

Ortogonalidad de caracteres sobre un grupo conmutativo finito

Objetivos. Demostrar las relaciones de ortogonalidad de caracteres sobre un grupo conmutativo finito.

Estos apuntes están basados en el libro Lidl, Niederreiter, “Finite fields”, 2nd. ed., 1997.

Usamos la notación aditiva para el grupo G .

Proposición 1 ($\hat{G}$ separa los elementos de G , repaso). Si G es un grupo conmutativo finito, $x, y \in G$, $x \neq y$, entonces existe χ en $\hat{G}$ tal que $\chi(x) \neq \chi(y)$.

Definición 2. Denotemos por $1_{\hat{G}}$ al caracter constante 1:

$$1_{\hat{G}}(x) := 1 \quad (x \in G).$$

Es el elemento neutro del grupo $\hat{G}$.

Proposición 3. Si G es un grupo conmutativo finito y $\varphi \in \hat{G}$, entonces

$$\frac{1}{\#G} \sum_{x \in G} \varphi(x) = \delta_{\varphi, 1_{\hat{G}}}.$$

Demostración. Si $\varphi = 1_{\hat{G}}$, entonces todos los sumandos en la suma valen 1.

Consideremos el caso $\varphi \neq 1_{\hat{G}}$. Encontramos a en G tal que $\varphi(a) \neq 1$. Denotamos la suma por S :

$$S := \sum_{x \in G} \varphi(x).$$

Hacemos en la suma el cambio de variable $y = x - a$. Usamos el hecho que la función $x \mapsto x - a$ es una biyección.

$$S = \sum_{y \in G} \varphi(y + a) = \sum_{y \in G} \varphi(y) \varphi(a) = S \varphi(a).$$

De aquí se sigue que $(\varphi(a) - 1)S = 0$ y $S = 0$. □

Lema 4. El grupo $\hat{G}$ es finito.

Demostración. Sea $n := \#G$. Si $\varphi \in \hat{G}$, entonces los valores de φ pertenecen al conjunto

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

Como $\hat{G} \subseteq R_n^G$ y $\#R_n = n$, concluimos que $\#\hat{G} \leq n^n$. □

Proposición 5. Si G es un grupo conmutativo finito y $x \in G$, entonces

$$\frac{1}{\#G} \sum_{\varphi \in \hat{G}} \varphi(x) = \delta_{x,0_G}.$$

Demostración. Sea

$$S := \sum_{\varphi \in \hat{G}} \varphi(x).$$

Si $x = 0_G$, entonces cada sumando en la suma es 1.

Supongamos que $x \neq 0_G$. Usando la Proposición 1 encontramos χ en $\hat{G}$ tal que $\chi(x) \neq 1$. Es fácil de ver que la función $\varphi \mapsto \varphi\bar{\chi}$ es una biyección del grupo $\hat{G}$. Usamos esta función como el cambio de variable en la suma:

$$S \stackrel{\psi=\varphi\bar{\chi}}{=} \sum_{\psi \in \hat{G}} \psi(x)\chi(x) = S\chi(x).$$

De aquí $S(\chi(x) - 1) = 0$ y $S = 0$. □

Proposición 6. $\#\hat{G} = \#G$.

Demostración. Consideremos la suma doble

$$s = \sum_{\varphi \in \hat{G}} \sum_{x \in G} \varphi(x).$$

Por la Proposición 3,

$$s = \sum_{\varphi \in \hat{G}} \delta_{\varphi,1_{\hat{G}}} \#G = \#\hat{G}.$$

Por otro lado, podemos cambiar el orden de las sumas, y la Proposición 5 obtenemos

$$s = \sum_{x \in G} \sum_{\varphi \in \hat{G}} \varphi(x) = \sum_{x \in G} \#\hat{G} \delta_{x,0_G} = \#G. \quad \square$$

Proposición 7. Si $x, y \in G$, entonces

$$\frac{1}{\#G} \sum_{\varphi \in \hat{G}} \varphi(x) \overline{\varphi(y)} = \delta_{x,y}.$$

Demostración. Ejercicio. Poner $z := x - y$. □

Proposición 8. Si $\varphi, \psi \in \hat{G}$, entonces

$$\frac{1}{\#G} \sum_{x \in G} \varphi(x) \overline{\psi(x)} = \delta_{\varphi,\psi}.$$

Demostración. Ejercicio. Poner $\chi := \varphi\bar{\psi}$. □