

1 What requirements S must fulfil in order to become a field?

In order to show that S is a field, we'll need to prove the following *binary operator* properties:

1. In S , there are two members, zero - 0_S and one - 1_S
2. S supports the addition and multiplication binary operators
3. Every member in S can be negated, i.e. for every x there is $-x$
4. For every member in S that is not 0_S , $\exists x^{-1} \in S$, it is called the multiplicative inverse of x

In addition, the mentioned binary operators should satisfy the following properties, referred to as *field axioms*:

1. Associativity of addition(A1) and multiplication(M1):

$$a + (b + c) = (a + b) + c$$

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

2. Commutativity of addition(A2) and multiplication(M2):

$$a + b = b + a$$

$$a \cdot b = b \cdot a$$

3. Additive identity(A3) and multiplicative identity(M3)

$$a + 0 = a$$

$$a \cdot 1 = a$$

4. Additive inverse(A4) and multiplicative inverse(M4)

$$a + (-a) = 0$$

$$a \cdot a^{-1} = 1$$

5. Distributivity(D)

$$a(b + c) = (a \cdot b) + (a \cdot c)$$

2 Prove: $((a+b)+c)+d = (a+b)+(c+d) = a+(b+(c+d))$

2.1 $((a+b)+c)+d = (a+b)+(c+d)$:

First of all, we'll take a look at the left side of the equation.
We'll mark:

$$h = (a+b)$$

Therefore:

$$(h+c)+d = ((a+b)+c)+d$$

$$(h+c)+d \stackrel{(A1)}{=} h+(c+d)$$

We'll substitute h with $(a+b)$:

$$h+(c+d) = (a+b)+(c+d)$$

$$\Downarrow$$

$$((a+b)+c)+d = (a+b)+(c+d)$$

2.2 $a+(b+(c+d)) = (a+b)+(c+d)$:

We'll mark:

$$h = (c+d)$$

Therefore:

$$a+(b+h) = a+(b+(c+d))$$

$$a+(b+h) \stackrel{(A1)}{=} (a+b)+h$$

We'll substitute h with $(c+d)$:

$$(a+b)+h = (a+b)+(c+d)$$

$$\Downarrow$$

$$a+(b+(c+d)) = (a+b)+(c+d)$$

■

3 Prove: $\forall x, y \in F, x(y-z) = xy - xz$

$$x(y-z) = x(y+(-z)) \text{ (A1)}$$

$$x(y+(-z)) = (x \cdot y) + (x \cdot (-z)) \text{ (D)}$$

$$(x \cdot y) + (x \cdot (-z)) = (x \cdot y) + (-x \cdot z) = (x \cdot y) - (x \cdot z)$$

$$(x \cdot y) - (x \cdot z) = xy - xz$$

■

4 **Prove:** $\forall x, y \in F, (x + y)(x + y) = xx + xy + yx + yy$

let $h = (x + y)$ $(x + y)(x + y) = h \cdot (x + y)$
 $h \cdot (x + y) = (x \cdot h) + (y \cdot h) = x(x + y) + y(x + y)$ (D)
 $x(x + y) + y(x + y) = xx + xy + yx + yy$ (D)

■

5 **Prove:** $\forall x, y \in F, (x + y)(x - y) = xx - yy$

$(x + y)(x - y) = xx - xy + yx - yy$ (ex. 4)
 $xx - xy + yx - yy = xx + (-xy + yx) - yy$ (A1)
 $(-xy + yx) = (-xy + xy)$ (A2)
 $(-xy + xy) = 0$ (A4)
 \Downarrow
 $xx + (-xy + yx) - yy = xx + 0 - yy = xx - yy$ (A3)

■

6 **Prove:** $(a = b) \wedge (c = d) \Rightarrow (a + c = b + d) \wedge (ac = bd)$

6.1 $(a = b) \wedge (c = d) \Rightarrow a + c = b + d$:

