MATH 2022 Linear and Abstract Algebra

LECTURE 04 Tuesday 03/03/2020

Matrix arithmetic over a field $\mathbb{F}$:

- in First Year, matrix enties typically come from $\mathbb{R}$ or $\mathbb{C}$.

However, all usual definitions and properties work with matrix entries from any given field $\mathbb{F}$.

However, all usual definitions and properties work with matrix entries from any given field $\mathbb{F}$.

e.g. Working over $\mathbb{Z}_3$:

$$\begin{bmatrix} 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 1 & 2 \\ 2 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 1+0 & 2+1 & 0+2 \\ 2+2 & 0+1 & 1+2 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 2 \\ 1 & 1 & 0 \end{bmatrix}$$

e.g. Working over $\mathbb{Z}_3 = \{0,1,2\}$:

$$\begin{bmatrix} 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix} + \begin{bmatrix} 0 & 1 & 2 \\ 2 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 1+0 & 2+1 & 0+2 \\ 2+2 & 0+1 & 1+2 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 2 \\ 1 & 1 & 0 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix} - \begin{bmatrix} 0 & 1 & 2 \\ 2 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 1-0 & 2-1 & 0-2 \\ 2-2 & 0-1 & 1-2 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 1 \\ 0 & 2 & 2 \end{bmatrix},$$

$$2\begin{bmatrix} 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 2(1) & 2(2) & 2(0) \\ 2(2) & 2(0) & 2(1) \end{bmatrix} = \begin{bmatrix} 2 & 1 & 0 \\ 1 & 0 & 2 \end{bmatrix}.$$

e.g. Working over $\mathbb{Z}_2 = \{0,1\}$, put

$$A = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

2×4 $\qquad$ 4×2 $\qquad$ 2×3

Then

$$AB = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

2×2

e.g. Working over $\mathbb{Z}_2$, put

$$A = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

Then

$$AB = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 0 \end{bmatrix} = \underbrace{\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}}_{2\times 2},$$

$$BA = \underbrace{\begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 0 \end{bmatrix}}_{4\times 2} \underbrace{\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}}_{2\times 4} = \underbrace{\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}}_{4\times 4}$$

e.g. Working over $\mathbb{Z}_2$, put

$$A = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

Then

$$AB = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 0 \end{bmatrix} = \underbrace{\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}}_{2\times 2},$$

$$BA = \underbrace{\begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 0 \end{bmatrix}}_{4\times 2} \underbrace{\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}}_{2\times 4} = \underbrace{\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}}_{4\times 4}$$

$\boxed{\text{Note: } AB \neq BA \quad \text{(not even of the same size)}}$

e.g. Working over $\mathbb{Z}_2$, put

$$A = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

Then

$$AB = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}.$$

Further,

$$(AB)C = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix},$$

and

$$A(BC) = A\left(\begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} \right) = A \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

e.g. Working over $\mathbb{Z}_2$, put

$$A = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

Further,

$$(AB)C = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix},$$

and $\Vert$

$$A(BC) = A\left(\begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} \right) = A \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix},$$

so $(AB)C = A(BC)$

instance of associativity

e.g. Working over $\mathbb{Z}_2$, put

$$A = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

Further,

$$(AB)C = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix},$$

and

$$A(BC) = A\left(\begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} \right) = A \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix},$$

