Elementos de Algebra MA3101
Profesor: Ángel Pardo J.
Auxiliares: Alonso Cancino T.
Juan Pedro Ross O.
Fecha: Viernes 16 de Agosto 2019

Trabajo dirigido, Control 1

P1. Sea p primo y $m \in \mathbb{N}$.

a) Mostrar que $\prod_{i=1}^{m} C_p \ncong C_{p^m}$.
R: El de la derecha tiene un elemento de orden p^m, y el de la izquierda no.

b) Usando lo anterior proponga cuales los grupos abelianos de orden p^m y luego demuestre por inducción que efectivamente no hay más.
R: Lo anterior indica que $C_p \times C_p \times .... \times C_p$(p factores) $\ncong C_{p^2} \times C_p \times ... \times C_p$ (p-1 factores). Esto dice que los $\prod_{i=1}^{k} C_{p^{m_i}}$, con $\sum_{i=1}^{k} m_i = m$, son grupos abelianos de orden p^m no isomorfos. Veamos por inducción que son los únicos. Primero, recordar que como H es abeliano, todo subgrupo es normal. Segundo, sea G con cardinal p^{m+1}, por Sylow 1, existe subgrupo de orden p^m, llamémoslo H, luego $|G/\langle H\rangle| = p$. Como este es un grupo de orden primo, es cíclico, sea su generador g_jH. Si es que $\langle g_j\rangle \cap H = \{e\}$, Entonces $G = \langle g_j\rangle \times H$ y por hipótesis inductiva se concluye. Si es que no, sea $h \in H \cap \langle g_j\rangle$, luego $\langle g_j\rangle = \langle h\rangle \Rightarrow \langle g_j\rangle \leq H \Rightarrow g_jH = H \Rightarrow G/H = \{H\} \Rightarrow G = H$, lo que contradice su cardinal.

c) Clasificar todos los grupos abelianos finitos.
R: Por el teorema de Lagrange sabemos que si $|A| = p^k$ y $|B| = q^j$, con p, q coprimos $A \cap B = \{e\}$, por ende todo grupo abeliano lo podemos escribir como producto de grupos cuyo cardinal son la potencia de cada primo que divide a su cardinal (Existen por Sylow 1). Luego si aplicamos la parte anterior cada uno de esos grupos lo escribimos como productos de cíclicos, y por ende concluimos que G se escribe como producto de cíclicos cuyos cardinales multipliquen el de G.

P2. a) Sea G un grupo finito y p primo que divide a $|G|$. Entonces para todo p-subgrupo S de G, se cumple que $S \in S_p(G)$ si y solo si p no divide a $[G : S]$
R: Recordar que $[G : S]|S| = |G|$. Sea $\prod q_i^{\alpha_i}$ la factorización prima de $[G : S]$, $\prod p_i^{\beta_i}$ la de $|S|$ y $\prod r_i^{\gamma_i}$ la de G. Luego si $\exists i : r_i = p$, entonces $p \neq q_i \forall i \Leftrightarrow \exists p_i : p = p_i \wedge \beta_i = \gamma_i$

b) Demuestre que si p, q son primos distintos y $|G| = pq^2$, entonces G no es simple.
R: Por Sylow, existe subgrupo de tamaño p y de tamaño q^2. Por Sylow 3, $n_p \in \{1, q, q^2\}$ y $n_q \in \{1, p\}$, luego si n_p o n_q es 1 se concluye que ese grupo es normal y por lo tanto G no es simple. Supongamos que $n_p = q$ y $n_q = p$, también por Sylow 3, sabemos que $n_p - 1 = q - 1 = k_1 p$ y $n_q - 1 = p - 1 = k_2 q$, por ende $q - 1 = k_1(k_2 q + 1) = k_1 k_2 q + k_1 k_2 \Rightarrow q(1 - k_1 k_2) = 1 + k_1 k_2$, lo que es una contradicción porque un lado es negativo (o nulo) y el otro es positivo. Por último si $n_p = q^2$ y $n_q = p$, notemos que cada $p - subgrupo$, tiene cardinal p, por ende son cíclicos y por ende no se intersectan más que en el neutro, así con estos se cubren $(p - 1)q^2 = pq^2 - q^2$ elementos. Así los q^2 elementos faltantes deben estar en los $q-$subgrupos, pero cada uno de estos tiene esa cantidad de elementos, así solo puede haber un $q-$subgrupo, lo que contradice que $n_q = p$.

