Sea $b \in \bar{a}$. Luego, $b \equiv a \pmod{H}$. Es decir, existe $h \in H$ tal que

$$b \cdot a^{-1} = h$$
$$b = h \cdot a.$$

Entonces, todo $b \in \bar{a}$ es de la forma $b = h \cdot a$ con $h \in H$. Recíprocamente, para todo $h \in H$ y $a \in G$, notamos que $h \cdot a \in \bar{a}$. Por lo tanto, conviene cambiar la notación de $\bar{a}$ por

$$Ha = \{ h \cdot a \,/\, h \in H \}$$

Como G es finito, existe un número finito de clases de equivalencia, digamos

$$H, Ha_1, \dots, Ha_{q-1}$$

(donde H corresponde a la clase de e). Sabemos además que G se descompone como unión disjunta de sus clases de equivalencia.

$$G = H \cup Ha_1 \cup \dots \cup Ha_{q-1}.$$

Luego,

$$o(G) = \text{Card}(H) + \text{card}(Ha_1) + \dots + \text{Card}(Ha_{q-1}).$$

Notamos además que $h \longmapsto h \cdot a_i$ define una biyección entre H y Ha_i, por lo cual

$$\text{Card}(Ha_i) = \text{Card}(H) = o(H)$$

para todo $1 \le i \le q$

Escaneado con CamScanner

Por lo tanto,

$$o(G) = o(H) + o(H) + \cdots + o(H) \quad (q \text{ veces})$$

$$o(G) = q \cdot o(H).$$

Es decir, $o(H) \mid o(G)$, lo cual demuestra el Teorema de Lagrange.

Veamos ahora algunas aplicaciones.

Aplicación 1: Sea $(G, \cdot)$ un grupo finito. Si $o(G)$ es primo, entonces G es cíclico.

- Demostración: Note que $G \neq \{e\}$, ya que $o(G) \neq 1$. Sea $g \in G$ y consideremos $H = \langle g \rangle$. Sabemos por un lado que $o(H) = o(g) \neq 1$. Por otro lado, por el Teorema de Lagrange, se tiene que $o(H) \mid o(G)$. Como $o(G)$ es primo y $o(H) \neq 1$, tenemos que $o(H) = o(G)$. Luego, H es un subgrupo de G con la misma cantidad de elementos que G, por lo cual $G = H = \langle g \rangle$. ∎

Aplicación 2 (teorema de Fermat-Euler): Sea $m \in \mathbb{Z}^+$, $m \geq 2$, y $a \in \mathbb{Z}$ tal que $\text{mcd}(a, m) = 1$. Entonces,

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Escaneado con CamScanner

· Demostración: Para $a \in \mathbb{Z}$ con $\text{mcd}(a, m) = 1$, tenemos que $\bar{a} \in U(m)$. Por el Teorema de Lagrange, $o(\langle \bar{a} \rangle) \mid o(U(m))$, es decir,

$$o(\bar{a}) \mid \varphi(m).$$

Entonces, $\bar{a}^{\varphi(m)} = \bar{1}$, es decir,

$$a^{\varphi(m)} \equiv 1 \pmod{m}. \quad \blacksquare$$

Aplicación 3 (infinitud de los primos): Se puede demostrar que hay infinitos números primos a partir del Teorema de Lagrange.

Supongamos que hay un número finito de primos, y sea p el primo más grande. Consideremos el número de Mersenne $2^p - 1$, y sea q un factor primo de $2^p - 1$.

$$q \mid (2^p - 1) \Longrightarrow 2^p \equiv 1 \pmod{q}.$$

En el grupo $\mathbb{Z}_q^*$ (q es primo), tenemos que

$$\bar{2}^p = \bar{1}.$$

Como p es primo, $o(\bar{2}) = p$. Por el Teorema de Lagrange, $o(\bar{2}) \mid o(\mathbb{Z}_q^*)$, es decir, $p \mid (q-1)$. De esto se sigue que $p < q$, lo cual es una contradicción (recuerde que p es el primo más grande dentro del conjunto de números primos, asumido finito). $\blacksquare$

Escaneado con CamScanner

Homomonfismos

Idea central: $(G, *)$ grupo (conjunto con operación)

φ (función)

(K, Δ) grupo

¿Cuáles son las funciones que preservan las operaciones entre grupos?

Esto lo responde el concepto de homomonfismo.

