The Natural Numbers $\mathbb{N}$

(7/11/23)

Alex Nita

Contents

1 The Background

Let us start with an observation by the historian of mathematics, Jeremy Gray:

> *"The origin of modern mathematics can be found in the mathematical practices of the nineteenth century. It has become a commonplace that the nineteenth century saw the rigorization of analysis under the slogan, coined by Felix Klein in a public lecture in 1895, of the "arithmetization of analysis." (Gray [7][p. 18])*

The nineteenth century attempt to ground the calculus of Newton and Leibniz in axioms analogous to those which support Euclidean geometry led inexorably to axiomatizations of numbers, their arithmetic and limiting properties. The subsequent derivation of analysis from numbers follows fairly straightforwardly. Why numbers and not geometry? Following the discovery that Euclid's fifth postulate was independent of the other four, and the attendant proliferation of non-Euclidean geometries, confidence in geometry faded. Arithmetic was the last bastion of certainty, and hence it was that the foundations of analysis were steered in that direction. The outcome was the development of the theory now known as *real analysis*, which is a strange hybrid of physical intuition and mathematical rigor: on the one hand, analysis is the handmaiden of classical mechanics, the theory of motion; on the other hand, it is a formal logical theory grounded in something "real" and "certain," namely numbers.

> *"There are indeed two foundational aspects at work–one largely* ontological, *the other largely* epistemological. *The first is the one usually called the* arithmetization of analysis. *It traces a path from Cauchy's novel theory of functions in the 1820s that was based on certain limiting processes defining continuity, differentiability, and integrability through its unclear notion of the real numbers to an eventual resolution somewhere in the use of limiting processes to* define *the real numbers...The* epistemological *aspect stays with the notion of continuity: its separation from differentiability [and] the emergence of a class of phenomena sometimes called pathological and which required special techniques to handle..." (Gray [7][p. 20])*

The "certainty" of numbers mentioned above refers to the certainty of the natural numbers $\mathbb{N}$, for certainty was the very thing missing from the reals $\mathbb{R}$ prior to the nineteenth century. We will assess this certainty below, but let us merely assume it for the moment. *The important point here is that, given* $\mathbb{N}$, *there are explicit, formal constructions of the integers* $\mathbb{Z}$ *out of the natural numbers* $\mathbb{N}$ *(by "adding in" the negatives), of the rationals* $\mathbb{Q}$ *out of the integers* $\mathbb{Z}$ *(by "adding in" the quotients), and finally of the reals* $\mathbb{R}$ *out of the rationals* $\mathbb{Q}$ *(there are several such constructions,* *all isomorphic, all somehow "adding in" the limits).* See Olmsted [14], chapters 3 and 5, for the formal development of $\mathbb{N}$ to $\mathbb{Q}$, and see chapter 9 for $\mathbb{R}$; we give a brief sketch below in sections 5-6. A few points concerning these constructions:

(1) The natural numbers $\mathbb{N}$ must also be axiomatized, and constructions offered, as we explain below. But the axiomatizations of $\mathbb{Z}$ and $\mathbb{Q}$ aren't really needed, since all of the important properties of these objects are encoded in the axioms of $\mathbb{N}$. The constructions of $\mathbb{Z}$ and $\mathbb{Q}$ are all isomorphic, anyway. We will discuss $\mathbb{N}$ in the next section.

*(2) There is a sort of "quantum leap" when going from $\mathbb{Q}$ to $\mathbb{R}$, identifiable by the fact that it requires a new axiom, the **Axiom of Completeness** for $\mathbb{R}$. We will spend the first half of the semester characterizing this new axiom, among other things.*

*(3) The axiomatic nature of $\mathbb{R}$ becomes important here. The various constructions of $\mathbb{R}$ out of $\mathbb{Q}$ mentioned above must be viewed as **models** in the sense of model theory. The difference between axioms and models has its origin in the separation of syntax from semantics in mathematical logic, which occurred in the early 20th century, with the resulting separation of axiomatics and proofs, on the one hand, from their interpretations or realizations on the other. One can assert that a theorem is provable from the axioms without saying that the theorem is true, for truth requires meaning and hence an interpretation of the terms involved.*

Let us elaborate a little on this last point. We will see, for example, that the Intermediate Value Theorem (IVT) is provable from the Axiom of Completeness (and vice-versa, as it turns out), but to say that the IVT is "true" requires something else, some notion of what the IVT *means*. This meaning is encoded in a model, or construction, of $\mathbb{R}$. But now comes an important curveball: all models of $\mathbb{R}$ are isomorphic (a theorem we will prove below, called the **categoricity** of $\mathbb{R}$) *if we are working in a second-order theory*, as we will be, but not if, as with most logicians, we work in a first-order theory (see the Remark at the end of Subsection 2.2.3). Thus, if all models of $\mathbb{R}$ are isomorphic, there is no ambiguity concerning meaning, and we may identify provability and meaning. See Awodey and Reck [1]-[2] and Baez [3] for an overview, and Hedman [8] for the details.

Let us add a fourth observation, of a slightly different flavor:

(4) *The real numbers $\mathbb{R}$ are required for analysis because we want to say things like*

$$\lim_{x\to a} f(x) = f(a) \quad \text{and} \quad f'(a) = \lim_{x\to a}\frac{f(x)-f(a)}{x-a}$$

and these involve the word limit *and the statement $x \to a$. Before we even discuss limits, however, we notice that functions are relations between variable quantities x and y, which means x and y* vary over $\mathbb{R}$, *or* take numerical values in $\mathbb{R}$. *This definition doesn't require anything special about $\mathbb{R}$; we could have used $\mathbb{Q}$ or $\mathbb{C}$ or even arbitrary sets X and Y. However, when we let x "approach" $a \in \mathbb{R}$, and check whether $f(x)$ "approaches" $f(a)$, or in the other case, whether $\frac{f(x)-f(a)}{x-a}$ approaches a real number we call $f'(a)$, then we recognize the need for an elaboration of what all this means.* ***The limiting properties of functions, central to calculus, requires the limiting properties of $\mathbb{R}$.***

These are some of the issues we should have in the back of our minds as we go forward into the details. Our main focus in this course will be on $\mathbb{R}$, but we now stop briefly to outline some of the highlights of the development from $\mathbb{N}$ to $\mathbb{Q}$ in the next section.

2 The Peano Axioms for $\mathbb{N}$

2.1 The Rules of Arithmetic for $\mathbb{N}$

The **natural numbers** $\mathbb{N}$ are the proper theater for **arithmetic**, which is the correct application of the **rules of counting**. In fact, as the category theorist Saunders MacLane observes ([13][p. 42]), it is precisely the long human experience with counting and listing that resulted in the distillation of the *rules of reckoning* to a short *formal* list:

For all $n, m, p \in \mathbb{N}$, we have the following **rules of arithmetic**:

(1) $n + 0 = n$ (0 *is the **additive identity***)

(2) $n + m = m + n$ (***commutativity** of* $+$)

(3) $(n + m) + p = n + (m + p)$ (***associativity** of* $+$)

(4) $1n = n = n1$ (1 *is the **multiplicative identity***)

(5) $mn = nm$ (***commutativity** of* $\cdot$)

(6) $(mn)p = m(np)$ (***associativity** of* $\cdot$)

(7) $p(m + n) = pm + pn$ (***distributivity** of* $\cdot$ *over* $+$)

MacLane ([13][p. 42]) succinctly summarizes the nature of these rules:

> *"[T]hese (long-established) rules are inviolate: If it doesn't turn out as they specify, I know that I have made a mistake somewhere. This is the merit of a formal rule: Once firmly established, it can be applied mechanically and is an infallible guide."*

This list is the manifestation of the certainty we feel arithmetic possesses. Indeed, these rules are so simple, so inviolable, they might even be used to *characterize* or perhaps *define* the natural numbers. That is the natural inclination one feels at first.

The only problem, the only cloud on the horizon, is the claim that this list holds true *for all* natural numbers m, n and p. But there are *infinitely many* such numbers, so the best we could ever do is incrementally increase our confidence in the list (by verifying it for larger and larger numbers), but we will never attain certainty. Even putting this issue aside, it is *practically* more and more difficult to verify the rules for larger and larger numbers. The upshot is that there is no effective way to *verify* this list. Why, then, should we believe it?

2.2 The Need for Grounding the Arithmetical Rules of $\mathbb{N}$

Reflection on this issue demonstrates the need for some sort of **grounding** of the rules of $\mathbb{N}$, and hence for $\mathbb{N}$ itself. Historically, there have been two main attempts:

2.2.1 The Metaphysical Grounding of $\mathbb{N}$ and $\mathbb{R}$ in Forms

For this section, refer to Klein [11]. In the olden days of Plato and the Neo-Pythagoreans of late antiquity, numbers had a **metaphysical** grounding in **forms**, those ideal structural skeletons underlying matter and giving it shape. Aristotle, at *Metaphysics* 987b20-22, says, "As the matter (of number) [Plato] posits the great and small for principles, as substance [or form] the one; for by mixture of the one with them he says numbers arise." *Matter*, according to Aristotle and the Platonists, is shapeless, unbounded, and indefinite; it is the purpose of *form* to shape it. Bronze (matter) may be moulded into a statue (form), or melted down into bars (another form). The **one**, or the **monad**, is the *form* of **quantitative variation**, represented by what they called the **indefinite dyad** of small-to-large, and identified with *matter* precisely because of its indefiniteness, it's ambiguity between the two poles of smallness and largeness.

