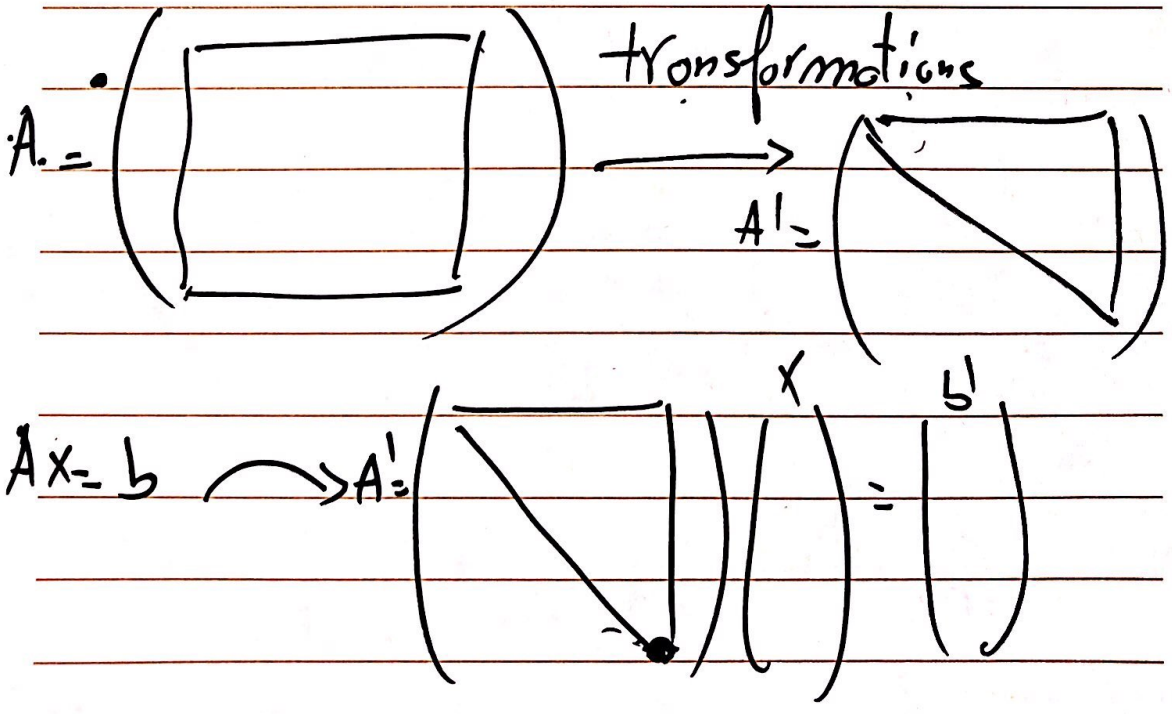
EE 510 09/11/20

Outline:

- Gaussian Elimination
- Vector spaces
- Finite Fields.



- $R_1 \longleftrightarrow R_1$ (R_1 ↔ R_2)
- $R \longleftarrow \alpha R$; $\alpha \neq 0$ (αR)
- $R \longleftarrow R + \beta R_1$; β any value

Pivot

$$\begin{cases} x+2y+2z=2 \\ x+3y+2z=2 \\ 3x+7y+8z=8 \end{cases} \Rightarrow \begin{pmatrix} 1 & 2 & 2 \\ 1 & 3 & 3 \\ 3 & 7 & 8 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \\ 8 \end{pmatrix}$$

