

**Control 1****P1. [Morfismos y otros]**

- a) **(1.5 pts)** Sea G un grupo finito de orden $2n$, entonces existe $g \in G$, $g \neq e$ tal que $g^2 = e$. Si además G abeliano y n es impar, entonces este es único.

R: Forma 1 Si es que la proposición es falsa, entonces $\forall g \in G : g \neq g^{-1}$, Luego G tiene cardinal impar (pues tiene a todos los elementos, sus inversos y el neutro. Si es que el elemento no es único entonces hay al menos dos, luego $\{e, a, b, ab\}$ es un subgrupo, y tiene cardinal 4, lo que contradice que $|G| = 2n$, con n impar (por Lagrange).

R: Forma 2 Como $2 \mid |G|$, tenemos que existe $P \leq G$ un 2-subgrupo de Sylow de G , sabemos que $|P| = 2^m$ con $|G| = 2^m q$, con $q \notin 2\mathbb{N}$, Sea $p \in P \setminus \{e\}$, luego $|\langle p \rangle| = 2^s$, para algún $1 \leq s \leq m$, entonces $p^{\frac{|(p)|}{2}}$ tiene orden 2.

Como antes, ahora tenemos que $|P| = 2$, supongamos que $P = \{e, p\}$, sabemos que $|p| = 2$, supongamos que $q \notin P$ tiene orden 2, luego, como P es el único 2-subgrupo de Sylow, $P \trianglelefteq G$, así podemos considerar $qP \in G/P$, sabemos que $|\langle qP \rangle| = 2$, pero esto contradice Lagrange, porque $|G/P| = n \notin 2\mathbb{N}$ y $\langle qP \rangle \mid |G/P|$

- b) **(1.5 pts):** Sean $M, N \trianglelefteq G$ tales que $G = MN = NM$, demostrar que:

$$G/(M \cap N) \simeq (G/M) \times (G/N)$$

R: Forma 1 Consideremos el morfismo $\varphi : G \rightarrow (G/M) \times (G/N)$, tal que $\varphi(g) = (gM, gN)$. Como M, N son normales, es efectivamente un morfismo. Y es claro que $(gM, gN) = (M, N) \Leftrightarrow g \in M \cap N$, es decir que $\text{Ker}(\varphi) = M \cap N$. Por primer teorema de isomorfismos, basta que sea sobreyectivo para concluir. En efecto, sea (g_1N, g_2M) , como $G = MN = NM$ existen $n_1, n_2 \in N, m_1, m_2 \in M$ tales que $g_1 = m_1n_1, g_2 = n_2m_2$, luego $(g_1N, g_2M) = (m_1N, n_2M)$. Por último $\varphi(m_1n_2) = (m_1n_2N, m_1n_2M) = (m_1N, m_1n_2M)$ y como $m_1n_2(n_2)^{-1} = m_1 \in M$, se concluye que $\varphi(m_1n_2) = (m_1N, m_1n_2M) = (m_1N, n_2M) = (g_1N, g_2N)$. Es decir, es sobreyectiva.

R: Forma 2 Para ver que $G/(M \cap N)$ es un producto directo de G/M con G/N basta encontrar $A, B \trianglelefteq G/(M \cap N)$ subgrupos normales tales que $A \cap B = \{(M \cap N)\}$, $AB = G/(M \cap N)$, y además $A \simeq G/M$, $B \simeq G/N$.

Sea $A = N/(M \cap N)$, $B = M/(M \cap N)$, podemos notar que si $g(M \cap N) \in A \cap B$, entonces $g \in (M \cap N)$ luego:

$$g(M \cap N) = (M \cap N)$$

Por otro lado:

$$AB = NM/(M \cap N) = G/(M \cap N)$$

Puesto que $NM = G$.

Y finalmente $A, B \trianglelefteq G/(M \cap N)$ se obtiene de las normalidades de N y M en G , respectivamente.

Así se concluye:

$$G/(M \cap N) \simeq A \times B \simeq (G/M) \times (G/N)$$

- c) **(1.5 pts):** Sea $f : G \rightarrow H$ morfismo, con $N = \text{Ker} f$ y $K \leq G$, probar que $f^{-1}(f(K)) = KN$, luego $f^{-1}(f(K)) = K \iff N \leq K$.

R: Veamos las dos inclusiones:

$(\subseteq)$: Sea $y \in f^{-1}(f(K))$, entonces:

$$f(y) \in f(K)$$

Luego $\exists k \in K$ tal que:

$$f(y) = f(k) \implies f(k)^{-1}f(y) = e_H$$

$$\implies k^{-1}y \in N$$

Así tenemos que $\exists n \in N$ tal que:

$$k^{-1}y = n \implies y = kn \implies y \in KN$$

$(\supseteq)$: Sea $kn \in KN$, veamos que $kn \in f^{-1}(f(K))$, en efecto:

$$f(kn) = f(k)f(n) = f(k) \in f(K)$$

Esto pues $n \in N = \text{Ker} f$, y luego $f(n) = e_H$.