1. **Natural numbers** $\mathbb{N}$ can be used for *counting*, and the count puts a measure or form on the otherwise amorphous collection of objects being observed. A restaurant's count of 100 wine bottles puts a measure on the otherwise shapeless mass of wine bottles, telling us how many "ones" there are of those bottles. Debts can be measured by negative integers. If we consider m even divisions of a unit length, the resulting pieces have length $1/m$. Then k/m measures the resulting length of the concatenation of k pieces of length $1/m$. This roughly describes the appearance of the **integers** $\mathbb{Z}$ and **rational numbers** $\mathbb{Q}$ as measures of (ac)counting variation.

2. **Real numbers** $\mathbb{R}$ can be used to measure *length* more generally, for length is a *continuously* variable physical property. Length varies from zero to infinity, i.e. some very large positive numbers when you go to the astronomical scale, with no visible upper limit. The *unit* of measure, the "one," captures and shapes this amorphous blob by putting a scale on it, e.g. the metric scale. All bodies can be compared to the meter stick and measured to be some number of these units. Since lengths can be irrational multiples of the unit (e.g. the diagonal of the unit square has length $\sqrt{2}$, and the arclength of the unit circle is 2π), this sort of number is more like a real number. Negative real numbers arise when we think of length *directionally*, or *vectorially*. Negative numbers arise once we specify an *origin* on an infinite line.

   - In fact, $\mathbb{R}$ may be used to measure *any continuously varying quantity*, such as area, volume, speed, acceleration, pressure, temperature, luminosity, and many others. The real numbers are the generic tool for measurement.

Musical harmonics (3rds, 5ths, etc), too, were some of the earliest discoveries of the Pythagoreans, who saw in harmonies precise forms of an otherwise amorphous cacophany of pitches at other positions.

- When more complicated, higher-dimensional phenomena are measured, we may need several copies of $\mathbb{R}$: the **vector space** $\mathbb{R}^n = \mathbb{R} \times \cdots \times \mathbb{R}^n$ is used to house things like velocities, accelerations, forces, and rotations. These may be said to be the forms of linear motion in space.
- The **complex numbers** $\mathbb{C}$ consist of the vector space $\mathbb{R}^2$ endowed with a certain multiplication operation; this is the setting for complex analysis, complex vector spaces, unitary matrices, and Fourier analysis.
- When several quantities vary together, each being linear separately, we may use **tensors** and their associated tensor spaces, $\mathbb{R}^{\otimes n} = \mathbb{R} \otimes \cdots \otimes \mathbb{R}$. (This is a topic of (multilinear) algebra. See e.g. Knapp [12]).
- A **probability model** uses the real numbers to put a measure on the collection of outcomes of an experiment. It assigns nonnegative real numbers to the otherwise amorphous collection of possibilities. It gives shape to possibilities.
- In actually conducting any measurement there is always an **error**. One may average repeated measurements and their errors, and obtain a numerical confidence of the actual value of the measured phenomenon being within certain bounds. This is the subject of **statistics** which uses $\mathbb{R}$ to describe empirical observations. One might say that statistics, at least in this case, puts a measure or bound on the otherwise amorphous collection of measurements and their errors.

Yet more exotic concoctions exist, but you get the idea. Copies of $\mathbb{R}$ may be combined in creative ways to generate more "measurement"-type objects.

Examples could be produced ad infinitum, but the basic point is this: **The nature of number is to tame variation. Number is to variation as form is to matter.** The basic intuition is powerful and insightful. It interprets number as a type of bounding or shaping of natural variation. The theory takes as primitive and irreducible our ability to "see" the unit (the "one") with our mind's eye (the Platonists were never interested in the practical matter of measurement, which concerns our sensory access to numbers by means of comparison (with a unit stick, say)). It is easy to understand how the Pythagoreans could conclude that "everything is number." That they were overconfident was already noted by Plato and Aristotle, but we will see below that even "number" itself is not entirely clear, so that the statement "everything is number" fizzes rather than roars. Nevertheless, as a *metaphor* it is the guiding principle of mathematics and physics to this day.

The problem with the metaphysical grounding is that it suffers from some fatal weaknesses. Firstly, it is useless. If we are to use numbers to build machines and computers, and if these machines are in turn to help us do even more difficult computations, then we need a more machine-oriented account of numbers. But more fundamentally problematic is the unscientific nature of forms themselves. For forms are unobservable:

we can see them only with our "mind's eye," not with our sense organ. Phenomena are observable, but forms are *hypothesized* (literally "placed under" the phenomena, in Greek). The whole of metaphysics was rejected by the modern turn towards empirical science in the 17th century, on this ground. Science must be empirically verifiable in some sense, and concepts must be useful. Numbers are already fuzzy things, so grounding them in something unobservable compounds rather than solves the problem.

2.2.2 The Logical Grounding of $\mathbb{N}$ and $\mathbb{R}$ in Axioms and Formal Languages

Remark 1 Some good secondary resources for this section are Awodey and Reck [1], [2], Coffa [4], Gray [7], Ferreirós [5], Tiles [15]. ■

The metaphysical grounding for $\mathbb{N}$ and $\mathbb{R}$ proved suggestive but fruitless, so naturally other foundations were sought. The most promising was a *logical foundation*. Indeed, *logicism* was a late 19th and early 20th century movement to do just that.

> *"The idea that at least elementary number theory lay among the eternal verities offered two possibilities. One might hope to give geometry and even mechanics the certainty of arithmetic by founding them impeccably on arithmetic. Or one might hope to ground all of mathematics, numbers included, on some absolutely secure foundation. The one that commended itself was logic, and its attendant philosophy...became known as logicism..." (Gray [7][p. 27])*

The logicist agenda was overly ambitious, too, as it turned out, and its failure left only arithmetic to lean on (see the references mentioned above for the precise reasons; we explain briefly in the next paragraph). Nevertheless, the attempt to ground all of math in logic has had a deep effect on modern mathematics, and its work is visible today in all areas of math—not just in the field of mathematical logic itself, but in the various branches of math themselves (analysis, geometry, algebra) which underwent logicization but whose logically incomplete structures are all that remains standing today.

Real analysis is a perfect example. The possibility of grounding analysis in $\mathbb{R}$ and then somehow grounding $\mathbb{R}$ in $\mathbb{N}$ failed at the first step, for $\mathbb{N}$ itself proved impossible to ground completely in logic. Gödel's Incompleteness Theorems, which roughly say that any formal logical system from which the Peano axioms for $\mathbb{N}$ (see below) may be derived cannot decide whether a theorem in that system is provable or not. The reason is precisely the infinite size of $\mathbb{N}$. It seems that mathematics requires infinity not only for geometry and analysis, but even for arithmetic, and yet this infinity is precisely the thing which crashes logic. Infinity is "extralogical," and we have to add it in as an axiom (Zermelo's Infinity Axiom for set theory, see Section 3 below).

Nevertheless, *the initial hope of grounding all of analysis in $\mathbb{R}$ and hence in $\mathbb{N}$ was in fact realized, but the solid foundation thought to be $\mathbb{N}$ dissolved.* Thus, what we will study in this course is the logical development of real analysis, the conceptual theory underlying the calculus, but we should not expect perfect logical consistency, completeness, or anything else, nor will we explore these topics, as they are the subject of mathematical logic.

By the way, all of this is today the subject of a standard undergraduate courses in mathematical logic, see for example Hedman [8] or Johnstone [10].

We will take as our foundation the *axioms* of $\mathbb{R}$. Then we will study the nature of the extra axiom, the Axiom of Completeness, and map out its precise relations to the major theorems of real analysis: Nested Interval Property, Monotone Convergence Theorem, Bolzano-Weierstrass Theorem, Cauchy Criterion, and Intermediate Value Theorem. It turns out these are all *logically equivalent*, a theorem we will prove.

As a reward for our efforts, we will have the makings of a new concept, **topology**, to characterize our new axiom. The Axiom of Completeness gives $\mathbb{R}$ a topology, the *metric topology* whose open sets are the unions of intervals of the form (a, b). With this in our hands, we can prove such topological theorems as the Extreme Value Theorem and the Heine-Borel Theorem. Furthermore, we will have the wherewithal to start talking about **function spaces** such as $C[a, b]$, the continuous functions on $[a, b]$, and their relationship to known functions such as *polynomials*. Where do trigonometric functions like $\sin x$ and $\cos x$ fall into this scheme? Where do *trigonometric polynomials* like $\frac{a_0}{2} + \sum_{n=1}^{\infty} a_n \sin nx + b_n \cos nx$ fit into this? This is the subject of the higher parts of analysis, Taylor's Theorem, the Weierstrass Approximation Theorem, and Fourier theory, on which we will end the course.

2.2.3 Peano Axioms for $\mathbb{N}$

Let us now turn to a brief sketch of the Peano Axioms for $\mathbb{N}$.

Remark 2 Below, we will write $n \in \mathbb{N}$ as though $\mathbb{N}$ were a set, but we mean only "n is a natural number." Similarly, with "0," "1," and "successor of n," they just "are natural numbers." Also, we do not now worry overmuch about what '0' '1,' and 'successor of n' *are* in any Platonic sense—as we said, these are axioms, not models or realizations. ■

The basic idea of Peano's Axioms is that *the infinity expressed in the phrase "for all n, m and p" in the preamble of the arithmetic rules for $\mathbb{N}$ may be replaced by a* **successor function**, whose job is to add 1:

$$s : \mathbb{N} \to \mathbb{N}$$
$$s(n) \overset{\text{def}}{=} n + 1$$

and then to derive the arithmetical rules of $\mathbb{N}$ one-by-one, using the successor function.

Remark 3 Now, we must mention that we have to strip s of its function status, strictly speaking, unless we decide to work with sets from the get-go. But this would be to work in a model. So, by themselves, the natural numbers do not form a set, and s is not a function. We do not know what it is.

