CONTROL 3
ALGEBRA MA11A

26 DE JUNIO, 2003

Tiempo : 3 horas

Problema 1:

(1) (a) Sea $z \in \mathbb{C}$, entonces pruebe que

$$|z+i| = |z-i| \Longleftrightarrow z \in \mathbb{R}.$$

(1.5 ptos.)

Solución:

($\Longrightarrow$) Sea $z = a + bi \in \mathbb{C}$ tal que

$$|z+i| = |z-i|,$$

entonces se tiene que

$$\begin{aligned} |z+i|^2 = |z-i|^2 &\Longrightarrow a^2 + (b+1)^2 = a^2 + (b-1)^2 \\ &\Longrightarrow (b+1)^2 = (b-1)^2 \\ &\Longrightarrow b^2 + 2b + 1 = b^2 - 2b + 1 \\ &\Longrightarrow 2b = -2b \\ &\Longrightarrow 4b = 0 \\ &\Longrightarrow b = 0 \\ &\Longrightarrow z = a \in \mathbb{R}. \end{aligned}$$

($\Longleftarrow$) Sea $z \in \mathbb{R}$, luego

$$|z+i| = \sqrt{z^2 + 1^2} = \sqrt{z^2+1},$$

además

$$|z-i| = \sqrt{z^2 + (-1)^2} = \sqrt{z^2+1},$$

lo que prueba que

$$|z+i| = |z-i|.$$

Así se concluye que

$$|z+i| = |z-i| \Longleftrightarrow z \in \mathbb{R}.$$

(b) Muestre que el conjunto de todo los $z \in \mathbb{C}$ tales que

$$\left|\frac{z-2}{z+1}\right| = 4.$$

es una circunferencia en el plano complejo. Determine su centro y su radio.

(1.5 ptos.)

Solución:

Sea $z = a + ib \in \mathbb{C}$ tal que

$$\left|\frac{z-2}{z+1}\right| = 2,$$

luego

$$|z-2|^2 = 4\,|z+1|^2\,,$$

es decir,

$$\begin{aligned}(z-2)(\overline{z-2}) = 4\left((z+1)(\overline{z+1})\right) &\Longrightarrow z\overline{z} - 2(z+\overline{z}) + 4 = 4\left(z\overline{z} + (z+\overline{z}) + 1\right)\\ &\Longrightarrow z\overline{z} - 2(z+\overline{z}) = 4z\overline{z} + 4(z+\overline{z})\\ &\Longrightarrow -6(z+\overline{z}) = 3z\overline{z}\\ &\Longrightarrow a^2 + b^2 + 4a = 0\\ &\Longrightarrow (a+2)^2 + b^2 = 4\\ &\Longrightarrow |z+2|^2 = 2,\end{aligned}$$

es decir, el conjunto solución es una circunferencia de centro $z = -2$ y radio 2.

(2) Pruebe que para todo $n \in \mathbb{N}$ se tiene que

$$\left(1 + i\tan\left(\frac{\pi}{12}\right)\right)^n + \left(1 - i\tan\left(\frac{\pi}{12}\right)\right)^n = 2\left(\sec\left(\frac{\pi}{12}\right)\right)^n \cos\left(\frac{n\pi}{12}\right).$$

(3 ptos.)

Solución:

