42 problemas resueltos de Algebra I (Teoría de Grupos)

Yolanda Fuertes y Dragan Vukotić
(con la ayuda de Ernesto Girondo)
Universidad Autónoma de Madrid, 2007/08

Algunos de los ejercicios aquí presentados se han visto en clase como proposiciones o teoremas. Otros se pueden encontrar en las hojas de problemas o en los exámenes de años anteriores. En general deberían servir para profundizar en la comprensión de los conceptos básicos y preparar los exámenes.

Grupos. Propiedades básicas: conmutatividad, orden, subgrupos, índice

Problema 1. *Si G es un grupo de orden par, demostrar que el número de sus elementos de orden 2 es impar.*

Solución. Los elementos de G pueden dividirse en dos clases disjuntas: $Q = \{x \in G : x^2 \neq e\}$ y $G \setminus Q$. Si $x \in Q$, entonces $x \neq x^{-1}$ y $o(x^{-1}) \neq 2$. Por lo tanto, los elementos de Q van emparejados: cada x con su inverso x^{-1}; es decir, hay un número par de ellos. Se sigue que el número de elementos en $x \in G \setminus Q$ (para los cuales $x^2 = e$) también es par. De todos ellos, solamente $x = e$ no es de orden 2. Conclusión: G contiene un número impar de elementos de orden 2. ■

Problema 2. *Sea G un grupo de orden impar. Demostrar que para cada $x \in G$ existe $y \in G$ tal que $y^2 = x$.*

Solución. Sea $|G| = 2n - 1$, $n \in \mathbb{N}$. Entonces para todo $x \in G$ se tiene $x^{2n-1} = e$, es decir, $x^{2n} = x$. Por consiguiente, basta tomar $y = x^n$. ■

Problema 3. *Sea G un grupo y H, $K \leq G$ tales que $|H| = 38$ y $|K| = 55$. Demostrar que $H \cap K = \{e\}$.*

Solución. $H \cap K$ es un subgrupo tanto de H como de K. Por el Teorema de Lagrange, deducimos que $|H \cap K|$ tiene que dividir tanto a $|H| = 38$ como a $|K| = 55$. Pero $38 = 2 \times 19$ y $55 = 5 \times 11$ son coprimos, luego la única posibilidad es $|H \cap K| = 1$, es decir $H \cap K = \{e\}$. ■

Problema 4. *Denotemos, como es habitual, por HK al conjunto $\{hk : h \in H, k \in K\}$. Si G es un grupo y H, $K \leq G$, demuéstrese que $HK \leq G$ si y sólo si $HK = KH$.*

Solución. ($\Rightarrow$): Sea $HK \leq G$. Vamos a demostrar que $HK = KH$.

Si $a \in KH$ entonces $a = kh$, $k \in K$, $h \in H$. Por tanto, $a^{-1} = h^{-1}k^{-1} \in HK$ (siendo H un grupo y $h \in H$, se sigue que $h^{-1} \in H$ y análogamente para K). Puesto que $HK \leq G$, también tenemos que el inverso de a^{-1} pertenece a HK: $a = (a^{-1})^{-1} \in HK$. Esto demuestra que $KH \subset HK$.

Veamos ahora que $HK \subset KH$: si $b \in HK$ entonces $b^{-1} \in HK$ por ser $HK \leq G$; por consiguiente, $b^{-1} = hk$, para ciertos elementos $h \in H$, $k \in K$. Por tanto, $b = (b^{-1})^{-1} = k^{-1}h^{-1} \in KH$.

($\Leftarrow$): Supongamos ahora que $HK = KH$. Para probar que $HK \leq G$, utilizaremos el criterio habitual: demostraremos que a, $b \in HK$ implica $ab^{-1} \in HK$. Si a, $b \in HK$, entonces $a = hk$, $b = xy$, h, $x \in H$, k, $y \in K$. Por tanto, $x^{-1} \in H$, $ky^{-1} \in K$, luego $(ky^{-1})x^{-1} \in KH = HK$; por consiguiente, $(ky^{-1})x^{-1} = uv$, $u \in H$, $v \in K$. Finalmente,

$$ab^{-1} = (hk)(y^{-1}x^{-1}) = h(ky^{-1})x^{-1} = (hu)v \in HK\,,$$

lo cual completa la prueba. ■

Problema 5. *(a) Hallar un ejemplo de un grupo G infinito en el cual existe exactamente un elemento de orden 2.*

(b) Dar un ejemplo de un grupo G infinito en el cual todo elemento, salvo el neutro, tiene orden 2.

Solución. (a) Sea $G = \mathbb{Z} \oplus \mathbb{Z}_2$, suponiendo las operaciones aditivas habituales en $\mathbb{Z}$ y $\mathbb{Z}_2$. Es fácil comprobar que $a = (0, \overline{1})$ es el único elemento en G de orden 2; por ejemplo, todo elemento $(a, \overline{1})$ con $a \neq 0$ tiene orden infinito, etc.

(b) Sea G el conjunto de todas las sucesiones de números ± 1:

$$G = \{x = (x_n)_{n=1}^{\infty} : \; x_n = -1 \text{ ó } 1\,, \text{ para todo } n \in \mathbb{N}\}\,,$$

con la operación de multiplicación definida por coordenadas:

$$x \cdot y = (x_n \cdot y_n)_{n=1}^{\infty}$$

Entonces es obvio que G es cerrado respecto a la operación definida, ya que $(\pm 1) \times (\pm 1) = (\pm 1)$, la multiplicación es asociativa, la sucesión estacionaria $\mathbf{1} = (1, 1, 1, \ldots)$ actúa como neutro y cada elemento de G es obviamente su propio inverso, ya que $x \cdot x = ((\pm 1)^2)_{n=1}^{\infty} = \mathbf{1}$. ■

Problema 6. *Si $n \in \mathbb{N}$ y G es un grupo que tiene un único elemento a de orden n, demostrar que $a \in Z(G)$ y $n = 2$.*

SOLUCIÓN. Recordemos que $o(a) = o(xax^{-1})$ para cualquier $x \in G$. Puesto que a es el único elemento en G de orden n, tenemos que $a = xax^{-1}$ para todo $x \in G$; esto demuestra que $a \in Z(G)$.

Puesto que sólo el neutro puede tener orden uno, para demostrar que $n = 2$, supongamos que $n > 2$. Entonces existe un $m \in \mathbb{N}$ tal que $1 < m < n$ y $(m, n) = 1$ (por ejemplo, sea m el primer número primo entre 1 y n). Por una fórmula vista en clase tenemos:

$$o(a^m) = \frac{n}{(n, m)} = n = o(a) \ ;$$

pero $a^m \neq a$, ya que $1 < m < n = o(a)$, lo cual contradice la hipótesis del problema. Se sigue que $n = 2$. ■

Problema 7. *(Lema de Poincaré) Sea G un grupo, no necesariamente finito, y sean H, $K \leq G$, ambos de índice finito en G. Entonces el subgrupo $H \cap K$ también tiene índice finito en G.*

SOLUCIÓN. El punto clave consiste en ver que para todo $a \in G$ se tiene $(H \cap K)a = Ha \cap Ka$, lo cual es fácil de comprobar. En efecto, las inclusiones obvias $(H \cap K)a \subset Ha$ y $(H \cap K)a \subset Ka$ implican $(H \cap K)a \subset Ha \cap Ka$. Por otra parte, si $x \in Ha \cap Ka$, entonces $x = ha = ka$, $h \in H$, $k \in K$ y, por tanto, $h = k \in H \cap K$, lo cual nos dice que $x \in (H \cap K)a$. Por consiguiente, $Ha \cap Ka \subset (H \cap K)a$ también.

