COMPUTING WITH MATRICES, GROUPS

LA1 23/10/25

Review: A real $m \times n$ matrix

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & & \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

i-th row, j-th column

n-dim column / row vector
$n \times 1$ / $1 \times n$ matrix

Ex: description of solution set of $Ax=b$

zero matrix ... 0

Matrix addition $A+B$: matrix C s.t. $C_{ij} = A_{ij} + B_{ij}$, $\forall i,j$

Scalar multiplication of matrix A: $k \cdot A$ $\quad \cancel{Ak}$

Equality of matrices: $A=B$ if $A_{ij} = B_{ij}$, $\forall i,j$

(The following seems trivial - the hard part is to understand what are we doing and why)

Proposition (properties of matrix addition and scalar multipl.)

For any matrices $A, B, C \in \mathbb{R}^{m \times n}$ and scalars $s, t \in \mathbb{R}$, the following holds:

1. $A + B = B + A$ — commutative property
2. $(A+B)+C = A+(B+C)$ — associative property
3. $A + 0 = A$
4. $A + (-A) = 0$, where $-A = (-1)\cdot A$
5. $s\cdot(t\cdot A) = (s\cdot t)\cdot A$
6. $s(A+B) = s\cdot A + s\cdot B$
7. $(s+t)\cdot A = s\cdot A + t\cdot A$

6.–7.: distributive property

Proof: 1. We need to check that $\forall i,j$,

$$\begin{array}{ccc} (A+B)_{ij} & \overset{?}{=} & (B+A)_{ij} \\ \| & & \| \\ A_{ij}+B_{ij} & = & B_{ij}+A_{ij} \end{array}$$

$\leftarrow$ definition of matrix addition

$\uparrow$ commutativity of addition of real numbers

2.–7. – analogously, HW. $\blacksquare$

Note the similarity between addition of reals and matrices.

A small digression:

Def: Binary operation on a set T is a mapping $T \times T \to T$.

Notation: for a binary operation $\oplus : T \times T \to T$ and $x, y \in T$, we usually write $x \oplus y$ instead of $\oplus(x,y)$.

Ex. $+$ ... on $\mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{N}$ addition of reals, ...

$\cdot$ ... on $\mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{N}$ multiplication

$-$ ... on $\mathbb{R}, \mathbb{Q}, \mathbb{Z}, \cancel{\mathbb{N}}$ substraction

$:$ ... on $\mathbb{R} \setminus \{0\}, \mathbb{Q} \setminus \{0\}$ division

$+$ ... on real $m \times n$ matrices

composition of two rotations around the origin in 2D

Def: A group is a pair $(G, \oplus)$ where G is a set and $\oplus$ is a binary operation on G satisfying the following axioms:

1. $\forall a,b,c \in G : (a \oplus b) \oplus c = a \oplus (b \oplus c)$ associative property
2. $\exists n \in G \ \forall a \in G : a \oplus n = n \oplus a = a$ n ... neutral element of G
3. $\forall a \in G \ \exists b \in G : a \oplus b = b \oplus a = n$ b ... inverse element for a

If in addition

4. $\forall a,b \in G : a \oplus b = b \oplus a$ commutative prop.

holds, $(G, \oplus)$ is an Abelian group

Ex. • $(\mathbb{R},+), (\mathbb{Q},+), (\mathbb{Z},+), (\mathbb{C},+)$ neutral elem.... 0 $\cancel{(\mathbb{N},+)}$

• $(\mathbb{R}^{m \times n}, +)$ ... group of real $m \times n$ matrices

• $(\mathbb{R} \setminus \{0\}, \cdot), (\mathbb{Q} \setminus \{0\}, \cdot)$ neutral elem. ... 1

Finite examples

• $(\{n\}, +)$ where the bin. op. $+$ is given by

$+$	n
n	n

• $(\{0,1\}, +)$ where

$+$	0	1
0	0	1
1	1	0

i.e., $(\mathbb{Z}_2, \oplus)$

• $(\mathbb{Z}_n, \oplus)$ where $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ and $\forall a,b \in \mathbb{Z}_n$:
$a \oplus b = a+b \mod n$
the reminder after division of $a+b$ by n

• $(\{\text{True}, \text{False}\}, \text{XOR})$ where

XOR	T	F
True	F	T
False	T	F

XOR = exclusive OR

BEWARE – new level of abstraction!

1. working with (real) numbers
2. working with letters representing (real) numbers
3. working with elements from any structure satisfying certain axioms

axioms ~ interface of a procedure (for theorems, ...)

An illustration.

During back substitution we obtain an equation

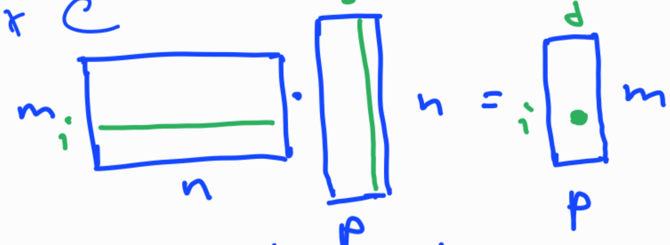
$x + 3 = 5$. What do we do?

