[redacted]

Guía de Álgebra
Control
N°2

MA11A-04

Tema: Estructuras Algebraicas

P1 Sea $(G,*)$ un grupo y $H \subseteq G$ tal que $(\forall x \in G)\ x*H = H*x$. Donde $x*H = \{x*h / h \in H\}$ y $H*x = \{h*x / h \in H\}$. Se define la relación de equivalencia R_H en G como:

$$x R_H y \Leftrightarrow x*y^{-1} \in H$$

(a) Probar que $*$ es compatible con R_H, es decir
$$(\forall x,y,z,w \in G)\ x R_H y \wedge z R_H w \Rightarrow (x*z) R_H (y*w)$$

(b) Probar que $[x]_{R_H} = \{y \in G / y = h*x \text{ para algún } h \in H\}$

(c) Se define para las clases de equivalencia de R_H
$$[x]_{R_H} \odot [y]_{R_H} = [x*y]_{R_H}$$
Probar que la operación está bien definida

(d) Probar que $(G/H, \odot)$ es un grupo (que se llama grupo cuociente) donde $G/H = \{[x]_{R_H} / x \in G\}$. Probar que $[e]_{R_H} = H$, donde e es el neutro de $(G,*)$

Solución:

(a) Notemos que $x*H = H*x$ nos dice que un elemento de $x*H$ (o sea de la forma $x*h_1$) puede ser escrito como un elemento de $H*x$ (o sea de la forma h_2*x)

En otras palabras tendremos que:

Dado $x*h_1 \in x*H$, $\exists h_2 \in H$ tal que
$$x*h_1 = h_2*x \quad (*)$$

Pdq: $x R_H y \wedge z R_H w \Rightarrow (x*z) R_H (y*w)$

Pero, por definición de R_H tenemos que:
$$x R_H y \wedge z R_H w \Leftrightarrow x*y^{-1} \in H \wedge z*w^{-1} \in H$$
y
$$(x*z) R_H (y*w) \Leftrightarrow (x*z)*(y*w)^{-1} \in H$$
$$\Leftrightarrow (x*z)*(w^{-1}*y^{-1}) \in H.$$

Entonces lo que en realidad buscamos probar es que:
$$x*y^{-1} \in H \wedge z*w^{-1} \in H \Rightarrow (x*z)*(w^{-1}*y^{-1}) \in H.$$

En efecto, $x*y^{-1} \in H$ nos dice que $x*y^{-1} = h_1$ para algún $h_1 \in H$. Analogamente $z*w^{-1} = h_2$ para algún $h_2 \in H$

Veamos ahora que $\underbrace{(x*z)*(w^{-1}*y^{-1}) = (x*(z*w^{-1}))*y^{-1}}_{\text{Asociatividad}} = (\underbrace{x*h_2}_{h_2})*y^{-1}$

Ahora por (*), $\exists h_3 \in H$ tal que $x * h_2 = h_3 * x$

Usando esto en lo anterior tendremos que:

$$(x*z)*(w^{-1}*y^{-1}) = (x*h_2)*y^{-1} = (h_3*x)*y^{-1}$$) Asociatividad

$$= h_3*(x*y^{-1})$$

Pues $x*y^{-1}=h_2$ ($= h_3 * h_2$

Nos gustaría entonces que esta última expresión estuviera en H (con lo cual nuestra demostración terminaría), o sea, que el "producto" de 2 elementos en H esté en H

Probemos entonces que:

$(\forall h_1, h_2 \in H)\ h_1 * h_2 \in H$ ← Notar que con esto nos basta para concluir nuestra demostración

Notemos que $h_1 R_H e \Leftrightarrow h_1 * e^{-1} \in H \Leftrightarrow h_1 * e \in H \Leftrightarrow h_1 \in H$
└ Pues ($e^{-1} = e$)

y que $e R_H h_2^{-1} \Leftrightarrow e * (h_2^{-1})^{-1} \in H \Leftrightarrow e * h_2 \in H \Leftrightarrow h_2 \in H$

Pero como $h_1 \in H$ y $h_2 \in H$, entonces se cumple que $h_1 R_H e$ y que $e R_H h_2^{-1}$, pero por transitividad de R_H se tiene que $h_1 R_H h_2^{-1}$, lo cual equivale a que $h_1 * (h_2^{-1})^{-1} \in H$, o sea $h_1 * h_2 \in H$. ▨

Nota: Es posible probar que H es un subgrupo de G (¡Hágalo!)

(b) $[x]_{R_H} = \{y \in G / y R_H x\} = \{y \in G / y * x^{-1} \in H\}$

$= \{y \in G / y * x^{-1} = h$ para algún $h \in H\}$

) pues $y * x^{-1} = h \Leftrightarrow y = h * x$ (*)

$= \{y \in G / y = h * x$ para algún $h \in H\}$

Luego, sólo nos basta probar (*), o sea

$$y * x^{-1} = h \Leftrightarrow y = h * x$$

$\Rightarrow]$ $y * x^{-1} = h \quad / * x$

$(y * x^{-1}) * x = h * x$

$y * (x^{-1} * x) = h * x$

$y * e = h * x$

$y = h * x$

$\Leftarrow]$ $y = h * x \quad / * x^{-1}$

$y * x^{-1} = (h * x) * x^{-1}$

$= h * (x * x^{-1})$

$= h * e = h$ ▨

(c) Probar que está bien definida quiere decir en este contexto que la operación $\odot$ es tal que $[x]_{R_H} \odot [y]_{R_H}$ no depende de los representantes que tomemos de las clases $[x]_{R_H}$ y $[y]_{R_H}$ (en este caso los representantes son x e y). Matemáticamente nos piden probar que:

$$[x_1]_{R_H} = [x_2]_{R_H} \text{ y } [y_1]_{R_H} = [y_2]_{R_H} \Rightarrow [x_1]_{R_H} \odot [y_1]_{R_H} = [x_2]_{R_H} \odot [y_2]_{R_H}$$

Dem: Tenemos que $[x_1]_{R_H} = [x_2]_{R_H}$ y $[y_1]_{R_H} = [y_2]_{R_H}$

Luego como $[x_1]_{R_H} = [x_2]_{R_H} \iff x_1 R_H x_2$

y $[y_1]_{R_H} = [y_2]_{R_H} \iff y_1 R_H y_2$

tendremos que $x_1 R_H x_2 \wedge y_1 R_H y_2$, que por la parte (a), implican que $(x_1 * y_1) R_H (x_2 * y_2)$, lo cual equivale a

$$[x_1 * y_1]_{R_H} = [x_2 * y_2]_{R_H}$$

o bien $[x_1]_{R_H} \odot [y_1]_{R_H} = [x_2]_{R_H} \odot [y_2]_{R_H}$) por definición de $\odot$ ■

(δ) Notemos que $[e]_{R_H} \underset{\text{Por parte (b)}}{=} \{ y \in G / y = \underset{=}{h * e}$ para algún $h \in H \}$

$$= \{ h \in H \} = H$$

Ahora probemos que $(G/H, \odot)$ es grupo.

(1) Claramente es l.c.i. pues

$$\left\{ \begin{array}{l} [x] \in G/H \\ [y] \in G/H \end{array} \right. \Rightarrow [x] \odot [y] = [x * y] \in G/H \quad \text{pues } x, y \in G$$

$x, y \in G$

Nota: Omitiré el subíndice R_H para comodidad de escritura.

(2) Es asociativa.

$$([x] \odot [y]) \odot [z] = ([x * y]) \odot [z] = [(x * y) * z]$$
$$= [x * (y * z)] \quad (* \text{ es asociativo})$$
$$= [x] \odot [y * z]$$
$$= [x] \odot ([y] \odot [z])$$

(3) Tiene neutro y es $[e]$ pues:

$$[x] \odot [e] = [x * e] = [x]$$
$$\text{y} \quad [e] \odot [x] = [e * x] = [x]$$

(4) $\forall [x] \in G/H$, $\exists [x]^{-1} = [x^{-1}] \in G/H$ (pues $x^{-1} \in G$) inverso de $[x]$ pues:

$$[x] \odot [x^{-1}] = [x * x^{-1}] = [e]$$
$$[x^{-1}] \odot [x] = [x^{-1} * x] = [e] \rightarrow \text{El neutro en } (G/H, \odot)$$

Luego $(G/H, \odot)$ es un grupo ■

P2 (a) Sea $(G, *)$ un grupo abeliano y $H, K \subseteq G$ subgrupos de G. Se define el conjunto:

$$H * K = \{ h * k \,/\, h \in H, k \in K \} \quad \text{(Control 3, 1998)}$$

Probar que $H * K$ es un subgrupo de G.