Puesto que el número de todas las clases por la derecha Ha es finito y lo mismo se tiene para las clases Ka, por ser ambos subgrupos de índice finito, se sigue inmediatamente que el número de todas las posibles intersecciones $Ha \cap Ka$ también es finito; por tanto, $[G\colon H \cap K]$ es finito. ■

Grupos cíclicos y finitamente generados

Problema 8. *Sea G un grupo (no necesariamente finito) con neutro e y $N \lhd G$ de índice n. Supongamos que $x \in G$ y $x^m = e$, donde $(m, n) = 1$. Demostrar que $x \in N$.*

SOLUCIÓN. Siendo N un subgrupo normal, el conjunto cociente $G/N = \{gN : g \in G\}$, con la operación dada por $xN \cdot yN = xyN$, es un grupo. Consideremos su elemento xN. Observando que $(xN)^m = x^m N = eN = N$,

el neutro en G/N, obtenemos la conclusión de que $o(xN)|m$. Por el teorema de Lagrange $o(xN)|\,|G/N| = [G : N] = n$. Por lo tanto, $o(xN)|(m, n) = 1$; es decir, xN es el neutro de G/N: $xN = N$, con lo cual $x \in N$. ■

Problema 9. *Consideremos el grupo aditivo* $(\mathbb{Z}_{220}, +)$.

(a) Determinar el índice del subgrupo H *de* $\mathbb{Z}_{220}$ *generado por* $\overline{28}$.

(b) ¿A qué grupo conocido es isomorfo H*?*

(c) ¿Cuántos subgrupos de $\mathbb{Z}_{220}$ *existen con el mismo índice que* H*?*

Solución. (a) Sabemos que siempre que un elemento g de un grupo G tiene orden n, entonces el orden de g^k es $\dfrac{n}{(n, k)}$.

$(\mathbb{Z}_{220}, +)$ es un grupo cíclico, con generador $\overline{1}$. Tratándose de un grupo aditivo, $\overline{28}$ es ciertamente la potencia de $\overline{1}$ con exponente $k = 28$ (en este grupo en que la operación es de suma, operar un elemento consigo mismo repetidamente quiere decir sumarlo consigo mismo repetidamente). Así que el orden de $\overline{28}$ es $\dfrac{220}{(220, 28)} = \dfrac{220}{4} = 55$. Por tanto $[\mathbb{Z}_{220} : H] = \dfrac{|\mathbb{Z}_{220}|}{|H|} = \dfrac{220}{55} = 4$.

(b) Todo subgrupo de un grupo cíclico es cíclico. Por tanto $H \cong \mathbb{Z}_{55}$, el grupo cíclico de 55 elementos.

(c) No existe ningún otro subgrupo de $\mathbb{Z}_{220}$ distinto de H que tenga también índice 4. Esta es una propiedad conocida de los grupos cíclicos: no hay en ellos dos subgrupos distintos que tengan el mismo índice.

(Nota: Lo que sí existe, por supuesto, son otros *generadores* de H distintos de $\overline{28}$.) ■

Problema 10. *¿Es finitamente generado el grupo* $(\mathbb{Q}, +)$*?*

Solución. No. Supongamos que $(\mathbb{Q}, +)$ sí es finitamente generado, digamos por los números racionales m_i/n_i, donde $m_i \in \mathbb{Z}$, $n_i \in \mathbb{N}$, $i = 1,\ldots,k$. Entonces para cualquier $q \in \mathbb{Q}$ existen números enteros $a_1,\ldots, a_k$ tales que

$$q = \sum_{i=1}^{k} a_i \frac{m_i}{n_i} = \frac{N}{n_1 n_2 \ldots n_k}$$

para algún número $N \in \mathbb{Z}$. Sin embargo, es fácil ver que esto es imposible si elegimos

$$q = \frac{1}{2n_1 n_2 \ldots n_k} \in \mathbb{Q}$$

porque las dos igualdades dadas arriba implicarían que $2N = 1$, lo cual es absurdo. Por tanto, $(\mathbb{Q}, +)$ no es finitamente generado. ■

Subgrupos normales. Conjugación. Centro

Problema 11. *Sea G un grupo, H, $N \leq G$ y $[G : N] = 2$. Demostrar que $H \cap N \lhd H$.*

Solución. Por un criterio visto en clase, $N \lhd G$, porque N es un subgrupo de índice 2. La conclusión deseada se sigue del siguiente lema (visto en clase): $H \leq G$ y $N \lhd G$ implica $H \cap N \lhd H$.

Repasemos la demostración del lema. Comprobaremos que

$$h(H \cap N)h^{-1} \subset (H \cap N) \quad \text{para todo } h \in H\,.$$

Por la inclusión trivial $H \cap N \subset H$ tenemos $h(H \cap N)h^{-1} \subset hHh^{-1}$. Puesto que N es un subgrupo normal de G, también tenemos $h(H \cap N)h^{-1} \subset hNh^{-1} \subset N$ para todo $h \in H$. Ahora bien, las inclusiones

$$h(H \cap N)h^{-1} \subset H \quad \text{y} \quad h(H \cap N)h^{-1} \subset N$$

implican $h(H \cap N)h^{-1} \subset H \cap N$. ■

Problema 12. *Supongamos que $H \leq G$ y $x^2 \in H$ para todo $x \in G$. Demostrar que $H \lhd G$ y G/H es abeliano.*

Solución. Observemos que para todo $h \in H$ y todo $x \in G$ tenemos

$$x\,h\,x^{-1} = x\,h\,x\,x^{-2} = x\,h\,x\,h\,h^{-1}\,x^{-2} = (x\,h)^2 h^{-1}(x^{-1})^2 \in H\,,$$

ya que $(xh)^2 \in H$ y $(x^{-1})^2 \in H$. Esto demuestra que $H \lhd G$.

Recordemos un ejercicio conocido: si en un grupo el cuadrado de cada elemento es el neutro, entonces el grupo es abeliano. Ahora sólo hace falta observar que para cada clase $xH \in G/H$, tenemos $(xH)^2 = x^2H = H$. Por lo tanto, el grupo G/H es abeliano. ■

Problema 13. *Si G es un grupo con centro $Z(G)$ y el grupo cociente $G/Z(G)$ es cíclico, demostrar que G es abeliano.*

Solución. Por las hipótesis, existe un $a \in G$ tal que todo elemento del grupo $G/Z(G)$ es de la forma $a^k Z(G)$, para algún $k \in \mathbf{Z}$.

