

Soluciones al Segundo parcial de Matemática Discreta 2

1. Sea $n \in \mathbb{N}$, $n > 1$. Se considera el conjunto

$$G_n = \{P : \mathbb{R} \rightarrow \mathbb{R} / P \text{ polinomio con coeficientes en } \mathbb{R} \text{ de grado } \leq n\}$$

con la suma usual de polinomios.

- (a) Probar que $(G_n, +)$ es un grupo abeliano.

Un polinomio genérico en G_n se escribe como

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = \sum_{h=0}^n a_h x^h$$

La suma de $P, Q \in G_n$ es

$$\sum_{h=0}^n a_h x^h + \sum_{h=0}^n b_h x^h = \sum_{h=0}^n (a_h + b_h) x^h$$

Esto muestra que el grado de $P + Q$ es menor o igual que n . Muestra también que tomando el polinomio idénticamente nulo (de grado $-\infty$) éste es el neutro de la suma y que el opuesto (inverso respecto a la operación suma) de $P(x) = \sum_{h=0}^n a_h x^h$ es $-P(x) = \sum_{h=0}^n (-a_h x^h)$. La asociatividad resulta de la asociatividad de $(\mathbb{R}, +)$. En efecto:

$$\begin{aligned} (P + Q) + R &= \left(\sum_{h=0}^n a_h x^h + \sum_{h=0}^n b_h x^h \right) + \sum_{h=0}^n c_h x^h = \\ &= \sum_{h=0}^n (a_h + b_h) x^h + \sum_{h=0}^n c_h x^h = \sum_{h=0}^n ((a_h + b_h) + c_h) x^h = \end{aligned}$$

(Por la asociatividad de la suma en \mathbb{R} , $(a_h + b_h) + c_h = a_h + (b_h + c_h)$)

$$= \sum_{h=0}^n (a_h + (b_h + c_h)) x^h = \sum_{h=0}^n a_h x^h + \sum_{h=0}^n (b_h + c_h) x^h = P + (Q + R)$$

Del mismo modo la abelianidad de G_n resulta de la conmutatividad en la suma de reales: $a_h + b_h = b_h + a_h$.

- (b) Se considera $H = \{P(x) \in G_n / P(0) = P'(0) = 0\}$ ($P'(x)$ es la derivada de $P(x)$). Probar que H es subgrupo normal de G_n .

Dado que G_n es abeliano, todos sus subgrupos son normales. Queda entonces ver que H es efectivamente un subgrupo. Es claro que $P \equiv 0$ (el polinomio nulo) está en H .

Si $P \in H$ entonces $P(0) = P'(0) = 0$, entonces el polinomio opuesto, $-P$ cumple también que $-P(0) = 0$. Como la derivada de $-P$ es $-P'$ también se cumple que $(-P)'(0) = -P'(0) = 0$. Luego $-P \in H$.

Si $P, Q \in H$ entonces $P(0) = Q(0) = 0$. Luego $(P+Q)(0) = P(0) + Q(0) = 0 + 0 = 0$. También se cumple que $(P+Q)' = P' + Q'$ y de aquí resulta que $(P+Q)'(0) = P'(0) + Q'(0) = 0$. Luego $P+Q \in H$.

Se probó que H es subgrupo (normal) de G_n .

- (c) Sea $\varphi : G_n \rightarrow G_n$ dado por $\varphi(P(x)) = P''(x)$ ($P''(x)$ es la derivada segunda de $P(x)$). Probar que φ es un homomorfismo de grupos. Hallar $Im(\varphi)$ y $Ker(\varphi)$.

Como $\varphi(P(x)) = P''(x)$ y $(P+Q)'' = P'' + Q''$ resulta que $\varphi(P+Q) = P'' + Q'' = \varphi(P) + \varphi(Q)$ probando que es un homomorfismo. Se cumple que $P \in Ker(\varphi)$ si y solo si $\varphi(P) = 0$ (el polinomio nulo), o sea, $P''(x) = 0 \forall x$. Como si $P(x) = \sum_{h=0}^n a_h x^h$ entonces $P''(x) = \sum_{h=0}^n h(h-1)a_h x^{h-2}$ para que se anule para todo x debe ocurrir que $a_2 = a_3 = \dots = a_n = 0$. Por lo tanto el grado de P debe ser menor o igual que 1 y $P(x) = a_1 x + a_0$. Por otro lado, si grado de P es menor o igual que 1 derivándolo 2 veces da el polinomio nulo y entonces $P \in Ker(\varphi)$ probando que $Ker(\varphi) = G_1$ = polinomios de grado menor o igual que 1.

