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

Matemática Discreta 2
Curso 2024

Examen - 8 de febrero de 2025.

Cédula de identidad	APELLIDO, Nombre	Número de lista

Ejercicio 1.

1) Enuncie y demuestre el Teorema Chino del Resto para el caso de dos ecuaciones.

2) Considere el sistema:

$$\begin{cases} 6x \equiv 2 \pmod{11}, \\ 6x \equiv 1 \pmod{17}. \end{cases}$$

Pruebe que existe una única solución módulo 187 y encuentre dicha solución.

Ejercicio 2.

1) Definir raíz primitiva.

2) Sea G un grupo, probar que si $x, y \in G$ son elementos de orden a, b respectivamente tales que $xy = yx$ y $\operatorname{mcd}(a, b) = 1$ entonces el orden de xy es ab.

3) Sabiendo que es válida la siguiente proposición: si p es un primo y d un divisor de $p-1$, entonces la ecuación $x^d \equiv 1 \pmod{p}$ tiene exactamente d soluciones distintas en $U(p)$; demostrar que si p es primo, entonces existen raíces primitivas módulo p.

Ejercicio 3. Sea $(GL_n(\mathbb{R}), \cdot, Id)$ el grupo de las matrices invertibles de tamaño $n \times n$ con coeficientes reales.

1) Probar que $O_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) : A^t A = AA^t = Id\}$ es un subgrupo de $GL_n(\mathbb{R})$ y que toda matriz de $O_n(\mathbb{R})$ tiene determinante 1 o -1.

2) Probar que $SO_n(\mathbb{R}) = \{A \in O_n(\mathbb{R}) : \det(A) = 1\}$ es un subgrupo normal de $O_n(\mathbb{R})$. Sugerencia: considerar la función $\det : O_n(\mathbb{R}) \to \mathbb{R}^*$.

3) Enunciar el primer teorema de isomorfismo.

4) Probar que el grupo cociente O_n/SO_n es isomorfo al grupo $(\{-1, 1\}, \times, 1)$.

Solución

Ejercicio 1.

1) Ver Teorema 2.5.1 de las notas del curso.

2) Dado que 11 y 17 son coprimos, por el teorema chino del resto, el sistema tiene una única solución módulo $11 \times 17 = 187$. Como $6^{-1} \equiv 2 \pmod{11}$ y $6^{-1} \equiv 3 \pmod{17}$, las soluciones del sistema

$$\begin{cases} 6x \equiv 2 \pmod{11} \\ 6x \equiv 1 \pmod{17}. \end{cases}$$

son las mismas que las del sistema

$$\begin{cases} x \equiv 4 \pmod{11} \\ x \equiv 3 \pmod{17}. \end{cases}$$

La primer ecuación es equivalente a $x = 11y + 4$ y la segunda es equivalente a $x = 17z + 3$. Por lo tanto, resolver el sistema anterior es equivalente a resolver la ecuación diofántica $17z - 11y = 1$. Fácilmente se ve que $y = 3$, $z = 2$ es una solución de la ecuación diofántica de lo que se deduce que $x \equiv 37 \pmod{11 \times 17}$ es la solución del primer sistema.

Ejercicio 2.

1) Ver Definición 4.1.1 de las notas del curso.

2) Ver Lema 4.1.7 de las notas del curso.

3) Ver Teorema 4.1.10 de las notas del curso.

Ejercicio 3.

1) Primero veamos que $O_n(\mathbb{R})$ es un subgrupo de $Gl_n(\mathbb{R})$.

   a. Es claro que $Id \in O_n(\mathbb{R})$ ya que $Id^t = Id$ y $Id^2 = Id$.

   b. Sean $A, B \in O_n(\mathbb{R})$, por lo tanto $A^tA = AA^t = Id$ y $B^tB = BB^t = Id$. Recordando que $(AB)^t = B^tA^t$ $\forall A, B \in GL_n(\mathbb{R})$ tenemos que $(AB)^t(AB) = (B^tA^t)(AB) = B^t(A^tA)B = B^t(Id)B = B^tB = Id$. Análogamente se prueba que $(AB)(AB)^t = Id$.

   c. Recordando que $(A^t)^{-1} = (A^{-1})^t$ y que $(AB)^{-1} = B^{-1}A^{-1}$ $\forall A, B \in GL_n(\mathbb{R})$, tenemos que $A^{-1}(A^{-1})^t = A^{-1}(A^t)^{-1} = (A^tA)^{-1} = Id^{-1} = Id$. Análogamente se prueba que $(A^{-1})^tA^{-1} = Id$.

   Veamos, ahora que si $A \in O_n(\mathbb{R})$ entonces $\det(A) \in \{-1, 1\}$. Como $A \in O_n(\mathbb{R})$, tenemos que $A^tA = AA^t = Id$ y, por lo tanto, $\det(AA^t) = \det(Id)$. Luego, dado que $\det(Id) = 1$ y $\det(A^t) = \det(A)$, obtenemos que $\det(A)^2 = 1$. Entonces $\det(A) = \pm 1$.

2) Se tiene que $\det : O_n(\mathbb{R}) \to \mathbb{R}^*$ es un morfismo de grupos cuyo núcleo es $SO_n(\mathbb{R})$. Por lo tanto, $SO_n(\mathbb{R})$ es un subgrupo normal (Ver Proposición 4 de notas Subgrupos normales, Grupo cociente y Teoremas de isomorfismos).

3) Ver Teorema 3 de notas Subgrupos normales, Grupo cociente y Teoremas de isomorfismos.

4) Como $\det : O_n(\mathbb{R}) \to (\{-1, 1\}, \times, 1)$ es un morfismo de grupos sobreyectivo, por el primer teorema de isomorfismo $O_n/\ker(\det) \cong (\{-1, 1\}, \times, 1)$. Por la parte 2) se concluye que $O_n/SO_n \cong (\{-1, 1\}, \times, 1)$.