

Course: Set Theory(Integers & Rationals)

Sebastián Caballero

February 3, 2023

A simple notes template. Inspired by Tufte-L^AT_EXclass and beautiful notes by

<https://github.com/abrandenberger/course-notes>

1 The need for new constructions

Since we have constructed the natural numbers, we have put a lot of mathematics in hands of the set theory. But they are not sufficient in most cases, so we need new types of numbers. The first ones are the integers, in which we include the negative numbers and later we construct the rational, which are all the possible fractions between integers.

2 What are integer numbers?

2.1 Origin of integers

In the first approaches a kid have in mathematics, he will learn that $2 - 3$ is not possible since you can subtract more than what you have. Later, we are taught that there is a solution called -1 , but this solution is also applicable to $3 - 4$ and so on. So, we have:

$$3 - 2 = 4 - 5$$

And we can do this with a lot of natural numbers. But we don't have $-$ operation on natural number, so we are going to do it convenience. For two integers $a - b$ and $c - d$:


$$a - b = c - d$$

$$a + d = c + b$$

And this will be our strategy.

Definition 2.1. We define the relation \sim over the set $\mathbb{N} \times \mathbb{N}$ such that $(a, b) \sim (c, d)$ if and only if $a + d = b + c$.

This relation will associate all numbers whose difference is the same. For example, $(2, 3) \sim (4, 5)$ since $2 + 5 = 4 + 3$ which implies that $2 - 3 = 4 - 5$.

 **Theorem 2.1.** *The relation \sim is an equivalence relation*

Proof. • First, note that $a + b = a + b$ which by definition implies that $(a, b) \sim (a, b)$

- Suppose that $(a, b) \sim (c, d)$ so $a + d = c + b$ and then:

$$a + d = c + b$$

$$c + b = a + d$$

Therefore $(c, d) \sim (a, b)$

- Suppose that $(a, b) \sim (c, d)$ and $(c, d) \sim (x, y)$. This implies:

$$a + d = c + b$$

$$c + y = x + d$$

If we add the two equalities we would have:

$$a + d + c + y = c + b + x + d$$


$$a + y + (c + d) = x + b + (c + d)$$

$$a + y = x + b$$

So we can conclude that $(a, b) \sim (x, y)$

□

We are done with our generalization! We are going to define just what is an integer.

 **Definition 2.2** (Integers numbers). *The set $(\mathbb{N} \times \mathbb{N}) / \sim$ will be called as the set of integer numbers and will be denoted as \mathbb{Z} . Any element in \mathbb{Z} will be called an integer number.*

Our next tasks is to define the operations over integers. Take for example the integers $a - b$ and $c - d$ we can sum them as:

$$a - b + c - d = (a + c) - (b + d)$$

So if $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$ we define $(a, b) \odot (c, d) = (a + c, b + d)$.


Also, if we want to multiply numbers like those, we would do:

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

$$= ac + bd - bc - ad$$

$$= (ac + bd) - (bc + ad)$$

So we define $(a, b) \odot (c, d) = (ac + bd, bc + ad)$. We need then a theorem to show that this election is independent of what we choose in the equivalence classes.

 **Theorem 2.2.** Suppose that $(a, b) \sim (x, y)$ and $(c, d) \sim (z, w)$, then:

- $(a, b) \odot (c, d) \sim (x, y) \odot (z, w)$
- $(a, b) \odot (c, d) \sim (x, y) \odot (z, w)$

Proof. Assume that $(a, b) \sim (x, y)$ and $(c, d) \sim (z, w)$, we would have:

$$a + y = b + x \qquad c + w = z + d$$

And we have that:

$$\begin{aligned} (a, b) \odot (c, d) &= (a + c, b + d) \\ (x, y) \odot (z, w) &= (x + z, y + w) \end{aligned}$$

And adding the equalities we have:

$$\begin{aligned} a + y + c + w &= b + x + z + d \\ (a + c) + (y + w) &= (b + d) + (x + z) \end{aligned}$$

So we conclude that $(a + c, b + d) \sim (x + z, y + w)$. And for the \odot :

$$\begin{aligned} (a, b) \odot (c, d) &= (ac + bd, bc + ad) \\ (x, y) \odot (c, d) &= (cx + dy, cy + dx) \end{aligned}$$

