Homomorfismos

Sésar

1. Definición

Definition 1. Sean $(G, *_G)$ y $(H, *_H)$. Una aplicación $f : G \to H$ es un **homomorfismo** si para todo $g_1, g_2 \in G$,

$$f(g_1 *_G g_2) = f(g_1) *_H f(g_2).$$

Remark 1. Mediante inducción uno puede probar que para un conjunto finito $\{g_1, \ldots, g_n\}$ de elementos se tiene que $f(g_1 * \ldots g_n) = f(g_1) * \ldots * f(g_n)$.

Proposition 1. Sea $f : G \to H$ un homomorfismo y $g \in G$. Entonces

1. $f(e_G) = e_H$.
2. $f(g)^{-1} = f(g^{-1})$.
3. $f(g^n) = f(g)^n$ para todo $n \in \mathbb{Z}$.

Demostración. En primer lugar, para todo $x \in G$, tenemos que $x = x * e_G$, por lo que $f(x) = f(x*e) = f(x)*f(e_G)$. Por la propiedad cancelativa, $f(e_G) = e_H$. Por otro lado, $gg^{-1}g^{-1}g = e_G$. Por lo tanto, $f(g)f(g^{-1}) = f(g^{-1})f(g) = f(e_G) = e_H$. De este modo, la inversa de $f(g)$ es $f(g^{-1})$. Finalmente, por el comentario anterior, tenemos que $f(a^n) = f(g * \ldots * g) = f(a) * \ldots * f(a) = f(a)^n$ si $n > 0$. Para el caso $n = 0$, se tiene que $f(a^0) = f(e_G) = e_H = f(a)^0$ y finalmente para el caso $n < 0$, $f(a^n) = f((a^{-1})^{-n}) = f(a^{-1})^{-n} = (f(a)^{-1})^{-n} = f(a)^n$. □

Proposition 2. Sea $f : G \to H$ homomorfismo.

1. Si $K \leq G$, entonces $f(K) \leq H$.
2. Si $L \leq H$, entonces $f^{-1}(L) \leq G$.

Demostración. Por la proposición anterior, $e_H = f(e_G) \in f(K)$ y si $h \in f(K)$, entonces existe un $k \in K$ tal que $h = f(k)$, por lo que $h^{-1} = f(k)^{-1} = f(k^{-1}) \in f(K)$. Finalmente, como f es homomorfismo, $f(k_1) * f(k_2) = f(k_1 * k_2) \in f(K)$. Por lo que $f(K)$ es un subgrupo.

Por otro lado, como $f(e_G) = e_H \in L$, entonces $e_G \in f^{-1}(L)$. Por otro lado, si $g_1, g_2 \in f^{-1}(L)$, entonces existen $l_1, l_2 \in L$ tales que $l_1 = f(g_1)$ y $l_2 = f(g_2)$, por lo que $f(g_1*g_2) = f(g_1)*f(g_2) = l_1*l_2 \in L$, y deducimos que la operación en $f^{-1}(L)$ es cerrada. Finalmente, si $g \in f^{-1}(L)$, entonces $g = f(l)$, y por tanto $g^{-1} = f(l)^{-1} = f(l^{-1}) \in f^{-1}(L)$. □

Corollary 1. Sea $f : G \to H$ homomorfismo.

1. Si $N \trianglelefteq G$, entonces $f(N) \trianglelefteq f(G)$.
2. Si $M \trianglelefteq H$, entonces $f^{-1}(M) \trianglelefteq G$.

Demostración. En primer lugar, es claro ver cómo $f(N) \leq f(G)$ —pues la inclusión se mantiene cuando aplicamos f en ambos conjuntos—. Veamos que $f(N)$ es un subgrupo normal. Sea $x \in f(G)$ y $m \in f(N)$. Entonces en particular existen $g \in G$ y $n \in N$ tales que $x = f(g)$ y $m = f(n)$. Entonces $xmx^{-1} = f(g)f(n)f(g)^{-1} = f(gng^{-1})$. Como $N \trianglelefteq G$, entonces $gng^{-1} \in N$ y por lo tanto, $xmx^{-1} \in f(N)$.

Por otro lado, tomemos $g \in G$ y $n \in f^{-1}(M)$. Entonces existirá un $m \in M$ tal que $f(n) = m$. De este modo, como $M \trianglelefteq H$, entonces $f(gng^{-1}) = f(g)f(n)f(g)^{-1} = f(g)mf(g)^{-1} \in M$, luego $gng^{-1} \in f^{-1}(M)$. Como esto es cierto para todo $g \in G$, entonces $f^{-1}(M) \trianglelefteq G$. $\square$

Corollary 2. Si $S \subseteq G$, entonces $f(\langle S\rangle) = \langle f(S)\rangle$.

