Ejercicio 2.

a. i) Definir grupo y homomorfismo de grupos.

ii) Enunciar el Primer Teorema de Isomorfismos.

b. Sea $f : G \to G'$ un morfismo de grupos. Probar que $\mathrm{Ker}(f) \lhd G$.

c. Se considera $\mathrm{GL}_n := \{A \in \mathcal{M}_{n\times n}(\mathbb{R}) \mid A \text{ es invertible}\}$ (el grupo multiplicativo de las matrices reales de $n \times n$). Se pide:

i) Probar que $\det : \mathrm{GL}_n \to \mathbb{R}^*$ es un morfismo de grupos.

ii) Sea $N := \{A \in \mathcal{M}_{n\times n}(\mathbb{R}) \mid \det(A) = 1\}$. Probar que $N \lhd \mathrm{GL}_n$, que $\dfrac{\mathrm{GL}_n}{N} \cong \mathbb{R}^*$ y que $A \sim_N B$ si y sólo si $\det A = \det B$.

$\det: GL_n \longrightarrow \mathbb{R}^*$

$GL_n/N \cong \mathrm{Im}\det$

$f: G \to G'$ morfismo de grupos

$\mathrm{Ker} f$ es un <u>subgrupo normal</u> de G

1er <u>teorema de isomorfismo</u>:

$f: G \longrightarrow G'$ morfismo de grupos <u>sobreyectivo</u>

entonces: $G/_{\mathrm{Ker} f} \cong G'$

1er <u>teorema de isomorfismo</u> (versión 2):

$f: G \longrightarrow G'$ morfismo de grupos $\rightarrow$ $\tilde{f}: G \longrightarrow \mathrm{Im} f$ morfismo de grupos sobreyectivo

entonces: $G/_{\mathrm{Ker} f} \cong \mathrm{Im} f$

c) $GL_n = \{A \in \mathcal{M}_{n\times n}(\mathbb{R}) : A \text{ es invertible}\}$

GL_n es un grupo con la multiplicación de matrices

i) $\det: \underset{\substack{\uparrow \\ \text{producto}}}{GL_n} \longrightarrow \underset{\substack{\uparrow \\ \text{producto}}}{\mathbb{R}^*}$ es un morfismo de grupos

$\det(AB) = \det(A)\det(B)$

entonces $\det$ es un morfismo de grupos.

ii) $N = \{A \in \mathcal{M}_{n\times n}(\mathbb{R}) : \det(A) = 1\}$

$* \; N \trianglelefteq Gl_n$

para probar que $N \trianglelefteq Gl_n$ veamos que $N = Ker(\det)$

$$\det : Gl_n \longrightarrow \mathbb{R}^*$$

el neutro es 1

$$Ker(\det) = \{A \in Gl_n : \det(A) = 1\}$$
$$= \{A \in \mathcal{M}_{n\times n} : \det(A) = 1\}$$
$$= N$$

N es el nucleo del morfismo $\det : Gl_n \to \mathbb{R}^*$ entonces $N \trianglelefteq Gl_n$

$* \; Gl_n / N \cong \mathbb{R}^*$

$\to$ vamos a probar que $\det : Gl_n \to \mathbb{R}^*$ es sobreyectivo.

sea $a \in \mathbb{R}^*$

buscamos $A \in Gl_n$ tal que $\det(A) = a$

tomamos $A = \begin{pmatrix} a & & & 0 \\ & 1 & & \\ & & 1 & \\ 0 & & & \ddots & \\ & & & & 1 \end{pmatrix}$

$\det(A) = a \neq 0$

entonces $A \in Gl_n$ y $\det(A) = a$

$\to$ tenemos:

$\det : Gl_n \to \mathbb{R}^*$ morfismo de grupos sobreyectivo

entonces por el primer teorema de isomorfismo

$$Gl_n / Ker(\det) \cong \mathbb{R}^*$$

pero ya vimos que $N = Ker(\det)$

entonces $GL_n / N \cong \mathbb{R}^*$

$*$ $\underbrace{A \sim_N B}_{AN = BN}$ si y sólo si $\det(A) = \det(B)$

AN clase lateral de A; BN clase lateral de B

$\widetilde{\det} : GL_n / N \longrightarrow \mathbb{R}^*$

$B \in [A]$

$A \sim_N B$ si y sólo si $\begin{cases} A = BC \text{ con } C \in N \\ B^{-1}A = C \text{ con } C \in N \end{cases}$

$A \sim_N B \iff A = BC$ para algún $C \in N$ $\longrightarrow \det(C) = 1$

$\Rightarrow \det(A) = \det(BC)$

$\Rightarrow \det(A) = \det(B)\det(C)$

$\Rightarrow \det(A) = \det(B)$

$\det(A) = \det(B) \Rightarrow \dfrac{\det(A)}{\det(B)} = 1$

$\Rightarrow \det(A) \dfrac{1}{\det(B)} = 1$

$\Rightarrow \det(A)\det(B^{-1}) = 1$

$\Rightarrow \det(B^{-1})\det(A) = 1$

$\Rightarrow \det(B^{-1}A) = 1$

$\Rightarrow B^{-1}A \in N$

$\Rightarrow B^{-1}A = C$ para algún $C \in N$

$\Rightarrow A = BC$ para algún $C \in N$

$\Rightarrow A \sim_N B$

d) Mostrar con dos ejemplos que cada hipótesis de la parte anterior es necesaria.

Ejercicio 2 (20 puntos)

a) Definir raíz primitiva módulo n.
b) Sea $n \in \mathbb{Z}^+$. Probar que si existe una raíz primitiva módulo n, entonces hay exactamente $\phi(\phi(n))$ raíces primitivas módulo n.
c) i) Hallar una raíz primitiva módulo 23.
   ii) Hallar todas las raíces primitivas módulo 23.

a) $g \in \{1, \dots, n\}$ es raiz primitiva modulo n si $\langle \bar{g} \rangle = U(n)$

b) $n \in \mathbb{Z}^+$

Sea g una raiz primitiva modulo n

$U(n) = \langle \bar{g} \rangle = \{ \bar{g}, \bar{g}^2, \bar{g}^3, \bar{g}^4, \dots, \bar{g}^{\varphi(n)} \}$

$o(\bar{g}) = \varphi(n)$

$\bar{g}^i$ es generador si y solamente si $mcd(i, o(\bar{g})) = 1$

$\bar{g}^i$ es generador si y solamente si $mcd(i, \varphi(n)) = 1$

conjunto de generadores de $U(n)$:

$\{ \bar{g}^i : 1 \leq i \leq \varphi(n),\ mcd(i, \varphi(n)) = 1 \}$

$$\left.\begin{array}{l} o(\bar{g}^i) = \dfrac{o(\bar{g})}{mcd(i, o(\bar{g}))} \\ o(\bar{g}^i) = o(\bar{g}) \end{array}\right] \Rightarrow mcd(i, o(\bar{g})) = 1$$

cantidad de generadores de $U(n)$:

$$\# \{ \bar{g}^i : 1 \leq i \leq \varphi(n),\ mcd(i, \varphi(n)) = 1 \} = \# \{ 1 \leq i \leq \varphi(n) : mcd(i, \varphi(n)) = 1 \}$$
$$= \varphi(\varphi(n))$$

c) i) Hallar una raiz primitiva modulo 23

$\varphi(23) = 22 = 2 \cdot 11$

2 es raiz primitiva modulo 23 $\Leftrightarrow \begin{cases} 2^{\varphi(23)/11} \not\equiv 1 \pmod{23} \\ 2^{\varphi(23)/2} \not\equiv 1 \pmod{23} \end{cases}$

$\Leftrightarrow \begin{cases} 2^{2} \not\equiv 1 \pmod{23} \\ 2^{11} \not\equiv 1 \pmod{23} \end{cases}$