$c = d = x$
 $a = b$
 $a + x = b + x$ (Consistency with addition)
 $a + x = a + c$ (x=c)
 $b + x = b + d$ (x=d)
 \Downarrow
 $a + c = b + d$

6.2 $(a = b) \wedge (c = d) \Rightarrow ac = bd$:

$c = d = x$
 $a = b$
 $ax = bx$ (Consistency with multiplication)
 $ax = ac$ (x=c)
 $bx = bd$ (x=d)
 \Downarrow
 $ac = bd$

■

$$\mathbf{7} \quad A = \left\{ \begin{pmatrix} 1 \\ a \end{pmatrix} \middle| a \in \mathbb{R} \right\}$$

7.1 Does A have a neutral additive member?

$$\begin{aligned} \begin{pmatrix} 1 \\ a \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 0 \end{pmatrix} &= \begin{pmatrix} 1 \\ a+0 \end{pmatrix} \\ \begin{pmatrix} 1 \\ a+0 \end{pmatrix} &= \begin{pmatrix} 1 \\ a \end{pmatrix} \quad (\mathbf{A3}) \\ \Downarrow \\ 0_A &= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{aligned}$$

7.2 Does A have a neutral multiplicative member?

$$\begin{aligned} \begin{pmatrix} 1 \\ a \end{pmatrix} \odot \begin{pmatrix} 1 \\ 1 \end{pmatrix} &= \begin{pmatrix} 1 \\ a \cdot 1 \end{pmatrix} \\ \begin{pmatrix} 1 \\ a \cdot 1 \end{pmatrix} &= \begin{pmatrix} 1 \\ a \end{pmatrix} \quad (\mathbf{M3}) \\ \Downarrow \\ 1_A &= \begin{pmatrix} 1 \\ 1 \end{pmatrix} \end{aligned}$$

7.3 Is A a field?

7.3.1 A1 - Additive Associativity

$$\begin{aligned} \left[\begin{pmatrix} 1 \\ a \end{pmatrix} \oplus \begin{pmatrix} 1 \\ b \end{pmatrix} \right] \oplus \begin{pmatrix} 1 \\ c \end{pmatrix} &\stackrel{?}{=} \begin{pmatrix} 1 \\ a \end{pmatrix} \oplus \left[\begin{pmatrix} 1 \\ b \end{pmatrix} \oplus \begin{pmatrix} 1 \\ c \end{pmatrix} \right] \\ \begin{pmatrix} 1 \\ a+b \end{pmatrix} \oplus \begin{pmatrix} 1 \\ c \end{pmatrix} &\stackrel{?}{=} \begin{pmatrix} 1 \\ a \end{pmatrix} \oplus \begin{pmatrix} 1 \\ b+c \end{pmatrix} \\ \begin{pmatrix} 1 \\ a+b+c \end{pmatrix} &= \begin{pmatrix} 1 \\ a+b+c \end{pmatrix} \\ \Downarrow \\ \left[\begin{pmatrix} 1 \\ a \end{pmatrix} \oplus \begin{pmatrix} 1 \\ b \end{pmatrix} \right] \oplus \begin{pmatrix} 1 \\ c \end{pmatrix} &= \begin{pmatrix} 1 \\ a \end{pmatrix} \oplus \left[\begin{pmatrix} 1 \\ b \end{pmatrix} \oplus \begin{pmatrix} 1 \\ c \end{pmatrix} \right] \end{aligned}$$

