Application of inverse matrix: Cryptography

A is used to encrypt the message
A^{-1} is used to decrypt the message

Hill algorithm:

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

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

ATTACK NOW

$$\begin{bmatrix} A \\ T \end{bmatrix} = \begin{bmatrix} 1 \\ 20 \end{bmatrix} \quad \begin{bmatrix} T \\ A \end{bmatrix} = \begin{bmatrix} 20 \\ 1 \end{bmatrix}$$

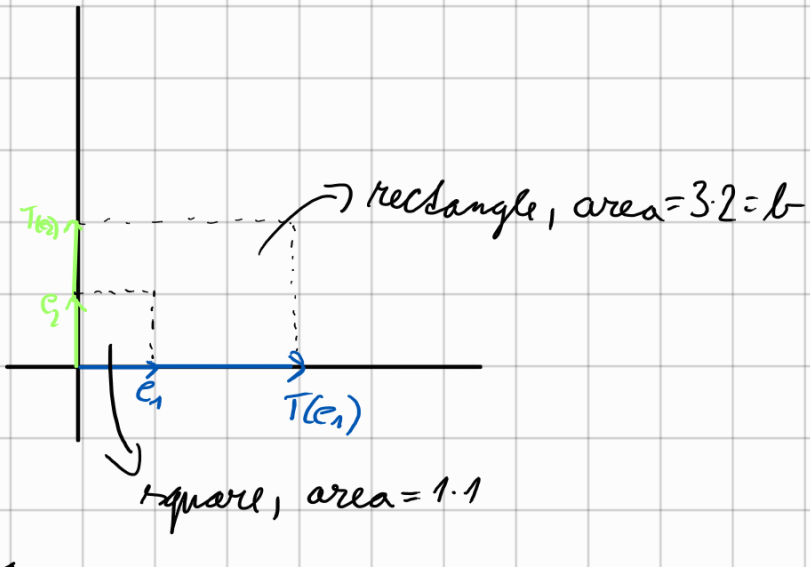
$$\begin{bmatrix} C \\ k \end{bmatrix} = \begin{bmatrix} 3 \\ 11 \end{bmatrix} \quad \begin{bmatrix} - \\ N \end{bmatrix} = \begin{bmatrix} 27 \\ \end{bmatrix} \ldots$$

$$A \begin{bmatrix} A \\ T \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 1 \\ 20 \end{bmatrix} = \begin{bmatrix} 41 \\ 61 \end{bmatrix}$$

$$A^{-1} \begin{bmatrix} 41 \\ 61 \end{bmatrix} = \begin{bmatrix} 1 \\ 20 \end{bmatrix} = \begin{bmatrix} A \\ T \end{bmatrix}$$

(EX) $A = \begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix}$ $\mathbb{R}^2 \to \mathbb{R}^2$

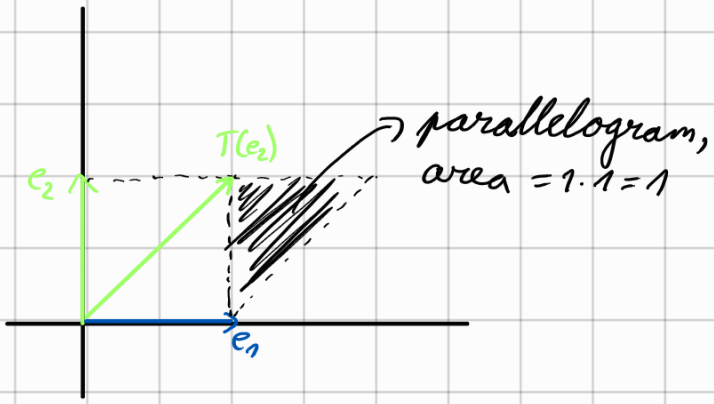
$T(e_1)$ $T(e_2)$



So, A is stretching objects in $\mathbb{R}^2$. The stretching/scaling factor is $b = \det(A)$