Sean x, $y \in G$ dos elementos cualesquiera; queremos demostrar que $xy = yx$. Para ello, observemos que $x = xe \in xZ(G)$ y, por lo tanto, $x = a^m g$ para algún $m \in \mathbf{Z}$ y $g \in Z(G)$. De manera similar se obtiene $y = a^n h$, para algún $n \in \mathbf{Z}$ y $h \in Z(G)$. Ahora es fácil comprobar lo que queríamos:

$$xy = a^m g a^n h = a^m a^n gh = a^n a^m hg = a^n h a^m g = yx\,,$$

puesto que g, $h \in Z(G)$. ■

Comentario: este resultado es muy útil e importante y conviene conocerlo y saber usarlo; más adelante veremos sus aplicaciones en otros problemas.

Problema 14. *El centro de un p-grupo finito (es decir, de un grupo de orden p^n, p primo, $n \in \mathbb{N}$) es siempre no trivial.*

Solución. La ecuación de las clases de conjugación es, en este caso, tiene la forma

$$p^3 = |G| = |Z(G)| + \sum_{i=1}^{n} [G : C_G(a_i)]\,,$$

donde la suma contiene exactamente un elemento a_i de cada clase de conjugación $C_G(a_i) = \{x \in G : xa_i = a_i x\}$. Cada clase es un subgrupo de G. Siendo G un p-grupo, para cada i ambos números $|C_G(a_i)|$ y $[G : C_G(a_i)]$ son divisores de $|G| = p^3$. Esto implica que

$$|Z(G)| = |G| - \sum_{i=1}^{n} [G : C_G(a_i)]$$

también tiene que ser divisible por p, pues no puede ser $= 1$. ■

Problema 15. *Demostrar que si G no es abeliano y tiene orden p^3 (p es un número primo), entonces $Z(G)$ tiene orden p.*

Solución. Puesto que $Z(G) \leq G$ y $Z(G) \neq G$, por el teorema de Lagrange tenemos $|Z(G)| = 1$, p o p^2.

El último caso queda excluido enseguida: si $Z(G)$ fuese un grupo de orden p^2, el grupo cociente $G/Z(G)$ tendría p elementos y, por consiguiente, sería cíclico. Por el problema anterior, esto es imposible, ya que G no es abeliano.

Por el ejercicio anterior, el caso $|Z(G)| = 1$ también es imposible.

Conclusión: el único caso posible es $|Z(G)| = p$. ■

Problema 16. *Sea G un grupo finito tal que el índice $[G\colon Z(G)]$ es un divisor de 15. Demostrar que G es conmutativo.*

Solución. Por la hipótesis del problema, $[G : Z(G)] \in \{1, 3, 5, 15\}$. Analicemos los cuatro casos.

El caso $[G : Z(G)] = 1$ es trivial: entonces $G = Z(G)$ y, por consiguiente, G es abeliano.

Si $[G : Z(G)] = 3$, entonces el grupo $G/Z(G)$ es cíclico (siendo un grupo de orden 3). Por el problema 13, G es abeliano.

El caso $[G : Z(G)] = 5$ es similar. También lo es el caso $[G : Z(G)] = 15$, por razones algo menos triviales. En general, un grupo cuyo orden no es primo no tiene porque ser cíclico. Sin embargo, por la teoría de los productos semidirectos, sabemos que cualquier grupo de orden 15 tiene que ser isomorfo a $\mathbb{Z}_{15}$ y, por lo tanto, es necesariamente cíclico. ■

Problema 17. *Sean p, q dos números primos (iguales o distintos). Sea G un grupo de orden pq que tiene un único subgrupo H de orden p. Demostrar las siguientes afirmaciones:*

(a) $H \lhd G$.

(b) El grupo cociente G/H es cíclico.

(c) Si $H \subset Z(G)$, entonces G es abeliano.

Solución. (a) H es un subgrupo normal, ya que es el único subgrupo de G de orden p. Esta observación, válida para cualquier grupo finito G, se ha comentado en clase; no obstante, repasaremos la demostración:

Sea $x \in G$ arbitrario. Entonces $I_x(H) = xHx^{-1}$, la imagen de H por el automorfismo interno I_x, denotada también a veces por H^x, es un subrupo de G y $|xHx^{-1}| = |H| = p$. Por lo tanto, $xHx^{-1} = H$. Esto significa que $H \lhd G$.

(b) $|G/H| = \frac{|G|}{|H|} = q$, un número primo. Se sigue que G/H es cíclico.

(c) $Z(G) \lhd G \Rightarrow |Z(G)| \in \{1, p, q, pq\}$. Puesto que $H \subset Z(G)$ y $|H| = p$, tenemos $|Z(G)| \in \{p, pq\}$ y, por lo tanto, $|G/Z(G)| \in \{q, 1\}$. En cada uno de estos casos, $G/Z(G)$ es un grupo cíclico y el problema 13 implica que G es conmutativo. ■

Problema 18. *Sea $H \leq K \lhd G$ y, además, sea K cíclico y finito. Demostrar que $H \lhd G$.*

SOLUCIÓN. Primero, para todo $g \in G$ se tiene $gHg^{-1} \subset gKg^{-1} \subset K$, puesto que $H < K$ y $K \lhd G$. Segundo, gHg^{-1} es un grupo. Por lo tanto, para cualquier elemento $g \in G$, el conjunto gHg^{-1} es un subgrupo de K. También sabemos que $|gHg^{-1}| = |H|$ (visto en clase). Luego, K es un grupo cíclico y finito, y por lo tanto tiene un único subgrupo de orden $|H|$. Por lo tanto, $gHg^{-1} = H$, y esto vale para todo $g \in G$. Esto significa que $H \lhd G$. ■

Problema 19. *Si $H \lhd G$ y el grupo G/H es cíclico, ¿es G necesariamente abeliano? Razónese la respuesta.*

SOLUCIÓN. La respuesta es: NO. Ejemplo: sea G el grupo diédrico de orden 6, en la notación de clase, $D_3 = \{I, A, A^2, B, AB, A^2B\}$ donde $A^3 = I = B^2$ y $BA = A^{-1}B$. Sea $H = \{I, A, A^2\}$, el subgrupo cíclico generado por A. Siendo H un subgrupo de índice 2 en G, por un teorema visto en clase, es un subgrupo normal de G. El grupo cociente G/H de orden 2 es obviamente cíclico. Sin embargo, el grupo G no es abeliano. ■

Homomorfismos de grupos. Teoremas de isomorfía

Problema 20. *Denotemos, como es habitual, por $\mathbb{Z}_n$ al grupo aditivo módulo n y por $Hom(A, B)$ al conjunto de todos los homomorfismos de un grupo A en otro grupo B.*

(a) Demostrar que si $f \in Hom(\mathbb{Z}_m, \mathbb{Z}_n)$, entonces f viene dado por $f(\overline{x}) = \overline{xr}$, donde el orden del elemento $\overline{r} \in \mathbb{Z}_m$ divide a (m, n).

(b) Describir los conjuntos $Hom(\mathbb{Z}_{21}, \mathbb{Z}_{10})$, $Hom(\mathbb{Z}_{21}, \mathbb{Z}_{12})$ y $Hom(\mathbb{Z}_{21}, \mathbb{Z}_7)$.

