Ma3101 Elementos de Álgebra **30 de Abril de 2011**

Pauta Control 1

Prof. Cátedra: M. Kiwi *Prof. Auxiliar: O. Rivera, D. Salas*

PROBLEMA 1:

(i).- Si $[G:H]=p$, entonces $\{gH : g \in G\}$ es un partición de G de cardinal p. Luego, existen $g_1,\ldots,g_p \in G$ tales que $\{gH : g \in G\} \subseteq \{g_1H,\ldots,g_pH\}$. Como los g_iH's son disjuntos y $gg_iH \in \{gH : g \in G\}$, sigue que existe un único $j \in [p]$ tal que $gg_iH = g_jH$, luego π_H está bien definida.

Veamos ahora que π_H es inyectiva. En efecto, si $\pi_H(i)=\pi_H(i')$, entonces $gg_iH = gg_{i'}H$. Como g es invertible, se concluye que $g_iH = g_{i'}H$. Dado que $\{g_1H,\ldots,g_pH\}$ es partición de G, debe tenerse que $i=i'$. Como el dominio y recorrdido de π_g tienen el mismo cardinal y que π_g es inyectiva, se tiene que π_g es biyección y por lo tanto está en S_p.

(ii).- Sean $g,g' \in G$. Sea $\pi_{g'}(i)=j$ y $\pi_g(j)=k$, i.e. $g'g_iH = g_jH$ y $gg_jH = g_kH$. Luego, $gg'g_iH = gg_jH = g_kH$. Se tiene entonces que $\pi_{gg'}(i)=k=\pi_g\circ\pi_{g'}(i)$ para todo $i\in[p]$, o equivalentement $\pi_{gg'}=\pi_g\circ\pi_{g'}$. En otras palabras, π_H es un morfismo de grupos. Por Teorema del Factor, se tiene que G/K es isomorfo a un subgrupo de S_p (específicamente a $\pi_H(G)\subseteq S_p$).

(iii).- Sea $k=[H:K]$. Por la fórmula de los índices, $|G/K|=[G:K]=[G:H]\cdot[H:K]=pk$. Como G/K es isomorfo a un subgrupo de S_p, por Lagrange se tiene que $|G/K|=pk$ divide a $|S_p|=p!$. Luego, k divide a $(p-1)!$. Observar además que $pk=|G/K|=|G|/|K|$ es un divisor de $|G|$. Por minimalidad de p, sigue que k no es divisible por ningún entero entre 1 y $p-1$. Si k divide a $(p-1)!$ y no tiene divisores entre 2 y $p-1$, entonces no queda otra que $k=1$. Hemos probado que $[H:K]=1$. Sigue que H es igual al kernel de un morfismo sobre G (específicamente π_H), luego debe ser normal en G.

PROBLEMA 2:

(i).- Sea N_q el número de conjugados de Q en G. Por el Segundo Teorema de Sylow, se tiene que $N_q \equiv_q 1$, N_q divide a $|G|$, y que $N_q \leq |G|/q = p$. Las dos últimas condiciones implican que N_q debe ser 1 o p. Como $p<q$, sigue que p no es congruente a 1 módulo q. La única posibilidad que queda es que $N_q=1$. Sigue que Q es normal en G.[1]

Como P y Q son grupos de orden p y q primos distintos, por Lagrange se tiene que $P\cap Q=\{1\}$. Por resultado visto, $|PQ|=|P||Q|/|P\cap Q|$. Luego $|PQ|=pq=|G|$, de donde se concluye que $G=PQ$.

En resumen, $G=PQ$, $P\cap Q=\{1\}$, y $Q\lhd G$. Por resultado visto se tiene que G es isomorfo a un producto semidirecto de Q y P como se pedía demostrar.