- d) **(1.5 pts):** Sea $f : G \rightarrow H$ morfismo, con H abeliano y $N \leq G$ con $\text{Ker} f \leq N$, entonces $N \trianglelefteq G$.

R: Sea $g \in G$, veamos que $gNg^{-1} \subseteq N$, por la parte anterior, tenemos que:

$$f^{-1}(f(gNg^{-1})) = gNg^{-1}$$

Esto ya que $\text{Ker} f \leq N$ y además $\text{Ker} f \trianglelefteq G$, entonces como f es morfismo, tenemos que:

$$f(gNg^{-1}) = f(g)f(N)f(g)^{-1}$$

Como H es abeliano, tenemos que:

$$f(gNg^{-1}) = (f(g)f(g)^{-1})f(N) = f(N)$$

Volviendo a la parte anterior, tenemos además que:

$$f^{-1}(f(N)) = N$$

Juntando lo anterior, tenemos lo que queríamos:

$$N = f^{-1}(f(N)) = f^{-1}(f(gNg^{-1})) = gNg^{-1}$$

P2. [Fórmula de clases]

- a) (1.5 pts) Sea G un grupo, demuestre que $Z(G) := \{a \in G : \forall g \in G, ag = ga\} \trianglelefteq G$ y que para $a \in G$ fijo, $c(a) := \{g \in G : ga = ag\} \leq G$.

R: En efecto, es claro que $Z(G)$ no es vacío pues tiene al neutro (conmuta con todos) y además $Z(G) \subseteq G$. Además si $x, y \in Z(G)$, se tiene que $g(xy^{-1}) = (gx)y^{-1} = (xg)y^{-1} = x(gy^{-1}) = x(y^{-1}g) = (xy^{-1})g$. Por lo tanto $Z(G)$ es subgrupo. Por último notar que $gZ(G) = Z(G)g$, pues $ga = ag, \forall z \in Z(G)$. Es decir, $Z(G) \trianglelefteq G$. Para la otra, como $ea = ae, c(a) \neq \emptyset$ y por definición $c(a) \subseteq G$. Además si $x, y \in c(a)$, se tiene que $a(xy^{-1}) = (ax)y^{-1} = (xa)y^{-1} = x(ay^{-1}) = x(y^{-1}a) = (xy^{-1})a$. Es decir, $c(a) \leq G$.

- b) (1.5 pts) En auxiliar se le presentó la relación de equivalencia de "conjugación", y las clases de equivalencia que esta genera. Esto es:

$$aCb \Leftrightarrow \exists g \in G : ag = gb \quad \text{con} \quad [a]_C = \{gag^{-1} : g \in G\}$$

Demuestre que $|[a]_C| = [G : c(a)]$.

R: Consideremos la función $\varphi : [a]_C \rightarrow G/c(a)$, tal que $\varphi(gag^{-1}) = c(a)g$. Veamos que está bien definida (y que es inyectiva).

$$g_1ag_1^{-1} = g_2ag_2^{-1} \Leftrightarrow g_1^{-1}g_2a = ag_1^{-1}g_2 \Leftrightarrow g_1^{-1}g_2 \in c(a) \Leftrightarrow g_1g_2^{-1} \in c(a) \Leftrightarrow c(a)g_1 = c(a)g_2$$

Además es sobreyectiva pues si tomamos un elemento de la forma $c(a)g$, por construcción se tiene que $\varphi(gag^{-1}) = c(a)g$.

- c) (1.5 pts) Concluya que para el caso en que G es finito, se cumple que

$$|G| = |Z(G)| + \sum_{\substack{T \in G/c \\ |T| \geq 2}} [G : c(a_T)]$$

Donde a_T es un representante fijo de la clase T .

R: Sabemos que todo conjunto cociente forma una partición, si a eso le agregamos la parte anterior se deduce que:

$$|G| = \sum_{T \in G/c} |T| = \sum_{T \in G/c} [G : c(a_T)] = \sum_{\substack{T \in G/c \\ |T|=1}} [G : c(a_T)] + \sum_{\substack{T \in G/c \\ |T| \geq 2}} [G : c(a_T)]$$

Donde a_T es un representante fijo de cada sumando T . Luego, basta ver que

$$|Z(G)| = \sum_{\substack{T \in G/c \\ |T|=1}} [G : c(a_T)].$$

Para ello notemos que

$$\begin{aligned} a \in Z(G) &\Leftrightarrow ag = ga \quad \forall g \in G \Leftrightarrow \forall g \in G, g \in c(a) \Leftrightarrow c(a) = G \\ &\Leftrightarrow G/\approx_{c(a)} = \{c(a)\} \Leftrightarrow [G : c(a)] = 1 \Leftrightarrow |[a]_c| = 1 \end{aligned}$$

Es decir cada vez que sumo uno a la derecha sumo uno a la izquierda (y viceversa) por lo que se tiene la igualdad.

