AM

IRREDUCIBILIDAD DE POLINOMIOS SOBRE LOS CUERPOS CLÁSICOS.

Los conjuntos clásicos de números:

$$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

permiten definir polinomios sobre ellos. Vamos a "repasar" la irreducibilidad de polinomios con coeficientes en estos conjuntos.

<u>OBSERVACIÓN</u>: En $\mathbb{Z}[x]$ no siempre se puede dividir polinomios.

<u>Ejemplo</u>: ¿ $3x^2+1 \;\underline{|\,5x+3}$?

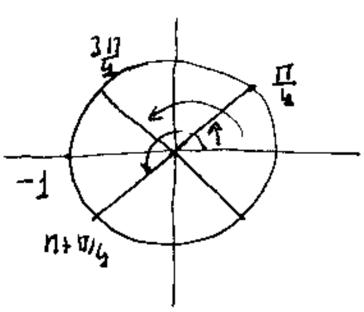
Esto es debido a que $\mathbb{Z}$ no es un cuerpo (en nuestro ejemplo <u>no</u> existe $\frac{3}{5} \in \mathbb{Z}$).

Como $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son cuerpos, sobre ellos sí se puede dividir polinomios y tiene sentido pleno hablar de irreducibilidad.

<u>Ejemplo</u> $x^4+2 \in \mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$.

$$x^4+2 \begin{cases} \text{no tiene raíces en } \mathbb{Q} \\ \text{no tiene raíces en } \mathbb{R} \\ \text{tiene 4 raíces en } \mathbb{C} \end{cases}$$

<u>Dem</u> No existe $r \in \mathbb{R}$ con $r^4 = -2$.



En $\mathbb{C}$

$\sqrt[4]{2}\left(\frac{1}{\sqrt2} + \frac{1}{\sqrt2} i\right)$

$\sqrt[4]{2}\left(-\frac{1}{\sqrt2} + \frac{1}{\sqrt2} i\right)$

$\sqrt[4]{2}\left(-\frac{1}{\sqrt2} - \frac{1}{\sqrt2} i\right)$

y $\sqrt[4]{2}\left(\frac{1}{\sqrt2} - \frac{1}{\sqrt2} i\right)$

| <u>Observar</u> la 1ª y la 4ª y la 2ª y la 3ª son conjugadas.

Son las cuatro raíces del polinomio en $\mathbb{C}$

<u>Ejemplo</u> $x^4+2 = \left(x - \sqrt[4]{2}\left(\frac{1}{\sqrt2}+\frac{1}{\sqrt2} i\right)\right)\left(x - \sqrt[4]{2}\left(\frac{1}{\sqrt2}-\frac{1}{\sqrt2} i\right)\right)\left(x-\sqrt[4]{2}\left(-\frac{1}{\sqrt2}-\frac{1}{\sqrt2} i\right)\right)\left(x-\sqrt[4]{2}\left(-\frac{1}{\sqrt2}+\frac{1}{\sqrt2} i\right)\right)$

$$= \left(x^2 - 2\sqrt[4]{2}\,\frac{1}{\sqrt2}\,x + \sqrt2\right)\left(x^2 + 2\sqrt[4]{2}\,\frac{1}{\sqrt2} + \sqrt2\right)$$

<u>OBSERVACIÓN</u>: x^4+2 es
- irreducible en $\mathbb{Q}[x]$
- se reduce como producto de 2 polinomios de grado 2 irreducibles en $\mathbb{R}[x]$.

tener en cuenta el teorema

OBSERVACIÓN: $\boxed{\text{UN POLINOMIO SERÁ O NO IRREDUCIBLE DEPENDIENDO DEL CUERPO (DE LOS COEFICIENTES) DONDE ESTEMOS TRABAJANDO.}}$

HAY CUERPOS DONDE LOS ÚNICOS POLINOMIOS IRREDUCIBLES SON LOS DE PRIMER GRADO: COMO $\mathbb{C}$ (*)

DADO UN POLINOMIO, VEREMOS QUE SIEMPRE EXISTE UN CUERPO (QUE CONTIENE AL CUERPO DE COEFICIENTES) DONDE EL POLINOMIO TIENE TODAS SUS RAÍCES Y SE DESCOMPONE EN PRODUCTO DE POLINOMIOS DE PRIMER GRADO: COMO $\forall f \in \mathbb{R}[x]$ SE DESCOMPONE COMPLETAMENTE EN $\mathbb{C}[x]$. (**)

VAMOS A JUSTIFICAR AQUÍ (*) Y (**). DESPUÉS, EN EL SIGUIENTE TEMA, VEREMOS QUE (**) OCURRE EN GENERAL, NO IMPORTA EL CUERPO $\mathbb{F}$ DEL QUE PARTAMOS.

