Universidad de Chile
Facultad de Ciencias Físicas y Matemáticas
Departamento de Ingeniería Matemática
MA1102 - 2 Álgebra Lineal
21 de Agosto de 2019

Pseudo Pauta Clase Auxiliar #3: Cálculo de Inversas

Profesora: Natacha Astromujoff
Profesor Auxiliar: Juan Pedro Ross

P1. Encuentre la inversa de la siguiente matriz:

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 0 \\ -1 & 1 & 1 & 1 \\ -1 & -1 & 1 & -1 \end{pmatrix}$$

R: Escribimos el sistema aumentado con la identidad y pivoteamos.

$$(A|I_4) = \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 & 1 & 0 & 0 \\ -1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ -1 & -1 & 1 & -1 & 0 & 0 & 0 & 1 \end{array}\right) \xRightarrow{E_{13}(1)} \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 2 & 2 & 2 & 1 & 0 & 1 & 0 \\ -1 & -1 & 1 & -1 & 0 & 0 & 0 & 1 \end{array}\right)$$

$$\xRightarrow{E_{14}(1)} \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 2 & 2 & 2 & 1 & 0 & 1 & 0 \\ 0 & 0 & 2 & 0 & 1 & 0 & 0 & 1 \end{array}\right) \xRightarrow{E_{23}(-2)} \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & -2 & 2 & 1 & -2 & 1 & 0 \\ 0 & 0 & 2 & 0 & 1 & 0 & 0 & 1 \end{array}\right)$$

$$\xRightarrow{E_{34}(1)} \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & -2 & 2 & 1 & -2 & 1 & 0 \\ 0 & 0 & 0 & 2 & 2 & -2 & 1 & 1 \end{array}\right) \xRightarrow{E_{43}(-1)} \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & -2 & 0 & -1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 2 & 2 & -2 & 1 & 1 \end{array}\right)$$

$$\xRightarrow{E_{32}(1)} \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 & 1 & 0 & -1 \\ 0 & 0 & -2 & 0 & -1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 2 & 2 & -2 & 1 & 1 \end{array}\right) \xRightarrow{E_{41}(\frac{-1}{2})} \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 0 & 0 & 1 & \frac{-1}{2} & \frac{-1}{2} \\ 0 & 1 & 0 & 0 & -1 & 1 & 0 & -1 \\ 0 & 0 & -2 & 0 & -1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 2 & 2 & -2 & 1 & 1 \end{array}\right)$$

$$\xRightarrow{E_{31}(\frac{1}{2})} \left(\begin{array}{cccc|cccc} 1 & 1 & 0 & 0 & \frac{-1}{2} & 1 & \frac{-1}{2} & -1 \\ 0 & 1 & 0 & 0 & -1 & 1 & 0 & -1 \\ 0 & 0 & -2 & 0 & -1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 2 & 2 & -2 & 1 & 1 \end{array}\right) \xRightarrow{E_{21}(-1)} \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & \frac{1}{2} & 0 & \frac{-1}{2} & 0 \\ 0 & 1 & 0 & 0 & -1 & 1 & 0 & -1 \\ 0 & 0 & -2 & 0 & -1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 2 & 2 & -2 & 1 & 1 \end{array}\right)$$

$$\xRightarrow{D(1,1,\frac{-1}{2},\frac{1}{2})} \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & \frac{1}{2} & 0 & \frac{-1}{2} & 0 \\ 0 & 1 & 0 & 0 & -1 & 1 & 0 & -1 \\ 0 & 0 & 1 & 0 & \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 1 & 1 & -1 & \frac{1}{2} & \frac{1}{2} \end{array}\right)$$

$$\therefore \quad A^{-1} = \begin{pmatrix} \frac{1}{2} & 0 & \frac{-1}{2} & 0 \\ -1 & 1 & 0 & -1 \\ \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ 1 & -1 & \frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

P2. Criptografía

El mundo de las telecomunicaciones y las nuevas tecnologías de la información se interesa cada vez más por la transmisión de mensajes encriptados que sean difíciles de desencriptar por otros, en caso de ser interceptados, pero que se decodifiquen con facilidad por quienes los reciben. Hay muchas formas interesantes de cifrar o encriptar mensajes, y en su mayor parte usan la teoría de números o el álgebra lineal. Describiremos aquí un método que es eficaz, en especial cuando se usa una matriz de gran tamaño.

Se debe establecer una matriz M invertible, que sólo la conocen quienes trasmiten y quienes reciben los mensajes. En este caso, consideraremos la matriz

$$\begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 2 \end{pmatrix}$$

Supongamos que el mensaje a encriptar es "HOLA MUNDO".

Se reemplaza cada letra por el el lugar que ocupa en el abecedario representando el espacio con 0. El mensaje anterior se ha convertido en la sucesión de números

$$8, 16, 12, 1, 0, 13, 22, 14, 4, 16$$

que agrupamos en una sucesión de vectores columna

$$\begin{pmatrix} 8 & 1 & 22 & 16 \\ 16 & 0 & 14 & 0 \\ 12 & 13 & 4 & 0 \end{pmatrix}$$

Para deformar el mensaje se premultiplica por la matriz M, que es el código que conocen ambas partes, y se envía la sucesión de números obtenido.

