AMPLIACIÓN DE MATEMÁTICAS

EJEMPLOS DE EXTENSIONES DE CUERPOS.

Comenzamos con el primer ejemplo. Aquí ya vamos a ver las ideas que después desarrollaremos.

Ejemplo 1. *Consideramos el polinomio $x^2 - 2 \in \mathbb{Q}[x]$ (o también lo podemos ver como un elemento de $\mathbb{Z}[x]$). No tiene raíces en $\mathbb{Q}$ y por tanto **no** se puede descomponer. Si se pudiese*

$$x^2 - 2 = (ax + b)(a'x + b') \qquad \Rightarrow \qquad \alpha = \frac{-b}{a} \ \ y \ \ \alpha' = \frac{-b'}{a'}$$

serían raíces del polinomio y no pertenecen a $\mathbb{Q}$.

¿Existe algún cuerpo mayor que $\mathbb{Q}$ donde el polinomio $x^2 - 2$ tenga raíces y por tanto pueda ser descompuesto?

- Una primera respuesta nos la da el cuerpo de los números reales, $\mathbb{R}$, que contiene a $\mathbb{Q}$ como **subcuerpo**; allí si existe $\sqrt{2}$. Esta forma de proceder no nos interesa mucho (**extensiones transcendentes de cuerpos).**
- Otra forma de abordar el mismo problema es la que sigue. El problema que tenemos es que en $\mathbb{Q}$ no existe un número que al cuadrado de 2. ¡ Inventémoslo ! LLamamos α a un número con la propiedad de que $\alpha^2 = 2$ (por simplicidad notaremos $\alpha = \sqrt{2}$). Ahora definimos el conjunto

  $$\mathbb{Q}[\sqrt{2}] = \{\, a + b\sqrt{2} \ \ : \ \ a, b \in \mathbb{Q} \,\}.$$

  Sobre el damos dos operaciones,

  - **una suma:**

  $$(a + b\sqrt{2}) + (a' + b'\sqrt{2}) = (a + a') + (b + b')\sqrt{2} \in \mathbb{Q}[\sqrt{2}];$$

  - **un producto:**

  $$(a + b\sqrt{2})(a' + b'\sqrt{2}) = (aa' + 2bb') + (ab' + a'b)\sqrt{2} \in \mathbb{Q}[\sqrt{2}].$$

Ahora es fácil ver que $(\mathbb{Q}[\sqrt{2}], +, \times)$ es un cuerpo, que contiene a $\mathbb{Q}$ y donde

$$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2}).$$

Demostración: El elemento $0 + 0\sqrt{2} = 0$ es el elemento neutro de la suma.

El elemento $1 + 0\sqrt{2} = 1$ es el elemento neutro de la multiplicación.

Lo único un poco más elaborado que tenemos que ver es como encontrar el inverso respecto de todo elemento $a+b\sqrt{2}$ con $b \neq 0$. Será un elemento $a' + b'\sqrt{2}$ de modo que $(a + b\sqrt{2})(a' + b'\sqrt{2}) = 1$ y por tanto

$$\begin{array}{ccccc} aa' & + & 2bb' & = & 1 \\ ba' & + & ab' & = & 0. \end{array}$$

Como el determinante de los coeficientes del sistema es

$$\left| \begin{array}{cc} a & 2b \\ b & a \end{array} \right| = a^2 - 2b^2 \neq 0 \qquad (\text{en otro caso} \qquad (\frac{a}{b})^2 = 2\,),$$

el sistema tiene solución única. El elemento inverso.

Ahora la identificación $a = a + 0\sqrt{2}$ para todo $a \in \mathbb{Q}$, nos dice que

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] \subset \mathbb{R}.$$

El polinomio $x^2 - 2$ lo podemos ver como un elemento de $\mathbb{Q}[\sqrt{2}][x]$. Aquí ya existe la raíz cuadrada de 2 y por tanto podemos descomponer el polinomio $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ □

Observación 1. *La construcción anterior es análoga a la que se hace para construir los números complejos a partir de los reales. En este caso nos "inventabamos" el número imaginario con la propiedad* $i^2 = -1$.

