We have the set of positive integers : $\{0, 1, 2, 3, \cdots\}$

the set of integers: $\{0, \pm 1, \pm 2, \pm 3, \cdots\} = \mathbb{Z}$

Today we introduce <u>the rational numbers:</u>

$$\mathbb{Q} = \left\{ \frac{m}{n} : n \neq 0, \ m, n \in \mathbb{Z} \right\}.$$

Every number in $\mathbb{Q}$ is called a rational number.

Otherwise, it is called an irrational numbers.

Theorem: $\sqrt{2}$ is an irrational number.

Proof: ($\sqrt{2}$ is an irrational number, this means $\sqrt{2}$ is not a rational number.)

(Proof by contradiction). Suppose that $\sqrt{2}$ is a rational number.

Then we can write $\sqrt{2} = \frac{m}{n}$ with $m, n \in \mathbb{Z}$.

We can further assume that $\gcd(m, n) = 1$

since $\frac{m}{n} = \dfrac{\frac{m}{\gcd(m,n)}}{\frac{n}{\gcd(m,n)}}$ and we can replace

(m, n) by $\left(\frac{m}{\gcd(m,n)}, \frac{n}{\gcd(m,n)}\right)$.

$\sqrt{2} = \frac{m}{n} \Rightarrow \sqrt{2} \cdot n = m \Rightarrow (\sqrt{2} \cdot n)^2 = m^2$

$\Rightarrow 2m^2 = n^2$.

This shows: $2 \mid n^2 \Rightarrow 2 \mid n$

Notice that n^2 is a square, $2 \mid n \Rightarrow 4 \mid n^2$

Then $4 \mid 2m^2 \Rightarrow 2 \mid m^2 \Rightarrow 2 \mid m$

This means $2 \mid \gcd(m, n)$. A contradiction! $\square$

Remark: This theorem shows the existence of an irrational number.

Indeed, there are "more" irrational numbers than rational numbers.

Relations to decimals:

We have 3 types of decimals:

(1) Finite decimal: 0.2, 0.414

(2) Repeated decimal: 0.333...., 0.143143143143...

(3) non repeating decimal: 1.414..., 3.1415926....

We can prove:

rational number $\Leftrightarrow$ finite decimal or repeating decimal

irrational number $\Leftrightarrow$ non repeating decimal.

Definition: Let A be a set. An <u>operation</u> is a map $A \times A \to A$.

Example: $A = \mathbb{R}$, then

$$\mathbb{R} \times \mathbb{R} \to \mathbb{R} \quad \text{is an operation}$$
$$(a, b) \mapsto a+b$$

$$\mathbb{R} \times \mathbb{R} \to \mathbb{R} \quad \text{is an operation.}$$
$$(a, b) \mapsto ab$$

Definition: Let F be a set with 2 operations $\oplus$, $\otimes$.

Then we say $(F, \oplus, \otimes)$ is a <u>field</u> if for any $a, b, c \in F$

(1) For $\oplus$

(a) Associative: $a \oplus (b \oplus c) = (a \oplus b) \oplus c$

(b) Commutative $a \oplus b = b \oplus a$

(c) Additive identity: we can find $z \in F$ such that

$$a \oplus z = a$$

(d) Additive inverse: for $a \in F$, we can always find an element, denoted by $-a$, such that

$$a \oplus (-a) = z.$$

(2) For $\otimes$

(a) Associative: $a \otimes (b \otimes c) = (a \otimes b) \otimes c$

(b) Commutative: $a \otimes b = b \otimes a$

(c) Multiplicative unit: we can find $e \in F$ such that

$$a \otimes e = a \quad \text{for any } a \in F$$

(d) Multiplicative inverse: for any $z \neq a \in F$, we can find an element, denoted by a^{-1}, such that $a \otimes a^{-1} = e$.

(3) compatibility between $\oplus$ and $\otimes$

(a) distributive: $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$

Theorem: $(\mathbb{Q}, +, \cdot)$ is a field. Here $+$ is the usual addition and $\cdot$ is the usual multiplication.

Proof: (1) For $+$

(a) Take $a, b, c \in \mathbb{Q}$, $a + (b + c) = (a + b) + c$

(b) Take $a, b \in \mathbb{Q}$, $a+b=b+a$

(c) We can check: for any $a \in \mathbb{Q}$,

$$a+0=a \quad 0 \text{ is the additive unit.}$$

(d) For any $a \in \mathbb{Q}$, we have:

$$a+(-a)=0.$$

(2) For $\cdot$

(a) Take $a, b, c \in \mathbb{Q}$, $a(bc)=(ab)c$

(b) For $a, b \in \mathbb{Q}$, $a \cdot b = b \cdot a$

(c) We can show: for any $a \in \mathbb{Q}$.

$$a \cdot 1 = a$$

(d) If $0 \neq a = \frac{m}{n} \in \mathbb{Q}$, then

$$a \cdot \frac{n}{m} = \frac{m}{n} \cdot \frac{n}{m} = 1$$

(3) Compatibility between $+$ and $\cdot$

Distribution law: $a \cdot (b+c) = a \cdot c + b \cdot c$.

Therefore, $(\mathbb{Q}, +, \cdot)$ is a field. $\square$.

Some other examples of field:

(1) $(\mathbb{R}, +, \cdot)$ real numbers

(2) $(\mathbb{C}, +, \cdot)$ complex numbers. (next class)

(3) Set: $\mathbb{F}_p = \{ a \pmod p : 0 \le a \le p-1 \}$, p a prime.

$$a \pmod p \oplus b \pmod p = (a+b) \pmod p$$

$$a \pmod p \odot b \pmod p = (ab) \bmod p$$

Then $(\mathbb{F}_p, \oplus, \odot)$ is a field.

This is the 1st example of <u>finite</u> field.