If we take the first equality from above we can manipulate as:


$$\begin{aligned} a + y &= b + x & a + y &= b + x \\ ac + cy &= bc + cx & ad + dy &= bd + dx \\ ac + cy &= bc + cx & bd + dx &= ad + dy \end{aligned}$$

And if we sum them up we would have:

$$\begin{aligned} ac + cy + bd + dx &= bc + cx + ad + dy \\ (ac + bd) + (cy + dx) &= (cx + dy) + (bc + ad) \end{aligned}$$

And we conclude that $(a, b) \odot (c, d) \sim (x, y) \odot (c, d)$. In a similar way we can conclude that $(x, y) \odot (c, d) \sim (x, y) \odot (z, w)$ and therefore $(a, b) \odot (c, d) \sim (x, y) \odot (z, w)$. \square


And with that we can define these operations in \mathbb{Z} as:

 **Definition 2.3** (Operations in \mathbb{Z}). Let $[(a, b)], [(c, d)] \in \mathbb{Z}$, we

define:

$$\begin{aligned} [(a, b)] + [(c, d)] &= [(a, b) \odot (c, d)] \\ [(a, b)] \cdot [(c, d)] &= [(a, b) \odot (c, d)] \end{aligned}$$

Now, the important part of this definition is the structure for \mathbb{Z} .

 **Theorem 2.3** (Structure of \mathbb{Z}). *The set \mathbb{Z} with $+$ and \cdot forms a ring.*

Proof. • The associative and commutative properties follows easily from the properties of \mathbb{N} . For a neutral element, we choose the class $[(0, 0)]$ and we would have that $[(a, b)] + [(0, 0)] = [(a, b)]$. For an inverse element of the integer $[(a, b)]$ we choose $[(b, a)]$ so that:

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

And since $(a + b, a + b) \sim (0, 0)$, it gives us the neutral element. So, we have an abelian group with $+$ under the set.

- The associative and commutative properties follows again from properties of \mathbb{N} , and we have an identity element $[(1, 0)]$ since we would have:

$$\begin{aligned} [(a, b)] \cdot [(1, 0)] &= [(a \cdot 1 + b \cdot 0, b \cdot 1 + a \cdot 0)] \\ &= [(a + 0, b + 0)] \\ &= [(a, b)] \end{aligned}$$

- To prove that distributive law holds, take three items $[(a, b)], [(x, y)], [(z, w)]$.

$$\begin{aligned} [(a, b)] \cdot ([[(x, y)] + [(z, w)]] &= [(a, b)] \cdot [(x + z, y + w)] \\ &= [(ax + az + by + bw, ay + aw + bx + bz)] \\ &= [(ax + by, ay + bx)] + [(az + bw, aw + bz)] \\ &= [(a, b)] \cdot [(x, y)] + [(a, b)] \cdot [(z, w)] \end{aligned}$$

□

The last property that \mathbb{Z} misses for be a field is the existence of inverses in the operation \cdot . Far from being an annoying problem, this led to the development to new interesting mathematic. Now, what is also important to define is the order for integers. If we have that $a - b \leq c - d$ then $a + d \leq c + b$ which is what we are going to use to define the order.

Definition 2.4 (Order in \mathbb{Z}). If $[(a, b)], [(c, d)] \in \mathbb{Z}$, we define $[(a, b)] \leq [(c, d)]$ if and only if $a + d \leq b + c$.

This indeed is an order and is easy to see it with the properties of natural numbers. Reflexive and antisymmetric properties are obvious. For transitivity, suppose that $[(a, b)] \leq [(c, d)]$ and $[(c, d)] \leq [(x, y)]$, then:

$$a + d \leq c + b \quad c + y \leq x + d$$

If we add the two inequalities:

$$\begin{aligned} a + d + c + y &\leq c + b + x + d \\ a + y + (c + d) &\leq x + b + (c + d) \\ a + y &\leq x + b \end{aligned}$$

So $[(a, b)] \leq [(x, y)]$. The trichotomy property is just an use of the trichotomy in natural numbers. Now, we have the option to represent the integers just as natural numbers in a easy way, but this depends on a theorem.