(b) Sea $(G, *)$ un grupo tal que $(\forall g \in G)(\exists m \geq 1)$ tal que $g^m = \underbrace{g * g * \ldots * g}_{m \text{ veces}} = e$ (el neutro). Probar que el único homomorfismo $F : (G, *) \to (\mathbb{Z}, +)$ es la función constante $F(g) = 0$ $(\forall g \in G)$ (Control 3, 1998)

(c) Sea $(G,*)$ un grupo que satisface la propiedad:
$(\forall a \in G)\ a*a = e$ (neutro del grupo)
o sea, el inverso de cada elemento del grupo es el mismo elemento. Pruebe que G es un grupo abeliano.
Indicación: Calcule $(a*b)*(b*a)$ (Control 3, 1978)

Solución:

(a) Como $H*K = \{h*k \mid h\in H, k\in K\}$
y $h*k \in G$ (pues $h\in H \subseteq G$ y $k \in K \subseteq G$)
G es cerrado para $*$

$\Rightarrow H*K \subseteq G$.

Ahora $H*K \neq \phi$ pues $\exists h \in H$ $(H\neq\phi)$ y $\exists k \in K$ $(K \neq \phi)$

y por lo tanto $h*k \in H*K$.

Luego solo nos falta probar que si
$$x, y \in H*K \Rightarrow x*y^{-1} \in H*K$$

En efecto $x \in H*K \Rightarrow x = h_1 * k_1$ $\quad h_1, h_2 \in H$
$y \in H*K \Rightarrow y = h_2 * k_2$ $\quad k_1, k_2 \in K$

$$\therefore x*y^{-1} = (h_1*k_1)*(h_2*k_2)^{-1}$$
$$= (h_1*k_1)*(k_2^{-1}*h_2^{-1})$$
$$= \underbrace{(h_1*h_2^{-1})}_{\in H} * \underbrace{(k_1*k_2^{-1})}_{\in K}$$

Reordenando por conmutatividad y agrupando por asociatividad.

$\Rightarrow x*y^{-1} \in H*K$ pues $h_1*h_2^{-1} \in H$, $k_1*k_2^{-1} \in K$. Pues H, K son subgr. de G. ▨

(b) Dado $g \in G$, probaremos que $F(g) = 0$

Como $g \in G$, $\exists m \geq 1$ tal que $\underbrace{g*g*\dots*g}_{m \text{ veces}} = e$ $(*)$

Como F es homomorfismo de $(G,*)$ en $(\mathbb{Z},+)$ tenemos que
$$F(\underbrace{g*\dots*g}_{m \text{ veces}}) \underset{\text{Por homomorfismo.}}{=} \underbrace{F(g)+\dots+F(g)}_{m \text{ veces}} \underset{\text{Por}(*)}{=} F(e) \quad (**)$$

Pero $F(e) = 0$ donde "0" es el neutro en $(\mathbb{Z},+)$
(Los homomorfismos entre grupos envían el neutro en el neutro, y $(\mathbb{Z},+)$ es un grupo)

Luego por $(**)$, $mF(g) = 0$
$\Rightarrow F(g) = 0$ pues $m \neq 0$ $(m \geq 1)$ ▨

(c) Notemos que
$$(a*b)*(b*a) \underset{*\text{ es asociativo}}{=} (a*(b*b))*a = (a*e)*a = a*a = e$$
Propiedad de $(G,*)$

Pero $(a*b)*(a*b) = e$ $\left(\begin{array}{c}\text{Propiedad del problema} \\ (\text{Algo})*(\text{Algo}) = e\end{array}\right)$ (5)

Luego $(a*b)*(b*a) = (a*b)*(a*b)$

$\therefore b*a = a*b$ ← Cancelabilidad (Cancelo $a*b$ por la izquierda) ▨

P3 Sea $f:(\mathbb{Z}_m, \oplus) \to (\mathbb{Z}, +)$ un homomorfismo cualquiera. Demuestre que f es la función constante igual a 0

(Indicación: $\underbrace{[1]\oplus[1]\oplus \dots \oplus[1]}_{m \text{ veces}} = [0]$)

Solución:

$$f(\underbrace{[1]\oplus[1]\oplus\dots\oplus[1]}_{m \text{ veces}}) \underset{\text{Por homomorfismo}}{=} \underbrace{f([1])+\dots+f([1])}_{m \text{ veces}} \underset{\text{Por indicación}}{=} f([0])$$

Pero $f(\underset{\substack{\uparrow \\ \text{El neutro} \\ \text{en } (\mathbb{Z}_m,+)}}{[0]}) = 0$ ← Neutro en $(\mathbb{Z},+)$ pues f es un homomorfismo entre grupos.

Luego $m\, f([1]) = 0 \Rightarrow f([1]) = 0$ (Pues $m \neq 0$)

Finalmente:

$$f([k]) = f(\underbrace{[1]\oplus\dots\oplus[1]}_{k \text{ veces}}) = k f([1]) = 0$$ ← pues $f([1]) = 0$

Esto último es $\forall [k] \in \mathbb{Z}_m$ ▨

Observación: En el **P2** (b) y en la **P3** he usado el siguiente hecho: Si (A, Δ) es una estructura algebraica y $(G,*)$ es un grupo, entonces si

$f:(A,\Delta) \to (G,*)$ es un morfismo,

se tiene que $f(\varepsilon) = e$ donde $\varepsilon \in A$ es neutro para Δ y $e \in B$ es neutro para $*$

Es "notable" el hecho de que no sea necesario que f sea sobreyectiva cuando el conjunto de llegada es un grupo. (Notar que sobre el conjunto de partida no hay mayores exigencias que ser estructura y tener neutro ε.)

P4 Dado $(G,*)$ un grupo y H subgrupo de G, definamos para $a \in G$, $b \in G$

$$a*H = \{a*h \,/\, h \in H\} \qquad H*b = \{h*b \,/\, h \in H\}$$

Pruebe que:

(a) Si $c \in G$, entonces $c \in H \Leftrightarrow c*H = H$

(b) $a*H \cap b*H \neq \phi \Rightarrow a*H = b*H$.
(c) Sea $\mathcal{F}: G \to G$ un homomorfismo y definamos $H = \{a \in G \mid \mathcal{F}(a) = e\}$ donde e es el neutro de G. Pruebe que H es un subgrupo de G y que $\forall a \in G,\ a*H = H*a$

(Control N° 3, 1990)

Solución:

(a) Pdq $c \in H \Leftrightarrow c*H = H$

($\Rightarrow$) Dado $c \in H$, nuestro objetivo es probar que $c*H = H$

(1) $c*H \subset H$. Sea $x \in c*H \Rightarrow x = \underbrace{c}_{\in H} * \underbrace{h}_{\in H}$ con $h \in H$

Luego $x \in H$ (Pues H es subgrupo)

(2) $H \subseteq c*H$. Si $x \in H \Rightarrow x = h$ con $h \in H$

y $x = c*(\underbrace{c^{-1}}_{\in H} * \underbrace{h}_{\in H})$ ← esto vale h

H subgrupo.

$\Rightarrow x \in c*H$.

($\Leftarrow$) Si $c*H = H$, nuestro objetivo es probar que c...
Como $e \in H$ (H subgrupo)

$\Rightarrow c*e \in c*H \subseteq H \Rightarrow \underbrace{c*e}_{c} \in H$ ▨

(b) Pdq $a*H \cap b*H \neq \phi \Rightarrow a*H = b*H$
Notemos que $a*H \cap b*H \neq \phi$ quiere decir que $\exists x$ tal que $x \in [a*H \cap b*H] \Leftrightarrow x \in a*H \wedge x \in b*H$.
Luego $x = a*h_1 = b*h_2$ para algún $h_1, h_2 \in H$.
Probemos ahora que $a*H = b*H$.

