Chapter 8

Linear Algebra

"Algebra is generous; she often gives more than is asked of her."
(Jean D'Alembert)

This chapter is called linear algebra, but what we will really see is the definition of a matrix, a few basic properties of matrices, and how to compute (reduced) row echelon form, with its applications. There is much more to linear algebra!

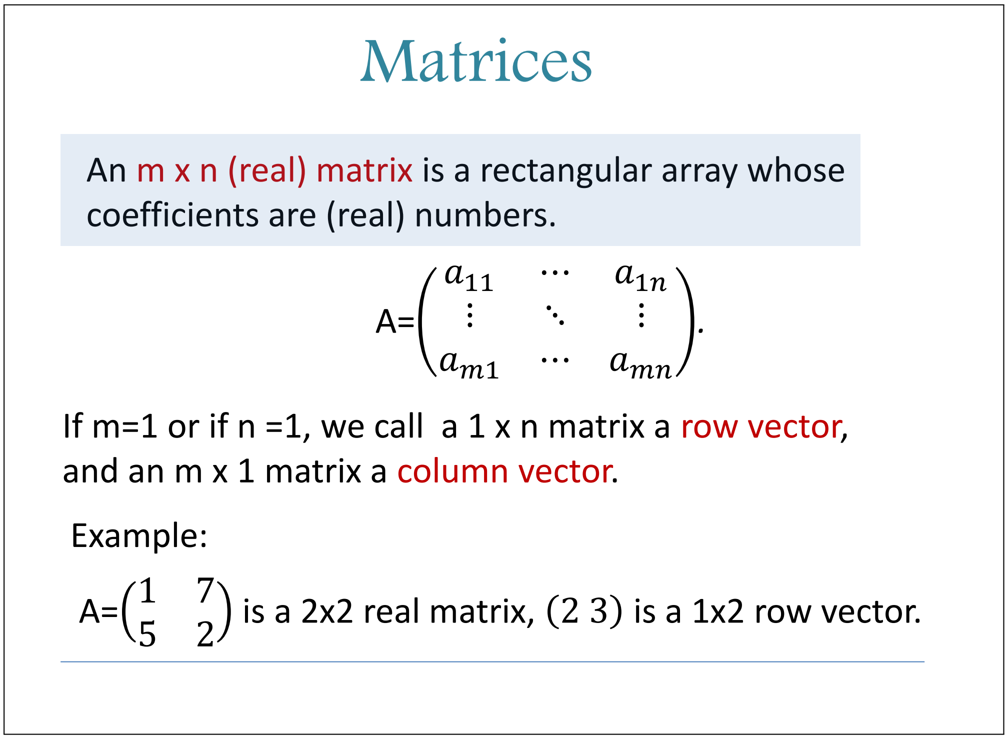
Let us start by defining a matrix.

Definition 42. A matrix is a rectangular array containing numbers, also called coefficients. We say that the matrix is an $m \times n$ matrix to specify that the array comprises m rows and n columns. If the matrix is called A, we usually write its coefficients as a_{ij}, where i tells us that this coefficient is on the ith row, and j that it is on the jth column:

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ a_{21} & \dots & a_{2n} \\ & \vdots & \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$$

Once the shape of the matrix is given, we need to specify where the coefficients belong to, namely whether they are real numbers, complex numbers, integer numbers. They could also be integers modulo n.

Definition 43. A $1 \times n$ matrix is called a row vector. An $m \times 1$ matrix is called a column vector.



Matrices

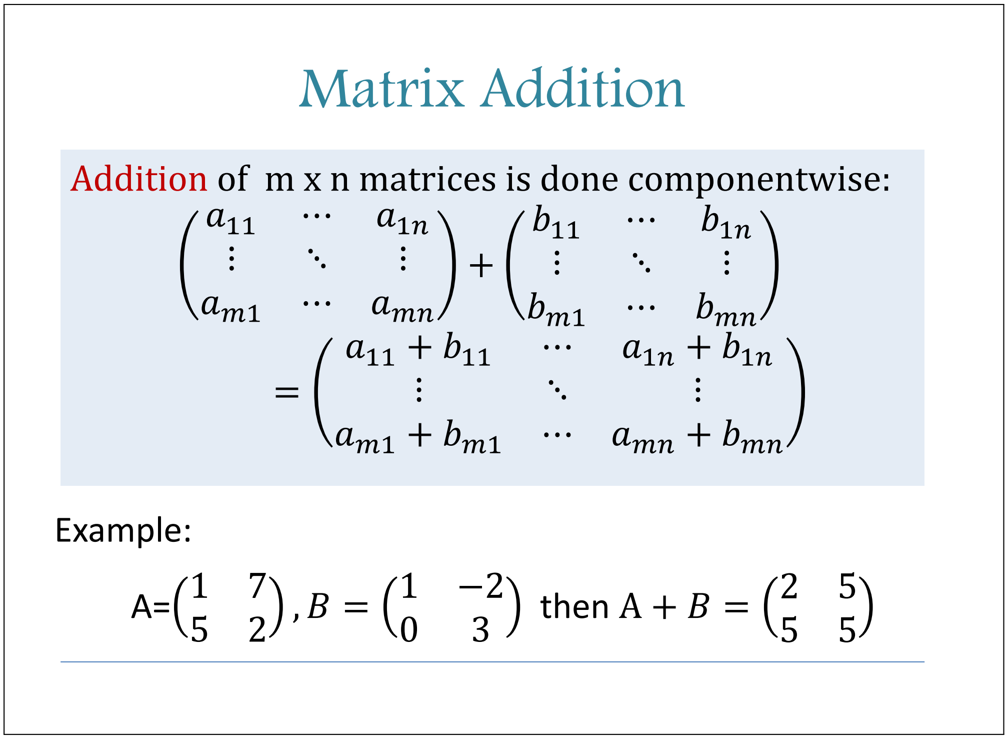
An m x n (real) matrix is a rectangular array whose coefficients are (real) numbers.

$$A=\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}.$$

If m=1 or if n =1, we call a 1 x n matrix a row vector, and an m x 1 matrix a column vector.

Example:

$A=\begin{pmatrix} 1 & 7 \\ 5 & 2 \end{pmatrix}$ is a 2x2 real matrix, $(2\ 3)$ is a 1x2 row vector.



Matrix Addition

Addition of m x n matrices is done componentwise:

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} + \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{m1} & \cdots & b_{mn} \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11} & \cdots & a_{1n}+b_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1}+b_{m1} & \cdots & a_{mn}+b_{mn} \end{pmatrix}$$

Example:

$A=\begin{pmatrix} 1 & 7 \\ 5 & 2 \end{pmatrix}, B = \begin{pmatrix} 1 & -2 \\ 0 & 3 \end{pmatrix}$ then $A + B = \begin{pmatrix} 2 & 5 \\ 5 & 5 \end{pmatrix}$

Example 69. The matrix

$$A = \begin{pmatrix} 1 & 7 \\ 5 & 2 \end{pmatrix}$$

is a 2×2 matrix with real coefficients, while $(2, 3)$ is a 1×2 row vector.

We are of course interested in performing operations on matrices. The easiest one is probably **matrix addition**. For this, we need two matrices A and B both with the same number of rows and columns, say, both of them are $n \times m$ matrices:

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ a_{21} & \dots & a_{2n} \\ & \vdots & \\ a_{m1} & \dots & a_{mn} \end{pmatrix}, \; B = \begin{pmatrix} b_{11} & \dots & b_{1n} \\ b_{21} & \dots & b_{2n} \\ & \vdots & \\ b_{m1} & \dots & b_{mn} \end{pmatrix}.$$

Then $A + B$ is computed componentwise, namely

$$A{+}B = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ a_{21} & \dots & a_{2n} \\ & \vdots & \\ a_{m1} & \dots & a_{mn} \end{pmatrix} + \begin{pmatrix} b_{11} & \dots & b_{1n} \\ b_{21} & \dots & b_{2n} \\ & \vdots & \\ b_{m1} & \dots & b_{mn} \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11} & \dots & a_{1n}+b_{1n} \\ a_{21}+b_{21} & \dots & a_{2n}+b_{2n} \\ & \vdots & \\ a_{m1}+b_{m1} & \dots & a_{mn}+b_{mn} \end{pmatrix}$$

Example 70. Consider the following two matrices:

$$A = \begin{pmatrix} 1 & 7 \\ 5 & 2 \end{pmatrix}, \; B = \begin{pmatrix} 1 & -2 \\ 0 & 3 \end{pmatrix}$$

Then

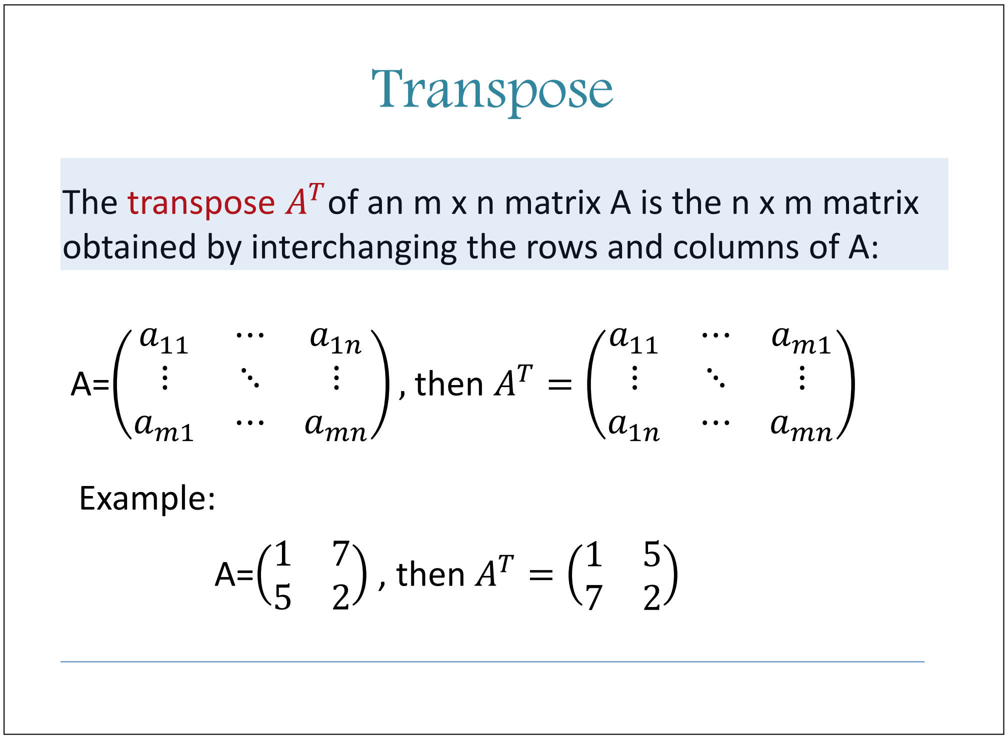
$$A + B = \begin{pmatrix} 1 & 7 \\ 5 & 2 \end{pmatrix} + \begin{pmatrix} 1 & -2 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} 1+1 & 7-2 \\ 5 & 2+3 \end{pmatrix} = \begin{pmatrix} 2 & 5 \\ 5 & 5 \end{pmatrix}.$$

Definition 44. Given an $m \times n$ matrix A its transpose matrix A^T is an $n \times m$ matrix obtaining by interchanging the rows and columns of A:

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ a_{21} & \dots & a_{2n} \\ & \vdots & \\ a_{m1} & \dots & a_{mn} \end{pmatrix}, \; A^T = \begin{pmatrix} a_{11} & \dots & a_{m1} \\ a_{12} & \dots & a_{m2} \\ & \vdots & \\ a_{1n} & \dots & a_{mn} \end{pmatrix}$$

Example 71.

$$A = \begin{pmatrix} 1 & 7 \\ 5 & 2 \end{pmatrix}, \; A^T = \begin{pmatrix} 1 & 5 \\ 7 & 2 \end{pmatrix}.$$



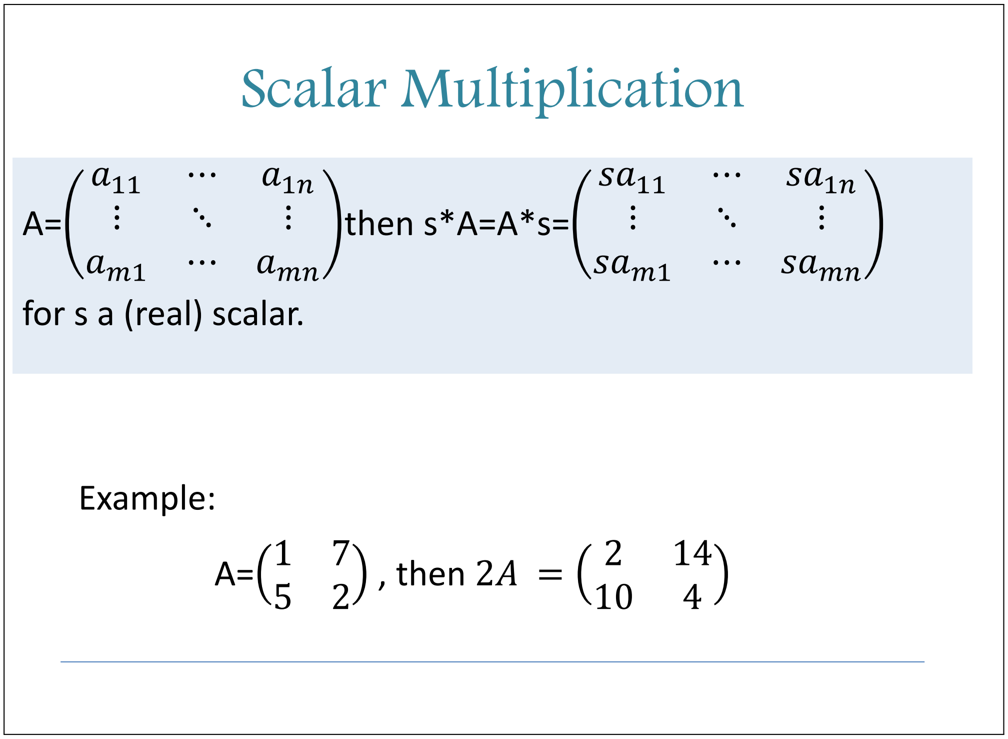
Transpose

The transpose A^T of an m x n matrix A is the n x m matrix obtained by interchanging the rows and columns of A:

A=$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$, then $A^T = \begin{pmatrix} a_{11} & \cdots & a_{m1} \\ \vdots & \ddots & \vdots \\ a_{1n} & \cdots & a_{mn} \end{pmatrix}$

Example:

A=$\begin{pmatrix} 1 & 7 \\ 5 & 2 \end{pmatrix}$, then $A^T = \begin{pmatrix} 1 & 5 \\ 7 & 2 \end{pmatrix}$



Scalar Multiplication

A=$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$then s*A=A*s=$\begin{pmatrix} sa_{11} & \cdots & sa_{1n} \\ \vdots & \ddots & \vdots \\ sa_{m1} & \cdots & sa_{mn} \end{pmatrix}$

for s a (real) scalar.

