Ejercicios de grupos cíclicos

1. Probar que el cociente de un grupo monógeno es monógeno; determínese su generador.

   Esquema de solución: El generador es la clase donde est¡a el generador del grupo de partida.

2. Descríbanse todos los subgrupos de $\mathbf{Z}/12\mathbf{Z}$. Esquema de solución: Son de orden $1, 2, 3, 4, 6, 12$.

$$\{0 + 12\mathbf{Z}\}, \{0 + 12\mathbf{Z}, 6 + 12\mathbf{Z}\} \dots$$

3. Pruébese que todo grupo de orden primo es cíclico. Descríbanse sus posibles generadores.

   Esquema de solución: Cada elemento distinto del neutro genera un subgrupo que por el teorema de Lagrange es el total.

4. Dado $x \in G$ de orden n pruébese

   - $x^m = e \Longrightarrow n \mid m$
   -
$$o(x^k) = \frac{n}{(k, n)}$$

   Esquema de solución:

   - División euclídea entre m y n
   -
$$(x^k)^{\frac{n}{(k,n)}} = x^{rn} = e \Longrightarrow o(x^k) \mid \frac{n}{(k, n)}$$

$$(x^k)^m = e \Longrightarrow n \mid km \Longrightarrow \frac{n}{(k, n)} \mid \frac{k}{(k, n)} m \Longrightarrow \frac{n}{(k, n)} \mid \frac{k}{(k, n)}$$

   pues $\frac{n}{(k,n)}$ y $\frac{k}{(k,n)}$ son primos entre sí.

5. Describir el conjunto de generadores de un grupo cíclico de orden n.

   Esquema de solución: Aplicando el ejercicio anterior

$$< x^k >= G \iff \frac{n}{(k, n)} = n \iff (k, n) = 1$$

   La función φ dada por $\varphi(n) = \#\{k < n \mid (k, n) = 1\}$ recibe el nombre de indicador de Euler

6. Dado un número natural n, probar que el conjunto

$$\{z \in \mathbf{C} \mid z^n = 1\}$$

   de las raíces n-simas de la unidad es un grupo cíclico con la multiplicación de números complejos. Sus generadores reciben el nombre de raíces n-simas primitivas de la unidad. Describirlas para $n \leq 5$.

Esquema de solución:

Que es grupo se deduce de que es un subgrupo de $(\mathbf{C}, .)$. Que es cíclico se puede deducir directamente del ejercicio 10; pero en este caso es conocido que se trata de

$$\{(\cos(2\pi/n) + i\ \sin(2\pi/n))^k \mid k = 1, \ldots, n\}$$

De acuerdo con el ejercicio 5, los generadores son

$$\{(\cos(2\pi/n) + i\ \sin(2\pi/n))^k \mid (k, n) = 1\}$$

Por tanto,

- $n = 1 \Longrightarrow \{1\}$
- $n = 2 \Longrightarrow \{-1\}$
- $n = 3 \Longrightarrow \{\cos(2\pi/3) + i\ \sin(2\pi/3), \cos(4\pi/3) + i\ \sin(4\pi/3)\}$
- $n = 4 \Longrightarrow \{i, -i\}$
- $n = 5 \Longrightarrow \{\cos(2k\pi/n) + i\ \sin(2k\pi/5) \mid k = 1, \ldots, 4\}$

7. Si G es abeliano, y $\text{mcd}(o(x), o(y)) = 1$, $o(xy) = o(x)o(y)$

   Esquema de solución: Es claro que $o(xy) \mid o(x)o(y)$. Recíprocamente,

   $$(xy)^m = 1 \Longrightarrow x^m = (y^m)^{-1} \Longrightarrow (x^m) \in < x > \cap < y > = 1 \Longrightarrow o(x) \mid m$$

   Análogamente, $o(y) \mid m$; por tanto, m es múltiplo de su mcm que es el producto.

8. Un grupo finito abeliano, contiene un elemento cuyo orden es

   $$\exp(G) = \text{mcm}\{o(x) \mid x \in G\}$$

   Esquema de solución: Por ser G finito podemos localizar $y \in G$ de orden maximal; es decir,

   $$x \in G \Longrightarrow o(x) \leq o(y)$$

   Basta probar que $x^{o(y)} = 1\,\forall x \in G$. Por reducción al absurdo, sea x tal que $x^{o(y)} \neq 1$; sean $\prod p_i^{n_i}$ y $\prod p_i^{m_i}$ las factorizaciones de $o(y)$ y $o(x)$. debe ser $n_1 < m_1$. Construyamos,

   $$z = y^{p_1^{n_1}} \quad t = x^{p_2^{m_2} \cdots p_r^{m_r}}$$

   Por el problema 4,

   $$o(z) = p_2^{n_2} \cdots p_r^{n_r} \quad o(t) = p_1^{m_1}$$

   Y por el problema anterior

   $$o(zt) = p_1^{m_1} p_2^{n_2} \cdots p_r^{n_r} > o(y)$$

   que es una contradicción.

9. Probar que un grupo finito abeliano es cíclico si y sólo si su exponente coincide con el orden del grupo.

   Esquema de solución: Es claro, que el exponente de un grupo finito es divisor del orden del grupo.

   Si G es cíclico generado por x, $|G| = o(x)$ que es divisor del exponente y ya está.

   Recíprocamente, por el problema anterior, existe un elemento $y \in G$ tal que $o(y) = \exp(G) = |G|$; así, $| < y > | = |G|$ y $G =< y >$.

10. Probar que un subgrupo finito del grupo multiplicativo de un cuerpo es cíclico.

    Esquema de solución:

    Cada elemento $x \in G$ cumple $x^{\exp(G)} = 1$, luego es raíz de $x^{\exp(G)} - 1$ y G tiene a lo sumo $\exp(G)$ elementos. Por tanto, $|G| = \exp(G)$ y G es cíclico.

11. Compruébese que el grupo de las simetrías del rectángulo no puede ser cíclico.

    Esquema de solución: Se trata de la identidad, la simetría respecto de la vertical que lo parte en dos, la simetría respecto de la horizontal que lo parte en dos y el giro de 180 grados; no hay elementos de orden 4.

12. Sea G un grupo $x \in G$ y $m, n \in \mathbf{Z}$. Probar que $x^{m+n} = x^m x^n$.

    Esquema de solución: La cuestión es simple si $m, n \geq 0$ ó $m + n = 0$. Los casos a analizar son:

    $m, n < 0$: Entonces, $m + n < 0$ y

    $$x^{m+n} = (x \overset{-(m+n)}{\cdots\cdots} x)^{-1} = [(x \overset{-n}{\cdots} x)(x \overset{-m}{\cdots} x)]^{-1} = (x \overset{-m}{\cdots} x)^{-1}(x \overset{-n}{\cdots} x)^{-1} = x^m x^n$$

    $m > 0, n < 0, m + n > 0$

    $$x^{m+n} = (x \overset{(m+n)}{\cdots} x) = (x \overset{m}{\cdots\cdots} x)(x \overset{-n}{\cdots} x)^{-1} = x^m x^n$$

    $m > 0, n < 0, m + n < 0$

    $$x^{m+n} = (x \overset{-(m+n)}{\cdots} x)^{-1} = (x \overset{m}{\cdots} x)(x \overset{-n}{\cdots\cdots} x)^{-1} = x^m x^n$$