LOS NÚMEROS ENTEROS. INTRODUCCIÓN.

Un número entero se puede descomponer en producto de números más pequeños; así por ejemplo

$$36 = 9 \times 4 = 3^2 \times 2^2 \times 1.$$

También los polonomios con coeficientes enteros pueden descomponerse en producto de polinomios de grados más pequeños; así por ejemplo

$$x^3 - x^2 + x - 1 = (x^2 + 1)(x - 1).$$

Tanto el conjunto de los enteros $\mathbb{Z}$ como un conjunto de polinomios $\mathbb{F}[x]$, este conjunto va a depender del conjunto de coeficiente $\mathbb{F}$ que elijamos, son ejemplos de anillos conmutativos. Como estructuras algebraicas se parecen mucho. Vamos a estudiar sus propiedades. En el caso de los enteros vamos a recordarlas y veremos que las de los polinomios se parecen a las anteriores. Así, tanto números como polinomios tienen un **Teorema de Factorización** que nos dice como **descomponerlos** en factores mas simples. **Potencias de primos** en el caso de los enteros y en polinomios **irreducibles** en el caso de los polinomios. En este último caso el conjunto de coeficientes $\mathbb{F}$ es esencial para comprender la descomposión. En los casos más útiles el conjunto $\mathbb{F}$ será un cuerpo finito. De ahí los temas que dedicaremos a cuerpos.

Veremos que el **algoritmo de Euclides** es la pieza básica para operar tanto con número como con polinomios.

El cálculo efectivo para descomponer un número grande o un polinomio de grado alto puede ser muy costoso. Puede llevar mucho tiempo realizarlo con los algoritmos que hoy se conocen. Este "coste" está en la base de emplear números y polinomios "grandes", cuya descomposición se conoce, para encriptar información.

Entre el estudio de $\mathbb{Z}$ y el de los polinomios hemos de pasar a comprender los grupos finitos. Los conceptos de **grupo cíclico**, la relación entre los **ordenes de los grupos** y él de sus **subgrupos**, así como la **clasificación de los grupos finitos** abelianos están detrás de la aplicaciones que iremos presentando a lo largo de los siguientes temas.

Referencias

Departamento de Análisis Matemático, Facultad de Matemáticas, Universidad Complutense, 28040 Madrid, Spain
E-mail address: Cesar_Ruiz@mat.ucm.es