- d) (1.5 pts) Demuestre que si $|G| = p^\alpha$, p primo y $\alpha \geq 1$, entonces $Z(G) \neq \{e_G\}$.

R: De la parte anterior sabemos que

$$p^\alpha = |G| = |Z(G)| + \sum_{\substack{T \in G/c \\ |T| \geq 2}} [G : c(a_T)]$$

Además, como ya probamos que $c(a_T) \leq G$, del Teorema de Lagrange sabemos que $[G : c(a_T)] \cdot |c(a_T)| = |G| = p^\alpha$. Como p es primo, $[G : c(a_T)] = p^{\beta_T}$, y como $2 \leq |T| = [G : c(a_T)]$, podemos decir que $1 \leq \beta_T$. Es decir tengo una suma de puras potencias de p , donde ninguno es 1. Se concluye que la suma entera es múltiplo de p . Luego si se pasa restando queda que $|Z(G)|$ es múltiplo de p y por lo tanto no puede ser 1.

P3. [Grupos de Sylow y Permutaciones]

- a) (1.5 pts) G es p -grupo ssi $\forall a \in G, \exists r \geq 0$ tal que $|\langle a \rangle| = p^r$.

R: La implicancia a la derecha es directa de Lagrange y de que $\forall a \in G, \langle a \rangle$ es subgrupo de G . Para la otra implicancia, si q primo divide a $|G|$, por el primer teorema de Sylow, se tiene que $\exists Q$ un q -subgrupo de Sylow, por el Teo. de Cauchy, $\exists a \in Q$, que tiene orden q . Luego por hipótesis $q = p$. Es decir el único primo que divide al cardinal de G es p .

- b) (1.5 pts) Sea G grupo, con $|G| = p^k m$, donde $\text{mcd}(p, m) = 1$, sea H un p -subgrupo de Sylow de G y $K \leq G$ con $|K| = p^d$, con $1 \leq d \leq k$, tal que $K \not\leq H$, entonces HK no es subgrupo de G .

R: Sabemos que $HK \leq G$ si y solo si $H \trianglelefteq G$ ó $K \trianglelefteq G$, sabemos que $\exists H'$ un p -subgrupo de Sylow, tal que $K \leq H'$. Notemos que $H \neq H'$, como todos los subgrupos de Sylow son conjugados, tenemos que $\exists x \in G$ tal que:

$$xHx^{-1} = H'$$

Luego $H \not\trianglelefteq G$, veamos que $K \not\trianglelefteq G$:

Sabemos también que $x^{-1}H'x = H$, luego $x^{-1}Kx \subset H$, pero como $K \not\leq H$, tenemos que $x^{-1}Kx \neq K$, entonces:

$$K \not\trianglelefteq G \implies HK \not\leq G$$

- c) (1.5 pts) Demuestre que A_4 no tiene ningún subgrupo H de orden 6. Indicación, puede ser útil mostrar que si existiese siempre, al menos un ciclo de largo 3, de no estaría en él.

R: Probemos primero la indicación, supongamos que sí existe, luego como $id \in H$, quedan solo 5 elementos desconocidos, además, sabemos que todo ciclo de largo 3, no es su propio inverso, sino que $x^{-1} = x^2$, por lo que si es que H tiene todos los ciclos de largo 3, estos son solo 4. Sin embargo esto no es real, pues $(123), (132), (124), (142), (134)$ ya son 5. Vamos a la pregunta, por Lagrange sabemos que $[A_4 : H] = 2$, y como todo subgrupo de índice 2 es normal, tiene sentido hablar del cociente. Luego, sea $x \notin H$ un ciclo de largo 3, entonces $A_4/H = \{H, xH\}$, es decir que $x^2H = H$, o bien $x^2H = xH$. Lo último no es posible pues $x^2H = xH \Leftrightarrow x^2x^{-1} = x \in H$. Por el otro lado si $x^2 \in H$, x no puede ser un ciclo de largo tres, ya que en ese caso $x^{-1} = x^2 \in H \Rightarrow x \in H$.

d) Demuestre que siempre hay más de un 5-subgrupo en A_5 . Luego explícelos todos.

R: Por Sylow 3, $n_5|60$, pero $n_5 = 1$, modulo 5. Esto solo deja como opción $n_5 = 1$ o $n_5 = 6$. Pero como A_5 es simple, se tiene que $n_5 = 6$. Basta tomar, por ejemplo,

$$\langle (12345) \rangle, \langle (13245) \rangle, \langle (14325) \rangle, \langle (15342) \rangle, \langle (12435) \rangle, \langle (12354) \rangle,$$

sabemos que todo ciclo de largo 5, está en A_5 (pues $(abcde) = (ab)(bc)(cd)(de)$), y todos son ciclos de orden 5, pero con generadores independientes, por lo que son distintos.

Tiempo: 3:00 hrs.

Muchas suerte! :D