TEOREMA FUNDAMENTAL DEL ALGEBRA

. LA IRREDUCIBILIDAD DE UN POLINOMIO ESTÁ RELACIONADA CON LA CARENCIA DE RAÍCES DE UN POLINOMIO

EN GENERAL UN POLINOMIO DE GRADO n SOBRE UN CUERPO $\mathbb{F}$ PUEDE TENER CUALQUIER NÚMERO DE RAÍCES, ENTRE CERO Y n; RAÍCES EN $\mathbb{F}$ SE ENTIENDE. LOS NÚMEROS COMPLEJOS SON UNA IMPORTANTE EXCEPCIÓN.

<u>TEOREMA FUNDAMENTAL DEL ALGEBRA</u> UN POLINOMIO DE GRADO POSITIVO Y COEFICIENTES EN EL CUERPO $\mathbb{C}$, TIENE AL MENOS UNA RAÍZ EN $\mathbb{C}$

<u>OBSERVACIÓN</u> A) (HISTORIA) ESTE TEOREMA FUE ENUNCIADO POR PRIMERA VEZ EN 1746 POR D'ALEMBERT (1717-83) CON UNA PRUEBA INCORRECTA. LA PRIMERA DEMOSTRACIÓN COMPLETA APARECE EN 1799 EN LA TESIS DOCTORAL DE KARL FRIEDRICH GAUSS (1777-1855)

B) (TÉCNICA) TODAS LAS DEMOSTRACIONES DEL TEOREMA FUNDAMENTAL DEL ALGEBRA HACEN USOS DE TÉCNICAS "SOFISTICADAS" DE ANÁLISIS MATEMÁTICO.

CLARO UNA VEZ QUE TENEMOS UNA RAÍZ, EL MISMO TEOREMA NOS PERMITE AFIRMAR QUE TENEMOS TODAS

<u>COROLARIO</u>: SI $p \in \mathbb{C}[x]$ Y $\operatorname{grad} p = n$, ENTONCES p TIENE n RAÍCES COMPLEJAS Y SE TIENE QUE $p(x) = c\,(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$ DONDE $\alpha_1\, \alpha_2 \ldots \alpha_n$ SON LAS n-RAÍCES (NO NECESARIAMENTE DISTINTAS) Y $c \in \mathbb{C}$.

<u>DEM</u> DADO $p \in \mathbb{C}[x]$ POR EL T.F.A. $\exists\, \alpha_1 \in \mathbb{C}$ CON $\bar{p}(\alpha_1) = 0$, ASÍ $p(x) = (x-\alpha_1)\,Q(x)$, CON $\operatorname{Grad} Q = n-1$ APLICANDO UN PROCESO DE INDUCCIÓN SOBRE EL GRADO DE LOS POLINOMIOS, SE PRUEBA EL RESULTADO

COROLARIO:

A) Los polinomios irreducibles de $\mathbb{C}[x]$ son los de primer grado

B) Los polinomios irreducibles de $\mathbb{R}[x]$ tienen a lo más grado 2

C) Todo polinomio de $\mathbb{R}[x]$ se descompone en producto de polinomios de grados 1 ó 2.

DEM B y C) Sea $p \in \mathbb{R}[x] \subseteq \mathbb{C}[x]$

Así $p(x) = a_0 + a_1 x + \dots + a_n x^n$ $\quad a_0, a_1, \dots, a_n \in \mathbb{R}$

y existe $\alpha \in \mathbb{C}$ con $p(\alpha) = 0$.

