

Estructuras Algebraicas
Convocatoria ordinaria, 19 de enero de 2022

DURACIÓN DEL EXAMEN: 2 HORAS Y 30 MINUTOS

APELLIDOS: _____
NOMBRE: _____ DNI/NIE: _____ GRUPO: 130 / 726

Ejercicio 3. (2 puntos) Razona si cada uno de los enunciados siguientes es verdadero o falso, aportando una prueba o un contraejemplo en cada caso.

a) Si N es un subgrupo normal de G con $G/N \cong C_{20}$ entonces G tiene exactamente 6 subgrupos normales M con $N \subseteq M$.

b) Si $G = HK$ con H y K subgrupos abelianos de G , entonces G es abeliano.

Solución. a) Verdadero. Por el Teorema de correspondencia en grupos existe una biyección entre el conjunto de subgrupos de G que contienen a N y el conjunto de subgrupos del cociente G/N . Además, esta correspondencia lleva subgrupos normales a subgrupos normales. En definitiva, se trata de probar que C_{20} tiene exactamente 6 subgrupos normales. Como C_{20} es un grupo abeliano, todo subgrupo es normal; así que se trata de probar que C_{20} tiene exactamente 6 subgrupos. Como C_{20} es cíclico, tiene un **único** subgrupo de orden d , para cada divisor d de su orden. El enunciado se sigue puesto que 20 tiene exactamente 6 divisores.

b) Falso. $G = S_3$, $H = \langle (123) \rangle$ y $K = \langle (12) \rangle$ constituyen un contraejemplo al enunciado.

Ejercicio 4. (3 puntos) Sea $\mathbb{F}_2[X]$ el anillo de polinomios sobre el cuerpo $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Escribimos $R = \mathbb{F}_2[X]/(X^3 + 1)$ donde $(X^3 + 1)$ es el ideal generado por $X^3 + 1 \in \mathbb{F}_2[X]$.

a) Describe todos los ideales del anillo R .

b) Decide si $X + (X^3 + 1) \in R$ es una unidad de R y, en caso afirmativo, encuentra su inverso.

c) Encuentra todos los polinomios $p(X) \in \mathbb{F}_2[X]$ tales que el anillo cociente $\mathbb{F}_2[X]/(p(X))$ sea un cuerpo con 16 elementos.

Solución. a) Por el Teorema de correspondencia en anillos existe una biyección entre los ideales del cociente R y los ideales I de $\mathbb{F}_2[X]$ que contienen a $(X^3 + 1)$. Como $\mathbb{F}_2[X]$ es un dominio de ideales principales, se tiene que cada ideal I está generado por un elemento $f(X) \in \mathbb{F}_2[X]$. Además, como la única unidad de $\mathbb{F}_2[X]$ es la unidad del anillo, el generador $f(X)$ de I es único. Recordamos que $(X^3 + 1) \subseteq (f(X))$ si, y solo si, $f(X)$ divide a $(X^3 + 1)$. Por tanto, los ideales de R son de la forma $(f(X))/(X^3 + 1)$ para cada uno de los divisores de $X^3 + 1$. La descomposición en irreducibles de $X^3 + 1$ es $X^3 + 1 = (X + 1)(X^2 + X + 1)$ de donde se sigue que los ideales de R son exactamente

$$\{\{0_R\}, (X + 1)/(X^3 + 1), (X^2 + X + 1)/(X^3 + 1), R\}.$$

b) $X + (X^3 + 1) \in \mathcal{U}(R)$ puesto que $\text{mcd}(X^3 + 1, X) = 1$. Como $X^3 + 1 - X^2 \cdot X = 1$, obtenemos que $(X + (X^3 + 1))^{-1} = X^2 + (X^3 + 1)$.

c) El anillo $\mathbb{F}_2[X]/(p(X))$ es un cuerpo si, y solo si, $(p(X))$ es maximal si, y solo si, $p(X)$ es irreducible. Por otro lado, $\mathbb{F}_2[X]/(p(X))$ tiene 16 elementos si, y solo si, $p(X)$ es un polinomio de grado 4 (usando el algoritmo de la división). Por tanto, el apartado nos pide calcular todos los polinomios irreducibles de grado 4 en $\mathbb{F}_2[X]$.

Notamos que $p(X)$ es irreducible si, y solo si, cumple las siguientes propiedades:

- $p(X)$ no tiene raíces en $\mathbb{F}_2[X]$.
- $p(X)$ no es producto de 2 polinomios irreducibles de grado 2 en $\mathbb{F}_2[X]$.

La primera de estas condiciones nos deja como candidatos los polinomios: $X^4 + X^3 + X^2 + X + 1$, $X^4 + X^3 + 1$, $X^4 + X^2 + 1$, $X^4 + X + 1$. La segunda condición nos dice que debemos descartar aquellos que son producto de 2 polinomios irreducibles de grado 2. Como $\mathbb{F}_2[X]$ tiene un único irreducible de grado 2, $X^2 + X + 1$, debemos descartar su cuadrado $(X^2 + X + 1)^2 = X^4 + X^2 + 1$. Por tanto, los polinomios buscados son

$$X^4 + X^3 + X^2 + X + 1, X^4 + X^3 + 1, X^4 + X + 1.$$
