3 The Principle of Mathematical Induction, Peano's Axioms, and Inductive Definitions

3.1 The principle of mathematical induction

In this section I recall the principle of mathematical induction by way of several examples. The principle of mathematical induction is the technique that allows us to give a mathematical formalization of an intuitively obvious fact that if in an infinite sequence of statements the first statement is true and any statement implies the next one, therefore all the statements must be true because the first one implies the second one, the second one implies the third one, the third one implies the fourth one, and so on. In some sense mathematical induction is a right tool to remove somewhat vague "and so on" from mathematical reasonings. It is important not to confuse the principle of mathematical induction with the general inductive thought process (inductive reasonings), which is frequently described as "from particular to general" and which is used in natural sciences (and sometimes even in mathematics) to provide support for some principles (laws of nature). Strictly speaking inductive reasonings cannot *prove* anything, whereas the principle of mathematical induction is a tool for a rigorous mathematical proof (somewhat probably confusing the principle of mathematical induction is an example of *deductive* reasonings).

Now to an informal description of the principle of mathematical induction. Assume that we have a statement $P(n)$, which we would like to prove (i.e., we would like to make sure that $P(n)$ is true for all $n \geq k$ for some given fixed k). To apply the principle of mathematical induction one needs to check two things: first, the *base case* $P(k)$. In many cases $k = 1$ but in general it is possible to start with any natural number. Second, one needs to prove the induction step $P(n) \implies P(n+1)$ for *any* $n \geq k$. In words, the induction step is as follows: *assuming* that $P(n)$ true one concludes that $P(n+1)$ is also true. (At this point some students get confused: "we need to prove that $P(n)$ is true, and in the middle of the proof we assume that $P(n)$ is true, isn't it a logical mistake?" There is no mistake, since we suppose that $P(n)$ is true to see what will happen in this case, whether $P(n+1)$ will be also true, that is the goal of the proof is the truth of the logical statement $P(n) \Rightarrow P(n+1)$, different from simply $P(n)$.)

Putting the general discussion aside, here are a few examples how the principle of mathematical induction can be used in proofs. Note that every time one uses the mathematical induction the final true outcome should be known; that is, while we can use the mathematical induction to prove something we already know or, more often, conjectured, it is impossible to discover something new by this technique.

Example 3.1. Recall that triangular numbers can be computed as

$$t_n = \frac{n(n+1)}{2}\,, \quad n = 1, 2, \ldots$$

and moreover

$$1 + 2 + \ldots + n = t_n = \frac{n(n+1)}{2}\,. \tag{3.1}$$

Let me prove this formula using the mathematical induction (let's assume that we checked this formula for $n = 1, 5, 10, 15$ but still unsure that it holds for all possible n).

Math 478/678: History of Mathematics by Artem Novozhilov
e-mail: artem.novozhilov@ndsu.edu. Spring 2024

Base case $n = 1$. I have (plugging $n = 1$ into both sides of (3.1))

$$1 = \frac{1(1+1)}{2} = 1,$$

which is true. Hence the base case holds.

Induction step: I suppose that $1 + \ldots + n = \frac{n(n+1)}{2}$ and will show that this implies $1 + \ldots + n + (n+1) = \frac{(n+1)(n+2)}{2}$ for all $n \geq 1$. Indeed,

$$1 + 2 + \ldots + n + (n+1) = \big(1 + 2 + \ldots + n\big) + (n+1) = \text{[by assumption]}$$
$$\frac{n(n+1)}{2} + (n+1) = \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2},$$

as required.

Example 3.2 (Bernoulli's inequality)**.** In this example I will prove

Theorem 3.3. *Let $x \geq -1$ and $n \in \mathbf{N}$. Then*

$$(1+x)^n \geq 1 + nx.$$

Proof. Proof by induction.

Base case $n = 1$:

$$(1+x)^1 = 1 + x = 1 + 1 \cdot x,$$

as needed.