Luego $0 = \overline{a_0 + a_1\alpha + \dots + a_n\alpha^n} = a_0 + a_1\bar{\alpha} + \dots + a_n\bar{\alpha}^n$

Así $\bar{\alpha}$ es otra raíz compleja de p

$p(x) = (x-\alpha)\,Q(x)$ y como $p(\bar{\alpha}) = 0 \Rightarrow Q(\bar{\alpha}) = 0$

Así $p(x) = (x-\alpha)(x-\bar{\alpha})\,R(x) =$

$$= \left(x^2 - (2\operatorname{Re}\alpha)\,x + |\alpha|^2\right) R(x).$$

donde $x^2 - (2\operatorname{Re}\alpha)x + |\alpha|^2 \in \mathbb{R}[x]$, así $R(x) \in \mathbb{R}[x]$.

Luego hemos probado que todo $p \in \mathbb{R}[x]$ con $\operatorname{grad} p > 2$ es descomponible en $\mathbb{R}[x]$ y lo es en producto de factores de grado a lo más 2.

DEF Un cuerpo $\mathbb{K}$ se llama algebraicamente cerrado si tiene la propiedad de que todo polinomio $p \in \mathbb{K}[x]$ se puede descomponer en $\mathbb{K}[x]$ como producto de polinomios de grado 1.

Ejemplo: $\mathbb{C}$ es algebraicamente cerrado

$\mathbb{R}$ **no** es " "

Observación: Se puede probar que todo cuerpo $\mathbb{K}$ está incluido en otro mayor que es algebraicamente cerrado

Ejemplo $\mathbb{R} \subseteq \mathbb{C}$.

IRREDUCIBILIDAD EN $\mathbb{Q}[x]$

En $\mathbb{R}[x]$ y $\mathbb{C}[x]$ es "fácil" encontrar los polinomios irreducibles ¿y en $\mathbb{Q}[x]$?

Ejemplo: Sabemos que $x^4+1 \in \mathbb{Q}[x]$ es irreducible.

Vamos a ver algunas condiciones suficientes para garantizar que un polinomio en $\mathbb{Q}[x]$ es irreducible.

Criterio de irreducibilidad de Eisenstein

Sea $f \in \mathbb{Q}[x]$ con coeficientes enteros.

$$f(x) = c_0 + c_1 x + \cdots + c_n x^n$$

Si existe un número primo p tal que p divide a todos los coeficientes de f excepto c_n y p^2 no divide a c_0, entonces f es irreducible en $\mathbb{Q}[x]$.

(Historia: Ferdinand G. M. Eisenstein (1823-52) fue alumno de Gauss. Publicó este resultado en 1850 en el "Crelle" Vol 39 pp 160-179.)

Observación: Si $f(x) = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + \cdots + \frac{a_n}{b_n}x^n$

y $b = m.c.m(b_0, b_1, \ldots, b_n) \Rightarrow bf \in \mathbb{Z}[x]$.

Y claramente f es irreducible $\Leftrightarrow$ bf es irreducible.

Dem: Si f no es irreducible, por el teorema de factorización única $f = g \cdot h$, grad $g \geq 1$, grad $h \geq 1$ y $g, h \in \mathbb{Z}[x]$

con $g(x) = a_0 + a_1 x + \cdots + a_r x^r$
$h(x) = b_0 + b_1 x + \cdots + b_s x^s$ $\quad r+s=n$

y $c_0 = a_0 b_0$, $c_1 = a_1 b_0 + a_0 b_1$, ..., $c_n = a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0$.

Por hipótesis $p | c_0 \Rightarrow p | a_0$ ó $p | b_0$, pero no a ambos a la vez, ya que $p^2 \nmid c_0$. Supongamos $p | a_0$ y $p \nmid b_0$. Se sigue que como $p | c_1 \Rightarrow p | a_1$ y siguiendo este proceso $p | a_j$ $j = 0, 1, \ldots, r$

$p \nmid b_0$

luego p divide a todos los coeficientes de g y como $f = g \cdot h$ (y $c_t = \sum_{j=0}^{t} a_j b_{t-j}$) se llega a que p divide a todos los coeficientes de f, lo cual no es posible, ya que por hipótesis $p \nmid c_n$.

AM

NECESITAMOS ALGUNA NUEVA DEFINICIÓN PARA DAR MÁS CRITERIOS DE IRREDUCIBILIDAD.

