Lecture 1

\[ \mathbb{R} \text{ is a commutative field} \]

\((G, \circ)\) is a set \(G\) with an operation \(\circ\) on \(G\), i.e. to any pair \(x, y \in G\) we associate a unique \(z = x \circ y\).

In other words, \(\circ\) is a function from \(G \times G\) into \(G\).

\[ G = \mathbb{Z}, \quad \circ = + \quad \text{all are} \]
\[ \circ = - \quad \text{well defined}, \]
\[ \circ = \cdot. \]

**Definition** \((G, \circ)\) is a group if

\(91\) \(x \circ (y \circ z) = (x \circ y) \circ z\) (associativity)

\(92\) \(\exists e \in G \quad \forall x \in G \quad x \circ e = e \circ x = x\) (\(e\) is said the neutral element)

\(93\) \(\forall x \in G \exists y \in G \quad x \circ y = y \circ x = e\) \(y \neq x^{-1}\) or \(-x\) the inverse of \(x\) wrt \(\circ\).
(g4) \( + x, y \in G \) \( x + y = y + x \)

(commutativity).

\((G, \circ)\) with \((g1) - (g4)\) is said a commutative group.

Examples:

1. \((\mathbb{Z}, +)\) \((\mathbb{Q}, +)\) \((\mathbb{R}, +)\)
2. \((\mathbb{Q}^*, \cdot)\) \((\mathbb{R}^*, \cdot)\)

where \(\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}\) \(\mathbb{R}^* = \mathbb{R} \setminus \{0\}\)

+ the usual addition

\(\circ\) the usual multiplication

(3) \(S_n = \{\sigma \in \{1, 2, \ldots, n\} \rightarrow \{1, 2, \ldots, n\}\ \text{one-to-one and onto}\}

with \(\circ = \circ\) (composition).

(4) \(Q(\sqrt{2}) = \{p + q\sqrt{2} \mid p, q \in \mathbb{Q}\}\)

with both \(+\) and \(\circ\) \((\text{after omitting zero})\)

(5) \(Q^2, \mathbb{Z}^2, \mathbb{R}^2 = \mathbb{R} \times \mathbb{R}\) with \(\) componentwise.
Definition \((G_1, +, \cdot)\) is a commutative field if

\[ x + (y + z) = (x + y) + z \]

\[ \forall x \quad x + 0 = 0 + x = x \quad (G_1, +) \quad \text{group} \]

\[ \forall x \quad x + (-x) = (-x) + x \]

\[ \forall x, y \quad x + y = y + x \]

\[ \forall x, y, z \quad x \cdot (y + z) = x \cdot y + x \cdot z \]

This is called distributivity of \(\cdot\) wrt + and relates the two operations in a consistent way.

\[ \forall 1 \quad x \cdot 1 = 1 \cdot x = x \quad (G_1^*, \cdot) \quad \text{group} \]

\[ \forall x \neq 0 \quad \exists x^{-1} \quad x \cdot x^{-1} = x^{-1} \cdot x = 1 \]

\[ \forall x, y \quad x \cdot y = y \cdot x \]

Note: \(x \cdot y\) is defined including for \(x = 0\) or \(y = 0\)

\[ \forall x, y, z \quad x \cdot (y + z) = x \cdot y + x \cdot z \]
Remark
\( (y+z) \cdot x = y \cdot x + z \cdot x \)
from distributivity and commutativity combined.

\( 0 \cdot x = 0 \) because

\[
\begin{align*}
(0+0) \cdot x &= 0 \cdot x + 0 \cdot x \\
&= 0
\end{align*}
\]

\( 0 \cdot x = 0 \)

Examples
1. \( (\mathbb{Q}, +, \cdot) \)
2. \( (\mathbb{Q}[\sqrt{2}], +, \cdot) \)
3. \( (\mathbb{C}, +, \cdot) \) complex numbers
4. \( (\mathbb{R}, +, \cdot) \)
5. \( (\mathbb{Z}, +, \cdot) \) Not true
6. \( (\mathbb{Z}_{p^*}, +, \cdot) \) if \( p \) prime

where \( \mathbb{Z}_p = \{0, 1, \ldots, p-1\} \) the class of remainders mod \( p \).