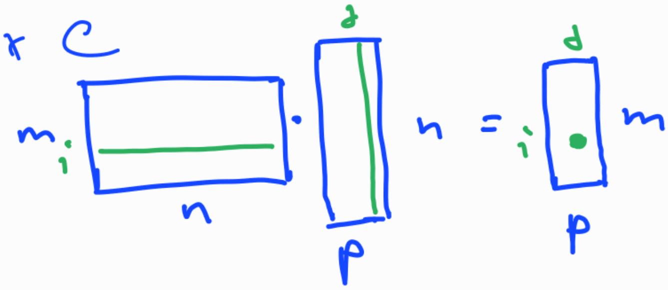
COMPUTING WITH MATRICES

LA1 30/10/25

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

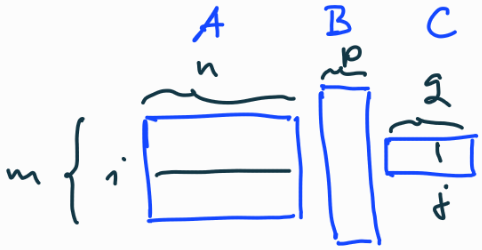
s.t. $c_{ij} = \sum_{k=1}^{n} a_{ik} \cdot b_{kj}$.



Proposition (properties of matrix multiplication).
For any matrices A, B, C of sizes $m \times n$, $n \times p$, $p \times q$, resp.:

1. $(A \cdot B) \cdot C = A \cdot (B \cdot C)$ assoc. prop.

2. . . . . .



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

Proof. Part 1: $A \dots m \times n$, $B \dots n \times p$, $C \dots p \times q$

Fix $i \in \{1, \dots, m\}$, $j \in \{1, \dots, p\}$.

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

$$= \sum_{l=1}^{n} \sum_{k=1}^{p} A_{il} \cdot B_{lk} \cdot C_{kj} = \sum_{l=1}^{n} A_{il} \cdot \underbrace{\sum_{k=1}^{p} B_{lk} \cdot C_{kj}}_{(B \cdot C)_{lj}}$$

factor out

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

the other parts - in a similar way - HW. ☒

Def: A matrix B is an inverse of $n \times n$ matrix A if $AB = I_n$.
$: A^{-1}$ $\qquad$ A : invertible.

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

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

$$\Rightarrow A\cdot \underbrace{\begin{pmatrix} | & | & & | \\ u^1 & u^2 & \cdots & u^n \\ | & | & & | \end{pmatrix}}_{A^{-1}} = \begin{pmatrix} | & | & & | \\ e_1 & e_2 & \cdots & e_n \\ | & | & & | \end{pmatrix} = I_n,$$ i.e., A^{-1} exists, is unique

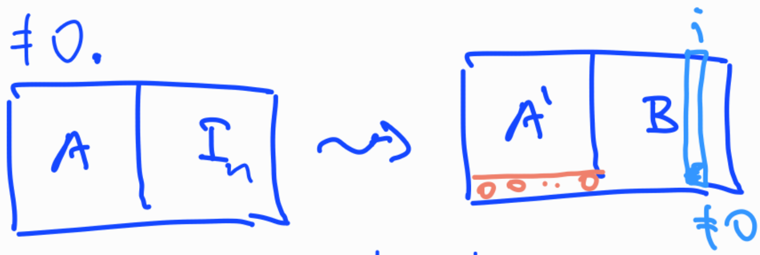
$\Rightarrow$ by contradiction. Assume A is invertible & $\mathrm{rank}(A)<n$

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

Then (*) $\begin{cases} \bullet \text{ the last row of } A' \text{ is } (0\cdots 0) & (\text{as } \mathrm{rank}(A')<n) \\ \bullet \text{ the last row of } B \text{ is non-zero} & (\text{as } \mathrm{rank}(B)=n) \end{cases}$

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

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



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

- a contradiction $\Rightarrow \mathrm{rank}(A)=n$.

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, $\mathrm{rank}(A^{-1})=\mathrm{rank}(I_n)=n$ - 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, $\mathrm{rank}(A\cdot B)=n$.

Proof: observe that $B^{-1}\cdot A^{-1}$ is an inverse of $A\cdot B$ as

$$(A\cdot B)\cdot(B^{-1}\cdot A^{-1}) \underset{\text{associativity of matrix multiplication}}{=} (A\cdot B\cdot B^{-1})\cdot A^{-1} = I \Rightarrow \mathrm{rank}(AB)=n \quad \blacksquare$$

EROs and MATRIX MULTIPLICATION

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

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

- addition of row j to row i:

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

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

B and C are called elementary matrices.

💡 B and C are invertible.