Induction step. Assume that $(1+x)^n \geq 1 + nx$. I need to show that $(1+x)^{n+1} \geq 1 + (n+1)x$ for all $n \geq 1$. I have

$$\begin{aligned}(1+x)^{n+1} &= (1+x)^n(1+x) \geq \text{[by assumption and using the fact that } x \geq -1\text{]} \\ &\geq (1+nx)(1+x) = 1 + nx + x + nx^2 \geq \text{[since } nx^2 \geq 0\text{]} \\ &\geq 1 + nx + x = 1 + (n+1)x\end{aligned}$$

as required. ■

Example 3.4. In this example I will show that it is not necessary to start the induction with $n = 1$.

Example 3.5 (Strong induction)**.**

3.2 Peano's axioms of natural numbers

Recall that when we discussed Euclid's Elements, we agreed that the system of axioms by Euclid, although an incredible breakthrough for the history of mathematics, is not exactly rigorous according to the modern mathematical standards. Certainly this is the place to give an example of a system of axioms that is rigorous. For such an example I picked the so-called Peano's axioms of natural numbers. I will not develop the whole theory of natural numbers in detail, and I will not try to be as precise as possible (this would require a long side trip into the realm of mathematical logic), and yet I will try to convey the main ideas.

In what follows I use the usual set theoretic notation such as $x \in X$ meaning that x is an element of set X, and $X \subseteq Y$ meaning that set X is a subset of set Y.

One of main psychological difficulties here is that I plan to talk about the objects such as $1, 2, 3, \ldots$, which we deal with since we are 2 or 3 year old, so in many situations it will look somewhat strange that a very basic fact that we knew for many years to be true requires a proof, and in certain cases requires, albeit still simple, but at the same time confusing for humans (or at least for me). I would request the student at this point to concentrate on the ultimate goal: To deduce (and prove!) as many properties of natural numbers as we know them from as few as possible initial axioms without assuming that anything is already known.

Definition 3.6. *Natural numbers are the elements of a set, which I will denote* $\mathbf{N}$*, that satisfy the following five axioms.*

$A1:$ The set $\mathbf{N}$ is non-empty and contains an element that I call 1 ("one").

$A2:$ For any $n \in \mathbf{N}$ there is unique natural number $n' \in \mathbf{N}$ (I call n' the *successor* of n).

$A3:$ For any $n' \in \mathbf{N}$, $n' \neq 1$ (in words, 1 is not a successor for any natural number).

$A4:$ If $m' = n'$ then $m = n$ (two different natural numbers cannot have the same successor).

Remark 3.7. Some people define natural numbers as $\mathbf{N} = \{0, 1, 2, \ldots\}$, i.e., starting with 0. There is no real difference with the approach I choose, clearly in this case the special element, which is not a successor for any other natural number, must be 0.

Axioms $A1$–$A4$ define the very basic properties of natural numbers, which we got used to since our childhood, and yet they are not sufficient for the development of all the properties of natural numbers. Note that if I consider the following set

$$\{1 \to 2 \to 3 \to 4 \to \ldots\} \cup \{A \leftrightarrows B\},$$

where $\to$ means exactly that the element on the right is the unique successor of the element at the left, and hence for the second set B is the successor of A and A at the same time is the successor of B, then this set satisfies all four axioms listed above. I need something else, which would make my set of natural numbers *minimally possible*, which would exclude the behavior I listed above. This can be done in different ways, but I choose probably the most popular one: I add the *the axiom of mathematical induction*:

$A5:$ If $M \subseteq \mathbf{N}$ has the properties

- (a) $1 \in M$,
- (b) If $n \in M$ then $n' \in M$,

then $M = \mathbf{N}$.

It is actually remarkable that now we can derive and prove all other familiar properties of natural numbers.

Remark 3.8. To be absolutely precise no one said that a set with properties $A1$–$A5$ exists. So we either need to postulate the existence of such set (this was Peano's sixth axiom) or somehow *prove* the existence of such set starting with some other axioms (this actually can be done rigorously, but would take us way too far from the main content of the class). So let us not worry about this issue at all.

Now I am in a position to define *addition* of two natural numbers, which will be based on the following theorem.

Theorem 3.9. *For any natural number $n \in \mathbf{N}$ there exists a unique function $f_n \colon \mathbf{N} \longrightarrow \mathbf{N}$ that satisfies*

(*a*) $f_n(1) = n'$;

(*b*) $f_n(m') = \big(f_n(m)\big)'$.