La misma fórmula para la derivada segunda da

$$P''(x) = \sum_{h=0}^n h(h-1)a_h x^{h-2} = \sum_{h=0}^{n-2} (h+2)(h+1)a_{h+2} x^h$$

Luego $Im(\varphi) \subset G_{n-2}$ = polinomios de grado menor o igual que $n-2$.

Pero dado un polinomio de grado menor o igual que $n-2$ es fácil encontrar uno en G_n que lo tenga por imagen mediante φ . Si $Q(x) = \sum_{h=0}^{n-2} b_h x^h$ tomamos

$$P(x) = \sum_{h=0}^{n-2} \frac{b_h}{(h+1)(h+2)} x^{h+2}$$

(primitivamos dos veces a Q) y entonces se tiene que $\varphi(P) = Q$. Por lo tanto $Im(\varphi) = G_{n-2}$.

- (d) Probar que $G_n/Ker(\varphi)$ es isomorfo a H . [Sugerencia: $Im(\varphi)$ es isomorfo a H definiendo una función $\psi(Q(x)) = x^2 Q(x)$, $Q(x) \in Im(\varphi)$, que hay que ver que es isomorfismo...]

$\psi(Q+R) = x^2(Q+R) = x^2 Q + x^2 R = \psi(Q) + \psi(R)$ probando que ψ es un homomorfismo. Está bien definida, pues multiplicando por x^2 a Q , queda un polinomio que cumple que $x^2 Q(x)$ evaluado en 0 da $0^2 Q(0) = 0$. Derivando una vez queda $2xQ(x) + x^2 Q'(x)$ que al evaluarlo en 0 da 0. Luego la imagen está en H .

Por la parte anterior, un elemento $Q(x)$ de $Im(\varphi)$ es cualquier polinomio en G_{n-2} , luego sus coeficientes b_h son cualesquiera. Al multiplicar $Q(x)$ por x^2 obtengo cualquier elemento de H (sus coeficientes pueden elegirse arbitrariamente). Luego ψ es sobreyectiva.

Finalmente, si $\psi(Q) = 0$, el polinomio nulo, quiere decir que todos los coeficientes de Q van a ser nulos. Luego $ker(\psi) = \{0\}$ y ψ es inyectiva. Entonces ψ es un isomorfismo de grupos. Luego H es isomorfo a $G_{n-2} = Im(\varphi)$. (Notación para decir que dos grupos son isomorfos: $G_{n-2} \cong H$.)

Por otra parte por el primer teorema de homomorfismos de grupos tenemos que $G_n/ker(\varphi) \cong Im(\varphi) = G_{n-2} \cong H$. Por transitividad de la relación de ser isomorfos tenemos que $G_n/ker(\varphi) \cong H$. Esto es lo que se pedía.

2. Recordar que dados $m_1, m_2 \in \mathbb{N}$ tales que $MCD(m_1, m_2) = 1$ y $a_1 \in \mathbb{Z}_{m_1}$, $a_2 \in \mathbb{Z}_{m_2}$ el Teorema Chino del Resto (TChR) dice que existe y es única módulo $m_1 m_2$ la solución b de
$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$$
 y está dada por $b = (a_1 m_2 N_1 + a_2 m_1 N_2) \pmod{m_1 m_2}$ donde $m_2 N_1 \equiv 1 \pmod{m_1}$ y $m_1 N_2 \equiv 1 \pmod{m_2}$.

- (a) Consideramos en $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$ la suma + dada por:

$$(a_1, a_2) + (b_1, b_2) = ((a_1 + b_1) \pmod{m_1}, (a_2 + b_2) \pmod{m_2})$$

Probar que $(\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}, +)$ es un grupo abeliano.