* $2^2 \equiv 4 \pmod{23}$ ✓
* $2^{11} \equiv ? \pmod{23}$

$$2^{11} = 2^8 \cdot 2^2 \cdot 2$$

$2^2 \equiv 4 \pmod{23}$

$2^4 \equiv (2^2)^2 \equiv 16 \pmod{23}$

$2^8 \equiv (2^4)^2 \equiv 16^2 \equiv (-7)^2 \equiv 49 \equiv 3 \pmod{23}$

$2^{11} \equiv 2^8 \cdot 2^2 \cdot 2 \equiv 3 \cdot 4 \cdot 2 \equiv 24 \equiv 1 \pmod{23}$

$\Rightarrow$ 2 no es raiz primitiva modulo 23

3 es raiz primitiva modulo 23 $\Leftrightarrow \begin{cases} 3^{2} \not\equiv 1 \pmod{23} \\ 3^{11} \not\equiv 1 \pmod{23} \end{cases}$

* $3^2 \equiv 9 \pmod{23}$ ✓
* $3^{11} \equiv ? \pmod{23}$

$$3^{11} = 3^8 \cdot 3^2 \cdot 3$$

$3^2 \equiv 9 \pmod{23}$

$3^4 \equiv 9^2 \equiv 81 \equiv 12 \pmod{23}$

$3^8 \equiv 12^2 \equiv 144 \equiv 6 \pmod{23}$

$3^{11} \equiv 3^8 \cdot 3^2 \cdot 3 \equiv 6 \cdot 9 \cdot 3 \equiv 6 \cdot 4 \equiv 24 \equiv 1 \pmod{23}$

$\Rightarrow$ 3 no es raiz primitiva modulo 23

5 es raiz primitiva modulo 23 $\Longleftrightarrow \begin{cases} 5^2 \not\equiv 1 \pmod{23} \\ 5^{11} \not\equiv 1 \pmod{23} \end{cases}$

* $5^2 \equiv 25 \equiv 2 \pmod{23}$
* $5^{11} \equiv ? \pmod{23}$

$5^{11} = 5^8\, 5^2\, 5$

$5^2 \equiv 2 \pmod{23}$

$5^4 \equiv 4 \pmod{23}$

$5^8 \equiv 16 \pmod{23}$

$5^{11} \equiv 16 \cdot 2 \cdot 5 \equiv 160 \equiv 22 \pmod{23}$

$\Rightarrow$ 5 es raiz primitiva modulo 23 ◡̈

ii) todas las raices primitivas modulo 23

\# de raices primitivas $= \varphi(\varphi(23)) = \varphi(22) = 22\left(1-\frac{1}{2}\right)\left(1-\frac{1}{11}\right) = 22 \cdot \frac{1}{2} \cdot \frac{10}{11} = 10$

$22 = 2 \cdot 11$

$U(23) = \{\bar{5}, \bar{5}^2, \bar{5}^3, \bar{5}^4, \dots, \bar{5}^{22}\}$

el conjunto de generadores de $U(23)$ es:

$\{\bar{5}^i : 1 \leq i \leq 22,\ \mathrm{mcd}(i, 22) = 1\}$

$1, \cancel{2}, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, 9, \cancel{10}, \cancel{11}, \cancel{12}, 13, \cancel{14}, 15, \cancel{16}, 17, \cancel{18}, 19, \cancel{20}, 21, \cancel{22}$

raices primitivas modulo 23:

5

$5^3 \equiv 10 \pmod{23}$

Ejercicio 6. Sea $n = pq$, con p y q primos.

a. Describir un método para factorizar n si se conocen los valores de n y $\varphi(n)$.

