Fields

1. Definition:

A field, f, is a set of elements with 2 operations,

1. $\oplus$ Addition
2. $\otimes$ Multiplication

2. Conditions:

A field must satisfy these 8 properties.
Let $a, b, c \in F$. Then:

1. The field is closed under addition and multiplication.

$$a \oplus b \in F$$
$$a \otimes b \in F$$

2. The field is commutative.

$$a \oplus b = b \oplus a$$
$$a \otimes b = b \otimes a$$

3. The field is associative.

$$a \oplus (b \oplus c) = (a \oplus b) \oplus c$$
$$a \otimes (b \otimes c) = (a \otimes b) \otimes c$$

4. The field is distributive.

$$a \otimes (b \oplus c) = a \otimes b \oplus a \otimes c$$

5. $\forall x \in F$, $\exists$ an element in F called the multiplicative identity, e, s.t. $x \otimes e = x$.

If $F \in \mathbb{R}$, $e = 1$

6. $\forall x \in F$, $\exists$ an element in F called the additive identity, z, s.t. $x \oplus z = x$.

If $F \in \mathbb{R}$, $z = 0$

7. $\forall x \in F$, $\exists$ an additive inverse, $-x \in F$, s.t. $x \oplus (-x) = z$.

8. $\forall x \in F$, $\exists$ a multiplicative inverse, $x^{-1} \in F$, s.t. $x \otimes (x^{-1}) = e$. Note, $x \neq z$.

3. Notations:

A set is a collection of objects.

1. R is the set of real numbers.
2. Z is the set of integers.
3. Q is the set of rational numbers
4. Zn is the set from 0 to n-1.
   E.g. $Z_3 = \{0,1,2\}$.

Note: To prove something is a field, you have to prove that it satisfies all 8 conditions.

Note: $\oplus$ and $\otimes$ are defined like this in Z_n:

1. $a \oplus b = (a+b) \bmod n$
2. $a \otimes b = (a \times b) \bmod n$

Note: Z_n is a field if n is prime.
E.g. Z_2 is a field, but Z_4 isn't.

E.g. 1 Show that $(Z_3, \oplus, \otimes)$ is a field.

$Z_3 = \{0,1,2\}$

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\otimes$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Proof Check:

1. The values of $a \oplus b$ and $a \otimes b$ are in Z_3.
2. Since the $\oplus$ and $\otimes$ tables are symmetric, Z_3 is commutative.

For 3 and 4, you need to check this using brute force.

5. $z=0$
6. $e=1$
7. From the $\oplus$ chart, we see the following:
   1. $0 \oplus 0 = 0$
   2. $1 \oplus 2 = 0 \rightarrow -1 = 2$
   3. $2 \oplus 1 = 0 \rightarrow -2 = 1$

8. From the $\otimes$ chart, we see the following:

1. $1 \otimes 1 = 1 \rightarrow 1^{-1} = 1$
2. $2 \otimes 2 = 2 \rightarrow 2^{-1} = 2$