Definición: Sean $(G, *)$ y (K, Δ) dos grupos. Un homomonfismo de $(G, *)$ a (K, Δ) es una función

$$\varphi : G \to K$$

tal que

$$\varphi(g_1 * g_2) = \varphi(g_1) \Delta \varphi(g_2)$$

$$\forall\, g_1, g_2 \in G.$$

Ejemplos:

1) $id : (G, *) \to (G, *)$ es claramente un homomonfismo.

$id(g) = g$

Escaneado con CamScanner

2) Homomorfismo trivial: $\varphi: (G, *) \to (K, \Delta)$

$\varphi(g) = e_K, \ \forall g \in G.$

$\varphi(g_1 \cdot g_2) = e_K = e_K \Delta e_K = \varphi(g_1) \Delta \varphi(g_2).$

3) $G = (\mathbb{R}, +)$, $K = (\mathbb{R}^+, \cdot)$

$\varphi: (\mathbb{R}, +) \longrightarrow (\mathbb{R}^+, \cdot)$

$\varphi(x) = e^x$ (función exponencial)

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

4) $\chi: (\mathbb{R}^+, \cdot) \longrightarrow (\mathbb{R}, +)$

$\chi(x) = Ln(x)$

$\chi(x \cdot y) = Ln(x \cdot y) = Ln(x) + Ln(y)$

$= \chi(x) + \chi(y).$

5) $G = (M_{m\times m}(\mathbb{R}), +)$, $K = (\mathbb{R}, +)$

$\varphi: M_{m\times m}(\mathbb{R}) \to \mathbb{R}$ $\qquad$ $\chi: M_{m\times m}(\mathbb{R}) \to M_{m\times m}(\mathbb{R})$

$\varphi(A) = \text{traza}(A)$ $\qquad$ $\chi(A) = A^t$

son ambos homomorfismos, por las propiedades de la traza y de la trasposición.

Escaneado con CamScanner

6) $G = (GL(n, \mathbb{R}), \cdot)$, $K = (\mathbb{R}^*, \cdot)$

$\det : GL(n, \mathbb{R}) \longrightarrow \mathbb{R}^*$ es un homomorfismo por la fórmula de Binet-Cauchy.

7) $G = (\mathbb{Z}, +)$, $n \in \mathbb{Z}$ fijo.

$\varphi_n(x) = nx$ es un homomorfismo de $\mathbb{Z}$ en sí mismo.

$$\varphi_n(x+y) = n(x+y) = nx + ny = \varphi_n(x) + \varphi_n(y).$$

8) Regla de los signos: $G = (\mathbb{R}^*, \cdot)$, $K = (\{-1, 1\}, \cdot)$

$$\varphi : \mathbb{R}^* \longrightarrow \{-1, 1\}$$

$$\varphi(x) = \begin{cases} 1 & \text{si } x > 0 \\ -1 & \text{si } x < 0. \end{cases}$$

φ es un homomorfismo.

Considere $x, y \in \mathbb{R}^*$.

i) $x, y > 0$: $\varphi(xy) = 1 = 1 \cdot 1 = \varphi(x) \cdot \varphi(y)$

ii) $x > 0$, $y < 0$: $\varphi(xy) = -1 = 1 \cdot (-1) = \varphi(x) \cdot \varphi(y)$

iii) $x < 0$, $y > 0$: $\varphi(xy) = -1 = -1 \cdot 1 = \varphi(x) \cdot \varphi(y)$.

iv) $x < 0$, $y < 0$: $\varphi(xy) = 1 = (-1) \cdot (-1) = \varphi(x) \cdot \varphi(y)$.

9) $G = (\mathbb{Z}, +)$, $K = (\mathbb{Z}_m, +)$, $m \in \mathbb{Z}^+$, $m \geq 2$ fijo

$\varphi : \mathbb{Z} \to \mathbb{Z}_m$

$\varphi(x) = \bar{x}$ es un homomorfismo (llamado proyección canónica).

Escaneado con CamScanner

10) $G = (D_4, \circ)$, $K = (GL(2, \mathbb{R}), \cdot)$

$$\varphi(r) = \begin{pmatrix} \cos(90°) & -\sin(90°) \\ \sin(90°) & \cos(90°) \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

$$\varphi(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Como r y s generan a todos los elementos de D_4, podemos extender φ a todo D_4 de la siguiente manera:

$$\varphi(id) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\varphi(r^2) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\varphi(r^3) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$\varphi(sr) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\varphi(sr^2) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$$

$$\varphi(sr^3) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

- $\varphi: D_4 \longrightarrow GL(2, \mathbb{R})$ es un homomorfismo (por construcción).

