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

$$f : G \longrightarrow K$$

$$\{e, x_1, x_2, \dots\} \longrightarrow e$$

$$\begin{tikzcd}
G \arrow[rr, "f"] \arrow[dr, "\Pi"'] & & Im(f) \\
& G/ker(f) \arrow[ur, "\bar{f}"'] &
\end{tikzcd}$$

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 $Im(f)$. Es decir: $G/\ker(f) \simeq Im(f)$. Esto quiere decir que ambos grupos son "iguales" en lo que respecta a la teoría de grupos.

demostración: $H = \ker f$ $\qquad f : G \longrightarrow \underset{\cup}{K}$ $\quad Im f$

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

$$gH \longmapsto f(g)$$

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

$$\{g, gh_1, gh_2, \dots\} \xrightarrow{\bar{f}} f(g)$$

elección $\downarrow$ $\qquad g \xmapsto{f} f(g)$

$$\{ge, gh_1, gh_2, \dots\} \subseteq G$$

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

① Veamos que $\bar{f}$ está bien definida

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

$g_1 \in gH \Rightarrow g_1 = gh_1$ con $h_1 \in H$

$g_2 \in gH \Rightarrow g_2 = gh_2$ con $h_2 \in H$

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

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

$$f(g_1) = f(g_2 h_2^{-1} h_1) \underset{\substack{\uparrow \\ f \text{ morfismo} \\ \text{de grupos}}}{=} f(g_2)\, f(\underbrace{h_2^{-1} h_1}_{\in \ker f}) = f(g_2)\, e = f(g_2)$$

② Veamos que $\bar{f}$ es morfismo de grupos para esto queremos ver que

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

$$\bar{f}((g_1H)(g_2H)) = \bar{f}((g_1g_2)H) = f(g_1g_2)$$

$$= f(g_1)f(g_2) \quad \text{porque } f \text{ es morfismo de grupos}$$

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

$f: G \to K$

(3) Veamos que $\bar{f}: G/_{\ker f} \to \operatorname{Im} f$ es sobreyectiva

sea $y \in \operatorname{Im} f$ buscamos $gH \in G/_{\ker f}$ tal que $\bar{f}(gH) = y$

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

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

(4) Veamos que $\bar{f}: G/_{\ker f} \to \operatorname{Im} f$ es inyectiva

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

queremos ver que $g_1H = g_2H$

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

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

porque f es morfismo de grupos

$$\Rightarrow f(g_1g_2^{-1}) = e$$

$$\Rightarrow g_1g_2^{-1} \in \underbrace{H}_{=\ker f}$$

$\Rightarrow g_1g_2^{-1} = h$ para algún $h \in H$

$$\Rightarrow g_1 = hg_2$$

$$\Rightarrow g_1 \in Hg_2$$

$\Rightarrow g_1 \in g_2 H$ 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 $2^{55} \equiv -45 \mod (253)$, hallar el orden de $\bar{2}$ en $U(253)$.

b) i) $20 = 16 + 4$

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

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

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

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

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

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

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

$\equiv 144 \pmod{253}$

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

$o(\bar{2})$ 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 $\varphi(253) = 220$?

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

$Div_+(220) = \{1, 2, 4, 5, 10, 11, 20, 22, 44, 55, 110, 220\}$

X X X X X X X X X X X

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

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

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

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

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

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

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

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

$\equiv 70 \pmod{253}$

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

$\equiv 93 \pmod{253}$

$U(n)$

$n = 2, 4, p^\alpha, 2p^\alpha$ p 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 es raiz primitiva modulo 101 $\Leftrightarrow \begin{cases} 98^{\varphi(101)/5} \not\equiv 1 \pmod{101} \\ 98^{\varphi(101)/2} \not\equiv 1 \pmod{101} \end{cases}$

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

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

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

$20 = 16 + 4$

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

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

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

* $98^{50} \pmod{101}$:

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

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

entonces 98 es raíz primitiva modulo 101

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

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

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

$\bar{\bar{1}}$

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

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

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

si tomamos $k = 4$

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

$$98^4 \equiv (-3)^4 \pmod{101}$$
$$\equiv 81 \pmod{101}$$

$\Rightarrow \overline{81}$ 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 $x_1 x_2 \in N_S$

* $x_1 \in N_S \Rightarrow x_1 S x_1^{-1} = S$
* $x_2 \in N_S \Rightarrow x_2 S x_2^{-1} = S$

$$x_1 \{s_1, s_2, \dots\} x_1^{-1} = \{s_1, s_2, \dots\}$$
$x_1 s_1 x_1^{-1}$

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

Forma 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 $e_G S e_G^{-1} = S$

$e_G s_1 e_G^{-1} = s_1$ para todo $s_1 \in S$

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