AMPLIACIÓN DE MATEMÁTICAS

TEOREMA DE EXTENSIÓN DE KRONECKER.

Los polinomios irreducibles sobre un cuerpo no tienen raíces sobre ese cuerpo, salvo que sean de grado uno. Ya hemos visto que

Ejemplo 1.
- $x^2 - 2 \in \mathbb{Q}[x]$ *es irreducible sobre* $\mathbb{Q}$.
- $x^2 - 2 \in \mathbb{Z}_3[x]$ *es irreducible sobre* $\mathbb{Z}_3$.

Los polinomios irreducibles que lo son en algunos cuerpos, siempre pueden ser descompuestos en un cuerpo mayor. Esto hace que en la Teoría de Cuerpos el estudio de las extensiones de cuerpos tenga un mayor protagonismo que el estudio de subcuerpos. En concreto.

Definición 1. *(**Extensiones de Cuerpos**).*

a: *Un subconjunto* $U \subset \mathbb{F}$ *de un cuerpo* $\mathbb{F}$ *se llama* ***subcuerpo*** *del cuerpo* $\mathbb{F}$ *si* $(U, +, \times)$, *con las misma operaciomes de* $\mathbb{F}$, *es a su vez un cuerpo.*

b: $(\mathbb{F}, +, \times)$ *se llama un cuerpo de* ***extensión*** *del subcuerpo* $(U, +, \times)$.

Teorema 1. *Sea* $p \in \mathbb{F}[x]$, *un polinomio con coeficientes en un cuerpo.*

A: *Se puede encontrar un cuerpo* $\mathbb{K}$ *que incluye a* $\mathbb{F}$ *como subcuerpo de modo que* p *tiene alguna raíz en* $\mathbb{K}$.

B: *Si el grado de* p *es* n, *se puede encontrar un cuerpo* $\mathbb{K}$ *que incluye a* $\mathbb{F}$ *como subcuerpo de modo que* p *tiene* n *raíces en* $\mathbb{K}$ *y por tanto se puede descomponer como producto de polinomios de grado* 1.

Demostración:

A:
- Si $p = ax + b$ un polinomio de grado 1, $\alpha = \frac{-b}{a}$ es una raíz y es suficiente con tomar $\mathbb{K} = \mathbb{F}$.
- Si p es un polinomio con alguna raíz α en $\mathbb{F}$, es decir

$$x - \alpha | p(x),$$

entonces es suficiente con tomar $\mathbb{K} = \mathbb{F}$.

- Si p no tiene raíces en $\mathbb{F}$ y es irreducible o existe $f \in \mathbb{F}[x]$ con $f|p$ y f irreducible (la primera posibilidad se reduce a tomar $f = p$), entonces

$$\mathbb{K} = \mathbb{F}[x]/f$$

es el cuerpo que buscamos. Claro,

1. como f es un polinomio irreducible en el anillo de polinomios $\mathbb{F}[x]$, el ideal generado por f es maximal y por tanto el anillo cociente para la relación $q_1 \sim_f q_2$ si y solo si $q_1 - q_2 \in < f >$, $\mathbb{F}[x]/f$, es un cuerpo.
2. La identificación de los elementos de $\mathbb{F}$, $r \in \mathbb{F}$, con su clase en el cuerpo cociente $[r] \in \mathbb{F}[x]/f$, hace que $\mathbb{F}$ sea un subcuerpo de $\mathbb{F}[x]/f$ (ya que $\sim_f$ es una congruencia).
3. Sea el polinomio $x \in \mathbb{F}[x]$ y sea su clase $\alpha = [x] \in \mathbb{F}[x]/f$, entonces $[x]$ es una raíz de f. Para ver esto último, supongamos que $f(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$, entonces

$$\overline{f}([x]) = b_m[x]^m + ... + b_1[x] + b_0$$

operando en congruencias

$$= [b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0] = [f] = [0] \in \mathbb{F}[x]/f.$$

Observemos que si f tiene una raíz en $\mathbb{K} = \mathbb{F}[x]/f$, como $f|p$, el polinomio p tiene la misma raíz que f.

B: Ahora procediendo como en **A**, a lo más tantas veces como el grado de p, llegaríamos a un cuerpo donde p tiene exactamente n raíces $\square$

El Teorema de Kronecker es la versión para polinomios del proceso en congruencias que vimos para los enteros.

Corolario 1. *Dado $f \in \mathbb{F}[x]$, $\mathbb{F}$ cuerpo y f irreducible, $(\mathbb{F}[x]/f, +, \times)$ es el conjunto de los posibles restos al dividir por f, salvo congruencias, con las operaciones en congruencias.*

Demostración: Sean $q_1, q_2 \in \mathbb{F}[x]$, con $q_1 \sim_f q_2$, es decir $q_1 - q_2 \in < f >$ o también que existe $k(x) \in \mathbb{F}[x]$ tal que $q_1 - q_2(x) = k(x)f(x)$. Si

$$q_1 = q(x)f(x) + r(x) \qquad \text{y} \qquad q_2 = q'(x)f(x) + r'(x)$$

con $grad.r$ y $grad.r'$ menores que el grado de f, entonces

$$(q_1 - q_2) = (q - q')f - (\, r - r' \,) = kf$$

y así $r - r' = (\,(q - q') - k\,)f$. Luego $f|q_1 - q_2$ si y solo si $f|r - r'$. Como el grado de $r - r'$ es menor que el grado de f, lo anterior solo es posible si $r - r' = 0$ □