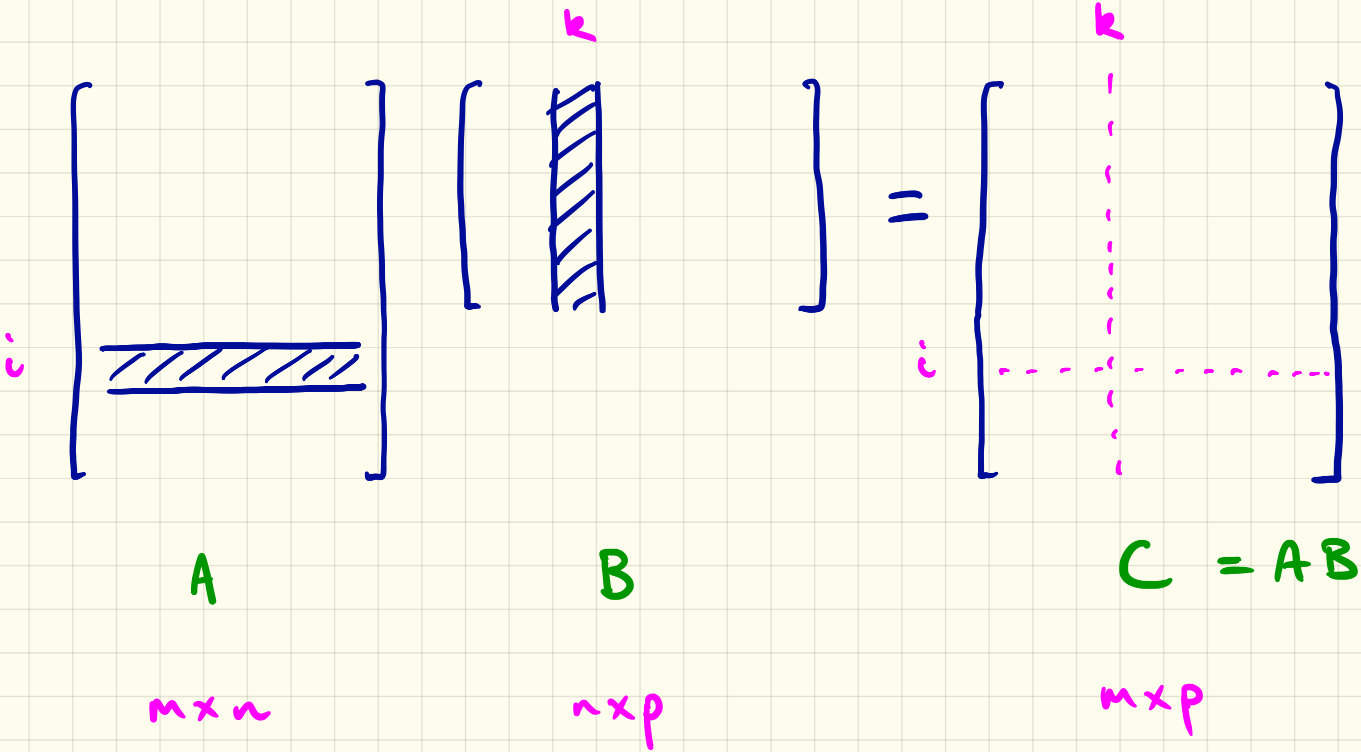
In general, let

A be $m \times n$, B be $n \times p$.

