

Example

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

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

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

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

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

$AB \neq BA$ in this example.

Scalar multiplication

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

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

Example

$$A = \begin{pmatrix} 1 & 5 \\ -3 & 7 \end{pmatrix}$$

$$k = -4$$

$$kA = -4 \begin{pmatrix} 1 & 5 \\ -3 & 7 \end{pmatrix} = \begin{pmatrix} -4 & -20 \\ 12 & -28 \end{pmatrix}$$

Identity Matrices

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

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

$$IA = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ -3 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ -3 & 4 \end{pmatrix} = A$$

$$AI = \begin{pmatrix} 2 & 1 \\ -3 & 4 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ -3 & 4 \end{pmatrix} = A$$

So $IA = AI$ in this example.

In general, let I denote the $n \times n$ matrix with each diagonal entry equal to 1, and each non-diagonal entry equal to 0.

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

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

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

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

$$IA = A = AI$$

We call I the identity matrix.

Proposition

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

if $ad-bc$ is invertible.

Example

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

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

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

Definition 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 write $A^{-1} = B$

Consider

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

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

$$= \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix}$$

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

$$= (ad-bc)I$$

Cryptography (again)

An affine cryptosystem

$$X \mapsto \alpha X + \beta$$

on single letter message units
over an n -letter alphabet
is easily broken.

- Using the fact that E is the most frequent letter of English, followed by T, we can use frequency analysis to break the code.

Affine matrix cryptosystems

To counter frequency analysis we could break the plain text message up into message units (x, y) of length 2.

There are many contenders for the most frequent pair of letters in English, and frequency analysis is harder.

HELLO - WORLD -

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

We can encipher using an affine cryptosystem

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

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

a 2×2 matrix with entries

from \mathbb{Z}_N , and

$B = \begin{pmatrix} e \\ f \end{pmatrix}$ is a column vector

with entries from \mathbb{Z}_N .

Hence the 2×2 matrix A needs to be invertible.