AMPLIACIÓN DE MATEMÁTICAS

EXTENSIONES DE CUERPOS.

Dado un cuerpo $\mathbb{F}$, nos interesa a veces encontrar un cuerpo más grande $\mathbb{K}$, de modo que el primero sea subcuerpo del segundo y que en $\mathbb{K}$ podamos encontrar algo que no es posible encontrar en $\mathbb{F}$. Por ejemplo raíces de un polinomio.

Aquí vamos a estudiar en abstracto las **extensiones de cuerpos**, aunque la que más nos interesa ya la hemos visto con el Teorema de Kronecker.

Definición 1. *Sea $\mathbb{F}$ un cuerpo y $\mathbb{K}$ una extensión del primer cuerpo.*

- **a:** *Un elemento $a \in \mathbb{K}$ se llama **algebraico**, con respecto al subcuerpo $\mathbb{F}$, si existe un polinomio $f \in \mathbb{F}[x]$ de modo que a es raíz de f, ($\overline{f}(a) = 0$).*
- **b:** *Los elemento de $\mathbb{K}$ que **no** son algebraicos se llaman **transcendentes.***
- **c:** *Una extensión de cuerpo $\mathbb{K}$ con respecto al cuerpo $\mathbb{F}$ se dice que es una **extensión algebraica** si todos los elementos de $\mathbb{K}$ son algebraicos.*
- **d:** *Una extensión de cuerpo $\mathbb{K}$ de $\mathbb{F}$ se llama transcendente si al menos un elemento de $\mathbb{K}$ es transcendente.*
- **e:** *Se llama **grado** de la extensión a la **dimensión** del espacio vectorial $\mathbb{K}$ respecto del cuerpo $\mathbb{F}$. (**Notación:** $[\mathbb{K} : \mathbb{F}] = \dim \mathbb{K}$).*
- **f:** *Se dice que una extensión de cuerpo es **finita** si $[\mathbb{K} : \mathbb{F}] = \dim \mathbb{K} < \infty$.*

Ejemplo 1. *$\mathbb{Q} \subset \mathbb{R}$ es una extensión de cuerpo **transcendente.***

Demostración: En $\mathbb{R}$ hay muchos más elementos que en $\mathbb{Q}$,

$$\text{Card}\mathbb{Q} = \text{Card}\mathbb{N} < \text{Card}\mathbb{R}$$

Ahora

$$\begin{array}{c}\text{Card}\{r \in \mathbb{R} \ : \ r \text{ raíz de un polinomio de } \ \mathbb{Q}[x] \ \} \\ =\text{Card} \bigcup_{n=1}^{\infty}\{r \in \mathbb{R} \ : \ r \text{ raíz de un polinomio de grado } \ n \text{ de } \mathbb{Q}[x] \ \} \\ =\text{Card}\mathbb{N} <\text{Card}\mathbb{R}.\end{array}$$

Luego en $\mathbb{R}$ hay muchos elementos que son transcendentes $\square$

Observación 1. *Es fácil ver que $\sqrt{2} \in \mathbb{R}\backslash\mathbb{Q}$ es algebraico ya que es raíz del polinomio $x^2 - 2 \in \mathbb{Q}[x]$. Sin embargo, ver que un elemento concreto de $\mathbb{R}$ es transcendente (por ejemplo $\pi \in \mathbb{R}$) es bastante difícil.*

Ejemplo 2. $\mathbb{R} \subset \mathbb{C}$ *es una extensión* ***algebraica*** *y* ***finita****.*

Demostración: Para todo $a + bi \in \mathbb{C}$, se tiene que

$$(x - (a + bi))(x - (a - bi)) = x^2 - 2ax + a^2 + b^2 \in \mathbb{R}[x].$$

Así vemos que todos los elementos de $\mathbb{C}$ son algebraicos con respecto a $\mathbb{R}$. Además, es claro que $\{1, i\}$ forman una base de $\mathbb{C}$ como espacio vectorial sobre $\mathbb{R}$. Luego $[\mathbb{C} : \mathbb{R}] = \dim \mathbb{C} = 2$ $\square$

Ejemplo 3. $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}]$ *es una extensión* ***algebraica*** *y* ***finita****.*

Demostración: Para todo $a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, se tiene que

$$(x - (a + b\sqrt{2}))(x - (a - b\sqrt{2})) = x^2 - 2ax + a^2 - 2b^2 \in \mathbb{Q}[x].$$

Así vemos que todos los elementos de $\mathbb{Q}[\sqrt{2}]$ son algebraicos con respecto a $\mathbb{Q}$. Además, es claro que $\{1, \sqrt{2}\}$ forman una base de $\mathbb{Q}[\sqrt{2}]$ como espacio vectorial sobre $\mathbb{Q}$. Luego $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = \dim \mathbb{Q}[\sqrt{2}] = 2$ $\square$

