| | |
|---|---|
| **Ma31a Elementos de Álgebra** | **12 de Septiembre de 2008** |

# Pauta Control 1

*Prof. Cátedra: M. Kiwi* — *Prof. Auxiliar: E. Araya, O. Rivera*

PROBLEMA 1:

(i).- Recordar que $\langle A\rangle_N = \bigcap_{H\triangleleft G: A\subseteq H} H$. Definimos el conjunto

$$W \quad = \quad \left\{ I_{g_1}(a_1^{m_1})\cdots I_{g_n}(a_n^{m_n}) \,:\, \begin{array}{c} n\in\mathbb{N}, m_1,\ldots,m_n\in\mathbb{Z}, \\ a_1,\ldots,a_n\in A, g_1,\ldots,g_n\in G \end{array} \right\}.$$

Queremos demostrar que $\langle A\rangle_N = W$.

Veamos primero que $\langle A\rangle_N \subseteq W$. Bastará demostrar que $W$ es un subgrupo normal de $G$ que contiene a $A$. Por convención tenemos que el neutro de $G$ pertenece a $W$. Además, si $w$ y $\widetilde{w}$ son elementos de $W$, entonces existen $n,\widetilde{n}\in\mathbb{N}$, enteros $m_1,\ldots,m_n,\widetilde{m}_1,\ldots,\widetilde{m}_{\widetilde{n}}$, elementos de $a_1,\ldots,a_n,\widetilde{a}_1,\ldots,\widetilde{a}_{\widetilde{n}}\in A$, y $g_1,\ldots,g_n,\widetilde{g}_1,\ldots,\widetilde{g}_{\widetilde{n}}\in G$ tales que $w = I_{g_1}(a_1^{m_1})\cdots I_{g_n}(a_n^{m_n})$, y $\widetilde{w} = I_{\widetilde{g}_1}(\widetilde{a}_1^{\widetilde{m}_1})\cdots I_{\widetilde{g}_{\widetilde{n}}}(a_{\widetilde{n}}^{\widetilde{m}_{\widetilde{n}}})$. Luego,

$$w\cdot(\widetilde{w})^{-1} \quad = \quad I_{g_1}(a_1^{m_1})\cdots I_{g_n}(a_n^{m_n})\cdot I_{\widetilde{g}_{\widetilde{n}}}(\widetilde{a}_{\widetilde{n}}^{-\widetilde{m}_{\widetilde{n}}})\cdots I_{\widetilde{g}_1}(a_1^{-\widetilde{m}_1}).$$

Sigue que $w(\widetilde{w})^{-1}\in W$. Por resultados de caracterización de subgrupos se concluye que $W$ es un subgrupo de $G$. Notar además que $W$ es subgrupo normal de $G$. En efecto, por propiedades de automorfismos interiores, para todo $g\in G$,

$$I_g\left(I_{g_1}(a_1^{m_1})\cdots I_{g_n}(a_n^{m_n})\right) \quad = \quad I_{g\cdot g_1}(a_1^{m_1})\cdots I_{g\cdot g_n}(a_n^{m_n}) \;\in\; W.$$

En otras palabras, $W$ es invariante bajo conjugación por automorfismos interiores. Sigue que $W$ es subgrupo normal de $G$. Finalmente, como $I_1(a) = a$ cualquiera que sea $a\in A$, sigue que $A\subseteq W$.

Veamos ahora que $W\subseteq\langle A\rangle_N$. Sea $w\in W$ tal que para $n\in\mathbb{N}$, enteros $m_1,\ldots,m_n,$, elementos de $a_1,\ldots,a_n,\in A$, y $g_1,\ldots,g_n,\in G$ se tiene que $w = I_{g_1}(a_1^{m_1})\cdots I_{g_n}(a_n^{m_n})$.

