A Construction of the Numbers: The Integers

Mandar Juvekar and Arian Nadjimzadah
M14085-teachers@esp.mit.edu

1 So far...

- Intuitively, what is a (natural) number?
  - A way to count collections of objects.
- To have a coherent mathematical system to work with numbers, we must have rigorous formal definitions for them.
  - Informal definitions often lead to various paradoxes and other issues (for example Russel's paradox in set theory).
- One useful way to formalize concepts is with an **axiomatic system**.
  - An axiomatic system has a fixed set of **axioms** which are statements assumed to be true.[1]
  - A statement is said to be true if it follows logically from the axioms and other true statements. Such statements are often labelled **theorems**.
- We gave a formal definition of the natural numbers via an axiomatic system. These were the so-called **Peano axioms**.
- We inductively defined addition and subtraction on $\mathbb{N}$. We also defined an order on $\mathbb{N}$ by stating what it means for a number to be greater than another.

Today we will look past the naturals and define the integers. Note that while formally defining the integers we will assume that most properties of natural numbers that we learn in school can be (and have been) proved under our formalism. In theory we could go through and prove every single property we need, but that would be neither fun nor time-efficient.

Throughout this document we have marked a few results as "exercises". These aren't intended to be "homework" as such, but are rather results that we think you could prove in your spare time.

Administrative Note: There was a typo in the notes for day 1 in the teacher email for this course. Please be sure to use the email at the top of this document. We have uploaded an updated version the day 1 notes to course documents which can be accessed through the ESP website (the only change is the email).

2 Thinking Past the Naturals

Think of the statement $1 + x = 4$. Does there exist a natural number x such that the statement becomes true? Yes! We know that $x = 3$ makes the statement true. But what about the statement $4 + x = 1$? We know that adding natural numbers can only give larger natural numbers, and since $1 < 4$, this means that there is no $x \in \mathbb{N}$ that will make our statement true.

Let us try to generalize these equations a bit more. Let a and b be natural numbers. Let us define $E_{a,b}(x)$ to be the statement that $a + x = b$. We call an $x \in \mathbb{N}$ such that $E_{a,b}(x)$ is true a **solution** of the **equation** $E_{a,b}$. We observe that a solution to $E_{a,b}$ exists if and only if $a \leq b$.

Our aim is to find a meaningful "enlargement" of the set $\mathbb{N}$ such that all equations $E_{a,b}$ have solutions in that set. This set will end up being $\mathbb{Z}$, the set of integers.

[1] Technically we would also need to specify a set of rules of inference to work with statements, but as we said for the purposes of this course we will work with intuitive logical rules. See Section 4.2 from the day 1 notes.

2.1 Uniqueness of Solutions to Equations

Before we even define integers, we show that solutions to equations $E_{a,b}$ (which we assume will always exist in the system we will later define) are unique. In doing so, we will also assume that a + operation is defined which is consistent with the addition of natural numbers. Let r and s be solutions to $E_{a,b}$. Then we have:

$$a + r = b$$
$$a + s = b$$

By transitivity of equality, we get that $a + r = a + s$. We know that we can cancel a from both sides of the equation (that's an easy result to prove using the definition of addition on $\mathbb{N}$), and so we get $r = s$. Thus solutions to equations in our extended system would be unique.

2.2 When can two equations have the same solution?

Suppose $E_{a,b}$ and $E_{c,d}$ have the same solution r. Then we get:

$$a + r = b$$
$$d = c + r$$

Adding these equations, we get $a + r + d = b + c + r$, and cancelling r from both sides, we get $a + d = b + c$. Thus we see that $E_{a,b}$ and $E_{c,d}$ have the same solutions if and only if $a + d = b + c$. In symbols:

$$(\exists x \; E_{a,b}(x) \wedge E_{c,d}(x)) \iff a + d = b + c$$

3 Equivalence Relations

Suppose that you want to categorize pencils based on color. Consider creating a box for each possible color and throwing the pencils into their respective boxes. For pencil x in box B, x certainly has the same color as itself. Additionally if x has the same color as y then both are in the same box, and of course y has the same color as x. Finally if x and y have the same color and y and z do, then clearly x and z are in the same box.