(1) $a*H \subseteq b*H$. Sea $\mu \in a*H \Rightarrow \mu = a*h$ ($h \in H$)

$$\overset{(*)}{\Rightarrow} \mu = (b*h_2*h_1^{-1})*h = b*\underbrace{(\underbrace{h_2}_{\in H} * \underbrace{h_1^{-1}}_{\in H} * \underbrace{h}_{\in H})}_{\in H \text{ (H subgrupo)}} \in b*H$$

(*) Esto es pues
$a*h_1 = b*h_2 \quad /*h_1^{-1}$

$\Rightarrow \underbrace{(a*h_1)*h_1^{-1}}_{\underbrace{a*\underbrace{(h_1*h_1^{-1})}_{e}}_{a}} = b*h_2*h_1^{-1} \Rightarrow a = b*h_2*h_1^{-1}$

(2) $b*H \subseteq a*H$. Analogamente $a*h_1 = b*h_2 \quad /*h_2^{-1}$
$a*h_1*h_2^{-1} = b$

Luego si $\mu \in b*H \Rightarrow \mu = b*h$ ($h \in H$) $\Rightarrow \mu = (a*h_1*h_2^{-1})*h$

$$\Rightarrow \mu = a * (\underbrace{\underbrace{h_1}_{\in H} * \underbrace{h_2^{-1}}_{\in H} * \underbrace{h}_{\in H}}_{\in H \ (H \text{ subgrupo})}) \in a * H. \quad ■$$

(c) Probemos que H es subgrupo de G

(1) $H \subseteq G$ ✓

(2) $H \neq \phi$ pues $e \in H$ ya que $F(e) = e$ (Pues F homomorfismo y el espacio de llegada es un grupo)

(3) $\forall h_1, h_2 \in H \Rightarrow h_1 * h_2^{-1} \in H$

En efecto, si $h_1 \in H \Rightarrow F(h_1) = e$

$h_2 \in H \Rightarrow F(h_2) = e$

Luego $h_1 * h_2^{-1} \in H$ pues $F(h_1 * h_2^{-1}) \overset{F \text{ es homomorfismo}}{=} F(h_1) * F(h_2^{-1})$

$\overset{(*)}{=} F(h_1) * (F(h_2))^{-1}$

$= e * \underbrace{e^{-1}}_{e} = e$

En la cual a tiene inverso a^{-1} ← estructura

(*) He usado el hecho de que si $f : (A, \Delta) \to (G, *)$ es un homomorfismo, entonces $(f(a))^{-1} = f(a^{-1})$

Grupo

Finalmente probamos que $a * H = H * a$ (Nuevamente no necesito epiyectividad)

(1) $a * H \subseteq H * a$. Sea $x \in a * H$

$\Rightarrow x = a * h \quad (h \in H)$

$F(h) = e$

Yo quiero:
$x \in H * a \Leftrightarrow x = \tilde{h} * a$
o sea $a * h = \tilde{h} * a \ / \cdot a^{-1}$
$a * h * a^{-1} = \tilde{h}$

$\tilde{h} \in H$

$\Rightarrow x = (\underbrace{a * h * a^{-1}}_{\tilde{h}}) * a \in H * a$

Notar que es igual a $a * h$

siempre y cuando $\tilde{h} \in H$, o sea $F(\tilde{h}) = e$

Pero $F(\tilde{h}) = F(a * h * a^{-1})$

$= F(a) * F(h) * F(a^{-1})$

$= F(a) * e * F(a^{-1})$

$= F(a) * (F(a))^{-1} = e$

(2) $H * a \subseteq a * H$. Análogamente sea $x \in H * a$

$\Rightarrow x = h * a$ con $h \in H$ $(F(h) = e)$

Se razona en forma análoga $\Rightarrow x = a * (\underbrace{a^{-1} * h * a}_{\tilde{h}}) \in a * H$

pues $\tilde{h} \in H$ ya que

$F(\tilde{h}) = F(a^{-1}) * F(h) * F(a) \overset{\text{en forma análoga.}}{=} e$ ■

P5 Sea $(G,*)$ un grupo y G' un subgrupo de G. Sea $f: G \to G$ un homomorfismo de grupos que satisface la propiedad $f(G') \subseteq G'$. Se define el conjunto

$$V = \{g \in G \mid \exists m \in \mathbb{N},\ f^m(g) \in G'\}$$

donde f^m es la composición de f con sí misma m veces y $f^0 = id_G$. Probar que V es un subgrupo de G.

Indicación: Pruebe que:

$$f^m(g) \in G' \Rightarrow f^{m+1}(g) \in G' \qquad g \in G,\ m \in \mathbb{N}$$

Concluir que si $f^m(g) \in G' \Rightarrow (\forall m \geq m)\ f^m(g) \in G'$

(Control Recuperativo, 1998)

Solución:

Probemos primero la indicación:

Si $f^m(g) \in G' \Rightarrow f^{m+1}(g) = f(\underbrace{f^m(g)}_{\in G'})$

Luego $f^{m+1}(g) \in f(G') \subseteq G'$

Imagen — Propiedad del problema

$\therefore f^{m+1}(g) \in G'$. Luego hemos probado que:

$$f^m(g) \in G' \Rightarrow f^{m+1}(g) \in G'$$

pero entonces $f^{m+1}(g) \in G' \Rightarrow f^{m+2}(g) \in G'$

y $f^{m+2}(g) \in G' \Rightarrow f^{m+3}(g) \in G'$

o sea $f^m(g) \in G' \Rightarrow f^{m+1}(g) \in G' \wedge f^{m+2}(g) \in G' \wedge f^{m+3}(g) \in G' \wedge \cdots \wedge f^m(g) \in G'$

$\Leftrightarrow (\forall m \geq m)\ f^m(g) \in G'$

Pdq: V subgrupo de G

① $V \subseteq G$ ✓

② $V \neq \phi$ pues $G' \subseteq V$ ya que si $g \in G' \Rightarrow \exists m = 0$ tal que $f^0(g) = g$ ($id(g)$)

y $f^0(g) \in G'$

Esto es lo importante.

$\Rightarrow g \in V$

③ Sabemos que la composición de homomorfismos es homomorfismo por lo cual f^m es un homomorfismo, o sea

$$f^m(g_1 * g_2) = f^m(g_1) * f^m(g_2)$$

Probaremos finalmente que si $g_1, g_2 \in V$ se tendrá que $g_1 * g_2^{-1} \in V$

Luego basta encontrar un $m \in \mathbb{N}$ tal q.:
$f^m(g_1 * g_2^{-1}) \in G'$ ← La condición para estar en V

Ahora como $g_1, g_2 \in V$, $\exists m_1, m_2 \in \mathbb{N}$ tal que
$$f^{m_1}(g_1) \in G' \text{ y } f^{m_2}(g_2) \in G'$$
Si $m = \max\{m_1, m_2\}$ que es mayor o igual a m_1 y a m_2 se tendrá por la indicación (que ya probamos) que:
$$f^m(g_1) \in G' \text{ y } f^m(g_2) \in G'$$
Ahora verifiquemos que este es el m buscado:
$$\underset{\uparrow}{f^m(g_1 * g_2^{-1}) =} f^m(g_1) * f^m(g_2^{-1}) \underset{\uparrow}{=} f^m(g_1) * (f^m(g_2))^{-1}$$
f^m homomorfismo — Propiedad de los homomorfismos donde el conjunto de "llegada" es un "grupo"

y como $f^m(g_1) \in G'$, $f^m(g_2) \in G'$ (Luego $(f^m(g_2))^{-1} \in G'$ ← G' subgrupo de G.)
y G' es cerrada para la operación $*$
$$\therefore f^m(g_1 * g_2^{-1}) \in G' \quad ▨$$
G' subgrupo de G.

---

* **P6** Sea $(G, *)$ un grupo y $f: G \to G$
$$g \to f(g) = g^{-1}$$
Probar que f es isomorfismo $\Leftrightarrow$ G es grupo abeliano.