Example:

A=$\begin{pmatrix} 1 & 7 \\ 5 & 2 \end{pmatrix}$, then $2A = \begin{pmatrix} 2 & 14 \\ 10 & 4 \end{pmatrix}$

The next matrix operation is **scalar multiplication**. The term scalar refers to a 1 × 1 matrix. We have that an $n \times m$ matrix A multiplied by a scalar s is defined componentwise, namely:

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ a_{21} & \dots & a_{2n} \\ & \vdots & \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \Rightarrow sA = \begin{pmatrix} sa_{11} & \dots & sa_{1n} \\ sa_{21} & \dots & sa_{2n} \\ & \vdots & \\ sa_{m1} & \dots & sa_{mn} \end{pmatrix}.$$

Example 72.

$$A = \begin{pmatrix} 1 & 7 \\ 5 & 2 \end{pmatrix},\ 2A = \begin{pmatrix} 2 & 10 \\ 14 & 4 \end{pmatrix}.$$

We next recall the definition of scalar product, which will be needed to defined matrix multiplication. The term "scalar product" reflects the fact that we perform a "product", and that the result is a "scalar", so it is an operation that takes two vectors, and results in a 1 × 1 matrix.

Definition 45. The scalar product of a $1 \times n$ vector v with an $n \times 1$ column vector w is

$$v \cdot w = (v_1, \dots, v_n) \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix} = \sum_{i=1}^{n} v_i w_i.$$

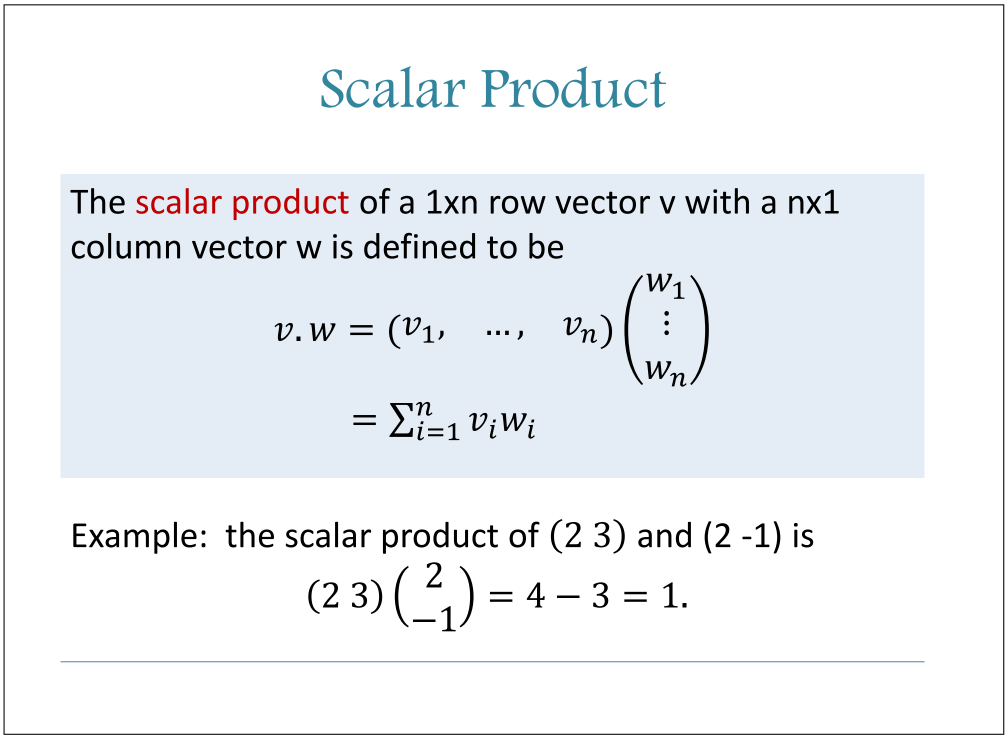
Sometimes, we may say the scalar product of v and w without specifying whether v and w are row or columns vectors, but for the scalar product to be valid, one need to be row and the other column. Note that $v \cdot w = w \cdot v$.

Example 73. The scalar product of $(2, 3)$ and $(2, -1)$ is

$$(2,3)\begin{pmatrix} 2 \\ -1 \end{pmatrix} = 2 \cdot 2 - 3 = 1.$$

We are now ready to define the **multiplication of two matrices** A and B, where A is an $m \times n$ matrix, and B is an $n \times r$ matrix. Then for

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ a_{21} & \dots & a_{2n} \\ & \vdots & \\ a_{m1} & \dots & a_{mn} \end{pmatrix},\ B = \begin{pmatrix} b_{11} & \dots & b_{1r} \\ b_{21} & \dots & b_{2r} \\ & \vdots & \\ b_{n1} & \dots & b_{nr} \end{pmatrix}$$



Scalar Product

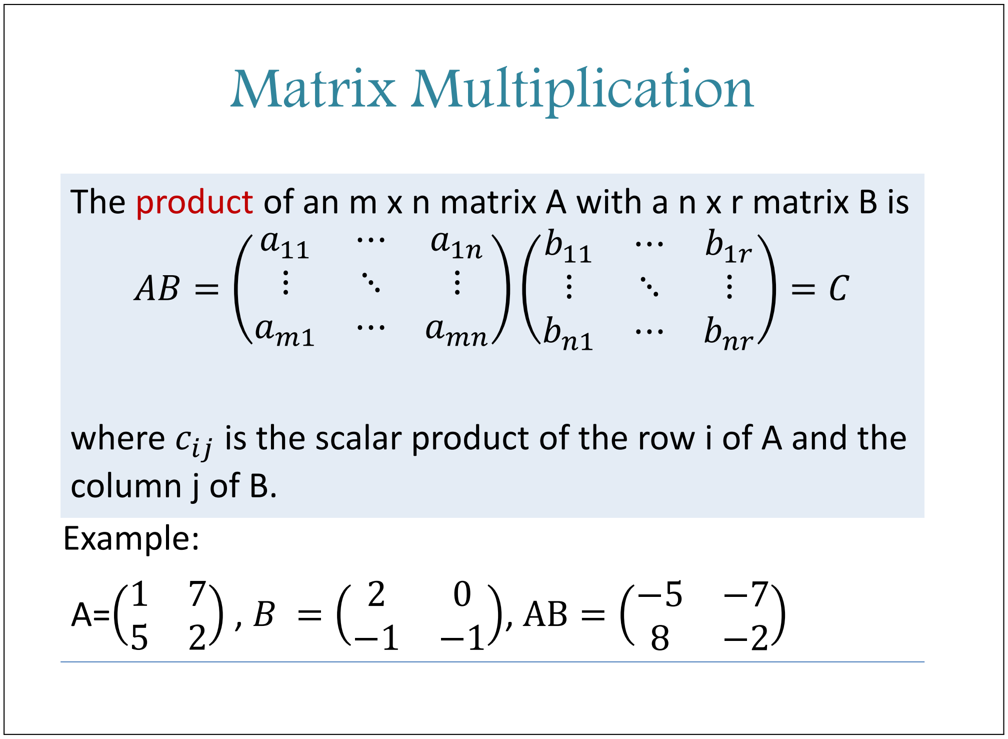
The scalar product of a 1xn row vector v with a nx1 column vector w is defined to be

$$v.w = (v_1, \quad \dots, \quad v_n)\begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix}$$

$$= \sum_{i=1}^{n} v_i w_i$$

Example: the scalar product of (2 3) and (2 -1) is

$$(2\ 3)\begin{pmatrix} 2 \\ -1 \end{pmatrix} = 4 - 3 = 1.$$



Matrix Multiplication

The product of an m x n matrix A with a n x r matrix B is

$$AB = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}\begin{pmatrix} b_{11} & \cdots & b_{1r} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nr} \end{pmatrix} = C$$

where c_{ij} is the scalar product of the row i of A and the column j of B.

Example:

A=$\begin{pmatrix} 1 & 7 \\ 5 & 2 \end{pmatrix}$, $B = \begin{pmatrix} 2 & 0 \\ -1 & -1 \end{pmatrix}$, AB $= \begin{pmatrix} -5 & -7 \\ 8 & -2 \end{pmatrix}$

we have $AB = C$, where c_{ij} is the scalar product of the row i of A and the column j of B. Note that typically $AB \neq BA$, therefore the ordering of the multiplication is very important! Furthermore, dimensions must be compatible for multiplication, namely to compute AB, we need the number of columns of A to be equal to the number of rows of B.

Example 74.

$$A = \begin{pmatrix} 1 & 7 \\ 5 & 2 \end{pmatrix}, \; B = \begin{pmatrix} 2 & 0 \\ -1 & -1 \end{pmatrix}.$$

Then

$$AB = C$$

where

$$c_{11} = (1,7)\begin{pmatrix} 2 \\ -1 \end{pmatrix} = -5, \; c_{12} = (1,7)\begin{pmatrix} 0 \\ -1 \end{pmatrix} = -7,$$

and

$$c_{21} = (5,2)\begin{pmatrix} 2 \\ -1 \end{pmatrix} = 8, \; c_{22} = (5,2)\begin{pmatrix} 0 \\ -1 \end{pmatrix} = -2.$$

Some matrices have a special shape, this is the case of diagonal matrices.

Definition 46. An $n \times n$ matrix A is said to be diagonal if its coefficients a_{ij} are 0 whenever $i \neq j$.

Example 75. The matrix

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -3 \end{pmatrix}$$

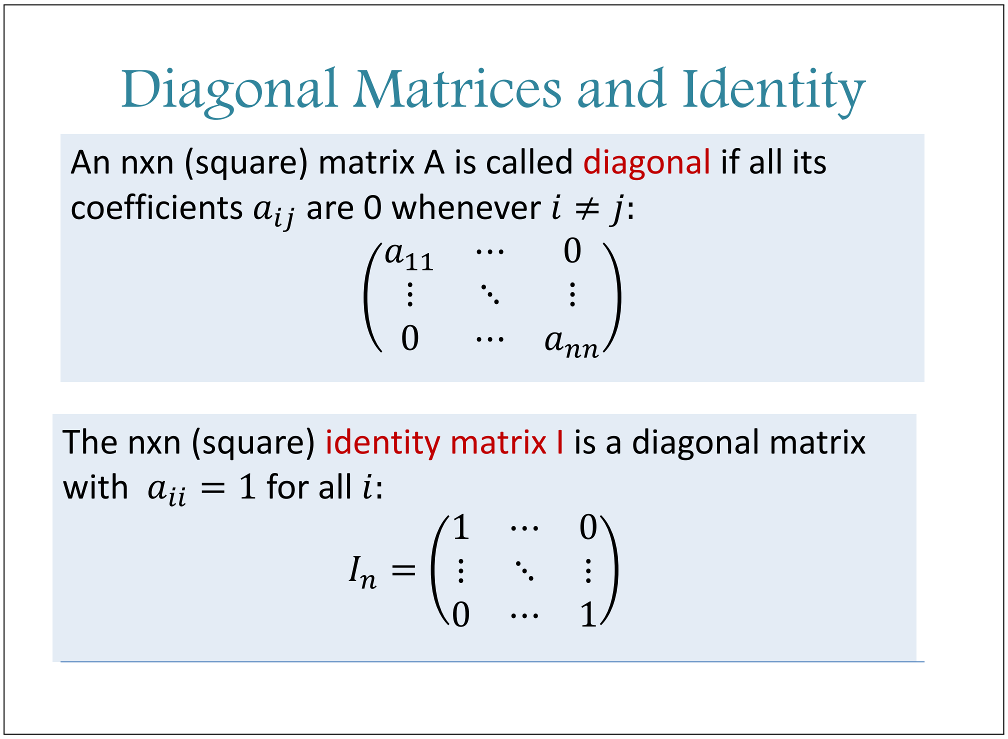
is diagonal.

The matrix identity is a special type of diagonal matrix.

Definition 47. The n-dimensional identity matrix I_n is a diagonal matrix whose diagonal coefficients are all 1.