What if the property of the object is harder to get our hands on? Is it possible to obtain these boxes based on a relation with the nice properties we discovered, instead of the other way around? In fact, yes! This is the notion of an *equivalence relation.*

Definition 1. An **equivalence relation** on a set S is a binary relation $\sim$ with the following properties: For any $x, y, z \in S$,

1. $x \sim x$ (reflexivity)
2. $x \sim y \implies y \sim x$ (symmetry)
3. $x \sim y$ and $y \sim z \implies x \sim z$ (transitivity)

We saw in lecture 1 that $=$ is an equivalence relation. Now we want to show that an equivalence relation has the sought after partitioning property.

Definition 2. Take $a \in S$ The **equivalence class of a**, denoted $[a]$ is given by

$$\{x \in S : x \sim a\} \tag{1}$$

These are the "boxes"... but we still don't know if they act like boxes!

Theorem 1. *Let S be a set with an equivalence relation $\sim$. For every $a, b \in S$, either $[a] = [b]$ or $[a]$ and $[b]$ are disjoint.*

Proof. Suppose that $[a]$ and $[b]$ are not disjoint. Then there is an element s in common, so $s \sim a$ and $s \sim b$. We show that $[a] \subseteq [b]$. Take any $x \in [a]$. Then $x \sim a$. By symmetry, $a \sim s$. Then by transitivity $x \sim s$. Again by transitivity, using $s \sim b$, we get $x \sim b$. Thus $x \in [b]$, giving $[a] \subseteq [b]$. By reversing the roles of a and b we get $[b] \subseteq [a]$, and so $[a] = [b]$, as desired. □

Now we know that two boxes are either the same or completely disjoint, but do we know that every element is in a box? Yes, this follows directly from reflexivity. Hence equivalence classes partition the set on which an equivalence relation is defined.

4 Defining the Integers

Notice that under our desired system, equations $E_{a,b}$ of natural numbers a and b have unique solutions in the integers. So we could identify a natural number with an equation $E_{a,b}$ whose solution it should be. A problem with this is that the same integer could also be an solution to other equations of natural numbers, and so we would have many ways to define the same number, which would make our definition faulty. However, the general idea of identifying integers by equations to which they are solutions is still valid. Could we somehow represent integers by the entire class of equations it is a solution to?

Definition 3. For the rest of this class, we define the relation $\sim$ to be a relation on pairs of natural numbers. Given $a, b, c, d \in \mathbb{N}$, we define $(a, b) \sim (c, d)$ if $E_{a,b}$ and $E_{c,d}$ have exactly the same solution, i.e. if $a+d = b+c$.

Exercise. Verify that $\sim$ is an equivalence relation. Do this by checking that it follows the three defining properties of equivalence relations from Definition 1.

Since $\sim$ is an equivalence relation, it must have disjoint equivalence classes that partition the set $\mathbb{N} \times \mathbb{N}$ (the set of pairs of natural numbers). Take a pair $(a, b) \in \mathbb{N} \times \mathbb{N}$. Let us denote the equivalence class of (a, b) under $\sim$ with $[a, b]$. Which pairs are in $[a, b]$? These are the pairs which are equivalent to (a, b), and so are all pairs (c, d) such that $E_{a,b}$ and $E_{c,d}$ have the same solutions. Thus the equivalence class $[a, b]$ is a set of pairs of natural numbers which represent a class of equations with the same solution. In fact, it contains representations of all such equations. We will now define the integers to be these classes.

Definition 4. Each equivalence class $[a, b]$ of the natural numbers under $\sim$ is an **integer**. The set of all such equivalence classes is the set of integers which we denote with $\mathbb{Z}$.

Now that we have a definition for the integers, we are left with a few different gaps to fill:

- We said that $\mathbb{Z}$ extends $\mathbb{N}$. In what sense can we consider $\mathbb{N}$ to be a subset of $\mathbb{Z}$?
- We need to come up with a way of adding, multiplying, and ordering integers that is compatible with the way we add, multiply, and order natural numbers.
- We still have to verify that the integers truly can be considered solutions of the equations $E_{a,b}$.

