SOLUCIONES

1. Estudia si las siguientes afirmaciones son verdaderas o falsas. Justifica tu repuesta.

a) Todo grupo finito que no tiene subgrupos no triviales tiene orden primo o uno.

Solución: Verdadero. Sea G es un grupo de orden no primo y distinto de 1; veamos que tiene subgrupos distintos de $\{1\}$ y G. Tomemos un elemento $x \in G$ distinto de 1. Si $\langle x \rangle \neq G$ hemos terminado. Si no, podemos suponer que $|x| = n$ no es primo. Si p es un primo que divide a n, entonces $\langle x^p \rangle$ es un subgrupo de $\langle x \rangle$ distinto de $\langle x \rangle$, luego también de G.

b) Sea G un grupo y $f : G \to G$ la aplicación definida por $f(x) = x^{-1}$. Entonces, f es isomorfismo si y sólo si G es abeliano.

Solución: Verdadero. Claramente f es siempre una biyección, ya que $x^{-1} = 1$ sólo si $x = 1$ y además $x = (x^{-1})^{-1}$. Sólo hay que ver cuándo f es homomorfismo. Pero como $(xy)^{-1} = y^{-1}x^{-1}$ tenemos que

$$f(xy) = f(x)f(y) \Leftrightarrow y^{-1}x^{-1} = x^{-1}y^{-1} \Leftrightarrow yx = xy$$

luego f es homomorfismo si y sólo si $yx = xy$ para todo $x, y \in G$.

c) Si $n \geq 5$ y $\alpha \in S_n$ es tal que $\alpha(1) = a$, $\alpha(3) = b$, $\alpha(5) = c$, entonces $\alpha(135)\alpha^{-1} = (abc)$.

Solución: Verdadero. Sea $\gamma = \alpha(135)\alpha^{-1}$. Tenemos que

$$\gamma(a) = \alpha(135)(1) = \alpha(3) = b,$$

y de la misma forma $\gamma(b) = c$ y $\gamma(c) = a$. Por otra parte, si $x \notin \{a, b, c\}$, entonces $y = \alpha^{-1}(x)$ tampoco pertenece a $\{a, b, c\}$, luego

$$\gamma(x) = \alpha(135)(y) = \alpha(y) = x.$$

Por tanto $\gamma(t) = (abc)(t)$ para todo $t \in \{1, \dots n\}$.

---

2. Sea $\zeta \in \mathbb{C}$ tal que $\zeta \neq 1$, $\zeta^3 = 1$. Considera el conjunto:

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^2 \end{pmatrix}, \begin{pmatrix} \zeta^2 & 0 \\ 0 & \zeta \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \zeta \\ \zeta^2 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \zeta^2 \\ \zeta & 0 \end{pmatrix} \right\}$$

a) Demuestra que G es un grupo.

Solución: Como G es finito y $G \subset GL(2, \mathbb{C})$, con $GL(2, \mathbb{C})$ el grupo de matrices con coeficientes en $\mathbb{C}$ y determinante distinto de cero, sólo debemos comprobar que G es cerrado por la operación multiplicación de matrices. En principio tendríamos que comprobar $6 * 6 = 36$ multiplicaciones, pero se puede hacer mucho más rápido. Sean

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad x = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^2 \end{pmatrix}, \qquad y = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Tenemos que

$$x^2 = \begin{pmatrix} \zeta^2 & 0 \\ 0 & \zeta \end{pmatrix}, \qquad xy = \begin{pmatrix} 0 & \zeta \\ \zeta^2 & 0 \end{pmatrix}, \qquad x^2y = \begin{pmatrix} 0 & \zeta^2 \\ \zeta & 0 \end{pmatrix},$$

luego $G = \{e, x, x^2, y, xy, x^2y\}$ y para demostrar que es subgrupo es suficiente ver que $G = \langle x, y \rangle$. Pero

$$x^3 = e, \qquad y^2 = e, \qquad yx = x^2y$$

luego $G = \langle x, y \rangle$.

b) ¿Es G isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_3$?
<u>*Solución*</u>: G no es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_3$, porque $yx = x^2y$ luego G no es abeliano, mientras que $\mathbb{Z}_2 \times \mathbb{Z}_3$ sí lo es.

c) Haz una lista de los grupos no isomorfos de orden 6 y señala justificadamente a cuál es isomorfo G.
<u>*Solución*</u>: Hay dos grupos no isomorfos de orden 6, $\mathbb{Z}_2 \times \mathbb{Z}_3$ y D_3. Como G no es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_3$, tiene que ser isomorfo a D_3. De hecho, enviando x a un giro e y a una reflexión conseguimos un isomorfismo de G en D_3.

---

3. Sea $R = \mathbb{Z}[\sqrt{5}] = \{n + m\sqrt{5} : n, m \in \mathbb{Z}\}$.
a) Demuestra que R es un subanillo de $\mathbb{R}$.

