

Formas bilineales sobre un grupo conmutativo finito

Estos apuntes están basados en el libro Tao, Vu “Additive combinatorics”.

Objetivos. Definir el concepto de formas bilineales (o biaditivas) $G \times G \rightarrow \mathbb{R}/\mathbb{Z}$, donde G es un grupo abeliano finito.

Prerrequisitos. Descomposición de grupos abelianos finitos en grupos cíclicos.

Definición 1. Sea G un grupo (usamos la notación aditiva para la operación en G). Una función $f: G^2 \rightarrow \mathbb{R}/\mathbb{Z}$ se llama *bilineal* o *biaditiva*, si

$$\begin{aligned}\forall \xi, x, y \in G & \quad f(\xi, x + y) = f(\xi, x) + f(\xi, y), \\ \forall \xi, \eta, x \in G & \quad f(\xi + \eta, x) = f(\xi, x) + f(\eta, x).\end{aligned}$$

Observación 2. Sea $f: G^2 \rightarrow \mathbb{R}/\mathbb{Z}$. Dado γ en G , definimos $g_{1,\gamma}: G \rightarrow \mathbb{R}/\mathbb{Z}$,

$$g_{1,\gamma}(x) := f(\gamma, x).$$

Dado a en G , definimos $g_{2,a}: G \rightarrow \mathbb{R}/\mathbb{Z}$,

$$g_{2,a}(\xi) := f(\xi, a).$$

La definición de forma bilineal se puede escribir en términos de estas funciones: para cada γ en G , $g_{1,\gamma}$ es un homomorfismo, y para cada a en G , $g_{2,a}$ es un homomorfismo.

Ejercicio 3. Demostrar que para cada x, ξ en G ,

$$f(0_G, x) = 0, \quad f(\xi, 0_G) = 0.$$

Definición 4. Una forma bilineal $f: G^2 \rightarrow \mathbb{R}/\mathbb{Z}$ se llama *no degenerada*, si

$$\left(\forall \xi \in G \setminus \{0_G\} \quad \exists x \in G \quad f(\xi, x) \neq 0 \right) \quad \wedge \quad \left(\forall x \in G \setminus \{0_G\} \quad \exists \xi \in G \quad f(\xi, x) \neq 0 \right).$$

Definición 5. Una forma bilineal $f: G^2 \rightarrow \mathbb{R}/\mathbb{Z}$ se llama *simétrica*, si

$$\forall x, y \in G \quad f(x, y) = f(y, x).$$

Proposición 6. Sea $n \in \mathbb{N}$, $n \geq 2$. Si $A = a + n\mathbb{Z} \in \mathbb{Z}_n$, $B = b + n\mathbb{Z}$, entonces

$$\frac{AB}{n} + \mathbb{Z} = \frac{ab}{n} + \mathbb{Z}.$$

Demostración. $\subseteq$. Sea $x \in \frac{AB}{n} + \mathbb{Z}$. Por las definiciones de la suma de Minkowski y producto de Minkowski de dos conjuntos, existen $u \in A$, $v \in B$, $w \in \mathbb{Z}$ tales que

$$x = \frac{uv}{n} + w.$$

Notemos que

$$x - \frac{ab}{n} = \frac{uv - ub + ub - ab}{n} + w = \frac{u(v - b)}{n} + \frac{(u - a)b}{n} + w \in \mathbb{Z},$$

así que $x \in \frac{ab}{n} + \mathbb{Z}$.

$\subseteq$. Como $a \in A$, $b \in B$, tenemos que

$$\frac{ab}{n} \in \frac{AB}{n}.$$

Ejercicio: completar la demostración. □

Proposición 7. $\mathbb{Z} + \mathbb{Z} = \mathbb{Z}$.

Demostración. $\subseteq$. Esta contención se sigue del hecho que la suma de dos números enteros es un número entero.

$\supseteq$. Dado x en $\mathbb{Z}$, tenemos que

$$x = x + 0 \in \mathbb{Z} + \mathbb{Z}. \quad \square$$

Ejemplo 8. Sea $n \in \mathbb{N}$, $n \geq 2$. Para $G = \mathbb{Z}_n$, definimos $f: \mathbb{Z}_n^2 \rightarrow \mathbb{R}/\mathbb{Z}$,

$$f(A, B) := \frac{AB}{n} + \mathbb{Z}.$$

Gracias al resultado de la Proposición 6, sabemos que el lado derecho es un elemento de $\mathbb{R}/\mathbb{Z}$, así que la definición es consistente.

Probemos que f es aditiva respecto al primer argumento. Aplicamos las Proposiciones 6 y 7. También usamos el hecho que la adición de Mikowski es asociativa.

$$\begin{aligned} f((\xi + n\mathbb{Z}) + (\eta + n\mathbb{Z}), x + n\mathbb{Z}) &= f((\xi + \eta) + n\mathbb{Z}, x + n\mathbb{Z}) = \frac{(\xi + \eta)x}{n} + \mathbb{Z} \\ &= \frac{\xi x}{n} + \frac{\eta x}{n} + \mathbb{Z} = \left(\frac{\xi x}{n} + \mathbb{Z} \right) + \left(\frac{\eta x}{n} + \mathbb{Z} \right) \\ &= f(\xi + n\mathbb{Z}, x) + f(\eta + n\mathbb{Z}, x). \end{aligned}$$

Obviamente, f es simétrica. Por lo tanto, f es aditiva respecto al segundo argumento.