Usamos que \mathbb{Z}_n es grupo abeliano con la suma módulo n .

$$(a_1, a_2) + (b_1, b_2) = ((a_1 + b_1) \pmod{m_1}, (a_2 + b_2) \pmod{m_2}) =$$

$$((b_1 + a_1) \pmod{m_1}, (b_2 + a_2) \pmod{m_2}) = (b_1, b_2) + (a_1, a_2)$$

Esto prueba la abelianidad. El neutro es $(0, 0)$ y el opuesto de $(a_1, a_2) = -(a_1, a_2) = (-a_1, -a_2) = (m_1 - a_1, m_2 - a_2)$ como se verifica de inmediato. Por ejemplo: $(a_1, a_2) + (m_1 - a_1, m_2 - a_2) = (m_1 \pmod{m_1}, m_2 \pmod{m_2}) = (0, 0)$ La asociatividad, como en el ejercicio anterior en que se deriva de la asociatividad en \mathbb{R} , se deriva ahora de la asociatividad en \mathbb{Z}_n .

- (b) Consideramos el grupo $(\mathbb{Z}_{m_1 \times m_2}, +)$ con la suma + módulo $m_1 \times m_2$ (aceptamos que es un grupo) y

$$\varphi : \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \rightarrow \mathbb{Z}_{m_1 \times m_2} / \varphi(a_1, a_2) = b$$

donde b es la solución dada por el TChR. Probar que φ es un homomorfismo de grupos.

Si tenemos que $\varphi((a_1, a_2) + (b_1, b_2)) = d$, la única solución de $(XX) \begin{cases} x \equiv a_1 + b_1 \pmod{m_1} \\ x \equiv a_2 + b_2 \pmod{m_2} \end{cases}$

Y si b es la única solución de $\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$

y c es la única solución de $\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \end{cases}$,

entonces $(b+c) \pmod{m_1 m_2}$ es solución de (XX) y por unicidad tiene que ser d . Luego

$$\varphi((a_1, a_2) + (b_1, b_2)) = d = b + c \pmod{m_1 m_2} = \varphi(a_1, a_2) + \varphi(b_1, b_2)$$

probando que es un homomorfismo.

(c) Probar que φ es inyectiva y sobreyectiva.

Sobreyectividad: Dado $b \in \mathbb{Z}_{m_1 \times m_2}$ tomemos $a_1 = b \pmod{m_1}$ y tomemos $a_2 = b \pmod{m_2}$. Al resolver $\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$ tenemos, teniendo en cuenta que $b =$

$a_1 \pmod{m_1}$ y que $b = a_2 \pmod{m_2}$, que es lo mismo que resolver $\begin{cases} x \equiv b \pmod{m_1} \\ x \equiv b \pmod{m_2} \end{cases}$.

Es obvio que una solución es $x = b$. De aquí resulta por unicidad que es la solución. Luego φ es sobreyectiva.

Para ver la inyectividad consideramos que $\varphi(a_1, a_2) = 0$. Entonces $0 = (a_1 m_2 N_1 + a_2 m_1 N_2) \pmod{m_1 m_2}$. La inyectividad es equivalente a que $\ker(\varphi) = (0, 0)$, o sea, que $a_1 = 0 \pmod{m_1}$ y que $a_2 = 0 \pmod{m_2}$. Tomando módulo respecto a m_1 y teniendo en cuenta que $m_2 N_1 = 1 \pmod{m_1}$ queda $0 \pmod{m_1} = a_1 + 0 \pmod{m_1}$. El "0" de la igualdad corresponde a que $m_1 N_2$ al ser múltiplo de m_1 es 0, módulo m_1 . Luego $a_1 = 0 \pmod{m_1}$. Del mismo modo, tomando módulos respecto a m_2 queda que $a_2 = 0 \pmod{m_2}$.

(d) Deducir que $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$ es un grupo cíclico.

El grupo $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$ resulta, vía φ , isomorfo a $\mathbb{Z}_{m_1 \times m_2}$. Este grupo, como todos los \mathbb{Z}_n , es cíclico. Por ejemplo, el 1 es generador de \mathbb{Z}_n . De aquí, tomando la preimagen de 1 por φ resulta un generador de $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$. Luego este grupo es cíclico.

