

Soluciones del 2do parcial de Matemática Discreta 2

02 de julio de 2005.

Ejercicio 1.

Sea G un grupo **no abeliano** de orden 385.

(1) (4 puntos) Probar que son únicos el subgrupo de Sylow S_{11} de orden 11 y el subgrupo de Sylow S_7 de orden 7. Deducir que son subgrupos normales.

SOLUCIÓN: $n_{11} = 1 + k11|35$, $k \in \mathbb{Z}$, luego $n_{11} = 1$, lo cual implica que existe un único subgrupo de Sylow S_{11} y además es normal en G .

$n_7 = 1 + k7|55$, $k \in \mathbb{Z}$, luego $n_7 = 1$, lo cual implica que existe un único subgrupo de Sylow S_7 y además es normal en G .

(2) (6 puntos) Probar que $S_{11}S_7$ es un subgrupo normal de G . Hallar su orden.

SOLUCIÓN: Al ser S_{11} y S_7 subgrupos normales de G , $S_{11}S_7$ es un subgrupo de G ya que $S_{11}S_7 = S_7S_{11}$. Por otro lado todo elemento de $S_{11}S_7$ es de la forma ab con $a \in S_{11}$ y $b \in S_7$.

$gabg^{-1} = gag^{-1}gbg^{-1} \in S_{11}S_7$, $\forall g \in G$ pues S_{11} y S_7 son normales. Luego $S_{11}S_7$ es un subgrupo normal de G .

$|S_{11}S_7| = \frac{|S_{11}||S_7|}{|S_{11} \cap S_7|} = \frac{11 \times 7}{|S_{11} \cap S_7|}$. Todo elemento distinto de e_G en S_{11} tiene orden 11 y todo elemento distinto de e en S_7 tiene orden 7, luego $S_{11} \cap S_7 = \{e_G\}$. Por lo tanto $|S_{11}S_7| = 77$.

(3) (8 puntos) Probar que hay exactamente 11 subgrupos de Sylow de orden 5.

Sugerencia: Si $n_5 = 1$, probar, usando la parte anterior, que $G \simeq S_{11} \times S_7 \times S_5$, lo cual contradice la "no abelianidad" de G .

SOLUCIÓN: $n_5 = 1 + k5|77$ luego $n_5 = 1$ o 11. Probemos que $n_5 \neq 1$. Supongamos, por absurdo, que $n_5 = 1$, entonces S_5 es único y normal.

$|S_{11}S_7S_5| = \frac{|S_{11}S_7||S_5|}{|S_{11}S_7 \cap S_5|}$. Como $S_{11}S_7 \cap S_5 = \{e_G\}$, se tiene que $|S_{11}S_7S_5| = 11 \times 7 \times 5 = 385 = |G|$, luego $S_{11}S_7S_5 = G$.

Luego G es isomorfo a $S_{11} \times S_7 \times S_5$. Como $S_{11} \times S_7 \times S_5$ es abeliano, deducimos que G es abeliano lo cual es absurdo.

(4) (7 puntos) Hallar la cantidad de elementos de orden 5 en G .

SOLUCIÓN: Por un lado, dados dos 5-Sylow distintos S_5 y S'_5 , se tiene que $S_5 \cap S'_5 = \{e_G\}$. Por otro lado, cada elemento de orden 5 en G genera un 5-Sylow y todos los elementos de orden 5 en G están en algún 5-Sylow. Luego cada subgrupo 5-Sylow tiene exactamente 4 elementos de orden 5 y como hay 11 subgrupos de Sylow diferentes se concluye que hay $4 \times 11 = 44$ elementos de orden 5 en G .

Ejercicio 2 (15 puntos).

$$\text{Sean } \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 1 & 6 & 2 \end{pmatrix} \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 6 & 5 \end{pmatrix} \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 6 & 5 \end{pmatrix}$$

(1) (5 puntos) Hallar los órdenes de α, β y σ .

SOLUCIÓN: $\alpha = (123)(4)(56)$ y $\beta = (132)(4)(56)$. El orden de una permutación es el *mcm* de los ordenes de los ciclos disjuntos en que se descompone. Luego el orden de α y el orden de β son iguales a $\text{mcm}(3, 2) = 6$. Por otro lado $\sigma = (134)(256)$, luego el orden de σ es 3.

