

Construction of \mathbb{Z}

March 16, 2024

Assumptions

- There exists a set $\mathbb{N} = \{0, 1, 2, \dots\}$.
- There exists $+$: $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ such that $(\mathbb{N}, +)$ forms a commutative monoid with identity 0. ¹
- The function $\text{succ} : \mathbb{N} \rightarrow \mathbb{N}^+, n \mapsto n + 1$ is injective.
- There exists \cdot : $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ such that (\mathbb{N}, \cdot) is a commutative monoid with identity 1
- The functions $\varphi_k : \mathbb{N} \rightarrow \mathbb{N}, x \mapsto kx$ are injective for $k \in \mathbb{N}^+$
- There exists the usual total order \leq on \mathbb{N}

¹We will use infix notation for $+$

- Constructing the set \mathbb{Z} .
- Defining $+$: $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ and \cdot : $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ ²
- Showing $(\mathbb{Z}, +, \cdot)$ is a commutative ring with multiplicative identity 1.
- Showing \leq is a total order on \mathbb{Z}
- Constructing the set \mathbb{Q}

²We will use infix notation for $+$ and \cdot

Defining the set \mathbb{Z}

Idea

We want $\underbrace{}_{\in \mathbb{Z}} \equiv \underbrace{(a, b)}_{\in \mathbb{N} \times \mathbb{N}} \Leftrightarrow z = a - b.$

Issue: This representation is not unique. E.g: $0 = 1 - 1 = 2 - 2 = \dots$

Definition: \sim

$$(a, b) \sim (c, d) :\Leftrightarrow a + d = b + c$$

Lemma

\sim is an equivalence relation

Defining the set \mathbb{Z}

Proof.

Reflexivity:

$$\forall (a, b) \in \mathbb{N} \times \mathbb{N} : a + b = b + a.$$

Symmetry:

$$(a, b) \sim (c, d) \Rightarrow c + b = b + c \stackrel{(a,b) \sim (c,d)}{=} a + d = d + a \Rightarrow (c, d) \sim (a, b).$$

Transitivity:

Let $(a, b) \sim (c, d), (c, d) \sim (e, f)$. Then

$$\text{succ}^{c+d}(a + f) = \underbrace{a + d}_{=b+c} + \underbrace{c + f}_{=d+e} = b + c + d + e = \text{succ}^{c+d}(b + e)$$

$$\stackrel{\text{succ injective}}{\Rightarrow} a + f = b + e \Rightarrow (a, b) \sim (e, f)$$



Defining the set \mathbb{Z}

Definition: \mathbb{Z}

$$\mathbb{Z} := \mathbb{N} \times \mathbb{N} / \sim = \{[(a, b)] \mid a, b \in \mathbb{N}\}$$

Defining $+$

Remark

$(\mathbb{N} \times \mathbb{N}, +_2)$ as direct product of $(\mathbb{N}, +)$ with itself is a semigroup.

Lemma

\sim is compatible with $+_2$.

Proof.

Let $(a, b) \sim (a', b'), (c, d) \sim (c', d')$. Then

$$(a + c) + (b' + d') = \underbrace{(a + b')}_{=b+a'} + \underbrace{(c + d')}_{=d+c'} = (b + d) + (a' + c')$$

$$\Rightarrow (a, b) +_2 (c, d) = (a + c, b + d) \sim (a' + c', b' + d') = (a', b') +_2 (c', d')$$



Defining $+$

Corollary: Definition of $+$

$[(a, b)] +_3 [(c, d)] := [(a, b) +_2 (c, d)] = [(a + c, b + d)]$ is well-defined and makes $(\mathbb{Z}, +_3)$ a semigroup.

Remark

This gives us the usual Addition on \mathbb{Z} :

$$y = a - b, z = c - d \Rightarrow y + z = a + c - (b + d)^a$$

^aFrom now on we will not distinguish between $+$, $+_2$ and $+_3$

Lemma

$(\mathbb{Z}, +)$ is an abelian group.

Defining +

Proof.

