Primer teorema de isomorfismo $\qquad$ f inyectivo $\Leftrightarrow$ $\ker f = \{e\}$

* sea $f: G_1 \to G_2$ un morfismo de grupos sobreyectivo

$$\underbrace{G_1/\ker f \simeq G_2}_{\text{isomorfos}}$$

$$g\ker f \quad \boxed{g, g', g''} \xrightarrow{f} h$$

$$k\ker f \quad \boxed{k, k', k''} \longrightarrow \tilde{h}$$

$$e_{G_1}\ker f \quad \boxed{e_{G_1}, r, r'} \longrightarrow e$$

* sea $f: G_1 \to G_2$ un morfismo de grupos

$\to f: G_1 \to \operatorname{Im} f$ morfismo de grupos sobreyectivo

$$G_1/\ker f \simeq \operatorname{Im} f$$

Ejercicio 7. Sea G un grupo, con neutro e_G. Probar que $G/\{e_G\} \simeq G$ y $G/G \simeq \{e_G\}$.

* $G/\{e_G\} \simeq G$

buscamos un morfismo de grupos $f: G \to G$ sobreyectivo tal que $\ker f = \{e_G\}$

tomamos: $\quad id: G \to G$

$\to$ es un morfismo de grupos

$$id(g * g') = g * g' = id(g) * id(g')$$

$\to$ es sobreyectivo

$\to \ker(id) = \{e_G\}$

entonces por el primer teorema de isomorfismo

$$G/\ker(id) \simeq G \iff G/\{e_G\} \simeq G$$

$$G/H = \{gH : g \in G\}$$

$$e_G H = H$$

$* \quad G/G \simeq \{e_G\}$

para aplicar el primer teorema de isomorfismo buscamos un morfismo de grupos $f: G \to \{e_G\}$ sobreyecho tal que $\ker f = G$

tomamos: $f: G \to \{e_G\}$ el morfismo trivial
$f(g) = e_G$ para todo $g \in G$

$\to$ morfismo de grupos : $f(g * g') = e_G = e_G * e_G = f(g) * f(g')$
$\to$ sobreyecho ✓
$\to \ker f = G$

entonces el primer teorema de isomorfismo nos dice

$$G/\ker f \simeq \{e_G\}$$

$$\Rightarrow G/G \simeq \{e_G\}$$

Ejercicio 8. Sea $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ dado por $f(x, y) = 17x - 12y$.

- **a**. Probar que f es un morfismo de grupos.
- **b**. Probar que $Ker(f)$ es el subgrupo de $\mathbb{Z} \times \mathbb{Z}$ generado por $(12, 17)$.
- **c**. Concluir que $\frac{\mathbb{Z}\times\mathbb{Z}}{\langle(12,17)\rangle} \simeq \mathbb{Z}$

$f: \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z} \qquad f(x,y) = 17x - 12y$

grupo con la suma coordenada a coordenada

grupo con la suma

a) veamos que f es morfismo de grupos
sean $(x,y), (x',y') \in \mathbb{Z}\times\mathbb{Z}$

$$f((x,y)+(x',y')) = f(x,y) + f(x',y')$$

$$f((x,y)+(x',y')) = f(x+x', y+y')$$
$$= 17(x+x') - 12(y+y')$$
$$= 17x - 12y + 17x' - 12y'$$
$$= f(x,y) + f(x',y')$$

$\Rightarrow f$ es morfismo de grupos.

b) $\ker f = \langle (12,17) \rangle$?

$$\langle (12,17) \rangle = \{(12,17), \overbrace{(12,17)+(12,17)}^{(2\cdot 12,\, 2\cdot 17)}, \overbrace{(12,17)+(12,17)+(12,17)}^{(3\cdot 12,\, 3\cdot 17)}$$
$$= \{\underbrace{(12k, 17k)}_{(12,17)^k} : k \in \mathbb{Z}\}$$

sea $(a,b) \in \ker f$

objetivo: $(a,b) = (12n, 17n)$ con $n \in \mathbb{Z}$

$$f(a,b) = 0 \Rightarrow 17a - 12b = 0$$
$$\Rightarrow 17a = 12b$$
$$\Rightarrow 12 \mid 17a$$
$$\Rightarrow 12 \mid a$$
$$\Rightarrow a = 12n \text{ para algún } n \in \mathbb{Z}$$