Example 76. The identity matrix I_3 is

$$I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$



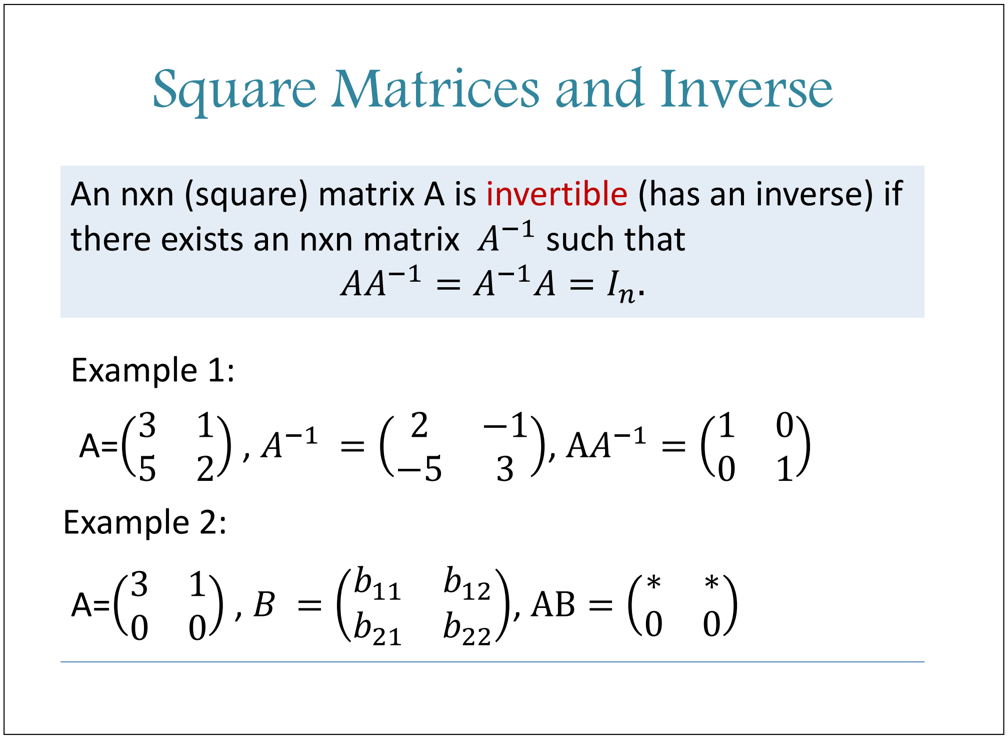
Diagonal Matrices and Identity

An nxn (square) matrix A is called diagonal if all its coefficients a_{ij} are 0 whenever $i \neq j$:

$$\begin{pmatrix} a_{11} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_{nn} \end{pmatrix}$$

The nxn (square) identity matrix I is a diagonal matrix with $a_{ii} = 1$ for all i:

$$I_n = \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix}$$



Square Matrices and Inverse

An nxn (square) matrix A is invertible (has an inverse) if there exists an nxn matrix A^{-1} such that

$$AA^{-1} = A^{-1}A = I_n.$$

Example 1:

A=$\begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix}$, $A^{-1} = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix}$, $AA^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Example 2:

A=$\begin{pmatrix} 3 & 1 \\ 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$, AB $= \begin{pmatrix} * & * \\ 0 & 0 \end{pmatrix}$

Thanks to the definition of identity matrix, we may introduce that of inverse of a matrix. For a real scalar, we say that the inverse of x when $x \neq 0$ is x^{-1}, and x^{-1} is such that $xx^{-1} = 1$. The identity matrix plays the role of 1 for matrices.

Definition 48. An $n \times n$ matrix A is invertible if there exists a matrix A^{-1} such that $AA^{-1} = A^{-1}A = I_n$. The matrix A^{-1} is called the inverse of A.

The definition mentions that multiplication of A by its inverse both on the right and on the left must give I_n. In practice, we will typically show only one of the two, the reason being that it can be proven that for a square matrix (square means that the number of rows is the same at the number of columns), the existence of an inverse on one side actually implies that of an inverse on the other side, and both of them are the same.

For real numbers x, as recalled above, only when $x = 0$ it is not possible to compute x^{-1}. For matrices, many of them are not invertible!

Example 77. The matrix

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

is invertible, because its inverse A^{-1} is

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

Indeed, one may check that $AA^{-1} = I_2$, or $A^{-1}A = I_2$. On the other hand

$$A = \begin{pmatrix} 3 & 1 \\ 0 & 0 \end{pmatrix}$$

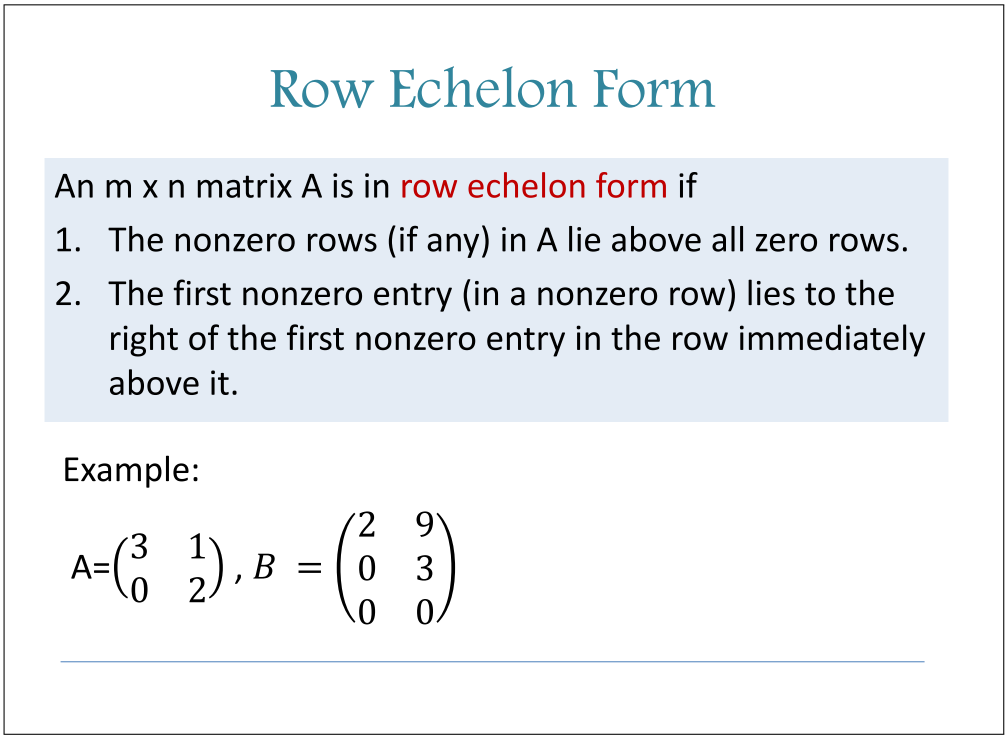
has no inverse. No matter which matrix B one takes, AB will always have a row of zeroes, and cannot possibly be equal to the identity matrix.

In the above example, A^{-1} is given and one can just check that AA^{1-} is indeed I_2. We next see a general technique, which among other things allows to compute the inverse of a matrix.

Definition 49. An $m \times n$ matrix A is in row echelon form if

1. The nonzero rows (if any) in A lie above all zero rows.

2. The first nonzero entry (in a nonzero row) lies to the right of the first nonzero entry in the row immediately above it.



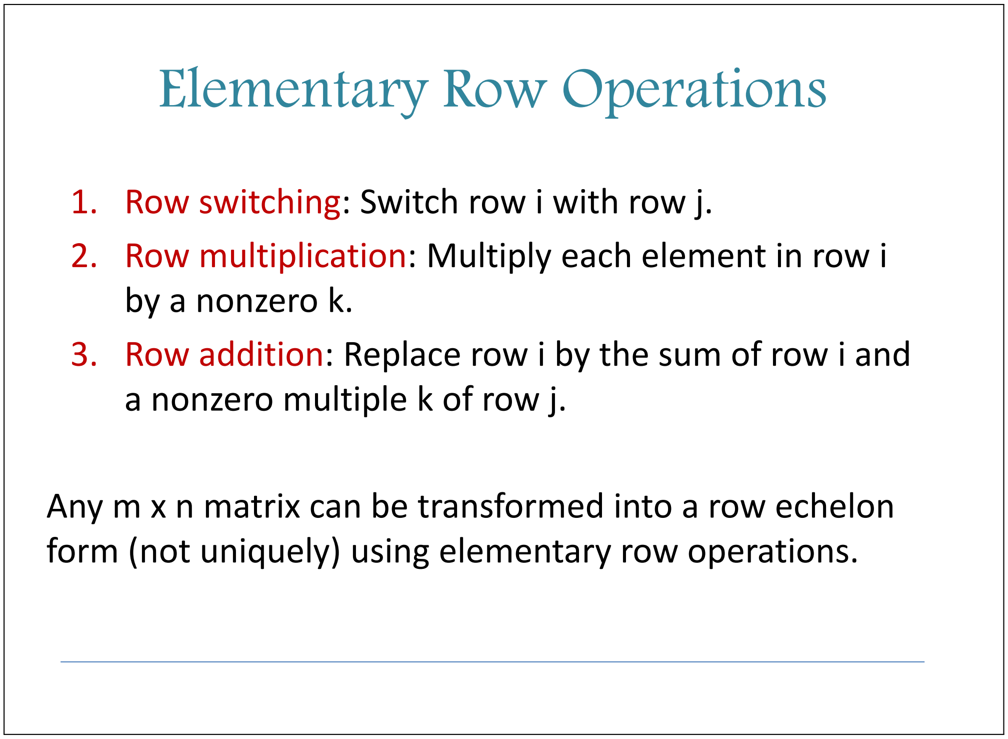
Row Echelon Form

An m x n matrix A is in row echelon form if

1. The nonzero rows (if any) in A lie above all zero rows.
2. The first nonzero entry (in a nonzero row) lies to the right of the first nonzero entry in the row immediately above it.

Example:

A=$\begin{pmatrix}3 & 1\\ 0 & 2\end{pmatrix}$, $B = \begin{pmatrix}2 & 9\\ 0 & 3\\ 0 & 0\end{pmatrix}$



Elementary Row Operations

1. Row switching: Switch row i with row j.
2. Row multiplication: Multiply each element in row i by a nonzero k.
3. Row addition: Replace row i by the sum of row i and a nonzero multiple k of row j.

Any m x n matrix can be transformed into a row echelon form (not uniquely) using elementary row operations.

Example 78. The matrices

$$A=\begin{pmatrix}3 & 1\\ 0 & 2\end{pmatrix},\ B=\begin{pmatrix}2 & 9\\ 0 & 3\\ 0 & 0\end{pmatrix}$$

are in row echelon form.

Now a matrix is not necessarily in row echelon form. However, there is a series of operations which we are allowed to do on a matrix, to bring it into such a form. These operations are called elementary row operations, and comprise:

1. **Row switching**: switch row i with row j.
2. **Row multiplication**: multiply each element in row i by a nonzero k. Note that k can be of the form $1/k'$, $k'\neq 0$, therefore division is allowed as well.
3. **Row addition**: replace row i by the sum of row i and a nonzero multiple k of row j.

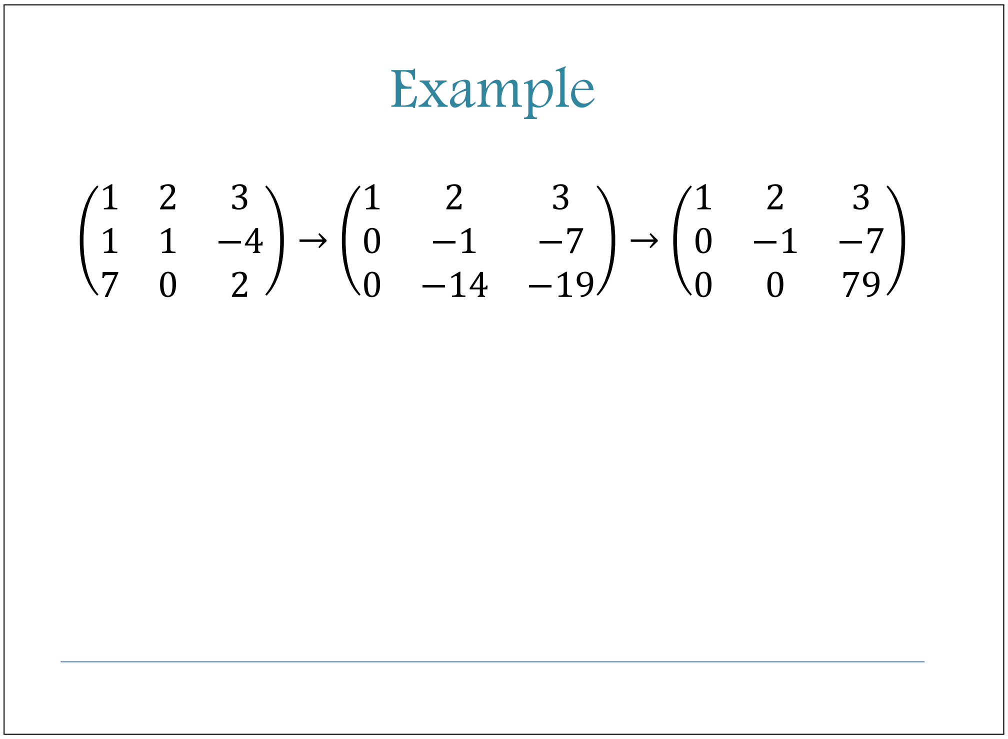
Note that it is always possible to bring a matrix into a row echelon form. Roughly, this is because either a column contains only zeroes, or only zeroes and one non-zero entry, in which case it is fine. If it contains two non-zero entries, then one can be used to cancel out the other one using elementary row operations.

