GyA - Tarea 1

Jose Antonio Lorencio Abril

29-03-2020

3.4.7. Decidir cuáles de los siguientes polinomios son irreducibles en los anillos que se indican

(1) $2x^2 + 2x + 2$ en $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}_5[x]$.

Será irreducible si, y solo si, lo es $x^2 + x + 1$. Ahora bien, usando la fórmula de resolución de la ecuación de segundo grado obtenemos el par de soluciones

$$x = -\frac{1}{2} \pm i\sqrt{3} \notin \mathbb{Z}, \mathbb{Q}$$

Por lo que este polinomio no tiene raíces, pero, como es de grado 2, por el Lema 3.22.(3) es irreducible en $\mathbb{Q}[x]$, y como este polinomio (el simplificado) es primitivo, por la Proposición 3.20, tenemos que también es irreducible en $\mathbb{Z}[x]$.

Para verlo en $\mathbb{Z}_5[x]$, voy a ver que tampoco tiene ninguna raíz, por lo que también será irreducible, como consecuencia de ese mismo lema.

$$P(0) = 2,\ P(1) = 6 = 1,\ P(2) = 14 = 4,\ P(3) = 26 = 1,\ P(4) = P(1) = 2$$

(2) $x^4 + 2$ en $\mathbb{Z}_7[x]$, $\mathbb{Q}[x]$

Lo voy a ver primero para $\mathbb{Z}_7[x]$. Comprobemos primero si tiene alguna raíz:

$$P(0) = 2,\ P(1) = 3,\ P(2) = 18 = 4,\ P(3) = 83 = 6,\ P(4) = 6$$

$$P(5) = P(-2) = 4,\ P(6) = P(-1) = 2$$

No tiene raíces. Por tanto, para no ser irreducible debe ser producto de dos polinomios de grado 2.

$$(x^2 + a_1x + a_0)(x^2 + b_1x + b_0) = x^4 + (b_1 + a_1)x^3 + (b_0 + a_1b_1 + a_0)x^2 + (a_1b_0 + a_0b_1)x + a_0b_0$$

De donde obtenemos

$$\begin{cases} b_1 + a_1 = 0 & \\ b_0 + a_1b_1 + a_0 = 0 & \\ a_1b_0 + a_0b_1 = 0 & \\ a_0b_0 = 2 & (4) \end{cases} \iff \begin{cases} b_1 = -a_1 & (1) \\ b_0 - a_1^2 + a_0 = 0 & (2) \\ 0 = a_1b_0 - a_0a_1 = a_1(b_0 - a_0) & (3) \\ a_0 \neq 0 \neq b_0 & \end{cases}$$

Supongamos en este punto, por (3) que $b_0 - a_0 = 0 \iff b_0 = a_0$

Sustituyendo en (2) y en (4) queda

$$\begin{cases} 2a_0 - a_1^2 = 0 \\ a_0^2 = 2 \end{cases}$$

Los cuadrados en $\mathbb{Z}_7$ son $1^2 = 1 = 6^2,\ 2^2 = 4 = 5^2,\ 3^2 = 2 = 4^2$. Por tanto a_0 debe ser 3 ó 4.

Supongamos que es 4, entonces

$$8 - a_1^2 = 0 \iff 8 = a_1^2 \iff 1 = a_1^2$$

Por lo que $a_1 = 1$ es válido.

Así, los valores $a_0 = 4,\ a_1 = 1,\ b_0 = 4,\ b_1 = -1 = 6$ nos dan dos polinomios de grado cuya multiplicación nos da P, que por tanto no es irreducible.

$$x^4 + 2 = (x^2 + x + 4)(x^2 + 6x + 4)$$

Pasamos ahora a verlo en $\mathbb{Q}[x]$.

Primero notemos que es primitivo. Además, 2 es irreducible en $\mathbb{Z}$ y tenemos que 2 divide a todos los coeficientes de P que no son el n-ésimo, pero su cuadrado no divide al término independiente:

$$2|a_i,\ \forall i < n \qquad 2 \nmid a_0$$

Por tanto, el criterio de Eisenstein nos asegura que P es irreducible en $\mathbb{Z}[x]$ y la proposición 3.20 nos lo asegura en $\mathbb{Q}[x]$.

(3) $x^3 - 18x^2 + 106x - 203$ en $\mathbb{Z}[x]$ y $\mathbb{Q}[x]$

Al ser primitivo, por la proposición 3.20, basta verlo para uno de los dos, pues es equivalente.

