NON-STANDARD ANALYSIS

DAVID PIERCE

These are notes for a course to be given August 10–16, 2009, at the Nesin Mathematics Village (*Nesin Matematik Köyü*) in Şirince, Selçuk, İzmir, Turkey. The source files are available at

`http://arf.math.metu.edu.tr/~dpierce/courses/Sirince/`

which is where I shall put corrections or other changes, if I should type up any. These notes are only a rough draft.

Contents

Date: August 7, 2009.

Introduction

Mathematical analysis is the theoretical side of calculus. Calculus consists of methods of solving certain sorts of problems; analysis studies those methods. The **standard** way of doing this is founded on the 'epsilon-delta' definition of *limit.* The **non-standard** approach uses *infinitesimals,* with rigorous logical justification. Abraham Robinson first gave this justification; it can be found in his book, *Non-standard Analysis* [13].

An **infinitesimal** is a number whose absolute value is less than than every positive rational number. If two numbers a and b differ by an infinitesimal, we write

$$a \simeq b.$$

Zero is an infinitesimal, but there are no other infinitesimals among the so-called *real numbers.*

In standard analysis, a function f is said to be **continuous** at an element a of its domain if

$$\lim_{x \to a} f(x) = f(a);$$

this means that, for all positive numbers ε, there is a positive number δ such that, for all x in the domain of f, if $|x - a| < \delta$, then $|f(x) - f(a)| < \varepsilon$.

In non-standard analysis, there is an alternative formulation of continuity: f is continuous at a just in case, for all x in the domain of f, if $x \simeq a$, then $f(x) \simeq f(a)$.

The alternative formulation of continuity and many other things will be worked out in the last section, § 6, of these notes. The other sections are meant to provide logical justication and motivation for this work. Section 1 looks at Archimedes's solution of a calculus problem, and also mentions the *Archimedean axiom,* which will come up later in various contexts. Today we think of calculus as involving the *complete ordered field* $\mathbb{R}$ of real numbers; this field is constructed in §§ 2 and 3. Non-standard analysis requires a certain larger ordered field, ${}^*\mathbb{R}$, which is an example of a *non-Archimedean* ordered field. Non-Archimedean ordered fields in general, and simple examples of these and related fields, are discussed in § 4. The field ${}^*\mathbb{R}$ can be obtained as an *ultrapower* of $\mathbb{R}$; this construction is treated in § 5. One can jump ahead to § 6 at any time, provided one understands the meaning of Theorem 41 in § 5.2.

1. Archimedes's quadrature of the parabola

In the last chapter of *Non-standard Analysis* [13], Robinson treats the history of calculus in the light of non-standard analysis. Robinson begins with Leibniz; but I think it worthwhile to go back much further—about two thousand years further. In the work of Archimedes, both standard and non-standard approaches to calculus (in our terms) can be discerned. For example, Archimedes takes up the following

Problem 1. *Find a square equal to a given segment of a parabola.*

Parabolas will be defined below; meanwhile, a segment of a parabola can be seen in Figure 1, with an inscribed triangle. A solution to Problem 1 is called a **quadrature** of

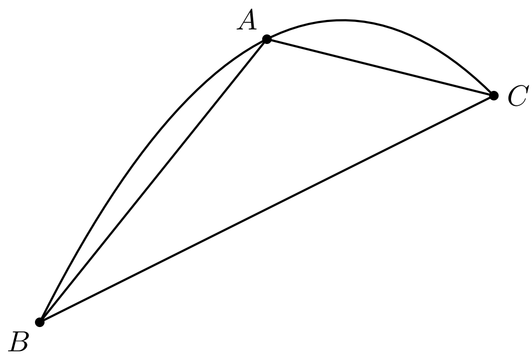


Figure 1

the parabola. Archimedes's solution is given by the following

Theorem 2 (Archimedes)**.** *A parabolic segment is a third again as large*[1] *as the inscribed triangle with the same altitude.*

In Figure 1, triangle ABC has the same altitude as the parabolic segment, because the tangent to the parabola at A is parallel to the chord BC. Archimedes proves Theorem 2 in two ways in his *Quadrature of the parabola:* in Proposition 17 (and the propositions leading up to it), and in Proposition 24. Heath [2] provides an English version of this work, though rather than translating, he rewrites Archimedes in a way intended to be more comprehensible to his readers. Selections from the Greek text of Archimedes, with more literal English translations, are provided by Thomas [15]. The first volume of a faithful translation of all of Archimedes's works by Netz [3] has appeared; but this does not contain the works that we are particularly interested in here.