Si para cualquier $H$ subgrupo normal de $G$ tal que $A\subseteq H$ se tiene que $w\in H$, entonces $w\in\langle A\rangle_N$. Veamos que efectivamente $w\in H$ para un $H$ con las propiedades señaladas. En efecto, como $a_1,\ldots,a_n\in A$ y $H$ es un grupo que contiene a $A$, sique que $a_1^{m_1},\ldots,a_n^{m_n}\in H$. Como $H$ es subgrupo normal de $G$ y un grupo normal es cerrado bajo conjugación, sigue que si $g_1,\ldots,g_n\in G$, entonces $I_{g_1}(a_1^{m_1}),\ldots,I_{g_n}(a_n^{m_n})\in H$. Nuevamente, dado que $H$ es grupo, se concluye que $w = I_{g_1}(a_1^{m_1})\cdots I_{g_n}(a_n^{m_n})\in H$.

(ii).- Consideremos $\nu: G\to G/H\times G/K$ tal que $\nu(g) = (\nu_H(g),\nu_K(g))$, donde $\nu_H$ y $\nu_K$ denotan los epimorfismos canónicos de $G$ en $G/H$ y $G/K$ respectivamente. Se verifica fácilmente que $\nu$ es morfirmo. Además, si $\nu(g) = ([1]_H,[1]_K)$, entonces $g\in H\cap K = \{1\}$. Sigue que $\nu$ es un monomorfimo. Por el Teorema del Factor, concluimos que $G\approx \mathrm{Im}(\nu)$ con $\mathrm{Im}(\nu)$ subgrupo de $G/H\times G/K$.

(iii).- Consideremos las acción de $I: G\times G\to G$ tal que $I(g,x) = I_g(x)$ donde $I_g(x) = gxg^{-1}$. Sigue que $G$ se particiona en órbitas. Como $\mathrm{Orb}(x) = \{x' \,:\, gx = x'g\}$ sigue que $|\mathrm{Orb}x| = 1$ si y solo si $x\in Z(G)$. La condición

$Z(x_\lambda) \subsetneq G$ para todo $\lambda \in \Lambda$ y si $\lambda, \lambda' \in \Lambda$, $\lambda \neq \lambda'$, y $g \in G$, entonces $x_{\lambda'} \neq g x_\lambda g^{-1}$, equivale a decir que los $x_\lambda$'s son representantes de cada una de las órbitas de cardinal estrictamente mayor que 1. Luego,

$$|G| = |Z(G)| + \sum_{\lambda \in \Lambda} |\mathrm{Orb}(x_\lambda)|.$$

Por resultado visto, $\mathrm{Orb}(x_\lambda) \approx G/\mathrm{Est}(x_\lambda)$ como $G$-espacios. Además, como $\mathrm{Est}(x) = \{g \in G : gx = xg\} = Z(x)$, sigue que $|\mathrm{Orb}(x_\lambda)| = |G|/|Z(x_\lambda)| = [G : Z(x_\lambda)]$.

PROBLEMA 2: Sea $G$ un grupo de orden 28. Como $28 = 2^2 \cdot 7$ sigue que $G$ posee un 2-subgrupo de Sylow de orden 4 que denotaremos $P_2$, y un 7-subgrupo de Sylow de orden 7 que denotaremos $P_7$. Sean $N_2$ y $N_7$ el número de conjugados de $P_2$ y $P_7$ respectivamente.

De los Teoremas de Sylow tenemos que $N_7 \equiv_7 1$ y $N_7 | 4$. Sigue que $N_7 = 1$ y por lo tanto $P_7$ es invariante bajo conjugación, i.e. $P_7 \lhd G$. Además, como $P_7$ es de orden primo, se tiene que $P_7$ es isomorfo a $\mathbb{Z}_7$.

Por otro lado, también se cumple que $N_2 \equiv_2 1$ y que $N_2 | 7$. Sigue que $N_2$ puede ser igual a 1 o 7. Además, como $P_2$ tiene orden el cuadrado de un primo, debe ser abeliano. Se tienen los siguientes dos casos:

- $P_2$ tiene un elemento de orden 4: Entonces es isomorfo a $\mathbb{Z}_4$.
- $P_2$ no tiene elementos de orden 4: Entonces, por ser 2-subgrupo, sus elementos distintos del neutro deben ser todos de orden 2. Sea $x \in P_2$ de orden 2 e $y \notin P_2 \setminus \langle x \rangle$ ($y$ existe dado que $P_2$ y $\langle x \rangle$ tienen orden 4 y 2 respectivamente). Como $P_2$ es abeliano, se verifica fácilmente que $\langle \{x, y\} \rangle = \left\{ x^i y^j : 0 \leq i, j \leq 1 \right\} = P_2$. Sigue que $P_2$ es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Como los ordenes de $P_2$ y $P_7$ son primos relativos, por Lagrange concluimos que su intersección es necesariamente trivial, i.e. $P_2 \cap P_7 = \{1\}$. Por fórmula conocida, se tiene que $|P_2 P_7| = |P_2||P_7|/|P_2 \cap P_7| = 4 \cdot 7 = 28$. Luego, necesariamente debe cumplirse que $G = P_2 P_7$.

