Universidad de Chile
Facultad de Cs. Físicas y Matemáticas
Departamento de Ingeniería Matemática

Problemas Semana 10

Pregunta 1

Sea $(G, *)$ un grupo y $f : G \to G$ la función definida por $f(g) = g^{-1}$ para cada $g \in G$ (recordar que g^{-1} es el inverso de g para la operación *). Probar que

$$f \text{ es un isomorfismo} \Leftrightarrow G \text{ es un grupo Abeliano}$$

Solución

Para ver la implicancia hacia la derecha, falta la conmutatividad de la operación * (notemos que la operación * es la misma tanto para el dominio como para el recorrido). Sean x, y cualesquiera en G. Como f es biyectiva, en particular, es sobreyectiva, entonces, existen g_x, g_y que verifican:

$$f(g_x) = x = g_x^{-1}, \qquad f(g_y) = y = g_y^{-1}$$

Así, tenemos que $x * y = g_x^{-1} * g_y^{-1} = (g_y * g_x)^{-1} = f(g_y * g_x)$, pero además, sabemos que f es morfismo, entonces, podemos continuar la serie de igualdades:

$$x * y = f(g_y) * f(g_x) = g_y^{-1} * g_x^{-1} = y * x$$

lo que prueba la conmutatividad. Para demostrar el converso, debemos mostrar que f es morfismo y que es biyectivo. Para lo primero, necesitamos que para todo $g_1, g_2 \in G$, se verifique que $f(g_1) * f(g_2) = f(g_1 * g_2)$, o equivalentemente, $g_1^{-1} * g_2^{-1} = (g_1 * g_2)^{-1}$. Pero este último término en una estructura algebraica cualquiera (cuando los inversos respectivos están bien definidos, como en el caso de un grupo) siempre es igual a $g_2^{-1} * g_1^{-1}$; es decir, para que f sea morfismo, se requiere que

$$g_1^{-1} * g_2^{-1} = g_2^{-1} * g_1^{-1}$$

lo que se cumple dado que G es abeliano. La sobreyectividad se tiene debido a que, dado $a \in G$, siempre existe $a^{-1} \in G$ -G es grupo-, que sabemos que cumple $f(a^{-1}) = (a^{-1})^{-1} = a$. Por último, para ver la inyectividad, sean $y_1, y_2 \in G$, que satisfacen que $f(y_1) = f(y_2)$, o en otras palabras, $y_1^{-1} = y_2^{-1}$. Entonces

$$\begin{aligned} y_1^{-1} &= y_2^{-1} \qquad /y_1* \\ y_1 * y_1^{-1} = e &= y_1 * y_2^{-1} \qquad / * y_2 \\ e * y_2 &= y_1 * y_2^{-1} * y_2 = y_1 * e \\ y_2 &= y_1 \end{aligned}$$

lo que concluye la solución.

Pregunta 2

Sea $(G, *)$ un grupo con neutro $e \in G$ y

$$A = \{F : G \to G / \text{ F es un isomorfismo de } (G, *) \text{ en } (G, *)\}$$

(a) Probar que (A, o) es grupo
(b) Para cada g en G se define la función $F_g : G \to G$ tal que $F_g(x) = g * x * g^{-1}$ en cada $x \in G$. Pruebe que:

- F_g es un homomorfismo de $(G, *)$ en $(G, *)$
- $F_{g*h} = F_g \circ F_h$,para todo g, h en G
- $F_e = id_G$ (id_G es la función identidad de G en G)

Concluya que F_g es un isomorfismo y que $(F_g)^{-1} = F_{g^{-1}}, \forall g \in G$
(c) Pruebe que $B = \{F_g/g \in G\}$ es un subgrupo de $(A, \circ)$

Solución

(a) Sabemos que $A \neq \phi$ puesto que id_G es un isomorfismo de G en G. Ahora, la composición de funciones biyectivas es biyectiva, y también la composición de morfismos es morfismo (háganlo ustedes, está enunciado en la p. 130), luego la composición de isomorfismos es isomorfismos, por lo que $(A, \circ)$ es estructura algebraica. La asociatividad se tiene por la asociatividad de la composición de 3 funciones. El neutro está dado por $e_G = id_G$; y el inverso, para un isomorfismo F dado, por F^{-1}, puesto que este último también es isomorfismo. Esta propiedad está como tarea en la p. 130, veamos acá brevemente la demostración: es claro que si F es biyectiva, F^{-1} es biyectiva; veamos que si F es isomorfismo, entonces F^{-1} es morfismo. Sean x, y en G, por la sobreyectividad, existen $v, w \in G$ verificando que $F(w) = x, F(v) = y$, y también por la biyectividad, $w = F^{-1}(x), v = F^{-1}(y)$. Entonces, se cumplirá que:

$$F^{-1}(x * y) = F^{-1}(F(w) * F(v)) = F^{-1}(F(w * v)) = w * v = F^{-1}(x) * F^{-1}(y)$$