(c) ¿Cuantos de estos homomorfismos son sobreyectivos (inyectivos)?

SOLUCIÓN. (a) Cualquier $f \in Hom(\mathbb{Z}_m, \mathbb{Z}_n)$ queda completamente determinado por la imagen $f(\overline{1})$, ya que para $0 \leq x < m$ se tiene, por las propiedades elementales de los homomorfismos, $f(\overline{x}) = xf(\overline{1}) = \overline{xf(1)}$. Por lo tanto, todo $f \in Hom(\mathbb{Z}_m, \mathbb{Z}_n)$ tiene la forma indicada en el enunciado con $\overline{r} = f(\overline{1})$.

(Comentario: por las propiedades vistas en clase, la imagen $f(\mathbb{Z}_m)$ es un subgrupo de $\mathbb{Z}_n$. Aunque en algunos casos $\overline{1} \in \mathbb{Z}_n$ no pertenezca a esta imagen $f(\mathbb{Z}_m)$, un elemento de $f(\mathbb{Z}_m)$ desempeñará el papel de generador de $f(\mathbb{Z}_m)$, y éste será precisamente $\overline{r}$.)

La clase $\overline{r} = f(\overline{1})$, siendo un elemento del grupo cíclico $\mathbb{Z}_n$, tiene que cumplir la condición $o(\overline{r}) \mid o(\mathbb{Z}_n) = n$. También es evidente que

$$m\overline{r} = f(\overline{m}) = f(\overline{0}) = \overline{0}\,.$$

Así pues, $o(\overline{r}) \mid m$. Las dos conclusiones implican que $o(\overline{r}) \mid (m, n)$.

(b) Usaremos el apartado (a). Si $f \in Hom(\mathbb{Z}_{21}, \mathbb{Z}_{10})$, entonces el orden de $f(\overline{1})$ divide a $(21, 10) = 1$ y, por tanto, $f(\overline{1}) = \overline{0}$: el único homomofismo es el trivial: $f(\overline{x}) = \overline{0}$ para todo $\overline{x} \in \mathbb{Z}_m$.

En el caso $f \in Hom(\mathbb{Z}_{21}, \mathbb{Z}_{12})$, el orden de $f(\overline{1})$ tiene que ser un divisor de $(21, 12) = 3$; es decir, 1 ó 3. Por lo tanto, $f(\overline{1})$ tiene que ser uno de los elementos del (único) subgrupo de orden 3 del grupo aditivo $\mathbb{Z}_{12}$: $\{\overline{0}, \overline{4}, \overline{8}\}$ (por una proposición vista en clase, si B es un grupo cíclico de orden n y $k \mid n$ entonces G tiene un único subgrupo de orden k). Así pues, los candidatos para ser homomorfismos, además del homomorfismo trivial, son los siguientes:

$$f_1(\overline{x}) = \overline{4x}\ ; \quad f_2(\overline{x}) = \overline{8x}\,.$$

Es fácil comprobar que ambos lo son. Es completamente rutinario comprobar que $f(\overline{x}+\overline{y}) = f(\overline{x}) + f(\overline{y})$. A primera vista, esto parece siempre cierto, sea cual sea el elemento $\overline{r}$, pero también es importante comprobar que están bien definidos:

$$\overline{x} = \overline{y}\ (mod\ 21) \Rightarrow \overline{4x} = \overline{4y}\ (mod\ 12)\,.$$

Dicho de otra manera (suponiendo, sin pérdida de generalidad, que $0 < x$, $y < 21$), hemos de comprobar que

$$21 \mid (x - y) \Rightarrow 12 \mid 4(x - y)\,,$$

pero esto es inmediato. Lo mismo se obtiene con 8 en vez de 4. Por tanto, existen tres homomorfismos en este caso.

$Hom(\mathbb{Z}_{21}, \mathbb{Z}_7)$: ahora $o(\varphi(\overline{1})) \mid 7$, por lo cual $\varphi(\overline{1})$ puede ser cualquiera de los elementos de $\mathbb{Z}_7$, y es fácil ver que todos sirven. En este caso, hay 7 homomorfismos distintos.

(c) En el caso de $Hom(\mathbb{Z}_{21}, \mathbb{Z}_{10})$, ya sabemos que no hay ningún homomorfismo sobreyectivo.

Para que un homomorfismo $\varphi \in Hom(\mathbb{Z}_m, \mathbb{Z}_n)$ sea sobreyectivo, el elemento $\overline{r} = f(\overline{1})$ tiene que ser un generador de $\mathbb{Z}_n$ y, por tanto, de orden exactamente n. Esto nos dice que en el caso de $Hom(\mathbb{Z}_{21}, \mathbb{Z}_{12})$ tampoco puede haber homomorfismos suprayectivos. En el caso de $Hom(\mathbb{Z}_{21}, \mathbb{Z}_7)$ hay 6 homomorfismos (todos menos el trivial) que son sobreyectivos, ya que los elementos $\overline{1}$, $\overline{2}$, ..., $\overline{6}$ de $\mathbb{Z}_7$ todos tienen orden 7.

Evidentemente, ninguno de los homomorfismos considerados puede ser inyectivo, puesto que se trata de aplicaciones de un conjunto de 21 elementos en otros con menos elementos (10, 12, 7). ■

Problema 21. *Para $n \in \mathbb{N}$, describir el grupo $Aut(\mathbb{Z}_n)$ de todos los automorfismos del grupo aditivo $\mathbb{Z}_n$. En particular, para p primo, obtener una caracterización simple de $Aut(\mathbb{Z}_p)$.*

SOLUCIÓN. El argumento es parecido al anterior: si $f \in Aut(\mathbb{Z}_n)$, entonces $\overline{r} = f(\overline{1})$ tiene orden exactamente n (todo automorfismo es sobreyectivo). Si elegimos $0 < r < n$, se sigue que $(r, n) = 1$ (por la típica cuenta para el orden de un elemento en un grupo cíclico). Cada r coprimo con n genera un automorfismo y, por lo tanto, el grupo $Aut(\mathbb{Z}_n)$ tiene exactamente $\varphi(n)$ elementos, donde φ es la función de Euler. Es cierto algo más: los grupos $(Aut(\mathbb{Z}_n), \circ)$ (siendo $\circ$ la composición de aplicaciones) y $(U(\mathbb{Z}_n), \cdot)$, el grupo multiplicativo de las unidades de $\mathbb{Z}_n$, son isomorfos; es obvio que una composición de dos automorfismos $f_r(\overline{x}) = \overline{rx}$ y $f_{r'}(\overline{x}) = \overline{r'x}$ da el siguiente resultado:

$$(f_r \circ f_{r'})(\overline{x}) = \overline{rr'x} = f_{rr'}(\overline{x}) \,,$$

lo que sugiere un automorfismo natural $F : Aut(\mathbb{Z}_n) \to U(\mathbb{Z}_n)$ dado por $F(f) = f(\overline{1}) = \overline{r}$. La igualdad escrita arriba nos dice que $F(f_r \circ f_{r'}) = F(f_r) \cdot F(f_{r'})$.

