Universidad de la República
Facultad de Ciencias
Centro de Matemática **Álgebra Lineal II**
Segundo semestre 2023

Práctico 1: Diagonalización, forma de Jordan, cuerpos y polinomios.

1. Un número complejo es algebraico si existe un polinomio con coeficientes en $\mathbb{Q}$ que lo anula. El propósito de este ejercicio es repasar propiedades básicas de espacios vectoriales de dimensión finita, demostrando que la suma y el producto de dos números algebraicos son también algebraicos.

   a) Supongamos que $\alpha, \beta \in \mathbb{C}$ son algebraicos. Demostrar que el $\mathbb{Q}$-espacio vectorial formado por las combinaciones lineales racionales de números complejos de la forma $\alpha^i\beta^j$ con i, j enteros no negativos, tiene dimensión finita.

   b) Deducir que $(\alpha + \beta), (\alpha + \beta)^2, (\alpha + \beta)^3, \dots$ no pueden ser linealmente independientes, y concluir que $(\alpha + \beta)$ es anulado por algún polinomio de coeficientes racionales.

   c) Repetir el argumento para $\alpha\beta$ ¿Qué cota se obtiene sobre el grado del polinomio que lo anula?

   d) Encontrar un polinomio de coeficientes racionales que anula $\sqrt[2]{2} + \sqrt[3]{3}$.

2. Dos enteros son congruentes módulo un natural $n \geq 2$ si su diferencia es divisible entre n. Los *enteros módulo* n se denotan por $\mathbb{Z}_n = \mathbb{Z}/(n\mathbb{Z})$, y son el cociente de $\mathbb{Z}$ por la relación de congruencia módulo n, con las operaciones de suma y multiplicación heredadas. Las operaciones siguen siendo asociativas, commutativas, tienen neutros que son diferentes, la suma tiene opuestos, y el producto distribuye respecto a la suma. La única propiedad para que $\mathbb{Z}_n$ sea un cuerpo que no es automática es que los elementos no nulos tengan inverso.

   Una raíz primitiva modulo un primo p es un número natural k tal que todo número en $\{1, \dots, p - 1\}$ es congruente módulo p con algúna potencia de k. Por ejemplo 3 es una raíz primitiva módulo 7, sus potencias son congruentes con $3, 2, 6, 4, 5$ y 1 en ese orden (¡verificar!). El objetivo de este ejercicio es trabajar propiedades básicas de cuerpos y polinomios demostrando la existencia de raices primitivas.

   a) Demostrar que los enteros módulo n forman un cuerpo si y sólamente si n es un número primo.

   b) Calcular $\frac{1}{3}$ en $\mathbb{Z}_7$.

   c) Demostar que un polinomio de grado d con coeficientes en cuerpo $\mathbb{K}$ tiene a lo sumo d raices en $\mathbb{K}$. Para esto se puede usar la división de polinomios, es decir que dados polinomios p, q con $q \neq 0$, existen otros a, r tales que $p = aq + r$ y el grado de r es estríctamente menor al de q.

   d) Usando el ejercicio anterior mostrar que en $\mathbb{Z}_p$ donde p es primo, existe $x \neq 0$ tal que $x, x^2, \dots, x^{p-1}$ son todos los elementos no nulos.

   e) Calcular un raíz primitiva módulo 11.

3. El juego *Lights Out* consiste de una grilla de luces cuadradas, algunas encendidas y otros no. El objetivo del juego es apagar todas las luces. Para esto se apretan los cuadrados en algún orden. Al apretar un cuadrado él y sus vecinos immediatos en horizontal y vertical *cambian su estado* (es decir se apagan si estaban prendidos y vice versa).

