# Section 2: Why is $\mathbb{Z}$ better than $\mathbb{N}$?

**Properties of addition on $\mathbb{Z}$**

**(A1)** Associativity: for $a, b, c \in \mathbb{Z}$, $a + (b + c) = (a + b) + c$.

**(A2)** Commutativity: for $a, b \in \mathbb{Z}$, $a + b = b + a$.

**(A3)** Existence of neutral element: $\exists$ element $0 \in \mathbb{Z}$ s.t. $0 + a = a$ $\forall\, a \in \mathbb{Z}$.

**(A4)** Existence of opposite: $\forall\, a \in \mathbb{Z}\ \exists\, x \in \mathbb{Z}$ s.t. $a + x = 0$ (this $x$ is denoted by $-a$).

(A1), (A2) hold for $\mathbb{N}$ as well. However, (A3), (A4) fail for $\mathbb{N}$.
$\mathbb{Z}$ is "better" than $\mathbb{N}$.

If $+ : S \times S \to S$ satisfies (A1-4), then $(S, +, 0)$ is called an abelian (commutative) group.

Examples of abelian groups: $(\mathbb{Z}, +, 0)$, $(\mathbb{Q}, +, 0)$, $(\mathbb{R}, +, 0)$.

# Uniqueness of 0 and $-a$; subtraction

**Observation.** The neutral element is unique.

**Proof.** If $0, 0'$ are neutral elements, then $0 = 0 + 0' = 0'$. ■

**Observation.** For $a \in \mathbb{Z}$, its opposite $-a$ is unique.

**Proof.** Suppose $a + x = 0 = a + x'$. Then
$x = x + 0 = x + (a + x') = (x + a) + x' = 0 + x' = x'$. ■

**Observation.** For $a, b \in \mathbb{Z}$, there exists a unique $x \in \mathbb{Z}$ s.t. $a + x = b$. We denote this $x$ by $b - a$.

**Proof.** (1) Existence. Take $x = b + (-a)$, then
$x + a = \big(b + (-a)\big) + a = b + \big((-a) + a\big) = b + 0 = b$.

(2) Uniqueness. If $a + x = b$, then $(a + x) + (-a) = b + (-a)$.
LHS $= (x + a) + (-a) = x + \big(a + (-a)\big) = x + 0 = x$, so $x = b + (-a)$. ■

$\mathbb{N}$ has only addition, but no subtraction, due to the lack of (A3-4).

# Multiplication on $\mathbb{Z}$

**Multiplication:** an operation $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$.

Properties of multiplication

**(M1)** Associativity: for $a, b, c \in \mathbb{Z}$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

**(M2)** Commutativity: for $a, b \in \mathbb{Z}$, $a \cdot b = b \cdot a$.

**(M3)** Neutral element: $\exists$ element $1 \in \mathbb{Z}$ s.t. $1 \cdot a = a \; \forall \, a \in \mathbb{Z}$.

**(DL)** Distributive law: $\forall \, a, b, c \in \mathbb{Z}$, $(a + b) \cdot c = a \cdot c + b \cdot c$.

$(\mathcal{X}, +, 0, \cdot, 1)$ is called a commutative ring if (A1-4), (M1-3), and (DL) are satisfied.

**Examples:** $(\mathbb{Z}, +, 0, \cdot, 1)$, $(\mathbb{Q}, +, 0, \cdot, 1)$, $(\mathbb{R}, +, 0, \cdot, 1)$.

# Multiplication by 0

**Proposition**

*For any $a \in \mathbb{Z}$, $0 \cdot a = 0$.*

In fact, if $(\mathcal{X}, +, 0, \cdot, 1)$ is a commutative ring, then $0 \cdot a = 0$ for any $a \in \mathcal{X}$.

**Proof.** $a = 1 \cdot a = (1 + 0) \cdot a = 1 \cdot a + 0 \cdot a = a + 0 \cdot a$.
Add $-a$ to both sides:
$0 = a + (-a) = \big(a + 0 \cdot a\big) + (-a) = 0 \cdot a$. ∎

---

**$\mathbb{Z}$ is not enough**

On $\mathbb{Z}$, we have $+$ and $\cdot$; what else do we want?

**Recall:** For $a, b \in \mathbb{Z}$, there exists a unique $x \in \mathbb{Z}$ (denoted by $b - a$) s.t. $a + x = b$.

Suppose $a, b \in \mathbb{Z}$; can we always find $x \in \mathbb{Z}$ s.t. $a \cdot x = b$? **NO!**
For $b = 1$, $a \neq \pm 1$, the equation $a \cdot x = 1$ has no solutions $x \in \mathbb{Z}$.