(2) (5 puntos) Calcular $\alpha\sigma\beta$. (Sugerencia: puede ser útil calcular $\alpha\beta$).

SOLUCIÓN: $\alpha\sigma\beta = (142)(365)$.

(3) (5 puntos) Calcular σ^{2005} .

SOLUCIÓN: $\sigma^{2005} = ((134)(256))^{2005}$. Como (134) y (256) son ciclos disjuntos entonces conmutan y $\sigma = (134)^{2005}(256)^{2005} = (134)^{3 \times 668 + 1}(256)^{3 \times 668 + 1} = (134)(256)$.

Ejercicio 3 (20 puntos).

Sobre \mathbb{R}^2 consideramos la operación:

$$(a, b) \otimes (c, d) = (ac, ad + bc),$$

con la suma y el producto usual de \mathbb{R} .

(1) (a) (4 puntos) Probar que $A = (\mathbb{R}^2, +, \otimes)$ es un anillo conmutativo y con unidad.

SOLUCIÓN: A cargo del lector: se tiene que probar todas las propiedades. La unidad del anillo es $(1, 0)$ y el elemento neutro es $(0, 0)$.

(b) (3 puntos) Probar que el conjunto $I = \{(0, \alpha) : \alpha \in \mathbb{R}\}$ es un ideal de A .

SOLUCIÓN: - $(I, +, (0, 0))$ es un subgrupo de $(\mathbb{R}^2, +)$.

- si $(a, b) \in A$ y $(0, \alpha) \in I$, $(0, \alpha) \otimes (a, b) = (a, b) \otimes (0, \alpha) = (a \times 0, a \times \alpha + b \times 0) = (0, a\alpha) \in I$.

(c) (3 puntos) Hallar los divisores propios de cero de A .

Sean (a, b) y (c, d) dos elementos distintos de $(0, 0)$ en A . $(a, b) \otimes (c, d) = (0, 0)$ implica que $(ac, ad + bc) = (0, 0)$, es decir

$$\begin{cases} ac = 0 \\ ad + bc = 0 \end{cases} \rightarrow \begin{cases} a \text{ o } c = 0 \\ ad + bc = 0 \end{cases}$$

- Si $a = 0$ entonces $bc = 0$ lo cual implica que $b = 0$ o $c = 0$. Pero si $b = 0$, entonces $(a, b) = (0, 0)$, entonces $c = 0$

- Si $c = 0$ entonces $ad = 0$ lo cual implica que $a = 0$ o $d = 0$. Pero si $d = 0$, entonces $(c, d) = (0, 0)$, entonces $a = 0$.

Luego los divisores propios de cero son los elementos no nulos de I .

(2) Sean $\mathbb{R}[X]$ el anillo de los polinomios con coeficientes reales y $\varphi : \mathbb{R}[X] \longrightarrow A$ tal que

$$\varphi(p) = (p(0), p'(0))$$

con p' la derivada de p .

(a) (4 puntos) Probar que φ es un homomorfismo de anillos.

$$\varphi(p+q) = ((p+q)(0), (p+q)'(0)) = (p(0)+q(0), p'(0)+q'(0)) = (p(0), q(0)) + (p'(0), q'(0)) = \varphi(p) + \varphi(q).$$

$$\varphi(pq) = ((pq)(0), (pq)'(0)) = (p(0)q(0), p'(0)q(0) + p(0)q'(0)) = (p(0), p'(0)) \otimes (q(0), q'(0)) = \varphi(p) \otimes \varphi(q).$$

Concluimos que φ es un homomorfismo de anillos.

(b) (2 puntos) Probar que φ es sobreyectivo.

Dados $(a, b) \in A$, sea $p(x) = bx + a$. Entonces $\varphi(p) = (p(0), p'(0)) = (a, b)$, luego φ es sobreyectivo.

(c) (4 puntos) Probar que $\mathbb{R}[x]/(x^2) \simeq A$.

