CONSTRUCTION OF INTEGERS

0.1. **Natural numbers.** We assume that the set of natural numbers

$$\mathbb{N} = \{\ 0, 1, 2, 3, 4, \dots\ \}$$

is given. We also assume that we know all usual properties and structures. Specifically, $\mathbb{N}$ is well-ordered, it comes with addition and multiplication which satisfy usual properties like

$$a + b = b + a$$

for every $a \in \mathbb{N}$ and every $b \in \mathbb{N}$. At this point, we will not go deeper into a discussion of the definition of natural numbers and justification of their properties. Instead, we will try to construct all the rest out of them.

Note that the operation of subtraction cannot always been performed for natural numbers. Indeed, the difference $1 - 2$ is not a natural number.

Let us consider this operation in some details.

0.2. **Subtraction.** Subtraction is defined as the inverse operation to addition.

By definition, $a - b$ is a number x such that $x + b = a$. In other words, $a - b$ is a solution to the equation

$$x + b = a, \tag{1}$$

and the absence of a natural number $1 - 2$ translates to the absence of solutions for $x + 2 = 1$.

We construct integers with an idea to supply equations (1) with solutions.

0.3. **Underlying idea.** An integer should be a solution to (1). Every such equation is determined by an ordered pair of natural numbers (a, b). We cannot, however, think of an integer as such a pair, because different equations may have same solution. Indeed, the equations $x + 1 = 2$ and $x + 3 = 4$ have same solution $x = 1$. Thus an integer should be a set of these equations which have same solution, or, equivalently, a set of ordered pairs (a, b).

This consideration motivates our construction.

0.4. **Definition.** Consider the set $\mathbb{N} \times \mathbb{N}$ of ordered pairs of natural numbers. Consider the relation $\sim$ on this set defined by

$$(m, n) \sim (p, q) \quad \text{if and only if} \quad m + q = n + p$$

Proposition. *The relation $\sim$ is an equivalence relation.*

Exercise. Prove the proposition.

This proposition allows us to consider the factor. We *define* the set of integers as

$$\mathbb{Z} = \mathbb{N} \times \mathbb{N} / \sim .$$

We think about a pair (m, n) as the "difference $m - n$", that is the solution to the equation $x + n = m$, and about an equivalence class as the set of these equations with the same solution.

Thus, by our definition, an integer is nothing but an equivalence class of ordered pairs of natural numbers, $[(m,n)]_\sim$.

0.5. **Naturals among integers.** We have only defined integers as a set, but we want much more from our integers: they must satisfy all properties which we expect from integers. First of all same integers are naturals, and we identify an integer $n \in \mathbb{N}$ with the equivalence class $[(n,0)]_\sim$. Indeed, n is the solution of $x + 0 = n$.

This identification allows us to consider $\mathbb{N}$ as a subset of $\mathbb{Z}$.

0.6. **Addition and multiplication.** We need usual operations on integers, and we define them now.

Addition is defined by

$$[(m,n)]_\sim + [(p,q)]_\sim = [(m+p, n+q)]_\sim, \tag{2}$$

and multiplication is defined by

$$[(m,n)]_\sim \cdot [(p,q)]_\sim = [(mp+nq, np+mq)]_\sim. \tag{3}$$

0.7. **Well-defined operations.** The definition of addition and multiplication by (2) and (3) requires immediate support. One has to prove that these operations are *well-defined*. In order to explain that, consider addition first. Formula (2) supposedly defines what should be the sum of two equivalence classes $[(m,n)]_\sim$ and $[(p,q)]_\sim$. However, these equivalence classes are written with the help of a choice of representatives: $[(m,n)]_\sim$ is an equivalence class of all pairs (m',n') such that $(m,n) \sim (m',n')$, and (m,n) is only one of them. Pick another one, say, (m',n') such that $(m,n) \sim (m',n')$ but $(m,n) \neq (m',n')$. What happens with our sum defined by (2)? It should stay the same simply because

$$[(m,n)]_\sim = [(m',n')]_\sim,$$

and we must have that

$$[(m',n')]_\sim + [(p,q)]_\sim = [(m,n)]_\sim + [(p,q)]_\sim.$$

But do we really have that? This is subject to check. Of course, the same applies to the second summand (p,q).