   Modelamos este juego en un grilla 3×3 de la siguiente manera. Los estados posibles del tablero son las matrices 3×3 con entradas en $\mathbb{Z}_2$. Apretar un botón equivale a sumarle a la matriz de estado una matriz, por ejemplo si se apreta el boton en posición $(1, 1)$ se suma la matriz

$$A_{1,1} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Similarmente hay una matriz $A_{i,j}$ definida para cada par con $1 \leq i, j \leq 3$.

a) Llamemos V al espacio de estados posibles considerado como un $\mathbb{Z}_2$-espacio vectorial. Mostrar que se puede resolver el juego empezando en cualquier estado sí y sólo si el conjunto de vectores $A_{i,j}$ con $1 \leq i, j \leq 3$ genera V.

b) De la parte anterior concluir que apretar más de una vez el mismo cuadrado nunca es necesario para resolver el puzzle si es posible hacerlo.

c) Decidir si en el caso 3×3 se puede ganar el juego empezando en cualquier estado o no. En caso de que no dar un estado inicial desde el cuál no es posible apagar todas las luces.

d) Ganar el juego a partir del estado inicial $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$. ¿Cuántos pasos se necesitan?

4. La traza de una matriz cuadrada A con elementos en algún cuerpo $\mathbb{K}$ es la suma de los elementos en la diagonal principal.

   a) Demostar que la traza es una función lineal de las matrices $n \times n$ con entradas en $\mathbb{K}$ a $\mathbb{K}$.

   b) Demostrar que $\text{Traza}(AB) = \text{Traza}(BA)$ para todo par de matrices $n \times n$ con entradas en $\mathbb{K}$.

   c) Supongamos que $T : M_n(\mathbb{K}) \to \mathbb{K}$ es lineal (donde $M_n(\mathbb{K})$ es el $\mathbb{K}$-espacio vectorial de matrices $n \times n$ con entradas en $\mathbb{K}$) y satisface $T(AB) = T(BA)$ para todo par $AB \in M_n(\mathbb{K})$. Demostrar que T es un múltiplo de la traza. Esto se puede hacer explorando las diversas relaciones entre las matrices con un único 1 y todos los demás coeficientes iguales a cero.

   d) Dado una transformación lineal $T : V \to V$ de un $\mathbb{K}$-espacio vectorial de dimensión n en si mismo, demostrar que la traza de la matriz asociada en cualquier base es la misma (se usa la misma base como base de llegada y partida). Por lo tanto tiene sentido hablar de la traza de T.

   e) En el caso de que T sea diagonalizable mostrar que $\text{Traza}(T)$ es la suma de los valores propios de T.

5. En este ejercicio intentamos illustrar que conocer un polinomio que anula una transformación lineal $T : V \to V$ de un espacio vectorial V da mucha información.

   a) Demostrar que toda transformación lineal $T : V \to V$ donde V es un $\mathbb{K}$-espacio vectorial de dimensión finita es anulada por algún polinomio no nulo con coeficientes en $\mathbb{K}$. Para esto, observar que el espacio vectorial de tales transformaciones tiene dimensión finita. ¿Qué cota da este argumento sobre mínimo grado de un polinomio que anula una matriz 3×3?

   Una proyección es una transformación lineal P de un $\mathbb{K}$-espacio vectorial V en si mismo que cumple $P^2 = P$.

   b) Demostrar que si P es una proyección entonces los únicos valores propios posibles son 0 y 1.

   c) Suponiendo que ambos valores propios ocurren mostrar que $V = V_0 \oplus V_1$ donde V_i es el subespacio propio de valor propio i para $i = 0, 1$.

   d) Dados dos subespacios X, Y tales que $V = X \oplus Y$ definimos $P_{X,Y}(v) = y$ donde $v = x + y$ con $x \in X$ e $y \in Y$. Mostrar que $P_{X,Y}$ es una proyección. Se suele llamar *proyección sobre y en dirección de x*.

   e) Demostrar que dos proyecciones en un mismo espacio que tienen la misma traza son conjugadas, i.e. existe una transformación lineal invertible S tal que $P_1 = S^{-1} P_2 S$ donde P_1, P_2 son las proyecciones en cuestión.

