Conjuntos y Números

LISTA 7 CURSO 2018-19

1) Hallar el cociente $C(X)$ y el resto $R(X)$ que resultan de dividir el polinomio

$$P(X) = 3X^5 + 2X^3 + X + 1 \text{ entre el } Q(X) = 3X^2 + 1 \ .$$

Hallarlos primero en $\mathbb{Q}[X]$ y luego en $\mathbb{Z}_5[X]$.

2) Sean P, $Q \in \mathbb{Q}[X]$. Probar que P y Q son *coprimos* si y sólo si $P+Q$, $P \cdot Q$ también lo son.

3) Calcular el máximo común divisor $D(X)$ de los polinomios

$$P(X) = X^5 - 5X^3 + 4X \qquad \text{y} \qquad Q(X) = X^3 - 2X^2 - 5X + 6$$

Encontrar dos polinomios $A(X)$ y $B(X)$ tales que: $A(X)\cdot P(X)+B(X)\cdot Q(X) = D(X)$.

4) Encontrar polinomios $A(X)$ y $B(X)$ en $\mathbb{Q}[X]$ tales que:

$$A(X)(X^2 + 2X - 2) + B(X)(X^2 + X - 1) = 1.$$

5) Hallar un polinomio $P(X) \in \mathbb{Q}[X]$ tal que X^2+1 divida a $P(X)$, y X^3+1 divida a $P(X)-1$, siendo el grado de P el mínimo posible.

6) Hallar los ceros racionales del polinomio $P(X) = 20X^3 - 56X^2 + 33X + 9$

7) Hallar todos los ceros de $P(X) = X^4 + 7X^3 + 9X^2 - 27X - 54$, con sus multiplicidades. Razonar y comprobar lo que esos ceros implican para el máximo común divisor de $P(X)$ y su derivada $P'(X)$.

8) Los números $2+\sqrt[3]{3}$, $\sqrt{2}+\sqrt{3}$, son, cada uno de ellos, cero de algún polinomio de $\mathbb{Z}[X]$. Hallar esos polinomios.

9) a) Demostrar que para cualquier cuerpo conmutativo $\mathbb{K}$, existen infinitos polinomios irreducibles en $\mathbb{K}[X]$.
Sugerencia: recordar la prueba de Euclides de que hay en $\mathbb{Z}$ infinitos números primos.
b) Deducir que si $\mathbb{K}$ es un cuerpo con un número finito de elementos (por ejemplo $\mathbb{K} = \mathbb{Z}_p$ para p primo) habrá en $\mathbb{K}[X]$ polinomios irreducibles de grado arbitrariamente grande.

10) a) Deducir aplicando el criterio de irreducibilidad de Eisenstein que $\forall\ n > 1$ existen infinitos polinomios de grado n que son irreducibles en $\mathbb{Q}[X]$.
b) Descomponer $P(X) = X^5 - X^4 + 2X^3 - 2$ en factores irreducibles en $\mathbb{Q}[X]$.

11) a) Probar que un polinomio $P(X) \in \mathbb{K}[X]$ es irreducible si y solamente si es irreducible el polinomio $Q(X) = P(X + a)$ para cualquier $a \in \mathbb{K}$.

b) Aplicar el resultado anterior con $a = 1$ para demostrar que el *polinomio ciclotómico*

$$\frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + 1 \in \mathbb{Q}[X],$$

donde p es un número primo, es irreducible.

12) a) Determinar los polinomios mónicos irreducibles en $\mathbb{Z}_2[X]$ de grados $1, 2, 3$ y 4.

b) Demostrar que el polinomio $P(X) = X^4 + 3X^3 + 5X^2 + 7X + 1$ es irreducible en $\mathbb{Q}[X]$

13) Descomponer el polinomio $p(X) = X^4 + 3X^2 + 4$ en sus factores irreducibles en $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$ y en $\mathbb{Z}_p[X]$, para $p = 2, 3, 5$ y 7.

14) Sean $\mathbb{K}$ un cuerpo conmutativo y $P(X) \in \mathbb{K}[X]$. Se denota por $\mathbb{K}[X]/(P(X))$ el conjunto cociente de $\mathbb{K}[X]$ por la relación de equivalencia

$$Q_1(X)\, \mathcal{R}\, Q_2(X) \Leftrightarrow Q_1(X) - Q_2(X) = A(X)P(X) \text{ para algún } A(X) \in \mathbb{K}[X],$$

dotado de las operaciones

+) $\overline{Q_1(X)} + \overline{Q_2(X)} = \overline{Q_1(X) + Q_2(X)}$,

·) $\overline{Q_1(X)} \cdot \overline{Q_2(X)} = \overline{Q_1(X)Q_2(X)}$.

$\mathbb{K}[X]/(P(X))$ adquiere una estructura de anillo (de la misma forma que lo hacía el conjunto cociente $\mathbb{Z}/(m)$, donde ahora $\mathbb{K}[X]$ juega el papel de $\mathbb{Z}$ y $P(X)$ el de m).

a) Deducir del ejercicio 4 que $\overline{X^2 + 2X - 2}$ es una unidad de $\mathbb{Q}[X]/(X^2 + X - 1)$ y que $\overline{X^2 + X - 1}$ lo es de $\mathbb{Q}[X]/(X^2 + 2X - 2)$.

b) Más generalmente, probar que si $P(X), Q(X) \in \mathbb{K}[X]$ son primos entre sí, entonces $\overline{P(X)}$ es una unidad de $\mathbb{K}[X]/(Q(X))$ y que $\overline{Q(X)}$ lo es de $\mathbb{K}[X]/(P(X))$.

c) Deducir que si $P(X) \in \mathbb{K}[X]$ es irreducible entonces $\mathbb{K}[X]/(P(X))$ es un cuerpo.

d) Demostrar que $\mathbb{R}[X]/(X^2 + 1)$ es un cuerpo (isomorfo al cuerpo $\mathbb{C}$ de los números complejos).

15) Denotemos por $\mathbb{F}_p = \mathbb{Z}/(p) = \mathbb{Z}_p$ el cuerpo finito con p elementos.

a) Demostrar que $\mathbb{F}_2[X]/(X^2 + 1)$ no es un cuerpo y que $\mathbb{F}_2[X]/(X^2 + X + 1)$ sí lo es.

b) Escribir los 4 elementos del cuerpo $\mathbb{F}_2[X]/(X^2 + X + 1)$. (*Sugerencia:* $\overline{X^2} = \overline{X + 1}$).

c) Señalar en $\mathbb{F}_2[X]/(X^2 + 1)$ un elemento no nulo que no tenga inverso multiplicativo.

d) Señalar en $\mathbb{F}_2[X]/(X^2 + X + 1)$ el inverso multiplicativo de cada elemento no nulo.

e) Construir un cuerpo con 2^3 elementos como un cociente adecuado de $\mathbb{F}_2[X]$.

f) Construir cuerpos con 3^2 y 3^3 elementos como cocientes adecuados de $\mathbb{F}_3[X]$.