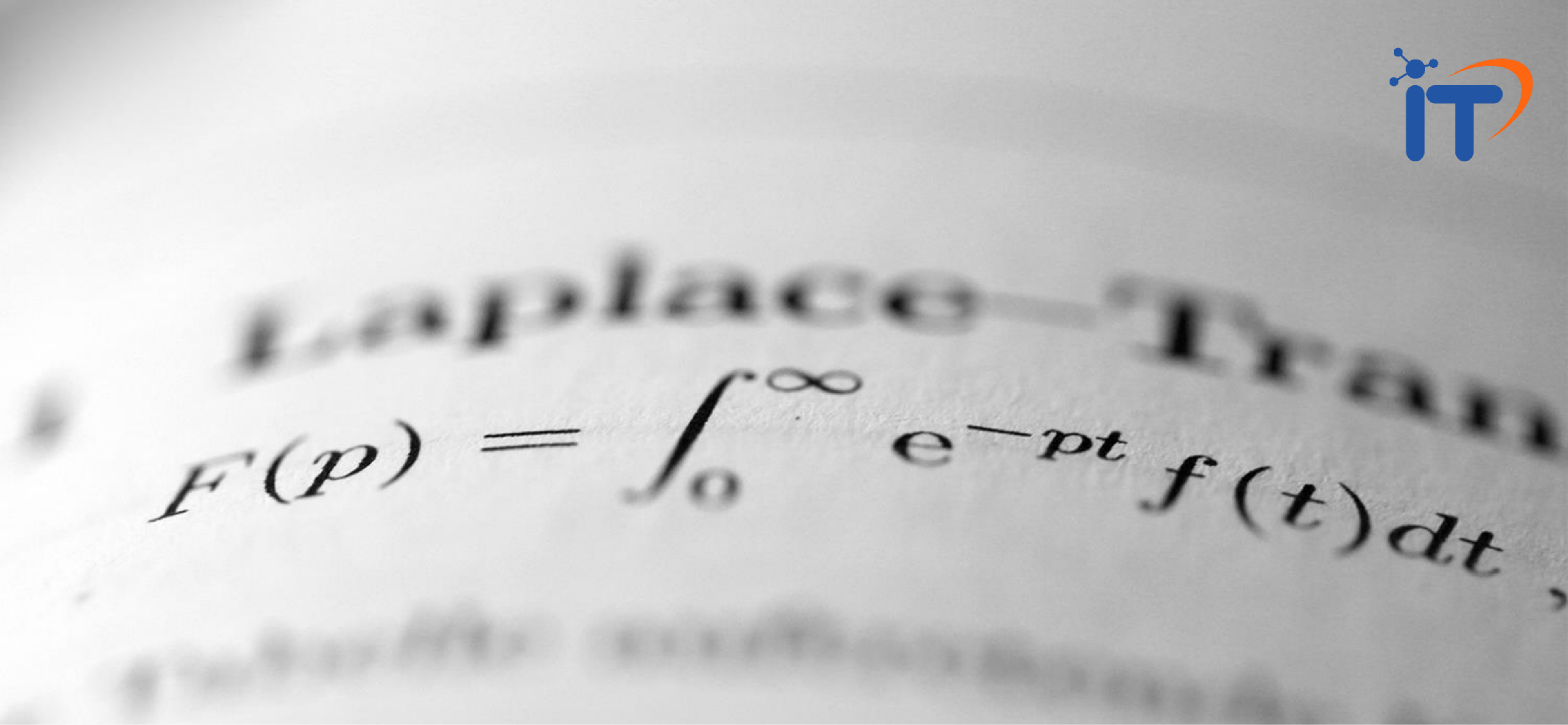


06016401

MATHEMATICS FOR INFORMATION TECHNOLOGY

Instructor: Asst. Prof. Dr. Praphan Pavarangkoon
Office: Room no. 418-5, 4th Floor
Email: praphan@it.kmitl.ac.th
Office hours: Wednesday at 9:00 – 12:00
or as an advance appointment

Outline

- Matrices
  - The Inverse of a Matrix
- Determinants
  - The Determinant of a Matrix
  - Applications of Determinants
- Applications of Matrix Operations
  - Cryptography

Key

- Symmetric matrix
- Singular/ matrix
Non-singular
- Square matrix
- Adjoint - Determinant
- Properties

The Inverse of a Matrix

Matrix ไม่เอกฐาน

An $n \times n$ matrix A is **invertible** (or **nonsingular**) if there exists an $n \times n$ matrix B such that

ขนาด $n \times n$ ทั้ง A และ B

$$AB = BA = I_n$$

where I_n is the identity matrix of order n. The matrix B is called the (multiplicative) **inverse** of A. A matrix that does not have an inverse is called **noninvertible** (or **singular**).

