

Inherited properties

Groups

X closure - $\forall x, y \in G \quad x * y \in G$

✓ associativity - $\forall x, y, z \in G \quad (x * y) * z = x * (y * z)$

X identity - $\exists 1 \in G \quad \text{st} \quad 1 * x = x * 1 \quad \forall x \in G$

X inverses - $\forall x \in G \quad \exists x^{-1} \in G \quad \text{st} \quad x * x^{-1} = x^{-1} * x = 1$

Rings + Fields

X closure - ~~$\forall x, y \in R$~~ $\forall a, b \in R$
 $a + b \in R$ and $ab \in R$

✓ A1 - $\forall a, b \in R \quad a + b = b + a$

✓ A2 - $\forall a, b, c \in R \quad (a + b) + c = a + (b + c)$

X A3 - $\exists 0 \in R \quad \text{st} \quad a + 0 = 0 + a = a \quad \forall a \in R$

X A4 - $\forall a \in R \quad \exists -a \in R \quad \text{st} \quad a + (-a) = (-a) + a = 0$

✓ M2 - $\forall a, b, c \in R \quad (ab)c = a(bc)$

✓ D - $\forall a, b, c \in R \quad a(b+c) = ab + ac$
 $(a+b)c = ac + bc$

X M3 - $\exists 1 \in F \quad 1 \neq 0 \quad \text{st} \quad 1a = a1 = a \quad \forall a \in F$

X M4 - $\forall a \in F \quad a \neq 0 \quad \exists a^{-1} \in F \quad \text{st} \quad aa^{-1} = a^{-1}a = 1$

\exists = there exists

\forall = for all

Proofs and Counter Examples

2

In each case we give a group/field/ring and a subset S

Groups

X closure / binary op

$$G = M_{2 \times 2}(\mathbb{R}) \quad \text{op} = \text{usual matrix addition}$$

$$S = \{ A \in G \mid \det(A) = 1 \} \subseteq G$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \in S$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 2 & 0 \\ 0 & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ 0 & \frac{3}{2} \end{pmatrix} \notin S$$

maybe check
this is a group
for some
practice

Associativity

let G be a group, $H \subseteq G$ which has the same binary op (H closed under the op)

let $a, b, c \in H$

$$\Rightarrow a, b, c \in G \quad \text{as } H \subseteq G$$

$$\Rightarrow (ab)c = a(bc) \quad \text{since } G \text{ a group so associative}$$

$\uparrow \quad \uparrow$
in G

since the op of H and G are the same

$(ab)c$ and $a(bc)$ are the same in H as in G

$$\Rightarrow (ab)c = a(bc)$$

$\uparrow \quad \uparrow$
in H

$\Rightarrow H$ is associative

X identity

$G = M_{2 \times 2}(\mathbb{R})$ op = usual matrix addition

$id = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ ← Practice check

$S = \{ A \in G \mid \det A = 1 \}$

assume $\begin{pmatrix} w & x \\ y & z \end{pmatrix}$ is the id

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} w & x \\ y & z \end{pmatrix} = \begin{pmatrix} a+w & b+x \\ c+y & d+z \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

$\Rightarrow w = x = y = z = 0$

$\Rightarrow \begin{pmatrix} w & x \\ y & z \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \notin S$

X inverse

* $G = M_{2 \times 2}(\mathbb{R})$ op = usual addition

$-\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$

$S = \{ A \in G \mid \det A = 1 \}$ (as above)

S has no identity \Rightarrow no inverses

* $G = \mathbb{R}$ op = multiplication

id = 1

$a \in \mathbb{R} \setminus \{0\}$ $a^{-1} = \frac{1}{a} \in \mathbb{R}$

← we need to know the id before we can think of inverses

$\mathbb{Z} \subseteq \mathbb{R}$

id = 1 as before

$a \in \mathbb{Z}$ $a \neq 1, -1, 0$

Suppose $x = a^{-1}$

$\Rightarrow ax = 1$

$\Rightarrow |ax| = |a||x| = 1$

$\Rightarrow |x| = \frac{1}{|a|} < 1$ and $\neq 0$

because

if $x \in \mathbb{Z} \Rightarrow |x| = 0$ or $|x| \geq 1$

either proof works



$2 \in \mathbb{Z}$

$2 \cdot x = 1$

$\Rightarrow x = \frac{1}{2} \notin \mathbb{Z}$

Rings + Fields

X closure

$$S_1, S_2 \subseteq M_{2 \times 2}(\mathbb{R}) \quad \text{usual + and } \times \text{ of matrices}$$

$$S_1 = \{ A \in G \mid \det(A) = 1 \}$$

$$S_2 = \left\{ \begin{pmatrix} \lambda & 2\lambda \\ 0 & \lambda \end{pmatrix} \mid \lambda \in \mathbb{R} \right\}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \in S_1$$

