Fields

Definition

To say that '*' is a binary operator on a set S means $\forall a, b \in S$, the operator '*' is:

1). Closed: $a * b \in S$

2). Well-defined: $a * b = c$ and $a * b = d \implies c = d$

Definition

A field is a mathematical object consisting of a non-empty set of elements F and two binary operators called addition $(a + b)$ and multiplication $(a \cdot b = ab)$ that satisfy the following nine axioms:

A1. Additive Commutivity: $\forall a, b \in F, a + b = b + a$

A2. Additive Associativity: $\forall a, b, c \in F, (a + b) + c = a + (b + c)$

A3. Additive Identity: $\exists\, 0 \in F, \forall a \in F, a + 0 = 0 + a = a$

A4. Additive Inverse: $\forall a \in F, \exists (-a) \in F, a + (-a) = 0$

M1. Multiplicative Commutivity: $\forall a, b \in F, ab = ba$

M2. Multiplicative Associativity: $\forall a, b, c \in F, (ab)c = a(bc)$

M3. Multiplicative Identity: $\exists\, 1 \in F, \forall a \in F, a1 = 1a = a$

M4. Multiplicative Inverse: $\forall a \in F - \{0\}, \exists a^{-1} \in F, aa^{-1} = 1$

LD. Left Distribution: $\forall a, b, c \in F, a(b + c) = ab + ac$

Theorem: Right Distribution (RD)

$\forall a, b, c \in F, (a + b)c = ac + bc$

Proof

Assume $a, b, c \in F$.

$a + b \in F$	closure
$(a + b)c = c(a + b)$	M1
$(a + b)c = ca + cb$	LD
$\therefore (a + b)c = ac + bc$	M1

Theorem: Right Cancellation

1). $\forall a, b, c \in F, a + c = b + c \iff a = b$

2). $\forall a, b, c \in F, ac = bc$ and $c \neq 0 \implies a = b$

3). $\forall a, b, c \in F, a = b \implies ac = bc$

<u>Proof</u>

1). Assume $a, b, c \in F$.

$\implies$ Assume $a + c = b + c$.

$\exists(-c) \in F, c + (-c) = 0$	A4
$(a + c) + (-c) = (b + c) + (-c)$	WD
$a + (c + (-c)) = b + (c + (-c))$	A2
$a + 0 = b + 0$	A4
$\therefore a = b$	A3

$\impliedby$ Assume $a = b$.

$\therefore a + c = b + c$ WD

2). Assume $a, b \in F$ and $c \in F - \{0\}$.
Assume $ac = bc$.

$\exists c^{-1} \in F, cc^{-1} = 1$	M4
$(ac)c^{-1} = (bc)c^{-1}$	WD
$a(cc^{-1}) = b(cc^{-1})$	M2
$a1 = b1$	M4
$\therefore a = b$	M3

3). Assume $a, b, c \in F$.
Assume $a = b$.

$\therefore ac = bc$ WD

<u>Theorem: Left Cancellation</u>

1). $\forall a, b, c \in F, c + a = c + b \iff a = b$

2). $\forall a, b, c \in F, ca = cb$ and $c \neq 0 \implies a = b$

3). $\forall a, b, c \in F, a = b \implies ca = cb$

<u>Proof</u>

1). Assume $a, b, c \in F$.

$$\begin{aligned} c + a = c + b &\iff a + c = b + c \quad \text{(A1)} \\ &\iff a = b \quad \text{(RCAN)} \end{aligned}$$

2). Assume $a, b \in F$ and $c \in F - \{0\}$.
Assume $ac = bc$.

$ac = bc$	M1
$\therefore a = b$	RCAN

3). Assume $a, b, c \in F$.
Assume $a = b$.

$ac = bc$	WD
$\therefore ca = cb$	M1

Theorem: Uniqueness

1). The additive identify is unique

2). $\forall a \in F, (-a)$ is unique

3). The multiplicative identify is unique

4). $\forall a \in F - \{0\}, a^{-1}$ is unique

Proof

1). Assume that there are two: 0 and $0'$.