Probemos que f es no degenerada. Si $a + n\mathbb{Z}$ y $a \notin n\mathbb{Z}$, entonces

$$f(a + n\mathbb{Z}, 1 + n\mathbb{Z}) = \frac{a}{n} + \mathbb{Z} \neq 0 + \mathbb{Z}.$$

Ejercicio 9. Sea $\varphi: G \rightarrow H$ un homomorfismo de grupos (usemos la notación aditiva para las operaciones en G y H). Muestre que las siguientes propiedades son equivalentes:

- $\varphi(0_G) \neq 0_H$;
- φ no es la función constante cero, es decir, existe x en G tal que $\varphi(x) \neq 0_H$.

Los homomorfismos con estas propiedades se llaman *no triviales*.

Teorema 10. *Cada grupo conmutativo finito tiene una forma bilineal simétrica no degenerada.*

Demostración. Sea G un grupo conmutativo finito. Sabemos que G es una suma directa de grupos cíclicos, es decir, existe m en $\mathbb{N}$ y existen grupos cíclicos $H_1, \dots, H_m$ tales que

$$G \cong \bigoplus_{j=1}^m H_j.$$

Elijamos un isomorfismo de grupos

$$\tau: G \rightarrow \bigoplus_{j=1}^m H_j.$$

Como vimos en el Ejemplo 8, en cada grupo cíclico finito existe una forma bilineal simétrica no degenerada. Para cada j en $\{1, \dots, m\}$, construyamos en H_j alguna forma bilineal simétrica no nula h_j . Definimos $f: G^2 \rightarrow \mathbb{R}/\mathbb{Z}$,

$$f(\xi, x) := \sum_{j=1}^m h_j(\tau(\xi)_j \tau(x)_j).$$

Es fácil de ver que f es una forma bilineal simétrica. Mostremos que f es no degenerada. Sea $x \in G$, $x \neq 0_G$. Como τ es un isomorfismo, $\tau(x)$ no es el elemento nulo de la suma directa. Encontremos r en $\{1, \dots, m\}$ tal que

$$\tau(x)_r \neq 0_{G_r}.$$

Como h_j es no degenerada, encontramos η en G_r tal que

$$h_r(\eta, \tau(x)_r) \neq 0_{\mathbb{R}/\mathbb{Z}}.$$

Sea e_r el siguiente elemento de la suma directa:

$$e_r := [\delta_{r,k}]_{k=1}^m.$$

Construimos

$$\xi := \tau^{-1}(\eta e_r).$$

Entonces,

$$f(\xi, x) = \sum_{j=1}^m h_j(\tau(\xi)_j \tau(x)_j) = \sum_{j=1}^m h_j(\eta \delta_{r,j}, \tau(x)_j) = h_r(\eta, \tau(x)_r) \neq 0_{\mathbb{R}/\mathbb{Z}}. \quad \square$$

Ejercicio 11. Consideremos el campo finito $\mathbb{F}_p := \mathbb{Z}_p$. Definimos $\varphi: \mathbb{F}_p \rightarrow \mathbb{R}/\mathbb{Z}$,

$$\varphi(x + p\mathbb{Z}) := \frac{x}{p} + \mathbb{Z}.$$

De manera equivalente,

$$\varphi(X) := \frac{X}{p}.$$

Muestre que φ es un homomorfismo no trivial.

Ejemplo 12. Sea $\varphi: \mathbb{F}_p \rightarrow \mathbb{R}/\mathbb{Z}$ el homomorfismo del ejercicio anterior. Como G , consideramos el espacio vectorial $\mathbb{F}_p^d$. Definimos $f: G^2 \rightarrow \mathbb{R}/\mathbb{Z}$,

$$f(\xi, x) := \varphi \left(\sum_{j=1}^d \xi_j x_j \right).$$

Se puede mostrar que la definición de f es consistente. Es fácil de ver que f es una forma bilineal simétrica. Mostremos que f es no degenerada. Sea $x \in \mathbb{F}_p^d$, $x \neq 0_{\mathbb{F}_p^d}$. Definimos m como el elemento mínimo del soporte de x :

$$m := \min \{ k \in \{1, \dots, d\} : x_k \neq 0_{\mathbb{F}_p} \}.$$

Notemos que $x_m \neq 0_{\mathbb{F}_p}$. Como $\mathbb{F}_p$ es un campo, el elemento x_m tiene un inverso.

Sea e_m el m -ésimo vector de la base canónica de $\mathbb{F}_p^d$:

$$e_m = [\delta_{m,k}]_{k=1}^d.$$

Como ξ , tomamos el vector e_m dividido entre x_m :

$$\xi := \frac{1}{x_m} e_m.$$

Entonces,

$$\sum_{k=1}^d \xi_k x_k = \xi_m x_m = 1_{\mathbb{F}_p}.$$

Como φ es un homomorfismo no trivial,

$$f(\xi, x) = \varphi(1_{\mathbb{F}_p}) \neq 0_{\mathbb{R}/\mathbb{Z}}.$$