

EL ORDEN DE UN PRODUCTO DE ELEMENTOS EN UN GRUPO ABELIANO

Vimos en clase que dados dos elementos a, b de un grupo abeliano G con $\text{ord}(a) = n$ y $\text{ord}(b) = m$, al tenerse

$$(a \cdot b)^{[n,m]} = a^{[n,m]} \cdot b^{[n,m]} = 1 \cdot 1 = 1,$$

el orden de $a \cdot b$ divide a $[n, m]$ (Recordar que el orden de un elemento x siempre divide a los exponentes k que cumplen $x^k = 1$.)

Nos preguntamos si sería siempre $[n, m]$ el orden del producto, pero vimos que no (tomando a de orden $n > 1$ y $b = a^{-1}$).

Nos fijamos si sería $[n, m]/(n, m)$, pero tampoco (tomando $a = (1, 0)$ y $b = (0, 1)$ en $\mathbb{Z}_2 \oplus \mathbb{Z}_6$).

Algo que sí vale es lo siguiente (ver: Teoría de Grupos, de Paul Dubreil ISBN 84-291-5071-4, página 51).

En el caso en que $(n, m) = 1$, se tiene $\text{ord}(a \cdot b) = [n, m] = n \cdot m$.

Veamos que $n | \text{ord}(a \cdot b)$ y $m | \text{ord}(a \cdot b)$.

Como $(a \cdot b)^m = a^m$, se tiene que $\text{ord}((a \cdot b)^m) = \text{ord}(a^m) = n / (n, m) = n$. Como una potencia del elemento $(a \cdot b)$ tiene orden n , se deduce que n divide al orden del grupo generado por $a \cdot b$, que es $\text{ord}(a \cdot b)$.

Análogamente se ve que $m | \text{ord}(a \cdot b)$, y luego $[n, m] = n \cdot m | \text{ord}(a \cdot b)$. Como siempre vale $\text{ord}(a \cdot b) | [m, n]$, se sigue que $\text{ord}(a \cdot b) = [n, m]$.