$a + 0 = a$	A3
$a + 0' = a$	A3
$a + 0 = a + 0'$	WD
$\therefore 0 = 0'$	LCAN

2). Assume that there are two: a' and a''.

$a + a' = 0$	A4
$a + a'' = 0$	A4
$a + a' = a + a''$	WD
$\therefore a' = a''$	LCAN

3). Assume that there are two: 1 and $1'$.

$a1 = a$	A3
$a1' = a$	A3
$a1 = a1'$	WD
$\therefore 1 = 1'$	LCAN

4). Assume that there are two: a' and a''.

$aa' = 1$	M4
$aa'' = 1$	M4
$aa' = aa''$	WD
$\therefore a' = a''$	LCAN

Properties of Zero

1). $0 = -0$

2). $\forall a \in F, a0 = 0a = 0$

3). $\forall a, b \in F, ab = 0 \iff a = 0$ or $b = 0$

Proof

1). $0 + (-0) = 0$ A4
$0 + (-0) = -0$ A3
$\therefore 0 = -0$

2). Assume $a \in F$.

$a0 \in F$	Closure
$a0 = a0 + 0$	A3
$a(0+0) = a0 + 0$	A3
$a0 + a0 = a0 + 0$	LD
$\therefore a0 = 0$	LCAN
$\therefore 0a = 0$	M1

3). Assume $a, b \in F$.

$\Longrightarrow$ Assume $ab = 0$.

AWLOG: $b \neq 0$	
$\exists b^{-1} \in F, bb^{-1} = 1$	M4
$(ab)b^{-1} = 0b^{-1}$	WD
$(ab)b^{-1} = 0$	prop of 0
$a(bb^{-1}) = 0$	M2
$a1 = 0$	M4
$\therefore a = 0$	M3

$\Longleftarrow$ AWLOG: $a = 0$

$ab = 0a = 0$ prop of 0

Properties of Negatives

1). $\forall a \in F, (-1)a = -a$

2). $\forall a \in F, -(-a) = a$

3). $\forall a, b \in F, (-a)b = -ab$

4). $\forall a, b \in F, a(-b) = -ab$

5). $\forall a, b \in F, (-a)(-b) = ab$

Proof

1). Assume $a \in F$

$a + (-1)a = 1a + (-1)a$	M3
$a + (-1)a = (1 + (-1))a$	RD
$a + (-1)a = 0a$	A4
$a + (-1)a = 0$	prop of 0
$\therefore (-1)a = -a$	uniqueness

2). Assume $a \in F$

$$\begin{array}{ll}
-(-a) + (-a) = (-1)(-a) + (-a) & \text{(1)} \\
-(-a) + (-a) = (-1)(-a) + 1(-a) & \text{M3} \\
-(-a) + (-a) = ((-1) + 1)(-a) & \text{RD} \\
-(-a) + (-a) = 0(-a) & \text{A4} \\
-(-a) + (-a) = 0 & \text{prop of 0} \\
\therefore -(-a) = a & \text{uniqueness}
\end{array}$$

3). Assume $a, b \in F$

$$\begin{array}{ll}
ab + (-a)b = (a + (-a))b & \text{RD} \\
ab + (-a)b = 0b & \text{A4} \\
ab + (-a)b = 0 & \text{prop of 0} \\
\therefore (-a)b = -ab & \text{uniqueness}
\end{array}$$

4). Assume $a, b \in F$

$$\begin{array}{ll}
ab + a(-b) = a(b + (-b)) & \text{LD} \\
ab + a(-b) = a0 & \text{A4} \\
ab + a(-b) = 0 & \text{prop of 0} \\
\therefore a(-b) = -ab & \text{uniqueness}
\end{array}$$

5). Assume $a, b \in F$

$$\begin{array}{ll}
(-a)(-b) + (-ab) = (-a)(-b) + (-a)b & \text{(3)} \\
(-a)(-b) + (-ab) = (-a)(-b + b) & \text{LD} \\
(-a)(-b) + (-ab) = (-a)0 & \text{A4} \\
(-a)(-b) + (-ab) = 0 & \text{A3} \\
\therefore (-a)(-b) = ab & \text{uniqueness}
\end{array}$$