Commutativity: $\forall [(a, b)], [(c, d)] \in \mathbb{Z} :$

$$[(a, b)] + [(c, d)] = [(a + c, b + d)] = [(c + a, d + b)] = [(c, d)] + [(a, b)]$$

Neutral Element: $\forall [(a, b)] \in \mathbb{Z} : [(a, b)] + [(0, 0)] = [(a, b)]$

Inverses: $\forall [(a, b)] \in \mathbb{Z} : [(a, b)] + [(b, a)] = [(a + b, b + a)] = [(0, 0)]$
 $\sim_{(0,0)}$



Difference representation

Definition: -

For $\alpha, \beta \in \mathbb{Z}$ we define: $\alpha - \beta := \alpha + (-\beta)$

Identification of \mathbb{N}

The Map $\iota : \mathbb{N} \rightarrow \mathbb{Z}, n \mapsto [(n, 0)]$ is injective and compatible with $+$.

Proof.

Injective:

$$[(a, 0)] = [(b, 0)] \Rightarrow a + 0 = b + 0 \Rightarrow a = b$$

Compatible: $\forall a, b \in \mathbb{N}$:

$$\iota(a + b) = [(a + b, 0)] = [(a, 0)] + [(b, 0)] = \iota(a) + \iota(b)$$



Difference representation

Identification of \mathbb{N}

We identify \mathbb{N} with the isomorphic set $\iota(\mathbb{N}) \subseteq \mathbb{Z}$.

Difference representation

We can now represent integers as

$$[(a, b)] = [(a, 0)] + [(0, b)] = [(a, 0)] - [(b, 0)] = a - b$$

Definition of \cdot

Idea

We want $(a - b)(c - d) = ac - ad - bc + bd = ac + bd - (ad + bc)$

Definition: \cdot

$$[(a, b)] \cdot [(c, d)] := [(ac + bd, ad + bc)] = [(ca + db, da + cb)] = [(c, d)] \cdot [(a, b)]$$

\cdot is well-defined

Let $[(a, b)] = [(a', b')]$. We have

$$\begin{aligned} [(a', b')] \cdot [(c, d)] &= [(a'c + b'd, a'd + b'c)] = \underset{\sim(ac, bc)}{[(a'c, b'c)]} + \underset{\sim(bd, ad)}{[(b'd, a'd)]} = \\ &[(ac + bd, ad + bc)] \end{aligned}$$

By symmetry \cdot is also invariant under changes of representative in the 2nd argument.

Definition of \cdot

Lemma

(\mathbb{Z}, \cdot) is a commutative monoid.

Proof.

Associativity: $\forall [(a, b)], [(c, d)], [(e, f)] \in \mathbb{Z}$:

$$\begin{aligned} [(a, b)] \cdot ([(c, d)] \cdot [(e, f)]) &= [(a, b)] \cdot [(ce + df, cf + de)] \\ &= [(e(ac + bd) + f(ad + bc), f(ac + bd) + e(ad + bc))] \\ &= [(ac + bd, ad + bc)] \cdot [(e, f)] \\ &= ([[(a, b)] \cdot [(c, d)]] \cdot [(e, f)]) \end{aligned}$$

Neutral Element: $\forall [(a, b)] \in \mathbb{Z}$:

$$[(a, b)] \cdot [(1, 0)] = [(a \cdot 1 + b \cdot 0, a \cdot 0 + b \cdot 1)] = [(a, b)]$$



\mathbb{Z} is an integral domain

Corollary

\mathbb{Z} is a commutative ring with identity.

Proof.

$(\mathbb{Z}, +)$ is an abelian group and (\mathbb{Z}, \cdot) is a commutative monoid. We also have:

Distributivity: $\forall [(a, b)], [(c, d)], [(e, f)]:$

$$[(a, b)] \cdot ([(c, d)] + [(e, f)]) = [(a(c + e) + b(d + f), a(d + f) + b(c + e))] = [(a, b)] \cdot [(c, d)] + [(a, b)] \cdot [(e, f)]$$



\mathbb{Z} is an integral domain

Corollary

\mathbb{Z} is an integral domain

Proof.