Why do this? Because by this ruse we kill two or three birds with one stone:

(a) We take infinity and replace it with the successor function, which will be infinite-valued instead.

(b) We get the Recursion Theorem, which says that recursively-defined sequences are in fact infinite sequences (and so may have limits), and this theorem underlies the all-important "for" loop in programming. Recursion is a topic in computer science.

(c) We get mathematical induction as a bonafide proof strategy. ■

Definition 1 (Peano Axioms for $\mathbb{N}$) The ***Peano axioms*** for the natural numbers $\mathbb{N}$ are:

(1) $0 \in \mathbb{N}$

(2) $n \in \mathbb{N} \implies s(n) \overset{\text{def}}{=} n + 1 \in \mathbb{N}$ (***successor of*** n)

(3) $0 \neq s(n)$ for any $n \in \mathbb{N}$

(4) $s(m) = s(n) \implies m = n$ for all $m, n \in \mathbb{N}$

(5) Let P be a property (hopefully of all $\mathbb{N}$). If 0 has P and whenever n has P so does $s(n)$, then all $n \in \mathbb{N}$ have P. (***Principle of Mathematical Induction***, non-set-theoretic) ■

Remark 4 Let us make some observations.

(1) First, in order to formalize the theory completely, we need a formal language $\mathcal{L}$, which consists of an alphabet $\mathcal{A}$ consisting of logical symbols (quantifiers $\forall$, $\exists$, connectives $\wedge$, $\vee$, $\rightarrow$, variables x, $y, \dots$ etc.) and non-logical symbols (binary relations like $+$ and $\cdot$, n-ary functions f^n, etc.), and formation rules (to construct well-formed-formulas, i.e. syntax). **First-order logic** quantifies only variables that range over individuals; **second-order logic**, in addition, also quantifies over sets.

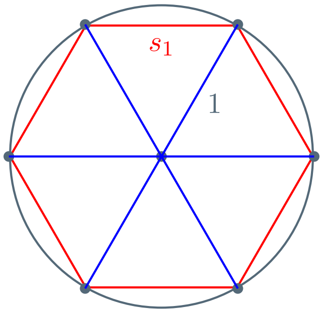
(2) If we look at Peano's Axioms, we see that, in a formal language, Axioms (1)-(4) would be considered *first-order* statements, while the crucial Axiom (5) is *second-order*, because the quantification is over sets. This makes $\mathbb{N}$ a second-order theory. On the plus side, all models of $\mathbb{N}$ are isomorphic (Theorem 11 below; see also Olmsted [14][p. 17])[1], meaning there is essentially only one mathematical structure $\mathbb{N}$ satisfying the Peano Axioms. On the minus side, second-order theories aren't sound, semantically complete, or effective. We could wake up tomorrow with problems in our theories. See Awodey and Reck [1]-[2] and Baez [3] for further details and references. ■

[1] Richard Dedekind proved this in his book *What are numbers and what should they be?* of 1888, a landmark in the arithmetization of analysis.

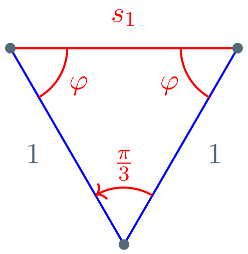
2.2.4 Recursion

Consider now the notion of **recursion**, a notion directly implied by the Peano Axioms. We illustrate it by constructing a recursive sequence converging to π. We will see later that this sequence consists of algebraic numbers, but that the limit, π, is irrational and in fact transcendental (not algebraic).

Example 5 (**Recursive Approximation of π by Inscribed Polygons**) Inscribe a regular hexagon in the unit circle,



and from elementary geometry you find that its sidelength s_1 is 1, as follows: zoom in on the top triangle, use the fact that it's isosceles with central angle $2\pi/6 = \pi/3$:



Since the angles in a triangle add up to π, we have

$$\frac{\pi}{3} + 2\varphi = \pi$$

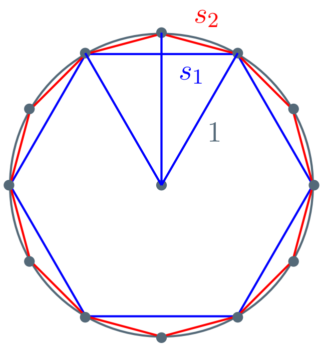
Solving for φ we have $\boxed{\varphi = \frac{\pi}{3}}$. This means the triangle is equilateral, so $\boxed{s_1 = 1}$.

A hexagon has six sides, therefore its perimeter is $\boxed{P_1 = 6}$. *This is our first approximation of 2π, the circumference of the circle, and it gives 3 as a first approximation of π.*

Let

$$a_1 \overset{\text{def}}{=} \frac{P_1}{2} = 3 \tag{2.1}$$

and **define the side-length sequence s_n recursively as follows**: Once we know s_1, we double the number of sides to inscribe a regular 12-gon,



The next exercise tells you how to carry out the calculation for s_2, and thence to a recursive definition of s_n:

Exercise 6 Using elementary geometry deduce that the new sidelength is

$$s_2 = \sqrt{2 - 2\sqrt{1 - \frac{s_1^2}{4}}}$$

In fact, once this trick is observed, it can be applied to get s_3 in terms of s_2, s_4 in terms of s_3, etc. In general, once we know s_n, we can get

$$\boxed{s_{n+1} = \sqrt{2 - 2\sqrt{1 - \frac{s_n^2}{4}}}} \tag{2.2}$$

Use mathematical induction to prove this claim. ■

Now, back to our approximating sequence a_n for π. Our regular polygons have, first, $6 = 3 \cdot 2$ sides ($n = 1$ here), then $12 = 3 \cdot 2^2$ sides ($n = 2$ here), etc. Half of this is our approximation to π,

$$\boxed{a_n = 3 \cdot 2^{n-1} \cdot s_n}$$ ■

The example above illustrates the technique. We started with

$$s_1 = 1$$

and defined

$$s_{n+1} = \sqrt{2 - 2\sqrt{1 - \frac{s_n^2}{4}}}$$

How should we interpret this? To connect it to the following Recursion Theorem, let us introduce some notation. If we define the functions

$$f : \mathbb{N} \to \mathbb{R}, \quad f(n) \overset{\text{def}}{=} s_n$$
$$g : \mathbb{R} \to \mathbb{R}, \quad g(x) = \sqrt{2 - 2\sqrt{1 - \frac{x^2}{4}}}$$

then the above two equations may be rephrased

$$f(1) \overset{\text{def}}{=} 1$$
$$f(s(n)) \overset{\text{def}}{=} g(f(n))$$

(Here, $s(n) = n+1$, the successor function.) ***We have thus defined f recursively***, using the ***recurrence relation*** g, and it is a sequence. We defined it for $n = 1$, and used $f(1)$ and g to get $f(2)$, then used $f(2)$ and g to get $f(3)$, etc. Since recursion is programmable/implementable, I used it to construct a MATLAB ‘for’ loop to run the computation ten steps for me:

```
s = 1;
P = 3*s;
fprintf(’s = %.10f,        P = %.10g \n’,s,P)

for i = 1:10
    s = sqrt(2-2*sqrt(1-s^2/4));
    P = 3*(2^i)*s;
    fprintf(’s = %.10f,        P = %.10g \n’,s,P)
end
```

Remark 7 Notice that $f : \mathbb{N} \to \mathbb{R}$ gives the values of a *sequence*, $f(n) = s_n$. This is a general fact. Any sequence $(a_n)_{n\in\mathbb{N}}$ can be thought of as a function $f : \mathbb{N} \to X$, where $f(n) = a_n \in X$. The set X may be a probability space, a manifold, a function space, or any other set. ■

We thus take the Recursion Theorem as a consequence of the Peano axioms, but as MacLane observes, this logical dependency could be reversed, since the recursion theorem is logically equivalent to the Peano axioms:

Theorem 8 (Recursion Theorem) *Let X be any set and let $a \in X$ be a fixed element. Given any function $g : X \to X$ we can* construct, *or more specifically* recursively define, *a function $f : \mathbb{N} \to X$ using a, g and the Peano axioms, by*

$$f(0) \overset{\text{def}}{=} a \tag{2.3}$$

$$f(s(n)) \overset{\text{def}}{=} g(f(n)) \tag{2.4}$$

Remark 9 In my example above, I started with $f(1) = 1$, instead of $f(0) = 1$, but this was only a cosmetic modification. I could just as easily have written $s_0 = 1$ instead of $s_1 = 1$, and made $f(0) = 1$. ■

Remark 10 As MacLane remarks (p. 45), 'A proof of this theorem uses axiom (v') and must depend upon the set-theoretic definition of "function."' Axiom (v') is an alternate version of our Peano axiom (5):

(5) If $S \subseteq \mathbb{N}$ is a set of natural numbers containing 0 and if every $n \in S$ has its successor $s(n) \in S$, then $\mathbb{N} \subseteq S$. (***Principle of Mathematical Induction***, set-theoretic)

Since $S \subseteq \mathbb{N}$ and $\mathbb{N} \subseteq S$, we conclude that $S = \mathbb{N}$. Thus, if we use *sets* S instead of properties P, we can get our proof, as in MacLane: ■

Proof: To use this axiom (5) we need our set S. Let

$$\mathbf{0} = \{0\},\ \mathbf{1} = \{0, 1\},\ \ldots\ , \mathbf{n} = \{0, 1, \ldots, n\}$$

and let P be the property of n

$$P = \text{'There is a unique function } f_n : \mathbf{n} \to X \text{ satisfying (2.3)-(2.4).'}$$