(Control 3, 1996)

Solución:

· Notar que f tiene sentido pues g^{-1} existe (G es grupo) y vive en G. Notemos además que f es biyectiva pues tiene inversa (que por cierto es ella misma) pues:
$$(f \circ f)(g) = f(f(g)) = f(g^{-1}) = (g^{-1})^{-1} = g$$
$$\text{o sea } f \circ f = id_G$$

Luego nuestro problema se reduce pues
$$f \text{ isomorfismo} \Leftrightarrow f \text{ homomorfismo} \wedge \overbrace{f \text{ biyectiva}}^{V}$$
$$\Leftrightarrow f \text{ homomorfismo.}$$
Así solo basta probar que f homomorfismo $\Leftrightarrow$ G es un grupo abeliano.

($\Leftarrow$) Pdq: f homomorfismo, o sea
$$f(a * b) = f(a) * f(b)$$
Pues "$*$" es la operación que "manda" en el conjunto de partida y en el de llegada

Pero $f(a*b) = (a*b)^{-1} = b^{-1}*a^{-1} = a^{-1}*b^{-1} = f(a)*f(b)$
$\uparrow$ Pues G es grupo abeliano.

$(\Rightarrow)$ Si f homomorfismo $\Rightarrow f(a*b) = f(a)*f(b)$
(Pdq: G abeliano) $\Leftrightarrow (a*b)^{-1} = a^{-1}*b^{-1}$
$\Leftrightarrow b^{-1}*a^{-1} = a^{-1}*b^{-1}$ $(*)$

Pdq: $x*y = y*x$ $(\forall x, y \in G)$
Evaluando en $(*)$ $\rightarrow$ $a = x^{-1}$, $b = y^{-1}$ $\rightarrow (y^{-1})^{-1}*(x^{-1})^{-1} = (x^{-1})^{-1}*(y^{-1})^{-1}$
$\Rightarrow y*x = x*y$ ▨

P-7 Considere $\mathbb{Z}_2 \times \mathbb{Z}_3$ con la operación definida por
$(a,b) \oplus (c,d) = (a +_2 c, b +_3 d)$
(a) Pruebe que $(\mathbb{Z}_2 \times \mathbb{Z}_3, \oplus)$ es un grupo.
(b) Construya un isomorfismo $f: (\mathbb{Z}_6, +_6) \rightarrow (\mathbb{Z}_2 \times \mathbb{Z}_3, \oplus)$ tal que $f([1]_6) = ([1]_2, [1]_3)$. Concluya que es único
(Control 3, 1996)

Solución:
(a) Pdq: $(\mathbb{Z}_2 \times \mathbb{Z}_3, \oplus)$ es grupo.
(Sabemos que $(\mathbb{Z}_2, +_2)$ y $(\mathbb{Z}_3, +_3)$ son grupos)
① $\oplus$ es l.c.i. en $\mathbb{Z}_2 \times \mathbb{Z}_3$ pues en cada componente actua una l.c.i.
② $\oplus$ es asociativa: ¡Pruebenlo ustedes! (Es porque se tiene asociatividad en cada componente)
③ Elemento Neutro: Este es $([0]_2, [0]_3)$ pues
$$([a]_2, [b]_3) \oplus ([0]_2, [0]_3) = ([a]_2 +_2 [0]_2, [b]_3 +_3 [0]_3)$$
$$= ([a+0]_2, [b+0]_3)$$
$$= ([a]_2, [b]_3)$$
Análogamente $([0]_2, [0]_3) \oplus ([a]_2, [b]_3) = ([a]_2, [b]_3)$
④ Inverso: Dado $([a]_2, [b]_3) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ su inverso es $([-a]_2, [-b]_3) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ pues
$$([a]_2, [b]_3) \oplus ([-a]_2, [-b]_3) = ([a]_2 +_2 [-a]_2, [b]_3 +_3 [-b]_3)$$
$$= ([a-a]_2, [b-b]_3)$$
$$= ([0]_2, [0]_3) \leftarrow \text{el neutro}$$
Analogamente $([-a]_2, [-b]_3) \oplus ([a]_2, [b]_3) = ([0]_2, [0]_3) \leftarrow$
Luego $(\mathbb{Z}_2 \times \mathbb{Z}_3, \oplus)$ es grupo (de hecho es abeliano)
¡Convencerse! ▨

(b) Recordemos que
$$\mathbb{Z}_6 = \{[0]_6, [1]_6, \ldots, [5]_6\}$$
$$\mathbb{Z}_2 = \{[0]_2, [1]_2\}$$
$$\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$$

Luego $|\mathbb{Z}_6| = 6$ y $|\mathbb{Z}_2 \times \mathbb{Z}_3| = 6$. Luego tiene sentido buscar un isomorfismo (pues tendrá que ser en particular biyectivo y por lo tanto el conjunto de partida y llegada tendrán el mismo "cardinal"). (11)

Como es un isomorfismo, en particular será un homomorfismo el cual lleva el neutro de $\mathbb{Z}_6$ al neutro de $\mathbb{Z}_2 \times \mathbb{Z}_3$ (Pues $(\mathbb{Z}_2 \times \mathbb{Z}_3, \oplus)$ es un grupo)

conjunto de llegada ← Parte (a)

Luego $f([0]_6) = ([0]_2, [0]_3)$ y por enunciado
$$f([1]_6) = ([1]_2, [1]_3)$$

Así
$$f([2]_6) = f([1]_6 +_6 [1]_6) = f([1]_6) \oplus f([1]_6)$$
$$= ([1]_2, [1]_3) \oplus ([1]_2, [1]_3)$$
$$= ([2]_2, [2]_3) = ([0]_2, [2]_3)$$

Analogamente:
$$f([3]_6) = f([1]_6 +_6 [1]_6 +_6 [1]_6) = f([1]_6) \oplus f([1]_6) \oplus f([1]_6)$$

análogo al calculo de $f([2]_6)$ $\rightarrow$ $= ([3]_2, [3]_3) = ([1]_2, [0]_3)$

$$f([4]_6) = ([4]_2, [4]_3) = ([0]_2, [1]_3)$$
$$f([5]_6) = ([5]_2, [5]_3) = ([1]_2, [2]_3)$$

y notamos que
$$\underbrace{f([6]_6)}_{f([0]_6)} = ([6]_2, [6]_3) = ([0]_2, [0]_3)$$
← Es consistente con el principio.

Como vemos existe una única forma de asigna a cada elemento de $\mathbb{Z}_6$ un elemento de $\mathbb{Z}_2 \times \mathbb{Z}_3$ (uno distinto para cada elemento de $\mathbb{Z}_6$) por lo que la fn. f es biyectiva y es tal que:
$$f([k]_6) = ([k]_2, [k]_3)$$

Luego es un homomorfismo pues
$$f([k_1]_6 +_6 [k_2]_6) = f([k_1 + k_2]_6)$$
$$= ([k_1 + k_2]_2, [k_1 + k_2]_3) = ([k_1]_2 + [k_2]_2, [k_1]_3 + [k_2]_3)$$
$$= ([k_1]_2, [k_1]_3) \oplus ([k_2]_2, [k_2]_3)$$ ← Por definición de $\oplus$
$$= f([k_1]_6) \oplus f([k_2]_6)$$

Finalmente como f es homomorfismo y es biyectiva, entonces f es un isomorfismo ▨

P8 Sea $(G, *)$ un grupo con neutro $e \in G$. Se define el conjunto A por:
$$A = \{F : G \to G \,/\, F \text{ es un isomorfismo de } (G,*) \text{ en } (G,*)\}$$

i) Probar que $(A, \circ)$ es un grupo ("$\circ$" es la composición de funciones)

ii) Para cada $g \in G$ se define la fn. $F_g : G \to G$ tal que $F_g(x) = g * x * g^{-1}$. Pruebe que:

a) F_g es un homomorfismo de $(G,*)$ en $(G,*)$.

b) $F_{g*h} = F_g \circ F_h$ para todo $g, h \in G$

c) $F_e = id_G$

Concluya que F_g es un isomorfismo y que $(F_g)^{-1} = F_{g^{-1}}$ para todo $g \in G$.

iii) Pruebe que $B = \{F_g / g \in G\}$ es un subgrupo de $(A, \circ)$.

