módulo 5:

5.1.- HOMOMORFISMO DE GRUPOS

En este capítulo presentaremos conceptos que consideramos fundamentales en el estudio de las estructuras algebraicas. Se definirán ciertas funciones de un grupo a otro que nos facilitará la comparación entre las estructuras de estos grupos. Se estudiará el concepto de isomorfismo que es de gran utilidad, pues nos permitirá decidir en qué casos estamos trabajando con grupos, que a pesar de tener elementos distintos, poseen una estructura idéntica.

Además, los conceptos que se estudiarán a continuación son prácticos, porque serán usados para reducir el análisis de propiedades de interés que pueda tener un grupo, al estudio de las mismas propiedades en otro grupo que tenga la misma estructura que el primitivo, pero sin embargo este sea más simple de manejar o más conocido por nosotros.

Definición 1: Dados $(G,*)$ y $(H,\circ)$ dos grupos. Un homomorfismo de G en H es una aplicación $f: G \to H$, tal que:

$$\forall\ g_1,\ g_2 \in G,\ f(g_1 * g_2) = f(g_1) \circ f(g_2)$$

Ejemplo 1: Sea $f: (\mathbb{C},+) \to (\mathbb{C},+)$, tal que $\forall\ z \in \mathbb{C},\ f(z) = \bar{z}$ es un homomorfismo de grupos.

Previamente se debe verificar si f es una aplicación.

Si $z_1 = a+bi = c+di = z_2$, por igualdad en $\mathbb{C}$

$$\Downarrow$$

$$\operatorname{Re}(z_1) = \operatorname{Re}(z_2) \wedge \operatorname{Im}(z_1) = \operatorname{Im}(z_2)$$

$$a = c \qquad\qquad b = d$$

$$\Downarrow$$

Re(z) es la parte Real del complejo z
Im(z) es la parte Imaginaria de z

$$a - bi = c - di$$
$$\overline{z_1} = \overline{z_2}$$

$\therefore$ f es una aplicación

Ahora, probaremos si f es un homomorfismo: dados $z_1 = a + bi \in \mathbb{C}$ y $z_2 = c + di \in \mathbb{C}$, entonces:

$$\begin{aligned} f(z_1 + z_2) &= f(a + bi + c + di) \\ &= f((a + c) + (b + d)\, i) \\ &= (a + c) - (b - d)\, i \\ &= a - bi + c + di \\ &= \overline{z_1} + \overline{z_2} \\ &= f(z_1) + f(z_2) \end{aligned}$$

$\therefore$ f es Homomorfismo.

Ejemplo 2: Consideremos los grupos $(\mathbb{Z},+)$ y $(\mathbb{R}^+,\cdot)$. Afirmamos que la función o aplicación: $f:\ \mathbb{Z} \to \mathbb{R}^+$ tal que $f(n) = 2^n$ es un homomorfismo de grupos.

En efecto:

$\forall\ r,\ s \in \mathbb{Z}:\ f(r + s) = 2^{r+s} = 2^r \cdot 2^s = f(r) \cdot f(s)$

Queda de ejercicio para el lector probar si es aplicación.

Ejemplo 3: $\wp = (S_n,\cdot) \to (\{1,-1\},\cdot)$, tal que $\forall\ \sigma \in S_n$, se tiene:

$$\wp(\sigma) = \begin{cases} 1 \ si\ \sigma\ es\ par \\ -1\ si\ \sigma\ es\ impar \end{cases}$$, es un homomorfismo de grupos.

En efecto:

Primer caso:

Dados σ, ρ $\in$ S_n, pares, se tiene que $\sigma\rho$ $\in$ S_n es par, luego $\wp(\sigma\rho) = 1$.

Por otro lado, si σ, ρ son par, entonces $\wp(\sigma) \cdot \wp(\rho) = (1)\cdot(1) = 1$

$$\therefore \wp(\sigma\rho) = \wp(\sigma) \cdot \wp(\rho)$$

Segundo caso:

Dados σ, ρ $\in$ S_n, impares, se tiene que $\sigma\rho$ $\in$ S_n es par, luego $\wp(\sigma\rho) = 1$

Por otro lado, si σ, ρ son impares, entonces $\wp(\sigma) \cdot \wp(\rho) = (-1)\cdot(-1) = 1$

$$\therefore \wp(\sigma\rho) = \wp(\sigma) \cdot \wp(\rho)$$

Tercer caso:

Dados $\sigma \in S_n$ par y $\rho \in S_n$ impar, se tiene que $\sigma\rho \in S_n$ es impar, luego $\wp(\sigma\rho) = -1$.