$\left.\begin{array}{l} 12 \mid 17a \\ 12 \text{ y } 17 \text{ coprimos} \end{array}\right\} \Rightarrow 12 \mid a$

lema de Euclides

entonces $17a = 12b \Rightarrow 17 \cdot 12n = 12b$
$$\Rightarrow 17n = b$$

$(a,b) \in \ker f \Rightarrow (a,b) = (12n, 17n) \in \langle (12,17) \rangle$

entonces $\ker f \subset \langle (12,17) \rangle$

nos falta ver que $\langle (12,17) \rangle \subset \ker f$:

sea $(x,y) \in \langle (12,17) \rangle$

$\Rightarrow (x,y) = (12k, 17k)$ para algún $k \in \mathbb{Z}$

$$f(x,y) = f(12k, 17k) = 17 \cdot 12k - 12 \cdot 17k = 0$$
$$\Rightarrow (x,y) \in \ker f$$

conclusión: $\ker f = \langle (12,17) \rangle$

c) $\mathbb{Z}\times\mathbb{Z}/\langle(12,17)\rangle \simeq \mathbb{Z}$

tenemos:

* $f: \mathbb{Z}\times\mathbb{Z} \longrightarrow \mathbb{Z}$ morfismo de grupos

  $f(x,y) = 17x - 12y$

* $\ker f = \langle(12,17)\rangle$

vamos a ver que f es sobreyectiva:

sea $m \in \mathbb{Z}$

buscamos $(x,y) \in \mathbb{Z}\times\mathbb{Z}$ tal que $f(x,y) = m$

es decir buscamos $x, y \in \mathbb{Z}$ tales que

$$17x - 12y = m$$

como 17 y 12 son coprimos esta ecuación diofántica tiene solución

es decir existen $x_0, y_0 \in \mathbb{Z}$ tales que

$$f(x_0,y_0) = 17x_0 - 12y_0 = m$$

Entonces: como $f: \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$ es morfismo de grupos sobreyectivo, por el teorema de isomorfismo

$$\mathbb{Z}\times\mathbb{Z}/\ker f \simeq \mathbb{Z}$$

$$\Rightarrow \mathbb{Z}\times\mathbb{Z}/\langle(12,17)\rangle \simeq \mathbb{Z}$$

Ejercicio 3

e. $G = U(15)$, $K = \mathbb{Z}_6$. Sugerencia: hallar el orden de todos los elementos de G.

buscamos $f: U(15) \to \mathbb{Z}_6$ morfismo de grupos no trivial

$|U(15)| = \varphi(15) = \varphi(3 \cdot 5) = \varphi(3)\varphi(5) = 2 \cdot 4 = 8$

U(15)

g	$o(g)$
$\bar{1}$	1
$\bar{2}$	4
$\bar{4}$	2
$\bar{7}$	4
$\bar{8}$	4
$\overline{11}$	2
$\overline{13}$	4
$\overline{14}$	2