(b)Veamos que es morfismo: Sean $x, y \in G$

$$\begin{aligned} F_g(x * y) &= g * x * y * g^{-1} \\ &= g * x * e * y * g^{-1} \\ &= (g * x * g^{-1}) * (g * y * g^{-1}) \quad (asoc.) \\ &= F_g(x) * F_g(y) \end{aligned}$$

Veamos la segunda propiedad requerida: sea x en G, entonces

$$\begin{aligned} F_g \circ F_h(x) = F_g(F_h(x)) = F_g(h * x * h^{-1}) &= g * (h * x * h^{-1}) * g^{-1} \\ &= (g * h) * x * (h^{-1} * g^{-1}) \\ &= (g * h) * x * (g * h)^{-1} = F_{g*h}(x) \end{aligned}$$

Por último, $F_e(x) = e * x * e^{-1} = (e * x) * e = x * e = x = id_G(x)$. Ahora, para probar que F_g es isomorfismo, resta demostrar la biyectividad (una vez hecho esto, de lo probado antes, es directo que $F_{g^{-1}} = (F_g)^{-1}$). Para la sobreyectividad, dado $y \in G$, basta tomar $x = g^{-1} * y * g$ (que está en G por la cerradura), que verificará $F_g(x) = y$. Para la inyectividad, tomen 2 elementos $z_1, z_2 \in G$ que satisfagan $F_g(z_1) = F_g(z_2)$, o escrito de forma más explícita, $g * z_1 * g^{-1} = g * z_2 * g^{-1}$. Aquí basta multiplicar por la izquierda por g^{-1}, y a la derecha por g, para llegar a que $z_1 = z_2$.

(c) Previamente, en (b) ya vimos que las funciones de la forma F_g son isomorfismos, luego, $B \subseteq A$ (Además, $B \neq \phi$ dado que $F_e \in B$). Para comprobar que B es subgrupo de A, usaremos la caracterización de la p. 126: Sean F_g, F_h en B. Por (b), $(F_h)^{-1} = F_{h^{-1}}$. Entonces, $F_g \circ (F_h)^{-1} = F_g \circ F_{h^{-1}} = F_{g*h^{-1}}$, donde el último término por def. está en B (la última igualdad es por (b)).

Pregunta 4

Sea $(G, *)$ un grupo tal que $G = \{e, a, b\}$ con e neutro en G. Pruebe que $a^{-1} = b$

Solución

Para probar esto, probaremos antes una caracterización de grupos finitos que puede serles útil en esta y en otras ocasiones:

Para un grupo de orden finito G, cada línea o columna de su tabla de doble entrada (tabla de Pitágoras), es una permutación de los elementos en G (no tienen elementos repetidos)

Por absurdo, supongamos que en alguna fila hay un elemento repetido, ie, existen a, b, c (distintos) $\in G$ que satisfacen $a * b = a * c$ (si fuese una columna, sería algo del estilo $x * y = z * y$, y sería totalmente análogo). Como en un grupo todo elemento es cancelable, a es cancelable, luego, $(a^{-1} * a) * b = (a^{-1} * a) * c \Leftrightarrow e * b = e * c \Leftrightarrow b = c$. Luego, dentro de una misma fila no pueden haber elementos repetidos.
Ahora, podemos dibujar la tabla de doble entrada de nuestro grupo G:

*	e	a	b
e	e	a	b
a	a	?	?
b	b	?	?

Supongamos que $a * a = e$, como cada fila es una permutación de los elementos de G, se deduce que $a*b = b$, pero esto es un absurdo, puesto que b se repetiría en la tercera columna. Así, $a*a = b$ ($a*a$ es distinto de a puesto que en un grupo el único elemento idempotente es el neutro e), $a * b = e$, y en la última fila, $b * a = e$ y $b * b = a$. De lo anterior, $a^{-1} = b$. De pasada, hemos probado que todos los grupos de orden 3 son isomorfos y abelianos.

Pregunta*

(a) Dado un grupo $(G, *)$, para $g \in G$ se define $< g >= \{g^p / p \in \mathbb{Z}\}$, (convención: $g^0 = e$, neutro en G) (el subgrupo generado por g). Demuestre que dicho conjunto es subgrupo de G.