Tanto $\mathbb{C}$ *como* $\mathbb{Q}[\sqrt{2}]$ *son espacios vectoriales de dimensión dos respecto de los cuerpos* $\mathbb{R}$ *y* $\mathbb{Q}$ *respectivamente. Claro, en el primer caso* $1 + 0i$ *y* $0 + i$ *forma una base;* $1 + 0\sqrt{2}$ *y* $0 + \sqrt{2}$ *lo hace en el segundo caso.*

Son ejemplos de ***extensiones algebraicas de cuerpos.***

Ejemplo 2. *Consideramos el polinomio*

$$\begin{aligned} p(x) &= (x - \sqrt{2})(x + \sqrt{2})(x - 2\sqrt{2})(x + 2\sqrt{2}) \\ &= (x^2 - 2)(x^2 - 8) = x^4 - 10x^2 + 16 \in \mathbb{Q}[x]. \end{aligned}$$

En este caso, p es un polinomio que no tiene raíces en $\mathbb{Q}$ (tiene sus cuatro raíces en $\mathbb{Q}[\sqrt{2}]$), pero sin embargo es **reducible.**

Ejemplo 3. *Consideramos el polinomio*

$$\begin{aligned} p(x) &= (x-\sqrt{2})(x+\sqrt{2})(x-\sqrt{3})(x+\sqrt{3}) \\ &= (x^2-2)(x^2-3) = x^4-5x^2+6 \in \mathbb{Q}[x]. \end{aligned}$$

Ahora, p es reducible en $\mathbb{Q}[x]$; tiene dos raíces en $\mathbb{Q}[\sqrt{2}]$ (por tanto en $\mathbb{Q}[\sqrt{2}][x]$ es reducible también), pero $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$.
Demostración: Si

$$(a+b\sqrt{2})^2 = 3 \;\Leftrightarrow\; a^2+2ab\sqrt{2}+2b^2 = 3$$

y despejando

$$\sqrt{2} = \frac{3-a^2-2b^2}{2ab} \in \mathbb{Q}$$

ya que $a, b \in \mathbb{Q}$. Hemos llegado a contradicción, lo que quiere decir que nuestro suposición inicial no es cierta $\square$

En el Ejemplo 2. p es un polinomio sin raíces en $\mathbb{Q}$. Con un raíz ($\sqrt{2}$) se puede generar un cuerpo ($\mathbb{Q}[\sqrt{2}]$) en el cuál p tiene todas sus raíces (**cuerpo de descomposición)**.

En el ejemplo siguiente, p no tiene ninguna raíz en $\mathbb{Q}$. Pero no parece que con una única raíz, o al menos con una cualquiera, podamos fabricar un "cuerpo de descomposición" para el polinomio.

Conocer un polinomio irreducible sobre un cuerpo conocido y encontrar una única raíz que permita encontrar el cuerpo donde se pueden encontrar todas las raíces del polinomio (y por tanto una descomposición completa del mismo), es decir el **cuerpo de descomposición** del polinomio, es un hecho esencial en Criptografía.

Ejemplo 4. *Consideramos el polinomio* $x^2-2 \in \mathbb{Z}_3[x]$. *Este polinomio es irreducible en* $\mathbb{Z}_3$ *ya que no existe* $r \in \mathbb{Z}_3$ *de modo que* $r^2 = 2$ *y el polinomio es de grado* 2.

Para encontrar un cuerpo donde el polinomio tenga raíces, procedemos como en el primer ejemplo. El problema que tenemos es que en $\mathbb{Z}_3$ no existe un número que al cuadrado de 2. ¡ Inventémoslo ! LLamamos α a un número con la propiedad de que $\alpha^2 = 2$. Ahora definimos el conjunto

$$\mathbb{Z}_3[\alpha] = \{\, a+b\alpha \;\; : \;\; a, b \in \mathbb{Z}_3 \,\}.$$

Sobre el damos dos operaciones,

- **una suma:**

$$(a + b\alpha) + (a' + b'\alpha) = (a + a') + (b + b')\alpha \in \mathbb{Z}_3[\alpha];$$