$n = pq$

$\varphi(n) = \varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$

$f(x) = (x-p)(x-q)$ ← las raices son p y q

$= x^2 - qx - px + pq$

$= x^2 - (p+q)x + pq = x^2 - (n+1-\varphi(n))x + n$

$\varphi(n) = (p-1)(q-1) = pq - q - p + 1$

$\varphi(n) = pq - q - p + 1$

$q + p = \underbrace{pq}_{n} + 1 - \varphi(n)$

(iii) *Determinar si la siguiente congruencia tiene solución $k \in \mathbb{Z}$, y en caso afirmativo hallar una solución:* $5^{27k} \equiv 39 \pmod{43}$.

Por la Parte (c,ii), sabemos que $5^3 \equiv 39 \pmod{43}$. Por lo tanto, buscamos $k \in \mathbb{Z}$, tal que: $5^{27k} \equiv 5^3 \pmod{43}$. Por la Parte (b), esto equivale a que se cumpla: $27k \equiv 3 \pmod{42}$. Esta es una ecuación diofántica: $27k - 42y = 3$. Como $\operatorname{mcd}(27, 42) = 3$, que divide a 3, sabemos que la ecuación tiene solución entera. Dividiendo entre 3 de ambos lados de la ecuación, esta equivale a: $9k - 14y = 1$. Es fácil ver que una solución de esta diofántica es: $(k, y) = (-3, -2)$. Por lo tanto: $k \equiv -3 \pmod{14} \equiv 11 \pmod{14}$.

(b) Hallar todos los morfismos no triviales entre D_3 y $\mathbb{Z}_2$.
Recordar: la composición de 2 rotaciones, o de 2 simetrías, es una rotación; mientras que la composición de una simetría y una rotación, es una simetría.

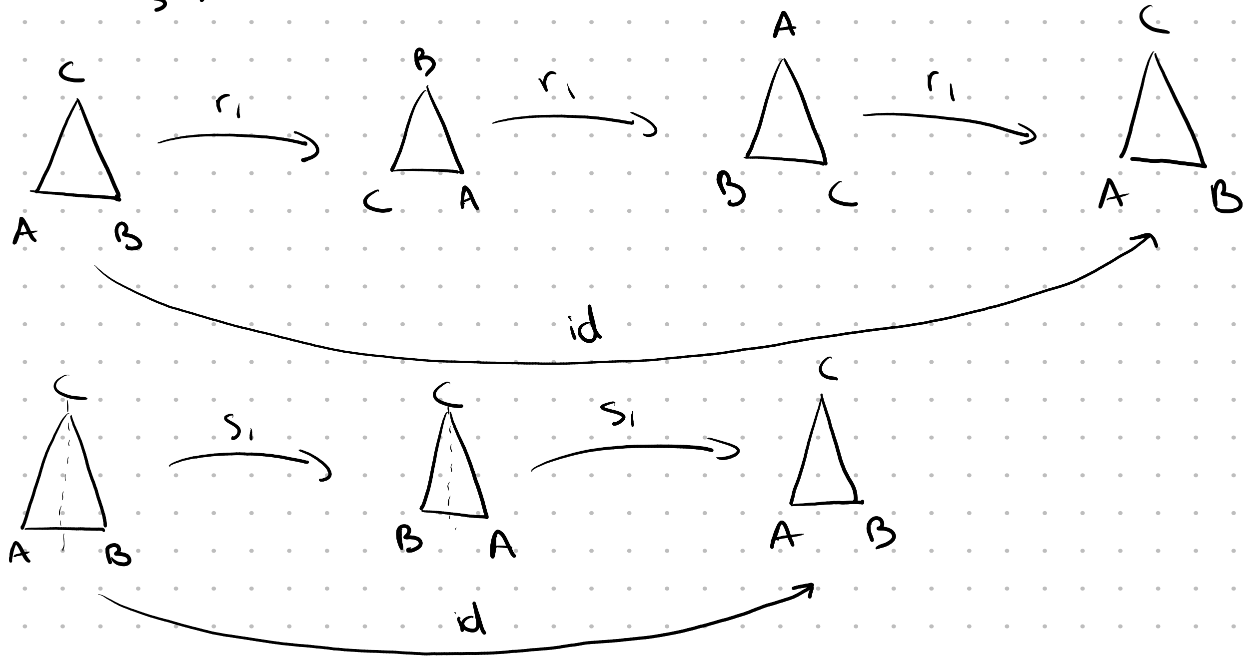
$f: D_3 \to \mathbb{Z}_2$ morfismo de grupos no trivial