Matrix เอกฐาน

- หา Inverse ไม่ได้

$ax = b \quad \Rightarrow \quad a^{-1} = \frac{1}{a} ; a \neq 0$

$(a^{-1}a)x = a^{-1}b$

$x = a^{-1}b$

a^{-1} called การผกผันการคูณ

multiplicative inverse

$\boxed{a^{-1}a = 1 \#}$

Finding the Inverse of a Matrix

Find the inverse of the matrix

$$A = \begin{bmatrix} 1 & 4 \\ -1 & -3 \end{bmatrix}.$$

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

$$A^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

$$= \frac{1}{\underbrace{\cancel{-3+4}}_{1}}\begin{bmatrix} -3 & -4 \\ 1 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} -3 & -4 \\ 1 & 1 \end{bmatrix}$$

$$\boxed{AB = BA = I}$$

$$AB = I$$

$$\begin{bmatrix} 1 & 4 \\ -1 & -3 \end{bmatrix}\begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} x_{11} + 4x_{21} & x_{12} + 4x_{22} \\ -x_{11} - 3x_{21} & -x_{12} - 3x_{22} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$x_{11} + 4x_{21} = 1$ — (1)

$x_{12} + 4x_{22} = 0$ — (2)

$-x_{11} - 3x_{21} = 0$ — (3)

$-x_{12} - 3x_{22} = 1$ — (4)

(1) + (3)

$$4x_{21} = 4$$

$$x_{21} = 1$$

$$x_{21} = 1$$

$$-x_{11} = 3$$

$$x_{11} = -3$$

Properties of Inverse Matrices

If A is an invertible matrix, k is a positive integer, and c is a scalar not equal to zero, then A^{-1}, A^k, cA, and A^T are invertible and the following are true.

1. $(A^{-1})^{-1} = A$
2. $(A^k)^{-1} = A^{-1}A^{-1} \cdot \cdot \cdot A^{-1} = (A^{-1})^k$
3. $(cA)^{-1} = \dfrac{1}{c}A^{-1}, \ c \neq 0$
4. $(A^T)^{-1} = (A^{-1})^T$

If A and B are invertible matrices of size n, then AB is invertible and

$$(AB)^{-1} = B^{-1}A^{-1}.$$

The Determinant of a Matrix

- Every *square* matrix can be associated with a real number called its determinant. → Scalar
- Historically, the use of determinants arose (start to exist) from the recognition of special patterns that occur in the solutions of systems of linear equations.

Definition of the Determinant of a 2 × 2 Matrix

The **determinant** of the matrix

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

is given by

$$\det(A) = |A| = a_{11}a_{22} - a_{21}a_{12}.$$

REMARK: In this text, $\det(A)$ and $|A|$ are used interchangeably to represent the determinant of a matrix. Vertical bars are also used to denote the absolute value of a real number; the context will show which use is intended. Furthermore, it is common practice to delete the matrix brackets and write

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \quad \text{instead of} \quad \left| \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \right|.$$

A convenient method for remembering the formula for the determinant of a 2 × 2 matrix is shown in the diagram below.

$$|A| = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{21}a_{12}$$

The determinant is the difference of the products of the two diagonals of the matrix. Note that the order is important, as demonstrated above.

The Determinant of a Matrix of Order 2

Find the determinant of each matrix.

(a) $A = \begin{bmatrix} 2 & -3 \\ 1 & 2 \end{bmatrix}$ (b) $B = \begin{bmatrix} 2 & 1 \\ 4 & 2 \end{bmatrix}$ (c) $C = \begin{bmatrix} 0 & 3 \\ 2 & 4 \end{bmatrix}$

$= 4 + 3$

$= 7$

$= 4 - 4$

$= 0$

$= -6$

Definitions of Minors and Cofactors of a Matrix

ตัวประกอบร่วมเกี่ยว

If A is a square matrix, then the **minor** M_{ij} of the element a_{ij} is the determinant of the matrix obtained by deleting the ith row and jth column of A. The **cofactor** C_{ij} is given by

$$C_{ij} = (-1)^{i+j} M_{ij}.$$

$C_{ij} = (-1)^{i+j} \cdot M_{ij}$

For example, if A is a 3×3 matrix, then the minors and cofactors of a_{21} and a_{22} are as shown in the diagram below.