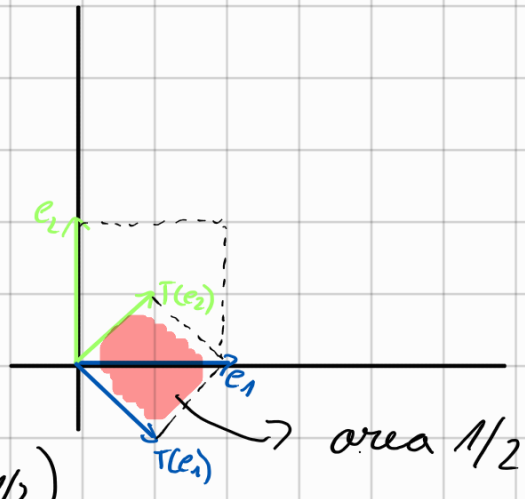
↳ > 1 because the area increases

(EX) $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$



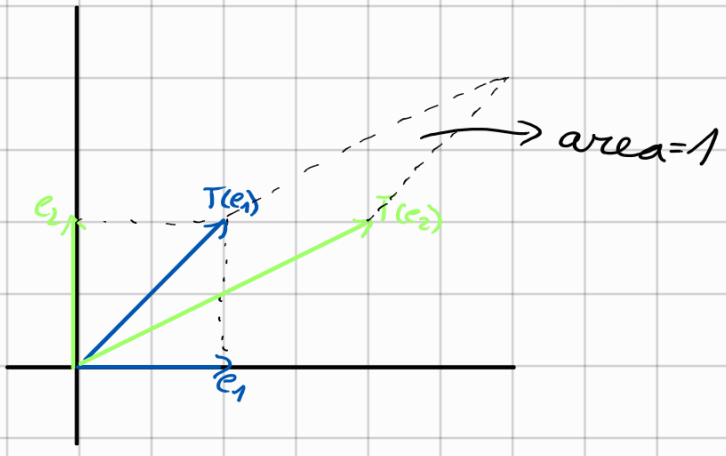
So $\det(A) = 1$ (because the area stays the same)

(EX) $A = \begin{bmatrix} 1/2 & 1/2 \\ -1/2 & 1/2 \end{bmatrix}$



So $\det(A) = 1/2$
(because the area squishes with a factor 1/2)

(EX) $A = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}$



However, the orientation of the space has been inversed. So, $\det(A) = -1$

The determinant of a square $(n \times n)$ matrix is a scalar associated with the matrix

Notation: $\det(A)$ or $|A|$

It measures how the transformation: $T: \underline{x} \to A\underline{x}$ scales space:

- → in $\mathbb{R}^2$ it measures the change in areas of objects by T
- → in $\mathbb{R}^3$ it measures the change in volumes of objects by T

$\det(A) = 0$ → spaces are flattened / we are loosing one dimension
→ range ≠ co-domain
→ transformation is not surjective (onto)
→ A is not invertible

How to compute the determinants?
→ Gaussian elimination
→ cofactor expansion

determinant of 2×2 matrix:

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

Cofactor expansion for an $n \times n$ matrix:

→

- focus on a specific row i or col j
→ for example, for row i: $\det(A) = \sum_{j=1}^{n} a_{ij} \cdot C_{ij}$

* a_{ij} : entry of A at (i, j)
* C_{ij} : (i, j)-cofactor $= (-1)^{i+j} \cdot \det(A_{ij})$
* A_{ij} : submatrix obtained by removing row i and col j

(EX) $A = \begin{bmatrix} 3 & 5 & 1 \\ 0 & 2 & 1 \\ 0 & 0 & 1 \end{bmatrix}$

Cofactor expansion across the 1st row:

$$\det(A) = 3 \cdot (-1)^2 \cdot \begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix} + 5 \cdot (-1)^3 \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} + 1 \cdot (-1)^3 \begin{bmatrix} 0 & 2 \\ 0 & 0 \end{bmatrix}$$

$$= 3 \cdot 2 - 5 \cdot 0 + 1 \cdot 0 = 6$$

Cofactor expansion across the 1st col:

$$\det(A) = 3 \cdot (-1)^2 \begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix} + 0 + 0 = 3 \cdot 2 = 6$$