$\to$ posibilidades para $o(g)$: 1, 2, 4, 8

$\bar{2}^2 = \bar{4}$ $\quad \bar{2}^4 = \bar{4}^2 = \overline{16} = \bar{1}$

$\bar{4}^2 = \overline{16} = \bar{1}$

$\bar{7}^2 = \bar{4}$ $\quad \bar{7}^4 = \bar{4}^2 = \bar{1}$

$\bar{8}^2 = \bar{4}$

$\overline{11}^2 = \overline{121} = \bar{1}$

$\overline{13}^2 = \bar{4}$

$\overline{14}^2 = \overline{196} = \bar{1}$

$\Rightarrow U(15)$ no es cíclico

$\mathbb{Z}_6$

g	$o(g)$
$\bar{0}$	1
$\bar{1}$	6
$\bar{2}$	3
$\bar{3}$	2
$\bar{4}$	3
$\bar{5}$	6

$\leftarrow$ posibilidades: 1, 2, 3, 6

$f: U(15) \to \mathbb{Z}_6$ morfismo de grupos

* $|\ker f|\,|\operatorname{Im} f| = |U(15)|$

$|\ker f|\,|\operatorname{Im} f| = 8$ $\quad |\operatorname{Im} f| \mid 8$

* $\operatorname{Im} f$ es subgrupo de $\mathbb{Z}_6$

$\Rightarrow |Imf| \mid |\mathbb{Z}_6|$

$$\boxed{|Imf| \mid 6}$$

tenemos dos posibilidades

① $|Imf| = 1 \Rightarrow Imf = \{\bar{0}\}$

$\Rightarrow f$ es el morfismo trivial

② $|Imf| = 2$ y $|Kerf| = 4$

* candidato a Imf:

$$Imf = \{\bar{0}, \bar{3}\}$$

es la única posibilidad porque $\{\bar{0}, \bar{3}\}$ es el único subgrupo de orden 2 de $\mathbb{Z}_6$

* candidato a Kerf:

una posibilidad es $Kerf = \langle \bar{2} \rangle$
$= \{\bar{2}, \bar{4}, \bar{8}, \bar{1}\}$

definimos $f: U(15) \longrightarrow \mathbb{Z}_6$

$f(\bar{2}) = \bar{0}$ $\quad$ $f(\bar{7}) = \bar{3}$

$f(\bar{4}) = \bar{0}$ $\quad$ $f(\overline{11}) = \bar{3} \longrightarrow f(\bar{2}^3 \cdot \bar{7}) = \bar{3}$

$f(\bar{8}) = \bar{0}$ $\quad$ $f(\overline{13}) = \bar{3} \longrightarrow f(\bar{2}^2 \cdot \bar{7}) = \bar{3}$

$f(\bar{1}) = \bar{0}$ $\quad$ $f(\overline{14}) = \bar{3} \longrightarrow f(\bar{2} \cdot \bar{7}) = \bar{3}$

$f(\bar{2}^k) = 0$ $\quad$ $\bar{2}^2 \cdot \bar{7} = \bar{4} \cdot \bar{7} = \overline{13}$

$f(\bar{2} \cdot \bar{4}) \stackrel{?}{=} f(\bar{2}) + f(\bar{4})$

$f(\bar{2}^k \cdot \bar{2}^m) = f(\bar{2}^{k+m}) = \bar{0} \Big| \Rightarrow f(\bar{2}^k \cdot \bar{2}^m) = f(\bar{2}^k) + f(\bar{2}^m)$

$f(\bar{2}^k) + f(\bar{2}^m) = \bar{0} + \bar{0} = \bar{0}$

$f: U(15) \longrightarrow \mathbb{Z}_6$

$f(\bar{2}^k) = \bar{0}$ es un morfismo de

$f(\bar{2}^k \cdot \bar{7}) = \bar{3}$ grupos no trivial

$$\left.\begin{array}{l} f(\bar{2}^k \cdot \bar{2}^m \cdot \bar{7}) = f(\bar{2}^{k+m} \cdot \bar{7}) = \bar{3} \\ f(\bar{2}^k) + f(\bar{2}^m \cdot \bar{7}) = \bar{0} + \bar{3} = \bar{3} \end{array}\right] \Rightarrow f(\bar{2}^k \cdot \bar{2}^m \bar{7}) = f(\bar{2}^k) + f(\bar{2}^m \cdot \bar{7})$$

$$\left.\begin{array}{l} f(\bar{2}^k \cdot \bar{7} \cdot \bar{2}^m \cdot \bar{7}) = f(\underbrace{\bar{2}^{k+m} \cdot \bar{4}}_{\bar{2}^{k+m+2}}) = \bar{0} \\ f(\bar{2}^k \cdot \bar{7}) + f(\bar{2}^m \cdot \bar{7}) = \bar{3} + \bar{3} = \bar{0} \end{array}\right] \Rightarrow f(\bar{2}^k \cdot \bar{7} \cdot \bar{2}^m \cdot \bar{7}) = f(\bar{2}^k \cdot \bar{7}) + f(\bar{2}^m \cdot \bar{7})$$