7.3.2 M1 - Multiplicative Associativity

$$\begin{aligned}
& \left[\begin{pmatrix} 1 \\ a \end{pmatrix} \odot \begin{pmatrix} 1 \\ b \end{pmatrix} \right] \odot \begin{pmatrix} 1 \\ c \end{pmatrix} \stackrel{?}{=} \begin{pmatrix} 1 \\ a \end{pmatrix} \odot \left[\begin{pmatrix} 1 \\ b \end{pmatrix} \odot \begin{pmatrix} 1 \\ c \end{pmatrix} \right] \\
& \begin{pmatrix} 1 \\ ab \end{pmatrix} \odot \begin{pmatrix} 1 \\ c \end{pmatrix} \stackrel{?}{=} \begin{pmatrix} 1 \\ a \end{pmatrix} \odot \begin{pmatrix} 1 \\ bc \end{pmatrix} \\
& \begin{pmatrix} 1 \\ abc \end{pmatrix} = \begin{pmatrix} 1 \\ abc \end{pmatrix} \\
& \Downarrow \\
& \left[\begin{pmatrix} 1 \\ a \end{pmatrix} \odot \begin{pmatrix} 1 \\ b \end{pmatrix} \right] \odot \begin{pmatrix} 1 \\ c \end{pmatrix} = \begin{pmatrix} 1 \\ a \end{pmatrix} \odot \left[\begin{pmatrix} 1 \\ b \end{pmatrix} \odot \begin{pmatrix} 1 \\ c \end{pmatrix} \right]
\end{aligned}$$

7.3.3 A2 - Additive Commutativity

$$\begin{aligned}
& \begin{pmatrix} 1 \\ a \end{pmatrix} \oplus \begin{pmatrix} 1 \\ b \end{pmatrix} \stackrel{?}{=} \begin{pmatrix} 1 \\ b \end{pmatrix} \oplus \begin{pmatrix} 1 \\ a \end{pmatrix} \\
& \begin{pmatrix} 1 \\ a+b \end{pmatrix} \stackrel{?}{=} \begin{pmatrix} 1 \\ b+a \end{pmatrix} \\
& \begin{pmatrix} 1 \\ a+b \end{pmatrix} = \begin{pmatrix} 1 \\ b+a \end{pmatrix} \quad (\mathbf{A2: In A}, a \in \mathbb{R}) \\
& \Downarrow \\
& \begin{pmatrix} 1 \\ a \end{pmatrix} \oplus \begin{pmatrix} 1 \\ b \end{pmatrix} = \begin{pmatrix} 1 \\ b \end{pmatrix} \oplus \begin{pmatrix} 1 \\ a \end{pmatrix}
\end{aligned}$$

7.3.4 M2 - Multiplicative Commutativity

$$\begin{aligned}
& \begin{pmatrix} 1 \\ a \end{pmatrix} \odot \begin{pmatrix} 1 \\ b \end{pmatrix} \stackrel{?}{=} \begin{pmatrix} 1 \\ b \end{pmatrix} \odot \begin{pmatrix} 1 \\ a \end{pmatrix} \\
& \begin{pmatrix} 1 \\ ab \end{pmatrix} \stackrel{?}{=} \begin{pmatrix} 1 \\ ba \end{pmatrix} \\
& \begin{pmatrix} 1 \\ ab \end{pmatrix} = \begin{pmatrix} 1 \\ ba \end{pmatrix} \quad (\mathbf{M2: In A}, a \in \mathbb{R}) \\
& \Downarrow \\
& \begin{pmatrix} 1 \\ a \end{pmatrix} \odot \begin{pmatrix} 1 \\ b \end{pmatrix} = \begin{pmatrix} 1 \\ b \end{pmatrix} \odot \begin{pmatrix} 1 \\ a \end{pmatrix}
\end{aligned}$$

7.3.5 A3 - Additive Identity

$$\begin{aligned}
& \exists \begin{pmatrix} 1 \\ a \end{pmatrix}, \begin{pmatrix} 1 \\ b \end{pmatrix} \in A \mid \begin{pmatrix} 1 \\ a \end{pmatrix} \oplus \begin{pmatrix} 1 \\ b \end{pmatrix} = \begin{pmatrix} 1 \\ a \end{pmatrix} ? \\
& \begin{pmatrix} 1 \\ a \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ a+0 \end{pmatrix} = \begin{pmatrix} 1 \\ a \end{pmatrix} \quad (\mathbf{A3: In A}, a \in \mathbb{R}) \\
& \Downarrow \\
& \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 0_A
\end{aligned}$$