Sea $n \in \mathbb{N}$, luego se tiene que

$$\begin{aligned}\left(1 + i\tan\left(\frac{\pi}{12}\right)\right)^n + \left(1 - i\tan\left(\frac{\pi}{12}\right)\right)^n &= \left(1 + i\frac{\operatorname{sen}\left(\frac{\pi}{12}\right)}{\cos\left(\frac{\pi}{12}\right)}\right)^n + \left(1 - i\frac{\operatorname{sen}\left(\frac{\pi}{12}\right)}{\cos\left(\frac{\pi}{12}\right)}\right)^n\\ &= \frac{\left(\cos\left(\frac{\pi}{12}\right) + i\operatorname{sen}\left(\frac{\pi}{12}\right)\right)^n}{\left(\cos\left(\frac{\pi}{12}\right)\right)^n} + \frac{\left(\cos\left(\frac{\pi}{12}\right) - i\operatorname{sen}\left(\frac{\pi}{12}\right)\right)^n}{\left(\cos\left(\frac{\pi}{12}\right)\right)^n}\\ &= \frac{\left(\cos\left(\frac{\pi}{12}\right) + i\operatorname{sen}\left(\frac{\pi}{12}\right)\right)^n}{\left(\cos\left(\frac{\pi}{12}\right)\right)^n} + \frac{\left(\cos\left(\frac{-\pi}{12}\right) + i\operatorname{sen}\left(\frac{-\pi}{12}\right)\right)^n}{\left(\cos\left(\frac{\pi}{12}\right)\right)^n}\\ &= \frac{\left(\cos\left(\frac{n\pi}{12}\right) + i\operatorname{sen}\left(\frac{n\pi}{12}\right)\right)}{\left(\cos\left(\frac{\pi}{12}\right)\right)^n} + \frac{\left(\cos\left(\frac{-n\pi}{12}\right) + i\operatorname{sen}\left(\frac{-n\pi}{12}\right)\right)}{\left(\cos\left(\frac{\pi}{12}\right)\right)^n} \quad \text{(De Moivre)}\\ &= \frac{1}{\left(\cos\left(\frac{\pi}{12}\right)\right)^n}\left[\cos\left(\frac{n\pi}{12}\right) + i\operatorname{sen}\left(\frac{n\pi}{12}\right) + \cos\left(\frac{-n\pi}{12}\right) + i\operatorname{sen}\left(\frac{-n\pi}{12}\right)\right]\\ &= \left(\sec\left(\frac{\pi}{12}\right)\right)^n\left[2\cos\left(\frac{n\pi}{12}\right)\right],\end{aligned}$$

lo que completa la demostración.

Problema 2:

Considere el conjunto $\mathbb{Z}_2 \times \mathbb{Z}_2$ con las operaciones

$$(a,b) + (c,d) = (a+c, b+d)$$
$$(a,b) \cdot (c,d) = (a \cdot c, b \cdot d),$$

donde $+$ y $\cdot$ son la suma y la multiplicación usual en $\mathbb{Z}_2$.

Definamos también la operación

$$(a,b) * (c,d) = (a \cdot c + b \cdot d, a \cdot b + b \cdot c + b \cdot d).$$

Usando el hecho de que $(\mathbb{Z}_2, +, \cdot)$ es un cuerpo pruebe que:

a) $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, \cdot)$ es un anillo conmutativo y con unidad ¿Es un cuerpo? Justifique su respuesta.

(2 ptos.)

b) $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, *)$ es un cuerpo.

(2 ptos.)

c) Pruebe que $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, *)$ no es isomorfo a $(\mathbb{Z}_4, +, \cdot)$, es decir, no existe ningun morfismo biyectivo entre $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, *)$ y $(\mathbb{Z}_4, +, \cdot)$.

(2 ptos.)

Solución:

a) En primer lugar veamos que $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, \cdot)$ es un anillo conmutativo con unidad. En efecto:

Veamos que $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ es un grupo Abeliano.

Sean $(a,b), (c,d), (e,f) \in \mathbb{Z}_2 \times \mathbb{Z}_2$, es claro que $+$ y $\cdot$ son l. c. i. para $\mathbb{Z}_2 \times \mathbb{Z}_2$ ya que $(\mathbb{Z}_2, +, \cdot)$ es un cuerpo y cada componente de la suma y la multiplicación son combinaciones y productos de elementos de $\mathbb{Z}_2$.

En primer lugar podemos ver que $+$ y $\cdot$ son operaciones conmutativas, en efecto

$$\begin{aligned} (a,b) + (c,d) &= (a+c, b+d) && \text{def. de la suma} \\ &= (c+a, d+b) && \text{conmutatividad de } + \text{ en } \mathbb{Z}_2 \\ &= (c,d) + (a,b) && \text{def. de la suma} \end{aligned}$$

y además

$$\begin{aligned} (a,b) \cdot (c,d) &= (a \cdot c, b \cdot d) && \text{def. del producto} \\ &= (c \cdot a, d \cdot b) && \text{conmutatividad de } \cdot \text{ en } \mathbb{Z}_2 \\ &= (c,d) \cdot (a,b) && \text{def. del producto} \end{aligned}$$

Además, si 0 es el neutro aditivo de $(\mathbb{Z}_2, +)$ entonces $(0,0)$ es el neutro aditivo de $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$, en efecto

$$\begin{aligned} (a,b) + (0,0) &= (a+0, b+0) && \text{def. de la suma} \\ &= (a,b) && 0 \text{ es neutro aditivo } + \text{ en } \mathbb{Z}_2, \end{aligned}$$

y dado que $+$ es conmutativo, se completa la demostración.