6. Uno de los usos de la diagonalización es calcular explícitamente potencias de matrices, o al menos tener una idea de a qué tasa crecen los coeficientes de estas potencias. Esto aparece en varias situaciones a priori no relacionadas en matemática.

   Un ejemplo es, dado un grafo dirigido con n vértices si A es la matriz $n \times n$ donde la entrada (i, j) es el número de caminos de largo 1 (i.e. aristas) entre el vértice i y el j, entonces las entradas de A^n cuentan la cantidad de caminos de largo n entre cada par de vértices.

   a) Usando la observación anterior dar una fórmula explícita para el número de palabras de largo n con las letras 'a' y 'b' que no contienen ni dos 'b' consecutivas ni tres 'a' consecutivas.

   b) El llamado *grupo modular* $\mathrm{PSL}(2, \mathbb{Z})$ está formado por las matrices 2×2 de entradas enteras y determinante 1 cocientado por opuestos (i.e. matrices opuestas se consideran el mismo elemento). Está en biyección con el conjunto de palabras anteriores asignando $b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ y $a = \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix}$. ¿Podés demostrarlo?

7. Un principio general es que si dos transformaciones lineales $S, T : V \to V$ de un espacio vectorial de dimensión finita conmutan entonces la unión de los subespacios S-invariantes es invariante por T. Esto significa que entender los subespacios invariantes de un operador ayuda a entender los del otro.

   Consideramos n números en círculo y la operación de cambiar cada número por el promedio de sus vecinos. ¿Qué sucede si repito esta operación muchas veces? ¿Cada número se acerca al promedio de los iniciales? ¿En caso afirmativo a qué velocidad?

   Para formalizar y responder estas pregundas consideramos el espacio vectorial complejo V de sucesiones $x = (x_1, \ldots, x_n) \in \mathbb{C}^{\mathbb{Z}_n}$ de n números complejos indexados por $\mathbb{Z}_n$) de modo que $x_{n+1} = x_1$. Y las transformaciones definidas por

   $$(Tx)_i = \frac{x_{i-1} + x_{i+1}}{2},$$

   y

   $$(Sx)_i = x_{i+1}.$$

   a) Calcular explícitamente los vectores y valores propios de S.

   b) Usando lo anterior calcular explícitamente los vectores y valores propios de T.

   c) Usando lo anterior responder a las preguntas que fueron planteadas inicialmente.

8. Una de las ecuaciones diferenciales más básicas de la física es la ecuación homogénea de segundo orden con coeficientes constantes en una variable. En la misma se buscan funciones $f : \mathbb{R} \to \mathbb{R}$ que cumplan

   $$af'' + bf' + cf = d,$$

   para ciertas constantes $a, b, c, d \in \mathbb{R}$ donde $a \neq 0$.

   Casos particulares de trayectorias físicas que pueden modelarse con esta ecuación son, partículas en caída libre, caída libre con rozamiento proporcional (y opuesto) a la velocidad, sistema de masa resorte con y sin rozamiento.

   Mediante el truco de definir $x(t) = f(t), y(t) = f'(t), z(t) = 1$ estas ecuaciones se convierten en

   $$\begin{pmatrix} x'(t) \\ y'(t) \\ z'(t) \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ -\frac{c}{a} & -\frac{b}{a} & \frac{d}{a} \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x(t) \\ y(t) \\ z(t) \end{pmatrix}.$$

Llamando A a la matrix 3×3 que aparece del lado derecho, esta última ecuación resulta tener solución explícita

$$\begin{pmatrix} x(t) \\ y(t) \\ z(t) \end{pmatrix} = \exp(tA) \begin{pmatrix} x(0) \\ y(0) \\ 1 \end{pmatrix},$$

donde la exponencial de la matriz tA se define como el límite

$$\exp(tA) = 1 + tA + \frac{1}{2}t^2A^2 + \cdots + \frac{1}{n!}t^nA^n + \cdots,$$

y 1 respresenta la matriz identidad en el lado derecho de esta fórmula.