We observe that, for $n = 0$, the theorem's hypothesis gives us $f(0) = a$ in (2.3), so we call this function $f_0 : \mathbf{0} \to X$. For $n = 1$ we'll have, by (2.4), that we can *define* $f(1) = f(s(0)) = g(f_0(0))$, and we call this $f_1 : \mathbf{1} \to X$,

$$\begin{aligned} f_1(0) &= f_0(0) = a \\ f_1(1) &= g(f_0(0)) = g(a) \end{aligned}$$

Next, we define $f(2) = f(s(1)) = g(f(1)) = g(g(a))$ using (2.3)-(2.4) and our previous result. Call this $f_2 : \mathbf{2} \to X$,

$$\begin{aligned} f_2(0) &= f_1(0) = f_0(0) = a \\ f_2(1) &= f_1(1) = g(f_1(0)) = g(a) \\ f_2(2) &= g(f_1(1)) \end{aligned}$$

the last of which, incidentally, equals $g(g(a))$ or $g^2(a)$ for short. Continuing in this way, once we have $f_n : \mathbf{n} \to X$ defined, we let f_{n+1} take on the same values on

0, 1, …, n, and define $f_{n+1}(n+1) = g(f_n(n))$ using (2.4). The list of functions $f_0, \ldots, f_{n+1}$ fit together, in the sense that f_{n+1} uses the other f_i's previously defined and only adds the next value. Let

$$S = \bigcup_{n \in \mathbb{N}} \mathbf{n}$$

and note that S satisfies the desired properties if we define $f = \bigcup_{n \in \mathbb{N}} f_n$, that is if we define $f(n) = f_n(n) = g(f_{n-1}(n-1))$, and this equals $g^n(a)$, incidentally. ■

All of this formalism is designed to make you feel better about plugging $g^n(a)$ back into g to get $g^{n+1}(a)$, because this is how we're defining $f(n+1)$!

3 Set-Theoretic Construction of the Natural Numbers

To use sets as building blocks for a concrete realization of $\mathbb{N}$, that is to construct a set-theoretic model, requires a choice of set theory. The current convention is Zermelo-Fraenkel with Choice (ZFC), whose nuances I leave to another course in the foundations of math. For us, the important axiom in ZFC is Zermelo's Axiom of Infinity:

(Axiom of Infinity) (Zermelo, 1908) There exists an infinite set, specifically an inductive set containing $\varnothing$.

An inductive set is exactly the sort of set you need to suppose the successor function is defined on it. Nevermind about the set-theoretic details. The point is the following: we merely assume we have a set X on which a successor function can be defined.

Definition 2 (Set-Theoretic Construction of $\mathbb{N}$) We define $\mathbb{N}$ using only the Axiom of Infinity, the empty set $\varnothing$ and curly brackets $\{\cdot\}$. By the Axiom of Infinity we have an infinite set N and a successor function on it:

$$\boxed{s : N \to N, \qquad s(n) \overset{\text{def}}{=} n \cup \{n\}} \tag{3.1}$$

Here, n must be a set, of course, so it makes sense to union it with another set. The inspiration for this is Kuratowski's set-theoretic definition of an ordered pair (see Definition 3 below) as $(a, b) \overset{\text{def}}{=} \{a, \{b\}\}$. Next, define 0 to be the empty set $\varnothing$,

$$\boxed{0 \overset{\text{def}}{=} \varnothing} \tag{3.2}$$

and, keeping those Peano axioms in mind, require $\forall n \in N, 0 \neq s(n)$. This way, we require $s(n)$ to contain n for all $n \in N$, and this allows the **partial order relation** $<$ on N to be defined to be set membership, $\in$,

$$\boxed{n < m \quad \overset{\text{def}}{\iff} \quad n \in m, \quad \text{for all } n, m \in N} \tag{3.3}$$

We would like each natural number n to have n elements as a set, in such a way as to mesh with our definition of $<$. In particular, we demand that

$$n \in n + 1 \tag{3.4}$$

Then, too, whenever $m < n$, i.e. $m \in n$, we must have $m \in n + 1$, or $m < n + 1$ by the transitivity of $< \iff \in$. We must accordingly require

$$n \subseteq n + 1 \tag{3.5}$$

So since $n \in n + 1$ and $n \subseteq n + 1$ by (3.4) and (3.5), we see that we *must* define S and $n + 1$ simultaneously by

$$\boxed{s(n) \overset{\text{def}}{=} n \cup \{n\} \overset{\text{def}}{=} n + 1} \tag{3.6}$$

For example, since

$$0 \overset{\text{def}}{=} \varnothing$$

1 and 2 are defined by

$$\begin{aligned} 1 &\overset{\text{def}}{=} 0+1 \\ &= S(0) \\ &= S(\varnothing) \\ &= \varnothing \cup \{\varnothing\} \\ &= \{\varnothing\} \end{aligned} \qquad\qquad \begin{aligned} 2 &\overset{\text{def}}{=} 1+1 \\ &= S(1) \\ &= 1 \cup \{1\} \\ &= \{\varnothing\} \cup \{\{\varnothing\}\} \\ &= \{\varnothing, \{\varnothing\}\} \end{aligned}$$

and so on. Using the symbols for the sets, this reduces to

$$\begin{aligned} 0 &= \varnothing \\ 1 &= \{0\} \\ 2 &= \{0, 1\} \\ &\vdots \\ n &= \{0, 1, \ldots, n-1\} \end{aligned}$$

Theorem 11 (Uniqueness of $\mathbb{N}$) *There exists exactly one set $\mathbb{N}$ satisfying*

(1) $\varnothing \in \mathbb{N}$

(2) $n \in \mathbb{N} \implies S(n) \in \mathbb{N}$

(3) *If K is any set satisfying* (1) *and* (2), *then $\mathbb{N} \subseteq K$.*

Proof: By the axiom of infinity there exists at least one set X satisfying (1) and (2). Let

$$\mathcal{F} = \{Y \in \mathcal{P}(X) \mid \varnothing \in Y \text{ and } x \in Y \implies S(x) \in Y\}$$

and

$$\mathbb{N} = \bigcap \mathcal{F}$$

Then $\mathbb{N}$ satisfies (1) and (2) because $\varnothing \in Y$ for all $Y \in \mathcal{F}$, so that $\varnothing \in \mathbb{N}$, and $x \in \mathbb{N} \implies x \in Y$ for all $Y \in \mathcal{F} \implies S(x) \in Y$ for all $Y \in \mathcal{F} \implies S(x) \in \mathbb{N}$. Now, if K is any set satisfying (1) and (2), then $X \cap K \in \mathcal{F}$, so that $\mathbb{N} = \bigcap \mathcal{F} \subseteq X \cap K \subseteq K$. Consequently, $\mathbb{N}$ is unique, for if $\mathbb{N}'$ is any other set satisfying (1)-(3), then $\mathbb{N}' \subseteq \mathbb{N}$ and $\mathbb{N} \subseteq \mathbb{N}'$ by (3), so that $\mathbb{N} = \mathbb{N}'$. ■

Remark 12 Of course, if $K \subseteq \mathbb{N}$, then $K = \mathbb{N}$, which is the ***induction property*** of $\mathbb{N}$, and which demonstrates that $\mathbb{N}$ satisfies the 5th Peano Axiom. Of course, $\mathbb{N}$ satisfies axioms 1-3 by design, and it satisfies axiom 4 by the next theorem. ■

Theorem 13 *For all $m, n, p \in \mathbb{N}$, as defined above, we have the following relations:*

(1) $n \subseteq n+1$ *and* $n \in n+1$

(2) $m \in n \implies m \in \mathbb{N}$

(3) $m \in n \implies m+1 \subseteq n$

(4) $m \in n$ *and* $n \in p \implies m \in p$

(5) $n \notin n$

(6) $n+1 = m+1 \implies m = n$

(7) $m \subseteq n$ *iff* $m = n$ *or* $m \in n$

(8) $m \subseteq n$ *or* $n \subseteq m$

I'll run through this proof, to give you a feel for how tedious this is. The point is, it could be done, and, if you're curious, maybe it should be done.

Proof: (1) Since $n+1 = n \cup \{n\}$, we have both $n \subseteq n+1$ and $n \in n+1$.

(2) Let $K = \{n \in \mathbb{N} \mid m \in n \implies m \in \mathbb{N}\}$. Then $0 = \varnothing \in K$ trivially, since there is no $x \in 0$. Now, if $n \in K$, let $m \in n+1 = n \cup \{n\}$. Then, either $m \in n$ or $m = n$. In the first case we have by the definition of K that $m \in \mathbb{N}$, which means $n+1 \in K$ by the definition of K, since $m \in n+1$. In the second case we have that $m = n \in \mathbb{N}$, so again $n+1 \in K$. Either way, $n \in K \implies n+1 \in K$, and since $K \subseteq \mathbb{N}$, we have by the induction property of $\mathbb{N}$ that $K = \mathbb{N}$, which means for all $m \in n \implies m \in \mathbb{N}$ for all $n \in \mathbb{N}$.

(3) Let $K = \{n \in \mathbb{N} \mid m \in n \implies m+1 \subseteq n\}$. Obviously $0 = \varnothing \in K$ trivially, while if $n \in K$, consider $n+1$ and any $m \in n+1$. Either $m \in n$ or else $m = n$. In the latter case we have that $m+1 = n+1 \subseteq n+1$, while in the former we have that $m+1 \subseteq n \subseteq n+1$, so that $m+1 \subseteq n+1$. Thus, either way we have that $n+1 \in K$, so by the induction property of $\mathbb{N}$ we have that $K \subseteq \mathbb{N}$ and hence $K = \mathbb{N}$, or $m \in n \implies m+1 \subseteq n$ for all $m, n \in \mathbb{N}$.