4.1 Finding $\mathbb{N}$ in $\mathbb{Z}$

We define a function $\iota : \mathbb{N} \to \mathbb{Z}$ by $\iota(n) = [0, n]$. We use this function to "identify" natural numbers n with a corresponding integer $\iota(n)$. Before we do that, we must verify that ι is 1-1[2], i.e. it doesn't send two different natural numbers to the same integer (if it did it would be a bad way to identify the naturals).

Theorem 2. *$\iota : \mathbb{N} \to \mathbb{Z}$ defined by $\iota(n) = [0, n]$ is 1-1.*

Proof. Suppose $\iota(a) = \iota(b)$ for some $a, b \in \mathbb{N}$. Then $[0, a] = [0, b]$. This gives us that $(0, a)$ and $(0, b)$ are in the same equivalence class, i.e. $(0, a) \sim (0, b)$. By definition of $\sim$ we have $0 + b = a + 0 \iff a = b$, and so we are done. □

[2]A function f is 1-1 (also called one-to-one or injective) if for all x, y we have $f(x) = f(y) \iff x = y$.

When we say that the natural numbers are a subset of the integers, we really mean that the corresponding integers as defined by ι behave the same as the original natural numbers, and so can in some sense be considered "the same" as the originals. We will verify this when we define addition and multiplication.

Exercise. Show that for any $a, b \in \mathbb{N}$ we have:

1. $[a, 0] = [b, 0] \iff a = b$
2. $[a + b, a] = [b, 0]$ and $[a, a + b] = [0, b]$

These are some facts that might be useful later.

5 Addition on the Integers

As we said before, we want integers to (intuitively) represent hypothetical solutions to equations of the form $E_{a,b}$. We use this idea to guide our definition of addition. Suppose r and s are hypothetical solutions to $E_{a,b}$ and $E_{c,d}$ respectively. What equation would $r + s$ be a solution of? Well, we have

$$a + r = b, \text{ and}$$
$$c + s = d$$

which we can add to get

$$(a + c) + (r + s) = (b + d)$$

In other words, $r+s$ would be the hypothetical solution for $E_{a+c,b+d}$. This motivates the following definition:

Definition 5. Given any integers $[a, b]$ and $[c, d]$ we define the **sum** $[a, b] \oplus [c, d]$ as:

$$[a, b] \oplus [c, d] = [a + c, b + d]$$

We use the symbol $\oplus$ instead of just $+$ to distinguish it from natural number addition and to remind ourselves that they are two differently defined operations. We will switch over to just $+$ later.

An important aspect of definitions involving equivalence classes is to make sure that the definition does not change if we change the representatives we use. For instance let $(a_1, b_1) \sim (a_2, b_2)$ and $(c_1, d_1) \sim (c_2, d_2)$. In this case $[a_1, b_1] = [a_2, b_2]$ and $[c_1, d_1] = [c_2, d_2]$. We need to make sure that $[a_1, b_1] \oplus [c_1, d_1] = [a_2, b_2] \oplus [c_2, d_2]$, because all of these are equally reasonable representatives for their respective equivalence classes. This is done in the following theorem:

Theorem 3. *Suppose* $(a_1, b_1) \sim (a_2, b_2)$ *and* $(c_1, d_1) \sim (c_2, d_2)$. *Then* $(a_1 + c_1, b_1 + d_1) \sim (a_2 + c_2, b_2 + d_2)$. *Hence* $[a_1, b_1] \oplus [c_1, d_1] = [a_2, b_2] \oplus [c_2, d_2]$ *which means that our definition is coherent.*

Proof. Since $(a_1, b_1) \sim (a_2, b_2)$ and $(c_1, d_1) \sim (c_2, d_2)$, we have (from the definition of $\sim$):

$$a_1 + b_2 = b_1 + a_2$$
$$c_1 + d_2 = d_1 + c_2$$

Adding these and using associativity we get:

$$(a_1 + c_1) + (b_2 + d_2) = (b_1 + d_1) + (a_2 + c_2)$$

which is simply by definition gives us $(a_1 + c_1, b_1 + d_1) \sim (a_2 + c_2, b_2 + d_2)$. □

The following theorem contains a few very important properties of integer addition.