Por otra parte, si dado $a \in \mathbb{Z}_2$ entonces existe $-a \in \mathbb{Z}_2$ el inverso aditivo de a. Así dado $(a,b) \in \mathbb{Z}_2 \times \mathbb{Z}_2$, entonces $(-a,-b) \in \mathbb{Z}_2 \times \mathbb{Z}_2$ es el inverso aditivo de (a,b). En efecto,

$$\begin{aligned} (a,b) + (-a,-b) &= (a + (-a), b + (-b)) && \text{def. de la suma} \\ &= (0,0) && -a, -b \text{ son los inversos aditivos } + \text{ en } \mathbb{Z}_2 \end{aligned}$$

Finalmente nos queda ver la asociatividad,luego

$$\begin{aligned} (a,b) + ((c,d) + (e,f)) &= (a,b) + (c+e, d+f) && \text{def. de la suma} \\ &= (a + (c+e), b + (d+f)) && \text{def. de la suma} \\ &= ((a+c) + e, (b+d) + b) && \text{asociatividad de } + \text{ en } \mathbb{Z}_2 \\ &= (a+c, b+d) + (e,f) && \text{def. de la suma} \\ &= ((a,b) + (c,d)) + (e,f) && \text{def. de la suma} \end{aligned}$$

Lo que prueba que $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ es un grupo Abeliano. Por otra parte, si 1 es el neutro multiplicativo de $\cdot$ en $\mathbb{Z}_2$, entonces $(1,1)$ es el inverso multiplicativo de $\cdot$ en $\mathbb{Z}_2 \times \mathbb{Z}_2$, ya que dado $(a,b) \in \mathbb{Z}_2 \times \mathbb{Z}_2$, entonces

$$\begin{array}{lll} (a,b)\cdot(1,1) & = (a\cdot 1, b\cdot 1) & \text{def. del producto} \\ & = (a,b) & 1 \text{ es neutro de } \cdot \text{ en } \mathbb{Z}_2 \end{array}$$

Veamos la distribituvidad del producto con respecto a la suma. En efecto

$$\begin{array}{lll} (a,b)\cdot((c,d)+(e,f)) & = (a,b)\cdot(c+e,d+f) & \text{def. de } + \\ & = (a\cdot(c+e), b\cdot(d+f)) & \text{def. de } \cdot \\ & = (a\cdot c + a\cdot e, b\cdot d + b\cdot f) & \text{distribitividad en } \mathbb{Z}_2 \\ & = (a\cdot c, b\cdot d) + (a\cdot e, +b\cdot f) & \text{def. de } + \\ & = (a,b)\cdot(c,d) + (a,b)\cdot(e,f) & \text{def. de } \cdot, \end{array}$$

lo que prueba la distributividad.

Así $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, \cdot)$ es un anillo conmutativo con unidad.

Notemos que $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, \cdot)$ no es un cuerpo ya que tiene divisores de cero, en efecto

$$(1,0)\cdot(0,1) = (0,0).$$

Otro argumento para mostrar que no es un cuerpo es el hecho que el elemento $(1,0)$ no tiene inverso multiplicativo, en efecto $(a,b) \in \mathbb{Z}_2 \times \mathbb{Z}_2$, entonces se tiene que

$$(1,0)\cdot(a,b) = (a,0) \neq (a,1) \qquad \forall (a,b).$$

b) De la parte anterior se tiene que $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ es un grupo Abeliano. Nos resta probar que

$$(\mathbb{Z}_2 \times \mathbb{Z}_2 \setminus \{(0,0)\}, *)$$

es un grupo Abeliano.

En primer lugar podemos ver que $*$ es una ley de composición interna en $\mathbb{Z}_2 \times \mathbb{Z}_2$ ya que sus componentes son sumas y productos de elementos de $\mathbb{Z}_2$ y la suma y la multiplicación son l.c.i. para $\mathbb{Z}_2$, ya que $(\mathbb{Z}_2, +, \cdot)$ es un cuerpo.

