a, b \in G$.

(c) $(ab)^{-1} = a^{-1}b^{-1}$para todo $a, b \in G$.

Solución:

(a) $\implies$ (b) Supongamos que G es un grupo abeliano. Para todo $a, b \in G$, tenemos que:

$$(ab)^2 = ab \cdot ab = a \cdot a \cdot b \cdot b = a^2b^2.$$

(b) $\implies$ (c) Supongamos que $(ab)^2 = a^2b^2$ para todo $a, b \in G$. Entonces:

$$ab \cdot ab = a^2 \cdot b^2 \underset{a^{-1}\cdot}{\implies} b \cdot ab = a \cdot b^2 \underset{\cdot b^{-1}}{\implies} b \cdot a = a \cdot b \implies (b \cdot a)^{-1} = (a \cdot b)^{-1} \implies a^{-1} \cdot b^{-1} = (a \cdot b)^{-1}$$

(c) $\implies$ (a) Supongamos que $(ab)^{-1} = a^{-1}b^{-1}$ para todo $a, b \in G$. Entonces:

$$ab \cdot a^{-1}b^{-1} = e \underset{\cdot b}{\implies} aba^{-1} = b \underset{\cdot a}{\implies} ab = ba.$$

Ejercicio 4. Hoja 1. Demostrad que un grupo G en el que todo $g \in G$ satisface $g^2 = 1$ es necesariamente abeliano.

Solución:

Supongamos que $g^2 = 1$ para todo $g \in G$. Entonces $g^{-1} = g$. Para todo $g, h \in G$, tenemos que

$$gh = g^{-1}h^{-1} = (hg)^{-1} = hg.$$

Por tanto, G es un grupo abeliano.

Ejercicio 5. Hoja 1. Demostrad que para que un subconjunto, distinto del vacío, de un grupo finito sea subgrupo basta que sea cerrado para la operación. Encontrad un contraejemplo en un grupo infinito.

Solución:

Sea G un grupo finito, con $|G| = n$. Supongamos que $H \subseteq G$ es un subconjunto no vacío cerrado para la operación de G. Veamos que H satisface las propiedades de subgrupo:

(S1) Por hipótesis, H es cerrado para la operación de G.

(S2) Para cada elemento $h \in H$, tenemos que $e_G = h^n \in H$. La igualdad es consecuencia de que h pertenece a G y la inclusión se deduce de la propiedad $(S1)$.

(S3) Para cada $h \in H$, como elemento de G, tenemos que $\mathrm{o}(h)$ es finito, digamos $\mathrm{o}(h) = m$. Entonces

$$e_G = h^m = h \cdot h^{m-1} \implies h^{-1} = h^{m-1}$$

Por (S1), concluimos que $h^{-1} \in H$.

El resultado no es cierto en general si el grupo es infinito. Consideramos el grupo multiplicativo $\mathbb{Q}^*$ y el subconjunto no vacío de las potencias positivas de 2, esto es, $H = \{2^n \ : \ n \geq 1\}$.

(S1) H es cerrado para la multiplicación, pues para todo $n, m \geq 1$ tenemos que $2^n \cdot 2^m = 2^{n+m}$, con $n + m \geq 1$.

(S2) Sin embargo, H no contiene al elemento neutro de $\mathbb{Q}^*$. Puesto que $1 = 2^0$, pero $0 < 1$.

(S3) Tampoco se cumple la propiedad de los inversos. Puesto que para cada elemento $2^n \in H$, su inverso es 2^{-n}, pero $-n < 1$. Por lo que, $(2^n)^{-1} \notin H$.

Ejercicio 17. Hoja 1. Demostrad que si un grupo G tiene orden par, entonces existe un elemento $g \neq 1$ de G que es su propio inverso. (Es decir, los grupos de orden divisible por 2 tienen al menos un elemento de orden 2.)

Solución:

Supongamos que $|G| = 2n$ y que ninguno de los elementos no neutros es su propio inverso. Entonces $|G\backslash\{e\}| = 2n - 1$. El inverso de un elemento es único y $(g^{-1})^{-1} = g$ para todo $g \in G$. Por tanto, si cada elemento de $G\backslash\{e\}$ tiene un inverso distinto de sí mismo, necesariamente $|G\backslash\{e\}|$ es un número par, dando lugar a una contradicción. Por tanto, existe al menos un elemento de $G\backslash\{e\}$ cuyo inverso es él mismo.