Example 79. Consider the matrix

$$\begin{pmatrix}1 & 2 & 3\\ 1 & 1 & -4\\ 7 & 0 & 2\end{pmatrix}.$$

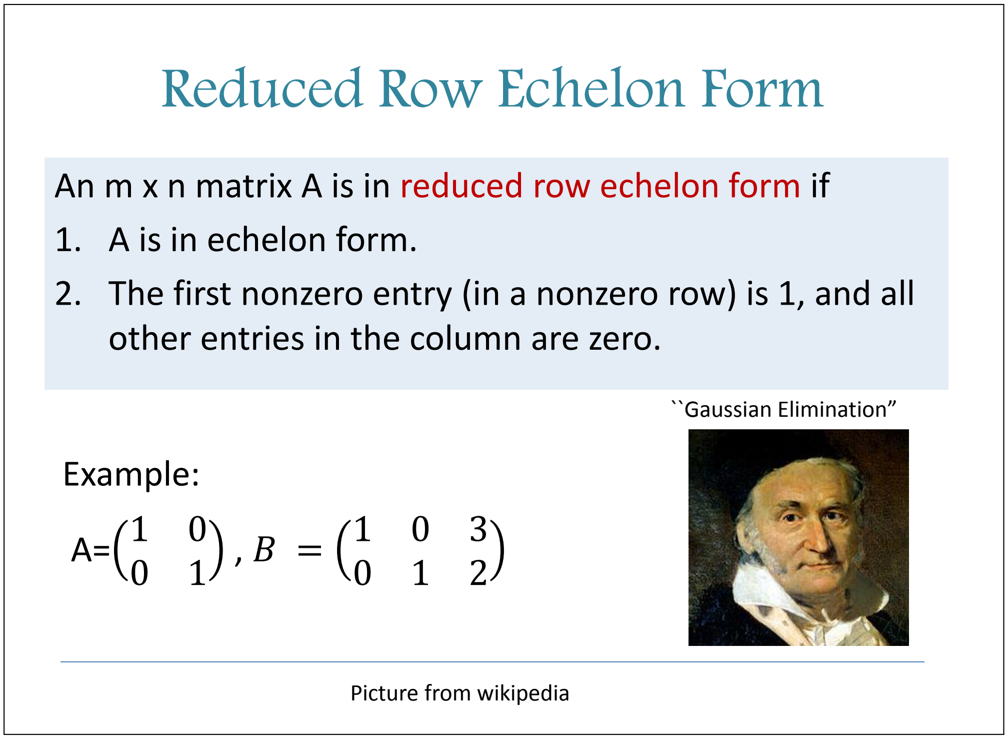
To obtain its row echelon form, we first take care of the first column. For this we replace (row 2) by (row 2)- (row 1), and then we replace (row 3) by (row 3) -7 (row 1), to get

$$\begin{pmatrix}1 & 2 & 3\\ 0 & -1 & -7\\ 0 & -14 & -19\end{pmatrix}.$$



Example

$$\begin{pmatrix}1 & 2 & 3\\ 1 & 1 & -4\\ 7 & 0 & 2\end{pmatrix} \rightarrow \begin{pmatrix}1 & 2 & 3\\ 0 & -1 & -7\\ 0 & -14 & -19\end{pmatrix} \rightarrow \begin{pmatrix}1 & 2 & 3\\ 0 & -1 & -7\\ 0 & 0 & 79\end{pmatrix}$$



Reduced Row Echelon Form

An m x n matrix A is in reduced row echelon form if

1. A is in echelon form.
2. The first nonzero entry (in a nonzero row) is 1, and all other entries in the column are zero.

``Gaussian Elimination”

Example:

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

Picture from wikipedia

The only step missing now is to change the second column, which is done by replacing (row 3) by (row 3)-14(row 2):

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & -1 & -7 \\ 0 & 0 & 79 \end{pmatrix}.$$

The row echelon form of a matrix is not unique, this can be seen by the fact that one is allowed to multiply a row by a non-zero constant. For example, the above matrix has last row $(0, 0, 79)$, any multiple of this row would also give a row echelon form.

One may however further reduce a matrix into what is a called a reduced echelon form, in which case it becomes unique. This procedure is also called Gaussian elimination.

Definition 50. An $m \times n$ matrix A is in reduced row echelon form if

1. A is in echelon form.
2. The first nonzero entry (in a nonzero row) is 1, and all other entries in the column are zero.

Example 80. We continue Example 79, with the matrix

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & -4 \\ 7 & 0 & 2 \end{pmatrix}$$

which has row echelon form

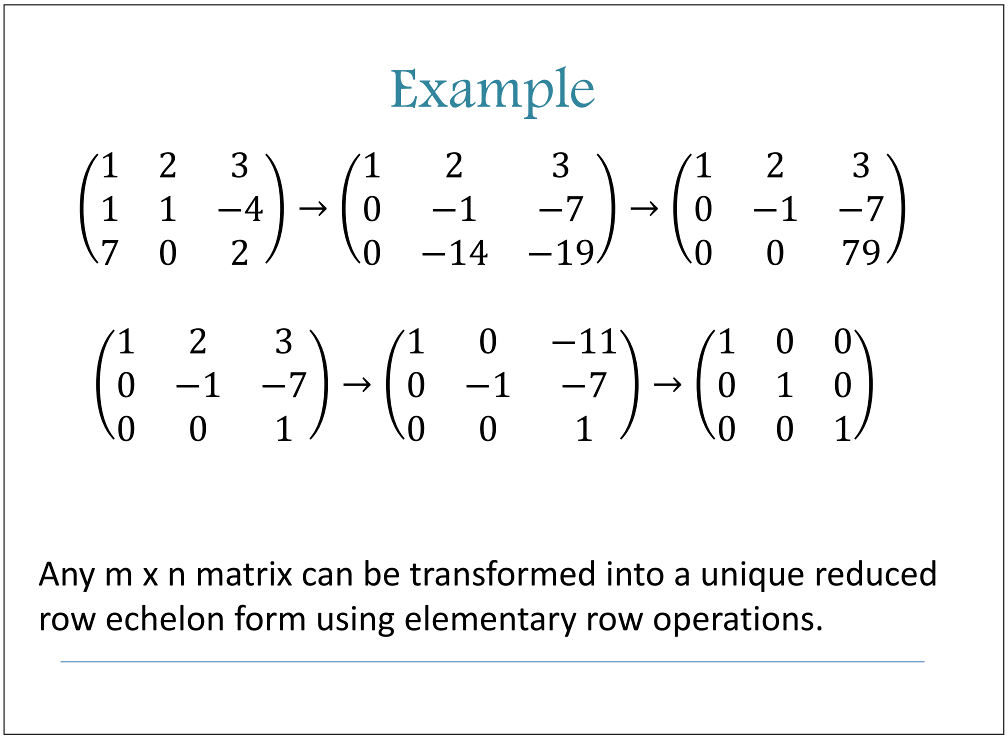
$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & -1 & -7 \\ 0 & 0 & 79 \end{pmatrix}.$$

We first divide the last row by 79, and add 2(row 2) to the first row:

$$\begin{pmatrix} 1 & 0 & -11 \\ 0 & -1 & -7 \\ 0 & 0 & 1 \end{pmatrix}.$$

We are left to add 11(row 3) to the first row, 7(row 3) to the second row, and multiply the second row by -1, to get I_3.

It may look surprising to find the identity matrix at the end, but this happens in fact whenever the matrix A we started with is invertible.

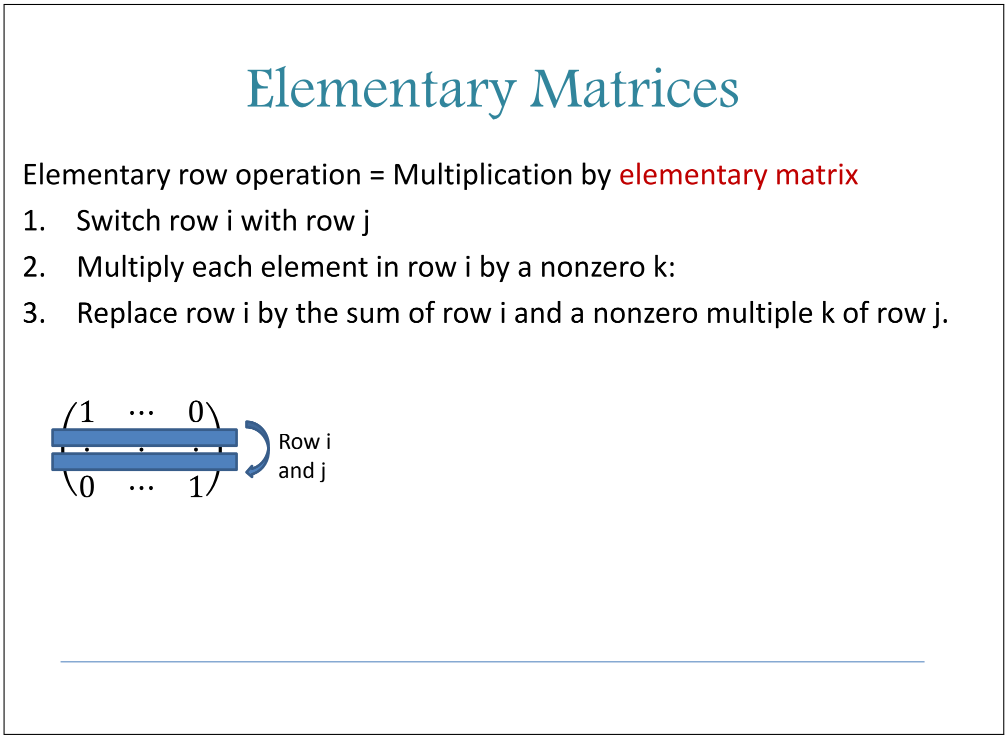


Example

$$\begin{pmatrix}1 & 2 & 3\\ 1 & 1 & -4\\ 7 & 0 & 2\end{pmatrix} \to \begin{pmatrix}1 & 2 & 3\\ 0 & -1 & -7\\ 0 & -14 & -19\end{pmatrix} \to \begin{pmatrix}1 & 2 & 3\\ 0 & -1 & -7\\ 0 & 0 & 79\end{pmatrix}$$

$$\begin{pmatrix}1 & 2 & 3\\ 0 & -1 & -7\\ 0 & 0 & 1\end{pmatrix} \to \begin{pmatrix}1 & 0 & -11\\ 0 & -1 & -7\\ 0 & 0 & 1\end{pmatrix} \to \begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}$$

Any m x n matrix can be transformed into a unique reduced row echelon form using elementary row operations.



Elementary Matrices

Elementary row operation = Multiplication by elementary matrix

1. Switch row i with row j
2. Multiply each element in row i by a nonzero k:
3. Replace row i by the sum of row i and a nonzero multiple k of row j.

$$\begin{pmatrix}1 & \cdots & 0\\ \vdots & \ddots & \vdots\\ 0 & \cdots & 1\end{pmatrix}$$

Row i and j

Let us try to understand why, which will also give us an algorithm to find the inverse of a matrix. First of all, we notice that all the elementary operations used for obtaining a row echelon form can be expressed by matrices, which are called elementary matrices.

1. **Row switching**: row i with row j are switched if the matrix is multiplied by a matrix obtained from the identity matrix by switching its row i with its row j.

2. **Row multiplication**: multiply each element in row i by a nonzero k. This is done by multiplication by a diagonal matrix, where all diagonal coefficients are 1 but for the ith row which contains a k.

3. **Row addition**: replace row i by the sum of row i and a nonzero multiple k of row j. This is done by using a matrix which has 1 on the diagonal, except for the row i, which further contains a k in the jth column.

Now take a matrix A, and suppose that it is invertible, in particular it is square, that is A is an $n \times n$ matrix. Once the matrix is in row echelon form, only two things can happen: either all the diagonal coefficients are non-zero, in which case the reduced form will give the identity matrix, or at least one row is a whole zero row. This really results from the fact the the number of rows and columns are the same. Next form an augmented matrix, which contains A and I_n, namely $(A|I_n)$. Multiply the matrix on the left with elementary matrices, say $M_1, \ldots, M_l$, to get a reduced row echelon form of A:

$$M_l M_{l-1} \cdots M_2 M_1 (A|I_n).$$

Now if A is invertible $M_l M_{l-1} \cdots M_2 M_1 \cdot A = I_n$, therefore $M_l M_{l-1} \cdots M_2 M_1 = A^{-1}$ and

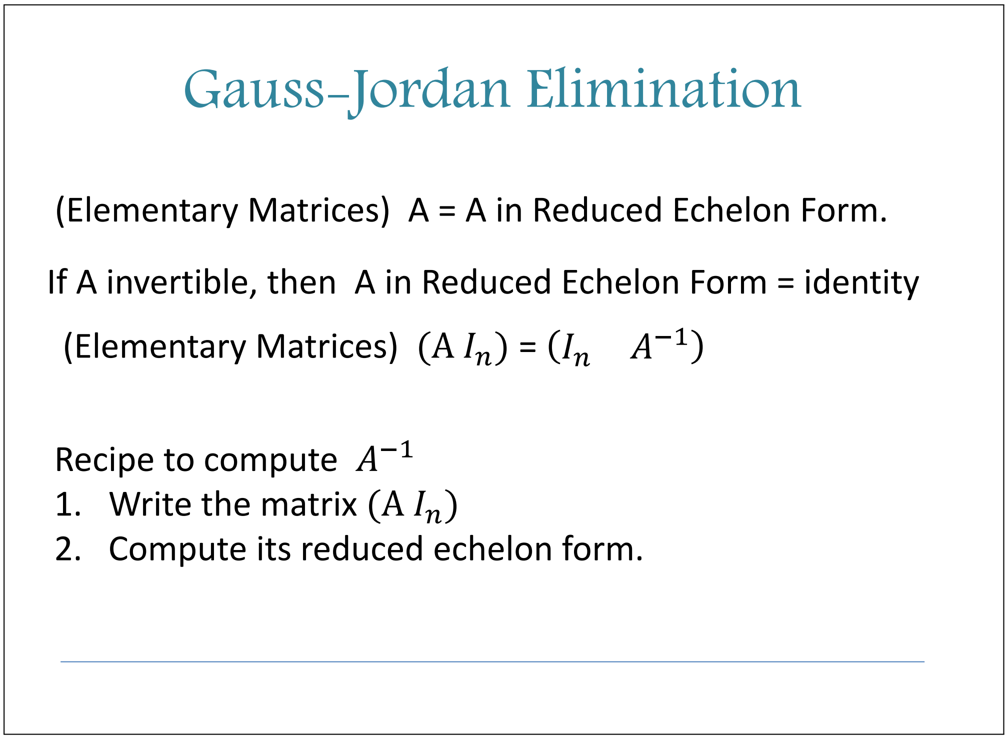
$$M_l M_{l-1} \cdots M_2 M_1 (A|I_n) = (I_n|A^{-1}).$$

If multiplication by elementary matrices result in a matrix with at least one row which is zero, then it is impossssible to obtain the identity matrix on the left hand side of $(A|I_n)$ and the matrix cannot be invertible.