Definition 3.10. *For any two natural numbers $n, m \in \mathbf{N}$ we define their sum, denoted $n + m$, as*

$$n + m := f_n(m),$$

where f_n specified in Theorem 3.9.

Remark 3.11. Now it could be useful to see that the definition of addition is simply

$$n + 1 := n'$$

and

$$n + m' := (n + m)' = (n + m) + 1,$$

which is an example of an *inductive definition*.

Proof of Theorem 3.9.

Uniqueness. My goal here is by fixing an arbitrary $n \in \mathbf{N}$ and assuming that there exist two functions that satisfy (*a*) and (*b*), i.e.,

$$f_n(1) = n', \quad f_n(m') = f_n(m)'$$

and

$$g_n(1) = n', \quad g_n(m') = f_n(m)'$$

to show that $f_n(m) = g_n(m)$ for all $m \in \mathbf{N}$, that is, $f_n = g_n$. Hopefully not surprisingly I will use mathematical induction since it is hidden in my goal that I need to check the required equality for all natural m at the same time, this is exactly what mathematical induction allows me to do.

Let $M \subseteq \mathbf{N}$ be the set of such m that $f_n(m) = g_n(m)$.

Base case: Since $f_n(1) = 1' = g_n(1)$ and by $A2$ the successor is unique, I have $1 \in M$.

Induction step: I need to show that if $m \in M$ then $m' \in M$, that is, if $f_n(m) = g_n(m)$ then $f_n(m') = g_n(m')$. Indeed,

$$\begin{aligned} f_n(m') &= \text{[by the property (}b\text{)]} = \\ &= \big(f_n(m)\big)' = \text{[by induction assumption]} = \\ &= \big(g_n(m)\big)' = \text{[by the property (}b\text{)]} = \\ &= g_n(m') \end{aligned}$$

as required. Hence by $A5$ $M = \mathbf{N}$ and such function, if exists, is unique.

Existence. Now I will show that a function that satisfies (a) and (b) exists (and by the previous is the only one). Before starting the proof let me try to point out what exactly I need to accomplish here. In statement of Theorem 3.9 I already inductively defined f_n for any fixed n by specifying two key properties. That is, if n is fixed, then for any m the properties (a) and (b) in the statement of the theorem are sufficient to compute $f_n(m)$. The remaining part I need to check is that it works for *all* n at the same time. It is tempting just to say something along the line "by induction our definition is true for any n and hence we defined our function for all natural n, m, and hence this function exists" but mathematically this still requires a proof. Which will be accomplished by the induction on n.

First, I *define* another function for any fixed $m \in \mathbf{N}$ inductively as

$$f_n(m) = \begin{cases} m', & n = 1, \\ f_{k'}(m) = \big(f_k(m)\big)', & n \neq 1,\ n = k'. \end{cases} \tag{3.2}$$

For the following note that (3.2) implies that $f_{n'}(m) = \big(f_n(m)\big)'$. I will show below that such defined function coincides with the function given in the statement of the theorem, and this is why I used the same notation for it. Now to the actual proof.

Let $N \subseteq \mathbf{N}$ be the set of those natural numbers n for which function (3.2) satisfies (a) and (b). I claim that $1 \in N$. Indeed, for $n = 1$ and $m = 1$ definition (3.2) implies that

$$f_1(1) = 1',$$

which coincides with property (a) for $n = 1$. For $n = 1$ and $m \neq 1$ definition (3.2) yields (I use twice (3.2) for $n = 1$)

$$f_1(m') = (m')' = \big(f_1(m)\big)',$$

which is Property (b) for $n = 1$. Base case is done.

Now I need to show that $n \in N \implies n' \in N$. I start with the case $m = 1$:

$$f_{n'}(1) = [\text{by (3.2)}] = \big(f_n(1)\big)' = [\text{by induction assumption}] = (n')',$$

which finishes proving property (a).

