

Example 1: ($M_2(\mathbb{R})$) Let

$M_2(\mathbb{R})$ denote the set of all 2×2 matrices with real entries.

$$\text{Let } A = [a_{ij}]_{i,j=1}^2,$$

$$B = [b_{ij}]_{i,j=1}^2, \text{ and}$$

$$C = [c_{ij}]_{i,j=1}^2 \text{ be in } M_2(\mathbb{R}).$$

Define

$$A + B = [a_{ij} + b_{ij}]_{i,j=1}^2$$

(add the corresponding entries)

$A \cdot B$ is the 2×2 matrix

with

$$(A \cdot B)_{i,j} = (a_{i,1} b_{1,j} + a_{i,2} b_{2,j})$$

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}$$

Under these operations, $M_2(\mathbb{R})$
is a ring!

Check! Since $(\mathbb{R}, +)$ is a commutative group and addition is component-wise, $(M_2(\mathbb{R}), +)$ is a commutative group.

Let's check distributivity in
one direction:

$$A(B+C) = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \cdot \begin{bmatrix} b_{11}+c_{11} & b_{12}+c_{12} \\ b_{21}+c_{21} & b_{22}+c_{22} \end{bmatrix}$$

$$= \begin{bmatrix} (a_{11}(b_{11}+c_{11}) + a_{12}(b_{21}+c_{21})) & (a_{11}(b_{12}+c_{12}) + a_{12}(b_{22}+c_{22})) \\ (a_{21}(b_{11}+c_{11}) + a_{22}(b_{21}+c_{21})) & (a_{21}(b_{12}+c_{12}) + a_{22}(b_{22}+c_{22})) \end{bmatrix}$$

↓ multiplication distributes over
addition in \mathbb{R}

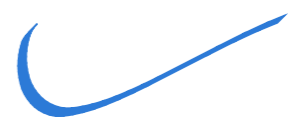
$$= \begin{bmatrix} (a_{11}b_{11} + a_{11}c_{11} + a_{12}b_{21} + a_{12}c_{21}) & (a_{11}b_{12} + a_{11}c_{12} + a_{12}b_{22} + a_{12}c_{22}) \\ (a_{21}b_{11} + a_{21}c_{11} + a_{22}b_{21} + a_{22}c_{21}) & (a_{21}b_{12} + a_{21}c_{12} + a_{22}b_{22} + a_{22}c_{22}) \end{bmatrix}$$

↓ definition of "+"
in $M_2(\mathbb{R})$

$$= \begin{bmatrix} (a_{11}b_{11} + a_{12}b_{21}) & (a_{11}b_{12} + a_{12}b_{22}) \\ (a_{21}b_{11} + a_{22}b_{21}) & (a_{21}b_{12} + a_{22}b_{22}) \end{bmatrix}$$

$$+ \begin{bmatrix} (a_{11}c_{11} + a_{12}c_{21}) & (a_{11}c_{12} + a_{12}c_{22}) \\ (a_{21}c_{11} + a_{22}c_{21}) & (a_{21}c_{12} + a_{22}c_{22}) \end{bmatrix}$$

$$= A \cdot B + A \cdot C$$



Associativity

Note that if $A \in M_2(\mathbb{R})$,

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},$$

A defines a (linear) function

$$S_A: \mathbb{R}^2 \rightarrow \mathbb{R}^2,$$

$$S_A \left(\begin{bmatrix} x \\ y \end{bmatrix} \right) = A \cdot \begin{bmatrix} x \\ y \end{bmatrix}$$

$$= \begin{bmatrix} a_{11}x + a_{12}y \\ a_{21}x + a_{22}y \end{bmatrix}$$

for $x, y \in \mathbb{R}$

If $B \in M_2(\mathbb{R})$, then

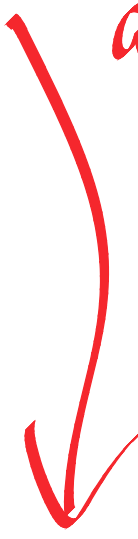
$$S_B \circ S_A = S_{BA}$$

Then associativity of matrix multiplication is equivalent to associativity of function composition, which we know to be true!

$$S_C(BA) = S_C \circ (S_{BA})$$

$$= S_C \circ (S_B \circ S_A)$$

Associativity
of function
composition



$$= (S_C \circ S_B) \circ S_A$$

$$= (S_{CB}) \circ S_A$$

$$= S_{(CB)A}$$

So $S_C(BA) = S_{(CB)A}$

$\Rightarrow C \cdot (BA) = (CB) \cdot A$

We need to prove this
last implication.

