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 $a = \dot{b}$), 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,*

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

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.

1.2. Mínimo común múltiplo y máximo común divisor

Dados números enteros $a_1, \ldots, a_n$, la intersección $(a_1) \cap \cdots \cap (a_n)$ es el conjunto de los números enteros múltiplos comunes de todos ellos de todos ellos. Este conjunto cumple las dos condiciones de la proposición 1.1, y por tanto, $(a_1) \cap \cdots \cap (a_n) = (m)$ para un m conveniente. Este m está carecterizado por las dos propiedades siguientes:

- m es múltiplo común de $a_1, \ldots, a_n$
- cualquier otro múltiplo común de $a_1, \ldots, a_n$ es múltiplo de m.

Diremos que m es el *mínimo común múltiplo* de $a_1, \ldots, a_n$ y escribiremos

$$m = \operatorname{mcm}(a_1, \ldots, a_n)$$

Observemos que también $-m$ es mínimo común múltiplo de $a_1, \ldots, a_n$.

Consideremos ahora la unión $(a_1) \cup \cdots (a_n)$. Este conjunto, en general, no cumple las condiciones de la proposición 1.1. Por ejemplo, $(2) \cup (3)$ no contiene el $5 = 2 + 3$. Formemos a partir de $(a_1) \cup \cdots \cup (a_n)$ un subconjunto I de $\mathbb{Z}$ que cumpla las condiciones de la proposición 1.1, Por la condición (1), I debe contener todas las sumas de múltiplos de $a_1, \ldots, a_n$: $a_1c_1 + \cdots + a_nc_n$. No hace falta ampliar más, el conjunto

$$I = \{a_1c_1 + \cdots + a_nc_n \mid c_1, \ldots, c_n \in \mathbb{Z}\}$$

cumple ya las condiciones de la proposición 1.1, y por tanto, existe un entero d tal que $I = (d)$. Denotaremos I por $(a_1, \ldots, a_n)$. Así pues, $I = (a_1, \ldots, a_n) = (d)$. Este número d está caracterizado por las dos propiedades siguientes:

- d es divisor común de $a_1, \ldots, a_n$, ya que ello equivale a a firmar que $a_i \in (d)$ para $i = 1, \ldots, n$. $(a_i = a_1 \cdot 0 + \cdots + a_i \cdot 1 + \cdots a_n \cdot 0 \in I)$.
- Cualquier otro divisor d' común a $a_1, \ldots, a_n$ divide a d. En efecto, que d' sea divisor de $a_1, \ldots, a_n$ significa que $a_i \in (d')$, $i = 1, \ldots, n$. Por tanto, $\{a_1c_1 + \cdots a_nc_n \mid c_i \in \mathbb{Z}\} \subset (d')$, es decir, $(d) \subset (d')$, lo cual implica que d' es un divisor de d.

El recíproco también es cierto.

Diremos que d es el *máximo común divisor* de $a_1, \ldots, a_n$ y escribiremos

$$d = \operatorname{mcd}(a_1, \ldots, a_n)$$

También $-d$ es máximo común divisor.

Observemos que el máximo común divisor d es una suma de múltiplos de $a_1, \ldots, a_n$

$$d = a_1r_1 + \cdots + a_nr_n$$

Esta expresión es conocida como *identidad de Bézout.*

Acabaremos este apartado con un método práctico de cálculo del máximo común divisor y de la identidad de Bézout. El método se basa en el siguiente resultado:

Proposición 1.2. *Sea $a = bq + r$ la división entera de a por b. Entonces,*

$$\operatorname{mcd}(a, b) = \operatorname{mcd}(b, r)$$