Proposición 1. *Sea $\mathbb{F}$ un cuerpo y sea $f \in \mathbb{F}[x]$ un polinomio de grado k. Entonces el anillo cociente*

$$\mathbb{F}[x]/f = \{ \ a_0 + a_1[x] + ... + a_{k-1}[x]^{k-1} \ : \ a_0, a_1, ..., a_{k-1} \in \mathbb{F} \ \}$$

es un espacio vectorial k-dimensional sobre el cuerpo $\mathbb{F}$ con base las potencias de la clase de la x

$$\{ \ 1, [x], [x]^2, ..., [x]^{k-1} \ \}.$$

Demostracción: Vimos que $\mathbb{F}[x]/f$ esta formado por las clases de los posibles restos de dividir por f en $\mathbb{F}[x]$. Es decir todos los polinomios en $\mathbb{F}[x]$ de grado menor o igual que $k - 1$, es decir

$$a_0 + a_1x + ... + a_{k-1}x^{k-1}$$

donde $a_0, a_1, ..., a_{k-1} \in \mathbb{F}$ (los coeficientes se pueden repetir y algunos pueden ser 0). Por tanto

$$\mathbb{F}[x]/f = \{[a_0 + a_1 x + ... + a_{k-1}x^{k-1}] \ : \ a_0, a_1, ..., a_{k-1} \in \mathbb{F}\}$$
$$= \{a_0 + a_1[x] + ... + a_{k-1}[x]^{k-1} \ : \ a_0, a_1, ..., a_{k-1} \in \mathbb{F}\}.$$

El conjunto anterior es como el espacio vectorial de vectores

$$\mathbb{F}^k = \{(a_0, a_1, ..., a_{k-1}) \ : \ a_0, a_1, ..., a_{k-1} \in \mathbb{F} \}$$

con la suma de vectores y el producto de un escalar por un vector habituales. Por tanto $\mathbb{F}[x]/f$ es un espacio vectorial sobre el cuerpo $\mathbb{F}$. Una base está formada, por lo visto arriba, por

$$\{ [1], [x], [x]^2, ..., [x]^{k-1} \}.$$

El que son independientes es sencillo de ver; si existe $a_0, a_1, ..., a_{k-1} \in \mathbb{F}$, no todos nulos, de modo que

$$[0] = \sum_{j=0}^{k-1} a_j [x]^j = [\sum_{j=0}^{k-1} a_j x^j],$$

entonces $f|(\sum_{j=0}^{k-1} a_j x^j)$ y como $grad.(\sum_{j=0}^{k-1} a_j x^j) = k-1 < grad.f$, se tiene que $\sum_{j=0}^{k-1} a_j x^j = 0$.

Como el cardinal de la base es k, la dimensión del espacio vectorial es k ($[\mathbb{F}[x]/f : \mathbb{F}] = k$) $\square$

Proposición 2. *Toda extensión finita $\mathbb{K}$ de un cuerpo $\mathbb{F}$ es algebraica.*

Demostracción: Sea $\alpha \in \mathbb{K}$. Consideramos la aplicación

$$\begin{array}{rccccc} T_\alpha & : & \mathbb{F}[x] & \to & \mathbb{K} & \\ & & f & \to & T_\alpha(f) & = & \overline{f}(\alpha). \end{array}$$

T_α es una aplicación lineal entre dos espacios vectoriales sobre el cuerpo $\mathbb{F}$. La dimensión de $\mathbb{F}[x]$ es infinita, mientras que la dimensión de $\mathbb{K}$ es finita por hipótesis. Por tanto la aplicación T_α **no** puede ser inyectiva (si lo fuese la dimensión de $\mathbb{F}[x]$ sería menor o igual que la de $\mathbb{K}$) y por tanto el núcleo de la aplicación $kerT_\alpha \neq \{0\}$. Así existe $f \in kerT_\alpha \subset \mathbb{F}[x]$ con $f \neq 0$ de modo que $\overline{f}(\alpha) = 0$. Lo cuál prueba que α es un elemento algebraico $\square$

Teorema 1. *Sea $\mathbb{F}$ un cuerpo y sea $f \in \mathbb{F}[x]$ un polinomio **irreducible** de grado k. Entonces $\mathbb{F}[x]/f$ es una extensión del cuerpo $\mathbb{F}$ algebraica y finita, con $[\mathbb{F}[x]/f : \mathbb{F}] = k$.*

Demostracción: Por ser el polinomio f irreducible, ya vimos (Teoría de Anillos; Teorema de Kronecker) que el anillo cociente $\mathbb{F}[x]/f$ es un cuerpo. Además la inclusión

$$\begin{array}{rccccc} i & : & \mathbb{F} & \to & \mathbb{F}[x]/f & \\ & & r & \to & i(r) & = & [r] \end{array}$$

hace que $\mathbb{F}$ sea un subcuerpo de $\mathbb{F}[x]/f$. La Proposición primera nos dice que esta extensión es finita ($[\mathbb{F}[x]/f : \mathbb{F}] = k$) y por tanto la segunda Proposición nos dice que también es algebraica $\square$

Ejemplo 4. *Consideramos el polinomio* $f(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$.