1. $(x+3)+(-3) = 5+(-3)$ — add the inverse elem. for 3 (axiom 3)
2. $x + (3+(-3)) = 5+(-3)$ — change the order of operations (axiom 1)
3. $x + (0) = 2$ — use properties of the inverse elem. (axiom 3)
4. $x = 2$ — use properties of the neutral elem. (axiom 2)

Back to real matrices

Def: For $m \times n$ matrix A and $n \times p$ matrix B, the matrix product $A \cdot B$ is $m \times p$ matrix C

s.t. $C_{ij} = \sum_{k=1}^{n} a_{ik} \cdot b_{kj}$.



Ex. $\begin{pmatrix} 2 & 1 & 0 \\ 1 & -2 & 3 \end{pmatrix}_{2\times 3} \cdot \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}_{3\times 1} = \begin{pmatrix} 2\cdot 1 + 1\cdot 0 + 0\cdot(-1) \\ 1\cdot 1 + (-2)\cdot 0 + 3\cdot(-1) \end{pmatrix} = \begin{pmatrix} 2 \\ -2 \end{pmatrix}_{2\times 1}$

Note: $C_{*j} = A \cdot B_{*j}$ ... j-th column of C

$C_{i*} = A_{i*} \cdot B$ ... i-th row of C

Def: The transpose of $m \times n$ matrix A is the $n \times m$ matrix A^T defined by $A^T_{ji} = A_{ij}$, $\forall i,j$

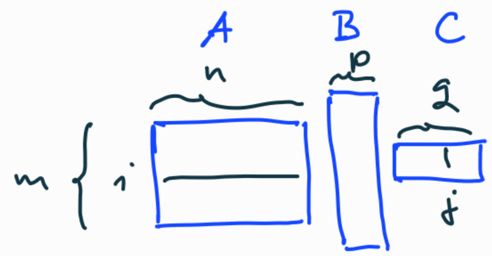
Ex. $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}^T = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}$

Def: For $n \in \mathbb{N}$, the identity matrix I_n is $n \times n$ matrix defined as $(I_n)_{ij} = \begin{cases} 1 & \text{for } i = j \\ 0 & \text{for } i \neq j \end{cases}$ Ex. $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

Proposition (properties of matrix multiplication).
For any matrices A, B, C, if all the matrix products and additions are defined, then:

1. $(A \cdot B) \cdot C = A \cdot (B \cdot C)$ associative prop.
2. $A(B+C) = A \cdot B + A \cdot C$
3. $(A+B) \cdot C = A \cdot C + B \cdot C$ (2., 3.: distributive prop.)
4. $(A \cdot B)^T = B^T \cdot A^T$
5. $A \cdot I_n = I_n \cdot A = A$

Note: not commutative: $A \cdot B \neq B \cdot A$



Proof. Part 1: $A \ldots m \times n$, $B \ldots n \times p$, $C \ldots p \times q$
Fix $i \in \{1, \ldots, m\}$, $j \in \{1, \ldots, p\}$.

$$((A \cdot B) \cdot C)_{ij} \overset{\text{def. of } \cdot}{=} \sum_{k=1}^{p} (A \cdot B)_{ik} \cdot C_{kj} \overset{\text{def. of } \cdot}{=} \sum_{k=1}^{p} \sum_{\ell=1}^{n} (A_{i\ell} \cdot B_{\ell k}) \cdot C_{kj} \overset{\text{properties of } \cdot, + \text{ for reals}}{=}$$

$$= \sum_{\ell=1}^{n} \sum_{k=1}^{p} A_{i\ell} \cdot B_{\ell k} \cdot C_{kj} = \sum_{\ell=1}^{n} A_{i\ell} \cdot \underbrace{\sum_{k=1}^{p} B_{\ell k} \cdot C_{kj}}_{(B \cdot C)_{\ell j}}$$

$$\overset{\text{def. of } \cdot}{=} (A(BC))_{ij}$$

the other parts - in a similar way - HW. $\blacksquare$

Def: A matrix B is an inverse of $n \times n$ matrix A, if $A \cdot B = I_n$. If an inverse of A exists, we denote it A^{-1} and A is called invertible.

Theorem: An $n \times n$ matrix A is invertible if and only if $\text{rank}(A) = n$. Moreover, in such case, the inverse of A is unique, and $A^{-1} \cdot A = I_n$.