Recipe to compute the inverse of a matrix A.

1. Write the augmented matrix $(A|I_n)$.

2. Compute its reduced row echelon form, to obtain $(I_n|A^{-1})$



Gauss-Jordan Elimination

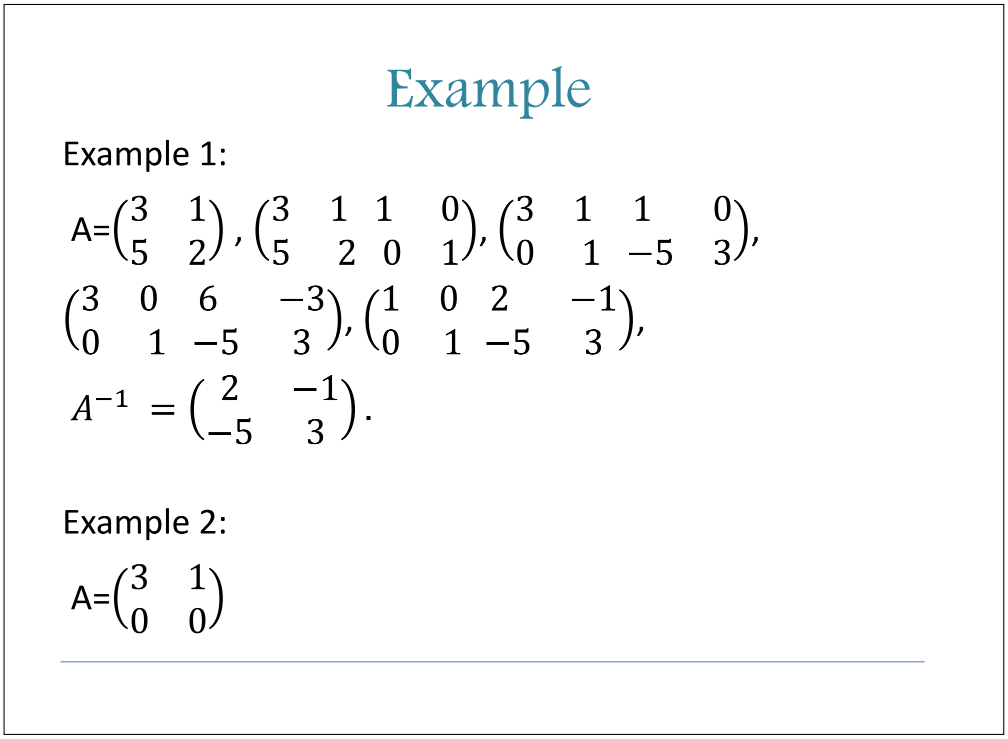
(Elementary Matrices) A = A in Reduced Echelon Form.

If A invertible, then A in Reduced Echelon Form = identity

(Elementary Matrices) $(\mathrm{A}\, I_n)$ = $(I_n \quad A^{-1})$

Recipe to compute A^{-1}

1. Write the matrix $(\mathrm{A}\, I_n)$
2. Compute its reduced echelon form.



Example

Example 1:

A=$\begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix}$, $\begin{pmatrix} 3 & 1 & 1 & 0 \\ 5 & 2 & 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 3 & 1 & 1 & 0 \\ 0 & 1 & -5 & 3 \end{pmatrix}$,
$\begin{pmatrix} 3 & 0 & 6 & -3 \\ 0 & 1 & -5 & 3 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 & 2 & -1 \\ 0 & 1 & -5 & 3 \end{pmatrix}$,
$A^{-1} = \begin{pmatrix} 2 & -1 \\ -5 & 3 \end{pmatrix}$.

Example 2:

A=$\begin{pmatrix} 3 & 1 \\ 0 & 0 \end{pmatrix}$

Example 81. Consider the matrix

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

To compute its inverse, create the augmented matrix:

$$A = \begin{pmatrix} 3 & 1 & 1 & 0 \\ 5 & 2 & 0 & 1 \end{pmatrix}$$

To obtain a row echelon form, replace (row 2) by -5(row 1)+3(row 2), which in matrix form is given by

$$\begin{pmatrix} 1 & 0 \\ -5 & 3 \end{pmatrix} \begin{pmatrix} 3 & 1 & 1 & 0 \\ 5 & 2 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 1 & 1 & 0 \\ 0 & 1 & -5 & 3 \end{pmatrix}$$

and we can tell that the matrix is invertible. Then replace (row 1) by (row 1)-(row 2):

$$\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -5 & 3 \end{pmatrix} \begin{pmatrix} 3 & 1 & 1 & 0 \\ 5 & 2 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 3 & 1 & 1 & 0 \\ 0 & 1 & -5 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 0 & -6 & -3 \\ 0 & 1 & -5 & 3 \end{pmatrix}$$

and we are left by dividing the first row by 3:

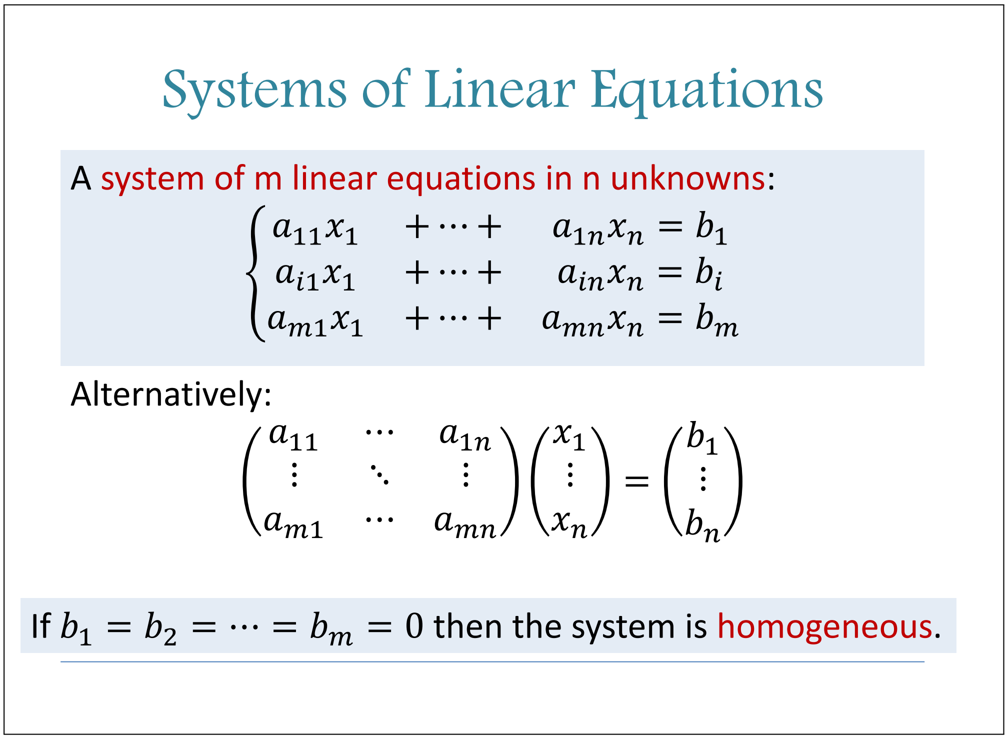
$$\begin{pmatrix} 1/3 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -5 & 3 \end{pmatrix} \begin{pmatrix} 3 & 1 & 1 & 0 \\ 5 & 2 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & -2 & -1 \\ 0 & 1 & -5 & 3 \end{pmatrix}.$$

Another application of the (reduced) row echelon form is solving systems of linear equations.

Definition 51. A system of m linear equations in n unknowns is of the form:

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n & = & b_1 \\ \vdots & & \\ a_{i1}x_1 + \ldots + a_{in}x_n & = & b_i \\ \vdots & & \\ a_{m1}x_1 + \ldots + a_{mn}x_n & = & b_m \end{cases}$$

It is said to be homogeneous when $b_1 = \ldots = b_m = 0$.



Systems of Linear Equations

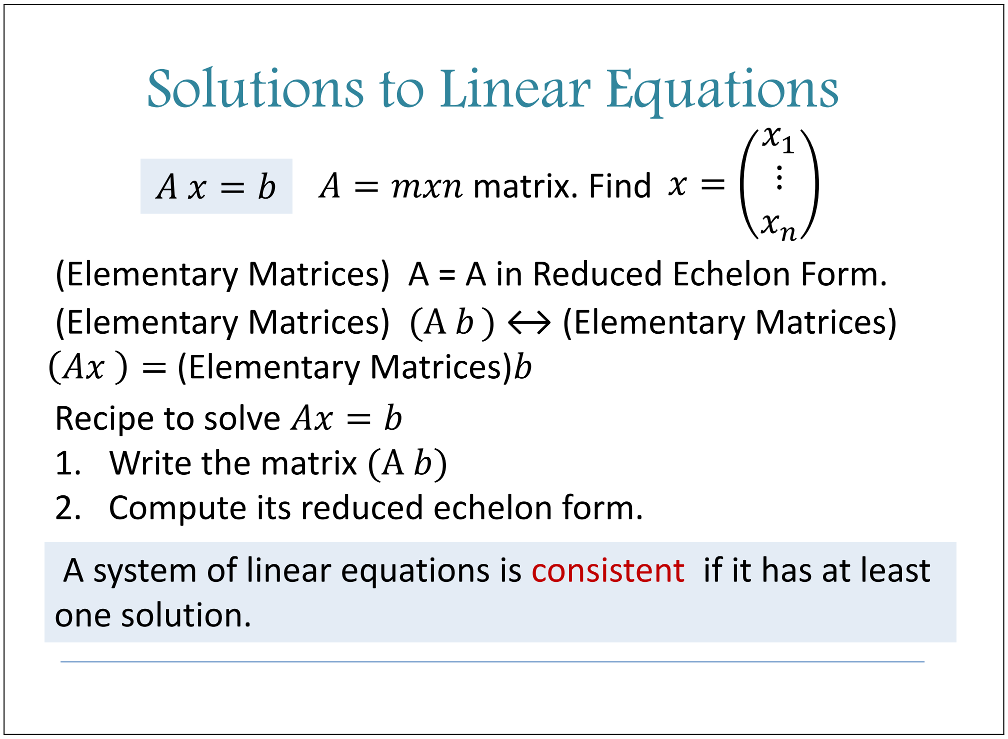
A system of m linear equations in n unknowns:

$$\begin{cases} a_{11}x_1 & + \cdots + & a_{1n}x_n = b_1 \\ a_{i1}x_1 & + \cdots + & a_{in}x_n = b_i \\ a_{m1}x_1 & + \cdots + & a_{mn}x_n = b_m \end{cases}$$

Alternatively:

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

If $b_1 = b_2 = \cdots = b_m = 0$ then the system is homogeneous.



Solutions to Linear Equations

$A\,x = b$ $A = mxn$ matrix. Find $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$

(Elementary Matrices) A = A in Reduced Echelon Form.

(Elementary Matrices) $(\mathrm{A}\ b\,) \leftrightarrow$ (Elementary Matrices) $(Ax\ ) =$ (Elementary Matrices)b

Recipe to solve $Ax = b$

1. Write the matrix $(\mathrm{A}\ b)$
2. Compute its reduced echelon form.

A system of linear equations is consistent if it has at least one solution.

