Caracteres del grupo finito cíclico

Recordamos que si G es un grupo abeliano localmente compacto, entonces los *caracteres* de G se definen como homomorfismos continuos $G \to \mathbb{T}$, donde $\mathbb{T} = \{z \in \mathbb{C}\colon\ |z| = 1\}$. El conjunto de todos los caracteres de G se denota por $\widehat{G}$. Este conjunto se considera con la operación de multiplicación natural (multiplicación de funciones punto a punto) y forma un grupo que se llama el *grupo dual* de G.

En este tema suponemos que n es un número entero fijo con $n \geq 2$. Denotamos $\exp \frac{2\pi \mathrm{i}}{n}$ por ε_n.

Recordemos que $\mathbb{Z}_n$ se define como el grupo cociente $\mathbb{Z}/(n\mathbb{Z})$.

Proposición 1. *Sean $a, b \in \mathbb{Z}$ y $p, q \in \mathbb{Z}$ tales que*

$$a - b \in n\mathbb{Z}, \qquad p - q \in n\mathbb{Z}.$$

Entonces

$$\varepsilon_n^{pa} = \varepsilon_n^{qb}.$$

Demostración. Notamos que

$$pa - qb = pa - pb + pb - qb = p(a - b) + (p - q)b \in n\mathbb{Z}.$$

Luego $\varepsilon_n^{pa} = \varepsilon_n^{qb}$. □

Definición 2. Sea $P \in \mathbb{Z}_n$. Definimos $\varphi_P\colon \mathbb{Z}_n \to \mathbb{T}$ mediante la regla

$$\varphi_P(A) := \varepsilon_n^{pa},$$

donde $p \in P$, $a \in A$. La Proposición 1 justifica que esta definición es consistente.

Proposición 3. *Sea $P \in \mathbb{Z}_n$. Entonces $\varphi_P \in \widehat{\mathbb{Z}_n}$.*

Demostración. La función φ_P es continua porque la topología en $\mathbb{Z}_n$ es discreta, es decir, cualquier subconjunto de $\mathbb{Z}_n$ es abierto. Sean $A, B \in \mathbb{Z}_n$, $p \in P$, $a \in A$, $b \in B$. Entonces $a + b \in A + B$,

$$\varphi_P(A + B) = \varepsilon_n^{p(a+b)} = \varepsilon_n^{pa}\varepsilon_n^{pb} = \varphi_P(A)\varphi_P(B).$$ □

Definición 4. Definimos $\Phi\colon \mathbb{Z}_n \to \widehat{\mathbb{Z}_n}$ mediante la regla

$$\Phi(P) := \varphi_P.$$

Proposición 5. Φ *es un isomorfismo de grupos.*

Demostración. I. Sean $P, Q \in \mathbb{Z}_n$ y sea $A \in \mathbb{Z}_n$. Eligimos $p \in P$, $q \in Q$, $a \in A$. Entonces $p + q \in Q$,

$$\Phi(P+Q)(A) = \varepsilon_n^{(p+q)a} = \varepsilon_n^p \varepsilon_n^q = \Phi(P)(A)\Phi(Q)(A) = (\Phi(P)\Phi(Q))(A).$$

Como A es arbitrario, concluimos que $\Phi(P+Q) = \Phi(P)\Phi(Q)$.

II. Sea $P \in \mathbb{Z}_n$ tal que $\varphi_P = 1_{\mathbb{Z}_n}$. Sea $p \in P$. Apliquemos φ_P a la clase $1 + n\mathbb{Z}$:

$$1 = 1_{\mathbb{Z}_n}(1 + n\mathbb{Z}) = \varphi_P(1 + n\mathbb{Z}) = \varepsilon_n^p.$$

De aquí concluimos que $p \in n\mathbb{Z}$, esto es, P es el elemento neutro de $\mathbb{Z}_n$.

III. Sea $\psi \in \widehat{\mathbb{Z}_n}$. Pongamos $\alpha \coloneqq \psi(1 + n\mathbb{Z})$. Entonces

$$\alpha^n = \psi(1 + n\mathbb{Z})^n = \psi\left(\underbrace{(1 + n\mathbb{Z}) + \cdots + (1 + n\mathbb{Z})}_{n \text{ veces}}\right) = \psi(n + n\mathbb{Z}) = \psi(n\mathbb{Z}) = 1.$$

Luego existe p en $\mathbb{Z}$ tal que $\alpha = \varepsilon_n^p$. Pongamos $P \coloneqq p + n\mathbb{Z}$. Ahora para cualquier k en $\mathbb{Z}$ tenemos

$$\psi(k + n\mathbb{Z}) = \psi(1 + n\mathbb{Z})^k = \alpha^k = \varepsilon_n^{pk} = \varphi_P(k + n\mathbb{Z}).$$

Hemos mostrado que $\psi = \varphi_P = \Phi(P)$. □