To have division, we need to consider $\mathbb{Q}$.

# $\mathbb{Q}$ is better than $\mathbb{Z}$

$\mathbb{Q}$ is the set of fractions $a/b$, with $a \in \mathbb{Z}$, $b \in \mathbb{N}$.

In $\mathbb{Q}$, addition satisfies (A1-4); multiplication has properties

**(M1)** Associativity: for $a, b, c \in \mathbb{Q}$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

**(M2)** Commutativity: for $a, b \in \mathbb{Q}$, $a \cdot b = b \cdot a$.

**(M3)** Neutral element: $\exists$ element $1 \in \mathbb{Q}$ s.t. $1 \cdot a = a \; \forall \, a \in \mathbb{Q}$.

**(M4)** The inverse: $\forall \, a \in \mathbb{Q} \backslash \{0\} \; \exists$ element $x \in \mathbb{Q}$ s.t. $x \cdot a = 1$ (write $x = a^{-1}$).

**(DL)** Distributive law: $\forall \, a, b, c \in \mathbb{Q}$, $(a + b) \cdot c = a \cdot c + b \cdot c$.

$(\mathcal{X}, +, 0, \cdot, 1)$ is called a field if (A1-4), (M1-4), and (DL) hold.

$\mathbb{R}$, $\mathbb{C}$ are fields, but $\mathbb{Z}$ is not ((M4) fails).

# Properties of fields

**Theorem (Theorem 3.1 – p. 15 of text)**

*Suppose $F$ is a field. Then:*

1. *If $a, b, c \in F$, and $a + c = b + c$, then $a = b$.*
2. *If $a \in F$, then $a \cdot 0 = 0$.*
3. *$(-a)b = -ab$ for all $a, b \in F$.*
4. *$(-a)(-b) = ab$ for all $a, b \in F$.*
5. *If $a, b, c \in F$, $ac = bc$, and $c \neq 0$, then $a = b$.*
6. *If $a, b \in F$, $ab = 0$, then either $a = 0$ or $b = 0$.*

We proved (ii) for commutative rings. For proofs of other items, see textbook.

# $\mathbb{Q}$ is not enough

There is no $x \in \mathbb{Q}$ with $x^2 = 2$. Later, we'll see that there exists $x \in \mathbb{R}$ s.t. $x \geqslant 0$, $x^2 = 2$ (this $x$ is called $\sqrt{2}$).

**Theorem (Rational zeros theorem – p. 9 of textbook)**

*Suppose $p(x) = c_n x^n + \ldots + c_1 x + c_0$ is a polynomial, with $c_0, \ldots, c_n \in \mathbb{Z}$, $c_0 \neq 0$, $c_n \neq 0$. Suppose $p(r) = 0$, $r = c/d$, with $c, d \in \mathbb{Z}$, $d \neq 0$, and $\gcd(c, d) = 1$. Then $c | c_0$ and $d | c_n$.*

**Notation.** $\gcd$ = greatest common divisor (factor).

**Corollary (Roots of monic ($c_n = 1$) polynomials)**

*Suppose $p(x) = x^n + c_{n-1} x^{n-1} + \ldots + c_1 x + c_0$, with $c_0, \ldots, c_{n-1} \in \mathbb{Z}$, $c_0 \neq 0$. If $r \in \mathbb{Q}$, and $p(r) = 0$, then $r \in \mathbb{Z}$, $r | c_0$.*

**Proof.** If $r \in \mathbb{Q}$, $p(r) = 0$, write $r = c/d$, $c, d \in \mathbb{Z}$, $d \neq 0$, and $\gcd(c, d) = 1$. $d$ divides $c_n = 1$, so $d = \pm 1$. $r = \pm c$, $c$ divides $c_0$. ∎

# $\sqrt{2} \notin \mathbb{Q}$

**Corollary (Irrationality of $\sqrt{2}$)**

*No rational number $r$ satisfies $r^2 = 2$.*

**Proof.** Suppose, for the sake of contradiction, $r \in \mathbb{Q}$, $r^2 = 2$. $r$ is a root of the monic polynomial $p(x) = x^2 - 2$. By Corollary, $r \in \mathbb{Z}$, $r|(-2)$. Thus, $r = \pm 1$, or $\pm 2$. Check: $1^2 = (-1)^2 = 1 \neq 2$, $2^2 = (-2)^2 = 4 \neq 2$. Contradiction! ■

# Proof of Rational Zeros Theorem

**Theorem (Rational zeros theorem – p. 9 of textbook)**

*Suppose* $p(x) = c_n x^n + \ldots + c_1 x + c_0$ *is a polynomial, with* $c_0, \ldots, c_n \in \mathbb{Z}$, $c_0 \neq 0$, $c_n \neq 0$. *Suppose* $p(r) = 0$, $r = c/d$, *with* $c, d \in \mathbb{Z}$, $d \neq 0$, *and* $\gcd(c, d) = 1$. *Then* $c | c_0$ *and* $d | c_n$.