Insight into the *discovery* of Theorem 2 is given in Archimedes's *Method.* This work was lost until 1906. Then, in İstanbul, the Danish scholar J.L. Heiberg discovered the *Archimedes Palimpsest:* a parchment codex of the works of Archimedes that had been washed and reused for writing Christian prayers.

Archimedes does not use the word *parabola* [2, p. clxvii], but refers to a *section of an orthogonal cone.*[2] Let me review what this means, sometimes following also the account of Apollonius [1]. A cone is determined by a circle, called its **base,** and a point, called the

[1]*ἐπίτριτος*, one and a third times as much. See Appendix A for the Greek letters.

[2]*ὀρθογωνίου κώνου τομή*.

apex of the cone, that is not in the plane of the base. The cone is traced out by a straight line, one endpoint of which is at the apex, the other being moved about the circumference of the base. The straight line drawn from the apex to the center of the base is the **axis** of the cone. A plane containing the axis intersects the cone in an **axial triangle.** If the axis is perpendicular to the base, then the cone is **right.** If an axial triangle of a right cone has a right angle at the apex, then the cone is an **orthogonal**[3] cone. In such a cone, if a plane is perpendicular to one of the sides of the axial triangle that are about the apex, then the plane cuts the cone in a curve that—following Apollonius—we call a **parabola.** The intersection of the cutting plane and the axial triangle is the **axis** of the parabola (which is different from the axis of the cone itself); the intersection of the axis of the parabola and the parabola itself is the **vertex** of the parabola.

A straight line dropped from the parabola perpendicularly to the axis may be called an **ordinate;** the part of the axis between the foot of the ordinate and the vertex is the corresponding **abscissa.** The word *abscissa* means *cut off* in Latin, while the word *ordinate* is related to *order,* which is used for, among other things, any of the several classical styles of architecture. These orders feature columns standing parallel, like ordinates of a parabola. Consider for example the columns of the Ionic order erected at Priene, Söke, Aydın (which is accessible on a day trip from Şirince): see Figure 2.

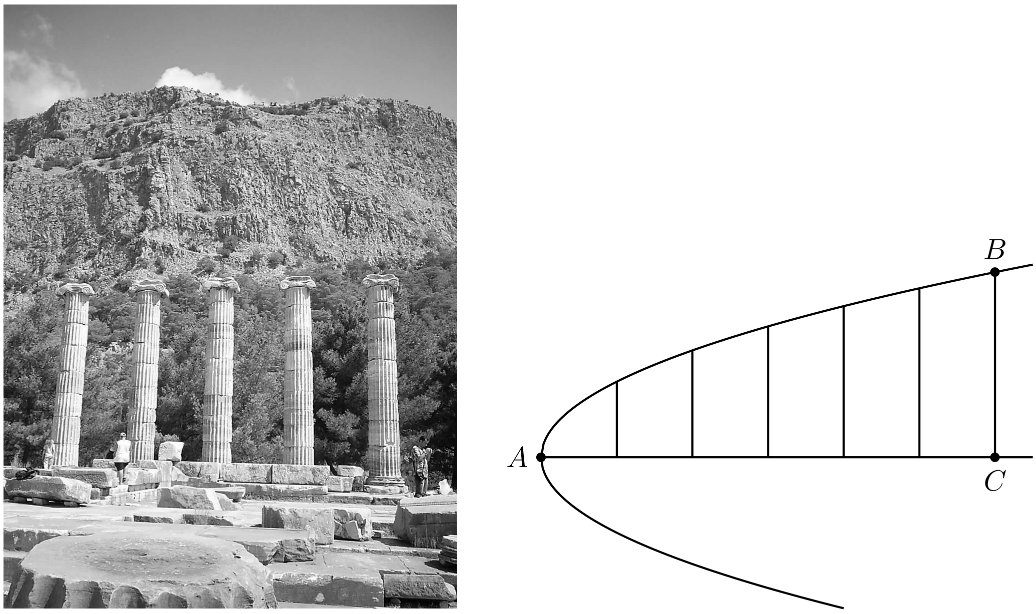


Figure 2. The ordinate BC cuts off from the axis the abscissa AC. On the left, Priene