Escaneado con CamScanner

Propiedades elementales de los homomorfismos:

Sean $(G, *)$ y $(K, \diamond)$ grupos, y $\varphi : G \to K$ un homomorfismo. Las siguientes afirmaciones se cumplen:

1) $\varphi(e_G) = e_K$.
2) $\varphi(g^{-1}) = [\varphi(g)]^{-1} \quad \forall g \in G$
3) $\varphi(g^m) = [\varphi(g)]^m \quad \forall g \in G, \forall m \in \mathbb{Z}$.
4) Si $g \in G$ y $o(g) < \infty$, entonces $o(\varphi(g)) < \infty$ y $o(\varphi(g)) \mid o(g)$.
5) Si $\chi : (K, \diamond) \to (H, \square)$ es otro homomorfismo de grupos, entonces $\chi \circ \varphi$ también lo es.

- **Demostración:**

1) $\varphi(e_G) = \varphi(e_G * e_G) = \varphi(e_G) \diamond \varphi(e_G)$

$\varphi(e_G) \diamond e_K = \varphi(e_G) \diamond \varphi(e_G)$

Por ley cancelativa, se tiene que $\varphi(e_G) = e_K$.

2) $\varphi(g) \diamond \varphi(g^{-1}) = \varphi(g * g^{-1}) = \varphi(e_G) = e_K$

Por la unicidad del elemento inverso de $\varphi(g)$, se tiene que $[\varphi(g)]^{-1} = \varphi(g^{-1})$.

3) i) $n > 0$: Usamos inducción sobre n

- $n = 2$ es el paso inicial.

$$\varphi(g^2) = \varphi(g * g) = \varphi(g) \diamond \varphi(g) = [\varphi(g)]^2$$

Escaneado con CamScanner

- Supongamos $\varphi(g^m) = [\varphi(g)]^m$.

$$\varphi(g^{m+1}) = \varphi(g^m * g) = \varphi(g^m) \triangle \varphi(g)$$
$$= [\varphi(g)]^m \triangle \varphi(g) \quad (\text{por hipótesis inductiva})$$
$$= [\varphi(g)]^{m+1}.$$

$\therefore \varphi(g)^m = \varphi(g^m) \quad \forall m \in \mathbb{Z}^+$.

ii) $n = 0$: $\varphi(g^0) = \varphi(e_G) = e_K = [\varphi(g)]^0$.

iii) $n < 0$: $\varphi(g^n) = \varphi((g^{-1})^{|n|})$

$$= [\varphi(g^{-1})]^{|n|} \quad (\text{por la parte i})$$
$$= [(\varphi(g))^{-1}]^{|n|} \quad (\text{por la parte 2})$$
$$= [\varphi(g)]^n.$$

4) Sea $m = o(g)$.

$$g^m = e_G \Rightarrow \varphi(g^m) = \varphi(e_G)$$
$$\Rightarrow [\varphi(g)]^m = e_K \quad (\text{por las partes 1) y 3})$$

Luego, $o(\varphi(g)) < \infty$ y $o(\varphi(g)) \mid m$.

5) Considere la composición $\chi \circ \varphi : (G, *) \to (H, \square)$.

Sean $g_1, g_2 \in G$.

$$(\chi \cdot \varphi)(g_1 * g_2) = \chi(\varphi(g_1 * g_2)) = \chi(\varphi(g_1) \triangle \varphi(g_2))$$
$$= \chi(\varphi(g_1)) \square \chi(\varphi(g_2))$$
$$= (\chi \circ \varphi)(g_1) \square (\chi \circ \varphi)(g_2). \blacksquare$$

Escaneado con CamScanner

Existen subgrupos especiales asociados a todo homomorfismo.

Definición: Sea $\varphi: (G,*) \longrightarrow (K,\circ)$ un homomorfismo. Se definen el núcleo e imagen de φ como los siguientes subconjuntos de G y K, respectivamente:

$$Ker(\varphi) = \{ g \in G \,/\, \varphi(g) = e_K \}$$

$$Im(\varphi) = \{ \varphi(g) \,/\, g \in G \}.$$

Ejemplos: Haciendo referencia a los homomorfismos del ejemplo anterior:

1) $Ker(id) = \{e_G\}$, $Im(id) = G$.