Por otro lado, σ es par y ρ es impar, entonces $\wp(\sigma) \cdot \wp(\rho) = (1)\cdot(-1) = -1$

$$\therefore \wp(\sigma\rho) = \wp(\sigma) \cdot \wp(\rho)$$

Cuarto caso:

Dados $\sigma \in S_n$ impar y $\rho \in S_n$ par, se tiene que $\sigma\rho \in S_n$ es impar, luego $\wp(\sigma\rho) = -1$.

Por otro lado, σ es impar y ρ es par, entonces $\wp(\sigma) \cdot \wp(\rho) = (-1)\cdot(1) = -1$

$$\therefore \wp(\sigma\rho) = \wp(\sigma) \cdot \wp(\rho)$$

En consecuencia de los cuatro casos, podemos asegurar que la aplicación $\wp$ es Homomorfismo de Grupos.

Observación: Dos grupos se dirán homomorfos si existe un homomorfismo entre ellos.

5.2.- Definición 2: Sean $(G,*)$ y $(H.\circ)$ dos grupos.

5.2.1.- Un $f \in Hom(G,G)$, recibe el nombre de ***Endomorfismo***.

Notación: $Hom(G,G) \coloneqq End(G)$, donde:

$End(G) \coloneqq \{f \ / \ f: G \to G$ es Homomorfismo$\}$

5.2.2.- Un $f \in Hom(G,H)$ inyectivo, recibe el nombre de ***Monomorfismo***.

Notación:

$Mon(G,H) := \{ f: G \to H \ / \ f$ es homo inyectivo $\}$

5.2.3.- Un $f \in Hom(G,H)$, tal que f es epiyectiva, recibe el nombre de ***Epimorfismo***.

Notación:

$Epi(G,H) := \{ f: G \to H \ / \ f$ es homo epiyectivo $\}$

5.2.4.- Un $f \in Hom(G,H)$, tal que f es biyectivo, recibe el nombre de ***Isomorfismo***.

Notación:

$Iso(G,H) := \{ f: G \to H \ / \ f$ es homo biyectivo $\}$

5.2.5.- Un $f \in Hom(G,G)$, talque f es biyectiva, recibe el nombre de ***Automorfismo***.

Notación:

$Aut(G) := \{ f: G \to G \ / \ f$ es homo biyectivo $\}$

$= \{ f: G \to G \ / \ f$ es isomorfismo $\}$

Dos grupos se dirán isomorfos, si existe un isomorfismo entre ellos. Si G y H son isomorfos, anotaremos $G \cong H$.

Ejemplo 4: ¿Es $f: (\mathbb{R},+) \to (\mathbb{R}^+,\cdot)$, tal que $\forall\ x \in \mathbb{R},\ f(x) = e^x$ un isomorfismo de grupos?

Para probar que la aplicación dada es un isomorfismo, se debe verificar lo siguiente:

i) f es homomorfismo

$\forall\ x,\ y \in \mathbb{R}$, se tiene:

$$f(x+y) = e^{x+y} = e^x \cdot e^y = f(x) \cdot f(y)$$

ii) f es inyectiva

$\forall\ x,\ y \in \mathbb{R}$. Si $f(x) = f(y)$, por demostrar que $x = y$.

De la hipótesis se tiene: $e^x = e^y$, aplicamos $\ln$ tenemos

$$\begin{aligned} \ln(e^x) &= \ln(e^y) \\ x \ln e &= y \ln e \\ x &= y \end{aligned}$$

$\therefore f$ es inyectiva

Hasta aquí, f es Monomorfismo

iii) f es epiyectiva

$\forall\ y \in \mathbb{R}^+$, debe existir $v \in \mathbb{R}$, tal que $f(v) = y$. Supongamos que $f(v) = y$, entonces $e^v = y$. Luego, por propiedad de *ln* se tiene que $v = \ln y$

En consecuencia de i), ii) y iii) f es isomorfismo

$$\therefore (\mathbb{R},+) \cong (\mathbb{R}^+,\cdot)$$

Ejemplo 5: Sea $f_g : G \to G$ talque $\forall\ x \in G$, $f_g(x) = gxg^{-1}$, g fijo con G grupo. ¿Es f_g un Automorfismo?

Para probar que f_g sea un automorfismo se debe verificar que sea homomorfismo y biyectiva.

i) Por ver si es homomorfismo

$\forall\ x,\ y \in G$, se tiene que $f_g(x) = gxg^{-1}$ y $f_g(y) = gyg^{-1}$, por demostrar que $f_g(x \cdot y) = f_g(x) \cdot f_g(y)$.