(Control 3, 1997)

Solución:

i) ① "$\circ$" es l.c.i. en A, o sea $f, g \in A \Rightarrow f \circ g \in A$

Como $f, g \in A$, entonces $f : G \to G$, $g : G \to G$, f, g biyectivas y f, g homomorfismos.

Notemos que $f \circ g : G \to G$ es biyectiva (Pues es composición de biyectivas). Solo queda probar que $f \circ g$ es un homomorfismo (o sea que composición de homomorfismos es homomorfismo ← Este hecho lo asumí en la P5)

Sean $x_1, x_2 \in G \Rightarrow (f \circ g)(x_1 * x_2) = f(g(x_1 * x_2))$ (g es homomorfismo)

$= f(g(x_1) * g(x_2))$ (f es homomorfismo)

$= f(g(x_1)) * f(g(x_2))$

$= (f \circ g)(x_1) * (f \circ g)(x_2)$

② "$\circ$" asociativa en A. La composición de funciones es asociativa, en particular las de A cumplen la propiedad asociativa.

③ Elemento neutro.

Buscamos $\tilde{f} : G \to G$ isomorfismo (o sea $\tilde{f} \in A$) tal que $\forall f \in A$ $\quad f \circ \tilde{f} = \tilde{f} \circ f = f$. (*)

Entonces pensamos en $\tilde{f} = id_G$ que satisface (*) por lo que solo debemos probar que es un isomorfismo!

Pero id_G es biyectiva y

$$id_G(x_1 * x_2) = x_1 * x_2 = id_G(x_1) * id_G(x_2)$$ //

④ Inversos.

Dado $f \in A$ ($f : G \to G$ un isomorfismo) necesitamos dar con un maravilloso $\hat{f} \in A$ tal que

(*) $\quad f \circ \hat{f} = \hat{f} \circ f = id_G$ ← Neutro de $(A, \circ)$

Sabemos que $\hat{f} = f^{-1}$ satisface (*) así que solo probaremos que es un isomorfismo.

Pero f^{-1} es biyectiva (pues f lo es) y solo nos queda probar que f^{-1} es un homomorfismo (seguramente usando el hecho de que f es un homomorfismo.), es decir $(\forall x_1, x_2 \in G)\ f^{-1}(x_1 * x_2) = f^{-1}(x_1) * f^{-1}(x_2)$ (Nota: $f^{-1}: G \to G$)

Sea $u = f^{-1}(x_1)$ y $v = f^{-1}(x_2)$

$\therefore f(u) = x_1$ y $f(v) = x_2$

Luego $f^{-1}(x_1 * x_2) = f^{-1}(f(u) * f(v)) \overset{\text{pues } f \text{ homomorfismo}}{=} f^{-1}(f(u * v))$

$= u * v$

$= f^{-1}(x_1) * f^{-1}(x_2)$ ...

ii) a) Pdq: $F_g(x_1 * x_2) = F_g(x_1) * F_g(x_2)\quad \forall x_1, x_2 \in G$

En efecto: $F_g(x_1) * F_g(x_2) = (g * x_1 * g^{-1}) * (g * x_2 * g^{-1})$

$= g * x_1 * (g^{-1} * g) * x_2 * g^{-1}$

asociatividad $= g * (x_1 * e) * x_2 * g^{-1}$

$= g * (x_1 * x_2) * g^{-1} = F_g(x_1 * x_2)$

b) Pdq: $F_{g*h}(x) = (F_g \circ F_h)(x)\quad \forall x \in G$

En efecto $(F_g \circ F_h)(x) = F_g(F_h(x)) = F_g(h * x * h^{-1})$

$= g * (h * x * h^{-1}) * g^{-1}$

asociatividad $= (g * h) * x * (h^{-1} * g^{-1})$

$= (g * h) * x * (g * h)^{-1}$

$= F_{g*h}(x)$

c) $F_e(x) = e * x * e^{-1} \overset{e^{-1} = e}{=} e * x * e = x = id_G(x)$

$\therefore F_e = id_G$

Finalmente veamos que F_g es un isomorfismo.

En efecto veamos que

$F_g \circ F_{g^{-1}} = F_{g * g^{-1}} = F_e = id_G$

y $F_{g^{-1}} \circ F_g \underset{(b)}{=} F_{g^{-1} * g} = F_e \underset{(c)}{=} id_G$

o sea F_g tiene inversa igual a $F_{g^{-1}}$ (o sea $(F_g)^{-1} = F_{g^{-1}}$) y por lo tanto es biyectiva y por (a), F_g es un homomorfismo y por lo tanto es un isomorfismo. ▨

iii) Pdq: $B = \{F_g / g \in G\}$ es un subgrupo de $(A, \circ)$

(1) $B \subseteq A$ pues probamos que los F_g son isomorfismos. Como A contiene a todos los isomorfismos, en particular debe tener a los de B.

(2) $B \neq \phi$. Como G grupo $\Rightarrow e \in G$. Luego $F_e \in B$, o sea $id_G \in B$. $\therefore B \neq \phi$.

③ Sean $F_g, F_h \in B$. Pdq $F_g \circ (F_h)^{-1} \in B$

Pero $F_g \circ (F_h)^{-1} \underset{\substack{\uparrow \\ \text{Por parte (2)}}}{=} F_g \circ F_{h^{-1}} \underset{\substack{\uparrow \\ \text{Por (b)}}}{=} F_{g*h^{-1}} \underset{\substack{\uparrow \\ \text{pues } g*h^{-1}\in G \\ \text{ya que } g,h\in G \\ \text{y } G \text{ es grupo}}}{\in} F$

$\therefore (B, \circ)$ es un subgrupo de $(A, \circ)$. ∎

---

* **P9** Sea $(G, *)$ un grupo, X un conjunto no vacío y una función $\varphi : G \times X \to X$

$$(g, x) \to \varphi(g, x)$$

Denotaremos $\varphi(g, x)$ por $g \cdot x$. Supongamos que φ satisface:

a) $(\forall x \in X)\ e \cdot x = x$, e neutro de $(G, *)$

b) $(\forall x \in X)(\forall g, h \in G)\ g \cdot (h \cdot x) = (g * h) \cdot x$

Dado $x_0 \in X$, sea $H_{x_0} = \{g \in G \,/\, g \cdot x_0 = x_0\}$

(i) Pruebe que H_{x_0} es un subgrupo de $(G, *)$

(ii) Sean $x_0, y_0 \in X$, $g_0 \in G$ tales que $g_0 \cdot x_0 = y_0$. Demuestre que:

$$H_{x_0} = \{g_0^{-1} * h * g_0 \,/\, h \in H_{y_0}\}$$

(iii) Sea R_{x_0} la relación de equivalencia en G definida por $g R_{x_0} h \iff g^{-1} * h \in H_{x_0}$

(iii.1) Pruebe que $(\forall g, h \in G)\ [g] = [h] \Rightarrow g \cdot x_0 = h \cdot x_0$

Considere

$$f : G/R_{x_0} \to X$$
$$[g] \to g \cdot x_0$$

(iii.2) Demuestre que f es inyectiva.

(iii.3) Suponga que se verifica que:

$$(\forall x, y \in X)(\exists g \in G)\ y = g \cdot x$$

Pruebe que entonces f es biyectiva

(Control 3, 1992)

Solución:

(i) Notemos previamente que $g \cdot x = y \Rightarrow x = g^{-1} \cdot y$

Esto es debido a que $g \cdot x = y \ / \ g^{-1} \cdot$ $\quad g \in G$, $x, y \in X$

Por (b)

$$\Rightarrow g^{-1} \cdot (g \cdot x) = g^{-1} \cdot y$$
$$\Rightarrow (g^{-1} * g) \cdot x = g^{-1} \cdot y$$
$$\Rightarrow \underbrace{e \cdot x = x}_{\text{por (a)}} = g^{-1} \cdot y$$

Probemos ahora que H_{x_0} es subgrupo de $(G, *)$.