En particular, para $n = p$ (primo) tenemos $(Aut(\mathbb{Z}_p), \circ) \cong (U(\mathbb{Z}_p), \cdot)$, que es un grupo multiplicativo cíclico (de orden $p - 1$) y, por tanto, es isomorfo al grupo aditivo $(\mathbb{Z}_{p-1}, +)$. ■

Problema 22. *Dado un grupo G y $a \in G$, denotemos por σ_a el automorfismo interno dado por $\sigma_a(x) = axa^{-1}$, con frecuencia también denotado por I_a y por Int (G) al grupo de todos los automorfismos internos de G. Hemos visto en clase que $\sigma_a \circ \sigma_b = \sigma_{ab}$ para todo a, $b \in G$ y que Int $G \lhd$ Aut G. Demostrar que $G/Z(G) \cong$ Int G.*

SOLUCIÓN. Sea ϕ: $G \to$ Int G, $\phi(a) = \sigma_a$. Entonces ϕ es obviamente suprayectiva y es un homomorfismo de grupos, puesto que

$$\phi(a) \circ \phi(b) = \sigma_a \circ \sigma_b = \sigma_{ab} = \phi(ab) \,.$$

Además, el núcleo de ϕ, $N(\phi) = \ker \phi$ es el centro de G: $a \in N(\phi)$ si y sólo si $\phi(a) = \sigma_a =$Id, lo cual se tiene si y sólo si $axa^{-1} = x$ para todo $x \in G$; es decir, si y sólo si $ga = ag$ para todo $x \in G$.

Aplicando el Primer teorema de isomorfía, obtenemos $G/Z(G) = G/N(\phi)$ $\cong \phi(G) =$ Int G. ■

Problema 23. *¿Cuántos homomorfismos suprayectivos existen del grupo diédrico D_{13} en $\mathbb{Z}_{12}$?*

SOLUCIÓN. Ninguno. Si existiese algún homomorfismo f del tipo indicado, el primer teorema de isomorfía implicaría que $D_{13}/N(f) \cong \mathbb{Z}_{12}$ y, por tanto, tendríamos que

$$|D_{13}/N(f)| = \frac{26}{|N(f)|} = |\mathbb{Z}_{12}| = 12\,,$$

es decir, que el núcleo de f tiene $26/12$ elementos, un número no entero, lo cual es absurdo. Por tanto, no existe ningún homomorfismo con las características exigidas. ■

Acciones de grupos

Problema 24. *Si un grupo G actúa sobre un conjunto X, demostrar que su acción puede extenderse al conjunto $\mathcal{P}(X) = \{S : S \subset X\}$.*

SOLUCIÓN. Denotemos por $\cdot : G \times X \to X$ la acción de G sobre X (por la izquierda). El razonamiento sería similar para una acción por la derecha $\cdot : X \times G \to X$. Podemos definir la función $*$ en el producto directo $G \times \mathcal{P}(X)$ como sigue:

$$a * S = \{a \cdot x : x \in S\}\,, \quad a \in G\,, \quad S \subset X\,.$$

Vemos inmediatamente que $* : G \times \mathcal{P}(X) \to \mathcal{P}(X)$ ya que $\cdot : G \times X \to X$. Entendemos que trata de una extensión de $\cdot$ pues $a * \{x\} = \{a \cdot x\}$, para todo $x \in X$.

Además, se cumplen ambas condiciones para que sea una acción, ya que la propiedad básica $e \cdot x = x$ implica:

$$e * S = \{e \cdot x : x \in S\} = \{x : x \in S\} = S$$

y la propiedad $a \cdot (b \cdot x) = (ab) \cdot x$ implica

$$\begin{aligned} a * (b * S) &= a * \{b \cdot x : x \in S\} = \{a \cdot (b \cdot x) : x \in S\} = \{(ab) \cdot x : x \in S\} \\ &= (ab) * S\,. \end{aligned}$$

Problema 25. *Consideremos la acción de un grupo G sobre sí mismo por conjugación: $a \cdot x = axa^{-1}$. Dado un elemento $x \in G$, hállnese:*

(a) su estabilizador (grupo de isotropía) G_x;

(b) su órbita $O(x)$;

(c) el número de elementos en la clase de conjugación de x.

Solución. (a) Por definición,

$$G_x = \{g \in G : \ g{\cdot}x = x\} = \{g \in G : \ gxg^{-1} = x\} = \{g \in G : \ gx = xg\} = C_G(x)\,,$$

el centralizador de x en G, estudiado en clase.

(b) Por definición,

$$O(x) = \{g \cdot x : \ g \in G\} = \{gxg^{-1} : \ g \in G\} = C(x)\,,$$

la bien conocida clase de conjugación de x en G.

(c) Sabemos de clase que $|O(x)| = [G\colon G_x]$, luego

$$|C(x)| = |O(x)| = [G\colon G_x] = [G\colon C_G(x)]\,.$$

Observación. Evidentemente, estas conclusiones pueden usarse para deducir la ecuación de las clases de conjugación mediante acciones de grupos. ■

Grupos de permutaciones

Problema 26. *(a) Descomponer la permutación σ en producto de ciclos disjuntos.*

(b) Hallar el orden de σ.

(c) Calcular σ^{2008}.

Solución. Puesto que $\sigma(1) = 3$, $\sigma(3) = 8$, $\sigma(8) = 1$, luego $\sigma(2) = 7$, $\sigma(7) = 2$, etc., vemos que la descomposición cíclica de σ es la siguiente:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 8 & 9 & 4 & 5 & 2 & 1 & 6 \end{pmatrix} = (138)(27)(4965)\,.$$

Sean

$$\alpha = (138)\,, \quad \beta = (27)\,, \quad \gamma = (4965)\,.$$

Los ciclos α, β y γ son disjuntos dos a dos, luego conmutan y, por tanto, sus potencias también conmutan. Por consiguiente,

$$\sigma^{2008} = \alpha^{2008}\beta^{2008}\gamma^{2008} = \alpha = (138)\,,$$

ya que el orden de un r-ciclo es exactamente r y, por tanto, $\alpha^3 = \beta^2 = \gamma^4 = I$ y $2008 \equiv 1\,(3)$, $2008 \equiv 0\,(2)$ y $2008 \equiv 0\,(4)$. ■

Problema 27. *Decidir justificadamente si las permutaciones* $\alpha = (12)(123)$ *y* $\beta = (145)$ *generan* S_5 *o no.*

SOLUCIÓN. Componiendo los dos ciclos que aparecen en la fórmula para α, vemos que la permutación fija el número 1 y que $\alpha = (23)$, una trasposición.

Puesto que los ciclos α y β son disjuntos, sabemos que $\alpha\beta = \beta\alpha$ por una propiedad básica vista en clase. Eso nos dice que el grupo $\langle \alpha, \beta \rangle$ generado por α y β es abeliano y, por tanto, no puede coincidir con S_5, que no es abeliano, como bien sabemos. ■

Problema 28. *Decidir justificadamente si los ciclos* $\alpha = (123)$ *y* $\beta = (25431)$ *generan* S_5*; es decir, si* $S_5 = \langle \alpha, \beta \rangle$.