Theorem 4. *Let* $a, b, c, d, e, f \in \mathbb{N}$. *Then the following hold:*

(a) $[a, b] \oplus ([c, d] \oplus [e, f]) = ([a, b] \oplus [c, d]) \oplus [e, f]$ *(associativity)*

(b) $[a, b] \oplus [0, 0] = [a, b] = [0, 0] \oplus [a, b]$ *($[0, 0]$ is an additive identity)*

(c) $[a,b] \oplus [b,a] = [0,0] = [b,a] \oplus [a,b]$ *(existance of additive inverses)*

(d) $[a,b] \oplus [c,d] = [c,d] \oplus [a,b]$ *(commutativity)*

Proof. These properties can be verified quite easily using the definition of addition. We leave this as an exercise to the reader. □

Remark.
1. Notice that part (b) shows that $[0,0]$ is the *additive identity* for the integers. In other words, this is the (integer) '0' we are used to. It is fairly straightforward (especially after we introduce groups) to show that the additive identity is unique.
2. Part (c) shows that $[b,a]$ is an *additive inverse* of $[a,b]$. We often write this as $[b,a] = -[a,b]$. Thus we can define *subtraction* to mean $[a,b] - [c,d] = [a,b] + (-[c,d]) = [a,b] + [d,c]$. Similar to the identity, it is easy to show that the additive inverse of a given integer is unique.
3. It is easy to see that $-(-[a,b])) = [a,b]$.

Theorem 5. *ι preserves addition. That is, for any $a, b \in \mathbb{N}$, $\iota(a+b) = \iota(a) \oplus \iota(b)$. Hence addition for natural numbers is indeed extended by integer addition.*

Proof.

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

□

Now that we have shown that addition of naturals is extended by integer addition, it makes sense to simply use $+$ instead of $\oplus$ to represent both integer and natural number addition. At this point, since we have identified $n \in \mathbb{N}$ with an integer $\iota(n)$, we would like to start denoting the integer $\iota(n)$ as just n. If we do need to distinguish between the natural number and integer n, we will specify as necessary.

Theorem 6. *Every integer is either a natural number or the additive inverse of a natural number. Hence it makes sense to write $\mathbb{Z} = \mathbb{N} \cup -\mathbb{N}$ where $-\mathbb{N}$ is the set of additive inverses of natural numbers (as integers, via ι of course).*

Proof. Take an arbitrary integer $[a,b]$. If $a = b$, then $[a,b] = [a,a] = 0$, which is a natural number. If $a \neq b$, then either $a < b$ or $a > b$. If $a < b$ then there is a natural number p such that $a + p = b$. Hence we have $a+p = b+0 \iff (a,b) \sim (0,p)$. This means that $[a,b] = [0,p]$, and so $[a,b]$ is a natural number (p, namely). If $a > b$ then there is a natural number q such that $a = b + q$. We have $a + 0 = b + q \iff (a,b) \sim (q,0)$. So $[a,b] = [q,0] = -[0,q]$, which means $[a,b]$ is the additive inverse of a natural number. □

5.1 Algebraic Structure of $\mathbb{Z}$ under Addition

This section is a quick note introducing the concept of a *group*, which is an important structure in abstract algebra.

Definition 6. A **group** is a set X equipped with a binary operation $\star$ such that the following properties hold:

1. For all $a, b \in X$, $a \star b \in X$.
2. For all $a, b, c \in X$, $a \star (b \star c) = (a \star b) \star c$ (associativity).
3. There is an element $e \in X$ such that for all $a \in X$ we have $a \star e = a = e \star a$ (existence of an identity).
4. For every $a \in X$ there exists an inverse element, $a^{-1} \in X$ such that $a \star a^{-1} = e = a^{-1} \star a$ (existence of inverses).

By definition, integer addition is closed, i.e. for every $a, b \in \mathbb{Z}$, $a + b \in \mathbb{Z}$. Also, we have shown that integer addition is associative, that 0 is an additive inverse, and that for every integer a there is an element $-a$ such that $a + (-a) = 0$. This means that *the integers under addition are a group.* Sometimes this is also written as $(\mathbb{Z}, +)$ *is a group.*

On the other hand, $(\mathbb{N}, +)$ is *not* a group. Why? Because condition 4 in Definition 6 is not met, since natural numbers (except 0) do not have additive inverses which are also natural numbers.