Theorem 2.4. Every integer number can be expressed as equivalence class with the form $[(n, 0)]$ or $[(0, n)]$ for $n \in \mathbb{N}$

Proof. Suppose that $[(a, b)]$ is an integer number. Then there are three options:

- $a = b$, in this case $[(a, b)] = [(0, 0)]$
- $a < b$, so we have that there is $k \in \mathbb{N}$ such that $b = a + k$, and then $[(a, a + k)]$ which is the same as $[(0, k)]$ since $a + k = a + k$.
- $a > b$, so we have that there is $k \in \mathbb{N}$ such that $a = b + k$, and then $[(b + k, b)]$ is the same as $[(k, 0)]$ since $b + k = b + k$.

□

For this, we represent 0 as $[(0, 0)]$, and we represent the integer $[(n, 0)]$ as n . Since $[(0, n)]$ would be the additive inverse we choose to represent it as $-n$. Note that the set $\mathbb{N}' := \{[(n, 0)] \in \mathbb{Z} : n \in \mathbb{N}\}$ is isomorphic to the set \mathbb{N} so we say that \mathbb{N} is a *subset* of the integers, and we denote the sets $\mathbb{Z}^* := \mathbb{Z} \setminus \{0\}$ and $\mathbb{Z}^+ := \mathbb{N}'$. Now, we can proof also some properties about order:

Theorem 2.5. Let $x, y, z \in \mathbb{Z}$:

- If $x < y$ then $x + z < y + z$

- If $x < y$ and $z > 0$ then $xz < yz$
- If $x < y$ and $z < 0$ then $xz > yz$
- If $x \neq 0$, then $x \in \mathbb{Z}^+$ or $-x \in \mathbb{Z}^+$
- $x < y$ if and only if $y - x \in \mathbb{Z}^+$

Proof. Let $x, y, z \in \mathbb{Z}$, without loss of generality we can say that $x = [(a, b)]$, $y = [(c, d)]$ and $z = [(e, f)]$.

- If $x < y$ then $a + d < b + c$ so if we add e, f to both sides, we would have $[(a + e, b + f)] < [(c + e, d + f)]$, which implies that $x + z < y + z$.
- If $x < y$ then $a + d < b + c$ and if $z > 0$, then $z = [(n, 0)]$ for some $n \in \mathbb{N}$. So, if we multiply by n to both sides, we would have that $an + dn < bn + cn$. Also, we would have:

$$\begin{aligned} [(a, b)] \cdot [(n, 0)] &= [(a \cdot n + b \cdot 0, a \cdot 0 + b \cdot n)] \\ &= [(a \cdot n, b \cdot n)] \\ [(c, d)] \cdot [(n, 0)] &= [(c \cdot n + d \cdot 0, d \cdot n + c \cdot 0)] \\ &= [(c \cdot n, d \cdot n)] \end{aligned}$$

And therefore $x \cdot z < y \cdot z$.

- If $x < y$ then $a + d < b + c$ and if $z < 0$, then $z = [(0, n)]$ for some $n \in \mathbb{N}$. So, if we multiply by n to both sides, we would have that $an + dn < bn + cn$. Also, we would have:

$$\begin{aligned} [(a, b)] \cdot [(0, n)] &= [(a \cdot 0 + b \cdot n, a \cdot n + b \cdot 0)] \\ &= [(b \cdot n, a \cdot n)] \\ [(c, d)] \cdot [(0, n)] &= [(c \cdot 0 + d \cdot n, d \cdot 0 + c \cdot n)] \\ &= [(d \cdot n, c \cdot n)] \end{aligned}$$

And therefore $xz > yz$.

- This is a consequence of the definition of \mathbb{Z}^+ and the representation of integers.
- Suppose that $x < y$, this means that $a + d < b + c$. Note that $-x$ is $[(b, a)]$ and now we can sum it with y so:

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

And if we compare to $[(0, 0)]$ since $a + d < b + c$ we would have that $y - x > 0$ and therefore it belongs to \mathbb{N}^+ . The reverse implication is equivalent.

□

Integers have some more interesting properties! But they are not for our interest in this course, so we are going to continue with the next set we need.