Suponga que recibe la siguiente sucesión de números

$$18, 19, -12, 17, 18, -11, -5, -4, 23, -5, -2, 19, -3, -10, 29, 7, 9, 17, 20, 8, -12.$$

¿Cuál es el mensaje encriptado?
R:

$$A = \begin{pmatrix} 18 & 17 & -5 & -5 & -3 & 7 & 20 \\ 19 & 18 & -4 & -2 & -10 & 9 & 8 \\ -12 & -11 & 23 & 19 & 29 & 17 & -12 \end{pmatrix}$$

¿Por qué esa cantidad de filas y no otra?, luego el problema se reduce a $MX = A \Rightarrow X = M^{-1}A$.

$$Diag\left(\frac{1}{2}, \frac{2}{3}, \frac{3}{4}\right) \cdot E_{21}\left(\frac{2}{3}\right) \cdot E_{32}\left(\frac{3}{4}\right) \cdot E_{23}\left(\frac{3}{2}\right) \cdot E_{12}\left(\frac{1}{2}\right) \cdot (M|I_3) \Rightarrow M^{-1} = \begin{pmatrix} \frac{3}{4} & \frac{1}{2} & \frac{1}{4} \\ \frac{1}{2} & 1 & \frac{1}{2} \\ \frac{1}{4} & \frac{1}{2} & \frac{3}{4} \end{pmatrix}$$

$$X = M^{-1}A = \begin{pmatrix} 20 & 19 & 0 & 0 & 0 & 14 & 16 \\ 22 & 21 & 5 & 5 & 3 & 21 & 12 \\ 5 & 5 & 14 & 12 & 16 & 19 & 0 \end{pmatrix}$$

Por lo tanto el mensaje es...

P3. Dado el siguiente sistema de ecuaciones:

$$\begin{cases} x + y - z = 0 \\ 3x + \alpha y - \alpha z = 0 \\ 4x + \alpha y = 0 \end{cases}$$

(a) Discutir, en función de α, cuando existen infinitas, ninguna, única solución.
R: Escribimos sistema matricial aumentado, pivoteamos con $E_{12}(-3), E_{13}(-4), E_{23}(\frac{-(\alpha-4)}{\alpha-3})$ (Para el último asumimos $\alpha \neq 3$), llegando a

$$\begin{pmatrix} 1 & 1 & -1 & | & 0 \\ 0 & \alpha-3 & -(\alpha-3) & | & 0 \\ 0 & 0 & 4+(\alpha-4) & | & 0 \end{pmatrix}$$

Luego si $\alpha = 3$ o $\alpha = 0$ hay infinitas soluciones, si ninguna de estas se cumple hay única solución.

(b) Resolverlo cuando sea compatible.
R: Imponemos $\alpha \neq 4$ y $\alpha \neq 3$, luego la solución de la tercera ecuación es $x_3 = 0$, por ende $x_2 = 0$ y así $x_1 = 0$. Es decir la única solución es $x = 0$... ¿Será coincidencia?

(c) Para el caso con infinitas soluciones, encontrar $p \in \mathbb{R}$, $v \in \mathbb{R}^3$, tales que la solución general del sistema sea de la forma pv. ¿Es única esta descomposición?
R:

- Caso $\alpha = 0$, de la tercera (en la matriz antes de la explicitada arriba) $x_2 = 4x_3$, luego de la primera $x_1 = -3x_3$.

$$\therefore x = x_3 \begin{pmatrix} -3 \\ 4 \\ 1 \end{pmatrix}, \quad x_3 \in \mathbb{R}$$

.

- Caso $\alpha = 4$, de la segunda $x_2 = x_3$, y por lo tanto $x_1 = 0$.

$$\therefore x = x_2 \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \quad x_2 \in \mathbb{R}.$$

No es única, basta tomar $v^* = \delta v$, con $\delta \in \mathbb{R} \setminus \{0\}$.

(d) Sabiendo que x_1 y x_2 son soluciones del sistema, ¿Qué puede decir de $\delta x_1 + x_2$, con $\delta \in \mathbb{R}$ cualquiera.
R: Recordando que $Ax_i = 0$ y aplicando distributividad, se concluye que también es solución. Otra forma de verlo es utilizando la parte anterior y escribiendo x_1 y x_2 como ponderación de v y concluyendo que $\delta x_1 + x_2$ también es ponderación de v.

(e) Si el lado de la derecha del sistema fuese un $b \in R^3 \setminus \{0\}$, ¿Seguiría cumpliéndose lo de la parte anterior?, por lo tanto ¿Es posible encontrar una descomposición pv en ese caso?
R: Recordando que $Ax_i = b$ y aplicando distributividad se ve que no es verdad. Por ende no es posible encontrar una descomposición de esa forma, si lo fuese, razonando como en la parte anterior, se llegaría a una contradicción.

P4. Sea $B \in \mathcal{M}_{nn}(\mathbb{R})$ no invertible tal que satisface que $B^3 = 0$.

Para cada $\alpha \in \mathbb{R}$ se define $M(\alpha) \in \mathcal{M}_{nn}(\mathbb{R})$ por:

$$M(\alpha) = I + \alpha B + \tfrac{\alpha^2}{2} B^2$$

(a) Pruebe que:

$$\forall \alpha, \beta \in \mathbb{R},\ M(\alpha + \beta) = M(\alpha) \cdot M(\beta)$$

y deduzca que $M(\beta) \cdot M(\alpha) = M(\alpha) \cdot M(\beta)$.
R: Para la primera igualdad, escoger un lado (se recomienda derecho), aplicar distributividad y reconocer cuadrado de binomio. Para la segunda notar que $\alpha + \beta = \beta + \alpha$.

(b) Pruebe que $M(\alpha)$ es invertible, y que $M(\alpha)^{-1} = M(-\alpha)$.
R: $M(\alpha)M(-\alpha) = ... = I$