El anillo cociente que genera este polinomio es

$$\mathbb{Z}_2[x]/(x^3 + x + 1) = \{a + b[x] + c[x^2] \ : \ a, b, c \in \mathbb{Z}_2 \ \}$$

$$= \{\, 0, 1, [x], 1 + [x], [x]^2, 1 + [x]^2, [x] + [x]^2, 1 + [x] + [x]^2 \,\}$$

Estamos ante un espacio vectorial sobre $\mathbb{Z}_2$ de dimensión 3, ya que una base está formada por

$$\{\ 1, [x], [x]^2\ \}.$$

Además en este caso como, el polinomio f es de grado 3 y $\overline{f(0)} = 1$ y $\overline{f}(1) = 1$ (no tiene raíces en $\mathbb{Z}_2$), el polinomo es irreducible y $\mathbb{Z}_2[x]/(x^3+x+1)$ es una extensión del cuerpo $\mathbb{Z}_2$, algebraica y finita $\square$

Ejemplo 5. *Consideramos el polinomio* $f(x) = x^2 + 1 \in \mathbb{Z}_3[x]$.

Este polinomio de grado dos no tiene raíces en $\mathbb{Z}_3$ (¡comprobad!). Por tanto el anillo cociente que genera es también una extensión del cuerpo $\mathbb{Z}_3$, de modo que

$$\mathbb{Z}_3[x]/(x^2 + 1) = \{a + b[x] \ : \ a, b \in \mathbb{Z}_3 \ \}$$

$$= \{\, 0, 1, 2, [x], 2[x], 1 + [x], 1 + 2[x], 2 + [x], 2 + 2[x] \,\} \ \square$$

Ejemplo 6. *Consideramos el polinomio* $f(x) = x^2 + 1 \in \mathbb{R}[x]$.

Este polinomio de grado dos no tiene raíces en $\mathbb{R}$. Por tanto el anillo cociente que genera es también una extensión del cuerpo $\mathbb{R}$, de modo que

$$\mathbb{R}[x]/(x^2 + 1) = \{a + b[x] \ : \ a, b \in \mathbb{R} \ \}.$$

Es una extensión finita y por tanto algebraica de $\mathbb{R}$. Observemos que en este caso la extensión **no** es un conjunto finito. Además como la clase

de la x es una raíz del polinomio (es decir $1+[x]^2=0$) identificando $[x]$ con el número imaginario i tenemos que $\mathbb{R}[x]/(x^2+1)$ es como $\mathbb{C}$ $\square$

Ejemplo 7. *Consideramos el polinomio* $f(x)=x^3+x+1$.

- Visto como un polinomio de $\mathbb{Z}_3[x]$, él no es irreducible ya que $\overline{f}(1)=0$. Por tanto, $\mathbb{Z}_3[x]/f$ **no** es un cuerpo. Esto no impide que la clase de la x tenga un inverso en $\mathbb{Z}_3[x]/f$. Veámoslo. Como $x \nmid x^3+x+1$, se tiene que

  $$m.c.d.(x, x^3+x+1)=1$$

  así por el Lema de Bezout, existen $v, u \in \mathbb{Z}_3[x]$ de modo que

  $$1=v(x)x+u(x)(x^3+x+1).$$

  En las operaciones en congruencias de $\mathbb{Z}_3[x]/f$, $u(x)(x^3+x+1)=0$, por tanto v es el inverso de x en $\mathbb{Z}_3[x]/f$. En concreto,

  $$x^3+x+1=0 \qquad \Rightarrow \qquad x(x^2+1)=-1=2$$

  Luego $x(2x^2+2)=1$ y así se tiene que $[x]^{-1}=[2x^2+2]$.

  Por otro lado, $x-1|x^3+x+1$, en concreto

  $$(x-1)(x^2+x+2)=x^3+x+1=0,$$

  luego $[x-1]$ es un divisor de cero en $\mathbb{Z}_3[x]/f$ y por tanto no puede tener inverso respecto del producto (en congruencias).
- Visto como un polinomio de $\mathbb{Z}_5[x]$, él es irreducible ya que es de grado 3 y además $\overline{f}(a)\neq 0$, para todo $a\in\mathbb{Z}_5$ (¡comprobad!). Por tanto $\mathbb{Z}_5[x]/f$ es un cuerpo y todo elemento en él, no nulo, tiene inverso. Así $[x-1]\in\mathbb{Z}_5[x]/f$ tiene inverso. ¿Cómo lo calculamos? Como $m.c.d.(x-1, x^3+x+1)=1$, el Lema de Bezout y el algoritmo de Euclides nos permiten calcular el inverso $\square$

Referencias

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