Conjuntos y números 17/12

(10) a) Dem. que $\forall n \geq 1$ existen infinitos pol. irred. de grado n en $\mathbb{Q}[x]$.

$P(x) = x^n + px^{n-1} + \dots + px + p$.

$P(x)$ es primitivo (en part. es mónico). Por el Lema de Gauss, $P(x)$ es irred. en $\mathbb{Q}[x]$ $\Leftrightarrow$ $P(x)$ es irred. en $\mathbb{Z}[x]$.

Por el criterio de Eisenstein: $p \mid \underbrace{a_0, a_1, \dots, a_{n-1}}_{= p}$; $p \nmid a_n = 1$ y $p^2 \nmid a_0 = p$.

Por lo tanto $P(x)$ es irred. en $\mathbb{Q}[x]$. Como sabemos que existen infinitos primos, concluimos.

b) $P(X) = X^5 - X^4 + 2X^3 - 2$, descomponer en $\mathbb{Q}[x]$.

Por el criterio de raíz racional, si x es solución $x \in \pm\{1, 2\}$

$P(1) = 1 - 1 + 2 - 2 = 0$.

$x^5 - x^4 + 2x^3 - 2 = (x-1)(x^4 + ax^3 + bx^2 + cx + 2)$

Con x^4: $-1 = -1 + a \Rightarrow a = 0$

Con x^3: $2 = b + a \Rightarrow b = 2$

Con x^2: $0 = -b + c \Rightarrow c = 2$

Nos queda $x^4 + 2x^2 + 2x + 2$. Aplicamos el razonamiento de arriba. (Eisenstein + Gauss) ■

$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \overset{?}{=} 0$, $x = p/q$ raíz $(p, q) = 1$

$a_n \left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \dots + a_1 (p/q) + a_0 \overset{\cdot q^n}{\Rightarrow} a_n p^n + a_{n-1} p^{n-1} q + \dots + a_1 p q^{n-1} + a_0 q^n = 0$

$p \mid$ (de $a_n p^n + \dots + a_1 p q^{n-1}$) $\quad q \mid$ (de $a_{n-1} p^{n-1} q + \dots + a_0 q^n$)

Luego $q \mid a_n$ $\quad p \mid a_0$

(11) a) $P(x) \in K[x]$ es irred. $\Leftrightarrow$ $P(x+a)$ es irred. para cualq. $a \in K$

Demostramos $P(x) \in K[x]$ es red. $\Leftrightarrow$ $P(X+a)$ es red. $a \in K$.

$\Rightarrow$) $P(X) = Q(X) R(X) \Rightarrow P(X+a) = Q(X+a) R(X+a)$.

grado ≥ 1

$\Leftarrow$) Sea $P(X+a) = Q(X) R(X) \Rightarrow P(X) = P((X+a) - a) = Q(X-a) \cdot R(X-a)$. ■

b) $P(x) = x^{p-1} + x^{p-2} + \dots + 1 = \dfrac{x^p - 1}{x-1}$ es irred. $\in Q[x]$

$$P(x+1) = \frac{(x+1)^p - 1}{(x+1)-1} = \frac{\left(x^p + \binom{p}{1}x^{p-1} + \dots + \binom{p}{p-1}x + 1\right) - 1}{x}$$

$$= x^{p-1} + \binom{p}{1}x^{p-2} + \dots + \binom{p}{p-1}$$

Por H.5. 16, $p \mid \binom{p}{k}$ para p primo y $1 \leq k < p-1$. Aplicamos:

- $P(x+1)$ es primitivo.
- $p \mid a_0, \dots, a_{n-2}$ $\Rightarrow$ $P(x+1)$ es irred.
- $p \nmid a_{n-1} = 1$ y $p^2 \nmid \binom{p}{p-1} = p$.

■

12) a) Determinar pol. mónicos irred. en $\mathbb{Z}/_2[x]$ de grados 1, 2, 3, 4.

- Grado 1 $\rightarrow$ todos son irred. x, $x+1$.
- Grado 2 $\rightarrow$ el pol. será irred. si no tiene raíces.

$$\begin{cases} x^2+x+1 \rightarrow ✓ \\ x^2+x \rightarrow \text{No} \\ x^2+1 \rightarrow 1 \text{ es raíz, no.} \\ x^2 \rightarrow \text{No, raíz } 0. \end{cases}$$

- Grado 3 $\rightarrow$ lo mismo. Tiene que tener término indep. (para que 0 no sea raíz) y un número impar de términos. $(P(1) \neq 0)$

$$\begin{cases} x^3+x^2+x+1 \rightarrow \text{nº par.} \\ x^3+x^2+1 \rightarrow ✓ \\ x^3+x+1 \rightarrow ✓ \\ x^3+1 \rightarrow \text{nº par términos.} \end{cases}$$

- Grado 4 $\rightarrow$ mirar dos cosas: no tiene raíces y no es producto de dos pol. de grado 2 irred.