1. Se considera la permutación $p \in S_{12}$ producto de

$$p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 2 & 5 & 4 & 1 & 3 & 7 & 8 & 11 & 12 & 6 & 9 & 10 \end{pmatrix}$$

y del ciclo $p_2 = (1, 8, 5, 4, 12)$; $p = p_1 p_2$.

Descomponer p en ciclos ajenos, hallar la paridad de p y calcular p^{344} .

Solución: $p = (1, 11, 9, 12, 2, 5)(3, 4, 10, 6, 7, 8)$. p es par pues el producto de dos 6-ciclos, cada ciclo es par o impar según el número de elementos, si interviene un número par de elementos es impar, y si interviene un número impar de elementos entonces es par, luego en este caso cada ciclo es impar. Pero como p es el producto de dos ciclos impares ambos, resulta que p es par. p tiene orden 6 porque el orden de p es el mínimo común múltiplo del orden de sus ciclos (una vez descompuesta p en ciclos ajenos). Por esto resulta que $p^{344} = (p^{6 \cdot 57 + 2} = (p^6)^{57} p^2 = p^2 = (1, 9, 2)(3, 10, 7)(4, 6, 8)(5, 11, 12)$

2. Se considera la permutación $p \in S_{12}$ producto de

$$p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 6 & 5 & 2 & 4 & 8 & 9 & 12 & 1 & 7 & 10 & 11 \end{pmatrix}$$

y del ciclo $p_2 = (12, 7, 4, 3, 11)$; $p = p_1 p_2$.

Descomponer p en ciclos ajenos, hallar la paridad de p y calcular p^{344} .

$p = (1, 3, 10, 7, 2, 6, 8, 12, 9)(4, 5)$, el 11 queda fijo. p impar, orden de p es $mcm\{9, 2\} = 18$. Luego $p^{344} = p^{18 \cdot 19 + 2} = (p^{18})^{19} p^2 = p^2 = (1, 10, 2, 8, 9, 3, 7, 6, 12)$.

3. Se considera la permutación $p \in S_{12}$ producto de

$$p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 12 & 3 & 2 & 11 & 1 & 5 & 6 & 9 & 10 & 4 & 7 & 8 \end{pmatrix}$$

y del ciclo $p_2 = (3, 10, 7, 6, 2)$; $p = p_1 p_2$.

Descomponer p en ciclos ajenos, hallar la paridad de p y calcular p^{344} .

$p = (1, 12, 8, 9, 10, 6, 3, 4, 11, 7, 5)$, p es par. Como el orden de p es 11 y el resto de dividir 344 por 11 es 3 queda que $p^{344} = p^3 = (1, 9, 3, 7, 12, 10, 4, 5, 8, 6, 11)$

4. Se considera la permutación $p \in S_{12}$ producto de

$$p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 4 & 5 & 1 & 2 & 11 & 8 & 7 & 12 & 6 & 9 & 10 \end{pmatrix}$$

y del ciclo $p_2 = (6, 8, 5, 3, 11)$; $p = p_1 p_2$.

Descomponer p en ciclos ajenos, hallar la paridad de p y calcular p^{343} .

$p = (1, 3, 9, 12, 10, 6, 7, 8, 2, 4)$, p es impar. El orden de p es 10. El resto de dividir 343 por 10 es 3 por lo que $p^{343} = p^3 = (1, 12, 7, 4, 9, 6, 2, 3, 10, 8)$.

5. Se considera la permutación $p \in S_{12}$ producto de

$$p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 10 & 9 & 6 & 1 & 3 & 7 & 8 & 11 & 12 & 4 & 5 & 2 \end{pmatrix}$$

y del ciclo $p_2 = (12, 6, 9, 4, 10)$; $p = p_1 p_2$.

Descomponer p en ciclos ajenos, hallar la paridad de p y calcular p^{338} .

$p = (1, 10, 2, 9)(3, 6, 12, 7, 8, 11, 5)$. p es impar. El orden de p es $mcm\{4, 7\} = 28$. El resto de dividir 338 por 28 es 2 por lo que $p^{338} = p^2 = (1, 2)(3, 12, 8, 5, 6, 7, 11)(9, 10)$.