Luego se tiene;

$$\begin{aligned} f_g(x \cdot y) &= gxyg^{-1} \quad ; G \text{ grupo, existe neutro} \\ &= gxeyg^{-1} \\ &= gxg^{-1}gyg^{-1} \\ &= f_g(x) \cdot f_g(y) \end{aligned}$$

$\therefore$ Es homomorfismo.

ii) Por ver si es inyectiva (monomorfismo)

$\forall \; x, y \in G$, si $f(x) = f(y)$, por demostrar que $x = y$

Se tiene;

$$\begin{aligned} f(x) &= f(y) \\ gxg^{-1} &= gyg^{-1} \quad / \; g^{-1} \text{ por la izquierda} \\ g^{-1}gxg^{-1} &= g^{-1}gyg^{-1} \\ exg^{-1} &= eyg^{-1} \quad / \; g \text{ por la derecha} \\ xg^{-1}g &= yg^{-1}g \\ xe &= ye \\ x &= y \end{aligned}$$

$\therefore$ Es inyectiva.

iii) Por ver si es epiyectiva $\forall \; u \in G$ (Codom), $\exists \; v \in G$ (Dom), tal que $f_g(v) = u$

Se tiene:

$$\begin{aligned} \text{Si } f(v) &= u \text{ , entonces} \\ gvg^{-1} &= u \quad / \; g^{-1} \text{ por la izq.} \\ g^{-1}gvg^{-1} &= g^{-1}u \\ evg^{-1} &= g^{-1}u \quad / \; g \text{ por la der.} \end{aligned}$$

$$\begin{aligned} vg^{-1}g &= g^{-1}ug \\ ve &= g^{-1}ug \\ v &= g^{-1}ug \end{aligned}$$

Luego, existe $v = g^{-1}ug$ en G tal que $f_g(v) = u$. Por lo tanto, f_g es epiyectiva.

$\therefore$ De todo lo anterior, $f_g : G \to G$ es un automorfismo.

Propiedad 1: Sea $f \in Hom(G,H)$ de grupos. Entonces: (1) $f(e_G) = e_H$ (2) $(f(g))^{-1} = f(g^{-1})$, $\forall\ g \in G$

Demostración:

(1) Sabemos que $e_G \cdot e_G = e_G$, pues e_G es neutro en G

Luego tenemos;

$$\begin{aligned} e_G \cdot e_G &= e_G & / \ f \\ f(e_G \cdot e_G) &= f(e_G) \\ f(e_G) \cdot f(e_G) &= f(e_G) & / \ (f(e_G))^{-1} \\ (f(e_G))^{-1} \cdot f(e_G) \cdot f(e_G) &= (f(e_G))^{-1} \cdot f(e_G) \\ \therefore \quad f(e_G) &= e_H \end{aligned}$$

(2) Sabemos que G es grupo, luego $\forall\ g \in G$, $\exists\ g^{-1} \in G$ tal que

$$g \cdot g^{-1} = e_G = g^{-1} \cdot g$$

Aplicando f, se tiene:

$$
\begin{array}{rcll}
f(g\cdot g^{-1}) & = & f(e_G) & /\ f \text{ es homomorfismo} \\
f(g)\cdot f(g^{-1}) & = & f(e_G) & /\ \text{propiedad 1} \\
f(g)\cdot f(g^{-1}) & = & e_H & /\ (f(g))^{-1} \in H \\
(f(g))^{-1}\cdot f(g)\cdot f(g^{-1}) & = & (f(g))^{-1}\cdot e_H & \\
e_H \cdot f(g^{-1}) & = & (f(g))^{-1} & \\
\therefore\ f(g^{-1}) & = & (f(g))^{-1} & \forall\ g \in G
\end{array}
$$

Propiedad 2:

Sea $f \in Hom(G,H)$ de grupos. Entonces:

(1) $Ker\ f := \{g \in G : f(g) = e_H\} \leq G$

(2) $\operatorname{Im} f := \{f(g) : g \in G\} \leq H$

$:= \{h \in H : \exists\ g \in G\ tal que\ f(g) = h\}$

Demostración:

(1) Por demostrar que $Ker\ f \coloneqq \{g \in G : f(g) = e_H\} \leq G$

i) Claramente $Ker\ f \subseteq G$, pues $e_G \in G$ y $e_G \in Ker\ f$ y $Ker\ f \neq \varnothing$.

ii) $\forall\ x, y \in Ker\ f$, talque $f(x) = e_H$ y $f(y) = e_H$, por demostrar que $f(x\cdot y) \in Ker\ f$. Luego se tiene que;

$$
\begin{array}{rcl}
f(x\cdot y) & = & f(x)\cdot f(y) \quad /\ f \text{ es homo} \\
& = & e_H \cdot e_H \\
& = & e_H \\
\end{array}
$$

$$\therefore\ f(x\cdot y) \in Ker\ f$$

iii) $\forall\ x \in Ker\ f$, tal que $f(x)=e_H$, por demostrar que $x^{-1} \in Ker\ f$, es decir $f(x^{-1})=e_H$. Luego se tiene;

$$\begin{aligned} f(x^{-1}) &= (f(x))^{-1} \\ &= (e_H)^{-1} \\ &= e_H \end{aligned}$$

$$\therefore\ x^{-1} \in Ker\ f$$

Por lo demostrado anteriormente $Ker\ f \leq G$.

