

Teorema 3 (Primer Teorema de Isomorfismos). Sea $f : G \rightarrow K$ un homomorfismo de grupos. Sea $\Pi : G \rightarrow G/\ker(f)$ la proyección canónica al cociente por el subgrupo normal $\ker(f)$. Existe un único isomorfismo $\bar{f} : G/\ker(f) \rightarrow \text{Im}(f)$, tal que: $f = \bar{f} \circ \Pi$. Esta última igualdad se suele expresar diciendo que "el diagrama de la Figura 3.1 conmuta".

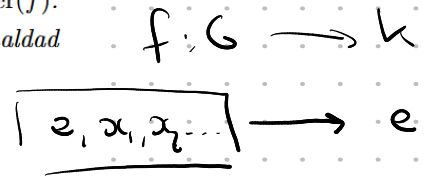
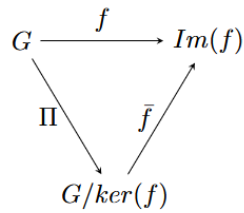


Figura 3.1: Primer Teorema de Isomorfismos.

Lo más relevante de este resultado, es que la existencia del isomorfismo implica que el grupo cociente $G/\ker(f)$ es isomorfo al grupo imagen $\text{Im}(f)$. Es decir: $G/\ker(f) \simeq \text{Im}(f)$. Esto quiere decir que ambos grupos son "iguales" en lo que respecta a la teoría de grupos.

demonstración: $H = \ker f$ $f : G \rightarrow K$
 \cup
 $\text{Im} f$

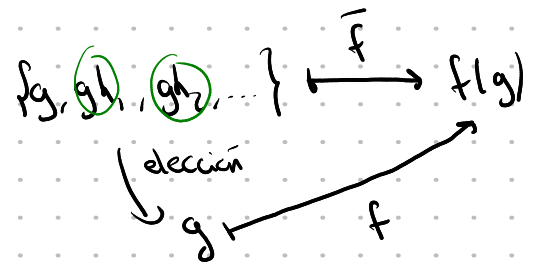
Consideramos $\bar{f} : G/\ker(f) \rightarrow \text{Im}(f)$

$$gH \longmapsto f(g)$$

$$\bar{f}(gH) = f(g)$$

$$\{g, gh_1, gh_2, \dots\} \in G$$

$$\rightarrow f(g) = f(gh_1) = f(gh_2) = \dots$$



① Veamos que \bar{f} está bien definida

para esto hay que ver que si $g_1, g_2 \in gH$ entonces $f(g_1) = f(g_2)$

$$g_1 \in gH \Rightarrow g_1 = gh_1 \text{ con } h_1 \in H$$

$$g_2 \in gH \Rightarrow g_2 = gh_2 \text{ con } h_2 \in H$$

$$g_2 = gh_2 \Rightarrow g_2 h_2^{-1} = g$$

$$\text{entonces } g_1 = gh_1 = g_2 h_2^{-1} h_1$$

$$f(g_1) = f(g_2 h_2^{-1} h_1) = f(g_2) f(\underbrace{h_2^{-1} h_1}_{\in \ker f}) = f(g_2) e = f(g_2)$$

f morfismo de grupos

② Veamos que \bar{f} es morfismo de grupos

para esto queremos ver que

$$\bar{f}((g_1H)(g_2H)) = \bar{f}(g_1H) \bar{f}(g_2H)$$

$$\begin{aligned} \bar{f}((g_1H)(g_2H)) &= \bar{f}((g_1g_2)H) = f(g_1g_2) \\ &= f(g_1)f(g_2) \end{aligned} \left. \vphantom{\bar{f}((g_1H)(g_2H))} \right\} \text{ porque } f \text{ es morfismo de grupos}$$
$$= \bar{f}(g_1H) \bar{f}(g_2H)$$

