

ALGEBRA II

Licenciatura en Ciencias Matemáticas

1. Decidir cuáles de los siguientes ideales de $\mathbb{Z}[x]$ son primos y cuáles son maximales:

$$(x+1); (2, x); (3, x); (6, x); (x^2).$$

Solución.

En primer lugar,

$\mathbb{Z}[x]/(x+1) \simeq \mathbb{Z}[-1] = \mathbb{Z}$. con lo que por ser íntegro el cociente, el ideal $(x+1)$ es primo.

Por otra parte,

$\mathbb{Z}[x]/(2, x) \simeq \mathbb{Z}_2$, que es un cuerpo, con lo que $(2, x)$ es un ideal maximal.

Análogamente

$\mathbb{Z}[x]/(3, x) \simeq \mathbb{Z}_3$, con lo que $(3, x)$ es maximal.

El ideal $(6, x)$ no es primo pues $2 \cdot 3 \in (6, x)$, y $2 \notin (6, x)$, $3 \notin (6, x)$. De otra forma: $\mathbb{Z}[x]/(6, x) \simeq \mathbb{Z}/(6)$, que no es un dominio de integridad, pues en este anillo $2 \cdot 3 \in (0)$.

Por último, de forma análoga, el ideal (x^2) no es primo en $\mathbb{Z}[x]$, pues $x \cdot x \in (x^2)$ y $x \notin (x^2)$.

2. Dado el polinomio $p(x) = x^3 + 2x^2 + 1$ estudiar si es irreducible en $\mathbb{Z}_3[x]$, $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}_{17}[x]$.

Solución.

El polinomio $p(x) = x^3 + 2x^2 + 1$ es irreducible como elemento de $\mathbb{Z}_3[x]$, si y sólo si p no tiene raíces en $\mathbb{Z}/(3)$, lo cual es muy fácil de comprobar.

De esta forma (criterio del módulo finito) p es irreducible como elemento de $\mathbb{Z}[x]$ y por tanto también como elemento de $\mathbb{Q}[x]$ (ya que \mathbb{Z} es DFU, y el contenido de p es 1).

En cambio, en \mathbb{Z}_{17} se tiene que $p(2) = 0$, lo que proporciona fácilmente la factorización:

$$p(x) = (x-2)(x^2 + 4x + 8) = (x-2)(x-6)(x-7).$$

3. Consideremos el polinomio $p(x) = x^3 + 2x^2 + 2x + 2$.

a) Estudiar si f es irreducible en $\mathbb{Q}[x]$.

- b) Sea u una raíz suya. Calcular el grado $[\mathbb{Q}[u]:\mathbb{Q}]$.
- c) Determinar una base de $\mathbb{Q}[u]$ como espacio vectorial sobre \mathbb{Q} .
- d) Hallar las coordenadas de $u^3 \in \mathbb{Q}[u]$ respecto de la base del apartado anterior.

Solución.

Es el ejercicio 95 de Fernández Laguna.

4. Calcular el resto de la división de $14!$ entre 17.

Solución.

Por la congruencia de Wilson sabemos que $16! \equiv -1 \pmod{17}$.

Pero $16! = 16 \cdot 15 \cdot 14! = (-1) \cdot (-2) \cdot 14! = 2 \cdot 14!$. Con lo que:

$$2 \cdot 14! \equiv -1 \pmod{17}.$$

Multiplicando por 9 (pues es el inverso de 2 en el anillo $\mathbb{Z}/(17)$),

$$18 \cdot 14! \equiv -9 \equiv 8 \pmod{17}.$$

En conclusión:

$$14! \equiv 8 \pmod{17}.$$