Minor of a_{21}

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}, \quad M_{21} = \begin{vmatrix} a_{12} & a_{13} \\ a_{32} & a_{33} \end{vmatrix}$$

Delete row 2 and column 1.

Cofactor of a_{21}

$$C_{21} = (-1)^{2+1} M_{21} = -M_{21}$$

Minor of a_{22}

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}, \quad M_{22} = \begin{vmatrix} a_{11} & a_{13} \\ a_{31} & a_{33} \end{vmatrix}$$

Delete row 2 and column 2.

Cofactor of a_{22}

$$C_{22} = (-1)^{2+2} M_{22} = M_{22}$$

Definitions of Minors and Cofactors of a Matrix (cont.)

As you can see, the minors and cofactors of a matrix can differ only in sign. To obtain the cofactors of a matrix, first find the minors and then apply the checkerboard pattern of $+$'s and $-$'s shown below.

Sign Pattern for Cofactors

$$\begin{bmatrix} + & - & + \\ - & + & - \\ + & - & + \end{bmatrix}$$

3×3 *matrix*

$$\begin{bmatrix} + & - & + & - \\ - & + & - & + \\ + & - & + & - \\ - & + & - & + \end{bmatrix}$$

4×4 *matrix*

$$\begin{bmatrix} + & - & + & - & + & \cdots \\ - & + & - & + & - & \cdots \\ + & - & + & - & + & \cdots \\ - & + & - & + & - & \cdots \\ + & - & + & - & + & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \end{bmatrix}$$

$n \times n$ *matrix*

Note that *odd* positions (where $i + j$ is odd) have negative signs, and even positions (where $i + j$ is even) have positive signs.

Find the Minors and Cofactors of a Matrix

Find all the minors and cofactors of

$$A = \begin{bmatrix} 0 & 2 & 1 \\ 3 & -1 & 2 \\ 4 & 0 & 1 \end{bmatrix}.$$

$M_{11} = \begin{vmatrix} -1 & 2 \\ 0 & 1 \end{vmatrix} = -1$

$C_{11} = -1$

$M_{12} = \begin{vmatrix} 3 & 2 \\ 4 & 1 \end{vmatrix} = 3-8 = -5$

$C_{12} = 5$

$M_{13} = \begin{vmatrix} 3 & -1 \\ 4 & 0 \end{vmatrix} = 4$

$C_{13} = 4$

$M_{21} = \begin{vmatrix} 2 & 1 \\ 0 & 1 \end{vmatrix} = 2$

$M_{22} = \begin{vmatrix} 0 & 1 \\ 4 & 1 \end{vmatrix} = -4$

$M_{23} = \begin{vmatrix} 0 & 2 \\ 4 & 0 \end{vmatrix} = -8$

$M_{31} = \begin{vmatrix} 2 & 1 \\ -1 & 2 \end{vmatrix} = 4+1 = 5$

$M_{32} = \begin{vmatrix} 0 & 1 \\ 3 & 2 \end{vmatrix} = -3$

$M_{33} = \begin{vmatrix} 0 & 2 \\ 3 & -1 \end{vmatrix}$

Definition of the Determinant of a Matrix

If A is a square matrix (of order 2 or greater), then the determinant of A is the sum of the entries in the first row of A multiplied by their cofactors. That is,

$$\det(A) = |A| = \sum_{j=1}^{n} a_{1j}C_{1j} = a_{11}C_{11} + a_{12}C_{12} + \cdot\cdot\cdot + a_{1n}C_{1n}.$$

The Determinant of a Matrix of Order 3

Find the determinant of

$$A = \begin{bmatrix} 0 & 2 & 1 \\ 3 & -1 & 2 \\ 4 & 0 & 1 \end{bmatrix}.$$

$-1, 5, 4$

C_{11}, C_{12}, C_{13}

$$= \cancel{0(C_{11})} + 2(C_{12}) + 1(C_{13})$$

$$= 10 + 4$$

$$= 14$$

ทำ row/column ไหนก็ได้

→ ผลลัพธ์เหมือนกัน

→ แต่ต้องใช้ cofactor ใน row/column นั้น #

Expansion by Cofactors

Let A be a square matrix of order n. Then the determinant of A is given by

$$\det(A) = |A| = \sum_{j=1}^{n} a_{ij}C_{ij} = a_{i1}C_{i1} + a_{i2}C_{i2} + \cdot\cdot\cdot + a_{in}C_{in}$$

or

$$\det(A) = |A| = \sum_{i=1}^{n} a_{ij}C_{ij} = a_{1j}C_{1j} + a_{2j}C_{2j} + \cdot\cdot\cdot + a_{nj}C_{nj}.$$