(ii).- De la parte anterior se tiene que $G\cong \mathbb{Z}_q \times_\phi \mathbb{Z}_p$ para algún morfismo $\phi:\mathbb{Z}_p \to Aut(\mathbb{Z}_q)$. Sea $\phi_1=\phi(1)\in Aut(\mathbb{Z}_q)$. Como $\mathbb{Z}_p$ es generado por 1 sigue que $id_{\mathbb{Z}_q}=\phi(0)=(\phi(1))^p=\phi_1^p$. Luego, $(\phi_1(1))^p=1$. Recordando que $Aut(\mathbb{Z}_q)\cong\mathbb{Z}_q^*$ via el isomorfismo que a $\varphi\in Aut(\mathbb{Z}_q)$ le asocia $\varphi(1)\in\mathbb{Z}_q^*$, sigue que $\phi_1(1)$

[1] A partir del Problema 1 también se puede concluir que Q es normal en G.

es un elemento de orden 1 o p en $\mathbb{Z}_q^*$. Pero $\mathbb{Z}_q^*$ tiene orden $q-1$, luego si $\phi_1(1)$ tuviese orden p se tendría que p divide a $q-1$, contradicción. Sigue que $\phi_1(1)$ tiene orden 1, o sea $\phi_1(1)=1$ y por lo tanto $\phi_1 = id_{\mathbb{Z}_q}$. Nuevamente dado que ϕ es morfismo, sigue que $\phi(a) = (\phi(1))^a = id_{\mathbb{Z}_q}$ para todo $a \in \mathbb{Z}_p$. Por resultado visto, $\mathbb{Z}_p \times_\phi \mathbb{Z}_q \cong \mathbb{Z}_p \times \mathbb{Z}_q$. En resumen, $G \cong \mathbb{Z}_p \times \mathbb{Z}_q$.

Afirmamos que $(1,1)$ genera $\mathbb{Z}_p \times \mathbb{Z}_q$. En efecto, sumando $(1,1)$ consigo mismo k veces, se obtiene (k mód p, k mód q), que es igual a $(0,0)$ si y solo si k es divisible por pq. Luego, $(1,1)$ es de orden pq en $\mathbb{Z}_p \times \mathbb{Z}_q$, lo que prueba la afirmación. Sigue que $G \cong \mathbb{Z}_p \times \mathbb{Z}_q$ es cíclico.

(iii).- Sea $\phi(b) = \phi_b \in Aut(\mathbb{Z}_q)$ donde $b \in \mathbb{Z}_p$. Como $\mathbb{Z}_p$ está generado por 1 y ϕ es morfismo, tenemos que $\phi(b) = (\phi(1))^b = \phi_1^b$. Por un argumento similar al de la parte (ii), se tiene que $\phi_1(1)$ tiene orden 1 o p. Si $\phi_1(1) = 1$, entonces por lo demostrado en la parte (ii), se tendría que ϕ sería trivial. Asumimos entonces que $\phi_1(1)$ tiene orden p (en particular es distinto 1). Claramente, $\phi_1(a) = \phi_1(1)a$ para todo $a \in \mathbb{Z}_q$, y como ϕ_1 es automorfismo sobre $\mathbb{Z}_q$, tenemos que $\phi_1(1) \in \mathbb{Z}_q^*$.

Por la afirmación del enunciado, $\mathbb{Z}_q^*$ tiene un único subgrupo de orden p, digamos $\langle\gamma\rangle$. Como $\phi_1(1)$ genera un subgrupo de $\mathbb{Z}_q^*$ de orden p, sigue que $\phi_1(1) \in \langle\gamma\rangle$, y como $\phi_1(1) \neq 1$, tenemos que $\phi_1(1) = \gamma^i$ para algún $1 \leq i \leq p-1$. Más aún, $\phi_b(a) = \phi_1^b(a) = \gamma^{ib}a$. Luego, la ley de composición interna en $\mathbb{Z}_p \times_\phi \mathbb{Z}_q$ queda:

$$(a,b) +_\phi (a',b') \;=\; (a +_q \phi_b(a'), b+b') \;=\; (a +_q \gamma^{ib}a', b +_p b').$$

(iii.1).- Basta observar que $(0,1) +_\phi (1,0) = (\gamma^i, 1)$ y que $(1,0) +_\phi (0,1) = (1,1)$. Como $\gamma^i \neq 1$, pues de lo contrario γ no sería de orden p, se tiene que $\mathbb{Z}_p \times_\phi \mathbb{Z}_q$ es no abeliano.

