MATH 2022 Linear and Abstract Algebra

LECTURE 04 Tuesday 05/03/2019

## Matrix arithmetic over a field $F$ :

- 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 $F$.

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

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 $\mathbb{Z}_3$:

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

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

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

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

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

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

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

$2 \times 4$ $\qquad$ $4 \times 2$ $\qquad$ $2 \times 3$

Then

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

$2 \times 2$

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

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

$2 \times 2$

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

$4 \times 2$ $\quad$ $2 \times 4$ $\quad$ $4 \times 4$

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

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

$2 \times 2$

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

$4 \times 2$ $\quad$ $2 \times 4$ $\quad$ $4 \times 4$

**Note:** $AB \neq BA$ (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

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

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

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 $n \times p$.

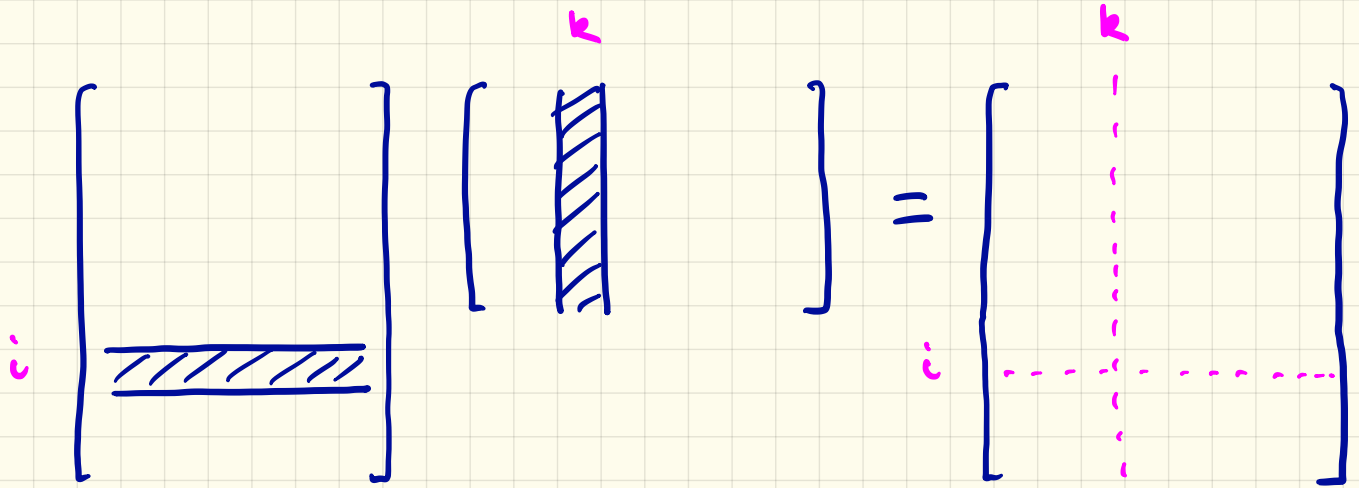
Then, the matrix product

$AB$ 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 $i$th row of $A$

with the $k$th column of $B$.