**Part 1:** $d|c_n$. $0 = p\left(\frac{c}{d}\right) = c_n \frac{c^n}{d^n} + c_{n-1} \frac{c^{n-1}}{d^{n-1}} + \ldots + c_1 \frac{c}{d} + c_0$. Multiply by $d^n$: $0 = c_n c^n + c_{n-1} c^{n-1} d + \ldots + c_1 c d^{n-1} + c_0 d^n$.
$c_n c^n = -c_{n-1} c^{n-1} d - \ldots - c_0 d^n$. $d$ divides RHS (right hand side), hence LHS. $\gcd(d, c^n) = 1$, hence $d | c_n$. ■

**Part 2:** $c|c_0$. $0 = c_n c^n + c_{n-1} c^{n-1} d + \ldots + c_1 c d^{n-1} + c_0 d^n$.
$c_0 d^n = -c_n c^n - \ldots - c_1 c d^{n-1}$. $c$ divides RHS, hence LHS.
$\gcd(c, d^n) = 1$, hence $c | c_0$. ■

# Section 3 (order)

**Definition:** A relation $\leqslant$ on a set $S$ is called linear (total) order if:

**(O1)** Totality: for $a, b \in S$, either $a \leqslant b$, or $b \leqslant a$.

**(O2)** Antisymmetry: if $a \leqslant b$ and $b \leqslant a$, then $a = b$.

**(O3)** Transitivity: if $a \leqslant b$ and $b \leqslant c$, then $a \leqslant c$.

Write $a < b$ if $a \leqslant b$, and $a \neq b$.

**Examples of totally ordered sets.** $(\mathbb{Z}, \leqslant)$, $(\mathbb{Q}, \leqslant)$, $\ldots$.

**Example.** $S = \mathcal{P}(\{1, 2\})$. We say $A \leqslant B$ if $A \subset B$.
(O2) and (O3) are satisfied, but (O1) fails:
take $A = \{1\}$ and $B = \{2\}$.

# Ordered fields

Definition: A field $F$ is called ordered if it is equipped with linear order $\leqslant$ s.t.:

**(O4)** If $a, b, c \in F$, and $a \leqslant b$, then $a + c \leqslant b + c$.

**(O5)** If $a, b, c \in F$, $a \leqslant b$, and $c \geqslant 0$, then $ac \leqslant bc$.

**Examples of ordered fields.** $(\mathbb{Q}, \leqslant)$, $(\mathbb{R}, \leqslant)$.

$\mathbb{C}$ is a field, but cannot be equipped with a linear order.

# Properties of ordered fields

## Theorem (Theorem 3.2 – p. 16 of text)

*Suppose $F$ is an ordered field, $a, b, c, \in F$. Then:*

1. *If $a \leqslant b$, then $-b \leqslant -a$.*
2. *If $a \leqslant b$, and $c \leqslant 0$, then $bc \leqslant ac$.*
3. *If $0 \leqslant a$ and $0 \leqslant b$, then $0 \leqslant ab$.*
4. $0 \leqslant a^2$ *(for all $a \in F$).*
5. $0 < 1$.
6. *If $0 < a$, then $0 < a^{-1}$.*
7. *If $0 < a < b$, then $0 < b^{-1} < a^{-1}$.*

**Proof of (iii).** $b \geqslant 0$, hence, by (O5), $0 \cdot b \leqslant ab$. But, $0 \cdot b = 0$. ∎

**Fact.** $\mathbb{C}$ is not an ordered field.

**Proof.** $\mathbb{C}$ is a field. Suppose, for the sake of contradiction, that $\leqslant$ determines a linear order on $\mathbb{C}$. Recall: $\iota^2 = -1$, where $\iota = \sqrt{-1}$. Then $-1 > 0$, hence $1 = -(-1) < -0 = 0$. However, $1 > 0$. ∎