$R_2 \longleftarrow R_2 - R_1$

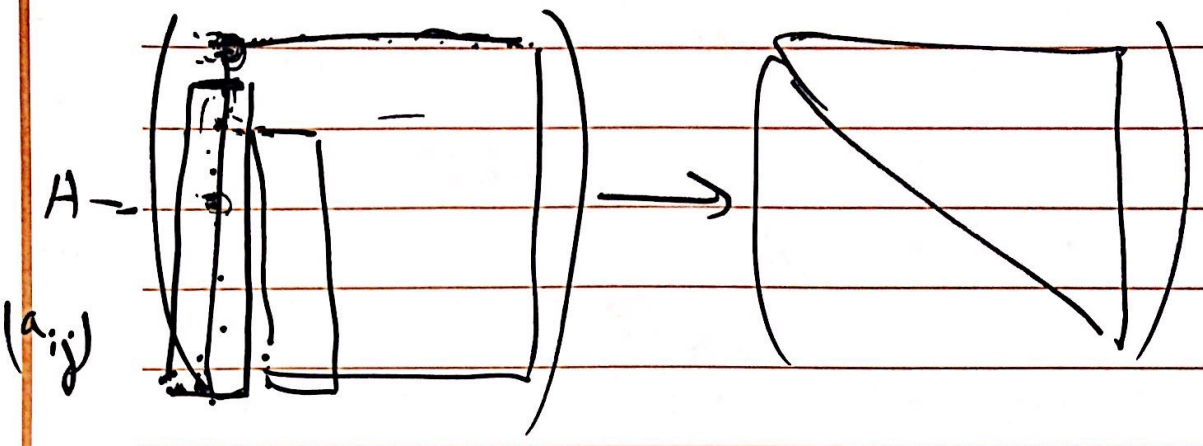
$R_3 \longleftarrow R_3 - 3R_1$

$$\Rightarrow \left(\begin{array}{ccc|c} 1 & 2 & 2 & 2 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 2 & 2 \end{array}\right)$$

$R_3 \longleftarrow R_3 - R_2$

$$\Rightarrow \left(\begin{array}{ccc|c} 1 & 2 & 2 & 2 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 2 \end{array}\right)$$

$$\begin{cases} x+2y+2z=2 \\ y+z=0 \\ z=2 \end{cases} \Rightarrow \begin{cases} x=2 \\ y=-2 \\ z=2 \end{cases}$$



$$R_i \leftarrow R_i - \frac{a_{i1}}{a_{11}} R_1 \; ; \; 2 \leq i \leq n$$

- $n-1$ division
- $n(n-1)$ multiplications

- $n(n-1)$ additions

For Pivot k: $\quad R_i \leftarrow R_i - \frac{a_{ik}}{a_{kk}} R_k$

$n-k$ divisions

$n(n-k+1)(n-k)$ multiplications

$n(n-k+1)(n-k)$ additions

$$n(n-k+1)(n-k) = (n-k)^2 + (n-k)$$

$$\sum_{k=1}^{n} (n-k) = \frac{n(n-1)}{2} \text{ divisions}$$

$$\sum_{k=1}^{n} (n-k)^2 + (n-k) = \frac{n^3-n}{3}$$

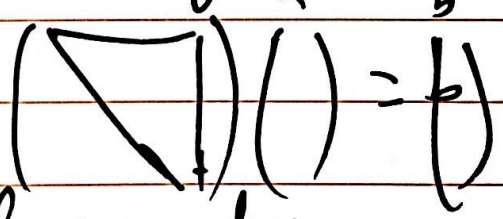
$\frac{n(n-1)}{2}$ division

$\frac{n^3-n}{3}$ multiplications

$\frac{n^3-n}{3}$ additions

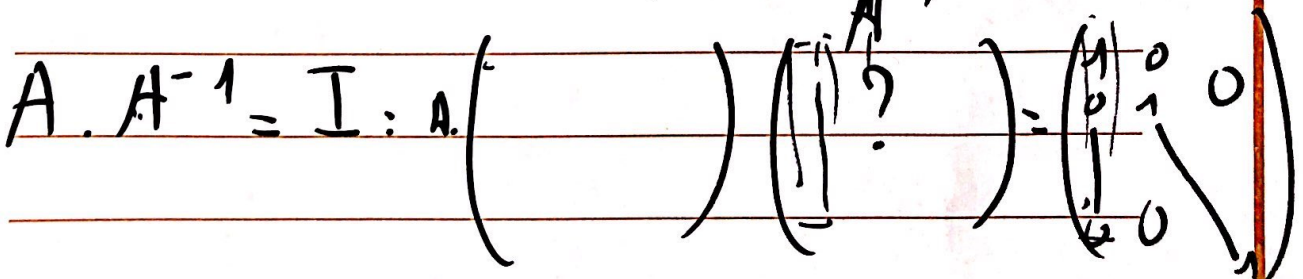
$\Rightarrow O(n^3)$.

