El grupo $\mathbb{Z}_n$

Objetivos. Definir el grupo $\mathbb{Z}_n \coloneqq \mathbb{Z}/(n\mathbb{Z})$ y estudiar sus propiedades elementales.

1. Congruencia módulo n. Es fácil ver que $n\mathbb{Z}$ es un subgrupo de $\mathbb{Z}$. Definimos la relación binaria $\overset{n}{\equiv}$ en $\mathbb{Z}$ mediante la regla

$$a \overset{n}{\equiv} b \qquad \Longleftrightarrow \qquad a - b \in n\mathbb{Z}.$$

En otras palabras,

$$a \overset{n}{\equiv} b \qquad \Longleftrightarrow \qquad n \mid (a - b).$$

Es fácil es una relación binaria. Denotamos por $\mathbb{Z}_n$ al conjunto de las clases de equivalencia. Cada clase de equivalencia es de la forma $k + n\mathbb{Z}$, donde $k \in \mathbb{Z}$.

2. $\mathbb{Z}_n$ consiste de n elementos diferentes entre si:

$$k + n\mathbb{Z}, \qquad k \in \{0, 1, \ldots, n-1\}.$$

3. La suma de dos conjuntos (repaso). Recordamos la definición de la suma de dos conjuntos. Si $A, B \subset \mathbb{Z}$, entonces

$$A + B \coloneqq \{c \in \mathbb{Z} \colon \quad \exists a \in A \quad \exists b \in B \quad c = a + b\}.$$

4. Proposición (sobre la adición en $\mathbb{Z}_n$). Si $A, B \in \mathbb{Z}_n$, entonces $A + B \in \mathbb{Z}_n$. Más precisamente, si $A = j + n\mathbb{Z}$, $B = k + n\mathbb{Z}$, entonces $A + B = (j + k) + n\mathbb{Z}$.

5. Definición de la adición en $\mathbb{Z}_n$. Definimos la adición, como en la proposición anterior.

6. Corolario. $\mathbb{Z}_n$ es un grupo conmutativo.

7. Notación para los múltiplos. Definimos ka, donde $a \in \mathbb{Z}_n$.

8. Definición del elemento generador de un grupo. Un elemento g de G se llama *generador* de G si cada elemento de G es una potencia de g (en la notación aditiva, un múltiplo).

9. Definición del grupo cíclico. Un grupo G se llama cíclico, si existe un elemento que genera G.

10. Grupo cíclico. $\mathbb{Z}_n$ es un grupo cíclico.

11. Sobre $\mathbb{Z}_n$ y las raíces de la unidad. Definimos la función $f \colon \mathbb{Z} \to C_n$ mediante la regla

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

Entonces f es un epimorfismo, su núcleo es $n\mathbb{Z}$, y por el teorema de isomorfismo $\mathbb{Z}_n$ es isomorfo a C_n.