Suppose $S_A = S_B$ where

$$B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}.$$

Then if $\{e_1, e_2\}$ is the
standard basis of \mathbb{R}^2 ,

$$\begin{aligned} & (S_A e_1) \cdot e_1 \\ &= \left(\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right) \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\ &= \left(\begin{bmatrix} a_{11} \\ a_{21} \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right) \end{aligned}$$

$$= a_{11}$$

Similarly,

$$(S_A e_2) \cdot e_2 = a_{22}$$

$$(S_A e_2) \cdot e_1 = a_{12}$$

$$(S_A e_1) \cdot e_2 = a_{21}$$

If $S_A = S_B$, then $\forall i, j$

$$1 \leq i, j \leq 2,$$

$$S_A e_i = S_B e_i, \text{ and so}$$

$$(S_A e_i) \cdot e_j = (S_B e_i) \cdot e_j.$$

The left-hand side is

$b_{j,i}$ and the right-hand

side is $a_{j,i}$, so we get

$$b_{j,i} = a_{j,i} \quad \forall 1 \leq j \leq 2$$

$$\Rightarrow A = B.$$

It only remains to prove that

$$S_B \circ S_A = S_{BA}$$

We check this at the level of vectors.

$$(S_B \circ S_A) \begin{bmatrix} x \\ y \end{bmatrix}$$

$$= S_B (S_A \begin{bmatrix} x \\ y \end{bmatrix})$$

$$= S_B (A \cdot \begin{bmatrix} x \\ y \end{bmatrix})$$

$$= S_B \left(\begin{bmatrix} a_{11}x + a_{12}y \\ a_{21}x + a_{22}y \end{bmatrix} \right)$$

$$= \begin{bmatrix} b_{11}(a_{11}x + a_{12}y) + b_{12}(a_{21}x + a_{22}y) \\ b_{21}(a_{11}x + a_{12}y) + b_{22}(a_{21}x + a_{22}y) \end{bmatrix}$$

$$= \begin{bmatrix} b_{11}a_{11}x + b_{11}a_{12}y + b_{12}a_{21}x + b_{12}a_{22}y \\ b_{21}a_{11}x + b_{21}a_{12}y + b_{22}a_{21}x + b_{22}a_{22}y \end{bmatrix}$$

$$= \begin{bmatrix} (b_{11}a_{11} + b_{12}a_{21})x + (b_{11}a_{12} + b_{12}a_{22})y \\ (b_{21}a_{11} + b_{22}a_{21})x + (b_{21}a_{12} + b_{22}a_{22})y \end{bmatrix}$$

$$= \begin{bmatrix} b_{11}a_{11} + b_{12}a_{21} & b_{11}a_{12} + b_{12}a_{22} \\ b_{21}a_{11} + b_{22}a_{21} & b_{21}a_{12} + b_{22}a_{22} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

$$= (B \cdot A) \begin{bmatrix} x \\ y \end{bmatrix} = S_{BA} \begin{bmatrix} x \\ y \end{bmatrix} \quad \checkmark$$

Recall: (unital and commutative rings)

A ring R is said to be
commutative if $\forall x, y \in R,$

$$x \cdot y = y \cdot x$$

R is said to be unital

if $\exists 1_R \in R$ such that

$$1_R \cdot x = x \cdot 1_R = x$$

$\forall x \in R,$

In the case that R is unital, $x \in R$ is said to be a **unit** if $\exists y \in R$,

$$x \cdot y = y \cdot x = 1_R$$

Example 2: (a non-unital ring)

Let \mathcal{R} be the even integers. All ring-theoretic properties, such as the commutative group structure, are inherited from \mathbb{Z} .

The things we should check are that the operations are binary!

Let $x, y \in \mathcal{R}$. Then

$\exists n, m \in \mathbb{Z}$,

$$x = 2n, \quad y = 2m.$$

Then $x+y = 2n+2m = 2(n+m) \in R$

$$x \cdot y = (2n)(2m) = 2(2 \cdot n \cdot m) \in R$$

So R will be a ring.

But there does not exist

$1_R \in R$, since if $z \in R$,

$$z \cdot x = x \quad \forall x \in R,$$

write $z = 2l$ for $l \in \mathbb{Z}$.

Then

$$(2l) \cdot (2n) = 2n$$

$$(2l - 1)(2n) = 0$$

$$\Rightarrow 2l - 1 = 0$$

Since we may choose $n = 1$,

$$l = \frac{1}{2}, \quad z \notin \mathbb{R}.$$

So no such element
can exist!

Definition : (ring homomorphism / isomorphism)

Let R, S be rings. A function

$\varphi: R \rightarrow S$ is said to be a

ring homomorphism if $\forall x, y \in R,$

$$1) \varphi(x + y) = \varphi(x) + \varphi(y)$$

\uparrow addition in R \uparrow addition in S

and

$$2) \varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$$

\uparrow multiplication in R \uparrow multiplication in S

If, in addition, φ is

bijective, we say φ is

a ring isomorphism and that

R and S are isomorphic (as rings).

Definition : (field) A ring K
is said to be a **field**
if K is a commutative
ring such that every $x \in K$
with x not equal to
the additive identity is
a unit.

Familiar Fields: the rational numbers \mathbb{Q} (inverse of $\frac{a}{b}$ is $\frac{b}{a}$ for $a \neq 0$), the real numbers \mathbb{R} (inverse of x is $\frac{1}{x}$ for $x \neq 0$) and the complex numbers \mathbb{C} (inverse of $z \in \mathbb{C}$ is $\frac{1}{z}$ - but this requires complex conjugation to see that $\frac{1}{z} \in \mathbb{C}$!)