- Solve Linear Systems.

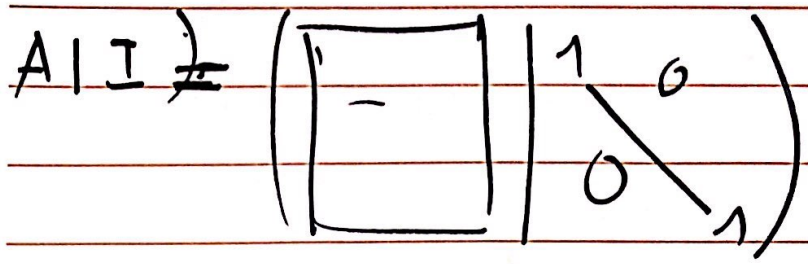
$Ax = b \xrightarrow{G.E}$ 

- Inverse of a matrix

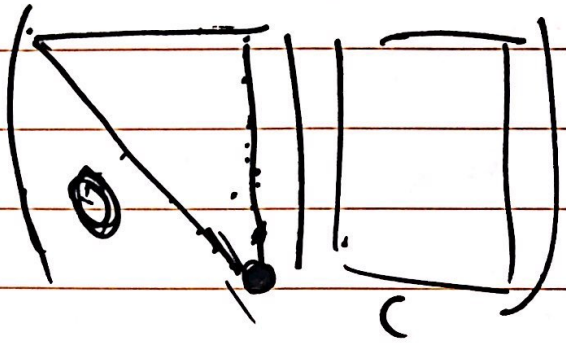
A invertible: $\exists A^{-1}$?!

$A \cdot A^{-1} = I$: 

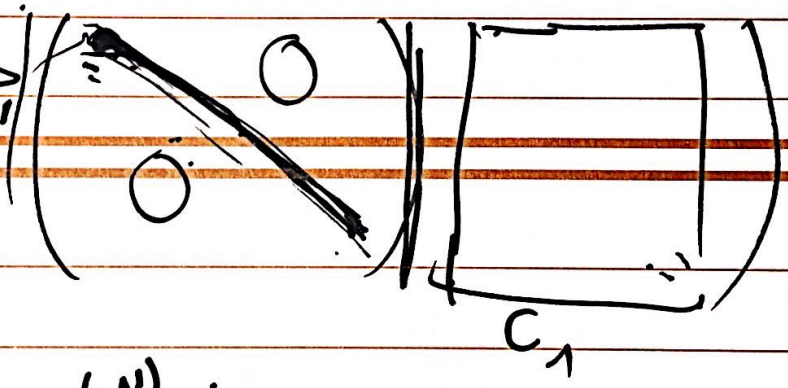
$(A \mid I)$



$\Rightarrow$



$\Rightarrow$ A'

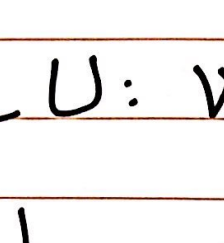
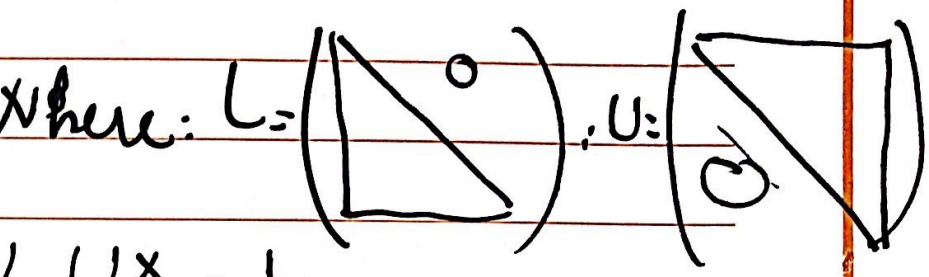


