

Example

$$A = \begin{pmatrix} 4 & 3 \\ 6 & 2 \end{pmatrix} \quad B = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

$$A+B = \begin{pmatrix} 5 & 5 \\ 9 & 6 \end{pmatrix}$$

$$A-B = \begin{pmatrix} 3 & 1 \\ 3 & -2 \end{pmatrix}$$

$$AB = \begin{pmatrix} 13 & 20 \\ 12 & 20 \end{pmatrix} \quad AB \neq BA$$

$$BA = \begin{pmatrix} 16 & 7 \\ 36 & 17 \end{pmatrix}$$

Scalar Multiplication

If A is a matrix and if k is a number then we let

$$kA$$

denote the matrix got from A by multiplying each entry of A by k .

Example

$$A = \begin{pmatrix} 1 & 2 & 3 \\ -2 & -4 & 5 \end{pmatrix}$$

$$k = -2$$

$$kA = \begin{pmatrix} -2 & -4 & -6 \\ 4 & 8 & -10 \end{pmatrix}$$

Identity Matrices

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad A = \begin{pmatrix} 7 & 13 \\ 8 & 9 \end{pmatrix}$$

$$IA = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 7 & 13 \\ 8 & 9 \end{pmatrix} = \begin{pmatrix} 7 & 13 \\ 8 & 9 \end{pmatrix} = A$$

$$AI = \begin{pmatrix} 7 & 13 \\ 8 & 9 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 7 & 13 \\ 8 & 9 \end{pmatrix} = A$$

In this example $AI = A = IA$

In general let I denote an $n \times n$ matrix with each diagonal entry equal to 1, and all other entries equal to 0.

e.g.

$$n=2 \quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$n=3 \quad I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$n=4 \quad I = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Check: For any $n \times n$ matrix A we have

$$AI = A = IA$$

We call I the identity matrix (of dimension $n \times n$)

Defn Let A be an $n \times n$ matrix.

The inverse of A is an $n \times n$ matrix B

Such that

$$AB = I = BA$$

We'll write $A^{-1} = B$.

Consider $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix}$$

$$= (ad-bc) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = (ad-bc)I$$

Proposition Given $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ we

have

$$A^{-1} = (ad-bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

provided $ad-bc$ is invertible.

Example $A = \begin{pmatrix} 1 & 4 \\ 5 & 7 \end{pmatrix}$

$$A^{-1} = \frac{1}{1 \cdot 7 - 5 \cdot 4} \begin{pmatrix} 7 & -4 \\ -5 & 1 \end{pmatrix}$$

$$A^{-1} = \begin{pmatrix} -\frac{7}{13} & \frac{4}{13} \\ \frac{5}{13} & -\frac{1}{13} \end{pmatrix}$$

Affine Matrix Cryptosystems

Suppose we wish to encipher

HELLO_WORLD_

and that we are happy to use 2-letter message units.

$$\begin{pmatrix} H \\ E \end{pmatrix} \begin{pmatrix} L \\ L \end{pmatrix} \begin{pmatrix} O \\ - \end{pmatrix} \begin{pmatrix} W \\ O \end{pmatrix} \begin{pmatrix} R \\ L \end{pmatrix} \begin{pmatrix} D \\ - \end{pmatrix}$$

using a correspondence

$$A \leftrightarrow 0$$

$$B \leftrightarrow 1$$

:

$$Z \leftrightarrow 25$$

$$- \leftrightarrow 26$$

27-letter alphabet

$$\begin{pmatrix} 7 \\ 4 \end{pmatrix} \begin{pmatrix} 11 \\ 11 \end{pmatrix} \begin{pmatrix} \\ \end{pmatrix} \begin{pmatrix} \\ \end{pmatrix} \begin{pmatrix} \\ \end{pmatrix} \begin{pmatrix} \\ \end{pmatrix}$$

For an enciphering program we could choose some matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with entries $a, b, c, d \in \mathbb{Z}_{27}$
and some matrix

$$B = \begin{pmatrix} e \\ f \end{pmatrix}$$

with $e, f \in \mathbb{Z}_{27}$.

For an enciphering function we could use

$$f_E: \begin{pmatrix} x \\ y \end{pmatrix} \mapsto A \begin{pmatrix} x \\ y \end{pmatrix} + B.$$

Here A needs to be invertible.

The deciphering function would be

$$\begin{aligned} f_D: \begin{pmatrix} x \\ y \end{pmatrix} &\mapsto A^{-1} \left(\begin{pmatrix} x \\ y \end{pmatrix} - B \right) \\ &= A^{-1} \begin{pmatrix} x \\ y \end{pmatrix} - A^{-1} B. \end{aligned}$$