(2) Por demostrar que $\operatorname{Im} f := \{f(g)\ :\ g \in G\} \leq H$

i) Claramente $\operatorname{Im} f \subseteq H$ por definición de $\operatorname{Im} f$, además, $\operatorname{Im} f \neq \varnothing$ pues $e_H \in \operatorname{Im} f$ ya que $f(e_G)=e_H$.

ii) $\forall\ x,\ y \in \operatorname{Im} f$, por demostrar que $x\cdot y \in \operatorname{Im} f$.

Si $x \in \operatorname{Im} f$, existe $a \in G$ tal que $f(a)=x$

Si $y \in \operatorname{Im} f$, existe $b \in G$ tal que $f(b)=y$

Luego,

$$\begin{aligned} x\cdot y &= f(a)\cdot f(b) && \text{, pero } f \text{ es homo} \\ &= f(a\cdot b), && \text{donde } a\cdot b=c, \text{ con } c \in G \end{aligned}$$

Luego $\exists\ c \in G$, tal que $f(\mathrm{c})=x\cdot y$. $\therefore\ xy \in \operatorname{Im} f$.

iii) $\forall\ h \in \operatorname{Im} f$, por demostrar que $h^{-1} \in \operatorname{Im} f$

Si $h \in \operatorname{Im} f$, existe $x \in G$ tal que $f(x)=h$

Como $\operatorname{Im} f \subset H$ y *H* es un grupo, se tiene $h^{-1}=(f(x))^{-1}$, pero f es homomorfismo, luego $h^{-1}=(f(x^{-1}))$ con $x^{-1} \in G$ grupo. Lo que demuestra $h^{-1} \in \operatorname{Im} f$.

Por lo anteriormente demostrado, $\operatorname{Im} f \leq H$.

□

Teorema 1:

Sea $f \in Hom(G,H)$, entonces son equivalentes:

(1) f es Monomorfismo

(2) $Ker\ f = \{e_G\}$

Demostración:

(1)$\Rightarrow$(2) Sea $x \in Ker\ f$ (cualquiera). Por demostrar que $x = e_H$.

Si $x \in Ker\ f \Rightarrow f(x) = e_H$, demás sabemos que $f(e_G) = e_H$, luego $f(x) = f(e_G)$ y como f es inyectiva, tenemos que por definición es Monomorfismo, finalmente $x = e_G$.

$\therefore\ Ker\ f = \{e_G\}$, cuando f es Monomorfismo.

(2) $\Rightarrow$ (1) Como f es homomorfismo, basta demostrar que f sea inyectiva.

Si $f(x) = f(y)$ con $x,\ y \in G$, entonces $f(x)\cdot f(y)^{-1} = e_H$, por propiedad anterior tenemos $f(x)\cdot f(y^{-1}) = e_H$ y como f es homomorfismo tenemos que $f(xy^{-1}) = e_H$, lo que implica que $xy^{-1} \in Ker\ f$, pero $Ker\ f = \{e_G\}$, luego $xy^{-1} = e_G$.

$$\therefore\ x = y$$

$\therefore\ f$ es inyectiva. Así f es Monomorfismo cuando $Ker\ f = \{e_G\}$.

5.3.- Caracterización de los Homomorfismos de un grupo G en un grupo H.

Definición 3: La aplicación $f: G \to H$, tal que $f(x) = a$ caracteriza un Homomorfismo de G en H si y sólo si $|a| \,\big|\, |G|$, donde $a \in H$.

Nota: Si G es un grupo cíclico, considérese el elemento x generador del grupo G.

Ejemplo 6: Caracterizar todos los homomorfismos de $\mathbb{Z}_6$ en $\mathbb{Z}_4$.

Primero debemos determinar los generadores del dominio $\mathbb{Z}_6$ que son: $\mathbb{Z}_6 = \langle \bar{1} \rangle = \langle \bar{5} \rangle$, luego $x \in \{\bar{1}, \bar{5}\}$

Por otro lado calcularemos el orden de los elementos del recorrido $\mathbb{Z}_4$, al realizar esto estamos buscando nuestros posibles elementos "a", talque su orden divida $|\mathbb{Z}_6|$ luego tenemos:

$$|\bar{0}| = 1; \quad |\bar{1}| = 4; \quad |\bar{2}| = 2; \quad |\bar{3}| = 4$$

Los "a" $\in \mathbb{Z}_4$, tal que su orden divida a $|\mathbb{Z}_6|$ son $\bar{0}$ y $\bar{2}$.