Similarly,

$$\begin{aligned} f_{n'}(m') &= [\text{by definition (3.2)}] = \\ &= \big(f_n(m')\big)' = [\text{by induction assumption}] = \\ &= \Big(\big(f_n(m)\big)'\Big)' = [\text{by (3.2)}] = \\ &= \big(f_{n'}(m)\big)', \end{aligned}$$

as required. Hence by $A5$ $N = \mathbf{N}$, which concludes the proof. ■

I actually proved a little bit more. Indeed, now using the standard notation "+" for addition, I have

Corollary 3.12. *For any $m \in \mathbf{N}$*

$$m + 1 = 1 + m.$$

Proof. By Theorem 3.9 and definition of addition

$$m+1 = [\text{by definition}] = f_m(1) = (a) = m' = (3.20) = f_1(m) = \text{by defintion} = 1+m.$$

■

Moreover, by agreeing that $2 = 1'$ (i.e., we denote by 2 the successor of 1), $3 = 2' = 1''$, $4 = 3' = 2'' = 1'''$ (here I use shorter notation, e.g., $1''$ for the successor of the successor of 1, etc.) we can prove the fundamental

Theorem 3.13.

$$2+2=4.$$

Proof.

$$2+2 = 1'+1' = (1'+1)' = \big((1+1)'\big)' = ((1')')' = 1''' = 4$$

as required. ■

Note that here I used $n'+m = (n+m)' = (n+m)+1$ in addition to the discussed earlier $n+m' = (n+m)' = (n+m)+1$.

Before moving forward with other properties of addition let me show that the axiom of mathematical induction $A5$ is equivalent to the principle of mathematical induction that I discussed in Section 3.1. I delayed this discussion to this point because, technically speaking, I did not know what $n+1$ means up till now.

Theorem 3.14. *Axiom $A5$ is equivalent to the principle of mathematical induction as stated in Section 3.1.*

Proof. Assume first the principle of mathematical induction holds, i.e., for some statement $P(n)$ we know that $P(1)$ holds, and $P(n) \implies P(n+1)$ (we now finally know what $n+1$ means!), and hence we know that $P(n)$ is true for any natural n. Consider the set $M = \{n\colon P(n) \text{ is true}\}$. Clearly, I have that $1 \in M$, $n \in M \implies n' \in M$, and $M = \mathbf{N}$, which is exactly axiom $A5$. In the opposite direction, assume $A5$ and consider the statement $P(n) =$"natural number n belongs to the set M." We have that, assuming $A5$, that two true statements $P(1)$ and $P(n) \implies P(n+1)$ imply that $P(n)$ for any natural n, and hence done. ■

Remark 3.15. Do not get confused by the proof above. We showed nothing else other than our ability to rewrite the same principle either in the language of the sets (axiom $A5$) or in the language of logic (the principle of mathematical induction).

After we defined the addition, the properties of this operations becomes *theorems*. Here is an example.

Theorem 3.16. *For any $k, m, n \in \mathbf{N}$ the addition is associative:*

$$(k+m)+n = k+(m+n).$$

Proof. Proof by induction on n.

Fix $k, m \in \mathbf{N}$ and let N be the set of those natural numbers n for which the associative property holds. First, $1 \in N$ since

$$(k+m)+1 = (k+m)' = k+m' = k+(m+1).$$

Now assume that $n \in N$ and consider

$$(k+m)+n' = ((k+m)+n)' = [\text{since } n \in N] = (k+(m+n))' = k+(m+n)' = k+(m+n')$$

as required. ■

Exercise 1. Use induction to show that the addition commutative, i.e.,

$$m+n = n+m$$

for any $m, n \in \mathbf{N}$.

Before moving forward, let me state the following theorem (and another inductive definition).

Theorem 3.17. *For any fixed $n \in \mathbf{N}$ there exists a unique function $g_n \colon \mathbf{N} \longrightarrow \mathbf{N}$ that satisfies for all $m \in \mathbf{N}$ the following two properties:*

(a) $g_n(1) = n$.

(b) $g_n(m') = g_n(m) + n$.

This function is called the multiplication of two natural numbers n, m and denoted $n \times m$ or $n \cdot m$ or simply nm.