7.3.6 M3 - Multiplicative Identity

$$\begin{aligned} & \exists \begin{pmatrix} 1 \\ a \end{pmatrix}, \begin{pmatrix} 1 \\ b \end{pmatrix} \in A \left| \begin{pmatrix} 1 \\ a \end{pmatrix} \odot \begin{pmatrix} 1 \\ b \end{pmatrix} = \begin{pmatrix} 1 \\ a \end{pmatrix} \right. ? \\ & \begin{pmatrix} 1 \\ a \end{pmatrix} \odot \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1a \end{pmatrix} = \begin{pmatrix} 1 \\ a \end{pmatrix} \quad (\mathbf{M3: In } A, a \in \mathbb{R}) \\ & \Downarrow \\ & \begin{pmatrix} 1 \\ 1 \end{pmatrix} = 1_A \end{aligned}$$

7.3.7 A4 - Additive Inverse

$$\begin{aligned} & \exists \begin{pmatrix} 1 \\ a \end{pmatrix}, \begin{pmatrix} 1 \\ b \end{pmatrix} \in A \left| \begin{pmatrix} 1 \\ a \end{pmatrix} \oplus \begin{pmatrix} 1 \\ b \end{pmatrix} = 0_A \right. ? \\ & \begin{pmatrix} 1 \\ a \end{pmatrix} \oplus \begin{pmatrix} 1 \\ -a \end{pmatrix} = \begin{pmatrix} 1 \\ a + (-a) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 0_A \quad (\mathbf{A4: In } A, a \in \mathbb{R}) \end{aligned}$$

7.3.8 M4 - Multiplicative Inverse

$$\begin{aligned} & \exists \begin{pmatrix} 1 \\ a \end{pmatrix}, \begin{pmatrix} 1 \\ b \end{pmatrix} \in A \left| \begin{pmatrix} 1 \\ a \end{pmatrix} \odot \begin{pmatrix} 1 \\ b \end{pmatrix} = 1_A \right. ? \\ & \begin{pmatrix} 1 \\ a \end{pmatrix} \odot \begin{pmatrix} 1 \\ \frac{1}{a} \end{pmatrix} = \begin{pmatrix} 1 \\ a \cdot \frac{1}{a} \end{pmatrix} \\ & \begin{pmatrix} 1 \\ a \cdot \frac{1}{a} \end{pmatrix} = \begin{pmatrix} 1 \\ \frac{a}{a} \end{pmatrix} \\ & \begin{pmatrix} 1 \\ \frac{a}{a} \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} = 1_A \end{aligned}$$

7.3.9 D - Distributivity

In order to display distributivity, we'll need to show the A equivalent of:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

We need to prove: $\begin{pmatrix} 1 \\ a \end{pmatrix} \odot \left[\begin{pmatrix} 1 \\ b \end{pmatrix} \oplus \begin{pmatrix} 1 \\ c \end{pmatrix} \right] \stackrel{?}{=} \begin{pmatrix} 1 \\ ab \end{pmatrix} \oplus \begin{pmatrix} 1 \\ ac \end{pmatrix}$
A's Addition property: $\begin{pmatrix} 1 \\ a \end{pmatrix} \odot \left[\begin{pmatrix} 1 \\ b \end{pmatrix} \oplus \begin{pmatrix} 1 \\ c \end{pmatrix} \right] = \begin{pmatrix} 1 \\ a \end{pmatrix} \odot \begin{pmatrix} 1 \\ b+c \end{pmatrix}$
A's Multiplication property: $\begin{pmatrix} 1 \\ a \end{pmatrix} \odot \begin{pmatrix} 1 \\ b+c \end{pmatrix} = \begin{pmatrix} 1 \\ a(b+c) \end{pmatrix}$
Since A's bottom member of the pair $\in \mathbb{R}$, we'll use Axiom D:

$$\begin{pmatrix} 1 \\ a(b+c) \end{pmatrix} = \begin{pmatrix} 1 \\ ab \end{pmatrix} \oplus \begin{pmatrix} 1 \\ ac \end{pmatrix}$$

■

8 Is B a field?

If B fulfills all 9 field's axioms, B is a field, let's check them one by one.