Demostración. Si $S = \varnothing$, entonces $\langle S\rangle = \{e_G\}$ y por lo tanto, $f(\langle S\rangle) = f(\{e_H\}) = \{f(e_H)\} = \{e_H\} = \langle\varnothing\rangle = \langle f(S)\rangle$. Por otro lado, si $S \neq \varnothing$, entonces $\langle S\rangle = \{s_1^{n_1} \ldots s_k^{n_k} \mid s_i \in S,\ n_k \in \mathbb{Z}\}$. Por lo tanto, $f(\langle S\rangle) = \{f(s_1^{n_1} \ldots s_k^{n_k}) \mid s_i \in S,\ n_k \in \mathbb{Z}\} = \{f(s_1)^{n_1} \ldots f(s_k)^{n_k} \mid s_i \in S,\ n_k \in \mathbb{Z}\} = \langle f(S)\rangle$. $\square$

Proposition 3. Si $G \xrightarrow{f} H \xrightarrow{g} K$ son homomorfismos, entonces $g \circ f$ es homomorfismo.

Demostración. Sean $x, y \in G$. Entonces como f es un homomorfismo, tenemos que $f(xy) = f(x)f(y)$. Por otro lado, $f(x)f(y) \in H$ y como g es también un homomorfismo, entonces $g(f(x)f(y)) = g(f(x))g(f(y)) = (g\circ f)(x)(g\circ f)(y)$. Pero por otro lado, $g(f(x)f(y)) = g(f(xy)) = (g \circ f)(x)$. Luego $(g \circ f)(x) = (g \circ f)(x)(g \circ f)(y)$. $\square$

Definition 2. Sea $f : G \to H$ homomorfismo.

1. El **núcleo** es el conjunto $\ker(f) := \{g \in G \mid f(g) = e_H\}$.
2. La **imagen** es el conjunto $\operatorname{im}(f) := \{h \in H \mid h = f(g),\ g \in G\}$.

Proposition 4. Sea $f : G \to H$ homomorfismo. Entonces $\ker(f) \trianglelefteq G$ e $\operatorname{im}(f) \leq H$.

Demostración. Basta con observar que $\ker(f) = f^{-1}(\{e_H\})$ e $\operatorname{im}(f) = f(G)$. $\square$

Proposition 5. Sea $f : G \to H$ homomorfismo.

1. f es inyectiva si y solo si $\ker(f) = \{e_G\}$.

2. f es sobreyectiva si y solo si $\mathrm{im}(f) = H$.

Demostración. Supongamos en primer lugar que f es un homomorfismo inyectivo. Si $x \in \ker(f)$, entonces $f(x) = e_H = f(e_G)$ y como es inyectivo, $x = e_G$, por lo que $\ker(f) \leq \{e_G\}$ y como la otra inclusión se da, tenemos la igualdad. Por otro lado, supongamos que el núcleo de f es trivial. Demostremos pues que f es inyectiva. Supongamos que $f(x) = f(y)$. Entonces como f es homomorfismo, $f(xy^{-1}) = e_H$, por lo que $xy^{-1} \in \ker(f) = \{e_G\}$, luego $xy^{-1} = e_G$ y por lo tanto, $x = y$. Finalmente, la demostración sobre la sobreyectividad de f es directa. $\square$

Decimos además que f es un **monomorfismo** si es un homomorfismo inyectivo y decimos que f es un **epimorfismo** si es un homomorfismo sobreyectivo.

Definition 3. Un **isomorfismo** es un homomorfismo biyectivo.

Proposition 6. Si $f : G \to H$ es un isomorfismo, entonces $f^{-1} : H \to H$ es también un isomorfismo.

Demostración. Si f es isomorfismo, entonces en particular es una biyección y se sabe que la aplicación inversa f^{-1} es también una biyección. Basta demostrar que f^{-1} es un homomorfismo. Sea $h_1, h_2 \in H$. Por un lado, como f es biyetiva, es en particular sobreyectiva y por tanto existen $g_1, g_2 \in G$ tales que $h_1 = f(g_1)$ y $h_2 = f(g_2)$. De este modo, obtenemos que $f^{-1}(h_1h_2) = f^{-1}(f(g_1)f(g_2)) = f^{-1}(f(g_1g_2)) = g_1g_2 = f^{-1}(f(g_1))f^{-1}(f(g_2)) = f^{-1}(h_1)f^{-1}(h_2)$. $\square$

Proposition 7. Si $G \xrightarrow{f} H \xrightarrow{g} K$ son isomorfismos, entonces $g \circ f$ es isomorfismo.