DEFINICIÓN SEA $f \in \mathbb{Q}[x]$, $f(x) = c_0 + c_1 x + \dots + c_n x^n$. DIREMOS QUE f ES UN POLINOMIO PRIMITIVO SI

1) $f \neq 0$
2) $c_0, c_1, \dots, c_n \in \mathbb{Z}$ (e.d. $f \in \mathbb{Z}[x]$)
3) $m.c.d(c_0, c_1, \dots, c_n) = 1$.

PROP EL PRODUCTO DE POLINOMIOS PRIMITIVOS ES DE NUEVO UN POLINOMIO PRIMITIVO.

DEM SEAN $g, h \in \mathbb{Q}[x]$ PRIMITIVOS

con $g(x) = \sum_{j=0}^{r} a_j x^j$ y $h(x) = \sum_{j=0}^{s} b_j x^j$

(OBVIAMENTE $g \cdot h \neq 0$ y $g \cdot h \in \mathbb{Z}[x]$).

SUPONGAMOS QUE $p \in \mathbb{Z}$, PRIMO DIVIDE A LOS COEFICIENTES DE $g \cdot h$. POR SER g PRIMITIVO, p NO DIVIDE A TODOS LOS COEFICIENTES DE g. SEA a_l EL PRIMER COEFICIENTE DE g $(0, 1, 2, \dots, l)$ DE MODO QUE $p \nmid a_l$. IGUALMENTE SEA b_k EL PRIMER COEFICIENTE DE h CON $p \nmid b_k$.
EL COEFICIENTE DE x^{l+k} DEL POLINOMIO gh.
ESTÁ DADO POR

(*) $a_0 b_{l+k} + \dots + a_{l-1} b_{k+1} + a_l b_k + a_{l+1} b_{k-1} + \dots + a_{l+k} b_0$

DIVISIBLES POR p. DIVISIBLES POR p

COMO HEMOS SUPUESTO QUE p DIVIDE A TODOS LOS COEFICIENTES DE $g \cdot h$, $p \mid (*) \Rightarrow p \mid a_l b_k$

$\Rightarrow p \mid a_l$ o $p \mid b_k$ UNA CONTRADICCIÓN
p PRIMO
EN CUALQUIER CASO.

PROP TODO POLINOMIO $f \in \mathbb{Q}[x] - \{0\}$, SE PUEDE ESCRIBIR DE FORMA ÚNICA COMO $f = c\bar{f}$ con $c \in \mathbb{Q}$ y $\bar{f} \in \mathbb{Z}[x]$ POLINOMIO PRIMITIVO

AM

DEMOSTRACIÓN: Es evidente que f se puede escribir como $f = a\hat{f}$ con $a \in \mathbb{Q}$ y $\hat{f} \in \mathbb{Z}[x]$

(si $f = \sum_{j=0}^{n} \frac{a_j}{b_j} x^j$ sea $\frac{1}{a} = mcm(b_j : j = 0 \dots n)$).

Así supondremos $f \in \mathbb{Z}[x] \setminus \{0\}$.

Sea $f(x) = \sum_{j=0}^{n} c_j f$; sea $c = mcd(c_j \; j = 0 \dots n)$.

Entonces $f(x) = c \sum_{j=0}^{n} \frac{c_j}{c} f$; como $c \mid c_j \; \forall j = 0 \dots n$

se sigue que $\frac{c_j}{c} \in \mathbb{Z}$.

Veamos que $\sum_{j=0}^{n} \frac{c_j}{c} f$ es primitivo; lo cual es evidente por la elección de c.

$\boxed{\text{Veamos la unicidad}}$ si $f = c\bar{f} = d\bar{g}$ $\bar{f}$ y $\bar{g}$ primitivos.

Sea $c = p/q$ y $d = r/s$ con $p, q, r, s \in \mathbb{N}$.

Entonces $sp\bar{f} = qr\bar{g}$ es un polinomio de coeficientes enteros que tienen como máximo común divisor a $sp = qr$. De ello se deduce que $c = p/q = r/s = d$ y en consecuencia $\bar{f} = \bar{g}$

COROLARIO (Lema de Gauss) Un polinomio no nulo $f \in \mathbb{Z}[x]$ es reducible en $\mathbb{Q}[x]$ si y solo si factoriza como un producto de dos polinomios con coeficientes enteros de grados positivos.