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 4 \\ 0 & 2 \end{pmatrix} \in S_2$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 2 & 0 \\ 0 & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ 0 & \frac{3}{2} \end{pmatrix} \notin S_1$$

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 4 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 8 \\ 0 & 2 \end{pmatrix} \notin S_2$$

A1, A2, M2, D

These are similar to the proof of associativity for groups. Try writing your own and email them to me if you want them checked!

X A 3

↙ invertible matrices

$$S = \{ A \in M_{2 \times 2}(\mathbb{R}) \mid \det(A) \neq 0 \} \subseteq M_{2 \times 2}(\mathbb{R})$$

$$\underline{0} \text{ in } M_{2 \times 2}(\mathbb{R}) \text{ is } \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{usual + and } \times \text{ of matrices}$$

$$\text{assume } \underline{0} = \begin{pmatrix} w & x \\ y & z \end{pmatrix} \in S \quad \text{and } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in S$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} w & x \\ y & z \end{pmatrix} = \begin{pmatrix} a+w & b+x \\ c+y & d+z \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$\Leftrightarrow w = x = y = z = 0$$

$$\Leftrightarrow \begin{pmatrix} w & x \\ y & z \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\text{but } \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \notin S$$

so no additive identity

X A4

$M_{2 \times 2}(\mathbb{R})$ usual addition and multi in \mathbb{R}

$$\underline{0} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad (\text{as in A3})$$

$$\Rightarrow -\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$$

so holds in $M_{2 \times 2}(\mathbb{R})$

$$S = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \geq 0 \right\} \subseteq M_{2 \times 2}(\mathbb{R})$$

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in S$$

$$\Rightarrow \underline{0} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

remember we need to find the id before we can think of inverses

assume $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in S$ and let $\begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}$ be the inverse

$$\Rightarrow \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a+b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\Rightarrow a+b=0$$

$$\Rightarrow b = -a$$

when $a \neq 0$ $b = -a < 0$

$$\Rightarrow \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} -a & 0 \\ 0 & 0 \end{pmatrix} \notin S$$

X M3

$M_{2 \times 2}(\mathbb{R})$ usual + and \times

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \leftarrow \text{easy to check}$$

$$S = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & 2\lambda \end{pmatrix} \mid \lambda \in \mathbb{R} \right\} \subseteq M_{2 \times 2}(\mathbb{R})$$

(S is a ring (but not a field) - why not check this for some practice)

taking $\lambda = 1$ gives $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \in S$

$$\text{suppose } \exists I \in S \quad I = \begin{pmatrix} x & 0 \\ 0 & 2x \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} x & 0 \\ 0 & 2x \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & 4x \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$$

$$\Rightarrow x = 1 \quad 4x = 2$$

$$\begin{array}{c} \downarrow \\ x = \frac{1}{2} \\ \# \quad 1 \neq \frac{1}{2} \end{array}$$

$\Rightarrow S$ has no id under multiplication

X M4

\mathbb{R} usual + and \times

multi id = 1

$$a \in \mathbb{R} \quad a \neq 0 \quad a^{-1} = \frac{1}{a}$$

$$\mathbb{Z} \subseteq \mathbb{R}$$

$$x \cdot 1 = 1 = 1 \cdot x \quad \forall x \in \mathbb{Z}$$

\Rightarrow multi id = 1

now we have the id we can check inverses

$$2 \in \mathbb{Z} \quad \text{suppose } 2^{-1} = x$$

$$2 \cdot x = 1$$

$$\Rightarrow x = \frac{1}{2} \notin \mathbb{Z}$$

$\Rightarrow \mathbb{Z}$ doesn't have multiplicative inverses