2) $Ker(\varphi) = G$, $Im(\varphi) = \{e_K\}$.

3) $\varphi(x) = 1 \quad \forall x \in Ker(\varphi)$.

$e^x = 1 \iff x = 0$

$Ker(\varphi) = \{0\}$.

Sea $y \in \mathbb{R}^+$. Luego, $y = \varphi(Ln(y)) \in Im(\varphi)$.

$Im(\varphi) = \mathbb{R}^+$.

4) De manera similar a 3), $Ker(\psi) = \{Id\}$ e

$Im(\psi) = \mathbb{R}$.

5) $Ker(\varphi) = \{A \in M_{n\times n}(\mathbb{R}) \,/\, traza(A) = 0\}$.

$Ker(\psi) = \{0_{n\times n}\}$.

Escaneado con CamScanner

$Im(\varphi) = \mathbb{R}$. Em efecto, para todo $x \in \mathbb{R}$ podemos construir

$$A = \begin{pmatrix} x & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix},$$

y así $x = traza(A) = \varphi(A)$.

$Im(\chi) = M_{m\times m}(\mathbb{R})$, ya que para todo $A \in M_{m\times m}(\mathbb{R})$ se tiene que

$$A = [A^t]^t = \chi(A^t).$$

6) Sea $A \in GL(m, \mathbb{R})$.

$det(A) = 1 \iff A \in SL(m, \mathbb{R})$.

$Ker(det) = SL(m, \mathbb{R})$.

$Im(det) = \mathbb{R}^*$. Em efecto, para $x \in \mathbb{R}^*$ podemos construir

$$A = \begin{pmatrix} x & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \in GL(m, \mathbb{R}),$$

y así $x = det(A)$.

7) $Ker(\varphi) = 0$ e $Im(\varphi) = n\mathbb{Z}$.

8) $Ker(\varphi) = \mathbb{R}^+$ e $Im(\varphi) = \{-1, 1\}$.

9) $Ker(\varphi) = n\mathbb{Z}$ e $Im(\varphi) = \mathbb{Z}_n$.

Escaneado con CamScanner

10) $\ker(\varphi) = \{id\}$, $\operatorname{Im}(\varphi) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$.

Propiedades del núcleo y la imagen: Sea $\varphi: (G, *) \to (K, \Delta)$ un homomorfismo de grupos. Las siguientes afirmaciones se cumplen:

1) $\ker(\varphi) < G$

2) $\operatorname{Im}(\varphi) < K$.

3) φ es inyectivo si y sólo si $\ker(\varphi) = \{e_G\}$.

4) φ es sobreyectivo si y solamente si $\operatorname{Im}(\varphi) = K$.

5) Si $H < K$, entonces $\varphi^{-1}(H) < G$ y $\ker(\varphi) \subseteq \varphi^{-1}(H)$.

Recuerde que $\varphi^{-1}(H)$ denota la imagen inversa de H a través de φ, es decir,

$$\varphi^{-1}(H) = \{ g \in G \mid \varphi(g) \in H \}.$$

· **Demostración:**

1) $\ker(\varphi) \neq \emptyset$ ya que $e_G \in \ker(\varphi)$ $(\varphi(e_G) = e_K)$.

Sean $g_1, g_2 \in \ker(\varphi)$. Luego,

$$\varphi(g_1 * g_2) = \varphi(g_1) \Delta \varphi(g_2) = e_K \Delta e_K = e_K \quad (\text{ya que } g_1 \in \ker(\varphi) \text{ y } g_2 \in \ker(\varphi))$$

$\therefore g_1 * g_2 \in \ker(\varphi)$.

Escaneado con CamScanner

Sea $g \in \ker(\varphi)$. Luego, $\varphi(g^{-1}) = [\varphi(g)]^{-1} = (e_K)^{-1} = e_K$.

Es decir, $g^{-1} \in \ker(\varphi)$.

$\therefore \ker(\varphi) < G$.

2) $\text{Im}(\varphi) \neq \emptyset$ ya que $e_K = \varphi(e_G) \in \text{Im}(\varphi)$.