P3. a) Sean G y H dos grupos tales que $|G| = n, |H| = m$, con $mcd(n, m) = 1$. Muestre que el único morfismo entre G y H es el trivial.
R: Por teorema de isomorfismo, sabemos que para todo morfismo $|Ker(\varphi)||Im(\varphi)| = |G| = n$ y por Lagrange existe un entero tal que, $k|Im(\varphi)| = |H| = m$. Así $|Im(\varphi)|$ divide a m y n, y por hipótesis debe ser 1. Que concluye lo pedido.

b) Demuestre que si un automorfismo fija más de la mitad de los elementos de un grupo, entonces es la identidad.
R Considere el conjunto $\{a \in G : \varphi(a) = a\}$, no es dificil notar que este es un subgrupo de G, por ende su cardinal lo debe dividir, pero es mayor a la mitad, por ende la única posibilidad es que tengan cardinales iguales y por lo tanto son el mismo conjunto.

c) Sean $H, N \trianglelefteq G$ con $N \leq H$, entonces $G/H \cong (G/N)/(H/N)$.
R: En efecto, por hipótesis G/H y G/N están bien definidos como grupos, luego si consideramos el morfismo $\varphi : G/N \to G/H$ tal que $\varphi(Na) = Ha$, por primer teorema de isomorfismo se concluye lo pedido. Veamos que está bien definido, $Na = Nb \Leftrightarrow ab^{-1} \in N \subseteq H \Rightarrow ab^{-1} \in H \Leftrightarrow Ha = Hb$. Además efectivamente es morfismo: $\varphi(NaNb) = \varphi(Nab) = Hab = HaHb = \varphi(Na)\varphi(Nb)$, y claramente es sobreyectivo. Con esto $(G/N)/Ker(\varphi) \cong Im(\varphi) = G/H$. Por último, $Na \in Ker(\varphi) \Leftrightarrow \varphi(Na) = Ha = H \Leftrightarrow a \in H$, es decir $Ker(\varphi) = \{Na : a \in H\} = H/N$.

P4. a) Sean $A \leq B \leq C$, con $[C : A] = p$, con p primo, entonces $A = B \vee B = C$.
R: Por el teorema de lagrange sabemos que

$$[C : B]|B| = |C| \quad \wedge \quad [C : A]|A| = |C| \quad \wedge \quad [B : A]|A| = |B|$$

Igualando las dos primeras y reemplazando $|B|$, se deduce que

$$[C : B][B : A]|A| = [C : A]|A| \Rightarrow [C : B][B : A] = [C : A] = p.$$

Luego como p es primo se tiene que alguno de los factores es 1 y el otro es p, si a eso le agregamos que $[X : Y] = 1 \Leftrightarrow X = Y$, se concluye.

b) Sea G un grupo, probar que:

$$G \text{ es abeliano} \iff \text{La función dada por } \psi(g) = g^{-1} \text{ es un automorfismo.}$$

R: ($\Longrightarrow$) Si G es abeliano, como es grupo ya tenemos que ψ es biyectiva, entonces solo basta ver que es morfismo, en efecto:

$$\psi(gh) = (gh)^{-1} = h^{-1}g^{-1} = g^{-1}h^{-1} = \psi(g)\psi(h)$$

($\Longleftarrow$) Si ψ es un automorfismo, entonces sean $g, h \in G$, consideremos:

$$\psi(g^{-1}h^{-1}) = (g^{-1}h^{-1})^{-1} = hg$$

Por otro lado, como ψ es morfismo:

$$\psi(g^{-1}h^{-1}) = \psi(g^{-1})\psi(h^{-1}) = gh$$

Juntando las dos anteriores $hg = gh$, y como $g, h \in G$ eran arbitrarios, se concluye.

c) Sea G grupo, probar que si G tiene un numero finito de subgrupos, entonces G es finito.
R: Si no fuese finito, y tuviese un numero finito de subgrupos entonces hay algun elemento $g \in G$ tal que $\langle g \rangle$ es infinito, luego $\langle g \rangle \simeq \mathbb{Z}$, y luego $\langle g^k \rangle \leq \langle g \rangle \leq G$, $\forall k \in \mathbb{N}$ es un subgrupo no trivial, luego la cantidad de subgrupos no era finita.

P5. Demuestre que A_4 tiene un subgrupo isomorfo a $C_2 \times C_2$
R: Con método exploratorio deducimos que $\{id, (12)(34), (13)(24), (14)(23)\}$, es el que cumple lo pedido, de todas formas podíamos intuir que se trataba de este pues como en $C_2 \times C_2$ cada elemento es su propio inverso, se debía tener que trabajar con trasposiciones. Luego como se necesitan "dos coordenas" resulta natural, pensar en multiplicación de trasposiciones disjuntas. (pues si no fuesen disjuntas, habría una "dependencia" entre ellas). En efecto, si comparamos las tablas de ambos grupos vemos que son isomorfas.

$\circ$	id	(12)(34)	(13)(24)	(14)(32)
id	id	(12)(34)	(13)(24)	(14)(32)
(12)(34)	(12)(34)	id	(14)(23)	(13)(24)
(13)(24)	(13)(24)	(14)(23)	id	(12)(34)
(14)(32)	(14)(32)	(13)(24)	(12)(34)	id

+	(0,0)	(1,0)	(0,1)	(1,1)
(0,0)	(0,0)	(1,0)	(0,1)	(1,1)
(1,0)	(1,0)	(0,0)	(1,1)	(0,1)
(0,1)	(0,1)	(1,1)	(0,0)	(1,0)
(1,1)	(1,1)	(0,1)	(1,0)	(0,0)