Fields

Def.: A field $\mathbb{F}$ is a set on which two operations $+$ and $\cdot$ are defined so that for each pair of elements $x, y$ in $\mathbb{F}$ there are unique elements $x + y$ and $x \cdot y$ in $\mathbb{F}$, for which the following conditions hold for all elements $a, b, c \in \mathbb{F}$:

(F1) (Commutativity of $+$ and $\cdot$) $a + b = b + a$ and $a \cdot b = b \cdot a$

(F2) (Associativity of $+$ and $\cdot$) $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(F3) (Unitarity of $+$ and $\cdot$) There exist distinct elements $0, 1 \in \mathbb{F}$ s.t.

$0 + a = a$ and $1 \cdot a = a$

(F4) (Existence of Inverses for Addition and Multiplication) For each $a \in \mathbb{F}$ there is $a \in \mathbb{F}$ with $a + b = 0$.

For each nonzero $c \in \mathbb{F}$ there is $d \in \mathbb{F}$ with $c \cdot d = 1$

(F5) (Distributivity of $+$ and $\cdot$) $(a + b) \cdot c = a \cdot c + b \cdot c$

Examples: $\mathbb{R}$ (real numbers), $\mathbb{Q}$ (rational numbers), $\mathbb{Z}_2 = \{0, 1\}$ with

Non-examples: $\mathbb{Z}$ (integers), positive real numbers
The complex numbers

We will now define a field structure on the set of pairs of real numbers via:

\[(a, b) + (c, d) = (a + c, b + d)\]
\[(a, b) \cdot (c, d) = (ac - bd, ad + bc)\]

Let us verify that these form a field:

F1) \[(c, d) + (a, b) = (c + a, d + b) = (a + c, b + d) = (a, b) + (c, d)\]
\[(c, d) \cdot (a, b) = (ca - db, da + cb) = (ac - bd, ad + bc) = (a, b) \cdot (c, d)\]

F2) \[(a, b) + (c, d) + (e, f) = (a + c + e, b + d + f) = (a, b) + ((c, d) + (e, f))\]
\[= (a, b) + (c, d) + (e, f) = (ace - bde - adf - bcf, acf - bdf + ade + bce)\]
\[= (a, b) + ((c, d) + (e, f)) = (a, b) - ((ce - df, cf + de))\]
\[= (ac - adf - bcf - bde, acf + ade + bce - bdf)\]

The same

F3) The additive inverse of \((a, b)\) is \((-a, -b)\).
\[(a, b) + (0, 0) = (a, b)\]
\[(a, b) + (0, 0) = (a, b)\]

F4) The additive inverse of \((a, b)\) is \((-a, -b)\).

The multiplicative inverse of \((a, b) \neq (0, 0)\) is \[
\left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\right) = \left(\frac{ab - ba}{a^2 + b^2}, \frac{-ab + ba}{a^2 + b^2}\right) = (1, 0) = 1
\]
\[(a, b) + (c, d) \cdot (e, f) = (ae + ce - bf - df, af + cf + be + de)\]

Def.: A subset \( S \) of a field \( F \) is called a subfield if

1) \( a + b \in S \) for \( a, b \in S \)
2) \( a \cdot b \in S \) for \( a, b \in S \)
3) \( -a \in S \) for \( a \in S \)
4) \( \frac{1}{a} \in S \) for \( a \in S \)
5) \( 0, 1 \in S \)

Remark: A subfield of a field is a field.

Examples: \( \mathbb{Q} \subseteq \mathbb{R} \)
\( \mathbb{R} \subseteq \mathbb{C} \) (\( \subseteq \) complex numbers)
\( \exists (a, 0) \mid a \in \mathbb{R} \)

HW: \( \exists a + b \cdot \mathbb{R}^2 \mid a, b \in \mathbb{Q}^2 \subseteq \mathbb{R} \).