Ejemplo 2. *Como $x^2 - 2$ es irreducible en $\mathbb{Z}_3[x]$, $[x] \in \mathbb{Z}_3[x]/(x^2 - 2)$ es una raíz del polinomio.*

Observemos que $[x]^2 - 2 = [0]$, luego $[x]^2 = 2$. Así el cuerpo $\mathbb{Z}_3[x]/(x^2 - 2) = \mathbb{Z}_3[\alpha]$, el cuerpo que construimos en el capítulo anterior. Además podemos ver que el conjunto cociente $\mathbb{Z}_3[x]/(x^2 - 2)$ está formado por los restos posibles de dividir un polinomio $p \in \mathbb{Z}_3[x]$ entre $x^2 - 2$ (por la definición de la congruencia). Por tanto

$$\mathbb{Z}_3[x]/(x^2 - 2) = \{\ 0, 1, 2, [x], [2x], [1 + x], [1 + 2x], [2 + x], [2 + 2x]\ \}.$$

El mismo conjunto que cuando cálculabamos $\mathbb{Z}_3[\alpha]$, para $\alpha^2 = 2$.

Ejemplo 3. *Dados $P(x) = x^4 + 2x^3 + 2x + 1, Q(x) = x^2 - 2 \in \mathbb{Z}_3[x]$, queremos calcular el inverso de P respecto del producto en $\mathbb{Z}_3[x]/(x^2 - 2)$.*

Podemos hacer dos cosas. La primera, dividir P entre Q. Identificar el resto y mirar en la tabla de $(\mathbb{Z}_3[x]/(x^2 - 2), \times)$ cuál es el inverso buscado (esta tabla la calculamos en el capítulo anterior).

Otra forma de verlo es hallar una identidad de Bezout entre P y Q (como $x^2 - 2$ es irreducible el $m.c.d.(P, Q)$ es un número). Así en primer lugar hay que dividir polinomios para calcular la sucesión de restos decrecientes en grado.

$$\begin{array}{l|l} x^4 + 2x^3 + 2x + 1 & x^2 - 2 \\ \underline{-x^4 \qquad + 2x^2} & x^2 + 2x + 2 \\ 2x^3 + 2x^2 + 2x + 1 & \\ \underline{x^3 \qquad\qquad + x} & \\ 2x^2 + 1 & \\ \underline{x^2 + 1} & \\ 2 & \end{array}$$

En este caso la identidad de Bezout es muy simple y no necesitamos usar el algoritmos de Euclides para calcularla,

$$P(x) - (x^2 + 2x + 2)(x^2 - 2) = 2.$$

Luego $[P(x)]^{-1} = [2]^{-1} = [2]$ $\square$

Observación 1. *(**Histórica.**) Leopoldo Kronecker (1823-1891) trabajo sobre formas cuadráticas y Teoría de Ideales. En algún momento escribió "...Dios hizo los números, todo lo demás es obra del hombre." Unos pocos años después, Peano estableció los axiomas, que llevan su nombre, con los cuáles se contruyen los números naturales y por tanto el resto de los números.*

Ahora vamos a completar el capítulo con algunos ejemplos que al trabajar en ellos nos ayuden a entender las nociones teóricas que hemos visto.

Ejemplo 4. *Vamos a encontrar todos los polinomios **mónicos** irreducibles de $\mathbb{Z}_3[x]$ de grado menor o igual a 3.*

- Los polinomios de grado uno son $x, x+1$ y $x+2$ y son todos irreducibles por definición.
- Los polinomios de grado dos mónicos son de la forma x^2+ax+b. Como los coeficientes solo pueden tomar tres valores $a, b \in \mathbb{Z}_3 = \{0,1,2\}$, solo existen nueve polinomios mónicos de grado 2 en $\mathbb{Z}_3[x]$. ¿Cuáles de ellos son irreducibles? Veámos.

  Si un polinomio p de grado 2 es reducible

  $$p(x) = x^2 + ax + b = (x-\alpha_1)(x-\alpha_2), entonces$$

  - si $\alpha_1 = \alpha_2 = \begin{cases} 0 & \Rightarrow \quad p(x) = x^2 \\ 1 & \Rightarrow \quad p(x) = x^2 + x + 1 \\ 2 & \Rightarrow \quad p(x) = x^2 + 2x + 1 \end{cases}$
  - si $\alpha_1 \neq \alpha_2, \begin{cases} \alpha_1 = 0, \alpha_2 = 1 & \Rightarrow \quad p(x) = x^2 + 2x \\ \alpha_1 = 0, \alpha_2 = 2 & \Rightarrow \quad p(x) = x^2 + x \\ \alpha_1 = 1, \alpha_2 = 2 & \Rightarrow \quad p(x) = x^2 + 2 \end{cases}$
  - De los nueve polinomios mónicos de grado 2 hay seis reducibles, luego los irreducibles son los que no están en la lista anterior, que son

    $$x^2+1, \;\; x^2+x+2 \text{ y } \; x^2+2x+2.$$

- Los polinomios de grado tres mónicos son de la forma x^3+ax^2+bx+c. Como los coeficientes solo pueden tomar tres valores $a, b, c \in \mathbb{Z}_3 = \{0,1,2\}$, solo existen 27 polinomios mónicos de grado 3 en $\mathbb{Z}_3[x]$. ¿Cuáles de ellos son irreducibles? Veámos.