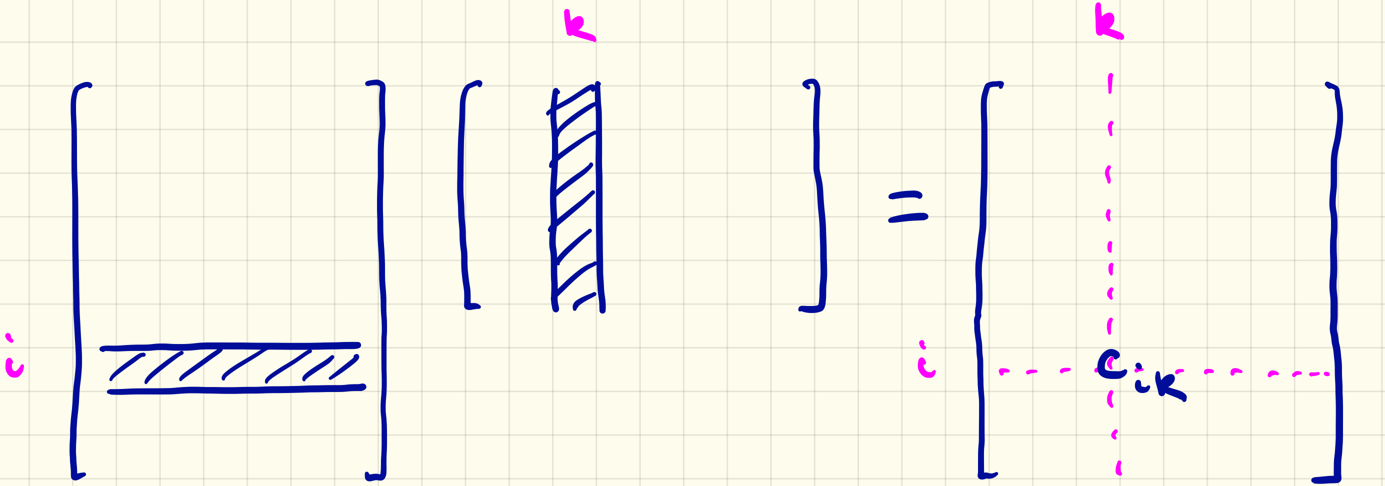
Then, the matrix product

AB is $m \times p$ the n's disappear

The (i,k)-entry of AB, for $1 \leq i \leq m$, $1 \leq k \leq p$, is the dot product of the ith row of A with the kth column of B.

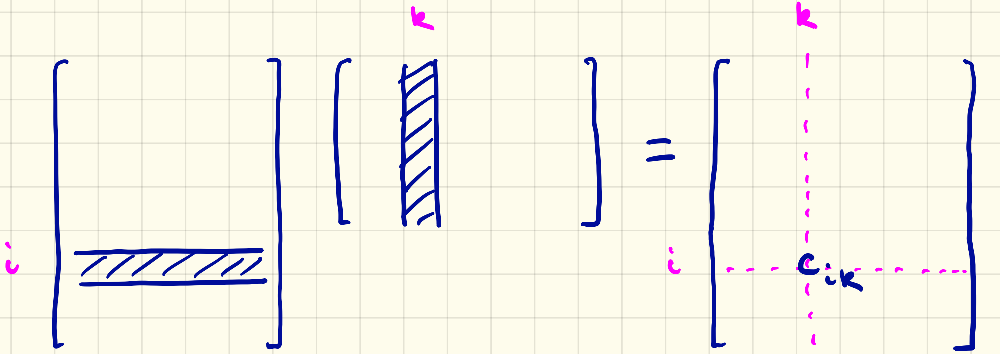


k
k
i
i
=
A
B
C = AB
m×n
n×p
m×p



A $\quad$ B $\quad$ $C = AB$

$m \times n$ $\quad$ $n \times p$ $\quad$ $m \times p$



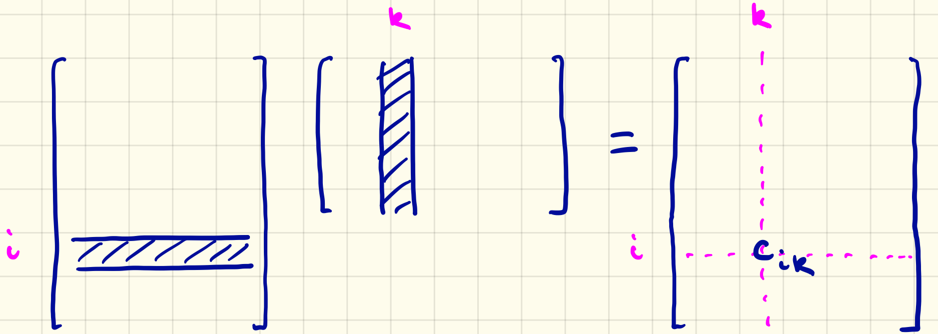
A $\qquad$ B $\qquad$ $C = AB$

$m \times n$ $\qquad$ $n \times p$ $\qquad$ $m \times p$

Let a_{ij} be the (i,j)-entry of A,

b_{jk} " " (j,k)-entry " B,

c_{ik} " " (i,k)-entry " $C = AB$.