① $H_{x_0} \subseteq G$ ✓
② $H_{x_0} \neq \phi$ pues $e \in H_{x_0}$ ya que $e \cdot x_0 = x_0$ (Por (a))
③ Pdq: $g_1, g_2 \in H_{x_0} \Rightarrow g_1 * g_2^{-1} \in H_{x_0}$
Pero $g_1, g_2 \in H_{x_0} \Rightarrow g_1 \cdot x_0 = x_0 \wedge \underbrace{g_2 \cdot x_0 = x_0}$

$\Rightarrow g_2^{-1} \cdot x_0 = x_0$ (Propiedad ya probada)

Luego $g_1 * g_2^{-1} \in H_{x_0}$ pues $(g_1 * g_2^{-1}) x_0 \underset{\text{Por (b)}}{=} g_1 \cdot (g_2^{-1} \cdot x_0)$
$= g_1 \cdot x_0 = x_0$ ■

(ii) Sea $\zeta = \{g_0^{-1} * h * g_0 / h \in H_{y_0}\}$. Probemos que $\zeta = H_{x_0}$,
o sea $\zeta \subseteq H_{x_0}$ y $H_{x_0} \subseteq \zeta$
① $\zeta \subseteq H_{x_0}$. $x \in \zeta \Rightarrow x = g_0^{-1} * h * g_0$ para $\underbrace{\text{algún } h \in H_{y_0}}$ $\Rightarrow h \cdot y_0 = y_0$
Pdq $x \in H_{x_0}$, o sea:
$x \cdot x_0 = x_0$
Efectivamente $x \cdot x_0 = ((g_0^{-1} * h) * g_0) \cdot x_0$
$= (g_0^{-1} * h) \cdot (g_0 \cdot x_0)$ ↩ Por (b)
$= (g_0^{-1} * h) \cdot y_0$ ↩ Hipótesis del problema.
$= g_0^{-1} \cdot (h \cdot y_0)$
$= g_0^{-1} \cdot y_0$ ⟵ Pero $g_0 \cdot x_0 = y_0 \Rightarrow x_0 = g_0^{-1} \cdot y_0$ (*)
$= x_0$ //

imagínenlo como un $(a * g_0) \cdot x_0 = a \cdot (g_0 \cdot x_0)$ con $a = g_0^{-1} * h$

② $H_{x_0} \subseteq \zeta$. Sea $x \in H_{x_0}$, o sea $x \cdot x_0 = x_0$
Pdq $x \in \zeta$, o sea que es de la forma $g_0^{-1} * h * g_0$ para algún $h \in H_{y_0}$

Notamos que $x = g_0^{-1} * \underbrace{(g_0 * x * g_0^{-1})}_{h} * g_0$

$x = g_0^{-1} * h * g_0 \quad / g_0 * (\ ) * g_0^{-1}$
$\Rightarrow h = g_0 * x * g_0^{-1}$

Luego solo basta probar que $h \in H_{y_0}$, o sea $h \cdot y_0 = y_0$. En efecto:
$((g_0 * x) * g_0^{-1}) \cdot y_0 = (g_0 * x) \cdot (g_0^{-1} \cdot y_0)$
$= (g_0 * x) \cdot (x_0)$ ↩ Por (*)
$= g_0 \cdot (x \cdot x_0)$ ↩ Por (b)
$= g_0 \cdot x_0$ ↩ Pues $x \in H_{x_0}$
$= y_0$ ↩ Enunciado del Problema. ■

Mismo argumento usado antes

(iii) (iii.1) Si $[g] = [h] \Rightarrow g R_{x_0} h \Rightarrow g^{-1} * h \in H_{x_0}$
$\overset{(b)}{\Rightarrow} (g^{-1} * h) \cdot x_0 = x_0$
$\Rightarrow g^{-1} \cdot (h \cdot x_0) = x_0$
$\Rightarrow h \cdot x_0 = g \cdot x_0$ ■

Propiedad probada al principio.

(iii.2) Pdq $f([g]) = f([h]) \Rightarrow [g]=[h]$

Pero si $f([g]) = f([h]) \Rightarrow g\cdot x_0 = h\cdot x_0$

Propiedad probada al principio. $\Rightarrow x_0 = g^{-1}\cdot(h\cdot x_0)$) Por (t.)

$\Rightarrow x_0 = (g^{-1}*h)\cdot x_0$

$\Rightarrow g^{-1}*h \in H_{x_0}$

$\Rightarrow g\, R_{x_0}\, h \Rightarrow [g]=[h]$

(iii.3) Pdq $(\forall y\in X)(\exists [g]\in G/R_{x_0})\ f([g])=y$

En efecto, dado $y\in X$ y $x_0\in X$ (el de la relación)

$\therefore\ \exists \tilde{g} \in G$ tal que $y=\tilde{g}\cdot x_0$ (Por propiedad del enunciado)

Entonces la clase a tomar en G/R_{x_0} es justamente la que tiene a $\tilde{g}$ como representante pues

$$f([\tilde{g}]) = \tilde{g}\cdot x_0 = y \quad \blacksquare$$

Notar que (iii.1) nos dice que la fn. f está bien definida

P10 Sea $(G,*)$ un grupo con neutro e tal que G es finito

(i) Para $h\in G$ cualquiera pruebe que

$$f: \mathbb{N} \to G \text{ tal que } f(m) = h^m = \underbrace{h*\dots*h}_{m \text{ veces}}$$

no es inyectiva. Concluya que $\exists m>0$ tal que $h^m = e$.

(ii) Sea $H\subseteq G$, $H\neq\emptyset$ tal que si $h, h'\in H \Rightarrow h*h'\in H$

(ii.1) Pruebe que si $h\in H$, entonces $h^{-1}\in H$

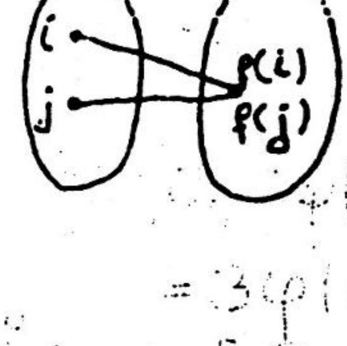
(ii.2) Concluya que H es un subgrupo de G.

(Control Recuperativo, 2001)

Solución:

(i) Si f fuera inyectiva $\Rightarrow |\mathbb{N}| < \underbrace{|G|}_{\text{finito}}$ $(\rightarrow\!\times\!\leftarrow)$

Luego f no es inyectiva, por lo que $\exists\, i,j\in\mathbb{N}$ $(i\neq j)$ tal que $f(i)=f(j)$



Luego $h^i = h^j$ y supongamos $i>j$ (No hay pérdida de generalidad)

$\Rightarrow h^{i-j} * h^j = h^j$) Por cancelabilidad (G un grupo)

$\Rightarrow h^{i-j} = e$

con $i-j>0$

Luego el m buscado es $i-j\in\mathbb{N}$. $(i-j = m > 0)$

(ii) (ii.1) Si $h\in H$, $\exists m>0$ tq $h^m = e$

Luego $h * h^{m-1} = h^{m-1} * h = e$

Por unicidad del inverso, h^{m-1} es el inverso de h

Pdq $h^{m-1}\in H$.

Hay 2 casos (como $m>0$)
① $m=1$ ② $m>1$

Si $m=1$ hay que probar que $h^0 = e \in H$
Pero $e = h^m$ ($m>0$) que es producto de elementos de H, por lo que por propiedad de enunciado $\underbrace{h^m}_{e} \in H$ (con $m>0$)

Si $m>1$ ($m-1>0$), hay que probar que $h^{m-1} \in H$.
Pero por la misma propiedad anterior h^{m-1} está en H por ser producto de elementos de H. ← pues $(m-1)>0$.

(ii.2) Por lo anterior, $e \in H \Rightarrow H \neq \phi$
y por enunciado $H \subseteq G$
Luego basta probar que $\forall h_1, h_2 \in H \Rightarrow h_1 * h_2^{-1} \in H$
Pero $h_2 \in H \Rightarrow h_2^{-1} \in H$ (Por (ii.1))
y por lo tanto $h_1, h_2^{-1} \in H$. Luego $h_1 * h_2^{-1} \in H$
(por prop. del enunciado)

Notar: que en el fondo hemos probado que para grupos finitos (H) solo basta probar la cerradura de la operación $*$ en H.

