Sets

$N = \{1, 2, 3, --\}$

$\mathbb{Z} = \{-1, 0, 1, 2, 3 ---\}$

$\mathbb{Q} = \{\frac{m}{n} \mid m, n \in \mathbb{Z},\ n \neq 0\}$

$\mathbb{Z}$ is not just a set there are operations like $+, -, \times, \div$ that satisfies the property like

$$(2+5)+3 = 2+(5+3)$$
$$0+7 = 7$$
$$7+(-7) = 0$$

$\mathbb{Z}$ with $+$ is a group

Def A group G is a set together with an operation $\circ$ which satisfies

① closure $\forall$ (for all) $a, b \in G$, $a \circ b \in G$

② associativity $(a \circ b) \circ c = a \circ (b \circ c)$, $\forall a, b, c \in G$

③ (identity) $\exists\ e \in G$ s.t $a \circ e = e \circ a = a$

④ inverse $\forall\ a \in G$, $\exists\ b \in G$ s.t $a \circ b = e$

$(N, +)$ is not a group (no inverse, no identity) remark ⇒ a group that satisfies another property namely that $a \circ b = b \circ a$ is called a commutative group.

eg ⇒ $(\mathbb{Z}, +)$ is a commutative group.

remark ⇒ matrix mult. is not commutative ;
~~Subs~~ Substraction in $\mathbb{Z}$ is not comm. $(1-3)-2 \neq 1-(3-2)$

ex ⇒ $(\mathbb{Z}, \times)$ is not a group

inverse ⇒ not exist

$a \to \frac{1}{a} \notin \mathbb{Z}$

eg ⇒ $(\mathbb{Q}, +)$ is a comm group

($\mathbb{Q}$ without 0, $\times$) is a comm group.

moreover, + and $\times$ are related by distributivity ⇒ $4 \times (3+5) = (4 \times 3) + (4 \times 5)$

Q is a field so are real no. $\mathbb{R}$, and the complex no. $\mathbb{C}$

Fields ⇒ Def ⇒ A set F with two operations $+, \cdot$ is called a field if the following hold.

① $\forall a, b \in F, a+b \in F$

closure

② $\forall a, b, c \in F, (a+b)+c = a+(b+c)$

assoc

③ $\exists\, 0 \in F$ s.t $a+0 = a, \forall a \in F$

identity

④ $\forall a \in F, \exists\, (-a) \in F$ s.t $a+(-a) = 0$

inverse

⑤ $\forall a, b \in F, a+b = b+a$

comm

⑥ $\forall a, b \in F, a \cdot b \in F$

⑦ $\forall a, b, c \in F, (a \cdot b) \cdot c = a \cdot (b \cdot c)$

⑧ $\exists\, 1 \in F$ s.t $a \cdot 1 = a, \forall a \in F$

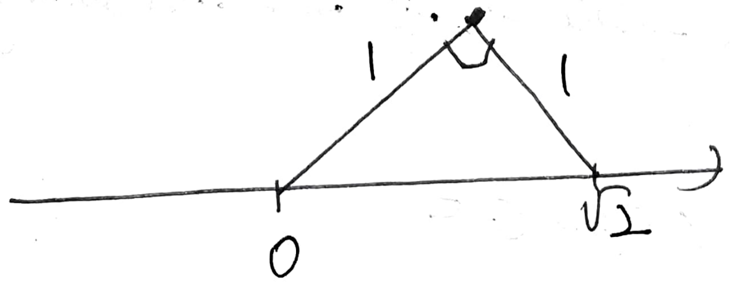
⑨ $\forall a \neq 0\ \exists\, a^{-1} \in F$ s.t $a \cdot a^{-1} = 1$

⑩ $\forall a, b \in F, a \cdot b = b \cdot a$

⑪ $\forall a, b, c \in F, a \cdot (b+c) = (a \cdot b) + (a \cdot c)$

D1.

(ex) $(\mathbb{Q}, +, \cdot)$ is a field (verify)



$\mathbb{R} = \{x \mid -\infty < x < \infty\}$ real

$\pi \in \mathbb{R}$, $\pi \notin \mathbb{Q}$, $\pi \in \mathbb{R} \setminus \mathbb{Q}$

remarks: 1. $\mathbb{R}$ is a field.

2. $\{0\}$ satisfies all 11 axioms, but usually we ~~requi~~ require that in a field $0 \neq 1$

3. there are more fields:

$\mathbb{C}$ — the complex no.

$\mathbb{Z}_n$ — fields (n is prime no)

More properties of fields ⇒

theorem → Let F be a field. Then:

1. 0 is unique, 1 is unique
2. $-a$ is unique, a^{-1} is unique
3. $a \cdot 0 = 0$

④ $\forall a, b \in F$, if $a \cdot b = 0$ then $a = 0$ or $b = 0$

⑤ $(-1) \cdot a = -a$

⑥ if $a + b = a + c$ then $b = c$

⑦ if $a \cdot b = a \cdot c$ then $b = c$ $(a \neq 0)$

Some proofs ① 0 is unique

suppose there twice zero elements: $0, \hat{0}$

$$\hat{0} = \hat{0} + 0 = 0 + \hat{0} = 0$$

③ $a \cdot 0 = 0$

proof $a \cdot 0 = a \cdot (0 + 0) = (a \cdot 0) + (a \cdot 0)$

(A-4) $\therefore$ $(a \cdot 0) + (-(a \cdot 0)) = 0$

$(a \cdot 0) + ((a \cdot 0) + (-(a \cdot 0))) = 0$

$\cancel{(a \cdot 0) = 0}$

$(a \cdot 0) + 0 = (a \cdot 0).$

④ $a \cdot b = 0$ lets suppose $a \neq 0$

$0 = a^{-1}(a \cdot b) = (a^{-1} a) b \Rightarrow$

$b = 0$