This operation of multiplication is distributive with respect to addition, i.e.,

$$k(m+n) = km + kn,$$

and

$$(k+m)n = kn + mn,$$

associative, i.e.,

$$(km)n = k(mn),$$

and commutative, i.e.,

$$nm = mn,$$

for all $k, m, n \in \mathbf{N}$.

Exercise 2. Prove this theorem. *Hint:* Prove the properties in the order given in the theorem statement.

Now we have two arithmetic operations "+" and "×" and showed that all the basic properties of these operations that we so got used to during the school years are the consequences of five axioms. Is it all about the natural numbers? Not really, since using addition I can introduce an *order* on the set of natural numbers. From a theoretical point of view an order is a relation on a set (i.e., a subset of Cartesian product $\mathbf{N} \times \mathbf{N}$) but to keep thing as simple as possible I just say

Definition 3.18. *We say that $m \leq n$ if either $m = n$ or there is $k \in \mathbf{N}$ such that $m + k = n$.*

Defined in this way order is a linear or total order on $\mathbf{N}$, i.e., for any $n, m \in \mathbf{N}$ it is either $m \leq n$ or $m \geq n$, moreover, by this definition $n \leq n + 1$ as our experience tells us. Strictly speaking it it necessary to prove that such order exists and actually is unique, but I will skip these proofs (it is quite a lengthy process but no more difficult than the proofs given above).

Since I have an order, I can look at a set version of the strong mathematical induction (recall the discussion from the previous section). If the student is comfortable with the material covered so far, it should be of no surprize that in the language of sets the principle of the strong mathematical induction takes the form

$A5'$: If $S \subseteq \mathbf{N}$ has the properties

(a) $1 \in S$,

(b) If $\{k\colon k \leq n\} \subseteq S$, then $n + 1 \in S$,

then $S = \mathbf{N}$.

It looks likes it is a stronger version compared to $A5$, but in reality they are equivalent. I will show that $A5$ implies $A5'$ and will leave formalization of the opposite (intuitively almost obvious) direction to the reader.

Proposition 3.19. $A5 \Rightarrow A5'$.

Proof. Assume $A5$ holds and that $1 \in S$ and $\{k\colon k \leq n\} \subseteq S \Rightarrow n + 1 \in S$. I need to show that $S = \mathbf{N}$.

Construct a new set M such that $n \in M \Leftrightarrow \{k\colon k \leq n\} \subseteq S$. Clearly $M \subseteq S$. Moreover $1 \in M$ since $\{1\} \subseteq S$, and $n \in M \Rightarrow n + 1 \in M$ since by assumption both $\{k\colon k \leq n\}$ and $\{k\colon k \leq n + 1\} = \{k\colon k \leq n\} \cup \{n + 1\}$ are subsets of S. Therefore, by $A5$ $M = \mathbf{N}$, i.e., $\mathbf{N} \subseteq S \subseteq \mathbf{N}$ and hence $S = \mathbf{N}$ as required. ■

My final key point in the discussion of natural numbers will be an explanation when one can use the principle of mathematical induction. Specifically, I will prove

Theorem 3.20. *Let $\mathbf{N}$ be the set that satisfies $A1$–$A4$, and let "$\leq$" be the total order on $\mathbf{N}$ for which $n \leq n+1$. Then axiom $A5'$ is equivalent to the well-ordering principle, i.e., to the fact that each nonempty subset of $\mathbf{N}$ has the minimal element. And therefore the well ordering principle is equivalent to the axiom of mathematical induction $A5$.*

Remark 3.21. Theorem 3.20 tells us a very important thing: It specifies for which sets one can use mathematical induction. Namely, if on a given set there is an order such that well-ordering principle holds then we can use induction. Interestingly, there is a way to introduce an order for any set such that well-ordering principle will be true; that is in principle the mathematical induction can be used on *any* set (if you became curious at this point, read about transfinite induction).

Proof of Theorem 3.20.