A

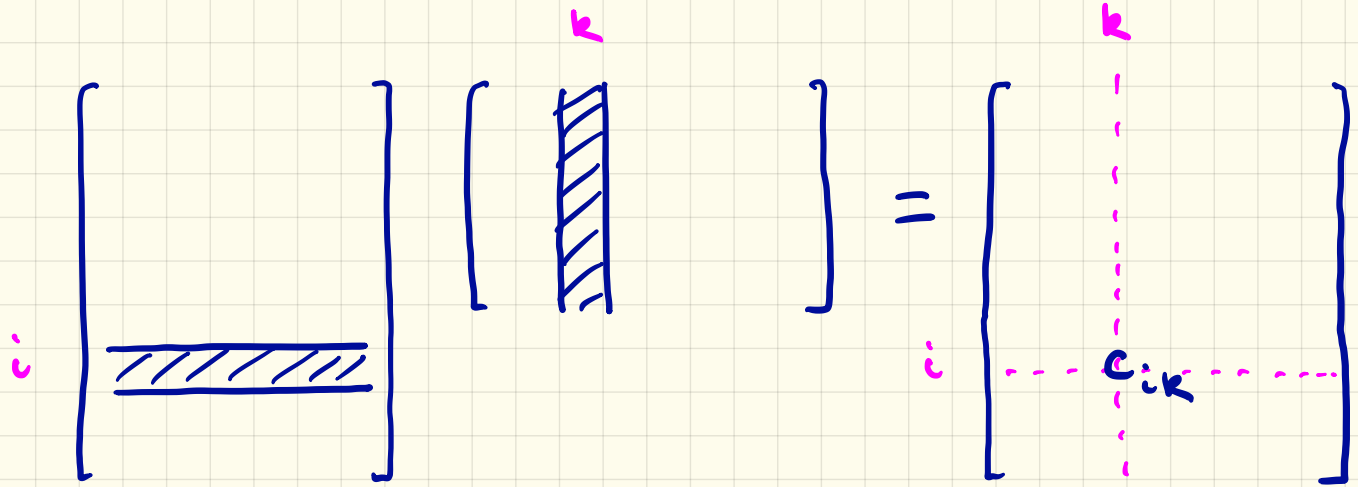
B

C = AB

m x n

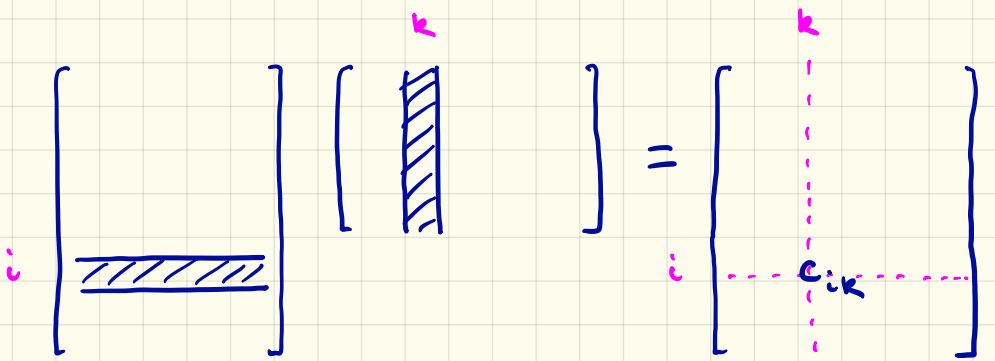
n x p

m x p




$A$ $B$ $C = AB$

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



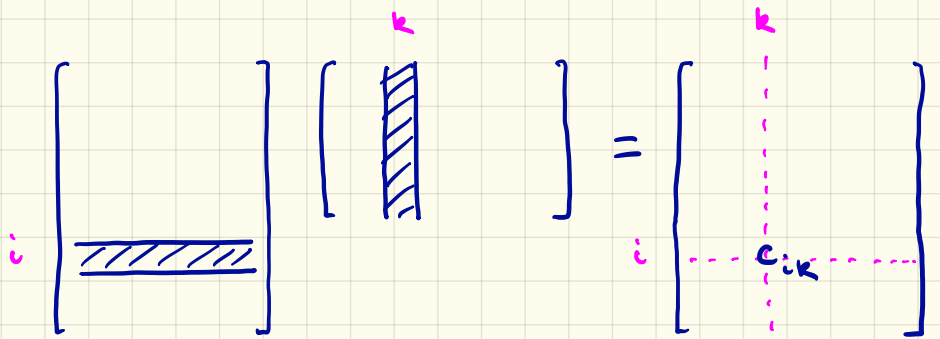

A B $C = AB$

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

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

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

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




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

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

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

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

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

Then

$$c_{ik} = a_{i1} b_{1k} + a_{i2} b_{2k} + \cdots + a_{in} b_{nk}$$

$$= \sum_{j=1}^{n} a_{ij} b_{jk} \quad \text{(using Sigma notation)}$$

**Associative Law**: $(AB)C = A(BC)$

when all matrix products are defined.

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

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

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

Then, the $(i,l)$-entry of $(AB)C$ is

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

Then, the $(i,\ell)$-entry of $(AB)C$ is

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

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

$(i,k)$-entry of $AB$

by distributivity in $F$

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

by associativity of $\cdot$ in $F$

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

$(i,k)$-entry of $AB$

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)

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

$(i,k)$-entry of $AB$

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 $F$

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

$(i,k)$-entry of $AB$

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

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

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 $F$

$P$

$D$

$P^{-1}$

conjugation principle

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

□

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.

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

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

the identity matrix (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 inverse 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

$$C = CI = C(AB) = (CA)B = IB = B.$$

associativity

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

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

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:

**Theorem** (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 $F$.

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

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

as before ✓