D_3

g	$o(g)$
id	1
r_1	3
r_2	3
s_1	2
s_2	2
s_3	2

$\mathbb{Z}_2$

g	$o(g)$
$\overline{0}$	1
$\overline{1}$	2



teorema de ordenes:

$f: D_3 \to \mathbb{Z}_2$ morfismo de grupos

$$\underbrace{|D_3|}_{6} = |\ker f| \times |\mathrm{Im} f|$$

posibilidades para $|\mathrm{Im} f|$

* $\underbrace{|D_3|}_{6} = |\ker f| \times \underbrace{|\mathrm{Im} f|}_{2} \Rightarrow |\mathrm{Im} f| \mid 6$

  $\to$ 1, 2, 3, 6

* $\mathrm{Im} f$ es un subgrupo de $\mathbb{Z}_2$

  $\Rightarrow |\mathrm{Im} f| \mid 2$

  $\to$ 1, 2

→ si $|\mathrm{Im} f| = 1$, f es el morfismo trivial

→ si $|\mathrm{Im} f| = 2$

$\Rightarrow |\mathrm{Ker} f| = 3$

D_3

g	$o(g)$
id	1
r_1	3
r_2	3
s_1	2
s_2	2
s_3	2

$\mathbb{Z}_2$

g	$o(g)$
$\bar{0}$	1
$\bar{1}$	2

$\mathrm{Ker} f = \{id, r_1, r_2\}$

$$\left.\begin{array}{l} o(r_1) = 3 \\ o(f(r_1)) \mid o(r_1) \end{array}\right] \Rightarrow o(f(r_1)) \mid 3$$

Si existe un morfismo de grupos no trivial de D_3 en $\mathbb{Z}_2$ tiene que ser:

$$f: D_3 \longrightarrow \mathbb{Z}_2$$
$$f(id) = \bar{0}$$
$$f(r_i) = \bar{0} \quad \text{con } i = 1,2$$
$$f(s_j) = \bar{1} \quad \text{con } j = 1,2,3$$

vamos a verificar que es un morfismo de grupos:

* $f(r_i \circ r_j) = f(r_i) + f(r_j)$ con $i,j = 1,2$, $i \neq j$

$f(r_i \circ r_j) = f(id) = \bar{0}$ ✓
$f(r_i) + f(r_j) = \bar{0} + \bar{0} = \bar{0}$

* $f(r_i \circ r_i) = f(r_i) + f(r_i)$ con $i=1,2$

$f(r_i \circ r_i) = f(r_j) = \bar{0}$

$f(r_i) + f(r_i) = \bar{0} + \bar{0} = \bar{0}$

* $f(s_i \circ s_i) = f(s_i) + f(s_i)$ con $i=1,2,3$

$f(s_i \circ s_i) = f(id) = \bar{0}$

$f(s_i) + f(s_i) = \bar{1} + \bar{1} = \bar{0}$

* $f(s_i \circ s_j) = f(s_i) + f(s_j)$ con $i,j=1,2,3$, $i \neq j$

$f(s_i \circ s_j) = f(r_k) = \bar{0}$

$f(s_i) + f(s_j) = \bar{1} + \bar{1} = \bar{0}$

* $f(s_i \circ r_k) = f(s_i) + f(r_k)$

$f(s_i \circ r_k) = f(s_j) = \bar{1}$

$f(s_i) + f(r_k) = \bar{1} + \bar{0} = \bar{1}$

* $f(r_k \circ s_i) = f(r_k) + f(s_i)$

$f(r_k \circ s_i) = f(s_j) = \bar{1}$

$f(r_k) + f(s_i) = \bar{0} + \bar{1} = \bar{1}$