The Determinant of a Matrix of Order 4

Key

- หา row/column ที่มี 0 เยอะๆ

ex. Column$_3$

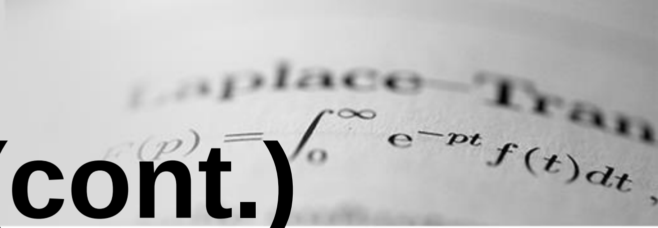
Find the determinant of

$$A = \begin{bmatrix} 1 & -2 & 3 & 0 \\ -1 & 1 & 0 & 2 \\ 0 & 2 & 0 & 3 \\ 3 & 4 & 0 & -2 \end{bmatrix}.$$

หา C_{13}

จะได้ det 3×3 แล้วค่อยหาย่อยลงไปเรื่อยๆ

Definition of the Determinant of a Matrix (cont.)



technique ต่อแถวต่อหลัก * ใช้ได้เหมือนกัน

There is an alternative method commonly used for evaluating the determinant of a 3×3 matrix A. To apply this method, copy the first and second columns of A to form fourth and fifth columns. The determinant of A is then obtained by adding (or subtracting) the products of the six diagonals, as shown in the following diagram.

Subtract these three products.

$$\begin{array}{ccccc} a_{11} & a_{12} & a_{13} & a_{11} & a_{12} \\ a_{21} & a_{22} & a_{23} & a_{21} & a_{22} \\ a_{31} & a_{32} & a_{33} & a_{31} & a_{32} \end{array}$$

Add these three products.

Try confirming that the determinant of A is

$$|A| = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{31}a_{22}a_{13} - a_{32}a_{23}a_{11} - a_{33}a_{21}a_{12}.$$

The Determinant of a Matrix of Order 3

ใช้ได้ 2 วิธี แต่ถ้า 0 เยอะใช้cofactorดีกว่า

Find the determinant of

$$A = \begin{bmatrix} 0 & 2 & 1 \\ 3 & -1 & 2 \\ 4 & -4 & 1 \end{bmatrix}. \quad \begin{matrix} 0 & 2 \\ 3 & -1 \\ 4 & -4 \end{matrix}$$

$= 16 - 12 + 4 - 6$

$= 4 + 4 - 6 = 8 - 6$

$= 2$ #

Conditions That Yield a Zero Determinant

det เป็น 0 แน่ๆ

If A is a square matrix and any one of the following conditions is true, then $\det(A) = 0$.

1. An entire row (or an entire column) consists of zeros.
2. Two rows (or columns) are equal.
3. One row (or column) is a multiple of another row (or column).

$$\begin{vmatrix} 0 & 0 & 0 \\ 2 & 4 & -5 \\ 3 & -5 & 2 \end{vmatrix} = 0, \qquad \begin{vmatrix} 1 & -2 & 4 \\ 0 & 1 & 2 \\ 1 & -2 & 4 \end{vmatrix} = 0, \qquad \begin{vmatrix} 1 & 2 & -3 \\ 2 & -1 & -6 \\ -2 & 0 & 6 \end{vmatrix} = 0.$$

The first row has all zeros.

The first and third rows are the same.

The third column is a multiple of the first column.

· -3 เท่า

$$\begin{vmatrix} 1 & -2 & 4 \\ 0 & 1 & 2 \\ 1 & -2 & 4 \end{vmatrix} \begin{matrix} 1 & -2 \\ 0 & 1 \\ 1 & -2 \end{matrix}$$

