1 Grupos monógenos y cíclicos

Recordemos que, dado un grupo G , para cada $x \in G$ el subconjunto

$$\langle x \rangle = \{x^n \mid n \in \mathbf{Z}\}$$

es un subgrupo de G , que se dice subgrupo monógeno de generador x . Nótese que se trata del subgrupo *más pequeño* que contiene a x ; la primera cuestión es

$$\langle x \rangle = G \quad \text{ó} \quad \langle x \rangle \subsetneq G$$

Definición 1.1 *Un grupo G se dice monógeno si existe $x \in G$ tal que $G = \langle x \rangle$.*

Ejemplo $(\mathbf{Z}, +)$ y $(\mathbf{Z}/n\mathbf{Z}, +)$ son monógenos de generador 1. Veamos que *en esencia* no hay más.

Proposición 1.2 *Un grupo monógeno es isomorfo a un cociente de $\mathbf{Z}$, y como consecuencia, es abeliano.*

Demostración: Sea $f: \mathbf{Z} \rightarrow G$ dado por $f(m) = x^m$. Se trata de un homomorfismo, que es epi por ser G monógeno; el primer teorema de isomorfía da:

$$\mathbf{Z}/\ker f \cong G$$

Observación 1.3 Veremos que $\ker f = n\mathbf{Z}$ y los grupos monógenos son $\mathbf{Z}$ y $\mathbf{Z}/n\mathbf{Z}$; es decir, el único grupo monógeno infinito es, salvo isomorfismos de grupo, $\mathbf{Z}$. Puede verse que $(\mathbf{Z}, +)$ no es isomorfo¹ a $(\mathbf{Q}, +)$, aunque son biyectivos.

Definición 1.4 *Un grupo monógeno finito se llama cíclico.*

Observación 1.5 Nótese que hay un grupo cíclico de cualquier orden n , $\mathbf{Z}/n\mathbf{Z}$. La propiedad clave de los grupos cíclicos es que constituyen el primer recíproco al teorema de Lagrange. Necesitamos analizar los subgrupos de $\mathbf{Z}/n\mathbf{Z}$.

Lema 1.6 *Los subgrupos de $\mathbf{Z}/n\mathbf{Z}$ son de la forma de $m\mathbf{Z}/n\mathbf{Z}$ con $m \mid n$.*

Demostración: Por el teorema de la correspondencia inversa basta ver que

$$n\mathbf{Z} \leq S \leq \mathbf{Z} \implies S = m\mathbf{Z}, \quad m \mid n$$

Al efecto, tómesese el menor entero positivo m de S ; así, $m\mathbf{Z} \subseteq S$; por división euclídea cada elemento de S es múltiplo de m y $S \subseteq m\mathbf{Z}$. Finalmente,

$$n \in m\mathbf{Z} \implies m \mid n$$

Teorema 1.7 *Sea G un grupo cíclico de orden n .*

- i) *Para cada divisor d de n existe un único subgrupo S de orden d .*
- ii) *S es cíclico.*
- iii) *Todos los subgrupos de un grupo cíclico son cíclicos.*

Demostración: Antes de leer la demostración se recomienda examinar un caso concreto; por ejemplo $\mathbf{Z}/12\mathbf{Z}$.

¹Si $m/n = f(1)$, $f(z) = zm/n$, pero si b no divide a n , $1/b \neq zm/n, \forall z$

Sea $n = dr$.

i) *Existencia*: G debe ser isomorfo a un cociente de $\mathbf{Z}$, que por órdenes será $\mathbf{Z}/n\mathbf{Z}$. Ahora, $r\mathbf{Z}/n\mathbf{Z}$ es un subgrupo de $\mathbf{Z}/n\mathbf{Z}$ y

$$n = |\mathbf{Z}/n\mathbf{Z}| = |r\mathbf{Z}/n\mathbf{Z}| \cdot |(\mathbf{Z}/n\mathbf{Z})/(r\mathbf{Z}/n\mathbf{Z})| = |r\mathbf{Z}/n\mathbf{Z}| \cdot |\mathbf{Z}/r\mathbf{Z}| = |r\mathbf{Z}/n\mathbf{Z}|r$$

Por tanto, $|r\mathbf{Z}/n\mathbf{Z}| = d$. Tómesese en G la imagen isomorfa de $r\mathbf{Z}/n\mathbf{Z}$.