In matrix form, such a system of linear equations can be rewritten as:

$$\underbrace{\begin{pmatrix} a_{11} & \dots & a_{1n} \\ & \vdots & \\ a_{i1} & \dots & a_{in} \\ & \vdots & \\ a_{m1} & \dots & a_{mn} \end{pmatrix}}_{A} \underbrace{\begin{pmatrix} x_1 \\ \vdots \\ x_i \\ \vdots \\ x_n \end{pmatrix}}_{x} = \underbrace{\begin{pmatrix} b_1 \\ \vdots \\ b_i \\ \vdots \\ b_m \end{pmatrix}}_{b}$$

We now form an augmented matrix, similarly to what was done for the inverse computation, which contains A and b, namely $(A|b)$, and we multiply the matrix $(A|b)$ on the left with elementary matrices, say $M_1, \dots, M_l$, to get a reduced row echelon form of A:

$$M_l M_{l-1} \cdots M_2 M_1 (A|b).$$

If A is invertible $M_l M_{l-1} \cdots M_2 M_1 \cdot A = I_n$, and as before

$$M_l M_{l-1} \cdots M_2 M_1 (A|I_n) = (I_n|A^{-1}b).$$

This means that

$$Ax = b \iff M_l M_{l-1} \cdots M_2 M_1 A x = M_l M_{l-1} \cdots M_2 M_1 b$$

which becomes

$$x = A^{-1}b$$

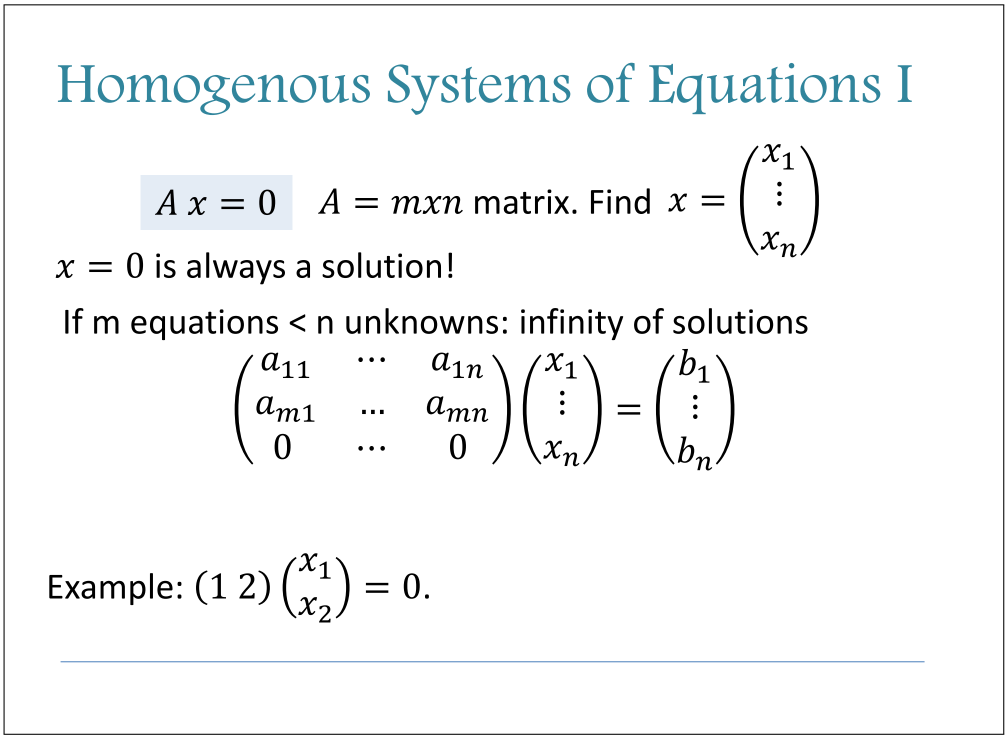
when A is invertible. If A is not invertible, the reduced echelon form still allows us to write the system $Ax = b$ in such a form that it is easy to read the solution x from it.

Recipe to solve a system $Ax = b$ of linear equations.

1. Write the augmented matrix $(A|b)$.

2. Compute its reduced row echelon form.

Let us first discuss the solutions when the system is homogeneous, that is $Ax = 0$. First note that $x = 0$ is always a solution. If $m < n$, namely there are less equations than unknowns, there will be infinitely many solutions. Some unknowns will be unconstrained, they can take any value.



Homogenous Systems of Equations I

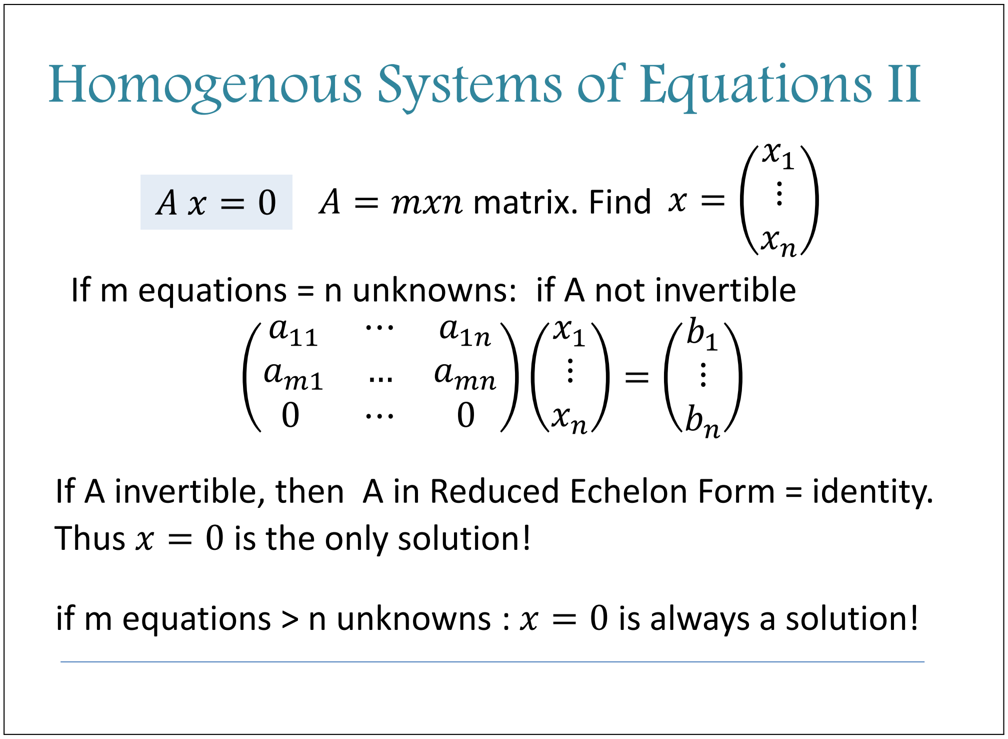
$A\,x = 0$ $A = mxn$ matrix. Find $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$

$x = 0$ is always a solution!

If m equations < n unknowns: infinity of solutions

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ a_{m1} & \dots & a_{mn} \\ 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

Example: $(1\ 2)\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = 0.$



Homogenous Systems of Equations II

$A\,x = 0$ $A = mxn$ matrix. Find $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$

If m equations = n unknowns: if A not invertible

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ a_{m1} & \dots & a_{mn} \\ 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

If A invertible, then A in Reduced Echelon Form = identity.
Thus $x = 0$ is the only solution!

if m equations > n unknowns : $x = 0$ is always a solution!

Example 82. The system

$$(1,2)\begin{pmatrix}x_1\\x_2\end{pmatrix}=0$$

has infinitely many solutions, no matter what is the value of x_1, there is a corresponding value for x_2 which satisfies this equation.

If $m = n$, we have the same number of equations as unknowns, two things can happen: if A is invertible, then $x = 0$ is the only solution, if A is not invertible, this means that when computing its row echelon form, rows of zeros will appear, and in fact, some of the equations were redundant. Therefore we will have as before infinitely many solutions.

The situation is similar when $m > n$. We still have $x = 0$ has a solution. Then when we compute the row echelon form of A, it could be that we still end up with many redundant equations, in which case infinitely many solutions still could happen, but if the number of non-zero rows is still bigger than n, then $x = 0$ is the only solution.

Let us now see what happens when the system is not homogeneous. The key thing, as noted for the homogeneous case, is to see the number of equations left once the matrix A is in reduced form.

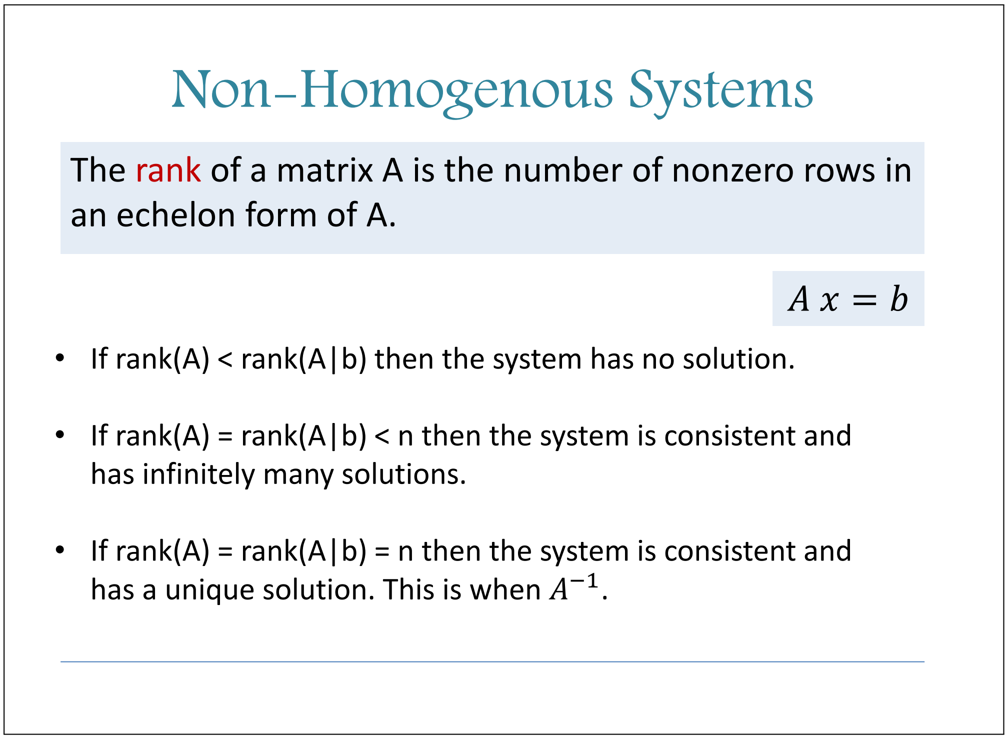
Definition 52. The rank of a matrix A is the number of non-zero rows in an echelon form of A.

For a system $Ax = b$ of linear questions, we thus get:

- If $\text{rank}(A) < \text{rank}(A|b)$, then the system has no solution. This is because when we compute the row echelon form of $(A|b)$, the part in A will have rows of zeroes, which are non-zero for $(A|b)$, corresponding to an equation of the form 0 is equal to something non-zero, which is not possible.

- If $\text{rank}(A) = \text{rank}(A|b) < n$, then the system has infinitely many solutions. The fact that both ranks are the same means that there are solutions. Now less than n means less equations than unknowns.

- If $\text{rank}(A) = \text{rank}(A|b) = n$, there is a unique solution. This corresponds to the case where A is invertible.

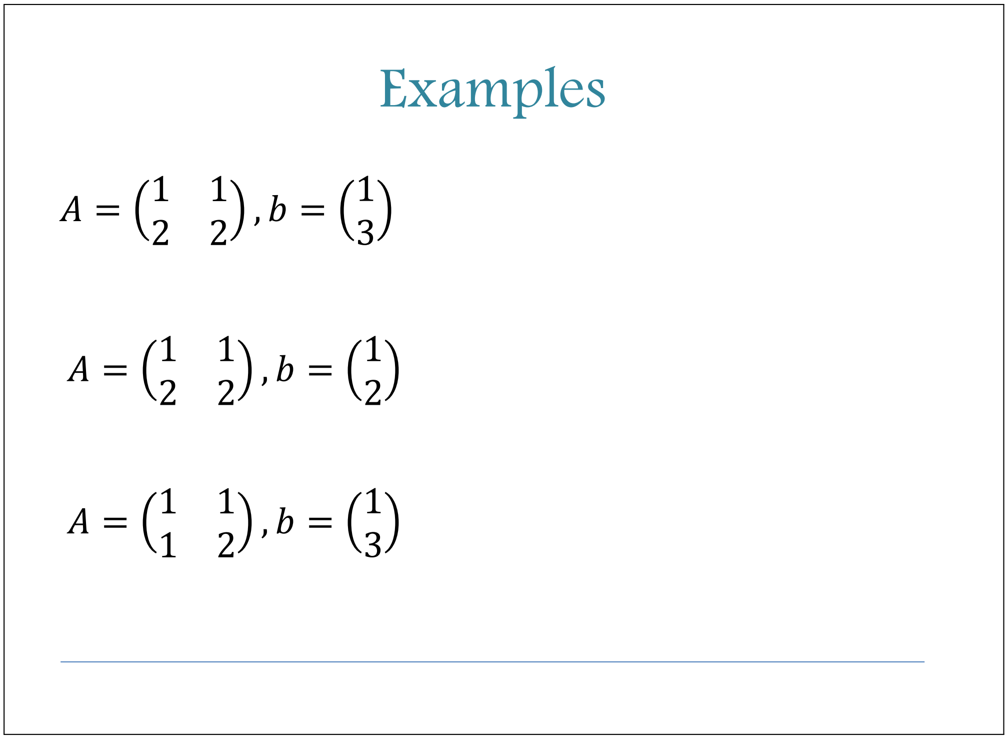


Non-Homogenous Systems

The rank of a matrix A is the number of nonzero rows in an echelon form of A.

$A\,x = b$

- If rank(A) < rank(A|b) then the system has no solution.
- If rank(A) = rank(A|b) < n then the system is consistent and has infinitely many solutions.
- If rank(A) = rank(A|b) = n then the system is consistent and has a unique solution. This is when A^{-1}.



Examples

$$A = \begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix}, b = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$$

$$A = \begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix}, b = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$$

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, b = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$$

Note that rank(A) is always less or equal rank$(A|b)$, this is because removing columns from $(A|b)$ cannot increase the number of non-zero rows, thus all cases have been considered.

Example 83. Consider the system $Ax = b$ with

$$A = \begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix}, \ b = \begin{pmatrix} 1 \\ 3 \end{pmatrix}.$$

The rank of A is 1, that of $(A|b)$ is 2, thus no solution. Now with

$$A = \begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix}, \ b = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$$

the rank of A stays 1, but that of $(A|b)$ is 1 as well, so we have infinitely many solutions. Finally, with

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, \ b = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$$

the matrix A is invertible, so there is a unique solution, given by $A^{-1}b$.