$\cancel{4} - 4 - \cancel{4}\,\cancel{4}\;4 -$

Properties of Determinants

If A and B are square matrices of order n, then

$$\det(AB) = \det(A)\det(B).$$

If A is an $n \times n$ matrix and c is a scalar, then the determinant of cA is given by

$$\det(cA) = c^n \det(A).$$

A square matrix A is invertible (nonsingular) if and only if

ไม่เอกฐาน → หา Inverse ได้

$$\det(A) \neq 0.$$

, if det(A) = 0

↳ not invertible

↳ ก็ต่อเมื่อ

If A is invertible, then

เพราะ $A^{-1} = \frac{1}{\det(A)} \cdot \text{adj}(A)$

เดี๋ยวส่วนติด 0

$$\det(A^{-1}) = \frac{1}{\det(A)}.$$

If A is a square matrix, then

$$\det(A) = \det(A^T).$$

The Adjoint of a Matrix

ตัวผูกพันธ์

- If A is a square matrix, then the **matrix of cofactors** of A has the form

$$\begin{bmatrix} C_{11} & C_{12} & \cdots & C_{1n} \\ C_{21} & C_{22} & \cdots & C_{2n} \\ \vdots & \vdots & & \vdots \\ C_{n1} & C_{n2} & \cdots & C_{nn} \end{bmatrix}.$$

- The transpose of this matrix is called the adjoint of A and is denoted by adj(A). That is,

$$\text{adj}(A) = \begin{bmatrix} C_{11} & C_{21} & \cdots & C_{n1} \\ C_{12} & C_{22} & \cdots & C_{n2} \\ \vdots & \vdots & & \vdots \\ C_{1n} & C_{2n} & \cdots & C_{nn} \end{bmatrix}.$$

เอา Cofactor มาเขียน Matrix
แล้ว transpose อีกรอบ
$\Downarrow$
Adjoint

Finding the Adjoint of a Square Matrix

Find the adjoint of

$$A = \begin{bmatrix} -1 & 3 & 2 \\ 0 & -2 & 1 \\ 1 & 0 & -2 \end{bmatrix}.$$

$M_{11} = \begin{vmatrix} -2 & 1 \\ 0 & -2 \end{vmatrix} = 4$

$M_{21} = \begin{vmatrix} 0 & 1 \\ 1 & -2 \end{vmatrix} = -1$

$M_{31} = \begin{vmatrix} 0 & -2 \\ 1 & 0 \end{vmatrix} = 0$

$M_{21} = \begin{vmatrix} 3 & 2 \\ 0 & -2 \end{vmatrix} = -6$

$M_{22} = \begin{vmatrix} -1 & 2 \\ 1 & -2 \end{vmatrix} = 2 - 2 = 0$

* another sol. is to write a big matrix with ± pattern

The Inverse of a Matrix Given by Its Adjoint

If A is an $n \times n$ invertible matrix, then

เอามาหา Inverse ได้!

$$A^{-1} = \frac{1}{\det(A)}\operatorname{adj}(A).$$

Using the Adjoint of a Matrix to Find Its Inverse

ติดเศษส่วนไว้ได้

Use the adjoint of

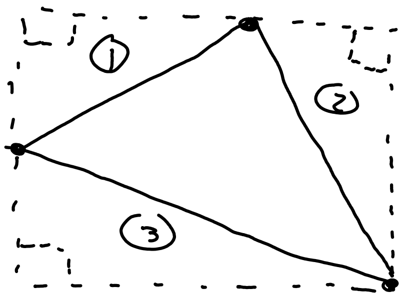
$$A = \begin{bmatrix} -1 & 3 & 2 \\ 0 & -2 & 1 \\ 1 & 0 & -2 \end{bmatrix}$$

to find A^{-1}.

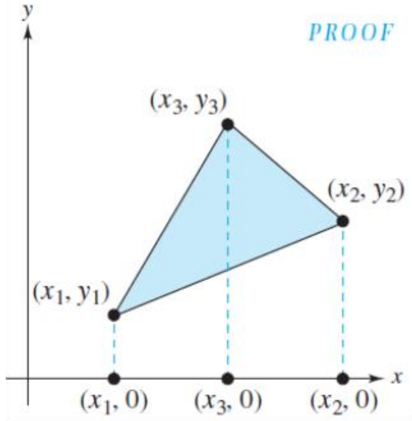
Applications of Determinants

- Area, Volume, and Equations of Lines and Planes
- Two-Point Form of the Equation of a Line
- Volume of a Tetrahedron

Area, Volume, and Equations of Lines and Planes



เป็นมุมฉาก, หา Area ได้



The area of the triangle whose vertices are (x_1, y_1), (x_2, y_2), and (x_3, y_3) is given by

$$\text{Area} = \pm\frac{1}{2}\det\begin{bmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{bmatrix},$$

จำไว้เลย, มี Proof แต่ยาว

(area ไม่ติดลบ)

เครื่องหมายขึ้นอยู่กับค่า det

where the sign ($\pm$) is chosen to yield a positive area.