Unicidad: Sea S un subgrupo de G de orden d y sea $m\mathbf{Z}/n\mathbf{Z}$ su imagen isomorfa en $\mathbf{Z}/n\mathbf{Z}$. Entonces, como antes $n = md$ y $m = r$.

ii) Veremos que $\mathbf{Z}/n\mathbf{Z}$ posee un subgrupo cíclico de orden d y la tesis se deduce por la unicidad.

Al efecto, tomando $n = rd$, el subconjunto $\{r + n\mathbf{Z}, 2r + n\mathbf{Z}, \dots, dr + n\mathbf{Z}\}$ de $\mathbf{Z}/n\mathbf{Z}$ cumple:

- (Opuesto) $ar + n\mathbf{Z} + (d - a)r + n\mathbf{Z} = dr + n\mathbf{Z} = 0$
- (Cerrado para la suma)

$$ar + n\mathbf{Z} + br + n\mathbf{Z} = (a + b)r + n\mathbf{Z} = c + n\mathbf{Z}$$

y $c - (a + b)r$ múltiplo de n , luego de r . Así c es un número acotado por n múltiplo de r , luego $c = sr, s = 1, \dots, d$. Por tanto, $ar + n\mathbf{Z} + br + n\mathbf{Z} = sr + n\mathbf{Z} \in \{r + n\mathbf{Z}, 2r + n\mathbf{Z}, \dots, dr + n\mathbf{Z}\}$,

que resulta ser un subgrupo, claramente cíclico de orden r .

iii) Basta aplicar el teorema de Lagrange y los items anteriores.

Observación 1.8 Dado $x \in G$ el subgrupo $\langle x \rangle$ puede ser finito o no. Si no es finito decimos que $o(x)$ es infinito; en caso de finitud², existen $m \neq p$ tales que $x^m = x^p$. Por tanto, existe $n > 0$ tal que $x^n = e$. Se dice orden de x a

$$o(x) = \min\{n > 0 \mid x^n = e\}$$

Corolario 1.9 Sea $x \in G$ y supongamos que $o(x)$ es finito. Entonces, $\langle x \rangle$ es cíclico y $o(x) = |\langle x \rangle|$. Como consecuencia³, en un grupo finito el orden de cada elemento es divisor del orden del grupo.

²lo que ocurre siempre si G es finito

³del teorema de Lagrange

Demostración: Si $o(x)$ es finito, $\langle x \rangle = \{x^m \mid m \in \mathbf{Z}\}$ es finito, luego cíclico. Por tanto, $\langle x \rangle$ es isomorfo a $\mathbf{Z}/n\mathbf{Z}$ para algún n . Este isomorfismo permite describir los elementos de $\langle x \rangle$ como, $\langle x \rangle = \{x, x^2, \dots, x^n = e\}$ y

$$|\langle x \rangle| = n = o(x)$$

EJERCICIOS

1. Probar que el cociente de un grupo monógeno es monógeno; determínese su generador.
2. Descríbanse todos los subgrupos de $\mathbf{Z}/12\mathbf{Z}$.
3. Pruébese que todo grupo de orden primo es cíclico. Descríbanse sus posibles generadores.
4. Dado $x \in G$ de orden n pruébese
 - $x^m = e \implies n \mid m$
 - $o(x^k) = n/(k, n)$

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

7. Si G es abeliano, y $\text{mcd}(o(x), o(y)) = 1$, $o(xy) = o(x)o(y)$
8. Un grupo finito abeliano, contiene un elemento cuyo orden es

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

9. Probar que un grupo finito abeliano es cíclico si y sólo si su exponente coincide con el orden del grupo.
10. Probar que un subgrupo finito del grupo multiplicativo de un cuerpo es cíclico.
11. Compruébese que el grupo de las simetrías del rectángulo no puede ser cíclico.