- **un producto:**

$$(a + b\alpha)(a' + b'\alpha) = (aa' + 2bb') + (ab' + a'b)\alpha \in \mathbb{Z}_3[\alpha].$$

Ahora es fácil ver que $(\mathbb{Z}_3[\alpha], +, \times)$ es un cuerpo, que contiene a $\mathbb{Z}_3$ y donde

$$x^2 - 2 = (x - \alpha)(x - 2\alpha).$$

Demostración: En primer lugar observemos que $\mathbb{Z}_3[\alpha]$ es un conjunto finito. En efecto,

$$\mathbb{Z}_3[\alpha] = \{\, 0, 1, 2, \alpha, 2\alpha, 1 + \alpha, 1 + 2\alpha, 2 + \alpha, 2 + 2\alpha \,\}$$

De aquí deducimos claramente que $\mathbb{Z}_3 \subset \mathbb{Z}_3[\alpha]$. Además haciendo la tabla de multiplicar:

$(\mathbb{Z}_3[\alpha]^*, \times)$	1	2	α	2α	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$
1	1	2	α	2α	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$
2	2	1	2α	α	$2+2\alpha$	$2+\alpha$	$1+2\alpha$	$1+\alpha$
α	α	2α	2	1	$2+\alpha$	$1+\alpha$	$2+2\alpha$	$1+2\alpha$
2α	2α	α	1	2	$1+2\alpha$	$2+2\alpha$	$1+\alpha$	$2+\alpha$
$1+\alpha$	$1+\alpha$	$2+2\alpha$	$2+\alpha$	$1+2\alpha$	2α	2	1	α
$1+2\alpha$	$1+2\alpha$	$2+\alpha$	$1+\alpha$	$2+2\alpha$	2	α	2α	1
$2+\alpha$	$2+\alpha$	$1+2\alpha$	$2+2\alpha$	$1+\alpha$	1	2α	α	2
$2+2\alpha$	$2+2\alpha$	$1+\alpha$	$1+2\alpha$	$2+\alpha$	α	1	2	2α

vemos que todos los números tienen inverso respecto del producto.

Por otro lado, como $\alpha^2 = 2$ y mirando la diagonal de la tabla $(2\alpha)^2 = 2$ $(-\alpha = 2\alpha)$ se tiene que

$$x^2 - 2 = (x - \alpha)(x - 2\alpha) \ \square$$

Observación 2. *El cardinal de $\mathbb{Z}_3$ es 3. El cardinal del nuevo cuerpo $\mathbb{Z}_3[\alpha]$ es nueve ($9 = 3^2$, el exponente 2 coincide con el grado del polinomio). Veremos que esto no es casual.*

Los ejemplos anteriores muestran nuestra línea argumental de los siguientes capítulos:

- Veremos que fijado un polinomio siempre existe un cuerpo donde este polinomio tiene al menos una raíz.

- Ampliando el cuerpo, si fuese necesario, encontraremos un cuerpo donde el polinomio tiene todas sus raíces (tantas como el grado). Es el **cuerpo de descomposición** del polinomio.
- Hay varias formas de extender un cuerpo. Transcendentes como pasar de $\mathbb{Q}$ a $\mathbb{R}$. Lo cuál no nos va a interesar.

  O las extensiones **algebraicas**, como las de pasar de $\mathbb{Q}$ o $\mathbb{Z}_3$ a $\mathbb{Q}[\sqrt{2}]$ o $\mathbb{Z}_3[\alpha]$ respectivamente. Estas si nos van a interesar.
- En el caso de los **cuerpos finitos**, el **cardinal** de estos cuerpos no es cualquiera sino siempre una potencia de un primo (este primo no es más que la **característica** del cuerpo, como en el caso de $\mathbb{Z}_3$ y $\mathbb{Z}_3[\alpha]$).
- Dado un polinomio irreducible de grado k con coeficientes en un cuerpo finito de cardinal n, el cuerpo que construimos para encontrar al menos una raíz del polinomio va a tener cardinal igual a n^k.

Referencias

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