It is possible to prove a lot of neat things about groups. Among others this includes the uniqueness of inverses and the identity element, and a lot of other properties. What's even cooler is that these results apply to every group out there. This means that results proved for groups not only hold for the integers under addition, but also for other groups including the invertible matrices under multiplication (the "general linear group"), permutations under composition (the "symmetric group"), and many more. Unfortunately this is out of the scope of this class. If you are interested, we encourage checking out [3] for a quick introduction to group theory, or [2] for a more comprehensive introduction (the latter is a standard algebra textbook).

6 Ordering the Integers

We can extend the ordering on the natural numbers to the integers.

Definition 7. Let $m, n \in \mathbb{Z}$. Then $m \leq n$ if there is some $k \in \mathbb{N}$ such that $m + k = n$. With $m < n$, we require that $k \neq 0$.

Theorem 7. *For any $m, n, p \in \mathbb{Z}$*

1. *Either $m < n$, $m = n$, or $m > n$.*
2. *The following are equivalent: $n \in \mathbb{N}$, $n \geq 0$, $-n \leq 0$.*
3. *$m < n \iff -n < -m$.*
4. *$m < n$ and $n < p$ implies $m < p$.*
5. *$m < n \implies m + p < n + p$.*

Proof. This proof is left as an exercise to the reader (just push around the definitions). □

Definition 8. We say an integer n is **positive** if $n > 0$ and **negative** if $n < 0$.

7 Multiplications on the Integers

To decide how we should define multiplication, we think back to our equations of the form $E_{a,b}(x)$. Let $r = [a, b]$ and $s = [c, d]$, that is r satisfies $a + r = b$, and s satisfies $c + s = d$. What equation would rs be a solution of? When we multiply these equations and add ac to both sides, we get

$$\begin{aligned}(a + r)(c + s) &= bd \\ ac + rc + as + rs + ac &= bd + ac \\ (a + r)c + a(c + s) + rs &= bd + ac \\ (bc + ad) + rs &= bd + ac.\end{aligned}$$

Thus we see that rs is a solution to $E_{bc+ad,bd+ac}$, and so we propose the following definition for multiplication (to distinguish this from multiplication over $\mathbb{N}$, we temporarily use the symbol $\otimes$).

Definition 9. For any $[a, b], [c, d] \in \mathbb{Z}$, we define $[a, b] \otimes [c, d]$ by

$$[a, b] \otimes [c, d] = [ad + bc, bd + ac]$$

As was done with addition, we are left to show that $\otimes$ is a well defined operation.

Theorem 8. *If $[a,b] = [w,x]$ and $[c,d] = [y,z]$, then $[a,b] \otimes [c,d] = [w,x] \otimes [y,z]$.*

Proof. The proof is left as an exercise to the reader. □

Again as we did with addition, we show that for natural numbers, $\otimes$ coincides with our definition of multiplication from last class. Take $n, m \in \mathbb{N}$. Then $\iota(n) \otimes \iota(m) = [0,n] \otimes [0,m] = [0 \cdot n + m \cdot 0, mn + 0 \cdot 0] = [0, mn] = \iota(mn)$.

Thus it is safe to adopt the usual notation, which we do in the theorem below.

Theorem 9. *Take any $m, n, p \in \mathbb{Z}$. Then*

1. $m(np) = (mn)p$
2. $mn = nm$
3. $m \cdot 1 = 1 \cdot m = m$
4. $m > 0$ *and* $n < p$ *implies* $mn < mp$
5. $m(n+p) = mn + mp$
6. *If* $mn = 0$ *then* $m = 0$ *or* $n = 0$.
7. *If* $m \neq 0$ *then* $mn = mp \iff n = p$

Proof. We leave the proof as an exercise to the reader. □

7.1 Algebraic Structure of $\mathbb{Z}$ under Multiplication

Is $(\mathbb{Z}, \cdot)$ a group? Well, to be a group it would have to satisfy the four defining properties of groups (see Definition 6). By the way we defined it, multiplication is closed, i.e. integers multiply to give integers. Also, we proved above that multiplication is associative, and that 1 is a multiplicative inverse. However, we know that inverses under multiplication do not exist in the integers. For example, it is easy to verify that there is no integer x such that $x \cdot 2 = 1$, which means that 2 has no multiplicative inverse in the integers. This means that $(\mathbb{Z}, \cdot)$ is *not* a group.