$\Rightarrow$ (axiom $A5'$ implies the well-ordering principle) Proof by contradiction. Looking for a contradiction, assume that we have set $B \subseteq \mathbf{N}$, $B \neq \varnothing$ and B has no minimal element. Let $M = \mathbf{N} \setminus B$, i.e.,

the complement of B. We know that $1 \in M$ since otherwise B would have the smallest element. Let $\{k\colon k \le n\} \subseteq M$, then $n+1 \in M$ because otherwise $n+1 \in B$ would be the smallest element. Axiom $A5'$ now implies that $M = \mathbf{N}$ or $B = \varnothing$, which is a contradiction.

$\Leftarrow$ (well-ordering principle implies axiom $A5'$) Let M be a set such that $1 \in M$ and $\{k\colon k \le n\} \subseteq M \Rightarrow n+1 \in M$. The goal is to show that $M = \mathbf{N}$. Looking for a contradiction, assume that $B = \mathbf{N} \setminus M \neq \varnothing$. Let $n \in B$ be its least element which exists by the well-ordering principle. Then by Peano's axioms, $n = m+1$ for some $m \in \mathbf{N}$. By our assumption $\{k\colon k \le m\} \Rightarrow m+1 \in M$, hence $n = m+1$ cannot be in B, which is a contradiction. ■

3.3 Integers, Rational, and Reals

Having at our disposal all the properties of natural numbers (addition, multiplication, and total order with the usual familiar from school properties) it is possible to construct *all* number sets we also deal with at school. I am not going to do it here, and will jump very fast from integers, to rational, to real numbers (saving the complex numbers for the next part of the course) emphasizing the key properties without much discussion. The only reason is that our time is limited, and it would be somewhat boring to spend the rest of the semester discussing precise constructions. For the interested student I will give a few literature references at the end of the next section.

So, let us start.

Definition 3.22. *The set of integers, which is usually denoted as* $\mathbf{Z}$ *or* $\mathbb{Z}$ *is, by the definition the union of three sets:*

$$\mathbf{Z} = \mathbf{N} \cup \{0\} \cup \{-k\colon k \in \mathbf{N}\}.$$

That is, to define the integers, I take the already defined set $\mathbf{N}$, add to it a special element that I call *zero*, and also add another copy of the set $\mathbf{N}$, now denoting all the elements with sign minus, to distinguish them from the first copy of $\mathbf{N}$. I also require that the following properties hold for the arbitrary x, y, z elements of $\mathbf{Z}$:

$$\begin{aligned}
(x+y)+z &= x+(y+z) && (\textit{associativity of addition})\\
x+y &= y+x && (\textit{commutativity of addition})\\
x+0 &= 0+x = x && (\textit{neutral element of addition})\\
x+(-x) &= 0 && (\textit{existence of inverses with respect to addition})\\
(xy)z &= x(yz) && (\textit{associativity of multiplication})\\
xy &= yz && (\textit{commutativity of multiplication})\\
1x &= x1 = x && (\textit{neutral element of multiplication})\\
x(y+z) &= xy+xz && (\textit{distributivity of multiplication w.r.t. addition})
\end{aligned} \tag{3.3}$$

If the student already has taken a class in abstract algebra, they should recognize that the set of integers $\mathbf{Z}$ forms an algebraic structure that is called *ring* (to be more precise, *commutative ring* since the operation of multiplication is commutative).

Moreover, set $\mathbf{Z}$ inherits the order from $\mathbf{N}$. That is, there is a total or linear order on the elements of $\mathbf{Z}$ (recall that this means that for any $x, y \in \mathbf{Z}$ either $x \le y$ or $y \le x$) which satisfies two properties

$$\begin{aligned}
x \le y &\Rightarrow x+z \le y+z,\\
0 \le x,\ 0 \le y &\Rightarrow 0 \le xy.
\end{aligned} \tag{3.4}$$

With these two order properties $\mathbf{Z}$ becomes an *ordered* ring.

Remark 3.23. I would like to emphasize that all the properties (3.3) and (3.4) can be made into theorems if a somewhat more precise definition of $\mathbf{Z}$ is used. None of this is postulated, all which is used is the axioms and already proved properties of $\mathbf{N}$ together with a new definition.

