**Universidad de la República**
**Facultad de Ingeniería**
**Instituto de Matemática y Estadística**

**Matemática Discreta 2**
**Curso segundo semestre 2024**

SEGUNDO PARCIAL - 2 DICIEMBRE 2024.

| Cédula de identidad | APELLIDO, Nombre | Número de lista |
|---|---|---|
| | | |

**Ejercicio 1.** $G$ y $H$ grupos finitos.

1) Enunciar el teorema de Lagrange.
2) Probar que si $f : G \to H$ es un homomorfismo entonces $|G| = |\ker(f)| \cdot |\operatorname{Im}(f)|$.
3) Probar que si $f : G \to H$ es un homomorfismo entonces $|\operatorname{Im}(f)|$ divide al $\operatorname{mcd}(|G|, |H|)$.
4) Cuantos homomorfirmos hay entre $\mathbb{Z}_8$ y $\mathbb{Z}_9$.

**Solución:**

1) Ver Teorema 3.8.1 página 55, Notas P.Q.R.
2) Ver Teorema 3.9.8 página 59, Notas P.Q.R.
3) Ver Corolario 3.9.11 página 61, Notas P.Q.R.
4) Solo el trivial por la parte $3$).

**Ejercicio 2.**

1) Enunciar el primer teorema de isomorfismo.
2) Probar que $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ dado por $f(x, y) = 3x - 4y$ es un morfismo de grupos, donde $\mathbb{Z} \times \mathbb{Z}$ es un grupo con la suma coordenada a coordenada y $\mathbb{Z}$ es un grupo con la suma.
3) Probar que $\operatorname{Ker}(f)$ es el subgrupo generado por $(4, 3)$.
4) Concluir que $\frac{\mathbb{Z}\times\mathbb{Z}}{\langle(4,3)\rangle} \simeq \mathbb{Z}$

**Solución:**

1) Ver notas sobre teoremas de isomorfismo. Teorema 3 página 22.
2) Sean $(x, y), (x', y') \in \mathbb{Z} \times \mathbb{Z}$.

$$\begin{aligned} f((x,y) + (x',y')) &= f(x + x', y + y') \\ &= 3(x + x') - 4(y + y') \\ &= 3x - 4y + 3x' - 4y' \\ &= f(x, y) + f(x', y') \end{aligned}$$

   Entonces, $f$ es un morfismo de grupos.

3) Si $(x, y) \in \operatorname{Ker}(f)$, tenemos que $f(x, y) = 0$ y por lo tanto $3x = 4y$. Entonces $3|4y$ y, como 3 y 4 son coprimos, por el lema de Euclides obtenemos que $3|y$. Luego $y = 3n$ para algún $n \in \mathbb{Z}$ y, por lo tanto, $x = 4n$. Concluímos que $(x, y) = (4n, 3n) \in \langle(4, 3)\rangle$.

   Recíprocamente, si $(x, y) \in \langle(4, 3)\rangle$, tenemos que $(x, y) = (4n, 3n)$ para algún $n \in \mathbb{Z}$. Luego $f(x, y) = f(4n, 3n) = 3 \cdot 4n - 4 \cdot 3n = 0$. Entonces $(x, y) \in \operatorname{Ker}(f)$.

4) Veamos que $f$ es un morfismo sobreyectivo. Sea $z \in \mathbb{Z}$. Dado que $3$ y $4$ son coprimos, la ecuación diofántica $3x - 4y = z$ tiene una solución $(x_0, y_0)$. Entonces $f(x_0, y_0) = z$ y obtenemos que $f$ es sobreyectiva.

   Luego, por el primer teorema de isomorfismo $\frac{\mathbb{Z}\times\mathbb{Z}}{\mathrm{Ker}(f)} \simeq \mathbb{Z}$, es decir $\frac{\mathbb{Z}\times\mathbb{Z}}{\langle(4,3)\rangle} \simeq \mathbb{Z}$

**Ejercicio 3.**

1) Sea $(G, \cdot, e)$ un grupo, $g \in G$. Defina orden del elemento $g$.

2) Sea $G$ un grupo, $g \in G$, $n \in \mathbb{Z}^+$, en donde $o(g)$ indica la notación por el orden de $g$. Probar la siguiente equivalencia:

$$o(g) = n \quad \Longleftrightarrow \quad \begin{cases} g^n = e \text{ y} \\ \text{si } g^m = e \text{ entonces } n|m. \end{cases}$$

3) Determinar si $x = 39$ es solución de la ecuación $3^x \equiv 1(\text{mod } 7)$.

**Solución:**

1) Ver Definición 3.7.6. página 53, Notas P.Q.R.

2) Ver Proposición 3.7.8. Ver Definición 3.7.8. página 53, Notas P.Q.R.

3) Calculemos el orden de $3$ módulo $7$ en el grupo multiplicativo: $3^2 \equiv 2(\text{mod } 7)$; $3^3 \equiv 3(\text{mod } 7)$; $3^4 \equiv 4(\text{mod } 7)$; $3^5 \equiv 5(\text{mod } 7)$; $3^6 \equiv 1(\text{mod } 7)$. Entonces el orden es $6$. Por lo que por la parte 2 del ejercicio si $x = 39$ fuese solución entonces $6$ debería dividir a $39$. Lo cual no es cierto.