Observ. Histórica: Art. 42 de "Disquisitiones Arithmeticae" (1801) Gauss)

DEM $\Leftarrow$) Es evidente, si $f \in \mathbb{Z}[x]$ y $f = g \cdot h$ con $g, h \in \mathbb{Z}[x]$ con $\text{grad}\, g \geq 1$ y $\text{grad}\, h \geq 1$, f es reducible en $\mathbb{Z}[x]$ y por tanto en $\mathbb{Q}[x]$.

$\Rightarrow$) Por la proposición anterior, $f = c\bar{f}$, $c \in \mathbb{Z}$ y $\bar{f}$ primitivo (c = m.c.d de los coeficientes de f).

Así podemos suponer que f es primitivo. Si $f = g \cdot h$ con $g, h \in \mathbb{Q}[x]$, por la proposición anterior, $f = c_1 \bar{g} c_2 \bar{h}$ con $c_1, c_2 \in \mathbb{Q}$ y $\bar{g}, \bar{h}$ primitivos. Como $\bar{g} \cdot \bar{h}$ es primitivo $c_1 \cdot c_2 = 1$ ya que hemos supuesto f primitivo.

A.11 EJERCICIO: El $\mathrm{Card}\{f \in \mathbb{Q}[x] : \mathrm{grad}\, f = n,\ f \text{ irreducible}\} =$ 40

$= \mathrm{Card}\, \mathbb{N}$.

DEM $f = c\bar{f}$, $c \in \mathbb{Q}$, $c > 0$ y $\bar{f} \in \mathbb{Z}[x]$ primitivo

f es irreducible $\iff$ $\bar{f}$ es irreducible en $\mathbb{Q}[x]$

Como $\mathrm{Card}\{f \in \mathbb{Q}[x] : \mathrm{grad}\, f = n\} = \mathrm{Card}\, \mathbb{Q}^{n+1} = \mathrm{Card}\, \mathbb{N}$.

Por otro lado $\forall\, p$ primo

$$f_p = p + px + \cdots + px^{n-1} + (p-1)x^n \in \mathbb{Z}[x]$$

es primitivo, $p \mid c_i$ $i = 0 \ldots n-1$ $\quad p \nmid p-1$

y $p^2 \nmid p$

Luego el criterio de Eisenstein para f_p nos dice que es irreducible. Luego el cardinal buscado es al menos igual que el de los primos $\therefore$

$\mathrm{Card}\, \mathbb{N}$.

Ejemplo $4x^3 - 3x - 1/2 \in \mathbb{Q}[x]$ es irreducible

ya que $4x^3 - 3x - 1/2 = 1/2\,(8x^3 - 6x - 1)$

$4x^3 - 3x - 1/2$ es irreducible $\iff$ lo es $8x^3 - 6x - 1$

(este es primo; si fuese reducible por

el lema de Gauss $8x^3 - 6x - 1 = g \cdot h$ con $\mathrm{grad}\, g \geq 1$ y $\mathrm{grad}\, h \geq 1$

así $8x^3 - 6x - 1 = (a_2x^2 + a_1x + a_0)(b_1x + b_0)$

con $a_i, b_i \in \mathbb{Z}$.

Se hace cuentas $\left\{ \begin{array}{l} a_0 b_0 = 1 \\ \vdots \\ \text{etc.} \end{array} \right.$

y se ve que las ecuaciones propuestas no tienen solución.

<u>CRITERIO DE IRREDUCIBILIDAD DE EUGEN NETTO</u>

Si $f \in \mathbb{Z}[x]$, $\mathrm{grad}\, f = 2m+1$, $m \in \mathbb{N}$

$f(x) = c_0 + c_1 x + \cdots + c_{2m+1} x^{2m+1}$, entonces

f es irreducible si existe p primo tal que

1) $p \nmid c_{2m+1}$ 2) $p \mid c_{m+1}$, $p \mid c_{m+2}$ $\cdots$ $p \mid c_{2m}$.

3) $p^2 \mid c_0$, $p^2 \mid c_1$, $\ldots$, $p^2 \mid c_m$ 4) $p^3 \nmid c_0$.

(Historia: Math Annalen 48 (1897).). SIN PRUEBA.