Demostración. La composición de funciones biyectivas es biyectiva y la composición de homomorfismos es un homomorfismo. Por tanto, la composición resultante es un homomorfismo biyectivo, luego un isomorfismo. $\square$

Definition 4. Dos grupos G y H son **isomorfos** $G \cong H$ si existe un isomorfismo $f : G \to H$.

Theorem 1. «Ser isomorfo» es una RBE en la clase de los grupos.

Demostración. En primer lugar, la reflexividad se da ya que $\mathrm{id}_G : G \to G$ es un isomorfismo. Por otro lado, si $G \cong H$, entonces $f : G \to H$ es un isomorfismo, por lo que $f^{-1} : H \to G$ es también isomorfismo y en consecuencia, $H \cong G$ dándose de esta manera la simetría. Finalmente, si $G \cong H$ y $H \cong K$, entonces $f : G \to H$ y $g : H \to K$ son isomorfismos y por proposición, $g \circ f : G \to K$ es un isomorfismo, por lo que $G \cong K$ probando que la transitividad se cumple. $\square$

2. Automorfismos

Definition 5. Un **automorfismo** de un grupo G es un isomorfismo $f : G \to G$.

$$\mathrm{Aut}(G) := \{f : G \to G \mid f \text{ isomorfismo}\}.$$

Proposition 8. $\mathrm{Aut}(G)$ con la composición de funciones es un grupo.

Demostración. En primer lugar, la composición de funciones isomorfas es un isomorfismo, luego la operación es cerrada en $\mathrm{Aut}(G)$. Además, la composición de funciones es claramente asociativa. Por otro lado, $\mathrm{id}_G \in \mathrm{Aut}(G)$ es el elemento neutro con respecto a la composición. Finalmente, si $f \in \mathrm{Aut}(G)$, entonces $f^{-1} : G \to G$ es también un isomorfismo, luego $f^{-1} \in \mathrm{Aut}(G)$. □

Definition 6. Un **automorfismo interno** en G es una aplicación de la siguiente forma:

$$\begin{aligned} \theta_g : G &\to G \\ x &\mapsto gxg^{-1} \end{aligned}$$

Denotamos el conjunto de automorfismos internos como $\mathrm{Inn}(G) := \{\theta_g \mid g \in G\}$.

Lemma 1. Los $\theta_g \in \mathrm{Inn}(G)$ son automorfismos.

Demostración. En primer lugar, veamos que son homomorfismos. Sea $g \in G$. Entonces $\theta_g(xy) = gxyg^{-1} = gxg^{-1}gxg^{-1} = \theta_g(x)\theta_g(y)$. Por otro lado, es claramente biyectiva, pues su función inversa puede calcularse como $(\theta_g)^{-1} = \theta_{g^{-1}}$. Por tanto, θ_g es un homomorfismo biyectivo de G en G, es decir, θ_g es un automorfismo. □

Proposition 9. $\mathrm{Inn}(G)$ con la composición de funciones es un grupo.

Demostración. En primer lugar, veamos que la operación es cerrada con la composición. Sean $g, h \in G$, entonces $(\theta_g \circ \theta_h)(x) = \theta_g(\theta_h(x)) = \theta_g(hxh^{-1}) = g(hxh^{-1})g^{-1} = (gh)x(h^{-1}g^{-1}) = (gh)x(gh)^{-1} = \theta_{gh}(x)$. Por lo tanto, $\theta_g \circ \theta_h = \theta_{gh} \in \mathrm{Inn}(G)$. Luego la operación es cerrada en este conjunto y además es claramente asociativa. Notemos por otro lado que $\mathrm{id}_G = \theta_e \in \mathrm{Inn}(G)$, luego existe elemento neutro en este conjunto. Finalmente. Es fácil comprobar que los automorfismos internos son biyectivos y que $(\theta_g)^{-1} = \theta_{g^{-1}} \in \mathrm{Inn}(G)$. □

Proposition 10. Sea G un grupo. Entonces $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G) \leq S(G)$.

Demostración. En primer lugar, es claro ver que $\mathrm{Inn}(G) \subseteq \mathrm{Aut}(G) \subseteq S(G)$ y como todos ellos formanun grupo con la misma operación composición de funciones, entonces por definición $\mathrm{Inn}(G) \leq \mathrm{Aut}(G) \leq S(G)$. Por otro lado, veamos que los automorfismos internos forman un subgrupo normal con los automorfismos. Sea $g \in G$ y $f \in \mathrm{Aut}(G)$. entonces $(f \circ \theta_g \circ f^{-1})(x) = f(\theta_g(f^{-1}(x))) = f(gf^{-1}(x)g^{-1}) = f(g)f(f^{-1}(x))f(g^{-1}) = f(g)xf(g)^{-1}$. De esta manera, $f \circ \theta_g \circ f^{-1} = \theta_{f(g)} \in \mathrm{Inn}(G)$. $\square$