Apollonius's reason for using the term *parabola* is shown in Proposition 11 of his *Conics* [1, 15]. Apollonius also shows that parabolas can be obtained from *all* cones, not necessarily orthogonal, not necessarily right. What is important for us are the following properties of a parabola, whose proofs can be found in Apollonius.

[3]Or 'right-angled'; but I want to avoid confusion with *right* cones in general.

1. The squares on two ordinates are in the ratio of the corresponding abscissas [1, I.11]. (Below we shall talk more about what this means.)

2. Suppose a parabola has the vertex A, and another point B is chosen on the parabola, and the ordinate BC is drawn. Extend the axis CA beyond A to a point D. The straight line BD is tangent to the parabola at B if and only if $AD = CA$ [1, I.33, 35] (see Figure 3).

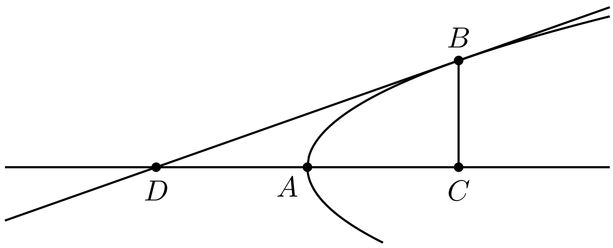


FIGURE 3. DB is tangent at B if and only if $CA = AD$

3. Every straight line parallel to the axis is a **diameter** in the following sense. Where this diameter meets the parabola, a tangent can be drawn. If a chord of the parabola is drawn parallel to this tangent, then the diameter bisects the chord [1, I.46]. Half of such a chord is an ordinate with respect to the corresponding diameter, and the squares on two such ordinates are in the ratio of the corresponding abscissas, as in 1 [1, I.49] (see Figure 4).

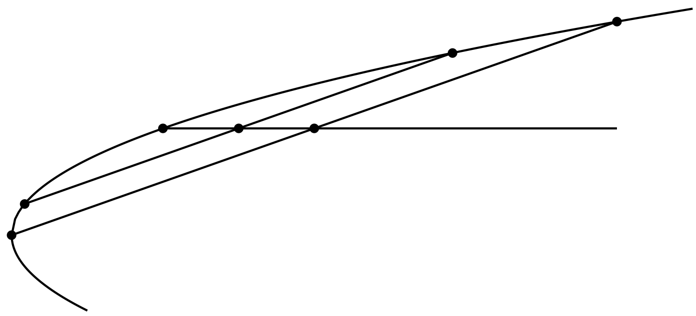


FIGURE 4. A new diameter

In the *Method,* Archimedes solves Problem 1 as follows. We add some straight lines to Figure 1, getting Figure 5. Here D is the midpoint of BC, so that (since BC is parallel to the tangent at A) the straight line AD must be a diameter of the parabola. The tangent to the parabola at C meets DA extended at E. Then A is the midpoint of DE, by 2 above. A straight line from B parallel to DA meets CE extended at F. Extend CA to meet BF at G, then extend further to H so that $GH = CG$. The idea now is to consider CH as a *lever* with *fulcrum* at G. If we conceive of our figures as having weights proportional to their sizes, then we shall show that, if we place the weight of the parabolic segment ABC at H, then it will just balance triangle BCF where it is.