Definition 10. A set X equipped with a binary operation $\star$ is a **monoid** if all the criteria for being a group are met except possibly the existence of inverses.

Is $(\mathbb{Z}, \cdot)$ a monoid? Yes! We now define a useful algebraic structure which ties together both our operations.

Definition 11. A set X equipped with two binary operations $+$ and $\cdot$ forms a **ring** if:

1. $(X, +)$ is a group
2. For all $a, b \in X$, $a + b = b + a$ ($+$ is commutative)
3. $(X, \cdot)$ is a monoid
4. $\cdot$ is distributive over $+$, i.e. for all $a, b, c \in X$ we have
   (a) $a \cdot (b + c) = a \cdot b + a \cdot c$
   (b) $(b + c) \cdot a = b \cdot a + c \cdot a$

Notice that we have verified all properties of rings for $\mathbb{Z}$ under addition and multiplication. Hence we say that $(\mathbb{Z}, +, \cdot)$ is a ring.

Remark. 1. While the definition of a ring uses the symbols $+$ and $\cdot$, it is important to note that these do not refer to addition and multiplication. Rather, they are just symbols referring to two binary operations on the set. There can, and do, exist rings where the two operations are nothing like addition and multiplication.

2. Notice that $\cdot$ does not need to be commutative in the definition of a ring. Matrix rings are examples of rings that have a non-commutative multiplication operation.

While ring theory is outside the scope of this course, we recommend [2] for a more in-depth explanation of rings and various other algebraic facts relating to them.

8 Limitations...

How well do the integers handle solutions to other very useful equations? Consider the statement $M_{a,b}(x) : ax = b$. There are many situations where this equation has no solutions.

Theorem 10. *Suppose $a \in \mathbb{Z}$ and $a > 1$. Then there is no $b \in \mathbb{Z}$ such that $ab = 1$.*

Proof. This is a relatively straightforward exercise using some of the theorems involving ordering. We leave this to the reader. □

This is a real defect in our system, so next class we will go through a similar process to enlarge $\mathbb{Z}$ to a system just powerful enough to solve any $M_{a,b}$ (except when $a = 0$ and $b \neq 0$).

9 Countability

Definition 12. A function $f : A \to B$ is bijective if

- For any $x, y \in A$, if $f(x) = f(y)$ then $x = y$. (f is **injective**)
- For any $b \in B$, $\exists x \in A$ such that $f(x) = b$. (f is **bijective**)

Definition 13. A set A is **countable** if there is a bijection between A and some subset of $\mathbb{N}$. A is **countably infinite** if there is a bijection between A and $\mathbb{N}$ itself.

$\mathbb{N}$ is of course countable, in particular by considering the bijection $f(x) = x$. $\mathbb{Z}$ is also countable. Let it be an exercise to find the bijection and prove it!

Definition 14. We say that two sets A and B are **equipotent** if there exists a bijection between A and B.

It isn't too hard to see that equipotence is an equivalence relation on the set of all sets. This means that all sets (yes, all of the uncountably infinite sets out there) can be characterized into "boxes" of equipotent sets. How cool!

10 More Information

A large part of this document follows [1], although we did change/simplify parts of it. The document more or less contains a more verbose and thorough write-up of the things we went over (and likely a bunch more). We recommend checking it out if interested.

References

[1] The Integers. `http://pi.math.cornell.edu/~web3040/integers_s11.pdf`. Accessed 2020-07-16.

[2] John B. Fraleigh. *A First Course in Abstract Algebra.* Addison-Wesley, Boston, 7th ed. edition.

[3] Jake Wellens. A friendly introduction to group theory. `http://math.mit.edu/~jwellens/Group%20Theory%20Forum.pdf`. Accessed 2020-07-17.