SOLUCIÓN. Basta observar que $\alpha = (13)(12)$, $\beta = (21)(23)(24)(25)$ y que, por tanto, ambos ciclos son permutaciones pares. Esto significa que $\langle \alpha, \beta \rangle \leq A_5 \neq S_5$. ■

Problema 29. *Si* $n \geq 3$*, demostrar que* $Z(S_n) = \{I\}$.

SOLUCIÓN. Sea $\sigma \in S_n$, $\sigma \neq I$. Supongamos que $\sigma(i) = j \neq i$; un par de números i, j con esta propiedad existe ya que $\sigma \neq I$. Puesto que $n \geq 3$, existe $k \in \{1, 2, \ldots, n\}$ tal que $k \neq i$, j. Consideremos una permutación $\tau \in S_n$ tal que $\tau(i) = i$, $\tau(j) = k$, $\tau(k) = j$, por ejemplo, la trasposición (jk). Entonces $\sigma\tau(i) \neq \tau\sigma(i)$ y, por tanto, σ y τ no conmutan. ■

Recordemos que este último ejercicio fue fundamental en la demostración del teorema de Abel.

Problema 30. *Determinar el número de homomorfismos de* $\mathbb{Z}_6$ *en* S_5 *que*
(a) son inyectivos;
(b) tienen imagen de orden 3.

SOLUCIÓN.

(a) Dado que $\mathbb{Z}_6$ es cíclico, para dar un homomorfismo de él, basta decir donde va el generador. Para que el homomorfismo sea inyectivo, el orden de la imagen del generador por el homomorfismo debe ser el mismo que el orden del generador, es decir, igual a 6. Buscamos, por tanto, los elementos de S_5 de orden 6. Los únicos que existen son la composición disjunta de un 3-ciclo y una transposición. Por tanto, tenemos $2 \cdot \binom{5}{3} = 20$.

(b) Sea $f : \mathbb{Z}_6 \to S_5$ un homomorfismo, entonces la imagen de f es el subgrupo de S_5 generado por $f(\bar{1})$. Si queremos que la imagen tenga orden 3, tenemos que enviar el generador, $\bar{1}$, de $\mathbb{Z}_6$ a un elemento de S_5 de orden 3. Un elemento de orden 3 sólo puede ser un $3-$ciclo y, por tanto, tenemos $2 \cdot \binom{5}{3} = 20$ tales homomorfismos. ■

Productos directos. Grupos abelianos finitos

Problema 31. *Hallar todos los grupos abelianos (no isomorfos entre sí) de orden* 360*.*

Solución. Por el teorema fundamental sobre la estructura de los grupos abelianos finitos (visto en clase), cualquier grupo conmutativo de orden $360 = 2^3 \cdot 3^2 \cdot 5$ es una suma directa de 2-grupos, 3-grupos y $\mathbb{Z}_5$. Hay 3 grupos abelianos distintos (no isomorfos entre si) de orden $2^3 = 8$:

$$\mathbb{Z}_8 \ , \quad \mathbb{Z}_8 \oplus \mathbb{Z}_4 \ , \quad \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

y dos grupos abelianos no isomorfos de orden $3^2 = 9$:

$$\mathbb{Z}_9 \ , \quad \mathbb{Z}_3 \oplus \mathbb{Z}_3 \ .$$

Por lo tanto, para un grupo abeliano de orden 360 hay, en total, $6 = 3 \cdot 2$ posibilidades:

$$\mathbb{Z}_8 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{360}$$

$$\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_{120}$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{180}$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_6 \oplus \mathbb{Z}_{60}$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{90}$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{30} \, .$$

Observación: los grupos $\mathbb{Z}_8$ y $\mathbb{Z}_2 \oplus \mathbb{Z}_4$ no son isomorfos porque $\mathbb{Z}_8$ tiene, al menos, un elemento de orden 8 (por ejemplo, $\bar{1}$), mientras que el máximo orden de un elemento de $\mathbb{Z}_2 \oplus \mathbb{Z}_4$ es 4. Este tipo de observaciones sobre los órdenes de elementos constituyen una de las herramientas básicas para demostrar que dos grupos dados no pueden ser isomorfos. Generalizando el mismo razonamiento, podemos concluir que los grupos $\mathbb{Z}_{mn}$ y $\mathbb{Z}_m \oplus \mathbb{Z}_n$ son isomorfos si y sólo si $(m, n) = 1$ (visto en clase). ■

Problema 32. *Escribir $U(\mathbb{Z}_{33})$, el grupo multiplicativo de las unidades de $\mathbb{Z}_{33}$, como producto de grupos cíclicos.*

SOLUCIÓN. Primero, $U(\mathbb{Z}_{33})$ es un grupo conmutativo y tiene $\varphi(33) = \varphi(3)\cdot\varphi(11) = 2\cdot 10 = 20 (= 2^2\cdot 5)$ elementos, según las propiedades básicas de la función de Euler. Aplicando el Teorema fundamental sobre la estructura de grupos abelianos finitos, concluimos que $U(\mathbb{Z}_{33})$ es isomorfo o bien al grupo cíclico $\mathbb{Z}_4 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{20}$ o bien al grupo $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{10}$.

Para decidir entre estos dos grupos, conviene aplicar la siguiente técnica (que también puede ser útil en algunos ejercicios con varios productos semidirectos): vamos a contar el número de elementos de cierto orden en cada uno de los grupos. El orden de cada elemento de un grupo de 20 elementos es un divisor de 20 (por Lagrange), ¿pero cuál deberíamos elegir entre ellos? Vamos a elegir el más pequeño posible, en este caso 2. Si $\overline{x} \in \mathbb{Z}_{20}$, $0 < x < 20$ y $2 = o(\overline{x}) = \frac{20}{(20,x)}$ entonces $(20, x) = 10$ y $x = 10$. Es decir, hay un único elemento $(\overline{10})$ de orden 2 en $\mathbb{Z}_{20}$.

Encontraremos ahora en el grupo $U(\mathbb{Z}_{33})$ más de un elemento de orden 2: si $x^2 \equiv 1\ (33)$, esto significa que $33 = 3\cdot 11 \mid x^2 - 1 = (x-1)(x+1)$. Puesto que 3 y 11 son primos, concluimos que $3 \mid (x-1)$ ó $3 \mid (x+1)$, y lo mismo para 11. Ahora es fácil encontrar $x = 10$ y $x = -1 = 32$. Puesto que este grupo tiene más de un elemento de orden 2, se sigue que no puede ser isomorfo a $\mathbb{Z}_{20}$ y, por lo tanto, es isomorfo al otro: $U(\mathbb{Z}_{33}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{10}$.
■

Teoremas de Cauchy y de Sylow

Problema 33. *Demostrar que no existe ningún grupo simple de orden 63.*

SOLUCIÓN. Puesto que $63 = 3^2 \times 7$, el Primer Teorema de Sylow implica la existencia de un subgrupo de orden 7 (7-subgrupo de Sylow en este caso, ya que $7^2 \not| 63$). Según el Tercer Teorema de Sylow, el número de 7-subgrupos de Sylow, denotado n_7, cumple las condiciones $n_7 \equiv 1\,(7)$ y $n_7 | 63/7 = 9$. Por tanto, $n_7 = 1$: hay un subgrupo único de orden 7. Puesto que es el único de ese orden, tiene que ser normal. Eso demuestra que un grupo de orden 63 siempre tiene un subgrupo normal no trivial y, por definición, no es simple.
■