3 Rational Numbers

In our everyday, we find expressions like *This pencil has a lead of 0.5cm* or *Give me half of the money*. These expressions are represented in mathematics in fractions, as a way to generalize the division for integers, and this structure is so important in algebra, number theory, and more; that is what we call rational numbers.

So, we think of them as fractions of the form $\frac{a}{b}$, like $\frac{1}{2}$. But also $\frac{1}{2}$ is the same as $\frac{2}{4}$ and $\frac{3}{6}$, so we can do a similar construction to which we did from natural numbers for integers. If two fractions $\frac{a}{b}$ and $\frac{c}{d}$ represent the same number, then $ad = bc$. We chose to construct this relation with all the coefficients except 0 since we are going to construct a field over this structure.

Definition 3.1. We define the relation \equiv over $\mathbb{Z} \times \mathbb{Z}^*$ in a way such that $(a, b) \equiv (c, d)$ if and only if $a \cdot d = b \cdot c$.

And what we have done is to relate all the elements which represent the same fraction.

Theorem 3.1. \equiv is an equivalence relation

Proof. • Note that $a \cdot b = a \cdot b$ so $(a, b) \equiv (a, b)$

- Suppose that $(a, b) \equiv (c, d)$, then $a \cdot d = b \cdot c$, so we can conclude that $c \cdot b = d \cdot a$ and therefore $(c, d) \equiv (a, b)$
- Suppose that $(a, b) \equiv (c, d)$ and $(c, d) \equiv (x, y)$. Then $a \cdot d = b \cdot c$ and $c \cdot y = d \cdot x$. If we multiply both sides we would have

$$\begin{aligned} a \cdot d \cdot c \cdot y &= b \cdot c \cdot d \cdot x \\ a \cdot y \cdot (c \cdot d) &= b \cdot x \cdot (c \cdot d) \\ a \cdot y &= b \cdot x \end{aligned}$$

And we conclude that $(a, b) \equiv (x, y)$.

□

Now, we have just a easy way to define what is a rational number in a similar way to what we did for integers with the relation we have constructed.

Definition 3.2 (Rational numbers). *The set $(\mathbb{Z} \times \mathbb{Z}^*) / \equiv$ will be denoted as \mathbb{Q} , the set of rational numbers and we call any element of \mathbb{Q} as a rational number.*

And what we need to complete the construction is operations over \mathbb{Q} . From our intuition, if we have $\frac{a}{b}$ and $\frac{c}{d}$ then

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

And also

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

And since by our construction $\frac{a}{b}$ is (a, b) then let us define the operations \oplus and \otimes as:

$$(a, b) \oplus (c, d) = (ad + bc, bd) \quad (a, b) \otimes (c, d) = (ac, bd)$$

If we prove that these operations are independent of the choice for (a, b) and (c, d) in the equivalence classes, we can take it as the definition for $+$ and \cdot over \mathbb{Q} .

Theorem 3.2. *If $(a, b), (c, d), (x, y), (z, w) \in \mathbb{Z} \times \mathbb{Z}^*$ such that $(a, b) \equiv (x, y)$ and $(c, d) \equiv (z, w)$ then:*

- $(a, b) \oplus (c, d) \equiv (x, y) \oplus (z, w)$
- $(a, b) \otimes (c, d) \equiv (x, y) \otimes (z, w)$

Proof. Note that the fact that $(a, b) \equiv (x, y)$ and $(c, d) \equiv (z, w)$ implies that:

$$ay = bx \quad cw = dz$$

For the first two operations we have:

$$\begin{aligned} (a, b) \oplus (c, d) &= (ad + bc, bd) \\ (x, y) \oplus (z, w) &= (xw + yz, yw) \end{aligned}$$

So, if we take the first equality we can operate like:

$$\begin{aligned} ay &= bx \\ ayd^2 &= bxd^2 \\ ayd^2 + bcdy &= xbd^2 + bcdy \end{aligned}$$

And this implies that $(a, b) \oplus (c, d) \equiv (x, y) \oplus (c, d)$. In a similar way we can prove that $(a, b) \oplus (c, d) \equiv (a, b) \oplus (z, w)$ and by transitivity we would have that $(a, b) \oplus (c, d) \equiv (x, y) \oplus (z, w)$.

