

Solución del SEGUNDO PARCIAL DE MATEMÁTICA DISCRETA II

Ejercicio 1.

- A.**
- Si $A, B \in G$, claramente las entradas de AB también son enteras. Además $\det(AB) = \det(A)\det(B) = 1 \Rightarrow AB \in G$.
 - La multiplicación de matrices es asociativa.
 - El neutro de la multiplicación de matrices, $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ tiene entradas enteras y $\det(I) = 1 \Rightarrow I \in G$. Entonces I es el neutro en G .
 - Si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$, entonces $A^{-1} = \frac{1}{\det(A)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Tenemos que las entradas de A^{-1} son enteras y $\det(A^{-1}) = \det(A) = 1$ y por lo tanto A tiene inverso en G .

Por todo lo anterior, G es un grupo.

B. $\ker \varphi = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G : \varphi \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \right) = \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix} \right\} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G : \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix} \right\} =$
 $\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G : a \equiv d \equiv 1 \pmod{n} \text{ y } b \equiv c \equiv 0 \pmod{n} \right\}.$

- C.** Primer Teorema de Isomorfismo: Si $\varphi : G \rightarrow K$ es un homomorfismo de grupos; entonces $G/\ker(\varphi) \simeq \text{Im}(\varphi)$.

Ejercicio 2. Sea G un grupo finito y H un subgrupo de G .

- A.**
- Sea $x \in G$, $x \sim x \Leftrightarrow xx^{-1} \in H \Leftrightarrow e \in H$ lo cual es cierto ya que H es subgrupo.
 - Si $x \sim y \Rightarrow xy^{-1} \in H$; como H es subgrupo tenemos que $(xy^{-1})^{-1} \in H \Rightarrow yx^{-1} \in H \Rightarrow y \sim x$.
 - Si $x \sim y$ e $y \sim z$, entonces $xy^{-1}, yz^{-1} \in H$ y como H es cerrado con la multiplicación, tenemos que $xy^{-1}yz^{-1} \in H \Rightarrow xz^{-1} \in H \Rightarrow x \sim z$.

- B.** Teorema de Lagrange: Si G es un grupo finito y H un subgrupo de G , entonces $|H||G|$. Demostración: Si C_1, \dots, C_k son las distintas clases de equivalencia dadas por la relación de equivalencia de la parte A, tenemos que $G = C_1 \cup \dots \cup C_k$, la unión disjunta. Entonces $|G| = \#C_1 + \dots + \#C_k$. Si probamos que $\#C_i = |H|$ tendremos que $|G| = \underbrace{|H| + \dots + |H|}_{k \text{ veces}} = k|H|$.

Ahora la clase de equivalencia de y es Hy ya que $x \sim y \Leftrightarrow xy^{-1} \in H \Leftrightarrow \exists h \in H : xy^{-1} = h \Leftrightarrow \exists h \in H : x = hy \Leftrightarrow x \in Hy$.

Tenemos que si $h_1, h_2 \in H$ y $h_1y = h_2y \Leftrightarrow h_1 = h_2yy^{-1} = h_2$ y por lo tanto $\#(Hy) = |H|$.

- C.** Sea $g \in G$ es tal que $\text{mcd}(o(g), |K|) = 1$. Entonces $e_K = \varphi(e_G) = \varphi(g^{o(g)}) = (\varphi(g))^{o(g)}$. Entonces $o(\varphi(g)) | o(g)$ y además $o(\varphi(g)) | |K|$, por lo tanto $o(\varphi(g)) | \text{mcd}(o(g), |K|) = 1$ entonces $o(\varphi(g)) = 1 \Rightarrow \varphi(g) = e_K \Rightarrow g \in \ker \varphi$.

Ejercicio 3.

- A. Sea $x = o(g)$ e $y = o(h)$. Como $gh = hg$ tenemos que para todo $n \in \mathbb{Z}$, $(gh)^n = g^n h^n$.

Tenemos $(gh)^{xy} = g^{xy} h^{xy} = (g^x)^y (h^y)^x = ee = e$. Falta ver que si $(gh)^n = e \Rightarrow xy|n$. Si $e = (gh)^n = g^n h^n \Rightarrow e = (g^n h^n)^x = h^{nx} \Rightarrow y|nx$ y como $\text{mcd}(x, y) = 1$ tenemos que $y|n$. Análogamente $e = (g^n h^n)^y = g^{ny} \Rightarrow x|ny \Rightarrow x|n$. Tenemos $y|n$, $x|n$ y $\text{mcd}(x, y) = 1$, entonces $xy|n$.

