Índice general

Capítulo 1

Divisibilidad en los números enteros

1.1. División entera. Ideales

Designaremos por $\mathbb{Z}$ el conjunto de los números enteros. La teoría de la divisibilidad en $\mathbb{Z}$ es consecuencia de la siguiente importante propiedad.

Teorema 1.1 (de la división entera). *Dados $a, b \in \mathbb{Z}$, $b \neq 0$, existen dos únicos números enteros q y r que cumplen $a = bq + r$, $0 \leq r < |b|$. Estos números q y r se llaman el cociente y el resto de la división entera de a por b.*

Ejemplo 1.1.

$$-8 = 3 \cdot (-3) + 1, \quad 3 = (-8) \cdot 0 + 3$$

Si el resto de la división entera de a por b es 0, se dice que a es un *múltiplo* de b (escribiremos $a \overset{\cdot}{=} b$), que b es un *divisor* de a (escribiremos $b \mid a$), o que a es *divisible* por b. Indicaremos por (b) el conjunto de los múltiplos de b. Observemos que (b) cumple las dos propiedades siguientes:

- es cerrado para la suma; es decir, $a, c \in (b) \Rightarrow a + c \in (b)$.
- si $a \in (b)$ y c es cualquier entero, entonces $ac \in (b)$.

Proposición 1.1. *Si el subconjunto $I \subset \mathbb{Z}$ cumple*

(1) $a, b \in I \Rightarrow a + b \in I$

(2) $a \in I, c \in \mathbb{Z} \Rightarrow ac \in I$

entonces existe un $b \in \mathbb{Z}$ tal que $I = (b)$.

Demostración. Si $I = \{0\}$, entonces $I = (0)$. Si I contiene un elemento no nulo a, también contiene $-a = a \cdot (-1)$, y o bien a o bien $-a$ es positivo. Por tanto, I contiene enteros positivos. Sea b el menor de los enteros positivos contenidos en I. Por (2), I contiene todos los múltiplos de b: $(b) \subset I$. Vamos a ver que $I \subset (b)$, y por tanto, $I = (b)$. En efecto, dado $a \in I$ cualquiera, por el teorema 1.1,

$$a = bq + r, \quad 0 \leq r < |b| = b$$

Por (1) y (2), $r = a - bq = a + b(-q) \in I$; pero $0 \leq r < |b| = b$ y b es el menor de los enteros positivos de I; así pues, $r = 0$, y por tanto $a = bq \in (b)$. □

Un subconjunto I que cumple las condiciones (1) y (2) de la proposición 1.1 se llama un *ideal* de $\mathbb{Z}$. El elemento b tal que $I = (b)$ se denomina *base* del ideal.

Ejercicio 1.1. *Demostrar que,*

$$(b) = (c) \textit{ si y sólo si } c = \pm b$$

Obsérvese que $(a) \subset (b)$ si y sólo si $b \mid a$. Las cuestiones de divisibilidad equivalen, por tanto, a cuestiones sobre inclusiones entre ideales.