Problema 34. *Sea G un grupo de orden 50 con un único subgrupo de orden 2. Deducir razonadamente que G es abeliano.*

SOLUCIÓN. Sabiendo que el subgrupo H de orden 2 es único, tiene que ser normal. Puesto que $50 = 2 \times 5^2$, debido al Primer Teorema de Sylow, el grupo G también tiene un subgrupo de orden $25 = 5^2$, digamos K. El número n_5 de subgrupos de ese orden cumple las siguientes condiciones:

$$n_5 \equiv 1(5)\,, \qquad n_5 | \frac{50}{5^2} = 2\,,$$

según el Tercer Teorema de Sylow. Puesto que los únicos divisores de 2 son 1 y 2, se sigue que $n_5 = 1$. Por tanto, hay un único 5-subgrupo de Sylow; de ahí se sigue que también $K \lhd G$.

Observemos ahora que si un elemento a del grupo G pertenece a $H \cap K$, entonces $o(a)|2$ y $o(a)|25$; pero $(2, 25) = 1$ y por tanto, $o(a) = 1$; es decir, $a = e$. Así pues, hemos probado que $H \cap K = \{e\}$.

Tenemos, pues: H, $K \lhd G$, $H \cap K = \{e\}$; por las propiedades vistas en clase y en las hojas de problemas, se sigue que

$$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{2 \cdot 25}{1} = 50 = |G|$$

y de ahí que $HK = G$. También tenemos en este caso que $HK \cong H \times K$, tal y como se ha visto en clase; es decir, $G \cong H \times K$.

Puesto que tanto H como K son abelianos (el primero, porque es de orden 2 y, por tanto, cíclico y el segundo, porque es de orden p^2, donde $p = 5$ es primo, otra propiedad vista en clase) y el producto directo de dos grupos abelianos es obviamente abeliano, se sigue que G es abeliano. ■

Problema 35. *Sea G un grupo de orden 20. Demostrar que G tiene un subgrupo normal de orden 5.*

SOLUCIÓN. Como 5 es un número primo que divide al orden de G, por el Teorema de Cauchy, sabemos que existe un elemento $a \in G$ de orden 5, o equivalentemente, que el subgrupo generado por a, que denotaremos por $< a >= H$, tiene orden 5. Para todo $g \in G$, denotaremos por $H^g = gHg^{-1}$ al subgrupo de G que se obtiene conjugando H por $g \in G$; ya sabemos que es un subgrupo de G y que tiene el mismo orden que H. Consideraremos el subconjunto de G, $H^g \cdot H \subseteq G$ (para saber que es un subgrupo, alguno de los dos grupos tendría que ser normal). Éste satisface $|H^g \cdot H| \leq |G| = 20$. Además, $H^g \cap H \leq H$, y por el Teorema de Lagrange tenemos que $|H^g \cap H|$ es un divisor de $|H| = 5$, luego $|H^g \cap H| = 1$ ó 5. Por otra parte,

$$|H^g \cdot H| = \frac{|H^g| \cdot |H|}{|H^g \cap H|} = \frac{5 \cdot 5}{|H^g \cap H|} = \begin{cases} \frac{25}{1} > 20 & , \quad \text{imposible} \\ \frac{25}{5} = 5 & , \quad \text{correcto} \end{cases}$$

Luego, $|H^g \cap H| = 5 = |H|$, de donde se deduce que $H^g \cap H = H \ \forall g \in G$ o, equivalentemente, $H^g = gHg^{-1} = H \ \forall g \in G$, luego H es un subgrupo normal de G y es el que buscábamos.

(Observar que el argumento anterior nos servirá, siempre que tengamos $|G| = p{\cdot}s$ (con un primo $p > s$, y s no necesariamente primo), para demostrar que el subgrupo generado por el elemento de orden p es un subgrupo normal). ■

Problema 36. *Sea G un grupo finito y H un subgrupo normal de G con $|H| = p^k$. Demostrar que $H \subset P$ para todo P $p-$subgrupo de Sylow de G.*

SOLUCIÓN. Sea P un $p-$subgrupo de Sylow de G. Según el Segundo Teorema de Sylow, existe $g \in G$ tal que $H \subset gPg^{-1}$. Luego $g^{-1}Hg \subset P$. Siendo $H \triangleleft G$, se cumple $g^{-1}Hg = H$ y, por tanto, $H \subset P$. ■

Productos semidirectos. Grupos de orden pequeño

Problema 37. *Demostrar que no existe ningún grupo G que cumpla las siguientes propiedades: $[G : Z(G)] = 4$ y $a^2 \notin Z(G)$ para algún $a \in G \setminus \{e\}$. (Como siempre, e es el neutro del grupo G).*

SOLUCIÓN. Supongamos que existe un grupo G con esas propiedades. Entonces $G/Z(G)$ es un grupo de orden 4 y, por tanto, o bien es isomorfo al grupo cíclico $\mathbb{Z}_4$ o bien al grupo de Klein V_4, producto directo de dos grupos cíclicos de orden 2 (demostrado en clase).

En el caso $G/Z(G) \cong \mathbb{Z}_4$, el problema 13 implica que G es abeliano, es decir, $G = Z(G)$, lo cual es imposible, ya que $a^2 \notin Z(G)$.

Recordemos que todo elemento de V distinto del neutro tiene orden 2; por lo tanto, el cuadrado de cada elemento de V es el neutro. Si suponemos que $G/Z(G) \cong V$, se sigue que $(xZ(G))^2 = x^2Z(G) = Z(G)$ para todo $x \in G$, o sea, $x^2 \in Z(G)$ para todo $x \in G$, mientras que $a^2 \notin Z(G)$. Contradicción. ■

Problema 38. *Encontrar todos los grupos de orden 21.*

SOLUCIÓN. Sea G un grupo tal que $|G| = 21$, como 3 y 7 son números primos que dividen a 21, nuevamente por el teorema de Cauchy, existen elementos a y $b \in G$ con órdenes 7 y 3, respectivamente. Sea $H =< a >$, vamos a probar que es un subgrupo normal de G, de manera similar a como

hicimos en el ejercicio anterior. Sea $H^g = gHg^{-1}$, para $g \in G$; sabemos que $H^g \cdot H$ es un subconjunto de G, luego $|H^g \cdot H| \leq 21 = |G|$ y $|H^g| = |H|$. Además, $H^g \cap H$ es un subgrupo de H, y por el teorema de Lagrange tenemos que $|H^g \cap H| = 1$ ó 7. Por otra parte,

$$|H^g \cdot H| = \frac{|H^g| \cdot |H|}{|H^g \cap H|} = \frac{7 \cdot 7}{|H^g \cap H|} = \begin{cases} \frac{49}{1} > 21 & , \quad \text{imposible} \\ \frac{49}{7} = 7 & , \quad \text{correcto} \end{cases}$$

Veamos ahora que $< a > \cap < b >= \{e\}$, donde e denota el elemento neutro del grupo, lo cual implicaría que $G \cong < a > \times_\theta < b >$ porque además tendríamos

$$| < a > \cdot < b > | = \frac{| < a > | \cdot | < b > |}{< a > \cap < b > |} = 21 = |G| \Rightarrow < a > \cdot < b >= G.$$

$\forall g \in < a > \cdot < b > \Rightarrow | < g > |$ divide al máximo común divisor 7 y 3 (los órdenes de a y b, respectivamente) que es 1, luego $g = e$.