(b) Sea $(G, *)$ un grupo abeliano y sean H, J 2 subgrupos de G. Se define el conjunto $H * J = \{h * j / h \in H, j \in J\}$. Pruebe que $H * J$ es subgrupo de G. Adicionalmente, verifique por qué tanto H como J son subgrupos de $H * J$

(c) Sea $(G, *)$ un grupo abeliano de cardinalidad 15 ($|G| = 15$). Se definen los conjuntos

$$F = \{g \in G / g^5 = e\},$$
$$H = \{g \in G / g^3 = e\}$$

(donde e es el neutro en G). Pruebe lo siguiente:

- (1) F y H son subgrupos de G
- (2) Pruebe que si F, H no son los subgrupos triviales ($F, H \neq \{e\}, G$), entonces $|F| = 5$ y $|H| = 3$
- (3) Pruebe que, con la misma hipótesis anterior para F y H, $F * H = G$

Solución

(a) Sean a, b en $< g > \Leftrightarrow \exists m, n \in \mathbb{Z}\ tq\ a = g^m, b = g^n$. Entonces

$$\begin{aligned} a * b^{-1} = g^m * (g^n)^{-1} = g^m * (g * g * \cdots * g)^{-1} &= g^m * (g^{-1} * \cdots * g^{-1}) \\ &= (g * \cdots * g) * (g^{-1} * \cdots * g^{-1}) \\ &= g^m * g^{-n} \\ &= g^{m-n} \end{aligned}$$

donde $m - n \in \mathbb{Z}$ $\quad (g^{-n} = (g^{-1})^n$ gracias a la convención $g^0 = e)$.

(b) Sean $g_1 = h_1 * j_1, g_2 = h_2 * j_2 \in H * J$. Entonces:

$$\begin{aligned} g_1 * g_2^{-1} &= (h_1 * j_1) * (h_2 * j_2)^{-1} \\ &= (h_1 * j_1) * (j_2^{-1} * h_2^{-1}) \\ &= (h_1 * j_1) * (h_2^{-1} * j_2^{-1}) \quad (conmut.) \\ &= h_1 * (h_2^{-1} * j_1) * j_2^{-1} \quad (asociat, conmut.) \\ &= (h_1 * h_2^{-1}) * (j_1 * j_2^{-1}) \quad (asociat.) \end{aligned}$$

Notemos que el término del primer paréntesis está en H puesto que H es subgrupo, y el del segundo está en J dado que J es subgrupo. Así, $g_1 * g_2^{-1} \in H * J$. Lo anterior, prueba que $H * J$ es subgrupo de G. Para ver que H es subgrupo de $H * J$, notemos que para todo elemento h de H, $h = h * e$, donde $e \in J$, ie, $H \subseteq H * J$. Como H ya es grupo, al igual que $H * J$, H es subgrupo de $H * J$. Análogamente, J es subgrupo de $H * J$.

(c) (1) Probemos que $*$ es l.c.i. para F y H, (Hagamos la demostración para n natural). Sean $f_1, f_2 \in F$, ie, $(f_1)^n = e, (f_2)^n = e$, entonces se tiene que (usando que G es abeliano):

$$(f_1 * f_2)^n = f_1^n * f_2^n = e * e = e$$

Así, si reemplazamos $n = 3$ y $n = 5$, se tiene que F y H son cerrados para $*$. La asociatividad se hereda de G, y el neutro e claramente está en F y en H. Para ver que todo elemento en F (o en H), posee inverso en F (o en H), sea f que satisface $f^n = e$. Entonces, el inverso de f, está dado por $f^{-1} = f^{n-1}$, y este elemento verifica que

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

Entonces, haciendo $n = 3$ y $n = 5$, se tiene que todo elemento en F -o H-, tiene su inverso en F -o H-, y de esta forma, tanto F como H son grupos (o subgrupos de G).

(2) Por Lagrange (y la parte (1)), las cardinalidades de F y H dividen a $|G| = 15$. Como estos subgrupos no son los triviales, $|F|$ y $|H|$ pueden valer 3 ó 5. Tomemos $f \in F$, sabemos por (a) que $< f >$ es un subgrupo de F. Como $f^n = e$, se cumple que

$$< f >= \{e, f, f^2, f^3, f^4\}$$

Luego, $| < f > | = 5$, y nuevamente por Lagrange, 5 debe dividir a $|F|$, que puede valer 3 ó 5. Necesariamente, $|F| = 5$. Análogamente, si tomamos $h \in H$, por (a), $| < h > |$ debe dividir a $|H|$, pero

$$< h >= \{e, h, h^2\} \Rightarrow | < h > | = 3$$

y esto implica que $|H| = 3$.

(3) Por (b), aplicando Lagrange, $|F * H|$ divide a $|G| = 15$. Por la hipótesis y la parte (2), $|F| = 5$ y $|H| = 3$, y nuevamente por (b), ambos deben dividir a $|F * H|$. Todo esto hace que $|F * H| = 15$, y como $F * H$ es subgrupo de G, necesariamente $F * H = G$.