(4) Suppose $m \in n$ and $n \in p$. Since $n \subseteq n+1$ we have that $m \in n+1$, and since by (3) we have that $n \in p$ implies that $n+1 \subseteq p$, we conclude that $m \in n+1 \subseteq p$, or $m \in p$.

(5) Let $K = \{n \in \mathbb{N}_0 \mid n \notin n\}$. Clearly $\varnothing \in K$, while if $n \in K$, then $n \notin n$. Suppose $n+1 \in n+1$. Then $n \cup \{n\} \in n \cup \{n\}$. Since $n \notin n$, we cannot have $n \cup \{n\} \in n$, so we must have $n \cup \{n\} \in \{n\}$. But then $n = n \cup \{n\}$, which is impossible since for that to be true we would need to have $\{n\} = \varnothing$. Hence $n+1 \notin n+1$, and so $K \subseteq \mathbb{N}_0$, whence $K = \mathbb{N}_0$, or $n \notin n$ for all $n \in \mathbb{N}$.

(6) If $n+1 = m+1$, then $n \cup \{n\} = m \cup \{m\}$, and suppose $n \neq m$. Then if by the axiom of extensionality, if $x \in n \cup \{n\}$, then $x \in m \cup \{m\}$. If $x = n$, then $n \in m \cup \{m\}$, and since by assumption $n \neq m$, we can't have $n \in \{m\}$, so we must have $n \in m$. But then we must also have $m \in n$ by the same reasoning, which is impossible because by (4) we'd have $m \in m$ and $n \in n$, which contradicts (5). Hence we must have $n = m$.

(7) If $m = n$ then $m \subseteq n$, while if $m \in n$ then by (1) and (3) we have $m \subseteq m+1 \subseteq n$, so $m \subseteq n$. Conversely, if $m \in \mathbb{N}_0$, let $K = \{n \in \mathbb{N}_0 \mid m \subseteq n \implies m \in n \text{ or } m = n\}$.

Clearly $0 = \varnothing \in K$ trivially, while if $n \in K$, then choose $m \subseteq n \cup \{n\} = n+1$. If $m \nsubseteq n$, then there is some $x \in m \cap (n \cup \{n\}) \backslash n = \{n\}$, so that $n \in m$. But then by (2) we have $n+1 \subseteq m$, which combined with $m \subseteq n+1$ implies that $m = n+1$, so that $n+1 \in K$. If $m \subseteq n$, then $n \in K$ we have $m \in n$ or $m = n$: if $m \in n \subseteq n+1$ so $m \in n+1$, which means $n+1 \in K$, while if $m = n$ then clearly $m = n \in \{n\} \subseteq n \cup \{n\} = n+1$, or $m \in n+1$, and $n+1 \in K$. Thus in all cases $n \in K \implies n+1 \in K$. Consequently $\mathbb{N}_0 \subseteq K \subseteq \mathbb{N}_0$, or $K = \mathbb{N}_0$.

(8) Define the set $\{n \in \mathbb{N}_0 \mid n \notin m \implies n \subseteq m\}$. Of course $0 = \varnothing \in K$ trivially since $\varnothing \subseteq m$ for all $m \in \mathbb{N}$. Now, if $n \in K$, then let $m \in \mathbb{N}_0$ and suppose that $m \notin n+1 = n \cup \{n\}$. Then $m \neq n$ and $m \notin n$, which means that since $n \in K$ we must have $n \subseteq m$. But since $m \neq n$ we must have by (7) that $n \in m$, and by (3) that $n+1 \subseteq m$. Consequently $n+1 \in K$, and by the induction principle we have $K = \mathbb{N}_0$. To finish the proof note that if $n, m \in \mathbb{N}$ and $n \subseteq m$ then we're done. So assume that $m \nsubseteq n$. By (7) we have $m \notin n$, and since $m \in \mathbb{N}_0 = K$ we conclude that $m \subseteq n$. ■

Theorem 14 (Basic Arithmetic Properties of $\mathbb{N}$) *If we define binary operations of addition + and multiplication · inductively on $\mathbb{N}$ by*

$$\begin{array}{lll} n+0=n & \textit{and} & n+(m+1)=(n+m)+1 \\ n0=0 & \textit{and} & n(m+1)=(nm)+n \\ & & (m+1)n=(mn)+n \\ n^0=1 & \textit{and} & n^{m+1}=n^m n \end{array}$$

for all $m, n \in \mathbb{N}$, then these operations satisfy the usual arithmetic properties: for all $m, n, p \in \mathbb{N}$, we have

(1) $m+(n+p)=(m+n)+p$ *(associativity of addition)*

(2) $m+n=n+m$ *(commutativity of addition)*

(3) $\exists 0 \in \mathbb{N}$ *such that* $n+0=n$ *(additive identity)*

(4) $m(np)=(mn)p$ *(associativity of multiplication)*

(5) $mn=nm$ *(commutativity of multiplication)*

(6) $\exists 1 \in \mathbb{N}$ *such that* $n1=n$ *(multiplicative identity)*

(7) $m(n+p)=mn+mp$ *and* $(n+p)m=nm+pm$ *(distributivity)*

(8) $n+m=n+p \implies m=p$ *(cancellation law for +)*

(9) $nm=np \implies m=p$ *if* $n \neq 0$ *(cancellation law for ·)*

(10) $n+m \leq n+p \iff m \leq p$ *(cancellation law for + and ≤)*

(11) $nm \leq np \iff m \leq p$ *if* $n \neq 0$ *(cancellation law for · and ≤)*

(12) $n^{m+k}=n^m n^k$ *(exponent law)*

Proof: Tedious application of the previous theorem. Exercise! ■

4 Equivalence Relations

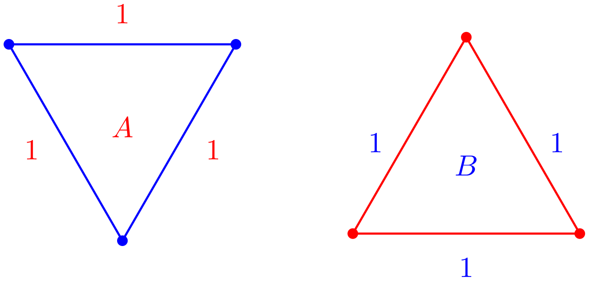
4.1 General Relations

We make a distinction between an **equality** and an **equivalence**. If two mathematical objects A and B are equal, $A = B$, then we consider them **the same object**. For example, $2+3=5$ says that the two objects, $2+3$ and 5 are in fact the same object. If A and B are *equivalent*, however, then they are **"the same but different"**. They are not the same object, but they are the **same type**.

Example 15 Before we lay down the definition, consider the following examples of "equivalent" objects which are not equal.

(1) The intervals $[0, 2\pi)$ and $[2\pi, 4\pi)$ are not the same intervals, but they are "equivalent," in the sense of *congruent* in Euclidean geometry, or *isomorphic* in the sense of metric spaces.

(2) The triangles ΔA and ΔB



are similarly "equivalent" in the sense of *congruent*, or *isomorphic*, but they are *not equal*.

(3) The hour hand on a clock repeats itself every 12 hours. We want to say that 3 o'clock is "equivalent" to 15 o'clock, and these are "equivalent" to 27 o'clock. To do this, partition $\mathbb{Z}$ into sets of size 12,

$$\mathbb{Z} = \bigcup_{n\in\mathbb{Z}} \{12n, 12n+1, \ldots 12n+11\}$$

When $n = 0$, the set is $\{0,\ 1, \ldots,\ 11\}$, when $n = 1$, the set is $\{12,\ 13, \ldots,\ 23\}$, and so on. Thus, $3 = 12 \cdot 0 + 3$ is in the first set and $15 = 12 \cdot 1 + 3$ is in the second set, but the reason they are equivalent is that remainder of 3 upon dividing by 12. We can use this to define an equivalence: say that two integers a and b are equivalent if their difference is divisible by 12:

$$a \sim b \quad \overset{\text{def}}{\Longleftrightarrow} \quad a - b = 12k, \quad \text{for some } k \in \mathbb{Z}$$

In this case we write $\boxed{a \equiv b \mod 12}$ and say "a is congruent to b modulo 12." For example $15 \equiv 3 \mod 12$, i.e. 15 is "the same but different" from 3.

(4) Suppose two functions f and g from $\mathbb{R}$ to $\mathbb{R}$ are equal except at a finite set of points $a_1, \ldots, a_n \in \mathbb{R}$. Then we can say they are "equivalent," but not exactly the same. ■

Definition 3 It is *not* necessary to have natural numbers defined ahead of the idea of **ordered pair** (a, b), since (a, b) could be defined in a purely set-theoretical way, as follows (definition due to Kuratowski):

$$(a, b) \overset{\text{def}}{=} \{\{a\},\ \{a, b\}\}$$

It should be clear that $(a, b) \neq (b, a)$, as sets. ■

Definition 4 Let X and Y be sets. Their **Cartesian product** $X \times Y$ consists of *ordered pairs* (x, y) where $x \in X$ and $y \in Y$,

$$X \times Y \overset{\text{def}}{=} \{(x, y) \mid x \in X,\ y \in Y\}$$

If $Y = X$, we usually write X^2 instead of $X \times X$. ■

Definition 5 If X and Y are any sets, then *any subset* R of their Cartesian product,

$$R \subseteq X \times Y$$

is called a **binary relation** on X and Y. If $X = Y$, we say R is a *relation on* X. Elements (a, b) in R are said to be *R-related*, and this is frequently denoted

$$aRb$$

instead of $(a, b) \in R$. Another common notation for relations is the tilde, $\sim$, but we will reserve this for a special type of relation, the equivalence relation.