Sean $\varphi(g_1), \varphi(g_2) \in \text{Im}(\varphi)$. Luego,

$$\varphi(g_1) * \varphi(g_2) = \varphi(g_1 * g_2) \in \text{Im}(\varphi).$$

Sea $\varphi(g) \in \text{Im}(\varphi)$. Luego,

$$[\varphi(g)]^{-1} = \varphi(g^{-1}) \in \text{Im}(\varphi).$$

$\therefore \text{Im}(\varphi) < K$.

3) ($\Rightarrow$) Supongamos que φ es inyectiva y sea $g \in \ker(\varphi)$.

$\varphi(g) = e_K = \varphi(e_G)$. Como φ es inyectiva, lo anterior implica que $g = e_G$.

$\therefore \ker(\varphi) = \{e_G\}$.

($\Leftarrow$) Supongamos que $\ker(\varphi) = \{e_G\}$, y sean $g_1, g_2 \in G$ tales que $\varphi(g_1) = \varphi(g_2)$. Multiplicando por el inverso de $\varphi(g_2)$, se obtiene:

$$\varphi(g_1) * [\varphi(g_1)]^{-1} = \varphi(g_2) * [\varphi(g_2)]^{-1}$$

$$\varphi(g_1) * \varphi(g_2^{-1}) = e_K$$

$$\varphi(g_1 * g_2^{-1}) = e_K,$$

es decir, $g_1 * g_2^{-1} \in \ker(\varphi) = \{e_G\}$. Entonces, $g_1 * g_2^{-1} = e_G$,

es decir, $g_1 = g_2$.

Escaneado con CamScanner

4) Es inmediato a partir de la definición de función sobreyectiva.

5) Sea $g \in Ker(\varphi)$. Luego,

$$\varphi(g) = e_K \in H \text{ ya que } H < K.$$

Entonces, $g \in \varphi^{-1}(H)$. Por lo tanto, $Ker(\varphi) \subseteq \varphi^{-1}(H)$.

Lo anterior implica que $\varphi^{-1}(H) \neq \emptyset$.

Ahora considere $g_1, g_2 \in \varphi^{-1}(H)$.

$$\varphi(g_1 * g_2^{-1}) = \varphi(g_1) \Delta \varphi(g_2^{-1}) = \varphi(g_1) \Delta [\varphi(g_2)]^{-1}$$

donde $\varphi(g_1), \varphi(g_2) \in H$. Como $H < K$, tenemos que

$$\varphi(g_1) \Delta [\varphi(g_2)]^{-1} \in H,$$

es decir,

$$\varphi(g_1 * g_2^{-1}) \in H$$

$$(g_1 * g_2^{-1} \in \varphi^{-1}(H))$$

Lo anterior implica que $\varphi^{-1}(H) < G$. ∎

El siguiente resultado da una relación entre los órdenes de G, $Ker(\varphi)$ e $Im(\varphi)$, donde $\varphi: (G, *) \to (K, \Delta)$ es un homomorfismo entre grupos finitos. Puede pensarse como el análogo en Teoría de grupos del teorema de las dimensiones visto en álgebra lineal. La demostración se verá posteriormente como consecuencia del Teorema de Lagrange y el Primer Teorema de Isomorfismos.

Escaneado con CamScanner

Teorema de los órdenes: Sea $\varphi : (G, *) \to (K, \Delta)$ un homomorfismo de grupos (finitos). Entonces,

$$o(G) = o(\text{Ker}(\varphi)) \cdot o(\text{Im}(\varphi)).$$

Observación: El teorema anterior también vale para homomorfismos entre grupos infinitos.

Estudiemos ahora los homomorfismos que son biyectivos.

Definición: Un homomorfismo de grupos

$$\varphi : (G, *) \to (K, \Delta)$$

es un <u>isomorfismo</u> si φ es biyectiva. En tal caso, diremos que los grupos G y K son <u>isomorfos</u>.

Los isomorfismos $(G, *) \to (G, *)$ son llamados <u>automorfismos</u>.

Ejemplos: Las siguientes funciones son isomorfismos entre sus respectivos grupos.

1) $id : (G, *) \to (G, *)$ es un automorfismo de $(G, *)$

2) $\exp : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ es un isomorfismo.

$\exp(x) = e^x$

Note que su inversa $\text{Ln} : (\mathbb{R}^+, \cdot) \to (\mathbb{R}, +)$ también es un homomorfismo.