P11 (Propuesto)

(a) Sea $(G,*)$ un grupo que verifica la propiedad $(\forall a,b \in G)$ $(a*b)^2 = a^2 * b^2$. Probar que $(G,*)$ es un grupo abeliano.

(b) Sean $G = \{f: \mathbb{R} \to \mathbb{R} / \exists a,b \in \mathbb{R}, a \neq 0, f(x) = ax+b\}$ y $\bar{G} = \{f: \mathbb{R} \to \mathbb{R} / \exists b \in \mathbb{R}, f(x) = x+b\}$. Sabiendo que $(G,\circ)$ es un grupo, probar que $(\bar{G},\circ)$ es un subgrupo de $(G,\circ)$
(Control Recuperativo, 1996)

P12 (Desafío)

Sea $(G,*)$ un grupo que satisface las siguientes propiedades:

(I) $(a*b)^2 = (b*a)^2$ para todo $a,b \in G$
(II) $x^2 = e \Rightarrow x = e$ (e neutro para $*$ en G)

Probar que $(G,*)$ es un grupo abeliano.

Indicación: Si pudieran demostrar que $(a*b*a^{-1}*b^{-1})^2 = e$ tendrían que $a*b*a^{-1}*b^{-1} = e$ (Por la propiedad II)
Pero $a*b*a^{-1}*b^{-1} = e \Leftrightarrow a*b = b*a$.

P13 Sea $(G,*)$ un grupo con neutro $e \in G$. Sea $\leq$ una relación de orden sobre G tal que:

$$(\forall x,y,z \in G)(x \leq y) \Rightarrow (x*z \leq y*z)$$

Sean $G_+ = \{x \in G / e \leq x\}$ y $G_- = \{x \in G / x \leq e\}$

Demuestre que:

(a) $G_+ \cap G_- = \{e\}$

(b) $(\forall x \in G)(x \in G_+ \Rightarrow x^{-1} \in G_-)$

(c) $(G_+,*)$ es una estructura algebraica.

(d) Si la relación de orden $\leq$ es total, entonces $G_+ \cup G_- = G$

Observación.. Una relación de orden R en un conjunto A se dice total cuando $(\forall x,y \in A)$ xRy v yRx

(e) Si $G_+ \cup G_- = G$, entonces la relación de orden $\leq$ es total.

(Control 3, 2002)

Solución:

(a) Notemos que $e \in G_+$ pues $e \leq e$ ($\leq$ es refleja)

Además $e \in G_-$ pues $e \leq e$ ($\leq$ es refleja)

$\Rightarrow \{e\} \subseteq G_+ \cap G_-$

Falta demostrar que $G_+ \cap G_- \subseteq \{e\}$. Sea $x \in G_+ \cap G_-$

Luego $x \in G_+ \wedge x \in G_- \Rightarrow e \leq x \wedge x \leq e \Rightarrow x = e$ ($\leq$ es antisimétrica)

$\Rightarrow x \in \{e\}$. $\therefore G_+ \cap G_- \subseteq \{e\}$

Finalmente $G_+ \cap G_- = \{e\}$ ▨

(b) Sea $x \in G_+ \Rightarrow e \leq x \Rightarrow e * x^{-1} \leq x * x^{-1} \Rightarrow x^{-1} \leq e$

$\Rightarrow x^{-1} \in G_-$ ▨

Por propiedad del enunciado (con $z = x^{-1}$)

(c) Hay que probar la cerradura de $*$ sobre G_+

Sean $a,b \in G_+$. Pdq $a*b \in G_+$

Dem: Como $a,b \in G_+ \Rightarrow e \leq a \wedge e \leq b$

Pero $e \leq a \Rightarrow e*b \leq a*b \Rightarrow b \leq a*b$

Prop. del enunciado con $z = b$

Por lo tanto $e \leq b \wedge b \leq a*b$

Luego $e \leq a*b$ (Pues $\leq$ es transitiva)

$\Rightarrow a*b \in G_+$ ▨

(d) Pdq $G_+ \cup G_- = G$

Pero $G_+ \subseteq G \wedge G_- \subseteq G \Rightarrow G_+ \cup G_- \subseteq G$

Luego basta probar que $G \subseteq G_+ \cup G_-$

Sea $x \in G$. Basta probar que $x \in G_+ \cup G_-$, o sea (19)
que $x \in G_+ \vee x \in G_-$. En otras palabras basta probar
que $e \leq x \vee x \leq e$, lo cual es cierto pues $\leq$ es una
relación de orden total, o sea

$$(\forall a, b \in G)\ a \leq b \vee b \leq a$$

y usamos esta propiedad en particular para $a = e$ y $b = x$.

$$\therefore G \subseteq G_+ \cup G_-$$

Se concluye que $G_+ \cup G_- = G$ ▪

(e) Pdq $(\forall x, y \in G)\ x \leq y \vee y \leq x$

Notemos que si $x, y \in G \Rightarrow x * y^{-1} \in G \overset{\text{dato}}{=} G_+ \cup G_-$.
Luego $x * y^{-1} \in G_+ \vee x * y^{-1} \in G_-$
o sea $e \leq x * y^{-1} \vee x * y^{-1} \leq e$

Pero $e \leq x * y^{-1} \Rightarrow (e) * y \underset{\text{Por prop. del enunciado (con } z=y)}{\leq} (x * y^{-1}) * y \Rightarrow y \leq x$

y $x * y^{-1} \leq e \Rightarrow (x * y^{-1}) * y \leq (e) * y \Rightarrow x \leq y$

$\therefore e \leq x * y^{-1} \vee x * y^{-1} \in G_- \Rightarrow y \leq x \vee x \leq y$ ▪

(Pues si $p \Rightarrow q$ y $r \Rightarrow s$ $\Rightarrow [p \vee r \Rightarrow q \vee s]$)

P11 En $\mathbb{Z}_3 \times \mathbb{Z}$ se define la ley de composición interna $\oplus$ como sigue:

$$([n], m) \oplus ([n'], m') = ([n + n'], m + m')$$

Sea $\varphi : \mathbb{Z}_3 \times \mathbb{Z} \to \mathbb{Z}$ un homomorfismo de $(\mathbb{Z}_3 \times \mathbb{Z}, \oplus)$ en $(\mathbb{Z}, +)$

(i) Demuestre que $\varphi(([1], 0)) = 0$

Indicación: Calcule $\varphi(([1], 0) \oplus ([1], 0) \oplus ([1], 0))$.

(ii) Concluya que $(\mathbb{Z}_3 \times \mathbb{Z}, \oplus)$ no es isomorfo con $(\mathbb{Z}, +)$

(Control 3, 2002)

Solución:

(i) Calculemos $\varphi(([1], 0) \oplus ([1], 0) \oplus ([1], 0))$ de dos formas distintas.

$$\varphi(([1], 0) \oplus ([1], 0) \oplus ([1], 0)) \underset{\varphi \text{ homomorfismo}}{=} \varphi(([1], 0)) + \varphi(([1], 0)) + \varphi(([1], 0))$$
$$= 3\varphi(([1], 0))$$

De otra manera:

$$\varphi(([1], 0) \oplus ([1], 0) \oplus ([1], 0)) \overset{\text{Definición de } \oplus}{=} \varphi(([1+1+1], 0+0+0))$$
$$= \varphi(([3], 0))$$
$$\underset{\text{pues } [3] = [0] \text{ en } \mathbb{Z}_3}{=} \varphi(([0], 0))$$

Probemos ahora que

Aquí aparece una propiedad "clave" para problemas de homomorfismos.

[Sea $\varphi : (A, *) \to (B, \Delta)$ un homomorfismo, $(A, *)$ es una estructura algebraica con neutro e y (B, Δ) un GRUPO. En este caso se puede afirmar categóricamente que $\varphi(e)$ es el neutro en B para la operación "Δ".]