Notamos que los homomorfismos, posibles, son:

$$f(\bar{1}) = \begin{cases} \bar{0} \\ \bar{2} \end{cases} \quad \text{y} \quad f(\bar{5}) = \begin{cases} \bar{0} \\ \bar{2} \end{cases}$$

Hay cuatro homomorfismos a saber:

(1) $f_1(\bar{1}) = \bar{0}$;

$$\begin{array}{ccc} & f_1 & \\ \bar{1} & \to & \bar{0} \\ \bar{2} & \to & \bar{0} \\ \bar{3} & \to & \bar{0} \\ \bar{4} & \to & \bar{0} \\ \bar{5} & \to & \bar{0} \\ \bar{0}=\bar{6} & \to & \bar{0} \end{array}$$

$\forall\ \bar{x} \in \mathbb{Z}_6,\ f(\bar{x}) = \bar{0}$

(2) $f_2(\bar{1}) = \bar{2}$;

$$\begin{array}{ccc} & f_2 & \\ \bar{1} & \to & \bar{2} \\ \bar{2} & \to & \bar{0} \\ \bar{3} & \to & \bar{2} \\ \bar{4} & \to & \bar{0} \\ \bar{5} & \to & \bar{2} \\ \bar{0}=\bar{6} & \to & \bar{0} \end{array}$$

(3) $f_3(\bar{5}) = \bar{0}$;

$$\begin{array}{ccc} & f_3 & \\ \bar{1} & \to & \bar{0} \\ \bar{2} & \to & \bar{0} \\ \bar{3} & \to & \bar{0} \\ \bar{4} & \to & \bar{0} \\ \bar{5} & \to & \bar{0} \\ \bar{0}=\bar{6} & \to & \bar{0} \end{array}$$

$\forall\ \bar{x} \in \mathbb{Z}_6,\ f(\bar{x}) = \bar{0}$

(4) $f_4(\bar{5}) = \bar{2}$;

$$\begin{array}{ccc} & f_4 & \\ \bar{1} & \to & \bar{2} \\ \bar{2} & \to & \bar{0} \\ \bar{3} & \to & \bar{2} \\ \bar{4} & \to & \bar{0} \\ \bar{5} & \to & \bar{2} \\ \bar{0}=\bar{6} & \to & \bar{0} \end{array}$$

Luego hay sólo dos homomorfismos distintos de $\mathbb{Z}_6$ en $\mathbb{Z}_4$ a saber:

$f_1 = f_3$ y $f_2 = f_4$

Ejemplo 7: Caracterice todos los homomorfismo distintos de $\mathbb{Z}_4$ en $(H = \{1, -1, i, -i\}, \cdot)$

Notamos que $\mathbb{Z}_4$ es cíclico, $\mathbb{Z}_4 = \langle \bar{1} \rangle = \langle \bar{3} \rangle$, es decir $x \in \{\bar{1}, \bar{3}\}$.

Ahora calcularemos el orden de los elementos de H (recorrido), estos son:

$$|1| = 1; \quad |-1| = 2; \quad |i| = 4; \quad |-i| = 4$$

Los elementos "a" de H tales que su orden divida a $|\mathbb{Z}_4|$ son: 1, -1, i, $-i$.
Los homomorfismos posibles de $\mathbb{Z}_4$ en H son:

$$f(x) = \begin{cases} 1 \\ -1 \\ i \\ -i \end{cases}, \text{ con } x \in \{\bar{1}, \bar{3}\}$$

Notemos que hay 8 homomorfismos de los cuales son sólo cuatro distintos.

(1) $f_1(\bar{1}) = 1$; (2) $f_2(\bar{1}) = \overline{-1}$; (3) $f_3(\bar{1}) = i$; (4) $f_4(\bar{1}) = -i$;

$$\begin{array}{ccc} & f_1 & \\ \bar{1} & \to & 1 \\ \bar{2} & \to & 1 \\ \bar{3} & \to & 1 \\ \bar{4} & \to & 1 \end{array} \qquad \begin{array}{ccc} & f_2 & \\ \bar{1} & \to & -1 \\ \bar{2} & \to & 1 \\ \bar{3} & \to & -1 \\ \bar{4} & \to & 1 \end{array} \qquad \begin{array}{ccc} & f_3 & \\ \bar{1} & \to & i \\ \bar{2} & \to & -1 \\ \bar{3} & \to & -i \\ \bar{4} & \to & 1 \end{array} \qquad \begin{array}{ccc} & f_4 & \\ \bar{1} & \to & -i \\ \bar{2} & \to & -1 \\ \bar{3} & \to & i \\ \bar{4} & \to & 1 \end{array}$$

$\forall\ \bar{x} \in \mathbb{Z}_4,\ f(\bar{x}) = 1$

Los anteriores son los cuatro homomorfismos distintos de $\mathbb{Z}_4$ en H.

