Construction of $\mathbb{Z}$

April 1, 2024

Assumptions

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

[1] We will use infix notation for $+$

Goals

- Constructing the set $\mathbb{Z}$.
- Defining $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ and $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ [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 $\mathbb{Q}$

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

Defining the set $\mathbb{Z}$

Idea

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

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

Transitivity:

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

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

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

$\square$

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 comptabile with $+_2$.

Proof.

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

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

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

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]

[a] From 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: $\forall [(a,b)] \in \mathbb{Z} : [(a,b)] + [(b,a)] = [(\underbrace{a+b, b+a}_{\sim(0,0)})] = [(0,0)]$ $\square$

Difference representation

Definition: -

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

Identification of $\mathbb{N}$

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

Proof.

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

Compatible: $\forall a, b \in \mathbb{N}$:
$\iota(a + b) = [(a + b, 0)] = [(a, 0)] + [(b, 0)] = \iota(a) + \iota(b)$ $\square$

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
$[(a',b')] \cdot [(c,d)] = [(a'c+b'd, a'd+b'c)] = \underbrace{[(a'c, b'c)]}_{\sim(ac,bc)} + \underbrace{[(b'd, a'd)]}_{\sim(bd,ad)} =$
$[(ac+bd, ad+bc)]$
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: $\forall [(a,b)], [(c,d)], [(e,f)] \in \mathbb{Z}$:

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

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

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

$\square$

$\mathbb{Z}$ 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: $\forall [(a, b)], [(c, d)], [(e, f)]$:
$[(a, b)] \cdot ([(c, d)] + [(e, f)]) = [(a(c + e) + b(d + f), a(d + f) + b(c + e))] =$
$[(a, b)] \cdot [(c, d)] + [(a, b)] \cdot [(e, f)]$ $\square$

$\mathbb{Z}$ is an integral doman

Corollay

$\mathbb{Z}$ 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 $k \geq 1$
$\Rightarrow kc = kd \underset{\substack{\varphi_k:\mathbb{N}\to\mathbb{N},x\mapsto kx \\ \text{injective for } k\in\mathbb{N}^+}}{\Rightarrow} c = d \Rightarrow [(c,d)] = [(0,0)]$

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

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 $a \leq b, b \leq c$.
$\Rightarrow \exists k_1, k_2 \in \mathbb{N} : a + k_1 = b,\ b + k_2 = c$
$\Rightarrow \exists k_3 \in \mathbb{N} : a + k_3 = c$
$\Rightarrow c - a \in \mathbb{N} \Rightarrow a \leq c$ $\square$

Ordering on $\mathbb{Z}$

Lemma

$\leq$ is a total order.

Proof.

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

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

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

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

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

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

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

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

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

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 $\frac{c}{d} \in \mathbb{Q}$:
$bd(a'd + b'c) = ddba' + bb'cd = ddab' + bb'cd = b'd(ad + bc)$
$\Rightarrow \frac{a'}{b'} + \frac{c}{d} = \frac{a'd+b'c}{b'd} = \frac{ad+bc}{bd} = \frac{a}{b} + \frac{c}{d}$

By Symmetry invariance under changes of the right represenative follows.

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

Proposition

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

Proof.

Associativity: $\forall \frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbb{Q}$:

$$\frac{a}{b} + \underbrace{\left(\frac{c}{d} + \frac{e}{f}\right)}_{=\frac{cf+de}{df}} = \frac{adf+bcf+bde}{bdf} = \underbrace{\left(\frac{a}{b} + \frac{c}{d}\right)}_{=\frac{ad+bc}{bd}} + \frac{e}{f}$$

Neutral Element: $\forall \frac{a}{b} \in \mathbb{Q}$:

$$\frac{0}{1} + \frac{a}{b} = \frac{a}{b}$$

Inverses: $\forall \frac{a}{b} \in \mathbb{Q}$:

$$\frac{a}{b} + \frac{-a}{b} = \frac{ab-ab}{ab} = \frac{0}{1}$$

□

$(\mathbb{Q} \setminus \{0\}, \cdot)$ is an abelian group

Definition

For $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$ we define: $\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd} = \frac{c}{d}\frac{a}{b}h$

$\cdot$ is well-defined

Let $\frac{a}{b} = \frac{a'}{b'}$. Then for $\frac{c}{d}$:
$ab' = ba' \Rightarrow ab'cd = ba'cd$
$\Rightarrow \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} = \frac{a'c}{b'd} = \frac{a'}{b'} \cdot \frac{c}{d}$

$(\mathbb{Q} \setminus \{0\}, \cdot)$ is an abelian group

Proposition

$(\mathbb{Q} \setminus \{0\}, \cdot)$ is an abelian group

Proof.

Associativity: $\forall \frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbb{Q} \setminus \{0\}$:
$\frac{a}{b} \cdot (\frac{c}{d} \cdot \frac{e}{f}) = \frac{ace}{bdf} = (\frac{a}{b} \cdot \frac{c}{d}) \cdot \frac{e}{f}$

Neutral Element: $\forall \frac{a}{b} \in \mathbb{Q}$:
$\frac{a}{b} \cdot \frac{1}{1} = \frac{a}{b}$

Inverses: $\forall \frac{a}{b} \in \mathbb{Q} \setminus \{0\}$:
$\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ab} = \frac{1}{1}$ $\square$

$\mathbb{Q}$ is a field

Lemma

$\mathbb{Q}$ is a field

Proof.

Since $(\mathbb{Q}, +)$ and $(\mathbb{Q} \setminus \{0\}, \cdot)$ are abelian groups, we only need to show Distributivity.
Distributivity: Let $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in \mathbb{Q}$. Then:

$$\frac{a}{b}\underbrace{\left(\frac{c}{d} + \frac{e}{f}\right)}_{\frac{cf+de}{df}} = \frac{acf+ade}{bdf} = \frac{b(acf+dae)}{bdbf} = \frac{ac}{bd} + \frac{ae}{bf} = \frac{a}{b}\frac{c}{d} + \frac{a}{b}\frac{e}{f} \qquad \square$$

Embedding of $\mathbb{Z}$ into $\mathbb{Q}$

Definition

The Map $\iota : \mathbb{Z} \to \mathbb{Q}, z \mapsto \frac{z}{1}$ is injective and compatible with $+, \cdot$.

Proof.

Injective: Let $\frac{z}{1} = \frac{z'}{1}$. By Definition of $\sim$ we get $z = z'$.
Addition: $\forall z, z' \in \mathbb{Z} : \iota(z + z') = \frac{z+z'}{1} = \frac{z}{1} + \frac{z'}{1} = \iota(z) + \iota(z')$
Multiplication: $\forall z, z' \in \mathbb{Z} : \iota(zz') = \frac{zz'}{1} = \frac{z}{1}\frac{z'}{1} = \iota(z)\iota(z')$ $\square$

Embedding of $\mathbb{Z}$

We identify $\mathbb{Z}$ with the isomorphic set $\iota(\mathbb{Z}) \subset \mathbb{Q}$