Ejercicio 7. Sea H un subgrupo con índice 2 en un grupo G. Es decir: H tiene exactamente 2 clases laterales por izquierda en G. Probar que H es un subgrupo normal de G. Sugerencia: todo grupo G se puede escribir como la unión disjunta de las clases laterales por izquierda de cualquier subgrupo H de G.

H subgrupo de G

$$[G:H] = \#\{gH : g \in G\}$$
$$= \#\{Hg : g \in G\}$$

ejemplo: $[\mathbb{Z} : 2\mathbb{Z}] = 2$

dos clases laterales: la de los pares y la de los impares

$$\mathbb{Z} = 0(2\mathbb{Z}) \cup 1(2\mathbb{Z})$$

H subgrupo de G tal que $[G:H] = 2$ = cantidad de clases laterales a izquierda (derecha)

Queremos ver que H es subgrupo normal

es decir queremos ver que $gH = Hg$ para todo $g \in G$

* si $g \in H$ $\quad H$ es una clase lateral : $e_G H$

$$\left.\begin{array}{l} gH = H \\ Hg = H \end{array}\right\} \Rightarrow gH = Hg$$

* si $g \notin H$

$gH \neq H$ mas bien $gH \cap H = \phi$

$[G:H] = 2 \rightsquigarrow$ hay exactamente dos clases laterales por izquierda

$\Rightarrow$ las clases laterales por izquierda son H y gH

$$G = H \underset{\substack{\uparrow \\ \text{unión disjunta}}}{\cup} gH$$ porque las clases laterales a izquierda forman una partición

$Hg \cap H = \phi \rightsquigarrow Hg$ y H son dos clases laterales por derecha diferentes.

$[G:H]=2 \rightsquigarrow$ hay exactamente dos clases laterales por derecha

$\to$ las clases laterales por derecha son H y Hg

$G = H \cup Hg$ porque las clases laterales a derecha forman una partición.

$\uparrow$ unión disjunta

Entonces tenemos:

$$\left.\begin{array}{l} G = H \cup gH \\ G = H \cup Hg \end{array}\right] \Rightarrow gH = Hg \checkmark$$

Homomorfismos de grupos

Sean $(G,*)$ y $(K,\cdot)$ dos grupos.

Una función $f: G \to K$ es un morfismo de grupos si

$$f(g*g') = f(g)\cdot f(g') \quad \text{para todo } g,g' \in G$$

Ejercicio 1

d. La función $f : (\mathrm{GL}_n(\mathbb{R}), \cdot) \to (\mathbb{R}^*, \cdot)$, dada por: $f(A) = det(A^2)$.

f morfismo de grupos?

sean $A, B \in Gl_n(\mathbb{R})$, queremos ver si

$$f(AB) = f(A)f(B) = det(A^2)\,det(B^2)$$

$$\begin{aligned} f(AB) = det((AB)^2) &= det(AB)\,det(AB) \\ &= det(A)\,det(B)\,det(A)\,det(B) \\ &= det(A)\,det(A)\,det(B)\,det(B) \\ &= det(A^2)\,det(B^2) \\ &= f(A)\,f(B) \end{aligned}$$

entonces $f(AB) = f(A)f(B)$

$\Rightarrow f$ es morfismo de grupos.

b. La función $f : (M_{n\times n}(\mathbb{R}), +) \to (\mathbb{R}, +)$, dada por: $f(A) = tr(A^2)$.

f morfismo de grupos?

$A, B \in M_{n\times n}(\mathbb{R})$, queremos ver si $\underbrace{f(A+B)}_{tr((A+B)^2)} = \underbrace{f(A)+f(B)}_{tr(A^2)+tr(B^2)}$

$$\begin{aligned} f(A+B) = tr((A+B)^2) &= tr((A+B)(A+B)) \\ &= tr(A^2 + AB + BA + B^2) \\ &= tr(A^2) + tr(AB) + tr(BA) + tr(B^2) \\ &= tr(A^2) + tr(B^2) + \underbrace{tr(AB) + tr(BA)} \\ &= f(A) + f(B) + \underbrace{tr(AB) + tr(BA)} \end{aligned}$$

ejemplo: $A = B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$$f(A) + f(B) = tr(A^2) + tr(B^2) = tr\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + tr\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 2+2 = 4$$

$$f(A+B) = tr((A+B)^2) = tr\left(\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}^2\right) = tr\begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix} = 8$$

$$f(A+B) \neq f(A) + f(B)$$

$\Rightarrow$ f no es un morfismo de grupos.

h. La función $f : (\mathbb{R}^3, +) \to (\mathbb{R}^*, \cdot)$, dada por: $f(x, y, z) = e^{x-2y+z}$.

f morfismo de grupos?

$(x,y,z), (x',y',z') \in \mathbb{R}^3$, queremos ver si

$$f((x,y,z) + (x',y',z')) = f(x,y,z) \cdot f(x',y',z')$$

$$\begin{aligned} f((x,y,z) + (x',y',z')) &= f(x+x', y+y', z+z') \\ &= e^{x+x' - 2(y+y') + z + z'} \\ &= e^{x-2y+z + (x'-2y'+z')} \\ &= e^{x-2y+z} e^{x'-2y'+z'} \\ &= f(x,y,z) f(x',y',z') \end{aligned}$$

$\Rightarrow$ f es un morfismo de grupos.

f. La función trasponer $T : (M_{n\times n}(\mathbb{R}), +) \to (M_{n\times n}(\mathbb{R}), +)$, dada por: $T(A) = A^t$.