Exercises for Chapter 8

Exercise 63. Compute the sum $A+B$ of the matrices A and B, where A and B are as follows:

1. $$A = \begin{pmatrix} 2 & \sqrt{2} \\ -1 & 3 \end{pmatrix}, \ B = \begin{pmatrix} 0 & \sqrt{2} \\ 4 & 2 \end{pmatrix}$$

   where A, B are matrices with coefficients in $\mathbb{R}$.

2. $$A = \begin{pmatrix} 2+i & -1 \\ -1+i & 3 \end{pmatrix}, \ B = \begin{pmatrix} -i & 1 \\ -1 & 2 \end{pmatrix}$$

   where A, B are matrices with coefficients in $\mathbb{C}$, and $i = \sqrt{-1}$.

3. $$A = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 2 \end{pmatrix}, \ B = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 1 \end{pmatrix}$$

   where A, B are matrices with coefficients that are integers $\mod 3$.

What are the dimensions of the matrices involved?

Exercise 64. 1. Compute the transpose A^T of A for

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

2. Show that $(A+B)^T = A^T + B^T$.

Exercise 65. Compute

$$2A + BC + B^2 + AD$$

where

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

are real matrices and $D = I_2$ is the 2-dimensional identity matrix.

Exercise 66. Consider the complex matrix

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

where $i = \sqrt{-1}$. What is A^l, for $l \geq 1$.

Exercise 67.

1. Let S be the set of 3×3 diagonal real matrices. Is S closed under matrix addition?
2. Consider the real matrix

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

Compute a matrix B such that $A + B$ is diagonal, and a matrix C such that AC is diagonal.

Exercise 68. Let A and B be $n \times n$ matrices which satisfy

$$A^2 + AB + A - I_n = 0,$$

where I_n means the $n \times n$ identity matrix, and 0 the $n \times n$ zero matrix. Show that A is invertible.

Exercise 69. Compute, if it exists, the inverse A^{-1} of the matrix A, where A is given by

- $$A = \begin{pmatrix} 2 & 3 & -2 \\ -1 & 1 & 2 \\ 3 & 7 & 2 \end{pmatrix}$$

  for A a real matrix.

- $$A = \begin{pmatrix} 1 & 1+i \\ 1-i & 1 \end{pmatrix}$$

  for A a complex matrix and $i = \sqrt{-1}$.

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

  for A a matrix with coefficients modulo 5.

Exercise 70. Write the following system of linear equations in a matrix form and solve it.

$$\begin{cases} x_1 + x_2 - 2x_3 & = & 1 \\ 2x_1 - 3x_2 + x_3 & = & -8 \\ 3x_1 + x_2 + 4x_3 & = & 7 \end{cases}$$

Exercise 71. Write the following system of linear equations in a matrix form and solve it.

$$\begin{cases} x_1 - x_2 + x_3 - x_4 & = & 2 \\ x_1 - x_2 + x_3 + x_4 & = & 0 \\ 4x_1 - 4x_2 + 4x_3 & = & 4 \\ -2x_1 + 2x_2 - 2x_3 + x_4 & = & -3 \end{cases}$$

Exercises for Chapter 8

We will provide some applications of matrices to cryptography. We start by explaning the notion of cipher and give some examples.

It is said that the roman general Caesar used to communicate secretly with his army commanders using the following cipher:

$$e_K : x \to e_K(x) = x + K \mod 26,\ K = 3.$$

What it means is the following thing: one can map letters from A to Z to the integers 0 to 25. Then to say A, which is 0, encrypt it $e_K(0) = K = 3$, which is D. Therefore to say A, Caesar would write in his message D, and similarly all his messages would be encrypted. We call e_K an encryption function, and K a secret key. If the key is known, it is easy to recover the original message.

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

To recover a message, one uses a decryption function d_K. In this case

$$d_K(y) = y - K \mod 26,\ K = 3.$$

Indeed

$$d_K(e_K(x)) = e_K(x) - K = x + K - K = x \mod 26.$$

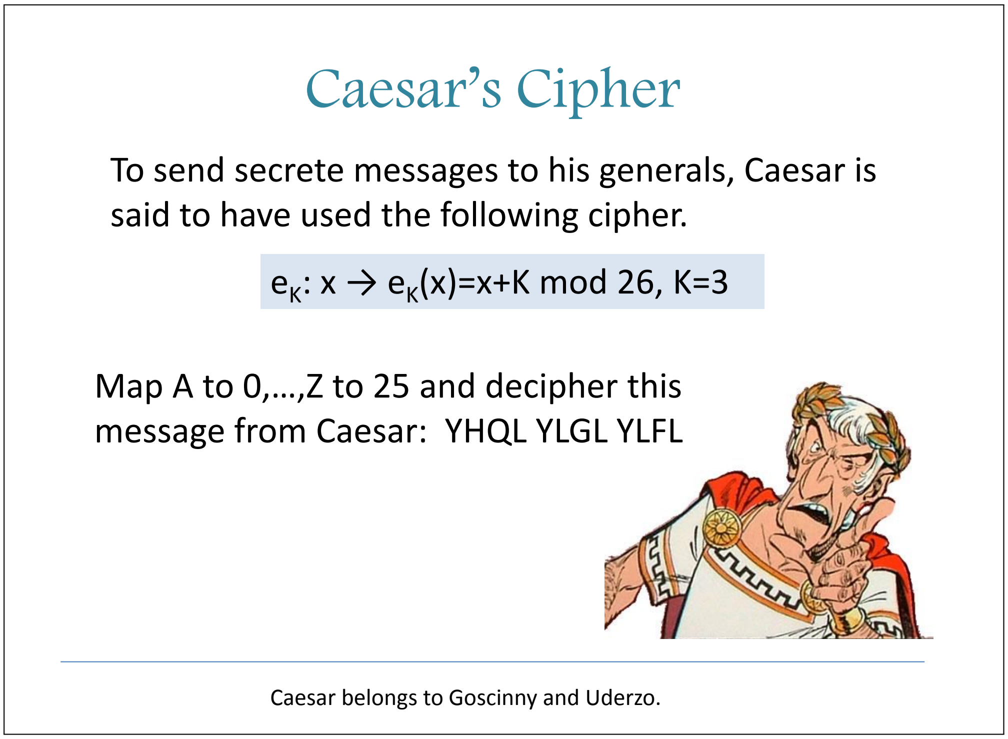
Suppose Caesar wrote $YHQL$, $YLGL$, $YLFL$. In numbers, it becomes $24, 7, 16, 11$, $24, 11, 6, 11$, $24, 11, 5, 11$ now we apply the decryption function on this, to find $21, 4, 13, 8$, $21, 8, 3, 8$, $21, 8, 2, 8$ that is VENI, VIDI, VICI. (This is a famous quote by Caesar, in latin, it means "I came, I saw, I conquered").

Caesar's cipher described above may look too simple to break. After all, one could just try all possible K, there are only 26 of them, and figure out which one works out. A variation of this cipher is called affine cipher. Now the encryption looks like this

$$e_K : x \to e_K(x) = k_1 x + k_2 \mod 26,\ K = (k_1, k_2).$$

The question is then, how to choose $K = (k_1, k_2)$? Well, the first important thing is that decryption must be possible, which is not possible for any choice of keys! For example, pick the key $K = (13, 7)$. Then

$$e_K : x \to e_K(x) = 13x + 7 \mod 26,\ K = (13, 7).$$



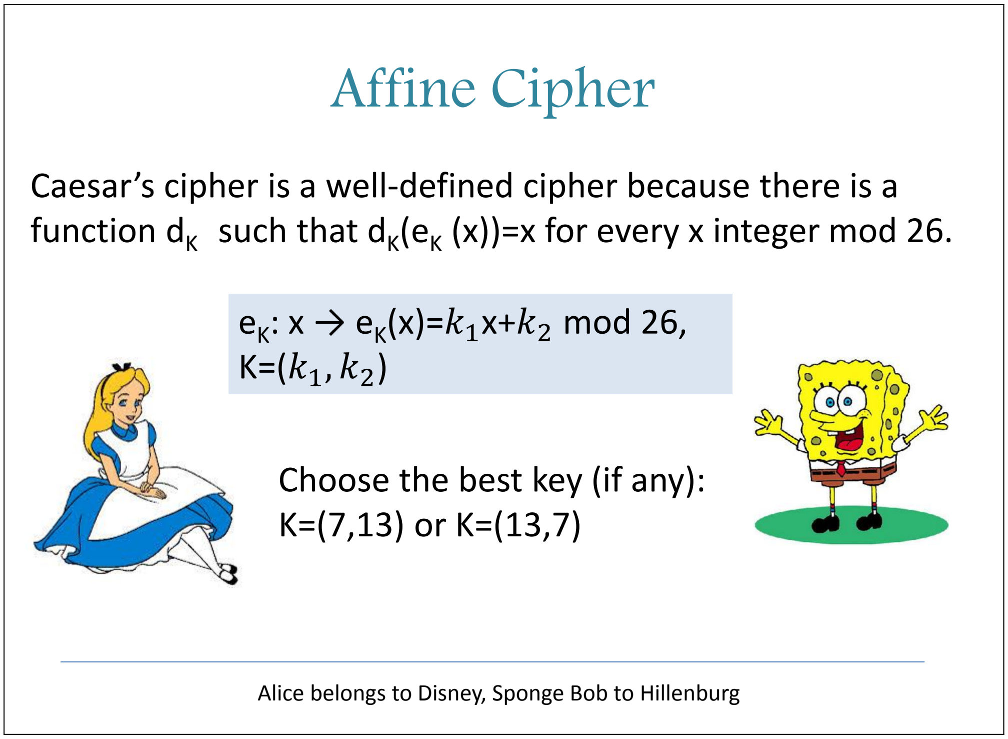
Caesar's Cipher

To send secrete messages to his generals, Caesar is said to have used the following cipher.

$e_K: x \rightarrow e_K(x)=x+K \bmod 26,\ K=3$

Map A to 0,…,Z to 25 and decipher this message from Caesar: YHQL YLGL YLFL

Caesar belongs to Goscinny and Uderzo.



Affine Cipher

Caesar's cipher is a well-defined cipher because there is a function d_K such that $d_K(e_K(x))=x$ for every x integer mod 26.

$e_K: x \rightarrow e_K(x)=k_1x+k_2 \bmod 26,$
$K=(k_1, k_2)$

Choose the best key (if any): K=(7,13) or K=(13,7)

Alice belongs to Disney, Sponge Bob to Hillenburg

To decrypt, let us try $d_K(y) = ay + b$, then

$$d_K(e_K(x)) = a(e_K(x)) + b = a(13x + 7) + b.$$

To be able to find x, we need to be able to solve $a(13x + 7) + b = x$, that is $13ax + 7a + b = x$, $7a + b = 0$, and $13a = 1$. But there is no such $a \mod 26$!

Let us try instead the key $K = (7, 13)$. Then

$$e_K : x \to e_K(x) = 7x + 13 \mod 26,\ K = (7, 13).$$

To decrypt, let us try $d_K(y) = ay + b$, then

$$d_K(e_K(x)) = a(e_K(x)) + b = a(7x + 13) + b.$$

To be able to find x, we need to be able to solve $a(7x + 13) + b = x$, that is $7ax + 13a + b = x$, $13a + b = 0$, and $7a = 1$. But now this is possible: take $a = 15$, then $105 = 104 + 1 \equiv 1 \mod 26$. Then $13 \cdot 15 = -b \equiv 13 \mod 26$ and

$$d_K(y) = 15y + 13.$$

Let us now move to an encryption scheme which uses matrices:

$$e_K : x \to e_K(x) = K_1 x + K_2 \mod 26,\ K = (K_1, K_2),$$

with

$$x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix},\ K_1 = \begin{pmatrix} 5 & 4 \\ 4 & 2 \end{pmatrix},\ K_2 = \begin{pmatrix} 4 \\ 2 \end{pmatrix}.$$

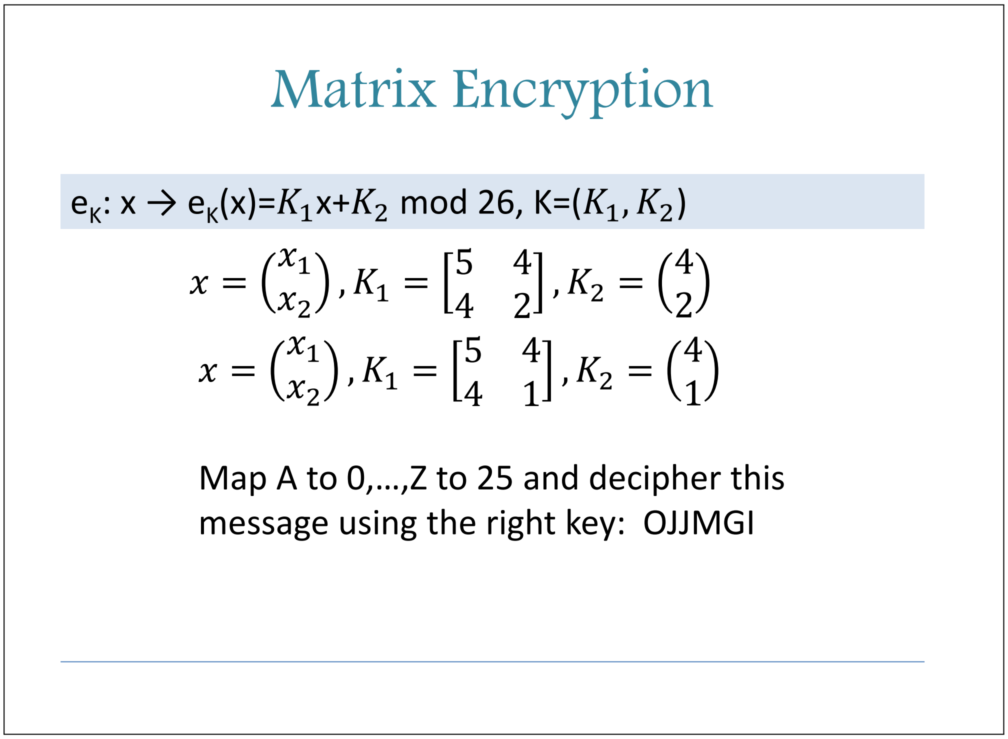
We encounter the same problem as before, namely, we need to make sure that d_K exists. Above, the trouble happened when the encryption was $13x + k_2$, because 13 is not invertible $\mod 26$. Here similarly we need to make sure that K_1 is invertible. Let us try to compute the inverse of K_1:

$$\begin{pmatrix} 5 & 4 & 1 & 0 \\ 4 & 2 & 0 & 1 \end{pmatrix}$$

Replace (row 2) by -5(row 2)+4(row 1):

$$\begin{pmatrix} 5 & 4 & 1 & 0 \\ 0 & 6 & 0 & -5 \end{pmatrix}$$

and the matrix is not invertible, because 6 is not invertible $\mod 26$, namely, it is not possible to find an element $x \mod 26$ such that $6x \equiv 1 \mod 26$.