Now, for the other two operations we would have:

$$\begin{aligned}(a, b) \otimes (c, d) &= (ac, bd) \\ (x, y) \otimes (z, w) &= (xz, yw)\end{aligned}$$

And if we multiply the first two equalities as follows we would have:

$$\begin{aligned}ac \cdot yw &= bd \cdot xz \\ acyw &= bdxz\end{aligned}$$

And we conclude that $(a, b) \otimes (c, d) \equiv (x, y) \otimes (z, w)$. □

And then we can define the operations over \mathbb{Q} :

Definition 3.3 (Operations over \mathbb{Q}). *Let $[(a, b)]$ and $[(c, d)]$ be rational numbers, we define:*

$$\begin{aligned}[(a, b)] + [(c, d)] &= [(a, b) \oplus (c, d)] \\ [(a, b)] \cdot [(c, d)] &= [(a, b) \otimes (c, d)]\end{aligned}$$

And this give us an important structure! A field!

Theorem 3.3. *The operations $+$ and \cdot forms a field over \mathbb{Q}*

Proof. • For rational numbers, the commutative and associative properties follows from the properties of \mathbb{Z} . The identity element $[(0, 1)]$ because:

$$\begin{aligned}[(a, b)] + [(0, 1)] &= [(a \cdot 1 + b \cdot 0, b \cdot 1)] \\ &= [(a + 0, b)] \\ &= [(a, b)]\end{aligned}$$

And for an inverse element for $[(a, b)]$ we have $[(-a, b)] = [(b, -a)]$ (Because of properties for rings in \mathbb{Z}). This can be view since:

$$\begin{aligned}[(a, b)] + [(-a, b)] &= [(a \cdot b - a \cdot b, b \cdot b)] \\ &= [(0, b^2)] \\ &= [(0, 1)]\end{aligned}$$

• The commutative and associative properties for \cdot follows again from properties from \mathbb{Z} . The identity element for this operation is given by $[(1, 1)]$ because:

$$\begin{aligned}[(a, b)] \cdot [(1, 1)] &= [(a \cdot 1, b \cdot 1)] \\ &= [(a, b)]\end{aligned}$$

And for the inverse element of $[(a, b)], [(b, a)]$:


$$\begin{aligned} [(a, b)] \cdot [(b, a)] &= [(a \cdot b, b \cdot a)] \\ &= [(a \cdot b, a \cdot b)] \\ &= [(1, 1)] \end{aligned}$$

- For the distributive property use:

$$\begin{aligned} [(a, b)] \cdot [(x, y)] + [(a, b)] \cdot [(z, w)] &= [(a, b)] \cdot [(xw + yz, yw)] \\ &= [(axw + ayz, byw)] \\ &= [(abxw + abyz, b^2yw)] \\ &= [(ax, by)] + [(az, bw)] \\ &= [(a, b)] \cdot [(x, y)] + [(a, b)] \cdot [(z, w)] \end{aligned}$$

So this holds for all rational numbers. □

And the last thing we need to define is an order for rational numbers. Think that a fraction is less than other, so $\frac{a}{b} \leq \frac{c}{d}$ then $ad \leq bc$. And that is what we are going to use.

 **Definition 3.4** (Order in \mathbb{Q}). Suppose that $[(a, b)]$ and $[(c, d)]$ are rational numbers with $b, d \in \mathbb{Z}^+ \cup \{0\}$. We say that $[(a, b)] \leq [(c, d)]$ if and only if $ad \leq bc$.