(iii.2).- Supongamos que $\phi_b(a) = \gamma^{\tilde{i}b}a$ y que $\tilde{\phi}_b(a) = \gamma^{\tilde{i}b}a$, con $1 \leq i, \tilde{i} \leq p-1$. Notar que $\tilde{i}$ tiene inverso en $\mathbb{Z}_p$, digamos $\tilde{i}^{-1}$. Sea $\Psi : \mathbb{Z}_q \times \mathbb{Z}_p \to \mathbb{Z}_q \times \mathbb{Z}_p$ tal que $\Psi(a,b) = (a, \alpha b)$ con $\alpha = i \cdot \tilde{i}^{-1} \in \mathbb{Z}_p^*$. Sigue que

$$\begin{aligned}\Psi(a,b) +_{\tilde{\phi}} \Psi(a',b') \;&=\; (a,\alpha b) +_{\tilde{\phi}} (a', \alpha b') \;=\; (a + \gamma^{\tilde{i}\alpha b}a', \alpha(b+b')) \\ &=\; (a+\gamma^{ib}a', \alpha(b+b')) \;=\; \Psi(a+\gamma^{ib}a', b+b') \;=\; \Psi((a,b) +_\phi (a',b')).\end{aligned}$$

Es fácil ver que Ψ es biyección, luego isomorfismo de $P \times_\phi Q$ en $P \times_{\tilde{\phi}} Q$.

(iv).- Aunque no se pedía, identificaremos los grupos involucrados cuando correspondan a estructuras vistas.

Como $6 = 2 \cdot 3$ y 2 divide a $2 = 3-1$, de la parte anterior se concluye que hay dos grupos de orden 6, uno abeliano ($\mathbb{Z}_2 \times \mathbb{Z}_3$) y otro no abeliano ($S_3 \cong D_3$).

Como $10 = 2 \cdot 5$ y 2 divide a $4 = 5-1$, de la parte anterior se concluye que hay dos grupos de orden 10, uno abeliano ($\mathbb{Z}_2 \times \mathbb{Z}_5$) y otro no abeliano ($D_5$).

Como $14 = 2 \cdot 7$ y 2 divide a $6 = 7-1$, de la parte anterior se concluye que hay dos grupos de orden 14, uno abelianos ($\mathbb{Z}_2 \times \mathbb{Z}_7$) y otro no abeliano ($D_7$).

Como $15 = 3 \cdot 5$ y 3 no divide a $4 = 5-1$, de la parte anterior se concluye que hay un único grupo de orden 15 y que este es abeliano ($\mathbb{Z}_3 \times \mathbb{Z}_5$).

Como $21 = 3 \cdot 7$ y 3 divide a $6 = 7-1$, de la parte anterior se concluye que hay dos grupos de orden 21, uno abeliano ($\mathbb{Z}_3 \times \mathbb{Z}_7$) y el otro no abeliano.

Como $22 = 2 \cdot 11$ y 2 divide a $10 = 11 - 1$, de la parte anterior se concluye que hay dos grupos de orden 22, uno abeliano ($\mathbb{Z}_2 \times \mathbb{Z}_{11}$) y otro no abeliano ($D_{11}$).

Como $26 = 2 \cdot 13$ y 2 divide a $12 = 13 - 1$, de la parte anterior se concluye que hay dos grupos de orden 26, uno abeliano ($\mathbb{Z}_2 \times \mathbb{Z}_{13}$) y otro no abeliano ($D_{13}$).

PROBLEMA 3:

Observemos que hay 20 cíclos distintos de largo 3 en S_5. En efecto, todo cíclo de largo 3 se puede representar de una única forma como (abc) donde $a < b, c$ y $a, b, c \in [5]$ son distintos. Si $a = 1$, entonces hay 4 opciones para b y 3 para c, es decir 12 posibilidades. Si $a = 2$, entonces hay 3 opciones para b y 2 para c, es decir 6 posibilidades. Si $a = 3$, entonces hay 2 opciones para b y 1 para c, es decir 2 posibilidades. En total, hay 20 posibilidades.

