Etructuras algebraicas **2º de Matemáticas**
CURSO 2020-2021 20 DE ENERO DE 2021

Ejercicio 3 (3,4 puntos)

(TIEMPO DISPONIBLE PARA TODO EL EXAMEN: 2 HORAS Y MEDIA.
DEBES PRESENTAR LOS 3 EJERCICIOS QUE ELIJAS).

APELLIDOS Y NOMBRE ______________________________

GRUPO ______ D.N.I. ____________________ FIRMA ______________

Denotemos por $\mathbb{F}_3[X]$ el anillo de polinomios con coeficientes en el cuerpo $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$ y por $(f(X))$ el ideal de $\mathbb{F}_3[X]$ generado por un polinomio $f(X) \in \mathbb{F}_3[X]$.

a) (1,6 puntos). Supongamos que $f(X) = X^2 + X + 1$. Se pide:
1) Decidir si $(f(X))$ es un ideal primo o maximal y si el anillo cociente $A = \mathbb{F}_3[X]/(f(X))$ tiene divisores de cero. Si tiene divisores de cero dar uno explícitamente.
2) Responder a las mismas preguntas para el polinomio $f(X) = X^2 + X + 2$.

a.1) $f(x) = x^2 + x + 1 \in \mathbb{F}_3[X]$

• Claramente, $f(1) = 0 \Rightarrow f(x)$ es reducible $\Rightarrow (f(x))$ no es un ideal primo $\Rightarrow \mathbb{F}_3[X]/(f(x))$ tiene divisores de cero.

• Como 1 es la única raiz, vemos que $f(x) = (x-1)^2 \in \mathbb{F}_3[X] \Rightarrow$
$\Rightarrow \overline{0} = \overline{f(x)} = \overline{(x-1)}^2 = \overline{(x-1)}\,\overline{(x-1)} \Rightarrow \overline{x-1}$ es un divisor de cero.
($\overline{x-1} \neq 0$ porque $x-1 \notin (x^2+x+1)$ ya que $\deg(x-1) = 1 < \deg(x^2+x+1) = 2$).

a.2) $f(x) = x^2 + x + 2 \in \mathbb{F}_3[X]$

Tenemos $f(0) = 2 \neq 0$, $f(1) = 1 \neq 0$, $f(2) = 2 \neq 0 \Rightarrow f(x)$ es irreduc.
$\Rightarrow (f(x))$ es un ideal primo (e incluso maximal) $\Rightarrow$
$\Rightarrow \mathbb{F}_3[X]/(f(x))$ es íntegro (e incluso un cuerpo) $\Rightarrow$ no tiene divisores de cero.

b) (0,6 puntos). Para cada uno de los anillos cociente $A = \mathbb{F}_3[X]/(X^2+X+1)$ y $B = \mathbb{F}_3[X]/(X^2+X+2)$ decidir si el elemento $\overline{X} = X + (f(X))$ es una unidad, y si lo es decir quién es su inverso.

b.1) $A = \dfrac{\mathbb{F}_3[X]}{(X^2+X+\bar{1})}$

Tenemos $\bar{0} = \overline{X^2+X+1} \Rightarrow \bar{1} = -\bar{X}^2 - \bar{X} = \bar{X}(-\bar{X}-\bar{1}) \Rightarrow \bar{X}$ es una unidad

y su inverso es $-\bar{X}-\bar{1} = \bar{2}\bar{X}+\bar{2}$.

b.2) $B = \dfrac{\mathbb{F}_3[X]}{(X^2+X+\bar{2})}$

B es un cuerpo, luego ahora seguro que $\bar{X}$ va a ser una unidad.

Procediendo como antes, tenemos:

$\bar{0} = \bar{X}^2+\bar{X}+\bar{2} \Rightarrow \bar{X}^2+\bar{X} = -\bar{2} = \bar{1} \Rightarrow \bar{X}(\bar{X}+\bar{1}) = \bar{1}$; luego el inverso de $\bar{X}$ es $(\bar{X}+\bar{1})$.

c) (1,2 puntos) De los dos grupos abelianos siguientes $(B,+)$ (grupo aditivo del anillo B del apartado anterior) y $(B^*,.)$ (grupo de las unidades del anillo B del apartado anterior) uno de ellos es cíclico y el otro no. Se pide:

1) dar un generador del que es cíclico y

2) descomponer el que no lo es como producto de grupos cíclicos.

2) $(B,+)$. Como $ch(B)=3$, para todo $\overline{q(X)} \in B = \dfrac{\mathbb{F}_3[X]}{(X^2+X+2)}$ se tiene:

$3\overline{q(X)} = \overline{q(X)}+\overline{q(X)}+\overline{q(X)} = (\bar{1}+\bar{1}+\bar{1})\overline{q(X)} = \bar{0}\cdot\overline{q(X)} = \bar{0} \Rightarrow$ todo elemento de $(B,+)$ distinto de $\bar{0}$ tiene orden 3.

Por otra parte $\deg(X^2+X+2)=2 \Rightarrow \mathrm{card}(B) = 3^2$.

Luego $(B,+) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

1) $(B^*, \cdot)$, donde $B = \mathbb{F}_3[X]/(X^2+X+2)$

Como $(B,+)$ no es cíclico el enunciado del ejercicio nos dice que $(B^*, \cdot)$ debe serlo (además de que ya hicimos un ejercicio en el que vimos que, en general, el grupo multiplicativo de un cuerpo finito es cíclico)

Queremos encontrar un generador, es decir un elemento de orden $|B^*| = 8$. Probemos con $\bar{x}$.

- $\bar{x}^2 = -\bar{x} - \bar{2} = 2\bar{x} + \bar{1} \neq \bar{1}$, pues $2x \notin (x^2+x+1)$, $\Rightarrow$

  $\Rightarrow \mathrm{ord}(\bar{x}) > 2 \Rightarrow \mathrm{ord}(\bar{x}) = 4$ ó 8. (Vamos bien)

- $\bar{x}^4 = (\bar{x}^2)^2 = (2\bar{x} + \bar{1})^2 = 4\bar{x}^2 + \bar{1} + 4\bar{x} = \bar{x}^2 + \bar{x} + 1 =$

  $= -\bar{x} - \bar{2} + \bar{x} + \bar{1} = -\bar{1} = \bar{2} \neq \bar{1} \Rightarrow \mathrm{ord}(\bar{x}) > 4 \Rightarrow$

  $\Rightarrow \mathrm{ord}(\bar{x}) = 8$.

Luego $(B^*, \cdot) = \langle \bar{x} \rangle$.