Every relation R on X and Y has a **domain** and a **range**,

$$\mathcal{D}(R) \overset{\text{def}}{=} \{x \in X \mid \exists y \in Y,\ xRy\}$$
$$\mathcal{R}(R) \overset{\text{def}}{=} \{y \in Y \mid \exists x \in X,\ xRy\}$$

The set Y is called the **codomain** of R. Thus, $\mathcal{D}(R) \subseteq X$, and $\mathcal{R}(R) \subseteq Y$. ■

Remark 16 R is *not necessarily* of the form $\mathcal{D}(R) \times \mathcal{R}(R)$, and in fact

$$R \subseteq \mathcal{D}(R) \times \mathcal{R}(R) \subseteq X \times Y$$

We usually picture $\mathcal{D}(R) \times \mathcal{R}(R)$ as a type of 'rectangle.' ■

Here are some more examples of well-known relations:

Example 17 *Inequalities*, $\leq$ and $\geq$, are binary relations on $\mathbb{N}$, called **partial order** relations. Strict inequalities $<$ and $>$ are also relations, but observe that $n \leq n$ but $n \not< n$ for any $n \in \mathbb{N}$. ■

Example 18 **Equality**, $=$, is a binary relation on any set X. Sometimes (e.g. in topology and other applications) equality is denoted Δ, which stands for **diagonal**, for it can be 'pictured' as the 'diagonal line' $y = x$ as in the xy-plane which is here $X \times X$. ■

From this point of view, there are many relations:

Example 19 Let $R = \{(x, y) \mid x^2 + y^2 = 1\}$. This is the unit circle S^1, but as a set explicitly stating that x and y are R-related by the equation $x^2 + y^2 = 1$, derived from the Pythagorean theorem. ■

Definition 6 Let X and Y be sets and $A \subseteq X$, then a **function** from X to Y is a binary relation f on X and Y with **domain** $\mathcal{D}(f) = A$, denoted here specially by

$$f : A \to Y$$

instead of $R \subseteq X \times Y$, and

$$f(x) = y$$

instead of xRy (for $x \in A$ and f-related $y \in Y$), and all-importantly satisfying

$$f(x) = y \ \text{ and } \ f(x) = z \quad \Longrightarrow \quad y = z \tag{4.1}$$

for all $x \in X$ and $y, z \in Y$. That is, only one y-value to each x, colloquially known as the ***vertical line test***, which tests whether a random relation R is a function by passing a vertical line through R: it should intersect R in at most one point at a time. One more time, now: A is the domain, Y the codomain, but now let us also include the ***range***, or ***image***, of f

$$f(A) = \{y \in Y \mid \exists x \in A \text{ such that } y = f(x)\} \tag{4.2}$$

The ***graph*** of f

$$\begin{aligned} \text{graph}(f) &\overset{\text{def}}{=} \{(x, y) \mid x \in A,\ y \in f(A)\} \qquad (4.3) \\ &= \{(x, f(x)) \mid x \in A\} \qquad (4.4) \end{aligned}$$

is thus identical with the definition of f as a set, $f = \text{graph}(f)$. ■

Definition 7 Let us define some **special types of relations**. We need these to get to equivalence relations, which is the right tool for constructing $\mathbb{Z}$ and $\mathbb{Q}$. Here, $X = Y$ and $R \subseteq X^2$.

- R is **reflexive** if aRa for all $a \in A$
- R is **irreflexive** if $a\not{R}a$ for all $a \in A$
- R is **symmetric** if $aRb \implies bRa$ for all $a, b \in A$
- R is **asymmetric** if $aRb \implies b\not{R}a$ for all $a, b \in A$
- R is **antisymmetric** if aRb and $bRa \implies a = b$ for all $a, b \in A$
- R is **transitive** if aRb and $bRc \implies aRc$ for all $a, b, c \in A$ ■

For example, on $\mathbb{N}$ the partial order $\leq$ is reflexive, antisymmetric and transitive. By contrast, strict inequality $<$ is *ir*reflexie, asymmetric, and transitive, while equality $=$ is reflexive, symmetric, and transitive.

4.2 Equivalence Relations

Definition 8 An ***equivalence relation*** on a set X is a binary relation which is

(1) *reflexive*
(2) *symmetric*
(3) *transitive* ■

This definition reflects our desire to define *sameness of properties in different individuals*, and to be able to say two objects are "the same but different." We simply group those individual objects (now residing in a definite set X) exhibiting the 'same' property into a subset and call this fact an equivalence relation between them. This will be argued explicitly below.

Example 20 **Congruence**, $\cong$, and **similarity**, $\sim$, of triangles, or indeed of any 'figures,' in the Euclidean plane $\mathbb{R}^2$ are two properties that give rise to two equivalence relations: triangles having the same length sides are congruent but *not necessarily equal*, and likewise triangles that possess the same angles are similar but *not necessarily equal*.

(1) Clearly a single triangle is both congruent and similar to itself, so both $\cong$ and $\sim$ are relexive.

(2) If we use the linear algebraic group $\mathrm{E}(2)$ of **Euclidean transformations**, or **rigid motions** (consisting of rotations, reflections and translations) for $\cong$, then we can actually prove that two triangles A and B have $A \cong B \implies B \cong A$. It is a theorem that any Euclidean transformation $f \in \mathrm{E}(2)$ can be written in the form $f(\mathbf{x}) = A\mathbf{x} + \mathbf{b}$ for $A \in \mathrm{O}(2)$ and $\mathbf{b} \in \mathbb{R}^2$. If we use the linear algebraic group $\mathrm{S}(n)$ of **similarity** transformations, consisting of those f which can be written as $f(\mathbf{x}) = rA\mathbf{x} + \mathbf{b}$ for $A \in \mathrm{O}(2)$ and $\mathbf{b} \in \mathbb{R}^2$ and $r > 0$, then we can prove that $A \sim B \implies B \sim A$, so both $\cong$ and $\sim$ are symmetric. This is just the statement that $\mathrm{E}(2)$ and $\mathrm{S}(2)$ are groups, and so closed under inversion.

(3) Finally three triangles A, B and C have $A \cong B$ and $B \cong C \implies A \cong C$, and likewise with $\sim$, so both $\cong$ and $\sim$ are transitive, and this is just the statement that E(2) and S(2) are groups, and so closed under composition (which is the multiplication operation).

■

Definition 9 If $\sim$ is an equivalence relation on X and $a \in X$, then the ***equivalence class*** of a is the set of all $x \in X$ which satisfy $x \sim a$, denoted

$$[a] = \{x \in X \mid x \sim a\}$$

The *set of all equivalence classes on* X is denoted $X/\sim$, and is called the ***quotient set on X by $\sim$***. The function $\pi : X \to X/\sim$ given by $\pi(x) = [x]$ is called the ***canonical projection***, or the ***quotient map***, of $\sim$. ■

Definition 10 If X is a set, and $\mathscr{P}$ is a collection of subsets of X, that is $\mathscr{P} \subseteq \mathcal{P}(X)$, satisfying:

(1) $\varnothing \notin \mathscr{P}$.

(2) $\bigcup_{A \in \mathscr{P}} A = X$ where $\bigcup_{A \in \mathscr{P}} A \overset{\text{def}}{=} \{a \in A \mid A \in \mathscr{P}\}$ is the ***union*** of all the A in $\mathscr{P}$.

(3) All *distinct* $A, B \in \mathscr{P}$ are ***disjoint***, $A \cap B = \varnothing$.

then we call $\mathscr{P}$ a ***partition*** of X. In plain English, a partition is a collection of disjoint nonempty subsets of X whose union is X. Incidentally, we can combine 'union' and 'disjoint' into one entity, the ***disjoint union*** of the the $A \in \mathscr{P}$ by using a *square* cup:

$$\bigsqcup_{A \in \mathscr{P}} A = X$$

This combines (2) and (3) into one statement. Alternative notations for union $\bigcup_{A \in \mathscr{P}} A$ and disjoint union $\bigsqcup_{A \in \mathscr{P}} A$ are

$$\bigcup \mathscr{P} \equiv \bigcup_{A \in \mathscr{P}} A \qquad \text{and} \qquad \bigsqcup \mathscr{P} \equiv \bigsqcup_{A \in \mathscr{P}} A$$ ■

Lemma 21 *If X is a set and $\sim$ is an equivalence relation on X, then two equivalence classes $[a]$ and $[b]$ of X are either disjoint or equal. Consequently, $X/\sim$ is a partition of X*

Proof: Suppose $[a] \cap [b] \neq \varnothing$ and let $x \in [a] \cap [b]$. Then, $x \sim a$ and $x \sim b$. By symmetry, $a \sim x$, and by transitivity $a \sim x$ and $x \sim b \implies a \sim b$. Also, $\forall y \in [a]$, $y \sim a$, and by transitivity again $y \sim a$ and $a \sim b \implies y \sim b \implies y \in [b]$, or $[a] \subseteq [b]$. Similarly, $\forall z \in [b]$, $z \sim a \implies [b] \subseteq [a]$, and so $[a] = [b]$. But then the set of all equivalence classes determined by $\sim$, namely the quotient set $X/\sim$, is a partition of X, since all it's elements are pairwise disjoint and their union is X. ■

Theorem 22 *If X is a set and $\mathscr{P}$ is a partition of X, then there is exactly one equivalence relation on X from which it is derived.*