$$f: G \rightarrow K$$

③ Veamos que $\bar{f}: G/\ker f \rightarrow \text{Im } f$ es sobreyectiva

sea $y \in \text{Im } f$ busquemos $gH \in G/\ker f$ tal que $\bar{f}(gH) = y$

$y \in \text{Im } f \Rightarrow$ existe $g \in G$ tal que $f(g) = y$

$$\Rightarrow y = \bar{f}(gH)$$

④ Veamos que $\bar{f}: G/\ker f \rightarrow \text{Im } f$ es inyectiva

sean $g_1H, g_2H \in G/\ker f$ tales que $\bar{f}(g_1H) = \bar{f}(g_2H)$

queremos ver que $g_1H = g_2H$

$$\bar{f}(g_1H) = \bar{f}(g_2H) \Rightarrow f(g_1) = f(g_2)$$

porque f
es morfismo
de grupos

$$\Rightarrow f(g_1) f(g_2)^{-1} = e$$

$$\Rightarrow f(g_1 g_2^{-1}) = e$$

$$\Rightarrow g_1 g_2^{-1} \in H = \ker f$$

$$\Rightarrow g_1 g_2^{-1} = h \text{ para algún } h \in H$$

$$\Rightarrow g_1 = h g_2$$

$$\Rightarrow g_1 \in H g_2$$

$\Rightarrow g_1 \in g_2 H$ porque H es subgrupo normal

$$\Rightarrow g_1 H = g_2 H$$

Ejercicio 11.

a. Probar que si $a \in U(n) \Rightarrow o(a) | \varphi(n)$.

b. i) Hallar el resto de dividir 2^{20} entre 253. Sugerencia: $2^8 = 256$.

ii) Sabiendo además que $2^{55} \equiv -45 \pmod{253}$, hallar el orden de $\bar{2}$ en $U(253)$.

b) i) $20 = 16 + 4$

$$\leadsto 2^{20} = 2^{16} \cdot 2^4$$

$$2^2 \equiv 4 \pmod{253}$$

$$2^4 \equiv 16 \pmod{253}$$

$$2^8 \equiv 256 \equiv 3 \pmod{253}$$

$$2^{16} \equiv 2^8 \cdot 2^8 \equiv 3 \cdot 3 \equiv 9 \pmod{253}$$

$$2^{20} \equiv 2^{16} \cdot 2^4 \pmod{253}$$

$$\equiv 9 \cdot 16 \pmod{253}$$

$$\equiv 144 \pmod{253}$$

ii) $2^{20} \equiv 144 \pmod{253}$ $2^{55} \equiv -45 \pmod{253}$

$o(\bar{2})$ en $U(253)$

$$\bar{2} \in U(253) \Rightarrow o(\bar{2}) | \varphi(253)$$

$$\varphi(253) = \varphi(11 \cdot 23) = \varphi(11) \varphi(23) = 10 \cdot 22 = 220$$

divisores de $\varphi(253) = 220$?

$$220 = 2^2 \cdot 5 \cdot 11$$

$$\text{Div}_+(220) = \{ \underset{\times}{1}, \underset{\times}{2}, \underset{\times}{4}, \underset{\times}{5}, \underset{\times}{10}, \underset{\times}{11}, \underset{\times}{20}, \underset{\times}{22}, \underset{\times}{44}, \underset{\times}{55}, \underset{\times}{110}, \underset{\times}{220} \}$$

↓

$$2^{20} \not\equiv 1 \pmod{253} \Rightarrow o(\bar{2}) \neq 5, o(\bar{2}) \neq 10$$

$$\& \circ(\bar{2}) = 5 \Rightarrow 2^5 \equiv 1 \pmod{253}$$

$$(2^5)^4 \equiv 1 \pmod{253}$$

$$2^{20} \equiv 1 \pmod{253} \text{ no es cierto}$$

$$g^n = e \text{ sii } o(g) \mid n$$

$$2^{20} \equiv 144 \pmod{253}$$

$$2^{22} \equiv 2^{20} \cdot 2^2 \pmod{253}$$

$$\equiv 144 \cdot 4 \pmod{253}$$

$$\equiv 70 \pmod{253}$$

$$2^{44} \equiv 70^2 \pmod{253}$$

$$\equiv 93 \pmod{253}$$

$U(n)$

$$n = 2, 4, p^\alpha, 2p^\alpha \quad p \text{ primo impar}$$

Ejercicio 2.

a. Probar que 98 es raíz primitiva módulo 101.

b. Hallar un elemento de $U(101)$ de orden 25.