Por lo tanto es útil diagonalizar o conocer la forma de Jordan de A para calcular esta exponencial.

a) Usando la exponencial de matries calcular explícitamente en términos de $f(0), f'(0)$ la solución a la ecuación diferencial $f''(t) = 10$ (grosso modo modela la distancia caída en metros para un objeto en caída libre en la tierra, ignorando rozamiento).

b) Hacer lo mismo para $f''(t) = 10 - f'(t)$ que modela caída libre con rozamiento lineal (pero ni idea cual sería el coeficiente para f' más adecuado para calcular la velocidad terminal de una gota de lluvia...).

c) Hacer lo mismo para $f''(t) = -f(t)$ comprobando que la exponencial de matrices devuelve las series de Taylor conocidas de las funciones trigonométricas.

d) En cada caso anterior discutir los vectores y valores propios de la matriz A asociada a la ecuación considerando $\mathbb{R}$ como el cuerpo base.

9. Supongamos que empezando en un número entero positivo se tira un dado balanceado y si sale 1 o 2 se suma 1 al número, mientras que si sale $3, 4, 5$ o 6 se resta 1.

Es intuitivo que repitiendo este procedimiento se llegará a 0 eventualmente, mientras que el número de turnos que se demore dependerá del azar. ¿Cuál es el número medio de turnos (por ejemplo si repetimos el experimento muchas veces y promediamos) que se demora en llegar a 0 empezando desde n?

Llamando $f(n)$ a esta cantidad es razonable pensar que esta sucesión cumple la ecuación

$$f(n) = 1 + \frac{2}{3}f(n-1) + \frac{1}{3}f(n+1),$$

para $n = 1, 2, \ldots$.

a) Mostrar que si $f(0) = a, f(1) = b$ para una solución a la ecuación anterior entonces

$$\begin{pmatrix} f(n) \\ f(n+1) \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ -2 & 3 & -3 \\ 0 & 0 & 1 \end{pmatrix}^n \begin{pmatrix} a \\ b \\ 1 \end{pmatrix}.$$

b) Encontrar una fórmula explícita para $f(n)$ en términos de a, b.

c) Dar una fórmula explícita para el número promedio de turnos hasta llegar a 0 si se empieza en n en el experimendo con dados descrito. Para esto usar que esta para esta solución $f(n)/n$ se mantiene acotada.

10. Pegando n triángulos por un vértice se obtiene un grafo no dirigido, conexo, sin lazos, ni aristas múltiples (i.e. aristas uniendo el mismo par de vértices), tal entre todo par de vértices distintos existe un único camino de largo 2. ¿Estos son los únicos grafos con estas propiedades? Erdös, Renyi, y Sos fueron los primeros en demostrar que sí, en la década de 1960.

    El enunciado informal es que, si en un grupo de personas todo par tiene exáctamente un amigo en común, entonces hay una persona que es amigo de todos.

    La demostración consiste primero en ver que cualquier otro grafo ejemplo debería ser regular, es decir, todo vértice tendría el mismo número de vecinos k.

    Luego se usa álgebra lineal para ver que esto es contradictorio.

    El propósito de este ejercicio es trabajar sobre esta segunda parte del argumento. Una demostración completa puede leerse del excelente libro "Proofs from de The Book"(capítulo 34).

    a) Llamando A la matriz de adyacencia de un supuesto grafo bueno k-regular con n vértices calcular A^2 explícitamente.

    b) Suponiendo que A^2 es diagonalizable calcular la forma diagonal en términos de n y k.

    c) Suponiendo que A es diagonalizable y tiene $a+1$ autovalores positivos y b negativos mostrar que $h = \sqrt{k-1}$ debe ser racional y por lo tanto entero.

    d) Obtener $h(a-b) = k = h^2 + 1$ de donde h debe dividir $h^2 + 1$ y se obtiene que $k = 2$.

    e) Demostrar que no puede existir un grafo bueno 2-regular.