Let $[(a, b)][(c, d)] = [(0, 0)]$, $[(a, b)] \neq [(0, 0)]$

$$\Rightarrow ac + bd = ad + bc$$

$$\Rightarrow (a - b)c = (a - b)d$$

Assume $a > b$, so $a - b = k$ for some $k \geq 1$

$$\Rightarrow kc = kd \Rightarrow c = d \Rightarrow [(c, d)] = [(0, 0)]$$

$\varphi_k: \mathbb{N} \rightarrow \mathbb{N}, x \mapsto kx$
injective for $k \in \mathbb{N}^+$

If $a < b$, then for $k := a - b$ the map $\varphi_{-k}: \mathbb{N} \rightarrow \mathbb{N}, x \mapsto (-k)x$ is injective. □

Ordering on \mathbb{Z}

Definition

For $a, b \in \mathbb{Z}$ we define $a \leq b :\Leftrightarrow b - a \in \mathbb{N}$

Lemma

\leq *is an order relation*

Ordering on \mathbb{Z}

Proof.

Reflexivity: $\forall a \in \mathbb{Z} : a - a = 0 \in \mathbb{N}$

Antisymmetry: Let $a \leq b, b \leq a$.

$\Rightarrow \exists n_1, n_2 \in \mathbb{N} : b - a = n_1, a - b = n_2$.

$\Rightarrow n_1 = b - a = -(a - b) = -n_2$

$\Rightarrow n_1 = b_2 = 0 \Rightarrow a = b$

Transitivity: Let $a \leq b, b \leq c$.

$\Rightarrow \exists k_1, k_2 \in \mathbb{N} : a + k_1 = b, b + k_2 = c$

$\Rightarrow \exists k_3 \in \mathbb{N} : a + k_3 = c$

$\Rightarrow c - a \in \mathbb{N} \Rightarrow a \leq c$



Ordering on \mathbb{Z}

Lemma

\leq is a total order.

Proof.

Let $a, b, c, d \in \mathbb{N}$, $[(a, b)] \not\leq [(c, d)]$.

$\Rightarrow [(c, d)] - [(a, b)] = [(b + c, a + d)] \notin \mathbb{N}$

$\Rightarrow \forall n \in \mathbb{N} : [(n, 0)] \neq [(b + c, a + d)]$

$\Rightarrow \forall n \in \mathbb{N} : a + d + n \neq b + c$

$\Rightarrow b + c \leq a + d$

$\Rightarrow a + d - (b + c) \in \mathbb{N}$

$\Rightarrow [(a, b)] - [(c, d)] = [(a + d, b + c)] = [(a + d - (b + c), 0)] \in \mathbb{N}$

$\Rightarrow [(c, d)] \leq [(a, b)]$



Definition of \mathbb{Q}

Definition

For $(a, b), (c, d) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ we define $(a, b) \sim (c, d) :\Leftrightarrow ad = bc$

\sim is an equivalence relation

Transitivity: $\forall (a, b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) : ab = ba$

Symmetry: Let $(a, b) \sim (c, d)$

$\Rightarrow cb = bc = ad = da \Rightarrow (c, d) \sim (a, b)$

Transitivity: Let $(a, b) \sim (c, d), (c, d) \sim (e, f)$

If $c = 0$ then $a = e = 0 \Rightarrow af = 0 = be \Rightarrow (a, b) \sim (e, f)$

Else $cd \neq 0$, therefore:

$cdaf = cdbe \Rightarrow af = be \Rightarrow (a, b) \sim (e, f)$

Definition of \mathbb{Q}

Definition: \mathbb{Q}

$\mathbb{Q} := \{[(a, b)] \mid (a, b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})\}$. We define $\frac{a}{b} := [(a, b)]$.

Definition of $+$

Definition

For $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$ we define $\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd} = \frac{cb+ad}{db} = \frac{c}{d} + \frac{a}{b}$.

$+$ is well-defined

Let $\frac{a}{b} = \frac{a'}{b'}$. Then for $\frac{c}{d} \in \mathbb{Q}$:

$$\begin{aligned} bd(a'd + b'c) &= ddba' + bb'cd = ddab' + bb'cd = b'd(ad + bc) \\ \Rightarrow \frac{a'}{b'} + \frac{c}{d} &= \frac{a'd+b'c}{b'd} = \frac{ad+bc}{bd} = \frac{a}{b} + \frac{c}{d} \end{aligned}$$

By Symmetry invariance under changes of the right representative follows.

$(\mathbb{Q}, +)$ is an abelian group