Proof: Define a binary relation $\sim$ on X by setting $x \sim y$ if $x, y \in A$ for some $A \in \mathscr{P}$. Now, $\sim$ is obviously symmetric, reflexive and transitive, and the relation applies to all elements of X, since $\bigsqcup \mathscr{P} = X$ and all elements of $\mathscr{P}$ are pairwise disjoint. Now, suppose there were two equivalence relations $\sim_1$ and $\sim_2$ on X with the above properties. Then, $\forall a \in X$ let $[a]$ and $[a']$ be the equivalence classes determined by a relative to $\sim_1$ and $\sim_2$, respectively. Consequently, $[a], [a'] \in \mathscr{P}$ must equal the unique element $A \in \mathscr{P}$ containing a (by the above paragraph), i.e. $\{x \in A \,|\, x \sim_1 a\} = [a] = A = [a'] = \{x \in A \,|\, x \sim_2 a\}$, which implies $\sim_1 = \sim_2$. Thus, $\sim$ is the unique equivalence relation from which $\mathscr{P}$ is derived. ■

5 The Integers $\mathbb{Z}$

If we try to define a **subtraction** operation "$-$" on $\mathbb{N}$, we notice that a given number k could be represented as the difference of two natural numbers m and n, such as $5 = 7 - 2$. But *this representation is not unique*, since $5 = 7 - 2 = 23 - 18 = \cdots$. However, notice that

$$7 - 2 = 23 - 18 \iff 7 + 18 = 23 + 2$$

where the latter expression makes no use of any "$-$" operation. This gives us a way to define negative numbers, too, namely:

Definition 11 Define a **relation** $\sim$ on $\mathbb{N}^2$, by

$$\boxed{(m,n) \sim (k,l) \overset{\text{def}}{\iff} m + l = k + n} \tag{5.1}$$

Proposition 23 *This is an equivalence relation.*

Proof: For all (m,n), (k,l), $(p,q) \in \mathbb{N}^2$ we have

(1) $m + n = m + n \implies (m,n) \sim (m,n)$ (reflexivity)

(2) $(m,n) \sim (k,l) \implies m + l = k + n \implies k + n = m + l \implies (k,l) \sim (m,n)$ (symmetry)

(3) $(m,n) \sim (k,l)$ and $(k,l) \sim (p,q) \implies m + l = k + n$ and $k + q = p + l \implies m + q + l = n + q + k = n + p + l \implies m + q = n + p \implies (m,n) \sim (p,q)$ (transitivity) ■

Definition 12 The **set of all integers** $\mathbb{Z}$ is then *defined as the set of all equivalence classes on* $\mathbb{N}^2$, *that is as the quotient set on* $\mathbb{N}^2$,

$$\boxed{\mathbb{Z} \overset{\text{def}}{=} \mathbb{N}^2 / \sim} \tag{5.2}$$

The arithmetic binary operations of **addition** $+$, **subtraction** $-$, and **multiplication** $\cdot$ on $\mathbb{Z}$ are defined as follows: for all $a = [(m,n)], b = [(k,l)] \in \mathbb{Z}$

$$\begin{aligned} a + b &= [(m,n)] + [(k,l)] = [(m+k, n+l)] \\ a - b &= [(m,n)] - [(k,l)] = [(m,n)] + [(l,k)] = [(m+l, n+k)] \\ ab &= [(m,n)][(k,l)] = [(mk+nl, ml+nk)] \end{aligned}$$

and a **partial order** $\leq$ given by

$$a = [(m,n)] \leq b = [(k,l)] \iff m + l \leq n + k$$

For example, we define -1 by $-1 \overset{\text{def}}{=} [(2,3)]$.

We will show below that these operations are well defined (i.e. do not depend on the choice of representatives of the equivalence classes in $\mathbb{N}^2/\sim$).

If we wish to have $\mathbb{N} \subseteq \mathbb{Z}$, then we will first need to embed the natural numbers as we have constructed them into $\mathbb{Z} = \mathbb{N}^2/\sim$ as we have constructed them. The canonical embedding $f : \mathbb{N} \hookrightarrow \mathbb{Z}$ is

$$f(n) = [(n,0)]$$

which is indeed an embedding: if $m, n \in \mathbb{N}$, then $f(m) = f(n)$ iff $[(m,0)] = [(n,0)]$ which implies $m = n$, since if $[(m,0)] = [(n,0)]$ then we clearly have $(n,0) \sim (m,0)$, or $m = m + 0 = n + 0 = n$. Moreover, f preserves the algebraic structure of $\mathbb{N}$:

$$f(m+n) = [(m+n,0)] = [(m,0)] + [(n,0)] = f(m) + f(n)$$

so that indeed $\mathbb{N} \overset{f}{\hookrightarrow} \mathbb{Z}$. When considering the subset $f(\mathbb{N})$ of $\mathbb{Z}$ we ususally write $\mathbb{N} \subseteq \mathbb{Z}$, strictly incorrectly of course, but in keeping with the intuitive notion of the natural numbers being a subset of the integers.

Proposition 24 *The binary operations of addition $+$, subtraction $-$, and multiplication $\cdot$ on $\mathbb{Z}$ are* **well defined**. *That is, if $[(m,n)] = [(m',n')]$ and $[(k,l)] = [(k',l')]$, then*

(1) $[(m+k, n+l)] = [(m'+k', n'+l')]$

(2) $[(m+l, n+k)] = [(m'+l', n'+k')]$

(3) $[(m,n)(k,l)] = [(m',n')(k',l')]$

(4) $[(m,n)] \le [(k,l)] \iff [(m',n')] \le [(k',l')]$

Proof: Tedious. Exercise! ∎

Lemma 25 *If we define the binary operations $+$ and $\cdot$ on $\mathbb{N}^2$ by*

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

for all $(a,b), (c,d), (e,f) \in \mathbb{N}^2$, then these operations satisfy

1. $(a,b) + (c,d) = (c,d) + (a,b)$ } *(commutativity)*
2. $(a,b)(c,d) = (c,d)(a,b)$
3. $((a,b) + (c,d)) + (e,f) = (a,b) + ((c,d) + (e,f))$ } *(associativity)*
4. $((a,b)(c,d))(e,f) = (a,b)((c,d)(e,f))$
5. $\exists (0,0) \in \mathbb{N}^2$ *s.t.* $(a,b) + (0,0) = (0,0) + (a,b) = (a,b)$ *(additive identity)*
6. $\exists (1,0) \in \mathbb{N}^2$ *s.t.* $(a,b)(1,0) = (1,0)(a,b) = (a,b)$ *(multiplicative identity)*
7. $((a,b) + (c,d))(e,f) = (a,b)(e,f) + (c,d)(e,f)$ *and* $(a,b)((c,d) + (e,f)) = (a,b)(c,d) + (a,b)(e,f)$ } *(distributivity)*

Proof: Tedious. Exercise! ∎

Theorem 26 (Arithmetic Properties of $\mathbb{Z}$) *For all $a, b, c \in \mathbb{Z}$ we have*

$$\left.\begin{array}{ll}1. & a+b\in\mathbb{Z}\\ 2. & a-b\in\mathbb{Z}\\ 3. & ab\in\mathbb{Z}\end{array}\right\}\ (\mathbb{Z}\textit{ is closed under }+,\,-\textit{ and }\cdot)$$

$$\left.\begin{array}{l}
\left.\begin{array}{ll}4. & a+b=b+a\\ 5. & ab=ba\end{array}\right\}\ (\textit{commutativity})\\
\left.\begin{array}{ll}6. & (a+b)+c=a+(b+c)\\ 7. & (ab)c=a(bc)\end{array}\right\}\ (\textit{associativity})\\
\begin{array}{lll}8. & \exists 0\in\mathbb{Z}\textit{ s.t. } a+0=0+a=a & (\textit{additive identity})\\ 9. & \exists 1\in\mathbb{Z}\textit{ s.t. } a1=1a=a & (\textit{multiplicative identity})\\ 10. & \forall a\in\mathbb{Z},\ \exists! b\in\mathbb{Z}\textit{ s.t. } a+b=0 & (\textit{additive inverse})\end{array}\\
\left.\begin{array}{ll}11. & (a+b)c=ac+bc\textit{ and}\\ & a(b+c)=ab+ac\end{array}\right\}\ (\textit{distributivity})
\end{array}\right\}\ (\mathbb{Z}\textit{ is a commutative ring})$$

$$\begin{array}{ll}12. & (-1)a=-a\end{array}$$

Proof: Tedious. Exercise! ■

Definition 13 If we take properties (1)-(3) as *definitions* of the binary operations of addition and multiplication,

$$\begin{array}{lll}+ : \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}, & (a,b)\mapsto a+b & (\textbf{addition})\\ \cdot : \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}, & (a,b)\mapsto ab & (\textbf{multiplication})\end{array}$$

along with the unary operation of negation

$$\begin{array}{lll}- : \mathbb{Z}\to\mathbb{Z}, & a\mapsto -a & (\textbf{negation})\end{array}$$

then the other properties, (4)-(12), become the **axioms of an abstract ring**: if we remove the *particular construction* of $\mathbb{Z}$ out of equivalence classes of $\mathbb{N}^2$ given above and ask only for a set R to be equipped with $+$, $\cdot$, and $-$, and to satisfy the axioms, then we have the definition of an algebraic ring. Actually, to be perfectly correct, properties (4)-(12) define a **commutative ring**, and a **ring** by itself only if we remove axiom (5). This allows, for example, square matrices to be considered a *noncommutative* ring.

The next idea then is to situate $\mathbb{Z}$ within the class of all rings. MacLane himself co-invented the way to do this: make rings into a category, and then see how $\mathbb{Z}$ fits in that category. The answer is: $\mathbb{Z}$ is an 'initial element' in the category of rings, because of a certain 'universal property' it satisfies. We have thus arrived at the culmination of Aristotle's original idea of conceptualizing Plato's form of 'integer number,' namely as the ring of integers, an initial element in its category. ■

6 The Rational Numbers $\mathbb{Q}$

Since we have, for example, $\frac{4}{6} = \frac{-8}{-12} = \cdots = \frac{2}{3}$, we may *define* division by means of multiplication: $(4,6) \sim (-8,-12) \overset{\text{def}}{\iff} 4 \cdot (-12) = 6 \cdot (-8) \iff \frac{2}{3} \overset{\text{def}}{=} [(4,6)]$.