diag (A'):

$$= \frac{a'_{11}}{a'_{11}}$$

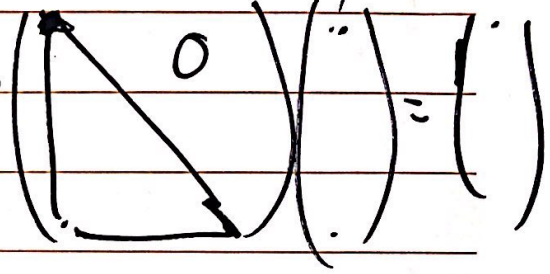
$\Rightarrow (I \mid A^{-1})$

LU decomposition:

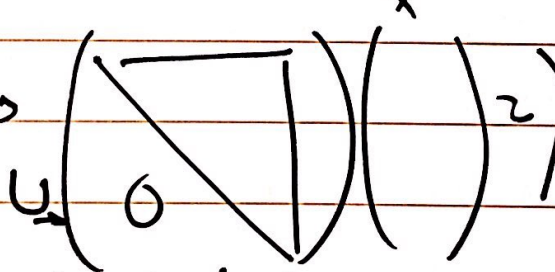
$A = LU$: where: $L =$  , $U =$ 

$AX = b \Rightarrow LUX = b$

$y = Ux$

$\Rightarrow Ly = b \Leftrightarrow$ 

forward substitution

$Ux = y \Rightarrow$ 

back substitution

$\Rightarrow X$: solution for $AX = b$

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 3 & 5 \\ 4 & 6 & 8 \end{pmatrix} \quad ; \quad L, U : A = LU,$$

$$L_1 \cdot A = \begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 2 & 3 & 5 \\ 4 & 6 & 8 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 3 \\ 4 & 6 & 8 \end{pmatrix}$$

$$L_2 \cdot A_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -4 & 0 & 1 \end{pmatrix} \times A_1 = \underbrace{\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 3 \\ 0 & 2 & 4 \end{pmatrix}}_{A_2} \quad A_1$$

$$L_3 \times A_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -2 & 1 \end{pmatrix} A_2 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 3 \\ 0 & 0 & -2 \end{pmatrix}$$

$$L_3 \times L_2 \times L_1 A = U$$

$$A = L_1^{-1} L_2^{-1} L_3^{-1} U$$

$$PA = LU$$

$$A = P^T LU \quad (P^{-1} = P^T)$$

$$L = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 4 & 2 & 1 \end{pmatrix} \quad ; \quad U = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 3 \\ 0 & 0 & -2 \end{pmatrix}$$

$\Rightarrow$ LU is not unique.

What is a vector space?

- Set V of abstract elements.
- A Field $\mathbb{F}$
- An internal operation "+"
  - set V is closed under summation; $x \in V$, $y \in V$ $\Rightarrow x+y \in V$
- An external operation "$\cdot$"
  $\alpha \in \mathbb{F}$; $x \in V$ $\Rightarrow (\alpha \cdot x) \in V$

- associative & Commutative
- additive identity.
  $\forall x \in V$
  $x + 0 = x$
- additive inverse.
  $\forall x \in V$:
  $x + (-x) = 0$

$\Rightarrow V$ is a vector space.

∴ V is a vector space.

In ~~gene~~ most applications:

V is ~~V~~ vector sub-space of a vector space.

- $\forall x, y \in V;\ \alpha \in \mathbb{F}$

  $\alpha x + y \in V$

$(\mathbb{R}, +, \times)$ is $\mathbb{R}$-vector space
$V = \mathbb{R}$; $\mathbb{F} = \mathbb{R}$.

$(\mathbb{C}, +, \times)$ is $\mathbb{R}$-vector space
$V = \mathbb{C}$; $\mathbb{F} = \mathbb{R}$.

Exercise: V is a vector space
V_1 is vector sub-space of V
V_2 is vector sub-space of V

Is $V_1 \cap V_2$ a vector space?