Ejercicio 21. Hoja 1. Sea G un grupo abeliano y $n \in \mathbb{N}$. ¿Es $G_n = \{x \in G \mid o(x) \text{ divide a } n\}$ un subgrupo de G? ¿Ocurre lo mismo si G no es abeliano?

Solución:

Si G es abeliano, G_n es un subgrupo. Basta con comprobar que G_n cumple las propiedades $(S1)$ y $(S3)$.

(S1) Sean $x, y \in G_n$. Denotamos $r = \mathrm{o}(x)$, $s = \mathrm{o}(y)$ y $t = \mathrm{mcm}(r, s)$. Veamos que $\mathrm{o}(xy) \mid t$:

$$(xy)^t = x^t y^t = x^{ar} y^{bs} = (x^r)^a (y^s)^b = 1.$$

Usando que G es abeliano en la primera igualdad. Nuestra hipótesis es que $r \mid n$ y $s \mid n$. Entonces n es un múltiplo común de r y s. Como $\mathrm{o}(xy)$ divide a t, que es el mínimo común múltiplo, entonces tenemos que $\mathrm{o}(xy) \mid n$. Por lo que, $xy \in G_n$.

(S3) Sea $x \in G_n$. Sabemos que $\mathrm{o}(x) = \mathrm{o}(x^{-1})$. Por lo que, $\mathrm{o}(x^{-1}) \mid n$ y concluimos que $x^{-1} \in G_n$.

Si el grupo G no es abeliano, G_n puede no ser un subgrupo. Consideramos $G = S_3$ y el conjunto $G_2 \subset G$. Se tiene que

$$G_2 = \{\sigma \in S_3 : \mathrm{o}(\sigma) \mid 2\} = \{\sigma \in S_3 : \mathrm{o}(\sigma) = 1, 2\} = \left\{(1), \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\right\}$$

Sin embargo, el producto de los elementos $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \in G_2$ es el 3-ciclo $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ que tiene orden 3, que no divide a 2. Por tanto, G_2 no es cerrado para la operación de S_3.

Ejercicio 23. Hoja 1. Encontrad el número de elementos de cada uno de los grupos cíclicos indicados:

(a) El subgrupo de $\mathbb{Z}/30\mathbb{Z}$ generado por la clase de $25 \in \mathbb{Z}$.

(b) El subgrupo de $\mathbb{C}^*$ generado por i.

(c) El subgrupo de $\mathbb{C}^*$ generado por $\frac{1+i}{\sqrt{2}}$.

(d) El subgrupo de $\mathbb{C}^*$ generado por $1 + i$.

Solución:

(a) Calculamos el orden del elemento [25]:

$[25] \neq [0]$, $2{\cdot}[25] = [50] = [20]$, $3{\cdot}[25] = [45] = [15]$. $4{\cdot}[25] = [40] = [10]$, $5{\cdot}[25] = [35] = [5]$, $6{\cdot}[25] = [30] = [0]$.

Por tanto, $\mathrm{o}([25]) = 6$. Alternativamente, como [1] es un generador de $\mathbb{Z}/30\mathbb{Z}$ y $[25] = 25 \cdot [1]$, tenemos

$$\mathrm{o}([25]) = \mathrm{o}(25 \cdot [1]) = \frac{\mathrm{o}([1])}{(\mathrm{o}([1], 25))} = \frac{30}{5} = 6.$$

(b) Calculamos el orden del elemento i:

$$i \neq 1, \quad i^2 = -1 \quad i^3 = -i, \quad i^4 = 1.$$

Por tanto, $\mathrm{o}(i) = 4$.

