AMPLIACIÓN DE MATEMÁTICAS

INTRODUCCIÓN

Recordemos que $\mathbb{R}$ es la recta real o equivalentemente el *cuerpo* de los números reales.

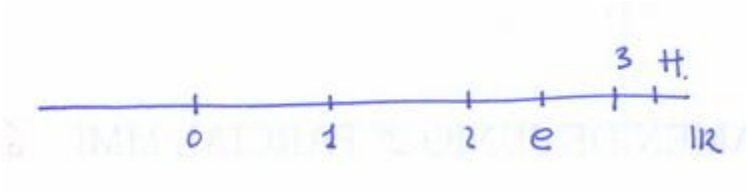

FIGURA 1. La recta real

Una "deformación"de $\mathbb{R}$ o de una parte suya no es más que una función f, que en este curso llamaremos *señal*.

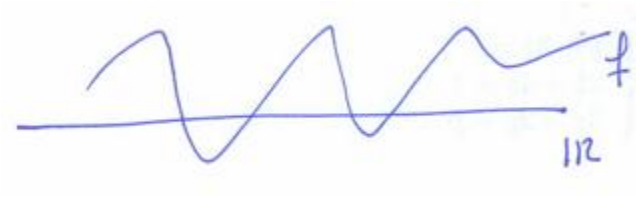

FIGURA 2. Gráfico de f

Las funciones más sencillas son los polinomios:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0,$$

donde $a_0, a_1, ..., a_n \in \mathbb{R}$ (en la segunda parte del curso estos coeficientes los tomaremos en cuerpos finitos).

En primer curso vimos que algunas funciones se pueden escribir como un "polinomio infinito", en forma de serie de Taylor

$$f(x) = \sum_{n=0}^{\infty} a_n (x-a)^n, \qquad \text{donde} \qquad a_n = \frac{f^{n)}(a)}{n!}\,.$$

Ejemplo 1. *La función exponencial tiene por desarrollo de Taylor*

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}.$$

En la primera parte de este curso vamos a ver como una señal empírica f, es decir unos datos muestreados, o medidos a intervalos de tiempos constantes, de cierto fenómeno (por ejemplo la vibración que produce un temblor de tierra o un sonido al propagarse), se puede recoger con una fórmula matemática del tipo:

$$f(t) = \frac{a_0}{2} + \sum_{n=1}^{\infty} a_n \cos(\frac{2\pi n t}{w}) + b_n \operatorname{sen}(\frac{2\pi n t}{w}) \qquad \text{(serie de Fourier de} f),$$

donde t es el tiempo y $f(t)$ es el valor de la magnitud que medimos. Los valores $\{\frac{n}{w} : n \in \mathbb{N}\}$ son las $frecuencias$ que forman el fenómeno. Veremos que les ocurre a estas frecuencias cuando las pasamos por un filtro RLC

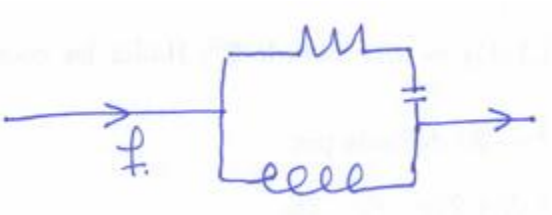

FIGURA 3. Circuito RLC

En la segunda parte del curso nos vamos a interesar por la estructura de cuerpo, es decir

Definición 1. *Un conjunto* $\mathbb{K}$ *se dice que es un cuerpo si sobre él hay definidas dos operaciones, usualmente una suma y un producto de modo que con la suma*

$$+ : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$$
$$(x, y) \to x + y$$

forma un Grupo Abeliano, es decir se verifican las propiedades:

1. *Asociativa:* $\forall x, y, z \in \mathbb{K},\ (x+y)+z = x+(y+z)$.
2. *Conmutativa:* $\forall x, y \in \mathbb{K},\ x+y = y+x$.
3. *Elemento Neutro:* $\exists r \in \mathbb{K}$ *para el cuál* $r+x = x+r = x,\ \forall x \in \mathbb{K}$ *(notación* $r = 0$*).*
4. *Elemento Opuesto:* $\forall x \in \mathbb{K}$ *existe un único* y *de modo que* $x+y = y+x = 0$ *(notación* $y = -x$*).*

Y con el producto

$$\times : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$$

$$(x, y) \to x \times y \qquad (o \qquad xy)$$

forma un Grupo Abeliano multiplicativo, es decir se verifican las propiedades

1. *Asociativa:* $\forall x, y, z \in \mathbb{K},\ (xy)z = x(yz)$.
2. *Conmutativa:* $\forall x, y \in \mathbb{K},\ xy = yx$.
3. *Elemento Neutro:* $\exists r \in \mathbb{K}$ *para el cuál* $rx = xr = x,\ \forall x \in \mathbb{K}$ *(notación* $r = 1$*).*
4. *Elemento Inverso:* $\forall x \in \mathbb{K}\backslash\{0\}$ *existe un único* y *de modo que* $xy = yx = 1$ *(notación* $y = x^{-1} = \frac{1}{x}$*).*

Además se verifica la propiedad Distributiva, es decir

$$\forall x, y, z \in \mathbb{K}, \qquad x(y+z) = xy + xz.$$

Ejemplos 1. *Los conjuntos de números racionales* $\mathbb{Q}$ *o reales* $\mathbb{R}$ *o complejos* $\mathbb{C}$*, son cuerpos en cada caso. Se verifican las propiedades usuales de las operaciones con números. Pero también los conjuntos* $\mathbb{Z}_p$*,* p *primo, con la suma y el producto en congruencias también son ejemplos de cuerpos, como veremos.*

Estos últimos ejemplos lo son de cuerpos finitos. Nos vamos a interesar por el problema de descomponer polinomios sobre cuerpos finitos. Este problema es semejante al de descomponer números enteros en sus factores primos, pero más complejo. De esa complejidad viene su uso en criptografía.

Ejemplos 2. *El polinomio* x^2+1 *no se puede descomponer sobre* $\mathbb{R}$*, es decir no existe números reales* a *y* b *de manera que*

$$x^2 + 1 = (x-a)(x-b).$$

Sin embargo sobre $\mathbb{C}$ *si se puede hacer esa descomposión,* $x^2+1 = (x-i)(x+i)$. *En* $\mathbb{Z}_2$, *también es posible hacer la descomposición* $x^2+1 = (x+1)^2$, *aunque esta última fórmula es bastante chocante.*

Referencias

Departamento de Análisis Matemático, Facultad de Matemáticas, Universidad Complutense, 28040 Madrid, Spain

E-mail address: Cesar_Ruiz@mat.ucm.es