Yo, be smart: choose row/col with many 0s

Triangular matrix: the entries below/above the main diagonal are all 0s

$$\begin{bmatrix} * & * & * & * \\ 0 & * & * & * \end{bmatrix} \qquad \begin{bmatrix} * & 0 & 0 & 0 \\ * & * & 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} * & * & * & * \\ 0 & * & * & * \\ 0 & 0 & * & * \\ 0 & 0 & 0 & * \end{bmatrix} \qquad \begin{bmatrix} * & * & * & 0 \\ * & * & * & * \\ * & * & * & * \\ * & * & * & * \end{bmatrix}$$

Diagonal matrix: a square matrix whose nondiagonal entries are all 0s.

$$\begin{bmatrix} * & 0 & 0 & 0 \\ 0 & * & 0 & 0 \\ 0 & 0 & * & 0 \\ 0 & 0 & 0 & * \end{bmatrix}$$

For **triangular** or **diagonal** matrices, the determinant equals the **product** of the entries on the **main diagonal**

$$\begin{bmatrix} * & * & * & * \\ 0 & * & * & * \\ 0 & 0 & * & * \\ 0 & 0 & 0 & * \end{bmatrix}$$

$$\det(A) = a_{11} \cdot a_{22} \cdot a_{33} \cdot \dots \cdot a_{nn}$$

REF is **upper triangular**

So maybe we can use **Gaussian elimination** to compute the determinant?

How do row operation change the determinant?

* two rows of A are **interchanged** to produce B
  $\det(B) = -\det(A)$
* one row of A is **multiplied** by k to produce B $\det(B) = k \det(A)$
* a **multiple** of one row of A is **added** to

another row to produce B

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

(EX) $\begin{bmatrix} 0 & 5 & 1 \\ 4 & -3 & 0 \\ 2 & 4 & 1 \end{bmatrix} \underset{R_1 \leftrightarrow R_3}{=} (-1)\begin{bmatrix} 2 & 4 & 1 \\ 4 & -3 & 0 \\ 0 & 5 & 1 \end{bmatrix} \underset{R_2 : R_2 - 2R_1}{=} (-1)\cdot\begin{bmatrix} 2 & 4 & 1 \\ 0 & -11 & -2 \\ 0 & 5 & 1 \end{bmatrix}$

$\underset{R_3 : R_3 + 5/11 R_2}{=} (-1)\cdot\begin{bmatrix} 2 & 4 & 1 \\ 0 & -11 & 2 \\ 0 & 0 & 1/11 \end{bmatrix} = (-1)\cdot 2 \cdot (-11) \cdot 1/11 = \underline{\underline{2}}$

Square matrix A not invertible

$\Rightarrow A$ is not row equivalent to I_n

eg. $\text{REF}\begin{bmatrix} 2 & 4 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$

$\Rightarrow$ a pivot is missing

$\Rightarrow \det(\text{REF of } A) = 0$

$\Rightarrow \det(A) = (-1)^{\#\text{swaps}} \cdot \det(\text{REF of } A) = (-1)^{\#\text{swaps}} \cdot 0 = 0$

$\Rightarrow \det(A) = 0$

Conclusion: square matrix A is not invertible $\Leftrightarrow \det(A) = 0$

Properties of determinants:

* $\det(A^T) = \det(A)$
* $\det(AB) = \det(A) \cdot \det(B)$
* but $\det(A+B) \neq \det(A) + \det(B)$ in general
* $\det(c \cdot A) = c^n \cdot \det(A)$

Theorem: $\det(A^{-1}) = \frac{1}{\det(A)}$ for all invertible matrices

Proof: $1 = \det(I_n) = \det(A \cdot A^{-1}) = \det(A) \cdot \det(A^{-1})$

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