Ma31a Elementos de Álgebra	**27 de Agosto, 2005**

Pauta Control 1

Prof. Cátedra: M. Kiwi — *Prof. Auxiliar: H. Castro, J. Soto*

PROBLEMA 1:

(i).- Como $K \lhd G$ y K es subgrupo de $H \subseteq G$, se tiene trivialmente que $K \lhd H$.

Sea ahora $g \in G$ y $h \in H$. Dado que $H \lhd G$, sigue que para algún $h' \in H$ se tiene que

$$[g]_K \cdot [h]_K = [g \cdot h]_K = [h' \cdot g]_K = [h']_K \cdot [g]_K \,.$$

En otras palabras, $H/K \lhd G/K$.

(ii).- Sea ν el epimorfismo canónico de G en G/K y sea μ el epimorfismo canónico de G/K en $(G/K)/(H/K)$. Como la composición de epimorfismos es epimorfismo, se tiene que $\mu \circ \nu$ es también un epimorfismo. Luego, por teorema del factor, $G/\mathbb{K}er\,(\mu \circ \nu) \cong (G/K)/(H/K)$. Pero,

$$\mathbb{K}er\,(\mu \circ \nu) = \nu^{-1}\left(\mathbb{K}er\,(\mu)\right) = \nu^{-1}\left(H/K\right) = H \,.$$

PROBLEMA 2:

(i.1).- Como p no es divisor de $ord\,(N)$ pero si de $ord\,(G)$, se tiene que p divide a $ord\,(G/N) = ord\,(G)\,/ord\,(N)$, digamos $ord\,(G/N) = tp$. Si G/N posee sólo subgrupos triviales, entonces es cíclico y tiene un generador $[h]_N$. Es fácil verificar que $Nh^t = [h^t]_N$ tiene orden p en G/N. Si $ord\,(G/N)$ posee subgrupos no triviales cuyo orden no es divisible por p, por hipótesis de inducción, sigue que existe $Nb = [b]_N \in G/N$ de orden p. Queda el caso en que G/N posee subgrupos no triviales, pero todos ellos tienen un orden múltiplo de p. Necesariamente debe existir $[h]_N \in G/N$ tal que $[h]_N \neq [1]_N$. Sigue que $\langle [h]_N \rangle$ tiene orden múltiplo de p, digamos sp. Equivalentemente, $[h]_N$ tiene orden sp. Es fácil verificar que $Nh^s = [h^s]_N \in G/N$ es de orden p.

(i.2).- Primero observemos que $N = [1]_N = [b]_N^p = [b^p]_N$ implica que $b^p \in N$. Luego, del Teorema de Euler se tiene que $c^p = b^{p \cdot ord(N)} = (b^p)^{ord(N)} = 1$. Sigue que el orden de c divide a p, i.e., $ord\,(c)$ es igual a 1 o p. Para concluir sólo nos basta mostrar que $ord\,(c) \neq 1$, ó lo que es equivalente, que $c \neq 1$. En efecto, si $c = 1$, entonces $b^{ord(N)} = 1$. Luego el orden de b divide el orden de N. Tendríamos entonces que p divide a N, una contradicción.

(i.3).- Supongamos que G sólo posee subgrupos triviales. Como $p > 1$ y p divide el orden de G, se tiene que existe $g \in G$, $g \neq 1$. Necesariamente deberá tenerse que $G = \langle g \rangle$ y que $g^{ord(G)} = 1$. Luego, para $h = g^{ord(G)/p}$, se tiene que $h^i \neq 1$ para todo $i \in \{1, \ldots, p{-}1\}$, y $h^p = 1$, i.e., h es de orden p.

Supongamos ahora que G posee subgrupos no triviales y todos dichos subgrupos tienen un orden divisible por p. Dichos subgrupos son grupos abelianos finitos de orden múltiplo de p de tamaño estrictamente menor al de G. Luego, por hipótesis inductiva contienen un elemento de orden p.

Nos queda considerar el caso en que G posee algún subgrupo N no trivial, de orden no divisible por p. De (i.1) e (i.2) se tiene que G tendrá un elemento de orden p.