T es morfismo de grupos?

sean $A, B \in M_{n\times n}(\mathbb{R})$ y queremos ver si $T(A+B) = T(A) + T(B)$

$$T(A+B) = (A+B)^t = A^t + B^t = T(A) + T(B)$$

$\Rightarrow$ T es morfismo de grupos.

g. La función trasponer $T : (\mathrm{GL}_n(\mathbb{R}), \cdot) \to (\mathrm{GL}_n(\mathbb{R}), \cdot)$, dada por: $T(A) = A^t$.

sean $A, B \in GL_n(\mathbb{R})$ y queremos ver si $T(AB) = T(A)T(B)$

$$\left.\begin{array}{l} T(AB) = (AB)^t = B^t A^t \\ T(A)T(B) = A^t B^t \end{array}\right] \Rightarrow T(AB) \neq T(A)T(B)$$

$\Rightarrow$ T no es un morfismo de grupos.

$\varphi : (G_1, *) \to (G_2, \cdot)$ morfismo de grupos:

① $\varphi(e_{G_1}) = e_{G_2}$

$$\varphi(e_{G_1}) = \varphi(e_{G_1} * e_{G_1}) = \varphi(e_{G_1}) \cdot \varphi(e_{G_1})$$

$$\Rightarrow \varphi(e_{G_1})(\varphi(e_{G_1}))^{-1} = \varphi(e_{G_1}) \cdot \varphi(e_{G_1}) \cdot (\varphi(e_{G_1}))^{-1}$$

$$\Rightarrow e_{G_2} = \varphi(e_{G_1})$$

② $g \in G_1$ un elemento de orden finito

$\Rightarrow o(\varphi(g)) \mid o(g)$ $\qquad \varphi(g^n) = \varphi(g * \cdots * g) = \varphi(g) \cdot \ldots \cdot \varphi(g) = (\varphi(g))^n$

<u>dem:</u> $n = o(g)$

$$g^n = e_{G_1} \Rightarrow \varphi(g^n) = \varphi(e_{G_1})$$

$$\Rightarrow (\varphi(g))^n = e_{G_2}$$

$$\Rightarrow o(\varphi(g)) \mid n$$

$$\Rightarrow o(\varphi(g)) \mid o(g)$$

Ejercicio 2. Sea $\varphi : G_1 \to G_2$ un homomorfismo de grupos finitos.

a. Sea $g \in G_1$. Probar que $o(\varphi(g))$ divide a $\mathrm{mcd}(|G_1|, |\mathrm{Im}(\varphi)|)$.

b. Probar que si $|G_1|$ y $|G_2|$ son coprimos, entonces φ es trivial.

c. Supongamos que φ es un isomorfismo de grupos. Sea $g \in G_1$. Probar que el orden de g en G_1 es igual al orden de $\varphi(g)$ en G_2.

d. Probar que $\mathbb{Z}_4$ y $\mathbb{Z}_2 \times \mathbb{Z}_2$ no son isomorfos.

a) $\varphi: G_1 \to G_2$ morfismo de grupos finito

$g \in G_1$

queremos ver que $o(\varphi(g))$ divide $\mathrm{mcd}(|G_1|, |\mathrm{Im}\varphi|)$

* $o(\varphi(g)) \mid |G_1|$

$o(g) = |\langle g \rangle|$ divide a $|G_1|$ por el teorema de Lagrange

$$\left.\begin{array}{l} o(\varphi(g)) \mid o(g) \\ o(g) \mid |G_1| \end{array}\right\} \Rightarrow o(\varphi(g)) \mid |G_1|$$

* $o(\varphi(g)) \mid |\mathrm{Im}\varphi|$

$\varphi(g) \in \mathrm{Im}\varphi$

$\Rightarrow \langle \varphi(g) \rangle$ es un subgrupo de $\mathrm{Im}\varphi$

$\Rightarrow \underbrace{|\langle \varphi(g) \rangle|}_{= o(\varphi(g))}$ divide a $|\mathrm{Im}\varphi|$

$\Rightarrow o(\varphi(g))$ divide a $|\mathrm{Im}\varphi|$

* $$\left.\begin{array}{l} o(\varphi(g)) \mid |G_1| \\ o(\varphi(g)) \mid |\mathrm{Im}\varphi| \end{array}\right\} \Rightarrow o(\varphi(g)) \text{ divide a } \mathrm{mcd}(|G_1|, |\mathrm{Im}\varphi|)$$

b. Probar que si $|G_1|$ y $|G_2|$ son coprimos, entonces $\underbrace{\varphi \text{ es trivial}}$.

$\varphi: G_1 \to G_2$ morfismo de grupos $\qquad \varphi(g) = e_{G_2}$ para todo $g \in G_1$

$g \in G_1$

para probar que $\varphi(g) = e_{G_2}$, vamos a probar que $o(\varphi(g)) = 1$

$|G_1|$ y $|G_2|$ son coprimos $\Rightarrow \mathrm{mcd}(|G_1|, |G_2|) = 1$

$\mathrm{Im}\,\varphi$ es un subgrupo de G_2

$\Rightarrow |\mathrm{Im}\,\varphi| \mid |G_2|$ $\Rightarrow \mathrm{mcd}(|G_1|, |\mathrm{Im}\,\varphi|) = 1$

entonces $o(\varphi(g)) \mid \underbrace{\mathrm{mcd}(|G_1|, |\mathrm{Im}\,\varphi|)}_{=1}$

$\Rightarrow o(\varphi(g)) = 1$

$\Rightarrow \varphi(g) = e_{G_2}$

$\Rightarrow \varphi$ es el morfismo trivial