Lemma: 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 $C = E_k \cdot \cdots E_2 \cdot E_1$, $C \cdot A = E_k \cdots E_2 \cdot E_1 \cdot A$ (assoc. of multipl)
and C is invertible by 💡 & previous corollary. ∎

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

Def: A group is a pair $(G, \oplus)$ where G is a set and $\oplus$ is a binary operation on G s.t.

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

PERMUTATIONS

Def: A permutation of a set X is a bijective mapping $\pi : X \to X$.

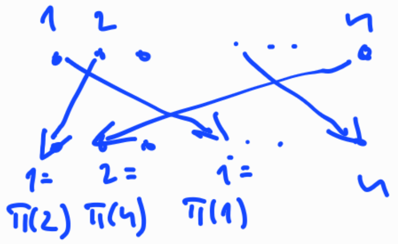
S_n ... the set of all permutations of $\{1, 2, \dots, n\}$.

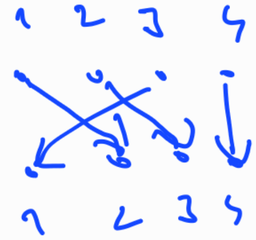
E.g. $\pi \in S_4$

Representations

- two row notation: $\begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}$ $\qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$

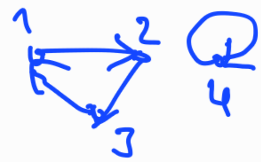
- arrow notation





- cycle notation

arrow from i to $\pi(i)$, etc.



- permutation matrix P:

$$P_{ij} = \begin{cases} 1 & \text{if } \pi(i) = j \\ 0 & \text{otherwise} \end{cases} \qquad P = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Def: Composition of permutations - as for mappings:

$p \circ q$ is defined as $p \circ q(i) = p(q(i)), \ \forall i$

For permutations p, q of X, $p \circ q$ is also a permutation of X.

Observation: $(S_n, \circ)$ is a group. $\quad$ (S_n - set, $\circ$ - composition)

Proof: Note:

- $\circ$ is a binary operation on S_n
- $\circ$ is associative (general property of mappings) (think about arrow notation)
- neutral element - identity
- inverse element for $\pi \in S_n$ - an inverse permut.

$\square$

Not a commutative group - find an example

The pair (i,j) is an inversion pair of $\pi \in S_n$ if

$i < j$ and $\pi(i) > \pi(j)$.

$I(\pi)$ ... the set of all inversion pairs of π

the sign of a permutation π: $\operatorname{sgn}(\pi) = (-1)^{|I(\pi)|} =$

$= \begin{cases} +1 & \text{for even } |I(\pi)| \\ -1 & \text{odd} \end{cases}$

transposition - a permutation π that swaps two elements and fixes all other:

i.e., $\exists\, i \neq j : \pi(i) = j,\ \pi(j) = i,\ \pi(k) = k$ for $k \neq i,j$.

<u>Def</u>: A <u>field</u> is a set T with two binary operations $(T,+,\cdot)$ on it, $+$ (addition) and $\cdot$ (multiplication) satisfying the following properties:

1. $(T,+)$ is an Abelian group, with neutral element 0; the inverse element for $\underline{a}$ is denoted $\underline{-a}$.
2. $(T\setminus\{0\},\cdot)$ is an Abelian group, with neutral element 1; the inverse element for $\underline{a}$ is denoted $\underline{a^{-1}}$.
3. $\forall a,b,c \in T$: $a\cdot(b+c) = a\cdot b + a\cdot c$ (distributive prop.)

<u>Ex.</u>: $\mathbb{R}, \mathbb{Q}, \mathbb{C}$ with standard $+, \cdot$; $\cancel{\mathbb{N}}, \cancel{\mathbb{Z}}$

$T = \{0,1\}$

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

HW: check that $(T,+,\cdot)$ is a field

The smallest field - two distinct neutral elements $0, 1$ are needed

Metatheorem: Everything we proved about real matrices holds for matrices over any field. (REF, Row reduction, ...)

Derived binary operations:

$\forall a, b \in T: \quad a - b = a + (\underset{\text{inverse for } b \text{ w.r.t. } +}{-b})$ **subtraction**

$\forall a \in T, \forall b \in T \setminus \{0\}: a/b = a \cdot (b^{-1})$ **division**

<u>Proposition</u>: 1. The elements 0 and 1 are unique.

2. $\forall a \in T$, the element $-a$ is unique, $\forall a \in T \setminus \{0\}$, a^{-1} unique.

<u>Proof</u>: 1. Assume there are neutral el. 0 and $\bar{0}$.

Then $0 = 0 + \bar{0} = \bar{0}$; similarly for 1: $1 = 1 \cdot \bar{1} = \bar{1}$.

2. Assume there are two inverse elements for a, $-a$, $\overline{-a}$:

$-a = -a + 0 = -a + (a + (\overline{-a})) = (-a + a) + (\overline{-a}) = \overline{-a}$.

for a^{-1} in the same way. $\boxtimes$