We can prove that this define an order:

 **Theorem 3.4.** \leq creates an order relation over \mathbb{Q}

Proof. Reflexive and antisymmetric are obvious. For transitivity suppose that $[(a, b)] \leq [(c, d)]$ and $[(c, d)] \leq [(x, y)]$, then:

$$ad \leq bc \qquad cy \leq dx$$

And if we multiply by y the first inequality and by b the second one:

$$ady \leq bcy \qquad bcy \leq bdx$$

And by the transitivity of \leq in \mathbb{Z} so:

$$\begin{aligned} ady &\leq bdx \\ ay &\leq bx \end{aligned}$$

And therefore $[(a, b)] \leq [(x, y)]$. And the linearity of \leq in \mathbb{Q} is a direct consequence of the linearity of \leq in \mathbb{Z} . □

If we denote $0 = [(0,0)]$ can define in a similar way as with the integers new sets with the order like $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ and also the set $\mathbb{Q}^+ = \{x \in \mathbb{Q} : x > 0\}$. Also, we can define an isomorphic set with \mathbb{Z} as $\mathbb{Z}' = \{[(m,1)] \in \mathbb{Q} : m \in \mathbb{Z}\}$, so we say that the integers are a *subset* of the rational numbers. We end this chapter with the last properties of rational numbers and we introduce the notation $\frac{p}{q}$ for the $[(p,q)]$ in way that $[(a,b)] = [(x,y)]$ then $\frac{a}{b} = \frac{x}{y}$.

 **Theorem 3.5.** Suppose that $x, y, z \in \mathbb{Q}$ then:

- If $x \leq y$ then $x + z \leq y + z$
- If $x \leq y$ and $z > 0$ then $x \cdot z \leq y \cdot z$
- If $x \leq y$ and $z < 0$ then $x \cdot z \geq y \cdot z$
- $x < y$ if and only if $y - x \in \mathbb{Q}^+$
- If $y > 0$ then there is $n \in \mathbb{N}$ such that $x < yn$
- If $x \leq y$ then there exists $a \in \mathbb{Q}$ such that $x \leq a \leq y$

Proof. We can suppose that $x = \frac{a}{b}$, $y = \frac{c}{d}$ and $z = \frac{e}{f}$

- If $x \leq y$ then $ad \leq bc$ and we can manipulate it as:

$$\begin{aligned}
 ad &\leq bc \\
 adf^2 &\leq bcf^2 \\
 adf^2 + bdf e &\leq bcf^2 + bdf e \\
 df(af + be) &\leq bf(cf + de)
 \end{aligned}$$

So we conclude that $\frac{af+be}{bf} \leq \frac{cf+de}{df}$ so $x + z \leq y + z$.

- If $\frac{e}{f} > 0$ then $e > 0$ and since $ad \leq bc$ then $ade \leq bce$ and since $f > 0$ by definition, $adf \leq bcf$ so $x \cdot z \leq y \cdot z$
- If $\frac{e}{f} < 0$ then $e < 0$ and since $ad \leq bc$ then $ade > bce$ and since $f > 0$ by definition, $adf > bcf$ so $x \cdot z \geq y \cdot z$
- If $x < y$ and $ad < bc$ and if we add $0 < bc - ad$ and since $\frac{c}{d} - \frac{a}{b} = \frac{ad-bc}{bd}$ and by definition it is greater than 0 so $y - x \in \mathbb{Q}^+$. The other side is the reverse implications.
- If $x \leq 0$ then $n = 1$ would be enough. If not, then note that $\frac{a}{b} \leq a$ since $a \leq a \cdot b$ because $1 \leq b$. And since $\frac{a}{b} > 0$ then $a \geq 1$ and therefore $a \leq a \cdot c$. And note that $a \cdot c = a \cdot d \cdot y$. Putting altogether

we would have:

$$\begin{aligned}
 \frac{a}{b} &\leq a \\
 &\leq a \cdot c \\
 &= ady \\
 &< ady + y \\
 &= (ad + 1)y
 \end{aligned}$$

- Take $a = \frac{1}{2}(x + y)$ which is:

$$\begin{aligned}
 a &= \frac{1}{2} \left(\frac{a}{b} + \frac{c}{d} \right) \\
 &= \frac{1}{2} \left(\frac{ad + bc}{bd} \right) \\
 &= \frac{ad + bc}{2bd}
 \end{aligned}$$

Note that due to the fact that $x \leq y$ we have that:

$$\begin{aligned}
 ad &\leq bc \\
 abd &\leq b^2c \\
 2abd &\leq abd + b^2c \\
 2b(ad) &\leq b(ad + bc)
 \end{aligned}$$

And we can conclude that $\frac{a}{b} \leq \frac{ad+bc}{2bd} = a$. In a similar way we can prove that $a \leq y$.

□