2550

Vectors ← vector space

Scalars/numbers ← field

Def: A **field** F is a set with two binary operations denoted by $+$ and $\cdot$, such that the following are true:

(F1) For every $a, b \in F$ there exist unique elements $a+b$ and $a \cdot b$ in F. (closure property)

(F2) For every $a, b, c \in F$ we have

$a+b=b+a$	$(a+b)+c=a+(b+c)$	$a\cdot(b+c)=a\cdot b+a\cdot c$
$a\cdot b=b\cdot a$	$(a\cdot b)\cdot c=a\cdot(b\cdot c)$	$(b+c)\cdot a=b\cdot a+c\cdot a$
[commutative properties]	[associative properties]	[distributive properties]

additive and multiplicative identities

F3 There exist elements 0 and 1 in F where

$$x + 0 = 0 + x = x$$

and $x \cdot 1 = 1 \cdot x = x$

for all $x \in F$.

additive inverses

F4 For every $a \in F$ there exists some $b \in F$ where $a + b = b + a = 0$.

multiplicative inverses

F5 For every $a \in F$ where $a \neq 0$ there exists $c \in F$ where $a \cdot c = c \cdot a = 1$

$\boxed{\text{End of definition}}$

Notes:

- In HW 1 you show that

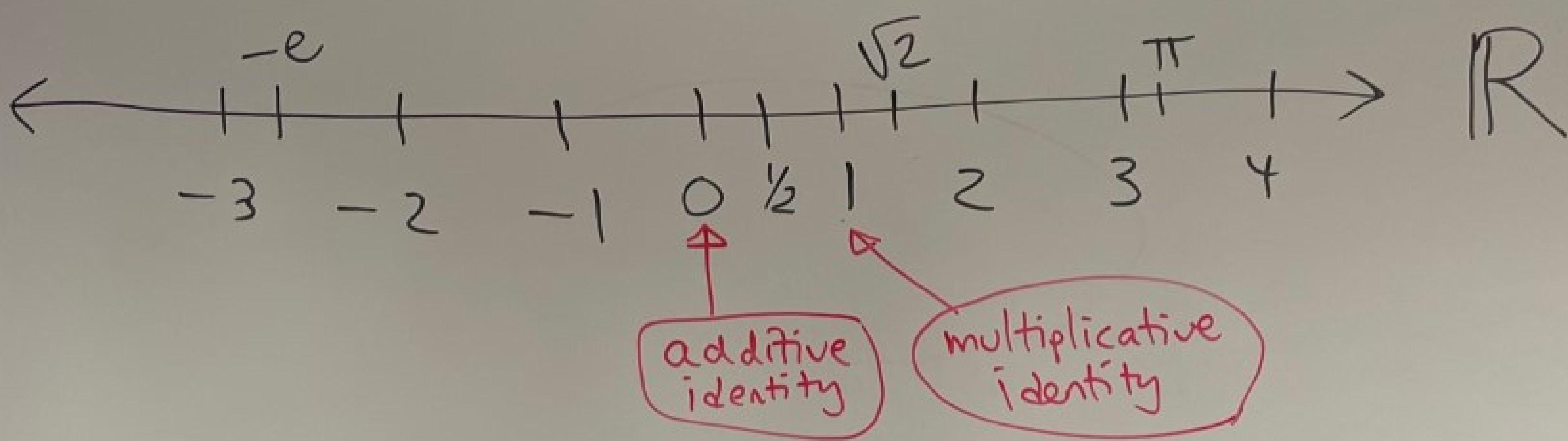
$$\underbrace{0, 1}_{F3}, \underbrace{b}_{F4}, \underbrace{c}_{F5}$$

from F3, F4, F5 are unique.

- We call 0 the <u>additive identity</u> of F
- We call 1 the <u>multiplicative identity</u> of F

- We denote b in F4 as $-a$ and call it the <u>additive inverse</u> of a.
- We denote c in F5 by a^{-1} and call it the <u>multiplicative inverse</u> of a.

Ex: $F = \mathbb{R}$ ← set of real numbers



If $a = 5$, then $-a = -5$

If $a = \frac{1}{4}$, then $a^{-1} = 4$

$\mathbb{R}$ is a field

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

rational numbers

$\mathbb{Z}$ integers

$= \left\{ \frac{5}{1}, -\frac{10}{1}, \frac{7}{12}, \ldots \right\}$

$\mathbb{Q}$ is a field

- F1 ✓
- F2 ✓

F3 $0, 1 \in \mathbb{Q}$ ✓

F4 ✓ ← If $a = \frac{1}{2}$, then $-a = -\frac{1}{2}$

F5 ✓ ← If $a = \frac{3}{7}$, then $a^{-1} = \frac{7}{3}$

Ex: $F = \mathbb{C}$ ← complex numbers

$\mathbb{C}$ is a field

Ex: $F = \mathbb{Z}_p$ ← (integers mod p)

if p is prime, then $\mathbb{Z}_p$ is a finite field

$\mathbb{Z}_p = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{p-1}\}$

Ex: $\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \dots\}$ ← integers

F1 ✓

F2 ✓

F3 ✓

F4 ✓

F5 X ← $\mathbb{Z}$ doesn't have all the inverses under multiplication

Ex: $a = 2$ is in $\mathbb{Z}$

but $a^{-1} = \frac{1}{2}$ is not in $\mathbb{Z}$

$\mathbb{Z}$ is not a field

Ex: The set of irrational numbers is not a field

F1 X ← $\underbrace{(\sqrt{2})}_{\text{irrational}}\underbrace{(\sqrt{2})}_{\text{irrational}} = \underbrace{2}_{\text{rational}}$