

| Nro de prueba | Cédula | Apellido y nombre |
|---------------|--------|-------------------|
| | | |

Ejercicio 1 (20 puntos)

- Sean G un grupo y $g \in G$.
- Definir el orden $o(g)$ de g .
 - Probar que $o(g^k) = \frac{o(g)}{\gcd(o(g), k)}$ para $k \in \mathbb{Z}$.
 - Sean $x, y \in G$ dos elementos de orden a y b respectivamente tales que $xy = yx$ y $\gcd(a, b) = 1$. Probar que el orden de xy es ab .
 - Mostrar con dos ejemplos que cada hipótesis de la parte anterior es necesaria.

Ejercicio 2 (20 puntos)

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

Ejercicio 3 (20 puntos)

- Definir subgrupo normal.
- Probar que para todo subgrupo normal H de G existen un grupo G' y un morfismo de grupos $\phi: G \rightarrow G'$ tales que H es isomorfo a su núcleo.
- Enunciar el Primer teorema de isomorfismo.
 - Probar que $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}^*$, siendo los grupos $GL_n(\mathbb{R}) = \{M \in M_{n \times n} : \det(M) \neq 0\}$ y $SL_n(\mathbb{R}) = \{M \in M_{n \times n} : \det(M) = 1\}$ ambos con la multiplicación de matrices como operación.

Solución

- Ejercicio 1**
- Ver notas de Matemática discreta 2, Definición 3.7.6. página 53.
 - Ver notas de Matemática discreta 2, Proposición 3.7.8. parte 7. página 54.
 - Ver notas de Matemática discreta 2, Lema 4.1.7. página 64.
 - Caso $xy \neq yx$ y $\gcd(o(x), o(y)) = 1$.

Consideremos el grupo $G = S_3$, y los elementos $x = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ e $y = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$.

Claramente se tiene que: $o(x) = 2$, $o(y) = 3$, $yx = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ y $xy = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ y $o(xy) = 2$.

- Caso $xy = yx$ y $\gcd(o(x), o(y)) \neq 1$. Consideremos el grupo $G = \mathbb{Z}_2 \times \mathbb{Z}_2$, y los elementos $x = (1, 0)$ e $y = (0, 1)$. Claramente se tiene que $o(x) = 2$, $o(y) = 2$ y $o(xy) = o(1, 1) = 2$.

- Ejercicio 2**
- Ver notas de Matemática discreta 2, Definición 4.1.1. página 62.
 - Ver notas de Matemática discreta 2, Proposición 4.1.3. página 63.
 - Como $\phi(23) = 22 = 2 \times 11$, usando la parte 3 de la Proposición 4.1.4 de las notas de Matemática discreta 2, para verificar que un g es raíz primitiva módulo 23 se debe cumplir $g^2 \not\equiv 1 \pmod{23}$

y $g^{11} \not\equiv 1 \pmod{23}$. En el caso de 5, se tiene $5^2 = 25 \not\equiv 1 \pmod{23}$ y $5^{11} \equiv 22 \pmod{23}$. Por lo tanto 5 es raíz primitiva.

- ii) Como 5 es raíz primitiva módulo 23, $\langle \bar{5} \rangle = U(23)$, usando la parte b) del ejercicio 1, sabemos que todas las raíces módulo 23 son de la forma 5^k con $\text{mcd}(k, 22) = 1$. Los valores posibles de k son $\{1, 3, 5, 7, 9, 13, 15, 17, 19, 21\}$ (son todas distintas por la parte 5 de la Proposición 3.7.8 de las notas de Matemática discreta 2), por lo tanto el conjunto de las raíces primitivas es

$$\{5^1 = 5, 5^3 = 10, 5^5 = 20, 5^7 = 17, 5^9 = 11, 5^{13} = 21, 5^{15} = 19, 5^{17} = 15, 5^{19} = 7, 5^{21} = 14\}.$$

Ejercicio 3 a) Ver libro Anillos y sus categorías de representaciones, Definición 1.3.4. página 11.

b) Ver libro Anillos y sus categorías de representaciones, Lema 1.4.4. página 15.

c) i) Ver libro Anillos y sus categorías de representaciones, Teorema 1.5.1. página 18.

ii) Sea $\det : GL_n(\mathbb{R}) \rightarrow \mathbb{R}^*$ la restricción de la función determinante en $GL_n(\mathbb{R})$.

Sabemos que $\det(MN) = \det(M)\det(N)$, la función \det es un morfismo de grupos.

Si consideramos $A_\lambda = (a_{ij})$ la matriz diagonal tal que $a_{1,1} = \lambda$ y $a_{i,i} = 1$ si $i = 2, 3, \dots, n$ se tiene que $\det(A_\lambda) = \lambda \forall \lambda \in \mathbb{R}^*$ y por lo tanto el morfismo de grupos \det es sobreyectivo.

Por el Primer teorema de isomorfismo tenemos que $\overline{\det} : GL_n(\mathbb{R}) / \ker(\det) \rightarrow \mathbb{R}^*$ es un isomorfismo de grupos. Solamente falta hallar el núcleo de \det . Como $\ker(\det) = \{M \in GL_n(\mathbb{R}) \text{ tal que } \det(M) = e_{\mathbb{R}^*} = 1\} = SL_n(\mathbb{R})$. Por lo tanto tenemos que $\overline{\det} : GL_n(\mathbb{R}) / SL_n(\mathbb{R}) \cong \mathbb{R}^*$ es un isomorfismo.