Por otra parte podemos ver que $*$ es conmutativa, en efecto sean $(a,b),(c,d) \in \mathbb{Z}_2 \times \mathbb{Z}_2$, luego

$$\begin{array}{lll} (a,b)*(c,d) & = (a\cdot c + b\cdot d, a\cdot d + b\cdot c + b\cdot d) & \text{def. de } * \\ & = (c\cdot a + d\cdot b, d\cdot a + c\cdot b + d\cdot b) & \text{conmutatividad de } \cdot \\ & = (c\cdot a + d\cdot b, c\cdot b + d\cdot a + d\cdot b) & \text{conmutatividad de } + \\ & = (c,d)*(a,b) & \text{def. de } *. \end{array}$$

Por otra parte, $(1,0)$ es el neutro de $*$. En efecto, sea $(a,b) \in \mathbb{Z}_2 \times \mathbb{Z}_2$, luego

$$\begin{array}{lll} (a,b)*(1,0) & = (a\cdot 1 + b\cdot 0, a\cdot 0 + b\cdot 1 + b\cdot 0) & \text{def. de } * \\ & = (a+0, 0+b+0) & 1 \text{ es neutro mult. y } 0 \text{ es neutro aditivo} \\ & = (a,b) & . \end{array}$$

Veamos que para cada $(a,b) \in \mathbb{Z}_2 \times \mathbb{Z}_2 \setminus \{(0,0)\}$, existe un inverso multiplicativo. Podemos notar que

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \setminus \{(0,0)\} = \{(1,0),(0,1),(1,1)\}$$

y puesto que $(1,0)$ es el neutro para $*$, entonces

$$(1,0)^{-1} = (1,0).$$

Veamos los inversos de $(0,1)$ y $(1,1)$. Como su segunda componente es 1, basta ver el caso $(a,1)$ con $a = 0,1$.

Si $(c,d) = (a,1)^{-1}$, entonces

$$\begin{array}{lll} (a,1)*(c,d) = (1,0) & \iff (a\cdot c + 1\cdot d, a\cdot d + 1\cdot c + 1\cdot d) = (1,0) & \text{def. } * \\ & \iff (a\cdot c + d, a\cdot d + c + d) = (1,0) & \text{def. } *, \end{array}$$

es decir

$$a \cdot c + d = 1 \qquad a \cdot d + c + d = 0.$$

Luego si $a = 0$, entonces

$$d = 1 \qquad c + d = 0 \quad \Longrightarrow c = d = 1 \Longrightarrow (0,1)^{-1} = (1,1),$$

si $a = 1$ entonces

$$c+d=1 \quad d+c+d=0 \quad \Longrightarrow c+d=1 \quad c+2d=0 \Longrightarrow c+d=1 \quad c=0 \Longrightarrow d=1 \quad c=0 \Longrightarrow (1,1)^{-1} = (0,1).$$

Lo que prueba que cada elemento no nulo tiene inverso para $*$.

Nos resta ver la asociatividad de $*$. En efecto, sean $(a,b),(c,d),(e,f) \in \mathbb{Z}_2 \times \mathbb{Z}_2$, entonces se tiene que

$$(a,b) * [(c,d) * (e,f)] \quad = \ldots$$

Esto prueba que $(\mathbb{Z}_2 \times \mathbb{Z}_2 \setminus \{(0,0)\})$ es un grupo Abeliano.

Para probar que $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, *)$ basta probar que se tiene la distributividad de $*$ con respecto a $+$, es decir, para todo $(a,b),(c,d),(e,f) \in \mathbb{Z}_2 \times \mathbb{Z}_2$, entonces

$$\begin{aligned}
(a,b) * [(c,d) + (e,f)] &= (a,b) * ((c+e, d+f)) && \text{def. } + \text{ y } * \\
&= (a \cdot (c+e) + b \cdot (d+f), a \cdot (d+f) + b \cdot ((c+e) + (d+f))) && \\
&= (a \cdot c + a \cdot e + b \cdot d + b \cdot f, a \cdot d + a \cdot f + b \cdot (c+d) + b \cdot (e+f)) && \text{distrib. en } \mathbb{Z}_2 \\
&= ((a \cdot c + b \cdot d) + (a \cdot e + b \cdot f), (a \cdot d + b \cdot (c+d)) + (a \cdot f + b \cdot (e+f)) && \text{asoc. y conmut. en } \mathbb{Z}_2 \\
&= (a \cdot c + b \cdot d, a \cdot d + b \cdot (c+d)) + (a \cdot e + b \cdot f, a \cdot f + b \cdot (e+f)) && \text{def. } + \\
&= (a,b) * (c,d) + (a,b) * (e,f) && \text{def. } *.
\end{aligned}$$

Lo que completa la demostración.

c) Notemos que $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, *)$ y $(\mathbb{Z}_4, +, \cdot)$ no son isomorfos ya que el primero es un cuerpo y el segundo no lo es ($(\mathbb{Z}_p, +, \cdot)$) es un cuerpo si y sólo si p es un número primo.