To sum up, the operations on equivalence classes in (2) and (3) are defined in terms of arbitrary choices of representatives in these classes. We have to check that the equivalence classes which we produce in the end does not depend on these arbitrary choices. That is what is called *well-defined*.

Proposition. *The operations on $\mathbb{Z} = \mathbb{N} \times \mathbb{N}/\sim$ described in (2) and 3) are well-defined.*

Proof. I provide here only a proof for the addition introduced by (2).

Let $(m,n) \sim (m',n')$ and $(p,q) \sim (p',q')$. That translates to

$$m + n' = m' + n \quad \text{and} \quad p + q' = p' + q \tag{4}$$

Then, according to (2) we have that

$$[(m',n')]_\sim + [(p',q')]_\sim = [(m'+p', n'+q')]_\sim.$$

We have to prove that the result of addition stays unaltered:

$$[(m'+p', n'+q')]_\sim = [(m+p, n+q)]_\sim,$$

or, equivalently, that

$$m' + p' + n + q = n' + q' + m + p,$$

and this immediately follows from (4). □

Exercise. Prove that multiplication is well-defined by (3).

0.8. **Extension of the operations from $\mathbb{N}$.** We have already identified some integers with natural numbers. If would be pretty bad if our newly-introduced operations have nothing to do with the operations of addition and multiplication defined for naturals. Specifically, let a and b be natural numbers. We have identified a with the integer $[(a,0)]_\sim$, and b with $[(b,0)]_\sim$. The sum $a+b$ is again a natural number which we may think about as an integer $[(a+b,0)]_\sim$. Do we produce same integer if we add integers $[(a,0)]_\sim + [(b,0)]_\sim$? The answer is yes, and it follows immediately from (2). We say that the operation of addition defined by (2) *extends* the addition of naturals. Equivalently, we can say that the operation of addition on $\mathbb{Z}$ defined by (2) being restricted to the subset $\mathbb{N} \subset \mathbb{Z}$ coincides with the usual operation of addition of natural numbers.

Proposition. *The operations of addition and multiplication on $\mathbb{Z}$ defined by (2) and (3) being restricted to the subset $\mathbb{N} \subset \mathbb{Z}$ coincide with the usual operations of addition and multiplication.*

Exercise. Give a full proof of the proposition.

0.9. **Distributive law.** There is a relation between addition and multiplication for natural numbers, namely the identity

$$a(b+c) = ab + ac \tag{5}$$

holds true for any $a, b, c\mathbb{N}$.

Exercise. Prove that (5) holds true for any $a, b, c\mathbb{Z}$.

0.10. **Subtraction of integers.** The goal of the construction of integers was to supply equations (1) with solutions. Let us now check that this goal is achieved. Indeed, for any integers

$$a = [(m,n)]_\sim \in \mathbb{Z} \quad \text{and} \quad b = [(p,q)]_\sim \in \mathbb{Z}$$

the equation (1) has solution

$$x = [(m+q, n+p)]_\sim \in \mathbb{Z}.$$

That is simply because by (2) we have

$$x + b = [(m+q, n+p)]_\sim + [(p,q)]_\sim = [(m+q+p, n+p+q)]_\sim = [(m,n)]_\sim,$$

where the last equality is implied by $(m+q+p, n+p+q) \sim (m,n)$. That allows us to introduce subtraction of integers

$$[(m,n)]_\sim - [(p,q)]_\sim = [(m+q, n+p)]_\sim,$$

for any naturals $m, n, p, q \in \mathbb{N}$ as the inverse operation to addition, and write

$$x = a - b$$

for the solution of (1).