3) $(-)^t : M_{m\times n}(\mathbb{R}) \to M_{n\times m}(\mathbb{R})$ es un automorfismo

Escaneado con CamScanner

Propiedades de los isomonfismos:

Sea $\varphi: (G, *) \to (K, \Delta)$ un homomonfismo de grupos.

1) φ es un isomonfismo si y solamente si $Ker(\varphi) = \{e_G\}$ e $Im(\varphi) = K$.

2) Si φ es un isomonfismo, entonces φ^{-1} también lo es.

3) Si φ es un isomonfismo, entonces $o(G) = o(K)$.

4) Si φ es un isomonfismo, entonces G es abeliano si y solamente si K es abeliano.

5) Si φ es un isomonfismo, entonces $o(g) = o(\varphi(g))$ $\forall g \in G$.

· Demostración:

1) φ isomonfismo $\Leftrightarrow$ φ ingectiva $\Leftrightarrow Ker(\varphi) = \{e_G\}$.
φ sobreyectiva $\Leftrightarrow Im(\varphi) = K$.

2) Basta probar que $\varphi^{-1}(k_1 \Delta k_2) = \varphi^{-1}(k_1) * \varphi^{-1}(k_2)$.

$\exists!\ g_1, g_2 \in G$ / $k_1 = \varphi(g_1)$ y $k_2 = \varphi(g_2)$.

Luego,

$$\varphi^{-1}(k_1 \Delta k_2) = \varphi^{-1}(\varphi(g_1) \Delta \varphi(g_2)) = \varphi^{-1}(\varphi(g_1 * g_2))$$
$$= g_1 * g_2$$
$$= \varphi^{-1}(k_1) * \varphi^{-1}(k_2).$$

3) Si G es infinito, entonces K también (de lo contrario, φ no sería ingectiva). En este caso,

$$o(G) = \infty = o(K).$$

Escaneado con CamScanner

Supongamos ahora que $o(G) < \infty$. Entonces, $o(K) < \infty$ (de lo contrario, φ no sería sobreyectivo). Al ser $\varphi: G \to K$ una función biyectiva, se tiene que

$$\text{Card}(G) = \text{Card}(K),$$

es decir,

$$o(G) = o(K).$$

4) Supongamos que φ es un isomorfismo y que G es abeliano. Sean $k_1, k_2 \in K$. Luego, existen $g_1, g_2 \in G$ tales que

$$k_1 = \varphi(g_1) \text{ y } k_2 = \varphi(g_2).$$

Entonces,

$$k_1 \Delta k_2 = \varphi(g_1) \Delta \varphi(g_2) = \varphi(g_1 * g_2) = \varphi(g_2 * g_1) = \varphi(g_2) \Delta \varphi(g_1)$$

(G abeliano)

$$k_1 \Delta k_2 = \varphi(g_2) \Delta \varphi(g_1) = k_2 \Delta k_1.$$

La demostración K abeliano $\Rightarrow$ G abeliano es análoga.

5) Sea $g \in G$.

- Si $o(g) = \infty$, entonces $o(\varphi(g)) = \infty$.

Supongamos lo contrario: $o(\varphi(g)) < \infty$.

$$= n$$

Luego, $[\varphi(g)]^n = \varphi(g^n)$

$$e_K = \varphi(g^n), \text{ i.e., } g^n \in \text{Ker}(\varphi) = \{e_G\}.$$

Entonces, $g^n = e_G$, de donde $o(g) < \infty$. ($\lightning$).

$\therefore o(\varphi(g)) = \infty = o(g)$.

Escaneado con CamScanner

- Si $o(g) = n < \infty$: Por una propiedad anterior, $o(\varphi(g)) = m < \infty$ y $o(\varphi(g)) \mid o(g)$.

Por otro lado,

$$e_k = [\varphi(g)]^m = \varphi(g^m).$$

Luego, $g^m \in \ker(\varphi) = \{e_G\}$, de donde $g^m = e_G$. Esto a su vez implica que

$$n \mid m \quad (o(g) \mid o(\varphi(g))).$$

Finalmente, $o(\varphi(g)) \mid o(g)$ y $o(g) \mid o(\varphi(g))$ implica que

$$o(g) = o(\varphi(g)). \quad \blacksquare$$

Escaneado con CamScanner