Remark 3.24. The properties of the set of integers allow us to give one possible answer to the question "why negative times positive is negative?" (or related question "why negative times negative is positive?"). Namely, we must have these rules to keep that structure of the ring intact (again, in any commutative ring properties (3.3) must be true). For instance, we know that $5 \cdot 5 = 25$ from the properties of natural numbers. Now we have that $5 = 7 + (-2)$. Therefore, one should have

$$25 = 5 \cdot 5 = 5(7 + (-2)) = 5 \cdot 7 + 5 \cdot (-2) = 35 + 5 \cdot (-2),$$

which will be true only if $5 \cdot (-2) = -(5 \cdot 2)$.

I stress that such "an explanation" is not appropriate at a school level, where some analogies with either movement (forward is positive direction and backward is negative direction) or lending and borrowing money are certainly more appropriate.

With rational numbers I would like to be more careful. So first I would like to recall an *equivalence relation* on a set X.

A Cartesian product of two sets X and Y is a set of all ordered pairs (x, y), i.e., $X \times Y = \{(x, y) \colon x \in X,\ y \in Y\}$. A relation R on a set X is by definition a subset of $X \times X$. Finally, a relation R called an equivalence relation on set X if

$$\begin{aligned} &(x, x) \in R && (\textit{reflexivity}) \\ &(x, y) \in R \Rightarrow (y, x) \in R && (\textit{symmetry}) \\ &(x, y) \in R,\ (y, z) \in R \Rightarrow (x, z) \in R && (\textit{transitivity}) \end{aligned}$$

Instead of writing $(x, y) \in R$ it is more convenient and suggestive to use the notation $x \sim y$, which I will be doing from now on. Examples of equivalence relation include "is congruent to," "in similar to" on the set of all triangles, "have the same birthday" on the set of all people, etc.

The utility of equivalence relation is the fact that it allows to give *classification* on the given set X, i.e., it allows to divide into mutually exclusive nonempty subset whose union gives the whole set.

Let me denote $[x]$ the set of all elements y of X that satisfy $x \sim y$, mathematically $[x] = \{y \in X \colon x \sim y\}$. This set is called *equivalence class* with representative x. Using this notation I state

Lemma 3.25. *Let $x, y \in X$. If $[x] \cap [y] \neq \varnothing$ then $[x] = [y]$.*

Proof. Let $z \in [x] \cap [y]$. This implies that $z \sim x$ and $z \sim y$, therefore, by symmetry and transitivity $x \sim y$, that is for any $a \sim y$ $x \sim a$ and for any $b \sim x$ $y \sim b$, as required. ■

Finally the definition of the set of rational numbers $\mathbf{Q}$.

Definition 3.26. *Let $X = \mathbf{Z} \times \mathbf{N}$. By definition the set of rational numbers $\mathbf{Q}$ is the set of all equivalence classes on X with the equivalence relation*

$$(a, b) \sim (c, d) \Longleftrightarrow ad = bc.$$

Remark 3.27. If the definition above seems to be confusing think about pairs (a, b) and (c, d) as ratios a/b and c/d.

Remark 3.28. To practice your understanding of the given definition, consider a different definition of set $\mathbf{Z}$. Let $X = \mathbf{N} \times \mathbf{N}$. Then set $\mathbf{Z}$ is the set of all equivalence classes on X with the equivalence relation $(a, b) \sim (c, d)$ if and only if $a + d = b + c$. Maybe you can try to use this definition to derive all the properties in (3.3) and (3.4)?

Exercise 3. Check that the defined relation is indeed an equivalence relation on X.

Set $\mathbf{Q}$ is an example of algebraic structure called *field*. To list all the axioms of a field I need to take all the axioms of a ring in (3.4) and add just one more thing: For any nonzero $x \in Q$ there exists its multiplicative inverse y such that $xy = yx = 1$. This inverse is usually denoted x^{-1}. It can be also checked that $\mathbf{Q}$ is an *ordered field*, i.e., it satisfies (3.4).

So far so good, but here comes the main question. Recalling the school years and other mathematics classes, it should be clear that the set of real numbers $\mathbf{R}$ is also an ordered field in exactly the same way as $\mathbf{Q}$ is. And yet there must be a difference because we already know that there are real numbers, which are not in $\mathbf{Q}$. The difference lies in the so-called *completeness axiom*.

