Math 4550
8/20/25

TOPIC 1 - Groups

Def: A group $\langle G, * \rangle$ is a set G with a binary operation $*$ such that four properties hold:

① (closure) If $a, b \in G$, then $a * b \in G$.

② (associativity) If $a, b, c \in G$, then $a * (b * c) = (a * b) * c$

③ (identity element) There exists an identity element $e \in G$ such that $a * e = a$ and $e * a = a$ for all $a \in G$.

④ (inverses) If $a \in G$, then there exists $b \in G$ where $a * b = e$ and $b * a = e$

Ex: $\langle \mathbb{Z}, + \rangle$ is a group where

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

is the set of integers.

① If $a, b \in \mathbb{Z}$, then $a + b \in \mathbb{Z}$. ✓

② If $a, b, c \in \mathbb{Z}$, ✓

then $a+(b+c)=(a+b)+c$

---

(3) Let $e=0$.

And $0+a=a=a+0$ for all $a\in\mathbb{Z}$ ✓

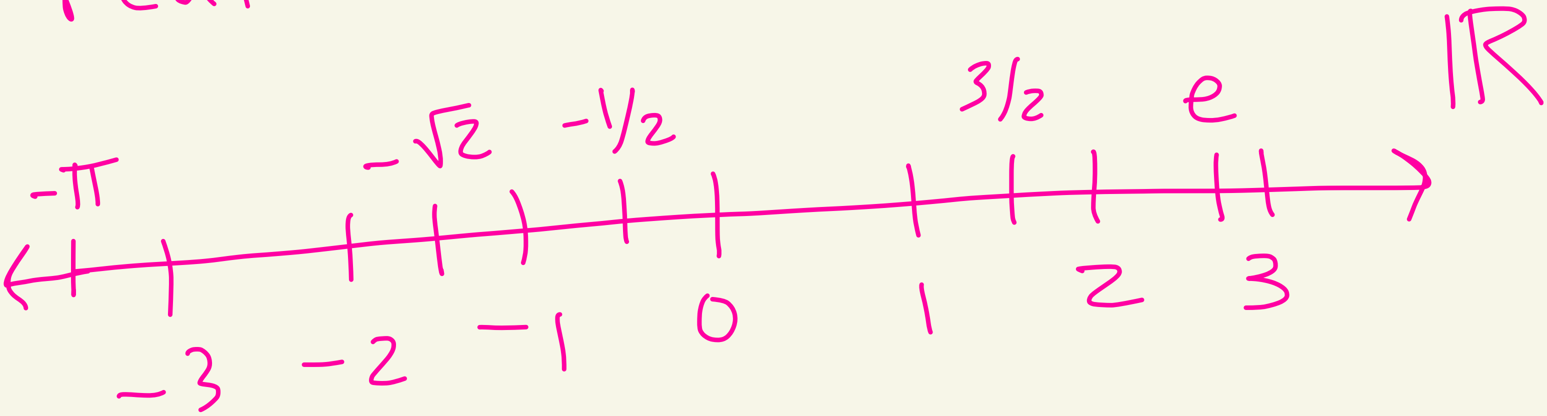
---

(4) Let $a\in\mathbb{Z}$.

Then, $-a\in\mathbb{Z}$ and $a+(-a)=0=(-a)+a$ ✓

$\blacksquare$

Ex: $\langle \mathbb{R}, + \rangle$ is a group where $\mathbb{R}$ is the set of real numbers.



1. ✓
2. ✓
3. $e = 0$
4. $a \in \mathbb{R}$, the inverse is $-a$

Ex: Is $\langle \mathbb{R}, \cdot \rangle$ a group?