A	B	$C = AB$
$m \times n$	$n \times p$	$m \times p$

Let a_{ij} be the (i,j)-entry of A,

b_{jk} " " (j,k)-entry " B,

c_{ik} " " (i,k)-entry " $C = AB$.

Then

$$\boxed{\begin{aligned} c_{ik} &= a_{i1} b_{1k} + a_{i2} b_{2k} + \cdots + a_{in} b_{nk} \\ &= \sum_{j=1}^{n} a_{ij} b_{jk} \quad \text{(using Sigma notation)} \end{aligned}}$$

$\boxed{\begin{array}{l}\underline{\text{Associative Law}}: \quad (AB)C = A(BC) \\ \text{when all matrix products are defined.}\end{array}}$

Proof: Let $A = [a_{ij}]$ be $m \times n$ $(1 \le i \le m,\ 1 \le j \le n)$

$B = [b_{jk}]$ be $n \times p$ $(1 \le j \le n,\ 1 \le k \le p)$

$C = [c_{k\ell}]$ be $p \times q$ $(1 \le k \le p,\ 1 \le \ell \le q)$.

Then, the (i, ℓ)-entry of $(AB)C$ is

(for $1 \le i \le m$, $1 \le \ell \le q$)

Then, the (i,ℓ)-entry of $(AB)C$ is

$\left(\text{for } 1 \le i \le m,\ 1 \le \ell \le q\right)$

$$\sum_{k=1}^{p} \Big(\underbrace{\sum_{j=1}^{n} a_{ij} b_{jk}}_{(i,k)\text{-entry of } AB} \Big) c_{k\ell} = \sum_{k=1}^{p} \Big(\sum_{j=1}^{n} (a_{ij} b_{jk}) c_{k\ell} \Big)$$

by distributivity in F

$$= \sum_{k=1}^{p} \Big(\sum_{j=1}^{n} a_{ij} (b_{jk} c_{k\ell}) \Big)$$

by associativity of $\cdot$ in F

$$\sum_{k=1}^{p} \Bigg(\underbrace{\sum_{j=1}^{n} a_{ij} b_{jk}}_{(i,k)\text{-entry of } AB} \Bigg) c_{k\ell} = \sum_{k=1}^{p} \Bigg(\sum_{j=1}^{n} (a_{ij} b_{jk}) c_{k\ell} \Bigg)$$

by distributivity in F

$$= \sum_{k=1}^{p} \Bigg(\sum_{j=1}^{n} a_{ij} (b_{jk} c_{k\ell}) \Bigg)$$

by associativity of $\cdot$ in F

$$= \sum_{j=1}^{n} \Bigg(\sum_{k=1}^{p} a_{ij} (b_{jk} c_{k\ell}) \Bigg)$$

by commutativity of $+$ in F

(and associativity also implicitly)

$$\sum_{k=1}^{p}\Big(\underbrace{\sum_{j=1}^{n} a_{ij} b_{jk}}_{(i,k)\text{-entry of } AB}\Big) c_{k\ell} = \sum_{k=1}^{p}\Big(\sum_{j=1}^{n} (a_{ij} b_{jk}) c_{k\ell}\Big)$$

by distributivity in F

$$= \sum_{k=1}^{p}\Big(\sum_{j=1}^{n} a_{ij} (b_{jk} c_{k\ell})\Big)$$

by associativity of $\cdot$ in F

$$= \sum_{j=1}^{n}\Big(\sum_{k=1}^{p} a_{ij} (b_{jk} c_{k\ell})\Big)$$

by commutativity of $+$ in F
(and associativity also implicitly)

