

0.0 Fields

Definition 0.4.1 (Field). A set F is called a **field** if we can define two binary operations addition $+$, and multiplication \cdot

$$+ : F \times F \rightarrow F, \quad \cdot : F \times F \rightarrow F$$

such that:

- (F1) $a + b = b + a$
- (F2) $(a + b) + c = a + (b + c)$
- (F3) There exists $0 \in F$ such that $a + 0 = a$.
- (F4) For every $a \in F$, there exists $-a \in F$ such that $a + (-a) = 0$.
- (F5) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- (F6) $a \cdot b = b \cdot a$
- (F7) There exists $1 \in F$ such that $1 \neq 0$ and $a \cdot 1 = a$.
- (F8) For every $a \in F \setminus \{0\}$, there exists $a^{-1} \in F$ such that $a \cdot a^{-1} = 1$.
- (F9) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

Remark. We can shorten “ F is a field with operations $+$ and \cdot ” to “ $(F, +, \cdot)$ is a field”. Moreover when the context of $+$ and \cdot is clear, we simply say “ F is a field”, which we will do most of the time in this book.

Example (Examples of Fields).

1. \mathbb{R} is a field.
2. \mathbb{C} is a field.
3. $\mathbb{Q} = \left\{ \frac{p}{q} : p, q \in \mathbb{Z}, \gcd(p, q) = 1 \right\}$ is a field.
4. \mathbb{Z} is **not** a field since **(F8)** fails.
5. $M_n(\mathbb{R})$ is **not** a field since **(F6)** fails.

Example (Finite Fields). Let \mathbb{F}_n be the finite field with n elements. Then $(\mathbb{F}_2, +, \cdot)$ is defined to be:

$$\mathbb{F}_2 = \{0, 1\}, \quad \begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}, \quad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}.$$

Then one can verify that $(\mathbb{F}_2, +, \cdot)$ is a field.