1 What requirements S must fullfil 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 $\underline{((a+b)+c)+d = (a+b)+(c+d)}$:

let $h = (a+b)$

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

$(h+c)+d = h+(c+d)$ **(A1)**

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

$\Downarrow$

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

2.2 $\underline{a+(b+(c+d)) = (a+b)+(c+d)}$:

let $h = (c+d)$

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

$a+(b+h) = (a+b)+h$ **(A1)**

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

$\Downarrow$

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

$\blacksquare$

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

$x(y-z) = x(y+(-z))$ **(A1)**

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

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

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

$\blacksquare$

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)**

$\blacksquare$

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)**

$\blacksquare$

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

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

$c = d = x$

$a = b$

$a + x = b + x$ **(Consistency with addition)**

$a + x = a + c$ **(x=c)**

$b + x = b + d$ **(x=d)**

$\Downarrow$

$a + c = b + d$

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

$c = d = x$

$a = b$

$ax = bx$ **(Consistency with multiplication)**

$ax = ac$ **(x=c)**

$bx = bd$ **(x=d)**

$\Downarrow$

$ac = bd$

$\blacksquare$

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

7.1 Does A have a neutral additive member?

$\begin{pmatrix} 1 \\ a \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ a+0 \end{pmatrix}$

$\begin{pmatrix} 1 \\ a+0 \end{pmatrix} = \begin{pmatrix} 1 \\ a \end{pmatrix}$ **(A3)**

$\Downarrow$

$0_A = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

7.2 Does A have a neutral multiplicative member?

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

$\begin{pmatrix} 1 \\ a \cdot 1 \end{pmatrix} = \begin{pmatrix} 1 \\ a \end{pmatrix}$ **(M3)**

$\Downarrow$

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

7.3 Is A a field?

7.3.1 A1 - Additive Associativity

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

$\begin{pmatrix} 1 \\ a+b \end{pmatrix} \oplus \begin{pmatrix} 1 \\ c \end{pmatrix} \stackrel{?}{=} \begin{pmatrix} 1 \\ a \end{pmatrix} \oplus \begin{pmatrix} 1 \\ b+c \end{pmatrix}$

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

$\Downarrow$

$\left[\begin{pmatrix} 1 \\ a \end{pmatrix} \oplus \begin{pmatrix} 1 \\ b \end{pmatrix}\right] \oplus \begin{pmatrix} 1 \\ c \end{pmatrix} = \begin{pmatrix} 1 \\ a \end{pmatrix} \oplus \left[\begin{pmatrix} 1 \\ b \end{pmatrix} \oplus \begin{pmatrix} 1 \\ c \end{pmatrix}\right]$

7.3.2 M1 - Multiplicative Associativity

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

7.3.3 A2 - Additive Commutativity

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

7.3.4 M2 - Multiplicative Commutativity

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

7.3.5 A3 - Additive Identity

$$\exists\begin{pmatrix}1\\a\end{pmatrix},\begin{pmatrix}1\\b\end{pmatrix}\in A\,\middle|\,\begin{pmatrix}1\\a\end{pmatrix}\oplus\begin{pmatrix}1\\b\end{pmatrix}=\begin{pmatrix}1\\a\end{pmatrix}?$$
$$\begin{pmatrix}1\\a\end{pmatrix}\oplus\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}1\\a+0\end{pmatrix}=\begin{pmatrix}1\\a\end{pmatrix}\ \textbf{(A3: In A, } a\in\mathbb{R}\textbf{)}$$
$$\Downarrow$$
$$\begin{pmatrix}1\\0\end{pmatrix}=0_A$$

7.3.6 M3 - Multiplicative Identity

$\exists \begin{pmatrix}1\\a\end{pmatrix}, \begin{pmatrix}1\\b\end{pmatrix} \in A \middle| \begin{pmatrix}1\\a\end{pmatrix} \odot \begin{pmatrix}1\\b\end{pmatrix} = \begin{pmatrix}1\\a\end{pmatrix}?$

$\begin{pmatrix}1\\a\end{pmatrix} \odot \begin{pmatrix}1\\1\end{pmatrix} = \begin{pmatrix}1\\1a\end{pmatrix} = \begin{pmatrix}1\\a\end{pmatrix}$ **(M3: In A,** $a \in \mathbb{R}$**)**

$\Downarrow$

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

7.3.7 A4 - Additive Inverse

$\exists \begin{pmatrix}1\\a\end{pmatrix}, \begin{pmatrix}1\\b\end{pmatrix} \in A \middle| \begin{pmatrix}1\\a\end{pmatrix} \oplus \begin{pmatrix}1\\b\end{pmatrix} = 0_A?$

$\begin{pmatrix}1\\a\end{pmatrix} \oplus \begin{pmatrix}1\\-a\end{pmatrix} = \begin{pmatrix}1\\a+(-a)\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix} = 0_A$ **(A4: In A,** $a \in \mathbb{R}$**)**

7.3.8 M4 - Multiplicative Inverse

$\exists \begin{pmatrix}1\\a\end{pmatrix}, \begin{pmatrix}1\\b\end{pmatrix} \in A \middle| \begin{pmatrix}1\\a\end{pmatrix} \odot \begin{pmatrix}1\\b\end{pmatrix} = 1_A?$

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

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

$\begin{pmatrix}1\\\frac{a}{a}\end{pmatrix} = \begin{pmatrix}1\\1\end{pmatrix} = 1_A$