$\ker(\varphi) = \{p(x) \in \mathbb{R}[x] : p(0) = 0, p'(0) = 0\}$. Si $p(x) = \sum_{i=0}^n a_i x^i$, $p(0) = 0$ si y solamente si $a_0 = 0$ y $p'(0) = 0$ si y solamente si $a_1 = 0$. Luego:

$$\ker(\varphi) = \{p(x) = a_n x^n + a_{n-1} x^{n-1} \cdots + a_2 x^2 + a_1 x + a_0 \in \mathbb{R}[x] : a_1 = a_0 = 0\},$$

$$\ker(\varphi) = \{p(x) \in \mathbb{R}[x] : p(x) \text{ es múltiplo de } x^2\}.$$

Luego $\ker(\varphi) = (x^2)$ y por el primer teorema de homomorfismo de anillos $\mathbb{R}^2/(x^2) \simeq A$.

Ejercicio 4 (10 puntos).

(1) (4 puntos) Determinar si el polinomio $x^2 + 1$ es irreducible en $\mathbb{Z}_2[x]$, $\mathbb{Z}_3[x]$ y $\mathbb{Z}_5[x]$. Justificar y, en caso de ser reducible, dar una factorización en irreducibles.

SOLUCIÓN: Un polinomio de grado 2 es irreducible en $k[X]$ si y solamente si no tiene raíces en k .

Consideramos $p(x) = x^2 + 1 \in \mathbb{Z}_2[x]$. $p(0) = 1 \neq 0$ y $p(1) = 0$, luego 1 es raíz por lo cual $p(x)$ es reducible en $\mathbb{Z}_2[x]$ y $p(x) = (x+1)(x+1)$.

Consideramos $p(x) = x^2 + 1 \in \mathbb{Z}_3[x]$. $p(0) = 1 \neq 0$, $p(1) \neq 0$ y $p(2) \neq 0$, luego $p(x)$ es irreducible en $\mathbb{Z}_3[x]$.

Consideramos $p(x) = x^2 + 1 \in \mathbb{Z}_5[x]$. $p(0) = 1 \neq 0$, $p(1) \neq 0$, $p(2) = 0$, $p(3) = 0$, $p(4) \neq 0$, luego 2 y 4 son raíces de $p(x)$ por lo cual $p(x) = (x+2)(x+4)$.

(2) (3 puntos) Dar una lista de todos los polinomios de grado 2 irreducibles en $\mathbb{Z}_2[x]$.

SOLUCIÓN: Sea $P(x) = ax^2 + bx + c \in \mathbb{Z}_2[x]$ con $a \neq 0$. Para que $P(x)$ sea irreducible entonces 0 y 1 no tienen que ser raíces de P .

$P(0) = c \neq 0$, es decir $c = 1$.

$P(1) = a + b + c \neq 0$ y al ser $c = 1$, esto implica $a + b \neq 1$, o sea $a + b = 0$, es decir que $a = b$ (En \mathbb{Z}_2 un elemento es opuesto de sí mismo). Como $P(x)$ es de grado 2, $a \neq 0$, luego $a = b = 1$. Concluimos que el único polinomio de grado 2 irreducible en $\mathbb{Z}_2[x]$ es $x^2 + x + 1$.

(3) (3 puntos) Dar una lista de todos los polinomios **mónicos** de grado 2 irreducibles en $\mathbb{Z}_3[x]$.

Sea $P(x) = x^2 + bx + c \in \mathbb{Z}_3[x]$. Para que $P(x)$ sea irreducible entonces 0, 1 y 2 no tienen que ser raíces de P .

$P(x) = x^2 + bx + c$ y $P(0) = c \neq 0$ solamente si $c = 1$ o $c = 2$.

- Si $c = 1$, $P(1) = 2 + b \neq 0$, luego $b \neq 1$, es decir $b = 0$ o $b = 2$.

$P(2) = 2 + 2b \neq 0$, luego $2(1+b) \neq 0$, es decir $b \neq 2$.

Concluimos que necesariamente, $b = 0$, por lo cual en este caso, el único polinomio irreducible es $p(x) = x^2 + 1$.

- Si $c = 2$, $P(1) = 3 + b \neq 0$, luego $b \neq 0$, es decir $b = 1$ o $b = 2$.

$P(2) = 3 + 2b \neq 0$, luego $b \neq 0$, es decir $b \neq 2$.

En este caso los polinomios irreducibles son $x^2 + x + 2$ y $x^2 + 2x + 2$.