Finding the Area of a Triangle

Find the area of the triangle whose vertices are $(1, 0)$, $(2, 2)$, and $(4, 3)$.

$$A = \frac{1}{2}\begin{bmatrix} 1 & 0 & 1 \\ 2 & 2 & 1 \\ 4 & 3 & 1 \end{bmatrix}$$

$$= \frac{1}{2}\begin{vmatrix} 1 & 0 & 1 \\ 2 & 2 & 1 \\ 4 & 3 & 1 \end{vmatrix}\begin{matrix} 1 & 0 \\ 2 & 2 \\ 4 & 3 \end{matrix}$$

$$= \frac{1}{2}\left(\overset{-2}{\cancel{2+6-8}} \; -3\right)$$

$$= \frac{1}{2}(-3)$$

$$= \frac{-3}{2}$$

$$\text{Area} = \frac{3}{2} \; \#$$

Two-Point Form of the Equation of a Line

An equation of the line passing through the distinct points (x_1, y_1) and (x_2, y_2) is given by

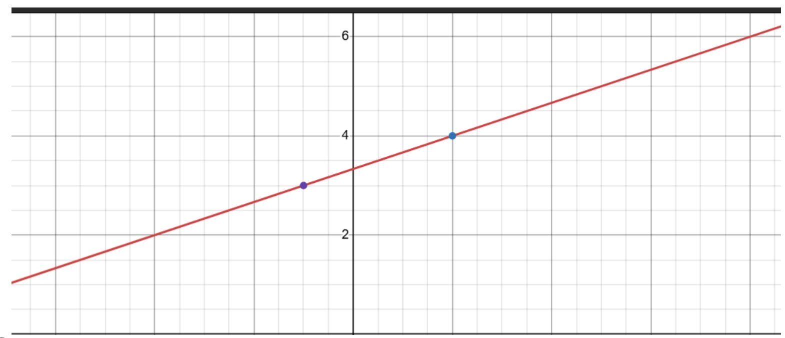
$$\det\begin{bmatrix} x & y & 1 \\ x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \end{bmatrix} = 0.$$

เอาไว้หาสมการเส้นตรงที่ 2 จุด

Finding an Equation of the Line Passing Through Two Points

Find an equation of the line passing through the points $(2, 4)$ and $(-1, 3)$.

$$\begin{vmatrix} x & y & 1 \\ 2 & 4 & 1 \\ -1 & 3 & 1 \end{vmatrix} = 0$$



$$\left|\begin{matrix} x & y & 1 \\ 2 & 4 & 1 \\ -1 & 3 & 1 \end{matrix}\right| \begin{matrix} x & y \\ 2 & 4 \\ -1 & 3 \end{matrix} = 0$$

$$x \ \cancel{4x} - y + 6 + 4 \ \cancel{-3x} - 2y = 0$$

$$x - 3y + 10 = 0 \ \checkmark$$

Volume of a Tetrahedron

- เตตระฮีดรอน ตรงกับภาษาอังกฤษว่า Tetrahedron (อ่านว่า tet-tra-he-dron) หมายถึงโครงสร้างปิระมิดฐานสามเหลี่ยม ซึ่งประกอบด้วย ด้าน (face) สามเหลี่ยม 4 ด้าน มุม (vertice) 4 มุม ขอบ (edge) 6 ขอบ เตตระฮีดรอนเป็นรูปทรงที่จัดอยู่ในประเภทพลาโทนิก (platonic)

The volume of the tetrahedron whose vertices are (x_1, y_1, z_1), (x_2, y_2, z_2), (x_3, y_3, z_3), and (x_4, y_4, z_4) is given by

$$\text{Volume} = \pm\frac{1}{6}\det\begin{bmatrix} x_1 & y_1 & z_1 & 1 \\ x_2 & y_2 & z_2 & 1 \\ x_3 & y_3 & z_3 & 1 \\ x_4 & y_4 & z_4 & 1 \end{bmatrix},$$

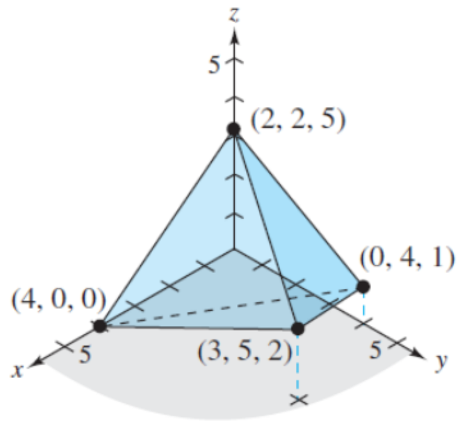
where the sign $(\pm)$ is chosen to yield a positive volume.