Definition 14 Formally, define the relation $\sim$ on $\mathbb{Z}^2$ by

$$\boxed{(a,b) \sim (c,d) \quad \overset{\text{def}}{\iff} \quad (ad = bc \text{ and } b \neq 0,\ d \neq 0) \text{ or } (b = d = 0)} \tag{6.1}$$

Proposition 27 *$\sim$ is an equivalence relation on $\mathbb{Z}^2$.* ■

Definition 15 Now, we can define the **rational numbers** $\mathbb{Q}$ as the quotient set of $\mathbb{Z}^2$ by $\sim$,

$$\boxed{\mathbb{Q} \overset{\text{def}}{=} \mathbb{Z}^2/\sim \overset{\text{def}}{=} \{[(a,b)] \mid a, b \in \mathbb{Z} \text{ and } b \neq 0\}} \tag{6.2}$$

Moreover, $\mathbb{Q}$ is endowed with the arithmetic operations of **addition** $+$ and **multiplication** $\cdot$ given by

$$[(a,b)] + [(c,d)] = [(ad + bc, bd)] \tag{6.3}$$

$$[(a,b)][(c,d)] = [(ac, bd)] \tag{6.4}$$

and a **partial order** $\leq$ given by

$$[(a,b)] \leq [(c,d)] \quad \overset{\text{def}}{\iff} \quad b, d \geq 0 \text{ and } ad \leq bc \tag{6.5}$$

which are also well-defined, as will be shown below. Moreover, $\mathbb{Q}$ contains an **additive identity**

$$0 = [(0, 1')] \tag{6.6}$$

where $1'$ is the multiplicative identity of $\mathbb{Z}$. Also, $\mathbb{Q}$ contains a **multiplicative identity**,

$$1 \overset{\text{def}}{=} [(1', 1')] \tag{6.7}$$

where $1'$ is the multiplicative identity of $\mathbb{Z}$. Finally, we endow $\mathbb{Q}$ with the unary **negative** function $-$ and the unary **multiplicative inverse** function $^{-1}$, which send each $[(a,b)] \in \mathbb{Q}$ into

$$-[(a,b)] \overset{\text{def}}{=} [(-a, b)] \tag{6.8}$$

and

$$[(a,b)]^{-1} \overset{\text{def}}{=} [(b, a)] \tag{6.9}$$

(the last only if $[(a,b)] \neq 0$). ■

Thus, $\mathbb{Q}$ *is an albegraic structure*, $(\mathbb{Q}, \leq, -, ^{-1}, +, \cdot, 0, 1)$. It remains to show that is is a *field* (every *nonzero* rational number has a multiplicative inverse), and an *ordered set* $(\mathbb{Q}, \leq)$. To show this, however, we first need to show that our addition and multiplication, as well as our order relation, are all well defined.

Remark 28 We may **embed the integers into the rationals** in a way similar to the embedding of the naturals into the integers. The function $f : \mathbb{Z} \to \mathbb{Q}$, i.e. $f : \mathbb{Z} \to \mathbb{Z}^2/\sim$, given by $f(a) = [(a, 1)]$, is injective, since $f(a) = f(b)$ implies $[(a, 1)] = [(b, 1)]$, so $(a, 1) \sim (b, 1)$, or $a = a1 = b1 = b$. Thus, $\mathbb{Z} \overset{f}{\hookrightarrow} \mathbb{Q}$, though we usually write $\mathbb{Z} \subseteq \mathbb{Q}$. ■

Proposition 29 *The unary negative $-$ and multiplicative inverse $^{-1}$ functions, the binary addition $+$ and multiplication $\cdot$ functions, and the partial order relation $\leq$ on $\mathbb{Z}^2/\sim$ are all well defined. That is, if $[(a, b)] = [(a', b')]$ and $[(c, d)] = [(c', d')]$ in $\mathbb{Z}^2/\sim$, then*

1. $-[(a, b)] = -[(a', b')]$
2. $[(a, b)]^{-1} = [(a', b')]^{-1}$
3. $[(ad + bc, bd)] = [(a'd' + b'c', b'd')]$
4. $[(ac, bd)] = [(a'c', b'd')]$
5. $[(a, b)] \leq [(c, d)] \iff [(a', b')] \leq [(c', d')]$

Proof: Tedious. Exercise! ■

Theorem 30 (Arithmetic Properties of $\mathbb{Q}$) *For all $a, b, c \in \mathbb{Q}$ we have*

1. $a + b \in \mathbb{Q}$
2. $a - b \in \mathbb{Q}$
3. $ab \in \mathbb{Q}$

} *($\mathbb{Q}$ is closed under $+$, $-$ and $\cdot$)*

4. $a + b = b + a$
5. $ab = ba$

} *(commutativity)*

6. $(a + b) + c = a + (b + c)$
7. $(ab)c = a(bc)$

} *(associativity)*

8. $\exists 0 \in \mathbb{Q}$ *s.t.* $a + 0 = 0 + a = a$ *(additive identity)*
9. $\exists 1 \in \mathbb{Q}$ *s.t.* $a1 = 1a = a$ *(multiplicative identity)*
10. $\forall a \in \mathbb{Q}$, $\exists! b \in \mathbb{Q}$ *s.t.* $a + b = 0$ *(additive inverse)*
11. $\forall a \in \mathbb{Q}\backslash\{0\}$, $\exists! b \in \mathbb{Q}$ *s.t.* $ab = 1$ *(multiplicative inverse)*
12. $(a + b)c = ac + bc$ *and* $a(b + c) = ab + ac$ } *(distributivity)*

} (items 4–12) *($\mathbb{Q}$ is a field)*

13. $(-1)a = a(-1) = -a$
14. $\forall a, b, \in \mathbb{Q}$, $a \leq b$ *or* $b \leq a$ *($\leq$ is total order)*

Thus, $\mathbb{Q}$ is a structure $(\mathbb{Q}, \leq, -, ^{-1}, +, \cdot, 0, 1)$ which is a totally ordered field.

Proof: Tedious. Exercise! ■

Definition 16 If we take properties (1)-(3) as *definitions* of the binary operations of addition and multiplication,

$$\begin{array}{rlll} + & : \mathbb{Q}\times\mathbb{Q}\to\mathbb{Q}, & (a,b)\mapsto a+b & (\textbf{addition}) \\ \cdot & : \mathbb{Q}\times\mathbb{Q}\to\mathbb{Q}, & (a,b)\mapsto ab & (\textbf{multiplication}) \end{array}$$

along with the unary operation of negation

$$\begin{array}{rlll} - & : \mathbb{Q}\to\mathbb{Q}, & a\mapsto -a & (\textbf{negation}) \end{array}$$

then the other properties, (4)-(13), become the **axioms of an abstract field**: if we remove the *particular construction* of $\mathbb{Q}$ out of equivalence classes of $\mathbb{Z}^2$ given above and ask only for a set F to be equipped with $+$, $\cdot$, and $-$, and to satisfy the axioms, then we have the definition of an algebraic field.

The next question concerning fields is not categorical, as with the integers. The next question concerns ideas from field theory itself, namely various extensions of the field $\mathbb{Q}$, which is typically studied in the second semester of an abstract algebra course. The most important extension of $\mathbb{Q}$ for us is $\mathbb{R}$, the real number field. ■

References

[1] Awodey, S., Reck, E. H., Completeness and Categoricity. Part I: Nineteenth-century Axiomatics to Twentieth-century Metalogic, *History and Philosophy of Logic*, **23**, 1-30 (2002)

[2] Awodey, S., Reck, E. H., Completeness and Categoricity. Part II: 20th Century Metalogic to 21st Century Semantics, *History and Philosophy of Logic*, **23**, 77-92 (2002)

[3] Baez, J., The Logic of Real and Complex Numbers, 2014, https://johncarlosbaez.wordpress.com/2014/09/08/the-logic-of-real-and-complex-numbers/

[4] Coffa, J. A., *The Semantic Tradition from Kant to Carnap: To the Vienna Station*, Cambridge, 1991

[5] Ferreirós, J., *Labyrinth of Thought: A History of Set Theory and Its Role in Modern Mathematics*, 2nd Ed., Birkhäuser, 2007

[6] Fine, B., Rosenberger, G., *The Fundamental Theorem of Algebra*, Springer, 1997

[7] Gray, Jeremy, *Plato's Ghost: The Modernist Transformation of Mathematics*, Princeton, 2008

[8] Hedman, S., *A First Course in Logic: An Introduction to Model Theory, Proof Theory, Computability, and Complexity*, Oxford, 2006

[9] Hintikka, J., *Lingua Universalis vs. Calculus Ratiocinator: An Ultimate Presupposition of Twentieth-Century Philosophy*, Springer, 1997

[10] Johnstone, P. T., *Notes on Logic and Set Theory*, Cambridge, 1987

[11] Klein, J., *Greek Mathematical Thought and the Origin of Algebra*, Dover, 1992

[12] Knapp, A. W., *Basic Algebra*, digital second edition published by the author, http://www.math.stonybrook.edu/~aknapp

[13] MacLane, S., *Mathematics: Form and Function*, Springer, 1986

[14] Olmsted, J. M. H., *The Real Number System*, Meredith Publishing Co., 1962 (reissued by Dover, 2018)

[15] Tiles, M., *The Philosophy of Set Theory: An Historical Introduction to Cantor's Paradise*, Basil Blackwell, 1989 (reissued by Dover, 2004)