Los divisores de 203 son

$$\pm 1 \pm 7 \pm 29 \pm 203$$

Y estas son las posibles raíces. De hecho, $P(7) = 0$. Por lo que P es divisible por $x - 7$, y no es irreducible, ni en $\mathbb{Z}[x]$ ni en $\mathbb{Q}[x]$.

(4) $x^5 + x + 2$ en $\mathbb{R}[x],\ \mathbb{Q}[x],\ \mathbb{Z}_3[x]$

Este es muy sencillo, pues tenemos que $P(-1) = 0$, lo que nos proporciona una raíz tanto en $\mathbb{Q}$ como en $\mathbb{R}$, donde no es irreducible.

En $\mathbb{Z}_3[x]$ nos sirve esa misma raíz, así que tampoco es irreducible aquí.

(5) $x^5 + x - 2$ en $\mathbb{R}[x],\ \mathbb{Q}[x],\ \mathbb{Z}_3[x]$

También muy sencillo, 1 es raíz en los 3 anillos. Por lo que no es irreducible en ninguno de ellos.

(6) $2x^5 - 6x^3 + 9x^2 - 15$ en $\mathbb{Z}[x]$, $\mathbb{Q}[x]$

El polinomio es primitivo, por lo que bastará verlo para uno de los anillos.

Además, tenemos que

$$3 \mid a_i, \ \forall i < n \qquad 9 = 3^2 \nmid 15 = a_0$$

Por el criterio de Eisenstein, tenemos que P es irreducible en $\mathbb{Z}[x]$, y así, también lo es en $\mathbb{Q}[x]$.

(7) $x^4 + 15x^3 + 7$ en $\mathbb{Z}[x]$

Es primitivo. Y 2 es un primo que no divide a a_4. Si fuera irreducible en $\mathbb{Z}_2[x]$, entonces, por el Corolario 3.26, también será irreducible en $\mathbb{Z}[x]$. Veamos si es así.

$$P_2(x) = x_4 + x^3 + 1$$

Con $P(0) = 1$ y $P(1) = 3 = 1$, por lo que no tiene raíces. Al ser de grado 4, y no tener divisores de grado 1, si no fuera irreducible, sería producto de dos polinomios de grado 2. Supongamos que es así para ver si esto es posible, sean $a_1, a_0, b_1, b_0 \in \{0, 1\}$:

$$(x^2 + a_1x + a_0)(x^2 + b_1x + b_0) = x^4 + (b_1 + a_1)x^3 + (b_0 + a_1b_1 + a_0)x^2 + (a_1b_0 + a_0b_1)x + a_0b_0$$

De donde obtenemos, igualando al polinomoi original:

$$\begin{cases} b_1 + a_1 = 1 & (1) \\ b_0 + a_1b_1 + a_0 = 0 & (2) \\ a_1b_0 + a_0b_1 = 0 & (3) \\ a_0b_0 = 1 & (4) \end{cases}$$

De (4) deducimos que $a_0 = 1 = b_0$. Sustituyendo en (3) queda

$$a_1 + b_1 = 0 \quad \#$$

Esto es una contradicción, pues no pueden ser (1) y (3) posibles simultáneamente.

Por tanto, no puede hacerse esta factorización con polinomios de grado 2, de forma que P es irreducible en $\mathbb{Z}_2[2]$, lo que hemos visto que implica que también es irreducible en $\mathbb{Z}[x]$.

(8) $x^n - p$ donde $n > 0$ y p es un entero primo con $p \equiv 1 \ mod \ 3$, en $\mathbb{R}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}_3[x]$

Primero, nótese que es primitivo en $\mathbb{Z}[x]$.

Comencemos en $\mathbb{Z}_3[x]$, donde

$$x^n - p = x^n - 1$$

Y tenemos que 1 es raíz del polinomio. Por lo que es divisible por $x - 1$ y, por tanto, no es irreducible en $\mathbb{Z}_3[x]$.

Para $\mathbb{Q}[x]$, al ser primitivo, puedo ver qué ocurre en $\mathbb{Z}[x]$, y el resultado será equivalente. Así, tenemos que

$$p| - p \implies p|a_i, \ \forall i < n$$

$$p^2 \nmid -p = a_0$$

El criterio de Eisenstein nos asegura que P es irreducible en $\mathbb{Z}[x]$, por lo que también lo es en $\mathbb{Q}[x]$.

Por último, en $\mathbb{R}[x]$.

Se tiene que

$$x^n - p = 0 \iff x^n = p \iff x = \sqrt[n]{p}$$

Y esta raíz existe $\forall n \in \mathbb{N}$, pues p se trata de un entero positivo. Por tanto, P tiene, al menos, una raíz en $\mathbb{R}$. Esto quiere decir que no es irreducible en $\mathbb{R}[x]$.