(ii.1).- La fórmula de las clases garantiza que

$$ord\,(G) = ord\,(Z(G)) + \sum_{\lambda \in \Lambda} \frac{ord\,(G)}{ord\,(Z(x_\lambda))}\,. \tag{1}$$

Si $ord\,(Z(x_\lambda))$ no es divisible por p y dado que $ord\,(G)$ si lo es, se tiene que $ord\,(G)\,/ord\,(Z(x_\lambda))$ debe ser divisible por p. Luego, si $ord\,(Z(x_\lambda))$ no es divisible por p para todo $\lambda \in \Lambda$, se tendrá que tanto el lado izquierdo de la igualdad como cada uno de los términos de la sumatoria en (1) es divisible por p. Se debe tener entonces que $ord\,(Z(G))$ también es divisible por p.

(ii.2).- El resultado es claramente cierto si $ord\,(G) = 2$, pues en dicho caso $G \cong \mathbb{Z}_2$ y $1 \in \mathbb{Z}_2$ es de orden 2. Supongamos entonces que el resultado es cierto para grupos de orden $n-1$ y sea G tal que $ord\,(G) = n$. Si $Z(G) = G$, entonces G es grupo abeliano y el resultado sigue de la conclusión obtenida en (i.3). Supongamos entonces que $Z(G)$ esta estrictamente contenido en G, se tiene necesariamente que el conjunto de clases de conjugación es no vac'io, i.e., $\Lambda \neq \emptyset$. Como el representante x_λ de cada clase de conjugación no pertenece al centro de G, sabemos que $Z(x_\lambda)$ esta estrictamente contenido en G. Luego, o existe algún $Z(x_{\lambda^*})$ estrictamente contenido en G y de orden divisible por p, o $Z(G)$ está estrictamente contenido en G y tiene un orden divisible por p. Cualquiera sea el caso, la hipótesis de inducción garantiza la existencia de un elemento g (en $Z(x_{\lambda^*})$ o $Z(G)$ dependiendo de cual sea el caso) de orden p.

(iii).- Por (ii.2) tenemos que existen elementos a y b en G de orden 2 y 3 respectivamente. Claramente $\langle b \rangle = \{1, b, b^2\}$.

Como $\langle a\rangle$ y $\langle b\rangle$ son grupos de órdenes primos relativos entre si, su intersección es el grupo trivial $\{1\}$. Luego, si $a^ib^j = a^{i'}b^{j'}$ con $0 \leq i, i' < 2$ y $0 \leq j, j' < 3$, sigue que $a^{i-i'} = b^{j'-j} \in \langle a\rangle \cap \langle b\rangle = \{1\}$, de donde $i = i'$ y $j = j'$. Se tiene entonces que $G = \{a^ib^j \,:\, 0 \leq i < 2, 0 \leq j < 3\}$.

Como los conjugados de $\langle b\rangle$ son un grupo de orden 3, se tiene por unicidad, que todo conjugado de $\langle b\rangle$ es igual a $\langle b\rangle$. En particular, $a\langle b\rangle a^{-1} = \langle b\rangle$.

Si $aba^{-1} = 1$, entonces $b = 1$, contradiciendo el hecho que b es de orden 3.

Si $aba^{-1} = b$, entonces $ab = ba$, i.e., a y b conmutan. Pero dado que a y b conmutan, se tendría que G sería abeliano, contradiciendo la hipótesis del enunciado.

Se debe tener entonces que $aba^{-1} = b^2$ es decir, $ab = b^2a$. Esto nos permite construir la tabla de multiplicación de G,

	1	a	b	b^2	ab	ab^2
1	1	a	b	b^2	ab	ab^2
a	a	1	ab	ab^2	b	b^2
b	b	ab^2	b^2	1	a	ab
b^2	b^2	ab	1	b	ab^2	a
ab	ab	b^2	ab^2	a	1	b
ab^2	ab^2	b	a	ab	b^2	1

Identificando 1, b, b^2, a, ab, ab^2 con

$$id\,, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

respectivamente, se verifica que $G \cong S_3$.