Finding the Volume of a Tetrahedron

Find the volume of the tetrahedron whose vertices are (0, 4, 1), (4, 0, 0), (3, 5, 2), and (2, 2, 5)

Final answer

≈ 72 (ลองหาดู)



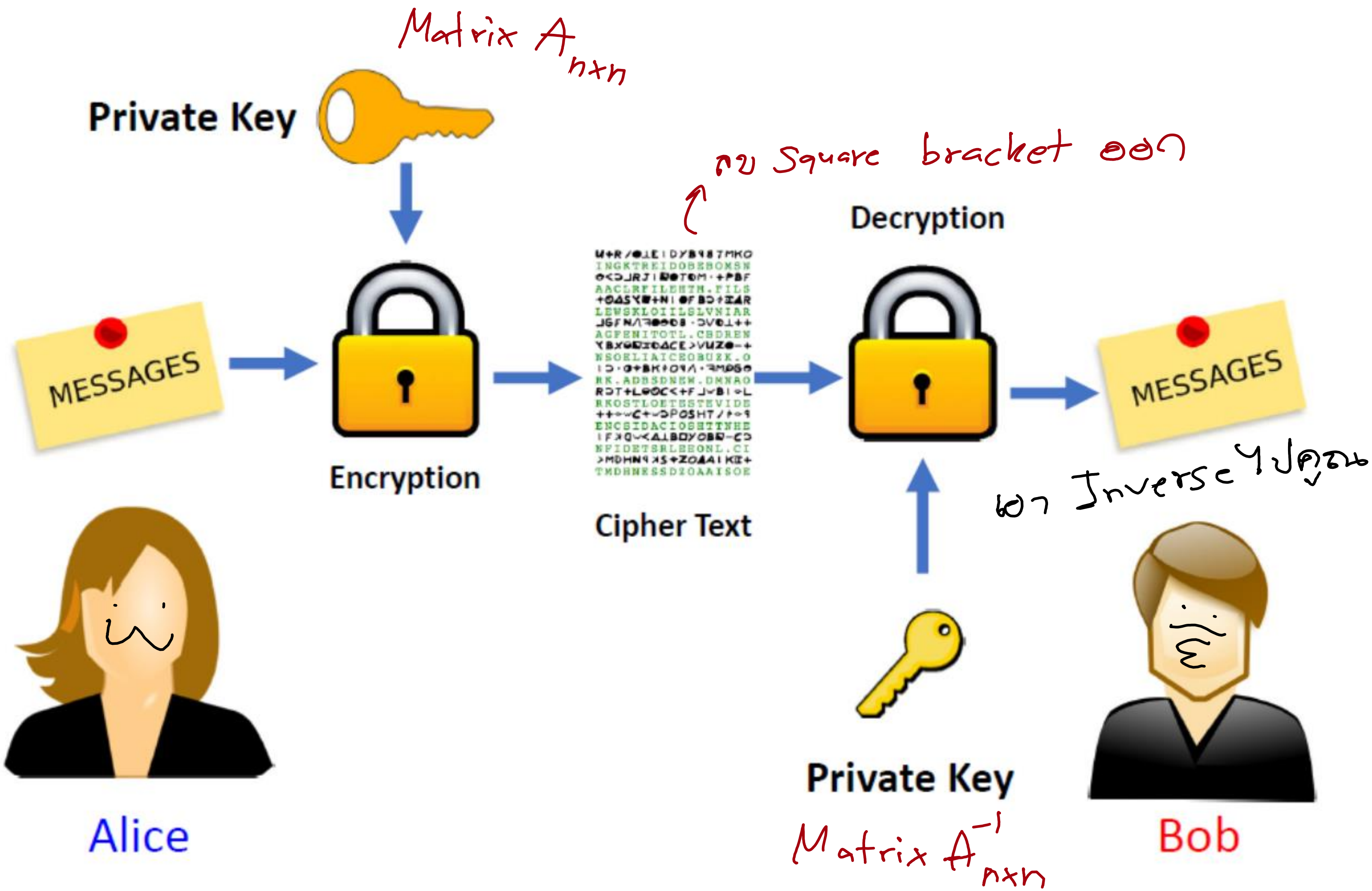
Applications of Matrix Operations

- Cryptography

Cryptography

- A **cryptogram** is a message written according to a secret code (the Greek word *kryptos* means "hidden").
- This section describes a method of using matrix multiplication to **encode** and **decode** messages.