Proof: $\Leftarrow$ $\text{rank}(A)=n \implies \forall i=1,\dots,n$, $Ax=e_i$ has a unique solution – denote it u^i. $\quad = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$ - i-th

Then
$$\underbrace{A\cdot\begin{pmatrix} | & | & & | \\ u^1 & u^2 & \cdots & u^n \\ | & | & & | \end{pmatrix}}_{A^{-1}} = \begin{pmatrix} | & | & & | \\ e_1 & e_2 & \cdots & e_n \\ | & | & & | \end{pmatrix} = I_n$$

i.e., A^{-1} exists and is unique.

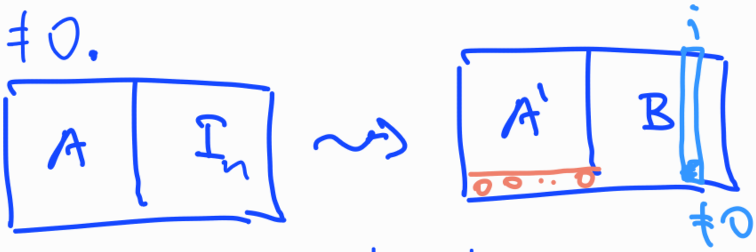
$\Rightarrow$ by contradiction. Assume A is invertible & $\text{rank}(A)<n$.

Let $(A'|B)$ be REF of $(A|I_n)$.

Then $(*)$
- the last row of A' is $(0\cdots0)$ (as $\text{rank}(A')<n$)
- the last row of B is non-zero (as $\text{rank}(B)=n$)

Let i be an index s.t. $B_{ni}\neq 0$.

By $(*)$, $Ax=e_i \cdots$ No solution (earlier theorem)



But $A\,A^{-1}_{*i} = e_i$ …there IS a solution – the i-th column of A^{-1}

– a contradiction.

Why $A^{-1}\cdot A = I_n$? (recall that in general, $A\cdot B\neq B\cdot A$)

Consider EROs: $(A|I_n)\rightsquigarrow(I_n|B)$. We observed in the proof of $\Leftarrow$ that $A^{-1}=B$. Thus, $\text{rank}(A^{-1})=\text{rank}(I_n)=n$ – A^{-1} is invertible by our THM.

$$(A^{-1})^{-1} = I\cdot(A^{-1})^{-1} = \underbrace{(A\cdot A^{-1})}_{I}\cdot(A^{-1})^{-1} \underset{\text{Proposition}}{=} A\cdot\overbrace{(A^{-1}\cdot(A^{-1})^{-1})}^{=I} \underset{\text{definition of inverse}}{=} A. \quad \blacksquare$$

Corollary: For invertible $n\times n$ matrices A, B, $\text{rank}(A\cdot B)=n$.

Proof: observe that $B^{-1}\cdot A^{-1}$ is an inverse of $A\cdot B$ as
$$(A\cdot B)\cdot(B^{-1}\cdot A^{-1}) = (A\cdot B\cdot B^{-1})\cdot A^{-1} = I \implies \text{rank}(AB)=n \quad \blacksquare$$

EROs and MATRIX MULTIPLICATION

- Scalar multiplication ... multiply row i by $k \neq 0$:

$$B = \begin{array}{cc} \begin{array}{ccccc} & & i & & \end{array} & \\ \begin{pmatrix} 1 & & \vdots & & 0 \\ & \ddots & \vdots & & \\ \cdots & \cdots & k & \cdots & \cdots \\ & & & 1 & \\ 0 & & & & 1 \end{pmatrix} & i \end{array} \qquad B \cdot A = \begin{array}{cc} \begin{pmatrix} - & A_{1*} & - \\ - & k \cdot A_{i*} & - \\ - & A_{m*} & - \end{pmatrix} & \begin{array}{c} \\ i\text{th} \\ \\ \end{array} \end{array}$$

- addition of row j to row i:

$$C = \begin{array}{cc} & \begin{array}{ccccc} & j & & & \end{array} \\ & \begin{pmatrix} 1 & \vdots & & & 0 \\ & 1 & & & \\ & \vdots & 1 & & \\ \cdots & 1 & \cdots & 1 & \cdots \\ & \vdots & 0 & & 1 \end{pmatrix} \\ i & \end{array} \qquad C \cdot A = \begin{array}{cc} \begin{pmatrix} - & A_{1*} & - \\ - & A_{j*} & - \\ - & A_{i*} + A_{j*} & - \\ - & A_{m*} & - \end{pmatrix} & \begin{array}{c} \\ j \\ i \\ \\ \end{array} \end{array}$$

$C_{kk} = 1 \ \forall k$, $C_{ij} = 1$, otherwise 0

B and C are elementary matrices.

☼ B and C are invertible.

☼ Every sequence of EROs can be expressed as multiplication (from left) by an invertible matrix.

Proof: Consider a sequence of EROs $R_1, \dots, R_k$ applied on A. Let E_i be the elementary matrix for R_i.
Then for $C = E_k \cdot \dots \cdot E_2 \cdot E_1$, $\quad E_k \cdots E_2 \cdot E_1 \cdot A = C \cdot A$
and C is invertible by ☼ & previous theorem. ∎