Ahora nos falta analizar todos los posibles homomorfismos de grupos $\theta :< b > \rightarrow \text{ Aut } (< a >)$, que nos darían todos los posibles productos semidirectos y, por tanto, todos los posibles grupos de orden 21.

Como $< b >$ es un grupo cíclico, para definir el homomorfismo θ, basta definir la imagen de un generador, es decir, basta definir $\theta(b) = \sigma_b \in \text{Aut}(< a >)$, y a su vez σ_b, por ser un automorfismo de $< a >$, queda determinado por su acción sobre a, que además por teoría sabemos que es de la forma $\sigma_b(a) = bab^{-1}$. Como $< a > \lhd G \Rightarrow bab^{-1} \in < a >$, luego $bab^{-1} = a^s$, con $s \in \{1, 2, 3, 4, 5, 6\}$. Por otra parte, como θ es un homomorphismo lleva el neutro (por ejemplo $b^3 = e$) al neutro (el automorfismo identidad, Id), es decir, $\text{Id} = \theta(b^3) = (\theta(b))^3$, lo cual implica que $a = \text{Id}(a) = (\theta(b))^3(a) = a^{s^3}$ o, equivalentemente, $a^{s^3-1} = 1$, lo cual nos dice que 7 divide a $s^3 - 1$ o, equivalentemente, que s^3 es congruente con 1 módulo 7. De ahí obtenemos que $s \in \{1, 2, 4\}$. Así pues, los casos posibles son:

i) $s = 1 \Rightarrow (\theta(b))(a) = a \Leftrightarrow \theta \equiv \text{ cte.} \Rightarrow < a > \times_\theta < b >$ es un producto directo, o equivalentemente,

$$G_1 \cong < a > \times < b > \cong \mathbb{Z}_7 \times \mathbb{Z}_3 \cong \mathbb{Z}_{21}, \text{ grupo cíclico.}$$

ii) $s = 2 \Rightarrow (\theta(b))(a) = a^2 = bab^{-1} \Leftrightarrow ba = a^2b$, lo cual implica que obtenemos un grupo no conmutativo, llamémosle G_2, de la forma

$$G_2 = \{a^i b^j : ba = a^2b \text{ con } 0 \leq i \leq 6,\ 0 \leq j \leq 2\}$$

iii) $s = 4 \Rightarrow (\theta(b))(a) = a^4 = bab^{-1} \Leftrightarrow ba = a^4b$, de donde aparentemente obtendríamos otro posible grupo, generado por dos elementos con la

relación descrita anteriormente. Observemos que la relación anterior es la misma que si describimos el grupo del apartado ii), G_2, como el generado por los elementos a y b^2, en lugar de a y b, porque $ba = a^2b$, aplicado sucesivamente, nos da

$$b^2a = b(ba) = b(a^2b) = (ba)(ab) = (a^2b)(ab) = a^2(ba)b = a^2(a^2b)b = a^4b\,,$$

que es la misma relación que satisfarían los dos generadores del grupo obtenido en este apartado iii), luego no obtenemos un grupo distinto.

Luego, sólo tenemos dos grupos no isomorfos de orden 21, G_1 y G_2. ■

Grupos resolubles

Problema 39. *Demostrar que el grupo D_n de las simetrías de un polígono regular de n lados es resoluble para todo $n \geq 3$.*

Solución. Puesto que $D_n =< \{a, b : a^n = 1 = b^2,\ bab^{-1} = a^{-1}\} >$, sabemos que $< a >$ es un subgrupo normal de índice 2 en D_n. Entonces tenemos la siguiente resolución:

$$\{1\} \lhd < a > \lhd D_n$$

ya que el primer factor es cíclico, luego abeliano, y el segundo factor es un grupo de orden 2, por tanto también cíclico. ■

Problema 40. *Obtener una resolución del grupo de los cuaterniones Q.*

Solución. Como $Q =< \{a, b : a^4 = 1 = b^4,\ b^2 = a^2,\ bab^{-1} = a^{-1}\} >$ y $|Q| = 8$, tenemos que $< a >$ es un subgrupo normal de índice 2 de Q. Así obtenemos la siguiente resolución:

$$\{1\} \lhd < a > \lhd Q$$

porque el primer factor es cíclico (luego abeliano) y el segundo factor es un grupo de orden 2 y, por tanto, también es cíclico. ■

Problema 41. *Sea $G = P \cdot Q$ con P y Q subgrupos abelianos de G y $P \lhd G$. Probar que G es resoluble.*

SOLUCIÓN. Tenemos la resolución:

$$\{1_G\} \lhd P \lhd G = P \cdot Q$$

El primer factor es P, que es abeliano. Por el Tercer Teorema de Isomorfía, el segundo factor es $P \cdot Q/P = Q \cdot P/P \cong Q/P \cap Q$, cociente de un abeliano, luego abeliano. ■

Problema 42. *Sea G un grupo de orden 12 con generadores a y b satisfaciendo las siguientes relaciones: $a^4 = b^3 = 1$ y $aba^{-1} = b^{-1}$.*

1. *Ecribir todos los elementos de G en la forma $a^k b^j$, sin incurrir en repeticiones.*
2. *Determinar si los subgrupos $H =< a >$ y $K =< b >$ son normales.*
3. *Determinar si G es resoluble y encontrar una serie normal de composición para G.*

SOLUCIÓN. (i) Dado que $aba^{-1} = b^{-1}$ tenemos que $ba^{-1} = a^{-1}b^{-1} = (ba)^{-1}$ o, equivalentemente, tomando inversos que $ba = ab^{-1} = ab^2$. Por tanto, los elementos de G son exactamente los siguientes:

$$\{1_G, a, a^2, a^3, b, ab, a^2b, a^3b, b^2, ab^2, a^2b^2, a^3b^2\} = \{a^i b^j : 0 \leq i \leq 3,\ 0 \leq j \leq 2\}.$$

(ii) Sea $H =< a >$. H no es un subgrupo normal de G porque, por ejemplo, $bab^{-1} = ab \notin < a >$. Por otra parte, si $K =< b >$ entonces K si es un subgrupo normal de G porque $aba^{-1} = b^{-1} \in < b >$ y G está generado por a y b.

(iii) G es resoluble porque como $K =< b >$ es normal en G, $G = H \cdot K$ y $H \cap K = \{1_G\}$, entonces tenemos la siguiente serie normal de G:

$$\{1_G\} \lhd K \lhd G$$

con cocientes K y H, respectivamente, ambos abelianos. Por tanto, dicha serie normal es una resolución de G.