En este caso $\varphi : (\mathbb{Z}_3 \times \mathbb{Z}, \oplus) \to (\mathbb{Z}, +)$ es un homomorfismo donde claramente $(\mathbb{Z}_3 \times \mathbb{Z}, \oplus)$ es una estructura algebraica con neutro $([0], 0)$ (convencerse de esto) y $(\mathbb{Z}, +)$ es un grupo. Luego $\varphi(([0], 0))$ es el neutro de $(\mathbb{Z}, +)$, o sea 0.

$$\therefore \varphi(([0], 0)) = 0$$

Por lo anterior $\underbrace{\varphi(([0], 0))} = 3\varphi(([1], 0))$

$$\therefore \varphi(([1], 0)) = 0 \blacksquare$$

(ii) Como $\varphi(([0], 0)) = \varphi(([1], 0)) = 0$ se tiene que si φ es algún homomorfismo de $(\mathbb{Z}_3 \times \mathbb{Z}, \oplus)$ en $(\mathbb{Z}, +)$, no puede ocurrir que φ sea inyectivo.

Luego φ no puede ser biyectivo

$\therefore \varphi$ algún homomorfismo nunca podría ser un isomorfismo (un homomorfismo biyecti

---

P15 Sea $(H, +)$ subgrupo de $(\mathbb{Z}, +)$ con $H \neq \{0\}$

(a) Pruebe que $\{h \in H \mid h > 0\} \neq \phi$

(b) Considere $d = \min\{h \in H \mid h > 0\}$. Se define el conjunto $d\mathbb{Z} = \{x \in \mathbb{Z} \mid (\exists k \in \mathbb{Z})\ x = dk\}$

Demuestre que $d\mathbb{Z} \subseteq H$.

(c) Sea $h \in H$ con $h > 0$. Demuestre que $h = dq$ para algún $q > 0$.

Indicación: Puede usar el teorema de la división.

$(\forall a, b \in \mathbb{N}, b \neq 0)(\exists! q, r \in \mathbb{N})\ 0 \leq r < b \wedge a = qb + r$

(d) Concluya que $H = d\mathbb{Z}$

(Este problema fue usado en el Control 3 de 1991 y en el Control 3 del 2002. El mismo año fue usado en el control recuperativo 2002)

Solución:

(a) $(H, +)$ es subgrupo de $(\mathbb{Z}, +) \Rightarrow H \neq \phi$ (y $H \neq \{0\}$)

Luego $\exists h \in H$ y $h \neq 0$ (H tiene al 0 y otros "h")

Si $h > 0$, $\{h \in H \mid h > 0\} \neq \phi$

Si $h < 0 \Rightarrow -h > 0 \Rightarrow -h \in \{h \in H \mid h > 0\} \neq \phi \blacksquare$

Nota: Al decir $H \neq \{0\}$ decimos que H no es solo el 0.
Como $(H,+)$ subgrupo de $(\mathbb{Z},+)$, H por lo menos contiene a 0 que es el neutro para $(\mathbb{Z},+)$ pero $H \neq \{0\}$ quiere decir que además del 0 hay otros elementos.

(b) Pdq $d\mathbb{Z} \subseteq H$

Sea $x \in d\mathbb{Z} \Rightarrow x = dk$ con $k \in \mathbb{Z}$ (y $d = \min\{h \in H / h > 0\}$)

Si $k = 0 \Rightarrow x = 0 \in H$.

Si $k > 0 \Rightarrow x = dk = \underbrace{d+d+\ldots+d}_{\substack{k \text{ veces} \\ (k>0)}} \in H$ ← pues $d \in H$ y la cerradura de + en H.

Si $k < 0 \Rightarrow x = dk = (-d)(-k)$ donde $-d \in H$ (pues $d \in H$) ← inverso. y $(-k) > 0$

$= \underbrace{(-d)+(-d)+\ldots+(-d)}_{\substack{(-k) \text{ veces} \\ ((-k)>0)}} \in H$ ← pues $-d \in H$ y la cerradura de + en H.

(c) Sea $h \in H$ con $h > 0$. Dividiendo h por d se tiene

$(\exists! q, r \in \mathbb{N})\ h = qd + r$ con $0 \leq r < d$

$d \neq 0$ pues $d = \min\{h \in H / h > 0\}$ — notar que la parte (a) garantiza que este mínimo existe.

Notemos que $h \in H$ y $dq \in H$ (análogamente a (b)) $\Downarrow$ $(-dq) \in H$ ← inverso.

$\Rightarrow r = \underbrace{\underbrace{h}_{\in H} + \underbrace{(-qd)}_{\in H}}_{\in H}$ ← subgrupo (cerradura de + en H)

$\therefore r \in H$, $r \geq 0$ y $r < d = \min\{h \in H / h > 0\}$

$\Rightarrow r = 0 \Rightarrow h = qd + \underset{0}{r} = qd$ con $q \in \mathbb{N}$ $(q > 0)$ ∎

(d) Pdq $H = d\mathbb{Z}$. Por (b), $d\mathbb{Z} \subseteq H$, por lo que basta demostrar que $H \subseteq d\mathbb{Z}$

Sea $h \in H$

Si $h > 0 \overset{\text{Por (c)}}{\Rightarrow} h = dq \Rightarrow h \in d\mathbb{Z}$

Si $h = 0 \Rightarrow h = d \cdot 0 \Rightarrow h \in d\mathbb{Z}$

Si $h < 0 \Rightarrow (-h) > 0 \underset{\text{Por (c)}}{\Rightarrow} (-h) = dq$

$\Rightarrow h = d(-q)$

$\Rightarrow h \in d\mathbb{Z}$

En todos los casos, si $h \in H \Rightarrow h \in d\mathbb{Z}$

$\therefore H \subseteq d\mathbb{Z} \Rightarrow H = d\mathbb{Z}$ ∎

Nota: Notar que $d\mathbb{Z}$ no son nada más ni nada menos que los múltiplos de d.
Luego los únicos subgrupos de $(\mathbb{Z},+)$ son aquellos cuyo elementos son múltiplos de algún d, o sea los subgrupos de $(\mathbb{Z},+)$ son de la forma
$$d\mathbb{Z} = \{\ldots, -3d, -2d, -d, 0, d, 2d, 3d, \ldots\}$$

P16 (Propuesto)
Sea $(G,*)$ una estructura algebraica, cuya l.c.i cumple:
(1) Asociatividad
(2) Conmutatividad
(3) Idempotencia $((\forall a \in G)\ a*a = a)$
Se define en G la siguiente relación:
$$xRy \iff x*y = x$$
i) Pruebe que R es una relación de orden en G
ii) Verifique que $(\forall a,b \in G)$ se cumple:
(a) $(a*b)\,R\,a$
(b) $(a*b)\,R\,b$
(c) Si $(\exists x \in G)(xRa \wedge xRb)$ entonces $xR(a*b)$
(Control Recuperativo, 1995)

Problemas sobre Anillos y Cuerpos los veremos en clases, aunque por lo que se ve, es muy poco preguntado en controles. No confiarse con el hecho de que relaciones no se va a preguntar por que ya se preguntó en el control 2. Verán en es guía que hay muchas preguntas de relaciones (mezcladas con teoría de grupos) y que son muy preguntables.
Por último aquí tienen un problema muy simpático
Sea "$*$" una relación en $\mathbb{R}$ definida por:
$$a*b = a+b-2ab$$
Calcule $\left(\left(\left(\left(\frac{1}{2004}*\frac{2}{2004}\right)*\frac{3}{2004}\right)*\frac{4}{2004}\right)*\ldots\right)*\frac{2002}{2004}\Big)*\frac{2003}{2004}$
Hint: Calcule $a*\frac{1}{2}$ y $\frac{1}{2}*a$ e inspírese. Va a ocurrir algo muy lindo.

Nota: Se dice que $\frac{1}{2}$ es el elemento absorvente para $*$. Además no toda operación tiene elemento absorvente.

Les deseo la mejor de las suertes, nunca se rindan y los resultados van a ir se dando poco a poco.
Auxiliar MA11A Sección 04 David Painequeo Santoro.