

El grupo finito cíclico $\{0, 1, \dots, n-1\}$

Objetivos. Mostrar que el conjunto $\{0, 1, \dots, n-1\}$ con cierta operación binaria es un grupo isomorfo al grupo $\mathbb{Z}_n$.

Prerrequisitos. El grupo $\mathbb{Z}_n$, isomorfismos de grupos.

En este tema suponemos que $n \in \mathbb{N}$.

Denotamos por G_n el conjunto $\{0, 1, \dots, n-1\}$:

$$G_n := \{k \in \mathbb{Z}: 0 \leq k < n\}.$$

Lema 1. Si $a, b \in G_n$ y $a + b \geq n$, entonces $a + b - n \in G_n$.

Demostración. En efecto, las suposiciones $a < n$, $b < n$ implican que $a + b < 2n$. Tenemos que $n \leq a + b < 2n$ y por eso $0 \leq a + b - n < n$. $\square$

Definición 2. Definimos $\oplus: G_n^2 \rightarrow G_n$,

$$a \oplus b := \begin{cases} a + b, & a + b < n; \\ a + b - n, & a + b \geq n. \end{cases}$$

Observación 3. Gracias al lema, es fácil ver que la definición es consistente, en el sentido que $a + b \in G_n$ para cualesquier a, b en G_n .

Proposición 4. La operación $\oplus$ es conmutativa.

Demostración. Se sigue fácilmente de la definición. $\square$

Proposición 5. La operación $\oplus$ es asociativa:

$$(a \oplus b) \oplus c = a \oplus (b \oplus c) \quad (a, b, c \in G_n).$$

Demostración. Si $a, b, c \in G_n$, entonces la expresión $a + b$ puede ser $< n$ o $\geq n$, la expresión $b + c$ puede ser $< n$ o $\geq n$, y la expresión $a + b + c$ puede ser $< n$ o entre n y $2n-1$, o $\geq 2n$.

Algunos casos son imposibles: por ejemplo, si $a + b \geq n$, entonces $a + b + c$ no puede ser $< n$.

Tenemos los siguientes casos que parecen posibles.

1. $a + b < n$, $b + c < n$, $a + b + c < n$,
2. $a + b < n$, $b + c < n$, $n \leq a + b + c < 2n$,
3. $a + b < n$, $b + c \geq n$, $n \leq a + b + c < 2n$,

$$4. a + b \geq n, b + c < n, n \leq a + b + c < 2n,$$

$$5. a + b \geq n, b + c \geq n, n \leq a + b + c < 2n,$$

$$6. a + b \geq n, b + c \geq n, a + b + c \geq 2n.$$

Hagamos una verificación de la propiedad asociativa solamente para el caso 3:

$$\begin{aligned} (a \oplus b) \oplus c &\stackrel{a+b < n}{=} (a + b) \oplus c \stackrel{(a+b)+c \geq n}{=} ((a + b) + c) - n \\ &\stackrel{b\mathbb{Z} \text{ es un grupo}}{=} a + (b + c - n) \stackrel{a+(b+c-n) < n}{=} a \oplus (b + c - n) \\ &\stackrel{b+c \geq n}{=} a \oplus (b \oplus c). \end{aligned}$$

Los demás casos se consideran de manera similar. □

Proposición 6. *0 es el elemento neutro de G_n .*

Demostración. En efecto, para cada a en G_n , tenemos que $a + 0 < n$, por eso

$$a \oplus 0 = a + 0 = a. \quad \square$$

Proposición 7. *Para cada a en G_n , el siguiente elemento es el inverso aditivo de a :*

$$\ominus a := \begin{cases} 0, & a = 0; \\ n - a, & a > 0. \end{cases}$$

Demostración. Si $a = 0$, entonces

$$a \oplus (\ominus a) = 0 + 0 = 0.$$

Si $a > 0$, entonces

$$a \oplus (\ominus a) = a \oplus (n - a) \stackrel{a+(n-a) \geq n}{=} a + (n - a) - n = 0. \quad \square$$

Teorema 8. *G_n con la operación $\oplus$ es un grupo conmutativo.*

Demostración. Se sigue de las proposiciones anteriores. □

Definición 9. Definimos $\varphi: G_n \rightarrow \mathbb{Z}_n$,

$$\varphi(k) := k + n\mathbb{Z}.$$

Proposición 10. *φ es una biyección.*

Demostración. 1. Propiedad inyectiva. Supongamos que $a, b \in G_n$ y $\varphi(a) = \varphi(b)$. Esto implica que

$$a + n\mathbb{Z} = b + n\mathbb{Z}$$

y $a - b \in n\mathbb{Z}$. Luego existe q en $\mathbb{Z}$ tal que $a - b = nq$, y

$$|a - b| = n|q|.$$

Por otro lado, las desigualdades $0 \leq a < n$, $0 \leq b < n$ implican que

$$-n < a - b < n,$$

esto es, $|a - b| < n$. De aquí se sigue que $|q| < 1$. Como $q \in \mathbb{Z}$, concluimos que $q = 0$ y $a = b$.

2. Propiedad suprayectiva. Sea $X \in \mathbb{Z}_n$. Tomamos $c \in X$. Entonces, $X = c + n\mathbb{Z}$. Usando el algoritmo de división encontramos d en $\mathbb{Z}$ y r en G_n tales que

$$c = dn + r.$$

Como $c - r \in n\mathbb{Z}$, tenemos que $X = c + n\mathbb{Z} = r + n\mathbb{Z} = \varphi(r)$. □

Corolario 11. *El conjunto $\mathbb{Z}_n$ tiene exactamente n elementos.*

Proposición 12. *Para cada a, b en G_n ,*

$$\varphi(a \oplus b) = \varphi(a) + \varphi(b).$$

Demostración. Si $a + b < n$, entonces

$$\varphi(a \oplus b) = \varphi(a + b) = a + b + n\mathbb{Z} = (a + n\mathbb{Z}) + (b + n\mathbb{Z}) = \varphi(a) + \varphi(b).$$

Si $a + b \geq n$, entonces

$$\begin{aligned} \varphi(a \oplus b) &= \varphi(a + b - n) = (a + b - n) + n\mathbb{Z} \\ &= a + b + n\mathbb{Z} = (a + n\mathbb{Z}) + (b + n\mathbb{Z}) = \varphi(a) + \varphi(b). \end{aligned} \quad \square$$

Observación 13. Usando la biyección φ y la Proposición 12, podemos demostrar de otra manera que G_n es un grupo. Por ejemplo, la propiedad asociativa se puede demostrar así:

$$\varphi((a \oplus b) \oplus c) = \varphi(a \oplus b) + \varphi(c) = (\varphi(a) + \varphi(b)) + \varphi(c) = \varphi(a) + (\varphi(b) + \varphi(c)) = \varphi(a \oplus (b \oplus c)).$$

Como φ es inyectiva, concluimos que

$$(a \oplus b) \oplus c = a \oplus (b \oplus c).$$

Teorema 14. *φ es un isomorfismo de grupos.*

Demostración. Se sigue de la Proposición 12, cuando ya sabemos que G_n y $\mathbb{Z}_n$ son grupos. □