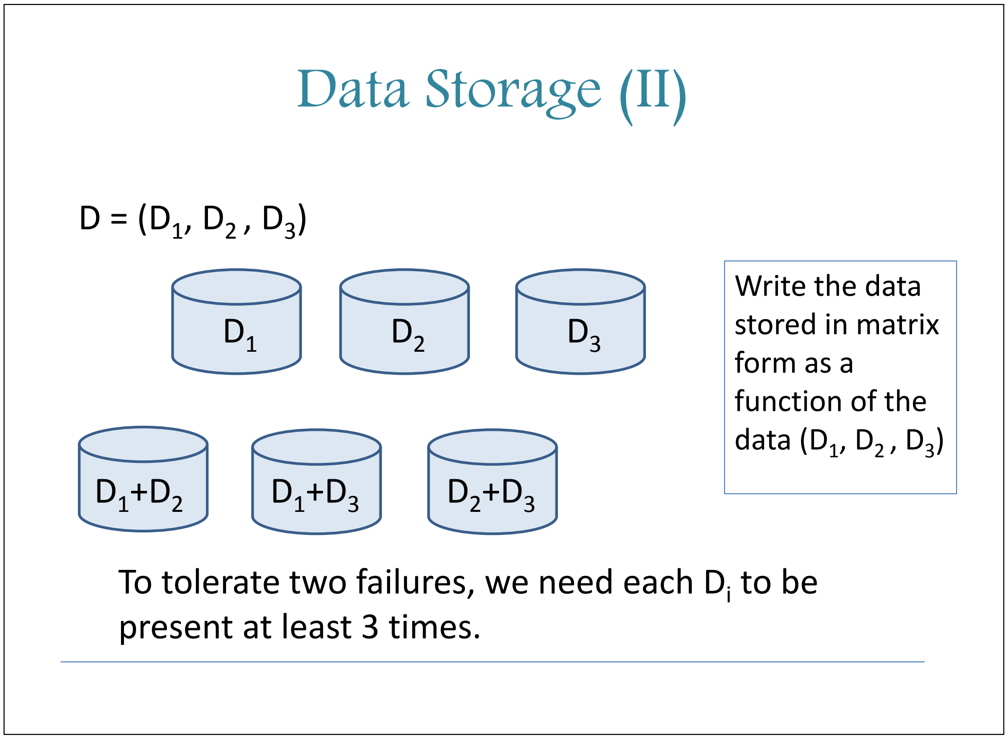
Matrix Encryption

e$_K$: x → e$_K$(x)=K_1x+K_2 mod 26, K=(K_1, K_2)

$$x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, K_1 = \begin{bmatrix} 5 & 4 \\ 4 & 2 \end{bmatrix}, K_2 = \begin{pmatrix} 4 \\ 2 \end{pmatrix}$$

$$x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, K_1 = \begin{bmatrix} 5 & 4 \\ 4 & 1 \end{bmatrix}, K_2 = \begin{pmatrix} 4 \\ 1 \end{pmatrix}$$

Map A to 0,…,Z to 25 and decipher this message using the right key: OJJMGI



Data Storage (II)

D = (D$_1$, D$_2$, D$_3$)

Write the data stored in matrix form as a function of the data (D$_1$, D$_2$, D$_3$)

To tolerate two failures, we need each D$_i$ to be present at least 3 times.

Let us try another encryption scheme which uses matrices:

$$e_K : x \to e_K(x) = K_1 x + K_2 \mod 26,\ K = (K_1, K_2),$$

with

$$x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix},\ K_1 = \begin{pmatrix} 5 & 4 \\ 4 & 1 \end{pmatrix},\ K_2 = \begin{pmatrix} 4 \\ 1 \end{pmatrix}.$$

Let us try to compute the inverse of K_1:

$$\begin{pmatrix} 5 & 4 & 1 & 0 \\ 4 & 1 & 0 & 1 \end{pmatrix}$$

Replace (row 2) by -5(row 2)+4(row 1):

$$\begin{pmatrix} 5 & 4 & 1 & 0 \\ 0 & 11 & 0 & -5 \end{pmatrix}$$

and this time, 11 is invertible $\mod 26$, namely $11 \cdot (-7) \equiv 1 \mod 26$. We then multiply the second row by -7:

$$\begin{pmatrix} 5 & 4 & 1 & 0 \\ 0 & 1 & -2 & 9 \end{pmatrix}$$

We then replace (row 1) by -4(row 2):

$$\begin{pmatrix} 5 & 0 & 9 & -10 \\ 0 & 1 & -2 & 9 \end{pmatrix}$$

Finally 5 is invertible, $5 \cdot 21 = 5 \cdot (-5) \equiv 1 \mod 26$. This gives

$$\begin{pmatrix} 1 & 0 & 7 & -2 \\ 0 & 1 & -2 & 9 \end{pmatrix}$$

and

$$K_1^{-1} = \begin{pmatrix} 7 & -2 \\ -2 & 9 \end{pmatrix}$$

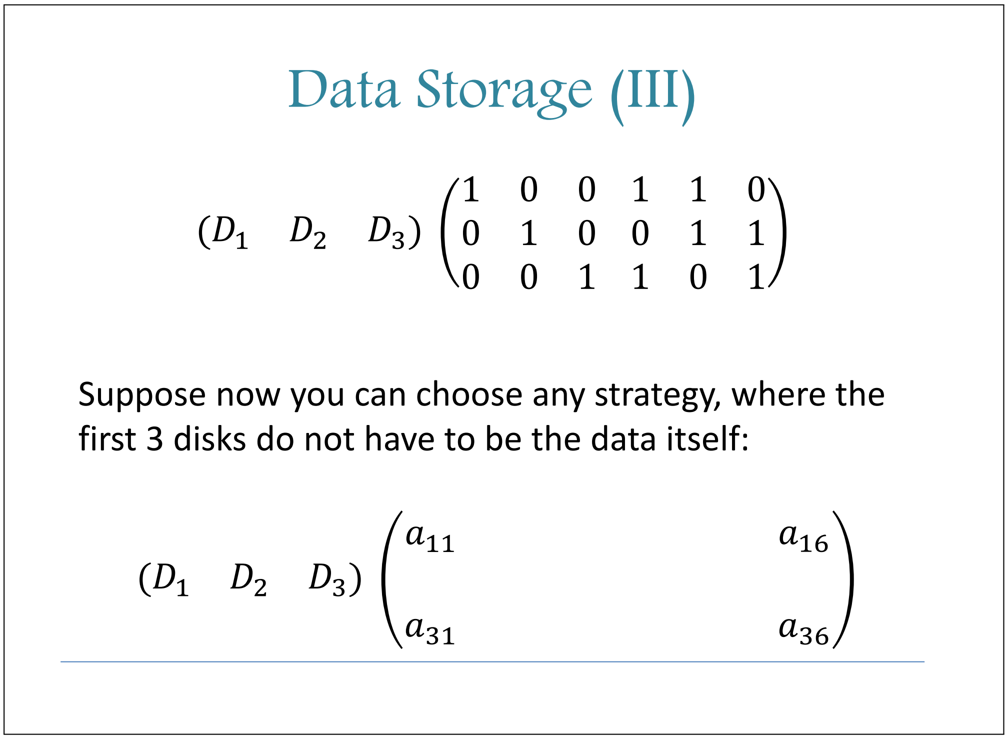
To decipher for example OJ, we map it to integers, namely $14, 9$, then

$$\begin{pmatrix} 14 \\ 9 \end{pmatrix} - \begin{pmatrix} 4 \\ 1 \end{pmatrix} = \begin{pmatrix} 10 \\ 8 \end{pmatrix}$$

and we apply K_1^{-1} to get

$$\begin{pmatrix} 7 & -2 \\ -2 & 9 \end{pmatrix} \begin{pmatrix} 10 \\ 8 \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \end{pmatrix}$$

that is the message CA. In a similar way, we find that $OJJMGI$ gives $CANLAH$.

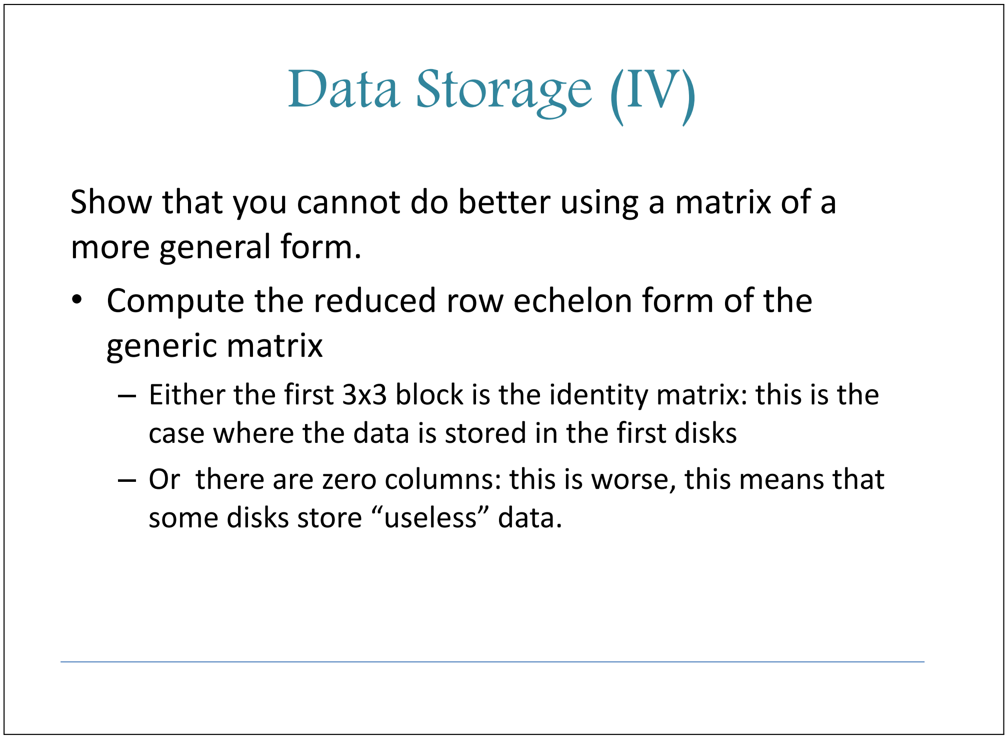


Data Storage (III)

$$(D_1 \quad D_2 \quad D_3)\begin{pmatrix}1 & 0 & 0 & 1 & 1 & 0\\ 0 & 1 & 0 & 0 & 1 & 1\\ 0 & 0 & 1 & 1 & 0 & 1\end{pmatrix}$$

Suppose now you can choose any strategy, where the first 3 disks do not have to be the data itself:

$$(D_1 \quad D_2 \quad D_3)\begin{pmatrix}a_{11} & & & & & a_{16}\\ & & & & & \\ a_{31} & & & & & a_{36}\end{pmatrix}$$



Data Storage (IV)

Show that you cannot do better using a matrix of a more general form.

- Compute the reduced row echelon form of the generic matrix
  - Either the first 3x3 block is the identity matrix: this is the case where the data is stored in the first disks
  - Or there are zero columns: this is worse, this means that some disks store "useless" data.

We finally come back once more to our example of data storage. Suppose that you have some data D, split into 3 parts $D = (D_1, D_2, D_3)$. We saw that to tolerate 2 failures, we need at least 6 disks, assuming that the first 3 disks are storing D_1, D_2, D_3 respectively. For example, one way of storing the data could be

disk 1: D_1 disk 4: $D_1 + D_2$
disk 2: D_2 disk 5: $D_1 + D_3$
disk 3: D_3 disk 6: $D_2 + D_3$

This way of storing data can be represented using matrices:

$$(D_1, D_2, D_3)\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

Now we want to check that any arbitrary strategy where we could have chosen any way of combining the data, not necessarily storing D_1, D_2, D_3 in the first 3 disks, cannot improve the one we already got. Write

$$(D_1, D_2, D_3)\underbrace{\begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} & a_{16} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} & a_{26} \\ a_{31} & a_{32} & a_{33} & a_{34} & a_{35} & a_{36} \end{pmatrix}}_{A}$$

To see this, visualize that whatever is stored in our 6 disks is obtained by combining the three rows of this matrix A. We can then try to combine them in any way we want using elementary operations (swap rows, add one row to another). Since every operation can be reversed, we can always go back and forth from one form to another. Then we compute the reduced row echelon form of this matrix, and two things can happen: either the first 3 columns are I_3, in which case we are back to the strategy we already know, or one column becomes zero, which is worse, since this corresponds to a disk storing no data.