Problema 3:

(1) Sea $(G,\cdot)$ un grupo Abeliano de cardinalidad $|G|=15$. Definamos los conjuntos:

$$F=\left\{g\in G\,:\,g^5=1\right\}$$

y

$$H=\left\{g\in G\,:\,g^3=1\right\},$$

donde 1 es el neutro del grupo G.

(a) Pruebe que F y H son subgrupos de G.

(b) Pruebe que

$$F\cap H=\{1\}.$$

(c) Pruebe que si F y H no son los subgrupos triviales ($F,H\neq\{1\}$ y G), entonces $|F|=5$ y $|H|=3$. Pruebe además que

$$\{\,f\cdot h\,:\,f\in F\,,h\in H\}=G.$$

(4 ptos.)

(2) Sea $(G,*)$ un grupo y sea $S\subseteq G$, un conjunto no vacío. Para cada $g\in G$ se definen los conjuntos

$$g*S=\{g*s\,:\,\forall s\in S\}$$

y

$$S*g=\{s*g\,:\,\forall s\in S\}\,.$$

Se definen los conjuntos:

$$C(S)=\left\{g\in G\,:\,g^{-1}*s*g=s,\,\forall s\in S\right\}$$

y

$$N(S)=\left\{g\in G\,:\,g^{-1}*S*g=S\right\}.$$

Pruebe que $C(S)\subseteq N(S)$, ambos no vacíos, además $C(S)$ y $N(S)$ son subgrupos de G.

(2 ptos.)

Solución:

(1) (a) Debemos probar en primer lugar que $\cdot$ es una ley de composición interna para F y H, en efecto sean g,f dos elementos tales que

$$f^n=1\qquad\wedge\qquad g^n=1,$$

entonces dado que G es un grupo Abeliano, tenemos que

$$f^n=1\quad\wedge\quad g^n=1\Longrightarrow(f\cdot g)^n=f^n\cdot g^n=1\cdot 1=1.$$

Además si $f^n=1$ entonces $f^{-1}=f^{n-1}\in G$, además

$$(f^{n-1})^n=(f^n)^{n-1}=1^{n-1}=1.$$

Lo que muestra que cada elemento de F y H tienen un inverso en dichos conjuntos. Luego, dados f,g tales que

$$f^n=1\quad g^n=1,$$

entonces de la conmutatividad del producto

$$\left[f\cdot g^{-1}\right]^n=f^n\cdot\left[g^{-1}\right]^n=f^n\cdot\left[g^{-1}\right]^n=f^n\cdot\left[g^{n-1}\right]^n=1$$

esto prueba que F y H son subgrupos de G considerando $n=5$ y $n=3$.

(b) Sea $g\in F\cap H$ luego

$$g^5=1\quad\wedge\quad g^3=1\Longrightarrow g^5=1\quad\wedge\quad g^6=1\Longrightarrow g^5=g^6$$

y como g^5 es cancelable por ser G un grupo se tiene que

$$g=1,$$

lo que completa la demostración.

(c) Como F y H son subgrupos no triviales de G, entonces sus cardinales dividen a 15, es decir sus cardinalidades son 3 ó 5.
Notemos que si $g \in H$ con $g \neq 1$, entonces

$$\left\{1, g, g^2\right\}$$

es un subgrupo de H y luego su cardinalidad 3 divide a la cardinalidad de H, que puede ser 3 ó 5, luego se concluye que la cardinalidad de H es 3.
Análogamente se tiene que si $g \in F$ con $g \neq 1$, entonces

$$\left\{1, g, g^2, g^3, g^4\right\}$$

es un subgrupo de F y luego su cardinalidad 5 divide a la cardinalidad de F, que puede ser 3 ó 5, luego se concluye que la cardinalidad de F es 5.

Finalmente notemos que tanto H como F son subgrupos de

$$F \cdot H = \{\, f \cdot h \,:\, f \in F\,, h \in H\}\,,$$

luego 3 y 5 dividen la cardinalidad de $F \cdot H$ y como éste es un subgrupo de G, necesariamente su cardinalidad debe ser 15. De donde se concluye que

$$F \cdot H = \{\, f \cdot h \,:\, f \in F\,, h \in H\} = G.$$

(2) Se debe probar que $N(S)$ es subgrupo de G y $C(S)$ es subgrupo de $N(S)$.
En efecto, podemos ver que tanto $N(S)$ como $C(S)$ son no vacíos ya que el neutro e de G pertenece a ambos conjuntos.
En efecto podemos observar que si $g, f \in G$ entonces

$$\begin{array}{lll} f*(g*S) & = \{f*(g*s) \,:\, s \in S\} & \text{def. de } g*S \\ & = \{(f*g)*s) \,:\, s \in S\} & \text{asoc. de } * \\ & = (f*g)*S & \text{def. de } (f*g)*S \end{array}$$

y además

$$\begin{array}{lll} (S*g)*f & = \{(s*g)*f) \,:\, s \in S\} & \text{def. de } S*g \\ & = \{s*(g*f) \,:\, s \in S\} & \text{asoc. de } * \\ & = S*(f*g) & \text{def. de } S*(f*g) \end{array}$$