Un polinomio p reducible de grado 3 es de la forma

$$p(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

o

$$p(x) = (x - \alpha)q(x)$$

con q un polinomoo de grado 2 irreducible. Como $\alpha_1, \alpha_2, \alpha_3 \in \{0, 1, 2\}$ y solo hay 3 polinomios de grado 2 irreducibles, las posibles combinaciones de estos elementos nos dice que hay $10 + 9 = 19$ polinomios reducibles de grado 3. Por tanto tenemos que buscar solo 8 polinomios irreducibles. Estos son de la forma

$$p(x) = x^3 + ax^2 + bx + c \qquad \text{con} \qquad c \neq 0.$$

Por tanto, cero no puede ser una raíz del polinomio. Ahora tenemos que encontrar los casos en los que ni $\alpha = 1$ ni $\alpha = 2$ sean raíces del polinomio.

- Si $c = 1$ y
  - $b = 0$, entonces $p(x) = x^3 + ax^2 + 1$ y solo $x^3 + 2x^2 + 1$ es irreducible.
  - $b = 1$, entonces $p(x) = x^3 + ax^2 + x + 1$ y solo $x^3 + 2x^2 + 2x + 1$ es irreducible.
  - $b = 2$, entonces $p(x) = x^3 + ax^2 + 2x + 1$ y solo $x^3 + 2x + 1$ y $x^3 + x^2 + 2x + 1$ son irreducibles.
- Si $c = 2$ y
  - $b = 0$, entonces $p(x) = x^3 + ax^2 + 2$ y solo $x^3 + x^2 + 2$ es irreducible.
  - $b = 1$, entonces $p(x) = x^3 + ax^2 + x + 2$ y solo $x^3 + x^2 + x + 2$ es irreducible.
  - $b = 2$, entonces $p(x) = x^3 + ax^2 + 2x + 2$ y solo $x^3 + 2x + 2$ $x^3 + 2x^2 + 2x + 2$ son irreducibles $\square$

Observación 2. *De un total de* $3 + 9 + 27 = 39$ *polinomios mónicos de grado menor o igual a* 3, *hemos hallado* $3 + 3 + 8 = 14$ *polinomios irreducibles. No son muchos y como hemos visto no es "rápida" la forma de determinar si son irreducibles o no.*

Pensemos en $\mathbb{Z}_p[x]$, *con* p *un primo grande y un grado elevado. Encontrar un polinomio irreducible o determinar si uno dado lo es parece*

que llevará un gran cálculo. Este es la "mala" cualidad de los polinomios irreducibles que les hace útiles en Criptografía.

Tenemos que entender que para descomponer un polinomio, o determinar si es irreducible, trabajar con raíces en cuerpos más grandes nos da nuevas posibilidades para hacerlo.

Ejemplo 5. *En $\mathbb{Z}[x]$ se define el subconjunto*

$$I = \{p \in \mathbb{Z}_3[x] \ : \ \overline{p}(0) \in 3\mathbb{Z} \ \}.$$

Es fácil ver que I es un ideal de $\mathbb{Z}[x]$. Además es el ideal generado por $I =< 3, x >$ (no es un ideal principal). La aplicación

$$\begin{array}{rccccl} \psi & : & \mathbb{Z}[x] & \to & \mathbb{Z}_3 & \\ & & p & \to & \psi(p) & = \ \overline{p}(3) = [\overline{p}(3)] \end{array}$$

es un homomorfismo suprayectivo de anillos. Claramente, el núcleo de la aplicación $ker\psi = I$ y según el Teorema de Isomorfía los anillos $\mathbb{Z}[x]/I$ y $\mathbb{Z}_3$ son isomorfos.

Observación 3. *El ejemplo anterior muestra que*

- *$\mathbb{Z}[x]$ no es dominio de ideales principales, ya que $\mathbb{Z}$ no es cuerpo.*
- *Aúnque $\mathbb{Z}$ no es un cuerpo, $\mathbb{Z}[x]/I$ si es un cuerpo (es isomorfo a $\mathbb{Z}_3$ que lo es). Aunque en este caso $\mathbb{Z} \nsubseteq \mathbb{Z}[x]/I$ ($\mathbb{Z}[x]/I$ es un cuerpo finito).*

Para entender mejor las extensiones de cuerpos, tendremos que estudiar un poco la Teoría de Cuerpos en abstracto. Esto lo vemos en los siguientes capítulos.

Referencias

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

Email address: Cesar_Ruiz@mat.ucm.es