<u>*Solución*</u>: Hay que ver que R es cerrado por resta y multiplicación. Pero si a, b, c, d son elementos de $\mathbb{Z}$ entonces

$$(a + b\sqrt{5}) - (c + d\sqrt{5}) = (a - c) + (b - d)\sqrt{5} \in R$$

y

$$(a + b\sqrt{5}) * (c + d\sqrt{5}) = (ac + 5bd) + (ad + bc)\sqrt{5} \in R.$$

b) Si $x = n + m\sqrt{5}$ se define la norma de x como $N(x) = n^2 - 5m^2$. Demuestra que si $x, y \in R$ entonces $N(xy) = N(x)N(y)$.
<u>*Solución*</u>: Sea $x = a + b\sqrt{5}$ e $y = c + d\sqrt{5}$. Hay que demostrar que

$$(a^2 - 5b^2)(c^2 - 5d^2) = (ac + 5bd)^2 - 5(ad + bc)^2.$$

Pero

$$\begin{aligned}(ac + 5bd)^2 - 5(ad + bc)^2 &= (ac)^2 + (5bd)^2 + 10acbd - 5(ad)^2 - 5(bc)^2 - 10adbc \\ &= a^2c^2 + 25b^2d^2 - 5a^2d^2 - 5b^2c^2 = (a^2 - 5b^2)(c^2 - 5d^2),\end{aligned}$$

luego dicha identidad es cierta.

c) Demuestra que $x = n + m\sqrt{5} \in R$ es una unidad si y sólo si $n^2 - 5m^2 = \pm 1$.
<u>*Solución*</u>: Si $n^2 - 5m^2 = \pm 1$, entonces

$$(n + m\sqrt{5}) * [\pm(n - m\sqrt{5})] = 1$$

y como $\pm(n - m\sqrt{5}) \in R$ entonces $n + m\sqrt{5}$ es una unidad.
Si $x = n + m\sqrt{5}$ es una unidad, entonces existe $y \in R$ tal que $xy = 1$. Pero entonces

$$N(x)N(y) = N(xy) = N(1) = 1$$

y como $N(x), N(y) \in \mathbb{Z}$, entonces $N(x) = \pm 1$.

d) Demuestra que 2, $3 - \sqrt{5}$, $3 + \sqrt{5}$ son elementos irreducibles en R.
<u>*Solución*</u>: Si 2 no fuera irreducible, entonces exisitirían $x, y \in R$ no unidades tales que $2 = xy$. Pero entonces

$$4 = N(2) = N(xy) = N(x)N(y),$$

y por el apartado anterior $N(x) \neq \pm 1$, luego $N(x) = \pm 2$. Pero si $x = a + b\sqrt{5}$, eso quiere decir que

$$a^2 - 5b^2 = \pm 2, \qquad a, b \in \mathbb{Z}.$$

Veamos que esto nos lleva a una contradición; dicha ecuación no tiene solución con $a, b \in \mathbb{Z}$, porque no la tiene con $a, b \in \mathbb{Z}_5$. En $\mathbb{Z}_5$, a^2 sólo toma los valores $0, 1, -1$, luego

$$a^2 - 5b^2 = a^2 \neq \pm 2.$$

Como $N(3 - \sqrt{5}) = N(3 + \sqrt{5}) = 4$, la misma demostración sirve para demostrar que $3 + \sqrt{5}$ y $3 - \sqrt{5}$ son irreducibles.

e) Demuestra que R no es un dominio de factorización única. *<u>Solución</u>*: Tenemos que

$$4 = 2 \cdot 2 = (3 + \sqrt{5})(3 - \sqrt{5}).$$

En el apartado anterior hemos demostrado que $5, 3 + \sqrt{5}$ y $3 - \sqrt{5}$ son irreducibles, luego es suficiente ver que $3 + \sqrt{5}$ y 2 no son asociados; si lo fueran existiría $u = a + b\sqrt{5}$ unidad tal que $3 + \sqrt{5} = 2u$, pero entonces $3 = 2a$ que no es posible porque 3 es impar.

---

4. Demuestra que todo grupo de orden 105 tiene un subgrupo de orden 35.
<u>Solución</u>: Sea G un grupo de orden $105 = 3 * 5 * 7$. Sea n_p el número de p-subgrupos de Sylow de G. Se cumple que $n_7 \equiv 1 \mod 7$ y $n_7 \mid 3 * 5$, luego $n_7 = 1$ o $n_7 = 15$; también se cumple que $n_5 \equiv 1 \mod 5$ y $n_5 \mid 3 * 7$, luego $n_5 = 1$ o $n_5 = 21$.
Veamos que no puede ocurrir que $n_7 = 15$ y $n_5 = 21$ al mismo tiempo. Si así fuera, tendríamos 15 grupos de distintos de orden 7; la intersección de dos de esos subgrupos es un subgrupo de ambos, luego debe ser la identidad, y por tanto tendríamos $15 * 6$ elementos de orden 7. De la misma forma, tendríamos $21 * 4$ elementos de orden 5. Pero entonces

$$|G| \geq 15 * 6 + 21 * 4 > 105$$

lo que no es posible.
Así, tenemos que $n_5 = 1$ o $n_7 = 1$. Si $n_5 = 1$, entonces existe un único 5-subgrupo de Sylow P_5, luego es normal en G. Si tomamos uno de los 7-subgrupos de Sylow, digamos P_7, tenemos que $H = P_5 P_7$ es un subgrupo de G (ya que P_5 es normal), y $|H| = 35$.
Si $n_7 = 1$ podemos hacer un argumento similar para encontrar un subgrupo de orden 35 (esta vez P_7 sería normal).