Symmetric Cryptography



Cryptography (cont.)

MEET ME MONDAY

- Begin by assigning a number to each letter in the alphabet (with 0 assigned to a blank space), as follows.

space

0 = _	14 = N
1 = A	15 = O
2 = B	16 = P
3 = C	17 = Q
4 = D	18 = R
5 = E	19 = S
6 = F	20 = T
7 = G	21 = U
8 = H	22 = V
9 = I	23 = W
10 = J	24 = X
11 = K	25 = Y
12 = L	26 = Z
13 = M	

Encryption

$$\begin{array}{c}\begin{matrix}M & E & E\end{matrix}\\ \begin{bmatrix}13 & 5 & 5\end{bmatrix}\end{array}\begin{array}{c}\begin{matrix}T & \_ & M\end{matrix}\\ \begin{bmatrix}20 & 0 & 13\end{bmatrix}\end{array}\begin{array}{c}\begin{matrix}E & \_ & M\end{matrix}\\ \begin{bmatrix}5 & \_ & 13\end{bmatrix}\end{array}\begin{array}{c}\begin{matrix}O & N & D\end{matrix}\\ \begin{bmatrix}15 & 14 & 4\end{bmatrix}\end{array}\begin{array}{c}\begin{matrix}A & Y & O\end{matrix}\\ \begin{bmatrix}1 & 25 & 0\end{bmatrix}\end{array}$$

- Then the message is converted to numbers and partitioned into **uncoded row matrices**, each having *n* entries.

Forming Uncoded Row Matrices

Write the uncoded row matrices of size 1×3 for the message MEET ME MONDAY.

space นับด้วย

(0)

ถ้า Matrix ลงไม่ครบ
เติม 0 แทนไปได้เลย

Cryptography (cont.)

- To **encode** a message, choose an $n \times n$ invertible matrix A and multiply the uncoded row matrices (on the right) by A to obtain **coded row matrices.**

uncoded row matrices $\cdot A =$ coded row matrix

Encoding a Message

Use the matrix

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

to encode the message MEET ME MONDAY.

A is the Key

Uncoded 1×3 Matrix · Key matrix = Coded 1×3 matrix

Encryption

$$\begin{array}{ccc} M & E & E \\ \hline \end{array}\!\!\begin{bmatrix} 13 & 5 & 5 \end{bmatrix}
\begin{array}{ccc} T & _ & M \end{array}\!\!\begin{bmatrix} 20 & 0 & 13 \end{bmatrix}
\begin{array}{ccc} E & & M \end{array}\!\!\begin{bmatrix} 5 & 0 & 13 \end{bmatrix}
\begin{array}{ccc} O & N & D \end{array}\!\!\begin{bmatrix} 15 & 14 & 4 \end{bmatrix}
\begin{array}{ccc} A & Y & O \end{array}\!\!\begin{bmatrix} 1 & 25 & 0 \end{bmatrix}$$

Cryptography (cont.)

- For those who do not know the matrix *A*, decoding the cryptogram found in the previous example is difficult.
- But for an authorized receiver who knows the matrix *A*, decoding is simple.
- The receiver need only multiply the coded row matrices by A^{-1} to retrieve the uncoded row matrices.
- In other words, if

$$X = [x_1 \ \ x_2 \ \cdot \ \cdot \ \cdot \ \ x_n]$$

  is an uncoded 1 × *n* matrix, then *Y* = *XA* is the corresponding encoded matrix.
- The receiver of the encoded matrix can decode *Y* by multiplying on the right by A^{-1} to obtain

$$YA^{-1} = (XA)A^{-1} = X.$$

Decoding a Message

* Gauss-Jordan elimation

Use the inverse of the matrix

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

ดูขนาด A เท่าไหร่ แล้วแบ่งข้อความ

to decode the cryptogram

$$\underbrace{13 \quad -26 \quad 21}_{\cdot A^{-1}} \quad 33 \quad -53 \quad -12 \quad 18 \quad -23 \quad -42 \quad 5 \quad -20 \quad 56 \quad -24 \quad 23 \quad 77.$$

แล้วเอามาเรียงกันใหม่
จะได้ข้อความที่ถูก
decoded

encrypted message (Matrix) $\cdot A^{-1} \longrightarrow$ Decrypted Message Matrix

Decoding a Message (cont.)

Q & A