En el caso que $P_2 \lhd G$, entonces por resultado visto en clases se concluye que $G$ es isomorfo a $P_7 \times P_2$. Sigue que en este caso $G$ es abeliano isomorfo a $\mathbb{Z}_7 \times \mathbb{Z}_4$ o $\mathbb{Z}_7 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Si $P_2$ no es normal en $G$, entonces actúa por conjugación sobre $P_7$. Consideremos entonces los siguientes dos casos:

- $\Phi : \mathbb{Z}_4 \to Aut(\mathbb{Z}_7)$ morfismo: Sea $\varphi_i = \Phi(i)$. Como $\Phi$ es morfismo, $\varphi_0 = id$ y $\varphi_1$ debe ser de orden divisor de 4. Pero el orden de $\mathbb{Z}_7^*$ es 6 que no es divisible por 4 y por lo tanto no contiene elementos de orden 4. Luego, el único caso interesante es cuando $\varphi_1$ tiene orden 2. Como $Aut(\mathbb{Z}_7)$ es isomorfo a $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$ y el único elemento de orden 2 en $\mathbb{Z}_7^*$ es $6 = -1 \bmod 7$, estudiemos el caso en que $\varphi_1 : \mathbb{Z}_7 \to \mathbb{Z}_7$ es tal que $\varphi_1(x) = -x$. Luego, en $\mathbb{Z}_7 \times_\Phi \mathbb{Z}_4$ se tiene la siguiente ley de composición interna:
$$(a, b)(a', b') \ = \ (a +_7 \varphi_b(a'), b +_4 b') \ = \ (a +_7 (-1)^b a', b +_4 b').$$
Se verifica que el grupo que se obtiene es isomorfo a $D_{14}$.
- $\Phi : \mathbb{Z}_2 \times \mathbb{Z}_2 \to Aut(\mathbb{Z}_7)$ morfismo: Usando la notación del caso anterior, ahora se observa que $\Phi(1, 0)$ y $\Phi(0, 1)$ deben ser de orden divisor de 2 y por lo tanto iguales a $id$ o $\varphi_6$. Sigue que los casos no triviales interesantes son:

- $\Phi(1,0) = id$ y $\Phi(0,1) = \varphi_6$: Observar que $\Phi(b,c) = \Phi(b,0) \circ \Phi(0,c) = \Phi(0,c)$ para todo $(b,c) \in \mathbb{Z}_2 \times \mathbb{Z}_2$. Luego, en $\mathbb{Z}_7 \times_\Phi (\mathbb{Z}_2 \times \mathbb{Z}_2)$ se tiene la siguiente ley de composición interna:

$$(a,(b,c))(a',(b',c')) \quad = \quad (a +_7 (-1)^c a', (b +_2 b', c +_2 c')) .$$

  Se verifica que el grupo que se obtiene es isomorfo a $D_7 \times \mathbb{Z}_2$.

- $\Phi(1,0) = \varphi_6$ y $\Phi(0,1) = id$: En este caso el grupo $P_7 \times_\Phi P_2$ es isomorfo al grupo del caso anterior.

- $\Phi(1,0) = \Phi(0,1) = \varphi_6$: En este caso, en $\mathbb{Z}_7 \times_\Phi (\mathbb{Z}_2 \times \mathbb{Z}_2)$ se tiene la siguiente ley de composición interna:

$$(a,(b,c))(a',(b',c')) \quad = \quad (a +_7 (-1)^{b+c} a', (b +_2 b', c +_2 c')) .$$

  Se verifica que el grupo que se obtiene es isomorfo a $D_{14}$.