(c) Calculamos el orden del elemento $\frac{1+i}{\sqrt{2}}$:

$$\frac{1+i}{\sqrt{2}} \neq 1, \quad \left(\frac{1+i}{\sqrt{2}}\right)^2 = i, \quad \left(\frac{1+i}{\sqrt{2}}\right)^3 = \frac{-1+i}{\sqrt{2}}, \quad \left(\frac{1+i}{\sqrt{2}}\right)^4 = -1.$$
$$\left(\frac{1+i}{\sqrt{2}}\right)^5 = \frac{-1-i}{\sqrt{2}}, \quad \left(\frac{1+i}{\sqrt{2}}\right)^6 = -i, \quad \left(\frac{1+i}{\sqrt{2}}\right)^7 = \frac{1-i}{\sqrt{2}}, \quad \left(\frac{1+i}{\sqrt{2}}\right)^8 = 1.$$

Por tanto, $\mathrm{o}\left(\frac{1+i}{\sqrt{2}}\right) = 8$.

(d) Calculamos el orden del elemento $1+i$. Para cada $n \in \mathbb{N}$, tenemos que $|(1+i)^n| = \sqrt{2}^n$. Si $(1+i)^n = 1$, entonces $\sqrt{2}^n = 1$. Pero esto solo sucede si $n = 0$. Por tanto, $\mathrm{o}(1+i) = \infty$.

Ejercicio 25. Hoja 1. Decide razonadamente si cada una de las siguientes afirmaciones es verdadera o falsa:

(a) Todo grupo cíclico es abeliano.

(b) Todo grupo abeliano es cíclico.

(c) El grupo aditivo $\mathbb{Q}$ es cíclico.

(d) Todo elemento no trivial de un grupo cíclico es generador.

(e) Todo grupo de orden menor o igual que 4 es cíclico.

(f) Todo grupo cíclico de orden mayor que 2 tiene al menos dos generadores distintos.

Solución:

(a) *Verdadero.* Sea $G = \langle g \rangle$. Todo elemento $a, b \in G$ se expresa como $a = g^i$ y $b = g^j$, para ciertos enteros i, j. Por tanto, tenemos que

$$ab = g^i g^j = g^{i+j} = g^j g^i = ba.$$

Entonces el grupo G es conmutativo.

(b) *Falso.* El grupo $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ es abeliano, pero no es un grupo cíclico. El orden del grupo es 4, pero todos los elementos no triviales tienen orden 2. Es decir, no existe ningún elemento de orden 4 que genere todo el grupo.

(c) *Falso.* El grupo aditivo $\mathbb{Q}$ no es cíclico. Supongamos que fuera cíclico, entonces estaría generado por un elemento $\frac{r}{s}$, con r, s enteros no nulos y coprimos entre sí. Es decir, $\mathbb{Q}$ sería el conjunto de los múltiplos enteros de $\frac{r}{s}$:

$$\mathbb{Q} = \left\langle \frac{r}{s} \right\rangle = \left\{ k \cdot \frac{r}{s} : k \in \mathbb{Z} \right\}$$

Consideramos el elemento $\frac{r}{2s}$. Claramente es un número racional, pero no es un múltiplo entero de $\frac{r}{s}$, puesto que $\frac{r}{2s} = \frac{1}{2} \cdot \frac{r}{s}$. Por tanto, $\mathbb{Q}$ no puede ser cíclico.

(d) *Falso.* Consideramos el grupo cíclico $\mathbb{Z}/4\mathbb{Z}$. Observamos que el elemento $[2]_4$ tiene orden 2, por lo que, no es un generador.

Afirmación. Sea $G = \langle g \rangle$ un grupo cíclico. Un elemento g^k es un generador si y solo si $(k, \mathrm{o}(g)) = 1$.

(e) *Falso.* El grupo $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ tiene orden 4, pero no es un grupo cíclico como vemos en el apartado (b).

(f) *Verdadero.* Sea $G = \langle g \rangle$ un grupo cíclico tal que $|G| > 2$. Sabemos que $\mathrm{o}(g) = \mathrm{o}(g^{-1})$. Por tanto, g^{-1} es un generador de G. Veamos que $g \neq g^{-1}$. Si no fuera así, entonces $g^2 = e$. Por lo que, $\mathrm{o}(g) \leq 2$. Como g es un generador, esto implica que $|G| = \mathrm{o}(g) \leq 2$, dando lugar a una contradicción.