$x \in V_1 \cap V_2$; $\alpha x + y \overset{?!}{\in} V_1 \cap V_2$
$y \in V_1 \cap V_2$

$x \in V_1 \Rightarrow \alpha x + y \in V_1$ (V_1 is a vector space)
$y \in V_2$

$x \in V_2 \Rightarrow \alpha x + y \in V_2$ "
$y \in V_2$

$\Rightarrow \alpha x + y \in V_1 \cap V_2$

$V_1 \cap V_2$ is a vector sub-space of V

Is $V_1 \cup V_2$ a vector space?

Generally, $V_1 \cup V_2$ is not a vector space!

$V_1 \cup V_2$ is a vector space iff $V_1 \subset V_2$ or $V_2 \subset V_1$

~~By Contradiction:~~

~~$V_1 \cup V_2$~~ ⊙ $V_1 \subset V_2$ or $V_2 \subset V_1$

$V_1 \cup V_2 = V_2$ or $V_1 \cup V_2 = V_1$

$\Rightarrow V_1 \cup V_2$ is a vector space.

⊙ $V_1 \cup V_2$ is a vector space.

By Contradiction: $V_1 \not\subset V_2$ and $V_2 \not\subset V_1$

$\exists x \in V_1$ and $x \notin V_2$

$\exists y \in V_2$ and $y \notin V_1$

$x \in V_1 \subset V_1 \cup V_2$; $y \in V_2 \subset V_1 \cup V_2$

$z = x + y \in V_1 \cup V_2$ ($V_1 \cup V_2$ is a vector space)

$\Rightarrow z \in V_1$ or $z \in V_2$

- $z \in V_1$: $y = z - x \in V_1$ (V_1 is a vector space)

Impossible

$z \in V_2 \Rightarrow x \in V_2$ impossible

$\Rightarrow V_1 \subset V_2$ or $V_2 \subset V_1$

- A field: $\mathbb{K}$
  - 2 internal operations "+" ; "×"
  - associative & commutative.
  - additive identity ; $x + a = x$
    multiplicative identity ; $x \times 1 = x$
  - additive inverse
  - multiplicative inverse

$$x + (-x) = 0 \quad ; \quad x * (x^{-1}) = 1$$

- $(\mathbb{R}, +, \times)$ is a field ✓
- $(\mathbb{N}, +, \times)$ no $\times$
- $(\mathbb{Z}, +, \times)$ no $\times$
- $(\mathcal{M}_n(\mathbb{R}), +, \times)$ not a field
- $(GL_n(\mathbb{R}), +, \times)$ is a field.

$\mathbb{F}_p = \{0, 1, \dots, p-1\}$ is a field
iff p is a prime number.

$p = 7$; $\mathbb{F}_7 = \{0, 1, 2, \dots, 6\}$

"+" modulus 7

"×" modulus 7

$2 + 6 = 1 \mod(7)$; $2 + 5 = 0 \mod(7)$

$2 \times 4 = 1 \mod(7)$

$2^{-1} = 4$; $3^{-1} = 5$; $6^{-1} = 6$.

- Polynomials over field $\mathbb{F}$

$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 ; a_i \in \mathbb{F}$

$\mathbb{F}_2 = \{0, 1\}$; $\{x, x+1, 1, 0\}$ set of polynomials of degree ≤ 1

Irreducible polynomials $\Leftrightarrow$ "prime numbers"

↓

Cannot be factorized over $\mathbb{F}$.

$P(x) = x^2 + 1$ ⟶ $\mathbb{F} = \mathbb{R}$ ✗

$\mathbb{F} = \mathbb{C}$ ✓ $(x-i)(x+i)$

$\mathbb{F} = \mathbb{F}_2$ ✓ ; $x^2+1 = (x+1)(x+1)$ mod (2)

- Irreducible polynomial of degree m over the field $\mathbb{F}_p$ (p is prime)

$\mathbb{F}_{p^m}$: the set of polynomials of degree $\leq m-1$ is a finite field with p^m elements.