Ejemplo 8: Determinar todos los homomorfismos de $\mathbb{Z}_6$ en $\mathbb{Z}_6$. ¿Cuáles son isomorfismos?

Debemos determinar los generadores del dominio $\mathbb{Z}_6$ que son: $\mathbb{Z}_6 = \langle \bar{1} \rangle = \langle \bar{5} \rangle$, luego $x \in \{\bar{1}, \bar{5}\}$.

Además calcularemos el orden de los elementos del recorrido $\mathbb{Z}_6$, buscando nuestros posibles elementos "a", talque su orden divida $\mathbb{Z}_6$ (dominio), luego tenemos:

$$|\bar{0}| = 1;\quad |\bar{1}| = 6;\quad |\bar{2}| = 3;\quad |\bar{3}| = 2;\quad |\bar{4}| = 3;\quad |\bar{5}| = 6$$

Los "a" $\in \mathbb{Z}_6$, talque su orden divida a $|\mathbb{Z}_6|$ son $\bar{0}$ y $\bar{2}$.

Notamos que hay 6 homomorfismos distintos de $\mathbb{Z}_6$ en $\mathbb{Z}_6$ a saber

(1) $f_1(\bar{1}) = \bar{0}$; (2) $f_2(\bar{1}) = \bar{1}$; (3) $f_3(\bar{1}) = \bar{2}$;

f_1			f_2			f_3		
$\bar{1}$	$\to$	$\bar{0}$	$\bar{1}$	$\to$	$\bar{1}$	$\bar{1}$	$\to$	$\bar{2}$
$\bar{2}$	$\to$	$\bar{0}$	$\bar{2}$	$\to$	$\bar{2}$	$\bar{2}$	$\to$	$\bar{4}$
$\bar{3}$	$\to$	$\bar{0}$	$\bar{3}$	$\to$	$\bar{3}$	$\bar{3}$	$\to$	$\bar{0}$
$\bar{4}$	$\to$	$\bar{0}$	$\bar{4}$	$\to$	$\bar{4}$	$\bar{4}$	$\to$	$\bar{2}$
$\bar{5}$	$\to$	$\bar{0}$	$\bar{5}$	$\to$	$\bar{5}$	$\bar{5}$	$\to$	$\bar{4}$
$\bar{0} = \bar{6}$	$\to$	$\bar{0}$	$\bar{0} = \bar{6}$	$\to$	$\bar{0}$	$\bar{0} = \bar{6}$	$\to$	$\bar{0}$

$\forall\ \bar{x} \in \mathbb{Z}_6,\ f(\bar{x}) = \bar{0}$

(4) $f_4(\bar{1}) = \bar{3}$; (5) $f_5(\bar{1}) = \bar{4}$; (6) $f_6(\bar{1}) = \bar{5}$;

$$\begin{array}{ccc} & f_4 & \\ \bar{1} & \to & \bar{3} \\ \bar{2} & \to & \bar{0} \\ \bar{3} & \to & \bar{3} \\ \bar{4} & \to & \bar{0} \\ \bar{5} & \to & \bar{3} \\ \bar{0}=\bar{6} & \to & \bar{0} \end{array} \qquad \begin{array}{ccc} & f_5 & \\ \bar{1} & \to & \bar{4} \\ \bar{2} & \to & \bar{2} \\ \bar{3} & \to & \bar{0} \\ \bar{4} & \to & \bar{4} \\ \bar{5} & \to & \bar{2} \\ \bar{0}=\bar{6} & \to & \bar{0} \end{array} \qquad \begin{array}{ccc} & f_6 & \\ \bar{1} & \to & \bar{5} \\ \bar{2} & \to & \bar{4} \\ \bar{3} & \to & \bar{3} \\ \bar{4} & \to & \bar{2} \\ \bar{5} & \to & \bar{1} \\ \bar{0}=\bar{6} & \to & \bar{0} \end{array}$$

Los homomorfismos distintos de $\mathbb{Z}_6$ en $\mathbb{Z}_6$ son los nombrados anteriormente y los isomorfismos son f_2 y f_6.

Observación:

- Todo isomorfismo preserva orden de sus elementos.
- Todo isomorfismo queda definido en sus generadores para grupos del mismo orden.
- De $\mathbb{Z}_n$ en $\mathbb{Z}_n$ se pueden definir $\phi(n)$ isomorfismos distintos.