$$= \sum_{j=1}^{n} a_{ij}\Big(\sum_{k=1}^{p} b_{jk} c_{k\ell}\Big)$$

by distributivity in F

$$\sum_{k=1}^{p}\underbrace{\left(\sum_{j=1}^{n} a_{ij}b_{jk}\right)}_{(i,k)\text{-entry of } AB} c_{kl} = \sum_{k=1}^{p}\left(\sum_{j=1}^{n}(a_{ij}b_{jk})c_{kl}\right)$$

by distributivity in F

$$= \sum_{k=1}^{p}\left(\sum_{j=1}^{n} a_{ij}(b_{jk}c_{kl})\right)$$

by associativity of $\cdot$ in F

$$= \sum_{j=1}^{n}\left(\sum_{k=1}^{p} a_{ij}(b_{jk}c_{kl})\right)$$

by commutativity of $+$ in F
(and associativity also implicitly)

$$= \sum_{j=1}^{n} a_{ij}\left(\sum_{k=1}^{p} b_{jk}c_{kl}\right)$$

by distributivity in F

which is the (i,l)-entry of $A(BC)$, proving $(AB)C = A(BC)$.

$\square$

$$\sum_{k=1}^{p}\Big(\underbrace{\sum_{j=1}^{n} a_{ij}b_{jk}}_{(i,k)\text{-entry of } AB}\Big)c_{k\ell} = \sum_{k=1}^{p}\Big(\sum_{j=1}^{n}(a_{ij}b_{jk})c_{k\ell}\Big)$$

by distributivity in F

P

$$= \sum_{k=1}^{p}\Big(\sum_{j=1}^{n} a_{ij}(b_{jk}c_{k\ell})\Big)$$

by associativity of $\cdot$ in F

D

$$= \sum_{j=1}^{n}\Big(\sum_{k=1}^{p} a_{ij}(b_{jk}c_{k\ell})\Big)$$

by commutativity of $+$ in F (and associativity also implicitly)

$$= \sum_{j=1}^{n} a_{ij}\Big(\sum_{k=1}^{p} b_{jk}c_{k\ell}\Big)$$

by distributivity in F

P^{-1}

conjugation principle

which is the (i,ℓ)-entry of $A(BC)$, proving $(AB)C = A(BC)$.

$\square$

Note: the only properties relied on were

- associativity of $+$ and $\cdot$
- and commutativity of $+$.

Thus, associativity of matrix multiplication holds for a very wide class of arithmetics of matrix entries, well beyond the class of fields.

<u>Matrix inverses</u> : Let $n \in \mathbb{Z}^+$ and put

$$I = I_n = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix},$$

the <u>identity matrix</u> (1 down the diagonal and 0 elsewhere)

Then I is the multiplicative identity element for the arithmetic

$$\mathrm{Mat}_n(F) = \{ n \times n \text{ matrices over } F \}.$$

If $A, B \in \mathrm{Mat}_n(F)$ such that

$$AB = BA = I$$

then we say that B is the <u>inverse</u> of A

and write

$$B = A^{-1}.$$

Note that B is unique with this property:

if also $AC = CA = I$ for some $C \in \mathrm{Mat}_n(F)$

then

$$C = CI = C(AB) \underset{\text{associativity}}{=} (CA)B = IB = B.$$

e.g. Working over $\mathbb{Z}_3 = \{0,1,2\}$:

$$\begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 2 & 2 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 2 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}$$

so that

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

and

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

e.g. Working over $\mathbb{Z}_3$:

$$\begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 2 & 2 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 2 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}$$

so that

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

and

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

In fact, one only has to check half of the definition:

<u>Theorem</u> (difficult): If $A, B \in \mathrm{Mat}_n(F)$ and $AB = I$ then $BA = I$, so that $A^{-1} = B$.

For 2×2 matrices, one can check that

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

provided $ad-bc \neq 0$ in F.

e.g. over $\mathbb{Z}_3 = \{0,1,2\}$:

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

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

as before ✓