Example

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix}$$

$$AB = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix} = \begin{pmatrix} 4 & 7 \\ 8 & 15 \end{pmatrix}$$

$$BA = \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 11 & 16 \end{pmatrix}$$

observe: $AB \neq BA$

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

$$A = \begin{pmatrix} 1 & 2 \\ -1 & 0 \\ 3 & -2 \end{pmatrix} \qquad k = -3$$

$$kA = \begin{pmatrix} -3 & -6 \\ 3 & 0 \\ -9 & 6 \end{pmatrix}$$

Inverse Matrices

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

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

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

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \qquad I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

check: $IA = A$

$AI = A$

In general, we let I denote the $n \times n$ matrix such that each diagonal entry is 1 and each non-diagonal entry is 0. We call I the identity matrix. It satisfies

$$IA = A = AI$$

for any $n \times n$ matrix A.

Definition If A and B are two $n \times n$ matrices satisfying

$$AB = I$$

then we write

$$B = A^{-1}.$$

We say that A^{-1} is the inverse of A.

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

Note

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

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

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

$$= (ad-bc) I$$

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

if $ad-bc$ is invertible.

Exemplo

$$A = \begin{pmatrix} 5 & 7 \\ 11 & 13 \end{pmatrix}$$

$$A^{-1} = \frac{1}{5.13 - 11.7} \begin{pmatrix} 13 & -7 \\ -11 & 5 \end{pmatrix}$$

$$= -\frac{1}{12} \begin{pmatrix} 13 & -7 \\ -11 & 5 \end{pmatrix}$$

$$A^{-1} = \begin{pmatrix} -\frac{13}{12} & \frac{7}{12} \\ \frac{11}{12} & -\frac{5}{12} \end{pmatrix}.$$

Cryptography

An affine cryptosystem

$$x \longmapsto \alpha x + \beta$$

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

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

Affine Matrix Cryptosystems

To counter frequency analysis we could break plaintext into message units (x, y) of length 2. There are many contenders for the most frequent pair (x, y) in English.

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 could encipher using

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

where:

- A denotes a fixed, invertible 2×2 matrix

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

mod N, N = number of letters in alphabet.

- B denotes a column vector

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

The enciphering key is

$$K_E = (A, B).$$

<u>Example</u> Use the enciphering function

$$f_E : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

to encipher the plaintext

NOANSWER

over a 26-letter alphabet with $A \sim 0$, $B \sim 1$, ..., $Z \sim 25$.

Sol^{n} plaintext

$$\begin{pmatrix} N \\ O \end{pmatrix} \begin{pmatrix} A \\ N \end{pmatrix} \begin{pmatrix} S \\ W \end{pmatrix} \begin{pmatrix} E \\ R \end{pmatrix}$$

$$\begin{pmatrix} 13 \\ 14 \end{pmatrix} \begin{pmatrix} 0 \\ 13 \end{pmatrix} \begin{pmatrix} 18 \\ 22 \end{pmatrix} \begin{pmatrix} 4 \\ 17 \end{pmatrix}$$

Ciphertext

$$\begin{pmatrix} 16 \\ 21 \end{pmatrix} \begin{pmatrix} 13 \\ 0 \end{pmatrix} \begin{pmatrix} \\ \end{pmatrix} \begin{pmatrix} \\ \end{pmatrix}$$

$$\begin{pmatrix} Q \\ V \end{pmatrix} \begin{pmatrix} N \\ A \end{pmatrix} \begin{pmatrix} \\ \end{pmatrix} \begin{pmatrix} \\ \end{pmatrix}$$

Ciphertext

QVNA ....