No raíces

$$\begin{cases} x^4+x+1 \rightarrow ✓ \\ x^4+x^2+1 \rightarrow (*) \\ x^4+x^3+1 \rightarrow ✓ \\ x^4+x^3+x^2+x+1 \rightarrow ✓ \end{cases}$$

Sólo hay un pol. irred. de grado 2: x^2+x+1.

$$(x^2+x+1)^2 = x^4+x^2+1$$

b) $P(x) = x^4+3x^3+5x^2+7x+1 \xrightarrow{\text{mod } 2} \tilde{P}(x) = x^4+x^3+x^2+x+1.$

$(\text{grado } \tilde{P}(x) = P(x)) \wedge (\tilde{P}(x) \text{ irred}) \Rightarrow P(x)$ es irred. ∎

(+ aplicar Lema Gauss)

(13) $p(x) = x^4+3x^2+4$ en $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}/_5[x]$.

- Empezar en $\mathbb{C}[x]$: $x^2=t$, $t = \dfrac{-3\pm\sqrt{9-4\cdot 4}}{2} = \dfrac{-3\pm\sqrt{7}\,i}{2}$

$$x = \begin{cases} \sqrt{\dfrac{-3+\sqrt{7}\,i}{2}} = \pm\sqrt{2}\left(\dfrac{-\sqrt{2}}{4} + \dfrac{\sqrt{7}}{2\sqrt{2}}\,i\right) \\ \sqrt{\dfrac{-3-\sqrt{7}\,i}{2}} = \pm\sqrt{2}\left(\dfrac{\sqrt{2}}{4} + \dfrac{\sqrt{7}}{2\sqrt{2}}\,i\right) \end{cases}$$

$$-3/_2 + \frac{\sqrt{7}\,i}{2} = 2\Big(\underbrace{-\frac{3}{4}}_{\cos\theta} + \underbrace{\frac{\sqrt{7}}{4}}_{\operatorname{sen}\theta}\,i\Big)$$

$$\cos\theta/_2 = \pm\sqrt{\frac{1+(-3/4)}{2}} = \frac{\pm 1}{\sqrt{8}} = \pm\frac{\sqrt{2}}{4}$$

$$\operatorname{sen}\theta/_2 = \pm\sqrt{\frac{1+3/4}{2}} = \pm\frac{\sqrt{7}}{\sqrt{8}} = \pm\frac{\sqrt{7}}{2\sqrt{2}}$$

Raíces en $\mathbb{C}$:

$-\frac{1}{2} + \frac{\sqrt{7}}{2}\,i = z$

$-\frac{1}{2} - \frac{\sqrt{7}}{2}\,i = \bar{z}$

(x^2-x+2)

$\frac{1}{2} - \frac{\sqrt{7}}{2}\,i = -z$

$\frac{1}{2} + \frac{\sqrt{7}}{2}\,i = -\bar{z}$

(x^2+x+2)

$P(x) = (x-z)(x-\bar{z})(x+z)(x+\bar{z})$ en $\mathbb{C}[x]$.

Para $\mathbb{R}[x]$, $(x-z)(x-\bar{z}) = x^2 - 2\operatorname{Re} z\, x + |z|^2$

En $\mathbb{R}[x]$: $P(x) = (x^2-x+2)(x^2+x+2)$.

Si es irred. en $\mathbb{R}[x]$, también lo es en $\mathbb{Q}[x]$ (misma descomp.)

En $\mathbb{Z}/_5$: $P(x) = x^4+3x^2+4 \equiv \begin{cases} 1+3x^2+4 \equiv 3x^2 & \text{si } x\neq 0 \\ 4 & \text{si } x=0 \end{cases}$

Luego no tiene raíces. ¿Factores de grado 2?

$x^4+3x^2+4 = (x^2+ax+b)(x^2+a'x+b')$ $\qquad bb' \equiv 4$

$\Rightarrow (b,b') \in \{(2,2);(4,1);(1,4)\}$

Con $x^3 \rightsquigarrow a'+a \equiv 0 \Rightarrow a' \equiv -a$

Con $x^2 \rightsquigarrow b'+b+a.a' \equiv 3$

Con $x \rightsquigarrow ab'+a'b \equiv 0 \rightsquigarrow -a'(b'-b) \equiv 0 \Rightarrow -a' \equiv 0$ ó $b' \equiv b$

$\downarrow$

No es posible

Con lo cual $b' \equiv b$, es decir $(b,b') = (2,2)$

Entonces $4+(-a')^2 \equiv 3 \Rightarrow a'^2 \equiv 1 \Rightarrow \begin{cases} a' \equiv 1 \Rightarrow a \equiv 4 \\ a' \equiv 4 \Rightarrow a \equiv 1 \end{cases}$

$x^4+3x^2+4 = (x^2+x+2)(x^2+4x+2)$ $\blacksquare$