Exercise. Make use of the cancellation property for naturals

$$(u + v = w + v) \implies (u = w)$$

for every $u, v, w \in \mathbb{N}$ to prove that equation (1) has *unique* solution.

0.11. **Traditional notations.** Of course, in order to simply use integers in the calculations, one does not need to understand the concept of equivalence classes. Instead, one writes negative integers with the minus-sign as $-n$ with a natural n (e.g. -2, etc.). As we have identified above natural numbers n with integers $[(n, 0)]_\sim$, we now identify negative numbers $-m$ with integers $[(0, m)]_\sim$ (here $m > 0$ is supposed to be natural).

Exercise. Derive from our definition that the product of two negative numbers is positive. Illustrate that with

$$(-2)(-3) = 6,$$

and take it for an explanation, not merely a rule.

0.12. **Order relation.** As I mentioned in the beginning, natural numbers come with an order relation $\leq$. We will use it in order to introduce an order relation on $\mathbb{Z}$ now.

$$[(m, n)]_\sim \leq [(p, q)]_\sim \quad \text{if and only if} \quad m + q \leq n + p \tag{6}$$

Exercise. Prove that the relation $\leq$ is well-defined by (6).

Exercise. Prove that the relation $\leq$ extends the relation $\leq$ on the subset $\mathbb{N} \subset \mathbb{Z}$.

Exercise. Prove that the relation $\leq$ on $\mathbb{Z}$ is an order relation.

The set $\mathbb{Z}$ is not well-ordered by $\leq$: already $\mathbb{Z}$ itself does not have a minimum with respect to $\leq$. One can, however, introduce another order relation on $\mathbb{Z}$ which is closely connected with $\leq$ and makes $\mathbb{Z}$ well-ordered by $\preceq$. Define the relation $\preceq$ by

$$[(m, n)]_\sim \preceq [(p, q)]_\sim \quad \text{if and only if} \quad (m - n)^2 \leq (p - q)^2.$$

Exercise. Prove that the relation $\preceq$ on $\mathbb{Z}$ is an order relation.

Exercise. Prove that set $\mathbb{Z}$ is not well-ordered by $\preceq$.

0.13. **Back from integers to naturals.** It is already observed in 0.5 above that we can think about natural numbers as a subset of integers: $\mathbb{N} \subset \mathbb{Z}$. We can also think about naturals as a quotient set of integers. What we are about to do is nothing but the consideration of the absolute value of an integer. Define equivalence relation $\approx$ on $\mathbb{Z}$ by

$$[(m, n)]_\sim \approx [(p, q)]_\sim \quad \text{if and only if} \quad ((m, n) \sim (p, q)) \vee (((n, m) \sim (p, q)). \tag{7}$$

With this definition, we have to prove that the relation $\approx$ on $\mathbb{Z}$ is well-defined. Specifically, assuming that $(m', n') \sim (m, n)$, and $(p', q') \sim (p, q)$, we need to prove that

$$[(m, n)]_\sim \approx [(p, q)]_\sim \quad \text{implies} \quad [(m', n')]_\sim \approx [(p', q')]_\sim.$$

While quite straightforward to verify using (7), this check-up s extremely important: without this verification, definition (7) canon be considered as a legitimate one.

Exercise. Prove that the relation $\approx$ on $\mathbb{Z}$ is well-defined.

Exercise. Prove that $\approx$ is an equivalence relation on $\mathbb{Z}$.

Exercise. Identify the quotient set $\mathbb{Z}/\approx$ of $\mathbb{Z}$ modulo $\approx$ with $\mathbb{N}$. Hint: for every integer $z \in \mathbb{Z}$, consider $|z| \in \mathbb{N}$.

Note that, with this construction, while the operation of multiplication still survives (because $|ab| = |a||b|$ for any integers a and b) the operation of addition fails to carry through.