Lecture 1

– $\mathbb{R}$ is a commutative field

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

In other words, $\odot$ is a function from $G \times G$ into G.

$G = \mathbb{Z}$, $\odot = +$, $\odot = -$, $\odot = \cdot$ all are well defined.

<u>Definition</u> $(G, \odot)$ is a group if

(g1) $x \odot (y \odot z) = (x \odot y) \odot z$ (associativity)

(g2) $\exists\, e \in G \quad \forall x \in G \quad x \odot e = e \odot x = x$
(e is said the <u>neutral element</u>)

(g3) $\forall x \in G \quad \exists\, y \in G \quad x \odot y = y \odot x = e$

$y \overset{\text{not}}{=} x^{-1}$ or $-x$ the inverse of x wrt $\odot$.

(g4) $\forall x, y \in G \quad x + y = y + x$

(commutativity).

$(G, \odot)$ 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

$\cdot$ the usual multiplication

(3) $S_n = \{\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ one-to-one and onto $\}$

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

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

with both $+$ and $\cdot$ (after omitting zero)

(5) $\mathbb{Q}^2$, $\mathbb{Z}^2$, $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ with $+$ componentwise.

<u>Definition</u> $(G, +, \cdot)$ is a <u>commutative field</u> if

$\forall x, y, z \quad x + (y+z) = (x+y) + z$

$\exists 0 \ \forall x \quad x + 0 = 0 + x = x$ $\quad (G, +)$ group.

$\forall x \ \exists (-x) \quad x + (-x) = (-x) + x$

$\forall x, y \quad x + y = y + x$

$\forall x, y, z \quad x \circ (y \circ z) = (x \circ y) \circ z$

$\exists 1 \ \forall x \quad x \cdot 1 = 1 \cdot x = x$ $\quad (G^*, \cdot)$ group

$\forall x \neq 0 \ \exists x^{-1} \quad x \cdot x^{-1} = x^{-1} \cdot x = 1$ $\quad G^* = G \setminus \{0\}$

$\forall x, y \quad x\,y = y\,x$

<u>Note</u> $x \circ y$ is defined including for $x = 0$ or $y = 0$

$\forall x, y, z \quad x \circ (y + z) = x \cdot y + x \cdot z$

This is called <u>distributivity</u> of $\circ$ wrt $+$ and relates the two operations in a consistent way.

<u>Remark</u> • $(y+z)\cdot x = y\cdot x + z\cdot x$

from distributivity and commutativity combined.

• $0\cdot x = 0$ because

$$\underbrace{(0+0)}_{0}\cdot x = 0\cdot x + 0\cdot x$$

$$\Downarrow$$

$$0\cdot x = 0 \checkmark$$

<u>Examples</u> (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.