$$a) \varphi(101) = 100 = 2^2 \cdot 5^2$$

los divisores primos de $\varphi(101)$ son 2 y 5

$$98 \text{ es raíz primitiva módulo } 101 \Leftrightarrow \begin{cases} 98^{\varphi(101)/5} \not\equiv 1 \pmod{101} \\ 98^{\varphi(101)/2} \not\equiv 1 \pmod{101} \end{cases}$$

$$\Leftrightarrow \begin{cases} 98^{20} \not\equiv 1 \pmod{101} \quad \checkmark \\ 98^{50} \not\equiv 1 \pmod{101} \quad \checkmark \end{cases}$$

$$\star 98^{20} \pmod{101}$$

$$98 \equiv -3 \pmod{101}$$

$$20 \equiv 16 + 4$$

$$(-3)^{20} = (-3)^{16} (-3)^4$$

n	$(-3)^{2^n} \pmod{101}$	
0	-3	
1	9	$\sim (-3)^2$
2	$81 \equiv -20$	$\sim (-3)^4$
3	$400 \equiv 97 \equiv -4$	$\sim (-3)^8$
4	16	$\sim (-3)^{16}$

$$\begin{aligned} 98^{20} &\equiv (-3)^{20} \pmod{101} \\ &\equiv (-3)^{16} (-3)^4 \pmod{101} \\ &\equiv 16 (-20) \pmod{101} \\ &\equiv -17 \pmod{101} \\ &\equiv 84 \pmod{101} \end{aligned}$$

$$\ast 98^{50} \pmod{101}$$

$$\begin{aligned} 98^{50} &\equiv (-3)^{50} \pmod{101} \\ &\equiv ((-3)^{20})^2 \cdot (-3)^8 \cdot (-3)^2 \pmod{101} \\ &\equiv (-17)^2 \cdot (-4) \cdot 9 \pmod{101} \\ &\equiv -1 \pmod{101} \end{aligned}$$

$$98^{100} \equiv 1 \pmod{101}$$

entonces 98 es raíz primitiva modulo 101

b) busquemos un elemento de $U(101)$ de orden 25

$$98 \text{ raíz primitiva modulo } 101 \Rightarrow U(101) = \langle \overline{98} \rangle$$

$$U(101) = \{ \overline{98}, \overline{98}^2, \overline{98}^3, \dots, \overline{98}^{100} \}$$

buscamos k tal que $o(\overline{98}^k) = 25$

$$o(\overline{98}^k) = \frac{o(\overline{98})}{\gcd(o(\overline{98}), k)} = \frac{100}{\gcd(100, k)} = 25$$

$$o(g^n) = \frac{o(g)}{\gcd(o(g), n)}$$

si tomamos $k = 4$

$$o(\overline{98}^4) = \frac{100}{\gcd(100, 4)} = \frac{100}{4} = 25$$

$$\begin{aligned} 98^4 &\equiv (-3)^4 \pmod{101} \\ &\equiv 81 \pmod{101} \end{aligned}$$

$\Rightarrow \overline{81}$ es un elemento de $U(101)$ de orden 25

b. Considere el siguiente subgrupo de S_3 :

$$H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

ii) Pruebe que H es un subgrupo normal de S_3 .

Ejercicio 9. Sea S un subconjunto de un grupo G . Se define el normalizador de S en G como:

$$N_S = \{x \in G : xSx^{-1} = S\}.$$

a. Probar que N_S es un subgrupo de G .

b. Supongamos que S es un subgrupo de G . Probar que S es un subgrupo normal de N_S .

$$a) N_S = \{x \in G : xSx^{-1} = S\}$$

* cerrado bajo la operación

$$x_1, x_2 \in G, (x_1 x_2) S (x_1 x_2)^{-1} = S$$

Sean $x_1, x_2 \in N_S$ queremos ver que $x_1 x_2 \in N_S$

$$* x_1 \in N_S \Rightarrow x_1 S x_1^{-1} = S$$

$$* x_2 \in N_S \Rightarrow x_2 S x_2^{-1} = S$$

$$x_1 \left\{ s_1, s_2, \dots \right\} x_1^{-1} = \{s_1, s_2, \dots\}$$
$$x_2 S x_2^{-1}$$

veamos que $(x_1 x_2) S (x_1 x_2)^{-1} = S$

$$\text{Firma 1: } \left. \begin{array}{l} x_1 S x_1^{-1} = S \\ S = x_2 S x_2^{-1} \end{array} \right\} \Rightarrow x_1 x_2 S x_2^{-1} x_1^{-1} = S$$

$$\Rightarrow (x_1 x_2) S (x_1 x_2)^{-1} = S$$

Forma 2: $(x_1 x_2) S (x_1 x_2)^{-1} = x_1 \underbrace{x_2 S x_2^{-1}}_S x_1^{-1}$

$$= x_1 S x_1^{-1}$$
$$= S$$

* $e_G \in N_S$:

tenemos que ver que $e_G S e_G^{-1} = S$

$$e_G s_i e_G^{-1} = s_i \text{ para todo } s_i \in S$$

$$\Rightarrow e_G S e_G^{-1} = S$$