PROBLEMA 3:

Primero recordamos que $A_5$ tiene orden $5!/2 = 60 = 2^2 \cdot 3 \cdot 5$. Luego, existen 2-, 3- y 5-subgrupos de Sylow en $A_5$ cuyos ordenes son $2^2$, 3 y 5 respectivamente. Sea $N_p$ el número de $p$-subgrupos de Sylow en $A_5$.

(i).- Si hubiera un único 5-subgrupo de Sylow en $A_5$, entonces este sería normal. Pero por resultado visto, $A_5$ es grupos simple, luego sus subgrupos normales son triviales.

Otra forma alternativa de abordar el problema es mostrar que existen dos subgrupos distintos de $A_5$ de orden 5. Los 5-ciclos en $S_5$ son todos pares y de orden 5 por lo tanto generan los distintos 5-subgrupos de Sylow de $A_5$. Como

$$\langle(12345)\rangle \quad = \quad \{id, (12345), (13524), (14253), (15432)\} ,$$

no contiene todos los ciclos de orden 5, entonces no existe un único 5-subgrupo de Sylow en $A_5$.

(ii).- Por los Teoremas de Sylow se tiene que $N_5 \equiv_5 1$ y $N_5 | 12$. Luego, $N_5$ es igual a 1 o 6. Por (i) sabemos entonces que $N_5 = 6$. Veamos que todos ellos son generados por ciclos de orden 5 (bastará exhibir 6 de estos grupos):

$$\begin{aligned}
\langle(12345)\rangle &= \{id, (12345), (13524), (14253), (15432)\} ,\\
\langle(13452)\rangle &= \{id, (13452), (14235), (15324), (12543)\} ,\\
\langle(14532)\rangle &= \{id, (14532), (15243), (13425), (12354)\} ,\\
\langle(15423)\rangle &= \{id, (15423), (14352), (12534), (13245)\} ,\\
\langle(15234)\rangle &= \{id, (15234), (12453), (13542), (14325)\} ,\\
\langle(14523)\rangle &= \{id, (14523), (15342), (12435), (13254)\} .
\end{aligned}$$

(iii).- El orden de un producto de cíclos disjuntos es el mínimo común múltiplo del largo de sus cíclos. Sigue que la única forma en que una permutación de $S_5$ puede tener orden 4 es que sea un ciclo de largo 4. Pero un ciclo de largo par es una permutación de signo impar, luego no está en $A_5$. Como los únicos grupos de orden 4 son $\mathbb{Z}_4$ y $\mathbb{Z}_2 \times \mathbb{Z}_2$, y el primero de estos posee elementos de orden 4, sigue que los 2-subgrupos de Sylow de $A_5$ son todos isomorfos a $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(iv).- Los 2-subgrupos de Sylow de $A_5$ tiene orden 4, luego contienen elementos cuyo orden es divisor de 4. Por (iii) sabemos que no existen elementos de orden 4 en $A_5$, luego los elementos no-triviales de un 2-subgrupo de Sylow de $A_5$ deben ser productos de trasposiciones disjuntas. Por paridad, una permutación en $A_5$ distinta de la identidad que se descompone en producto de trasposiciones disjuntas debe tener exactamente dos de tales cíclos. Por (iii) tenemos que los 2-subgrupos de Sylow de $A_5$ son abelianos. En resumen, los 2-subgrupos de Sylow de $A_5$ tienen 4 elementos, uno de ellos es la identidad y los otros 3 son productos de dos trasposiciones disjuntas. Más aún los 3 elementos distintos a la identidad conmutan entre si. Por indicación sigue que todo 2-subrupo de Sylow de $A_5$ tiene la forma

$$\{id, (ij)(kl), (ik)(jl), (il)(jk)\},$$

donde $i, j, k, l \in \{1, \ldots, 5\}$ son todos distintos. Los 5 casos posibles son:

$$\begin{gathered}
\{id, (12)(34), (13)(24), (14)(23)\}, \\
\{id, (12)(35), (13)(25), (15)(23)\}, \\
\{id, (12)(45), (14)(25), (15)(24)\}, \\
\{id, (13)(45), (14)(35), (15)(34)\}, \\
\{id, (23)(45), (24)(35), (25)(34)\}.
\end{gathered}$$