Definamos las permutaciones de $[5]$ dadas por $\varphi = (12)(45)$ y $\phi = (12345)$. Afirmamos que el subgrupo de S_5 generado por φ y ϕ es A_5. Para probarlo, basta verificar que $\langle\{\varphi, \phi\}\rangle$ contiene todos los cíclos de largo 3 (porque A_5 es generado por dichos cíclos). En fecto, observar que

$$\alpha_1 \;=\; \varphi \circ \phi \;=\; (12)(45)(12345) \;=\; (235)\,.$$

Luego,

$$\begin{aligned}
\alpha_2 &= \phi \circ \alpha_1 \circ \phi^{-1} &&= (134)\,,\\
\alpha_3 &= \phi \circ \alpha_2 \circ \phi^{-1} &&= (245)\,,\\
\alpha_4 &= \phi \circ \alpha_3 \circ \phi^{-1} &&= (135)\,,\\
\alpha_5 &= \phi \circ \alpha_4 \circ \phi^{-1} &&= (124)\,.
\end{aligned}$$

Sigue que $\alpha_6 = \alpha_1^2 = (253)$, $\alpha_7 = \alpha_2^2 = (143)$, $\alpha_8 = \alpha_3^2 = (254)$, $\alpha_9 = \alpha_4^2 = (153)$, y $\alpha_{10} = \alpha_5^2 = (142)$. Además,

$$\begin{aligned}
\alpha_{11} &= \varphi \circ \alpha_3 \circ \varphi^{-1} &&= (154)\,,\\
\alpha_{12} &= \varphi \circ \alpha_4 \circ \varphi^{-1} &&= (234)\,,\\
\alpha_{13} &= \varphi \circ \alpha_5 \circ \varphi^{-1} &&= (152)\,.
\end{aligned}$$

Sigue que $\alpha_{14} = \alpha_{11}^2 = (145)$, $\alpha_{15} = \alpha_{12}^2 = (243)$, $\alpha_{16} = \alpha_{13}^2 = (125)$

Finalmente, notar que

$$\begin{aligned}
\alpha_{17} &= \phi \circ \alpha_{12} \circ \phi^{-1} &&= (345)\,,\\
\alpha_{18} &= \phi \circ \alpha_{16} \circ \phi^{-1} &&= (123)\,.
\end{aligned}$$

Sigue que $\alpha_{19} = \alpha_{17}^2 = (354)$ y $\alpha_{20} = \alpha_{18}^2 = (132)$.

Notar que todos los α_i's son cíclos distintos de largo 3 y que estan en $\langle\{\varphi, \phi\}\rangle$. Como vimos, en A_5 hay 20 cícos de largo 3, luego

$$A_5 \;=\; \langle\{\sigma : \sigma \text{ es cíclo de largo } 3\}\rangle \;=\; \langle\{\alpha_i : i = 1, \ldots, 20\}\rangle \subseteq \langle\{\varphi, \phi\}\rangle\,.$$

Dado que φ y ϕ son pares, se tiene que $\langle\{\varphi, \phi\}\rangle \subseteq A_5$. Sigue que A_5 está generado por φ y ϕ.

Para concluir lo pedido, notar que si aplicamos la operación φ o ϕ a una configuración del juego de permutaciones $\pi \in S_5$, obtenemos las configuraciones $\pi \circ \phi$ o $\pi \circ \varphi$, respectivamente. Sea $\pi \in S_5$ par. Sigue que $\pi \in A_5$ y por lo tanto $\pi^{-1} \in A_5 = \langle \{\varphi, \phi\} \rangle$. Por caracterización de grupo generado, existe $k \in \mathbb{N}$, $n_1, \ldots, n_k \in \mathbb{Z}$, $\sigma_1, \ldots, \sigma_k \in \{\varphi, \phi\}$, tales que $\pi^{-1} = \circ_{i=1}^{k} \sigma_i^{n_i}$. Luego, partiendo de la configuración inicial π y aplicando n_k veces la operación σ_k, n_{k-1} veces la operación σ_{k-1}, ..., n_1 veces la operación σ_1, llegamos a la configuación $\pi \circ \pi^{-1} = id_{[5]}$, lo que equivale a lo que se pedía demostrar.