8.1 A1 - Additive Associativity

$$\begin{aligned}\left[\begin{pmatrix} a \\ b \end{pmatrix} \oplus \begin{pmatrix} c \\ d \end{pmatrix}\right] \oplus \begin{pmatrix} e \\ f \end{pmatrix} &\stackrel{?}{=} \begin{pmatrix} a \\ b \end{pmatrix} \oplus \left[\begin{pmatrix} c \\ d \end{pmatrix} \oplus \begin{pmatrix} e \\ f \end{pmatrix}\right] \\ \begin{pmatrix} a+c \\ b+d \end{pmatrix} \oplus \begin{pmatrix} e \\ f \end{pmatrix} &\stackrel{?}{=} \begin{pmatrix} a \\ b \end{pmatrix} \oplus \begin{pmatrix} c+e \\ d+f \end{pmatrix} \\ \begin{pmatrix} a+c+e \\ b+d+f \end{pmatrix} &= \begin{pmatrix} a+c+e \\ b+d+f \end{pmatrix}\end{aligned}$$

8.2 M1 - Multiplicative Associativity

$$\begin{aligned}\left[\begin{pmatrix} a \\ b \end{pmatrix} \odot \begin{pmatrix} c \\ d \end{pmatrix}\right] \odot \begin{pmatrix} e \\ f \end{pmatrix} &\stackrel{?}{=} \begin{pmatrix} a \\ b \end{pmatrix} \odot \left[\begin{pmatrix} c \\ d \end{pmatrix} \odot \begin{pmatrix} e \\ f \end{pmatrix}\right] \\ \begin{pmatrix} ac \\ bd \end{pmatrix} \odot \begin{pmatrix} e \\ f \end{pmatrix} &\stackrel{?}{=} \begin{pmatrix} a \\ b \end{pmatrix} \odot \begin{pmatrix} ce \\ df \end{pmatrix} \\ \begin{pmatrix} ace \\ bdf \end{pmatrix} &= \begin{pmatrix} ace \\ bdf \end{pmatrix}\end{aligned}$$

8.3 A2 - Additive Commutativity

$$\begin{aligned}\begin{pmatrix} a \\ b \end{pmatrix} \oplus \begin{pmatrix} c \\ d \end{pmatrix} &\stackrel{?}{=} \begin{pmatrix} c \\ d \end{pmatrix} \oplus \begin{pmatrix} a \\ b \end{pmatrix} \\ \begin{pmatrix} a+c \\ b+d \end{pmatrix} &\stackrel{?}{=} \begin{pmatrix} c+a \\ d+b \end{pmatrix}\end{aligned}$$

As $a, b \in \mathbb{R}$, we can use axiom A2:

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

8.4 M2 - Multiplicative Commutativity

$$\begin{aligned}\begin{pmatrix} a \\ b \end{pmatrix} \odot \begin{pmatrix} c \\ d \end{pmatrix} &\stackrel{?}{=} \begin{pmatrix} c \\ d \end{pmatrix} \odot \begin{pmatrix} a \\ b \end{pmatrix} \\ \begin{pmatrix} ac \\ bd \end{pmatrix} &\stackrel{?}{=} \begin{pmatrix} ca \\ db \end{pmatrix}\end{aligned}$$

As $a, b, c, d \in \mathbb{R}$, we can use axiom M2:

$$\begin{pmatrix} ac \\ bd \end{pmatrix} = \begin{pmatrix} ca \\ db \end{pmatrix}$$

8.5 A3 - Additive Identity

Now, we'll look for 0_B :

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

As $a, b \in \mathbb{R}$, we can use axiom A3:

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

Therefore:

$$\begin{pmatrix} 0 \\ 0 \end{pmatrix} = 0_B$$

8.6 M3 - Multiplicative Identity

Now, we'll look for 1_B :

$$\begin{pmatrix} a \\ b \end{pmatrix} \odot \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1a \\ 1b \end{pmatrix}$$

As $a, b \in \mathbb{R}$, we can use axiom M3:

$$\begin{pmatrix} 1a \\ 1b \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$$

Therefore:

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix} = 1_B$$

8.7 A4 - Additive Inverse

Now, let us find if exists a member, $\begin{pmatrix} c \\ d \end{pmatrix} \in B$, for any other member $\begin{pmatrix} a \\ b \end{pmatrix} \in B$, so that:

$$\begin{pmatrix} a \\ b \end{pmatrix} \oplus \begin{pmatrix} c \\ d \end{pmatrix} = 0_B$$

We'll start by adding the inverse of every number to itself:

$$\begin{pmatrix} a \\ b \end{pmatrix} \oplus \begin{pmatrix} -a \\ -b \end{pmatrix} = \begin{pmatrix} a+(-a) \\ b+(-b) \end{pmatrix}$$

As $a, b \in \mathbb{R}$, we can use axiom A4 to find the sum's value:

$$\begin{pmatrix} a+(-a) \\ b+(-b) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} = 0_B$$

8.8 M4 - Multiplicative Inverse

Now, let us find if exists a member, $\begin{pmatrix} c \\ d \end{pmatrix} \in B$, for any other member $\begin{pmatrix} a \\ b \end{pmatrix} \in B$, so that:

$$\begin{pmatrix} a \\ b \end{pmatrix} \odot \begin{pmatrix} c \\ d \end{pmatrix} = 1_B$$

Let's multiply every number by its multiplicative inverse:

$$\begin{pmatrix} a \\ b \end{pmatrix} \odot \begin{pmatrix} \frac{1}{a} \\ \frac{1}{b} \end{pmatrix} = \begin{pmatrix} a \cdot \frac{1}{a} \\ b \cdot \frac{1}{b} \end{pmatrix}$$

As $a, b \in \mathbb{R}$, we can use axiom M4:

$$\begin{pmatrix} a \cdot \frac{1}{a} \\ b \cdot \frac{1}{b} \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$
$$\begin{pmatrix} 1 \\ 1 \end{pmatrix} = 1_B$$

8.9 D - Distributivity

In order to display distributivity, we'll need to show the B equivalent of:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

i.e., we need to prove:

$$\begin{pmatrix} a \\ b \end{pmatrix} \odot \left[\begin{pmatrix} c \\ d \end{pmatrix} \oplus \begin{pmatrix} e \\ f \end{pmatrix} \right] = \begin{pmatrix} ac \\ bd \end{pmatrix} \oplus \begin{pmatrix} ae \\ bf \end{pmatrix}$$

First, let's solve:

$$\left[\begin{pmatrix} c \\ d \end{pmatrix} \oplus \begin{pmatrix} e \\ f \end{pmatrix} \right]$$

We use B 's binary additive operator:

$$\begin{pmatrix} c \\ d \end{pmatrix} \oplus \begin{pmatrix} e \\ f \end{pmatrix} = \begin{pmatrix} c + e \\ d + f \end{pmatrix}$$

We use B 's binary multiplicative operator:

$$\begin{pmatrix} a \\ b \end{pmatrix} \odot \begin{pmatrix} c + e \\ d + f \end{pmatrix} = \begin{pmatrix} a(c + e) \\ b(d + f) \end{pmatrix}$$

As $a, b, c, d, e, f \in \mathbb{R}$, we can use the distributivity axiom to unpack:

$$\begin{pmatrix} a(c + e) \\ b(d + f) \end{pmatrix} = \begin{pmatrix} ac + ae \\ bd + bf \end{pmatrix} = \begin{pmatrix} ac \\ bd \end{pmatrix} \oplus \begin{pmatrix} ae \\ bf \end{pmatrix}$$

■