Otra forma:

Como $\text{mcd}(x, y) = 1$ tenemos que $\langle g \rangle \cap \langle h \rangle = \{e\}$ (Lagrange). Si $e = (gh)^n = g^n h^n \Rightarrow g^n = h^{-n} \in \langle g \rangle \cap \langle h \rangle = \{e\}$. Por lo tanto $g^n = e \Rightarrow x|n$ y $h^n = e \Rightarrow y|n$; como $\text{mcd}(x, y) = 1$ resulta que $xy|n$.

- B. Tenemos que $5^2 = 25$ y $5^3 = 125 \equiv 1 \pmod{31}$, entonces $o(5) = 3$. Como $29 \equiv -2 \pmod{31}$ y $2^2 = 4$, $2^3 = 8$, $2^4 = 16$ y $2^5 = 32 \equiv 1 \pmod{31}$, tenemos que $o(29) = 10$.

Ahora, $21 \equiv -10 \pmod{31} \equiv (-2)(5) \pmod{31}$. Por la parte anterior, como $\text{mcd}(3, 10) = 1$, tenemos que $o(21) = o((-2)(5)) = (3)(10) = 30$.

Como $\varphi(31) = 30$ y $o(21) = 30$ tenemos que 21 es raíz primitiva módulo 31

- C. La clave común es $k \equiv x^{14} \pmod{31} \equiv 7^{14} \pmod{31}$.

Ahora, $21^2 \equiv (-10)^2 \pmod{31} \equiv 7 \pmod{31}$, entonces $k = 7^{14} \equiv 21^{28} \pmod{31}$ y como $21^{30} \equiv 1 \pmod{31}$, k es el inverso de $21^2 = 7$ en $U(31)$. Entonces $k = 9$.

Ejercicio 4.

- A. (i) $\sigma_1 = (abx)$ y $\sigma_2 = (day)$. Además $a = \sigma_2 \sigma_1(b) = \sigma_2(x)$ entonces $x = d$. También $y = \sigma_2(a) = \sigma_2 \sigma_1(x) = \sigma_2 \sigma_1(d) = c$.

(ii) Como todos los elementos de A_n son producto de una cantidad par de transposiciones, basta probar que cualquier producto de 2 transposiciones está en N :

Por la parte (i), el producto de 2 transposiciones disjuntas es el producto de dos 3-ciclos σ_1, σ_2 . Como $\sigma_1, \sigma_2 \in N$ y N es subgrupo, tenemos que $\sigma_2 \sigma_1 \in N$. El producto de 2 transposiciones distintas no disjuntas es de la forma $(ab)(bc) = (abc) \in N$. Y si las transposiciones son iguales entonces $(ab)(ab) = e \in N$.

- B. Sea $\alpha = (xyz)$ un 3 ciclo; tomando $\gamma \in S_5$ tal que $\gamma(a) = x$, $\gamma(b) = y$, $\gamma(c) = z$ tenemos $\gamma \sigma \gamma^{-1} = \alpha$; como $N \triangleleft S_5$ tenemos que $\alpha \in N$. Entonces N contiene a todos los 3-ciclos y por la parte anterior tenemos $N = A_5$.

- C. (i) $(abcde)\tau = (adb) \Leftrightarrow \tau = (abcde)^{-1}(adb) = (acbed)$.

(ii) $(ab)(cd)\gamma = (abe) \Leftrightarrow \gamma = ((ab)(cd))^{-1}(abe) = (ab)(cd)(abe) = (be)(cd)$.

- D. Por las partes anteriores, basta ver que N contiene un 3-ciclo. Como $N \neq e$, existe $\sigma \in N$, $\sigma \neq e$. Si descomponemos σ en producto de ciclos disjuntos tenemos 3 posibilidades (pues σ está en A_5): σ es un 3-ciclo, un producto de dos transposiciones disjuntas o un 5-ciclo. Si σ es un 3-ciclo, ya está.

Si $\sigma = (ab)(cd)$ entonces por la parte C(ii) tenemos que $(abe) = (ab)(cd)(be)(cd) = \sigma(be)(cd)$. Basta probar que $\alpha = (be)(cd) \in N$ (y entonces $(abe) = \sigma \alpha \in N$). Si tomamos $\gamma = (abe)$, tenemos que $\alpha = (be)(cd) = \gamma(ab)(cd)\gamma^{-1} \in N$ pues $N \triangleleft S_5$.

Si σ es un 5-ciclo, entonces por la parte C.(i) tenemos que si $\sigma = (a b c d e)$ entonces $(a b c d e)\tau = (a d b)$ con $\tau = (a c b e d)$. Basta ver que $\tau \in N$. Ahora $\tau = (bc)(de)\sigma((bc)(de))^{-1} \in N$ ya que $(bc)(de) \in S_5$