Isomorfismo entre el grupo finito cíclico y el grupo de las raíces de la unidad

Objetivos. Construir un isomorfismo entre el grupo $\mathbb{Z}_n$ y el grupo

$$R_n \coloneqq \{z \in \mathbb{C}\colon\ z^n = 1\}.$$

Prerrequisitos. Grupos $\mathbb{Z}_n = \mathbb{Z}/(n\mathbb{Z})$ y $G_n = \{0, 1, \ldots, n-1\}$, isomorfismo entre G_n y $\mathbb{Z}_n$, propiedades de la función exponencial.

Repaso 1 (propiedades de la función "exponencial imaginaria")**.** La función $E\colon \mathbb{R} \to \mathbb{T}$,

$$E(x) \coloneqq \exp(\mathrm{i}\, x),$$

es suprayectiva, es un homomorfismo y tiene núcleo $\ker(E) = 2\pi\mathbb{Z}$. Más aún, si $z \in \mathbb{T}$, entonces existe un único número x en $[0, 2\pi)$ tal que $E(x) = z$.

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

Definición 2. $R_n \coloneqq \{z \in \mathbb{C}\colon\ z^n = 1\}$.

Proposición 3. $R_n \subseteq \mathbb{T}$.

Demostración. Si $z^n = 1$, entonces $|z|^n = 1$ y $|z| = 1$. □

Proposición 4. *R_n es un grupo.*

Demostración. Mostremos que R_n es un subgrupo de $\mathbb{T}$. Si $z, w \in R_n$, entonces

$$(zw)^n = z^n w^n = 1.$$

Si $z \in R_n$, entonces

$$(z^{-1})^n = \frac{1}{z^n} = 1.$$

□

Definición 5. $\varepsilon_n \coloneqq \exp \frac{2\pi\,\mathrm{i}}{n}$.

Repaso 6. Sabemos que para cada k en $\mathbb{Z}$,

$$\varepsilon_n^k = 1 \qquad \Longleftrightarrow \qquad k \in n\mathbb{Z}.$$

Como consecuencia, para cada j, k en $\mathbb{Z}$,

$$\varepsilon_n^j = \varepsilon_n^k \qquad \Longleftrightarrow \qquad j - k \in n\mathbb{Z}.$$

Lema 7. *Si $j, k \in G_n$ y $j - k \in n\mathbb{Z}$, entonces $j = k$.*

Demostración. Si $0 \le j < n$ y $0 \le k < n$, entonces $-n < k \le 0$ y

$$-n < j - k < n,$$

así que $|j-k| < n$. Por otro lado, como $j - k \in n\mathbb{Z}$, obtenemos que $|j-k| \in n\mathbb{Z}$. Si $|j-k| = nq$ con q en $\mathbb{Z}$, entonces $|q| < 1$ y por eso $q = 0$. □

Teorema 8. *Definimos* $f\colon G_n \to R_n$,

$$f(k) \coloneqq \varepsilon_n^k.$$

Entonces, f *es un isomorfismo de grupos.*

Demostración. 1. Mostremos que f es un homomorfismo. Sean $j, k \in G_n$. Si $j + k < n$, entonces

$$f(j \oplus k) = f(j+k) = \varepsilon_n^{j+k} = \varepsilon_n^j \varepsilon_n^k = f(j)f(k).$$

Si $j + k \ge n$, entonces

$$f(j \oplus k) = f(j+k-n) = \varepsilon_n^{j+k-n} = \varepsilon_n^j \varepsilon_n^k \varepsilon_n^{-n} = f(j)f(k) \cdot 1 = f(j)f(k).$$

2. Mostremos que f es inyectiva. Si $j, k \in G_n$ y $f(j) = f(k)$, entonces $\varepsilon_n^j = \varepsilon_n^k$ y luego $j - k \in n\mathbb{Z}$. Por el Lema 7, concluimos que $j = k$.

3. Mostremos que f es sobre. Sea $z \in R_n$. Luego $z \in \mathbb{T}$. Por las propiedades de E, existe un único x en $[0, 2\pi)$ tal que $E(x) = z$. Además,

$$E(nx) = E(x)^n = z^n = 1.$$

Por lo tanto, $nx \in 2\pi\mathbb{Z}$, es decir, existe k en $\mathbb{Z}$ tal que

$$nx = 2\pi k.$$

De la desigualdad $0 \le x < 2\pi$ se sigue que $0 \le k < n$, es decir, $k \in G_n$. Finalmente,

$$z = \exp(\mathrm{i}\, nx) = \exp \frac{2\pi k\, \mathrm{i}}{n} = \varepsilon_n^k.$$

4. Otra demostración que f es sobre. Sea $p(z) \coloneqq z^n - 1$. Entonces, R_n es el conjunto de las raíces del polinomio p:

$$R_n = \big\{ z \in \mathbb{C} \colon\ p(z) = 0 \big\}.$$

Como p es un polinomio de grado n, el conjunto R_n tiene $\le n$ elementos. Como ya sabemos que f es inyectiva y G_n tiene n elementos, concluimos que f es sobre. □

Corolario 9. R_n *tiene exactamente* n *elementos.*

Corolario 10.

$$z^n - 1 = \prod_{k=0}^{n-1} (z - \varepsilon_n^k).$$

Demostración. Sean

$$p(z) \coloneqq z^n - 1, \qquad q(z) \coloneqq \prod_{k=0}^{n-1} \big(z - \varepsilon_n^k\big).$$

Como los números ε_n^k, donde $k \in G_n$, son raíces de p y son diferentes entre si, concluimos que $q \mid p$. Luego, como p y q son mónicos y tienen grado n, concluimos que $p = q$. □

Ejercicio 11. Construir un isomorfismo natural entre $\mathbb{Z}_n$ y R_n. Se puede considerar la función $g\colon \mathbb{Z} \to R_n$,

$$g(k) \coloneqq \varepsilon_n^k.$$

Mostrar que g realmente toma valores en R_n, es un epimorfismo, y $\ker(g) = n\mathbb{Z}$. Aplicar el primer teorema de isomorfismos.