Definition 3.29. *The set of real numbers, denoted* $\mathbf{R}$*, is an ordered field for which the completeness axiom holds: if* $A, B \neq \varnothing$ *are subsets of* $\mathbf{R}$ *and* $A \leq B$ *meaning that for any* $a \in A$ *and* $b \in B$ *we have* $a \leq b$ *then there is* $c \in \mathbf{R}$ *which divides* A *and* B*, i.e.,* $a \leq c \leq b$ *for all* $a \in A$ *and* $b \in B$*.*

First let me show that $\mathbf{Q}$ does not satisfy the completeness axiom.

Theorem 3.30. *Let* $A = \{a \in \mathbf{Q} \colon a^2 < 2,\, a > 0\}$ *and* $B = \{b \in \mathbf{Q} \colon b^2 > 2,\, b > 0\}$ *be two subsets of* $\mathbf{Q}$*. Then there is no rational* $c \in \mathbf{Q}$ *that divides* A *and* B*.*

Proof. By contradiction. Assume that there is such $c \in \mathbf{Q}$. Then three cases are possible:

$$\begin{aligned} (i) \quad & c^2 = 2, \\ (ii) \quad & c^2 < 2, \\ (iii) \quad & c^2 > 2. \end{aligned}$$

Consider one by one. Case (i) is not possible because as we already know there is no rational c that satisfies $c^2 = 2$.

For case (ii), assume that $c^2 < 2$ has been found as required. The idea is to find an $\varepsilon \in \mathbf{Q}, \varepsilon > 0$ for which $(c + \varepsilon)^2 < 2$ and hence $(c + \varepsilon) \in A$ thus reaching the contradiction that c divides A and B. Indeed, simplifying,

$$\begin{aligned} (c + \varepsilon)^2 < 2 \Leftrightarrow \\ c^2 + 2c\varepsilon + \varepsilon^2 < 2 \Leftrightarrow \\ 2c\varepsilon + \varepsilon^2 < 2 - c^2 \end{aligned}$$

Since $2c\varepsilon + \varepsilon^2 = \varepsilon(2c + \varepsilon) < \varepsilon(2c + 1)$ for small ε, if I find ε that satisfies

$$\varepsilon(2c + 1) < 2 - c^2$$

then I am done. I can take, e.g.,

$$\varepsilon = \frac{2 - c^2}{k(2c + 1)},$$

where $k > 1$ is any rational number that also guarantees that $\varepsilon < 1$, which concludes the proof of case (ii), since $c + \varepsilon \in A$ and clearly $c + \varepsilon > c$.

Case (iii) is left as an exercise. ■

Note that if we accept the *axiom of completeness* of set $\mathbf{R}$ then we get (think this out!)

Corollary 3.31. *In* $\mathbf{R}$ *for the sets* A, B *defined in the previous theorem the number that divides* A *and* B *is* $c = \sqrt{2}$.

So, does it mean that we have to add something to our list of axioms to actually build $\mathbf{R}$? The answer is no (in some situations, however, not to work sequentially through $\mathbf{N}, \mathbf{Z}, \mathbf{Q}$, the list of axioms of $\mathbf{R}$ is given at the beginning, which saves a lot of time). With a proper definition the set $\mathbf{R}$ can be constructed from $\mathbf{Q}$ such that the axiom of completeness becomes a theorem. This, however, will require much more mathematical sophistication compared to constructions of $\mathbf{Z}$ out of $\mathbf{N}$ or $\mathbf{Q}$ out of $\mathbf{Z}$ and $\mathbf{N}$, and will be skipped here (the details can be found in the literature at the end of the next section).

To finish this section I would like to mention that there are quite a few statements equivalent to the axiom of completeness. For instance, it is equivalent to the statement, which you might have seen in Calculus I, that any nondecreasing bounded sequence of real numbers has a limit (converges). Another equivalent statement is the intermediate value theorem, which states that any continuous function that takes negative and positive values on a given interval must have a zero in this interval (this is not true for continuous functions on $\mathbf{Q}$, which makes it impossible to have analysis on $\mathbf{Q}$ similar to the one we have on $\mathbf{R}$).