Veamos ahora que si $g_1, g_2 \in N(S)$ entonces $g_1 * g_2^{-1} \in N(S)$. Notemos que de las identidades anteriores se tiene lo siguiente:

$$\begin{array}{lll} (g_1*g_2^{-1})^{-1}*S*(g_1*g_2^{-1}) & = (g_2*g_1^{-1})*S*(g_1*g_2^{-1}) & \\ & = g_2*(g_1^{-1}*S*g_1)*g_2^{-1} & \text{asoc de } * \\ & = g_2*S*g_2^{-1} & g_1 \in N(S). \end{array}$$

Luego basta mostrar que si $g \in N(S)$, entonces $g^{-1} \in N(S)$, es decir

$$g^{-1}*S*g = S \Longrightarrow g*S*g^{-1} = S.$$

En efecto

$$\begin{array}{ll} g^{-1}*S*g = S & \Longrightarrow g*\left(g^{-1}*S*g\right) = g*S \\ & \Longrightarrow (g*g^{-1})*S*g = g*S \\ & \Longrightarrow e*S*g = g*S \\ & \Longrightarrow S*g = g*S \\ & \Longrightarrow (S*g)*g^{-1} = g*S*g^{-1} \\ & \Longrightarrow S*(g*g^{-1}) = g*S*g^{-1} \\ & \Longrightarrow S*e = g*S*g^{-1} \\ & \Longrightarrow S = g*S*g^{-1} \\ & \Longrightarrow g^{-1} \in N(S). \end{array}$$

De donde se concluye que si $g_1, g_2 \in N(S)$ entonces $g_1 * g_2^{-1} \in N(S)$, y así $N(S)$ es un subgrupo de G.

Nos resta mostrar ahora que $C(S)$ es un subgrupo de $N(S)$. Lo que podemos notar es que $C(S) \neq \emptyset$ ya que el neutro de G, $e \in C(S)$.

Además si $g \in C(S)$, entonces

$$g^{-1} * s * g = s, \qquad \forall s \in S,$$

luego

$$g^{-1} * S * g = S \implies g \in N(S)$$

es decir,

$$C(S) \subseteq N(S).$$

Veamos ahora que es un subgrupo, es decir, debemos probar que si g_1, $g_2 \in C(S)$ entonces $g_1 * g_2^{-1} \in C(S)$.

Sea $s \in S$, luego

$$\begin{array}{lll} (g_1 * g_2^{-1})^{-1} * s * (g_1 * g_2^{-1}) & = (g_2 * g_1^{-1}) * s * (g_1 * g_2^{-1}) & \text{def de inverso} \\ & = g_2 * (g_1^{-1} * s * g_1) * g_2^{-1} & \text{asoc. de } * \\ & = g_2 * s * g_2^{-1} & g_1 \in C(S). \end{array}$$

Pero como $g_2 \in C(S)$ tenemos que $\forall s \in S$

$$\begin{array}{lll} g_2^{-1} * s * g_2 = s & \implies g_2 * (g_2^{-1} * s * g_2) = g_2 * s & \\ & \implies (g_2 * g_2^{-1}) * s * g_2 = g_2 * s & \text{asoc. de } * \\ & \implies s * g_2 = g_2 * s & \text{def de neutro} \\ & \implies (s * g_2) * g_2^{-1} = (g_2 * s) * g_2{-}1 & \\ & \implies s * (g_2 * g_2^{-1}) = g_2 * s * g_2{-}1 & \text{asoc. de } * \\ & \implies s = g_2 * s * g_2{-}1 & \text{def. de neutro.} \end{array}$$

Luego

$$(g_1 * g_2^{-1})^{-1} * s * (g_1 * g_2^{-1}) = s \implies (g_1 * g_2^{-1}) \in C(S),$$

lo que prueba que $C(S)$ es un subgrupo de $N(S)$.