multiplication

① If $a, b \in \mathbb{R}$, then $a \cdot b \in \mathbb{R}$. ✓

② If $a, b, c \in \mathbb{R}$, then $a(bc) = (ab)c$ ✓

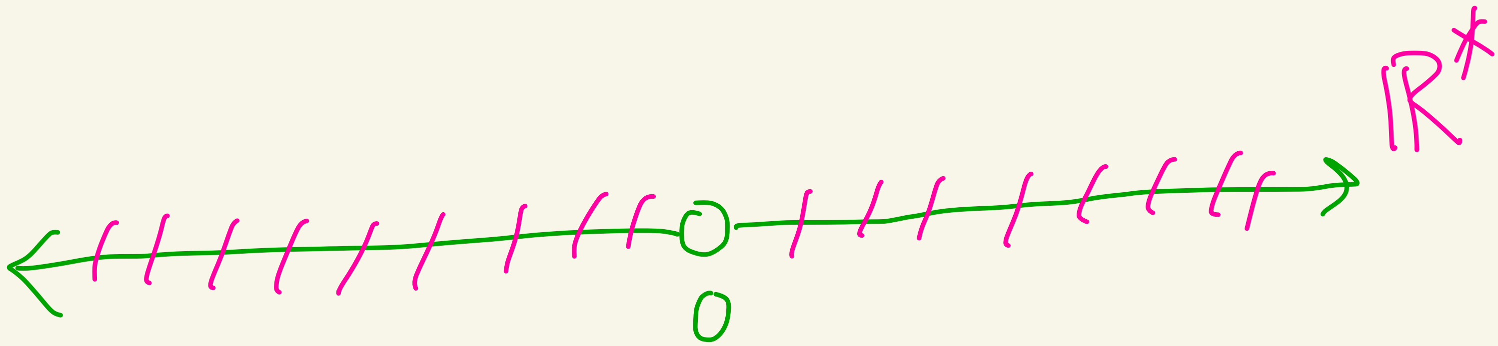
③ Set $e = 1$. Then $a \cdot 1 = a = 1 \cdot a$ for all $a \in \mathbb{R}$ ✓

④ $0 \in \mathbb{R}$ but there is no $b \in \mathbb{R}$ where $0 \cdot b = \underbrace{1}_{\text{identity } e}$. ✗

No, $\mathbb{R}$ is <u>not</u> a group under multiplication.

Ex: $\langle \mathbb{R}^*, \cdot \rangle$ is a group

where $\mathbb{R}^* = \mathbb{R} - \{0\}$



① Let $a, b \in \mathbb{R}^*$.

Then, $a, b \in \mathbb{R}$ and $a \neq 0, b \neq 0$.

So, $ab \in \mathbb{R}$ and $ab \neq 0$

Thus, $ab \in \mathbb{R}^*$.

② Let $a, b, c \in \mathbb{R}^*$ then

$a(bc) = (ab)c$.

③ Let $e = 1$.

Then $e \in \mathbb{R}^*$ and

$a \cdot 1 = a = 1 \cdot a$ for every $a \in \mathbb{R}^*$

(4) Let $a \in \mathbb{R}^*$.

Then, $a \in \mathbb{R}$ and $a \neq 0$.

Let $b = \frac{1}{a}$.

Then, $b \in \mathbb{R}^*$ because $b \neq 0$.

And $ab = a \cdot \frac{1}{a} = 1$

$ba = \frac{1}{a} \cdot a = 1$.

By (1) – (4), $\mathbb{R}^*$ is a group under multiplication. $\blacksquare$

Def: A group $\langle G, * \rangle$ is called **abelian** if $a * b = b * a$ for every $a, b \in G$.

Ex: $\langle \mathbb{Z}, + \rangle$ ← $\boxed{a+b=b+a}$

$\langle \mathbb{R}, + \rangle$ ←

$\langle \mathbb{R}^*, \cdot \rangle$ ← $\boxed{ab=ba}$

The above are all abelian.

Ex: The set of rational numbers

$$\mathbb{Q} = \left\{ \frac{a}{b} \;\middle|\; a, b \in \mathbb{Z}, b \neq 0 \right\}$$

is an abelian group under $+$.

Starting integers modulo n

Def: Let $a, b \in \mathbb{Z}$. We say that a *divides* b if there exists $k \in \mathbb{Z}$

where $b = ak$.

If this is so, then we write $\underbrace{a \mid b}$.

read: "a divides b"

Ex: $3 \mid (-12)$

because $-12 = (3)\underbrace{(-4)}_{k}$