Podemos determinar cuantos isomorfismos distintos hay de $\mathbb{Z}_{18}$ en $\mathbb{Z}_{18}$, ya que por la observación anterior sabemos que esta dada por $\phi(18)$ que al resolver obtendríamos: $\phi(18) =$ $\phi(2 \cdot 3^2) =$ $(2-2^0)\cdot(3^2 \cdot 3) =$ 6. Entonces $\mathbb{Z}_{18}$ posee 6 generadores con lo cual se pueden definir 6 isomorfismos distintos a saber: $f(\bar{1}) = \bar{1}$; $f(\bar{1}) = \bar{5}$; $f(\bar{1}) = \bar{7}$; $f(\bar{1}) = \overline{11}$; $f(\bar{1}) = \overline{15}$; $f(\bar{1}) = \overline{17}$.

Proposición 1: Dos grupos cíclicos del mismo orden son isomorfos

Demostración:

Hipótesis: Sean G y H dos grupos cíclicos con $G=\langle a\rangle$ y $H=\langle b\rangle$, donde $|G|=|H|$.

Tesis: Por demostrar que $G\cong H$.

Para demostrarlo definiremos una aplicación $f:G\to H$ talque $f(a)=b$, entonces $\forall\ x\in G$, diremos que $f(x)=f(a^r)=b^r$.

Sabiendo que $f(a^r)=\underbrace{f(a\cdot a\cdot\ldots a)}_{r\ veces}=\underbrace{f(a)\cdot f(a)\cdot\ldots\cdot f(a)}_{r\ veces}=b^r$, pues $f(a)=b$.

i) Por ver si f está bien definida;

$\forall\ x,y\in G$ si $x=y$ entonces $f(x)=f(y)$ donde $a^r=a^s$; $r,s\in\mathbb{Z}$, luego tenemos:

$$\begin{aligned}
a^r &= a^s \\
a^r\cdot(a^s)^{-1} &= e && \text{/ aplicamos } f \\
f(a^r\cdot(a^s)^{-1}) &= f(e) \\
f(a^{r-s}) &= e_H && /\ r-s\in\mathbb{Z}
\end{aligned}$$

Luego

$$\begin{aligned}
b^{r-s} &= e_H && /\ H \text{ es grupo} \\
b^r\cdot b^{-s} &= e_H \\
b^r &= b^s
\end{aligned}$$

$$\therefore\ f(x)=f(y)$$

ii) Por ver que f es homomorfismo.

$\forall\ x, y \in G$. Por demostrar que $f(x \cdot y) = f(x) \cdot f(y)$; se tiene:

$$\begin{aligned} f(x \cdot y) &= f(a^r \cdot a^s) \\ &= f(a^{r+s}) \\ &= b^{r+s} \\ &= b^r + b^s \\ &= f(a^r) + f(a^s) \\ &= f(x) \cdot f(y) \end{aligned}$$

$\therefore\ f$ es Homomorfismo.

iii) Por ver que f es inyectiva.

Para verificarlo utilizaremos la demostración no clásica.

Como f es homomorfismo, por demostrar que $Ker\,(f) = \{e_G\}$, luego se tiene;

$$\begin{aligned} Ker\,(f) &= \{\ a^r \in G / f(a^r) = e_H\ \} \\ &= \{\ a^r \in G / b^r = e_H\ \} \\ &= \{\ a^r \in G / r = n = |G| = |H|\ \} \\ &= \{e_G\} \end{aligned}$$

$\therefore\ f$ es Inyectiva.

iv) Por ver que f es epiyectiva.

$\forall\ b^r \in H$, debe existir $a^t \in G$ talque $f(a^t) = b^r$

Basta considerar $t = r$ talque $f(a^r) = b^r$

$\therefore\ f$ es Epiyectiva.

En consecuencia de i), ii), iii) y iv) se tiene que f es un isomorfismo.

$G \cong H$, cuando $|G| = |H|$, con G y H grupos cíclicos.

5.4.- Guía nº5

1.- ¿Cuáles de las siguientes funciones son homomorfismos de $\mathbb{R}^* \to \mathbb{R}^*$, con la multiplicación?

a) $f_1 : \mathbb{R}^* \to \mathbb{R}^*$, donde $f(x) = |x|$

Primero debemos verificar que esté bien definida la función;

$$\begin{aligned} x &= y \quad / \mid \mid \\ |x| &= |y| \\ f(x) &= f(y) \end{aligned}$$

$\therefore$, La función está bien definida.

Claramente es un homomorfismo, pues $\forall\ x, y \in \mathbb{R}^*$, $f(x \cdot y) = |x \cdot y| = |x| \cdot |y|$.

$\therefore$ f_1 es un homomorfismo de grupos.

b) $f_2 : \mathbb{R}^* \to \mathbb{R}^*$, donde $f(x) = 2x$

Verificando que la función esté bien definida:

$$\begin{aligned} x &= y \quad / (2) \\ 2x &= 2y \\ f(x) &= f(y) \end{aligned}$$

$\therefore$, La función está bien definida.

La función f_2 no es un homomorfismo, pues $f(x \cdot y) \neq f(x) \cdot f(y)$ y se verifica de la siguiente manera:

$$\begin{aligned} f(x \cdot y) &= 2xy \\ &= 2x \cdot y \\ &= f(x) \cdot y \end{aligned}$$

$\therefore$, La función no es un homomorfismo de grupos.

2.- Probar que $f:\mathbb{C}\rightarrow\mathbb{C}$, donde $f(a+bi)=a-bi$ es un automorfismo

a) Por ver que está bien definida, es decir: Si $a+bi=c+di$, por demostrar que $f(a+bi)=f(c+di)$, luego tenemos:

$$\begin{array}{ccc} a+bi & = & c+di \\ a=c & \wedge & b=d \\ a=c & \wedge & -b=-d \\ a-bi & = & c-di \\ f(a+bi) & = & f(c+di) \end{array}$$

$\therefore$, la función está bien definida.

b) Por ver que la función es homomorfismo, es decir, por demostrar que $f(z+u)=f(z)+f(u)$, entonces tenemos:

$$\begin{array}{rcl} f(a+bi+c+di) & = & f(a+c+(d+b)i) \\ & = & a+c-(b+d)i \\ & = & a+c-bi-di \\ & = & a-bi+c-di \\ & = & f(a+bi)+f(c+di) \end{array}$$

$\therefore$ f es un homomorfismo

c) Por ver si f es inyectiva, por demostrar que si $f(a+bi)=f(c+di)$, entonces $a+bi=c+di$, $\forall$ $(a+bi),(c+di)\in\mathbb{C}$. Tenemos:

$$\begin{array}{ccc} \text{Si } f(a+bi) & = & f(c+di) \\ a-bi & = & c-di \\ a=c & \wedge & -bi=-di \\ a=c & \wedge & bi=di \\ a+bi & = & c+di \end{array}$$

$\therefore$ f, es inyectiva

d) Por ver si f es epiyectiva, es decir $\forall\, u+vi \in \mathbb{C}_{\mathrm{Re}\,c}$, $\exists\, a+bi \in \mathbb{C}_{Dom}$, tal que $f(a+bi)=u+vi$, tenemos:

Supongamos $f(a+bi) = u+vi$

$$a-bi = u+vi$$

Consideremos:

$$a=u \quad \wedge \quad -bi=vi$$
$$-b=v$$
$$b=-v$$

Luego basta considerar $u-vi \in \mathbb{C}$, tal que $f(u-vi)=u+vi$

$\therefore$ $\mathrm{Im}\, f = \mathbb{C}$

Finalmente de a), b) , c) y d) f es un automorfismo

5.5.- Autoevaluación 5

1.- ¿Cuáles de las siguientes funciones son homomorfismos de $\mathbb{R}^* \to \mathbb{R}^*$, con la multiplicación?

a) Donde $f(x) = x^2$.

b) Donde $f(x) = \dfrac{1}{x}$

c) Donde $f(x) = -x$

d) Donde $f(x) = x^3$

e) Donde $f(x) = \dfrac{-1}{x}$

f) Donde $f(x) = +\sqrt{x}$

2.- Caracterizar todos los homomorfismos definidos a continuación

a) De $\mathbb{Z}_2$ en $\mathbb{Z}_4$.

b) De $\mathbb{Z}_4$ en $\mathbb{Z}_2$.

c) De $\mathbb{Z}_6$ en $\mathbb{Z}_8$

d) De $(G = \langle(1\,2\,3)\rangle, \cdot)$ en $(\mathbb{Z}_3,+)$

e) De $\mathbb{Z}_6$ en $G = S_3$, donde $S_3 = \{(1\,2\,3),(1\,3\,2),(1\,2),(1\,3),(2\,3),(1)\}$

f) De S_3 en $\mathbb{Z}_4$

g) De $\mathbb{Z}_3$ en $\mathbb{Z}_6$

h) De $\mathbb{Z}_2 \times \mathbb{Z}_2$ en $\mathbb{Z}_6$

3.- Demuestre que $f:(\mathbb{C}\text{-}\{0\},\ \cdot) \to (\mathbb{R}\text{-}\{0\},\ \cdot)$, donde $f(a+bi) = a^2 + b^2$, $\forall\ a,b \in \mathbb{R}$ es un homomorfismo. ¿Es isomorfismo?