Since A is the midpoint of DE, also G is the midpoint of BF. Let DF be drawn, intersecting CG at K. Since D is the midpoint of BC, we can conclude that K is the

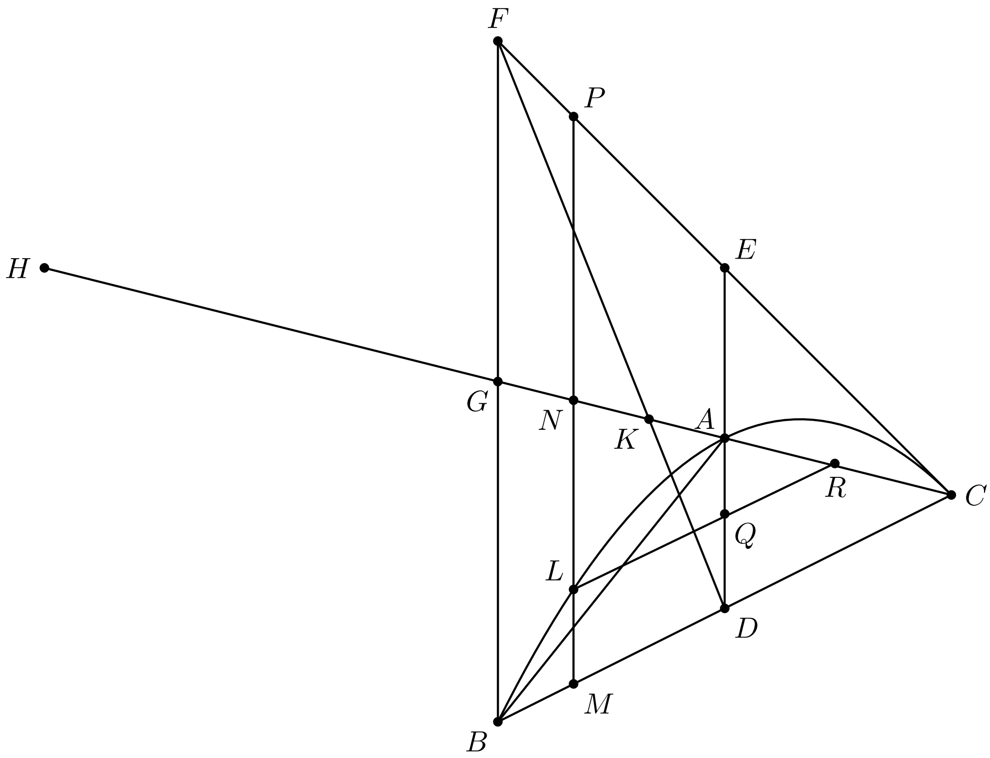


FIGURE 5

center of gravity (or centroid) of triangle BCF. Then GK is a third of CG, hence a third of GH. Therefore triangle BCF is balanced by a third of its weight at H. If we can show that the parabolic segment balances the triangle, then the segment must be a third of the triangle. But triangle BCF is four times triangle ABC (why?). Then Theorem 2 will follow.

Now, pick a point L at random on the parabola between B and C. Let the straight line drawn through L parallel to BF meet BC at M and CG at N and CF at P. It remains to show that

$$LM : MP :: GN : GH. \tag{1}$$

This is the key point. If (1) holds, then LM, if its midpoint is placed at H, will just balance MP. Since L was chosen arbitrarily, we conclude that, if all of the parabolic segment were placed at H, then it would balance BCF. Now, Archimedes does not find this sort of argument to be sufficiently rigorous. Indeed, in the preface to the *Method,* he writes

> For some things first became clear to me by mechanics, though they had later to be proved geometrically owing to the fact that investigation by this method does not amount to actual proof; but it is, of course, easier to provide the proof when some knowledge of the things sought has been acquired by this method rather than to seek it with no prior knowledge. [15, p.223]

I want to look at the 'actual proof' of Archimedes presently. Meanwhile, let us establish (1). You probably think of it as an equation of fractions: $LM/MP = GN/GH$. That is fine; but (1) simply expresses a relation of *proportionality* among four *magnitudes.* Here are Definitions 3–6 from Book V of Euclid's *Elements* [5, 6].

> 3. A **ratio** is a sort of relation in respect of size between two magnitudes of the same kind.
> 4. Magnitudes are said to **have a ratio** to one another which are capable, when multiplied, of exceeding one another.
> 5. Magnitudes are said to **be in the same ratio,** the first to the second and the third to the fourth, when, if any equimultiples whatever be taken of the first and third, and any equimultiples whatever of the second and fourth, the former equimultiples alike exceed, are alike equal to, or alike fall short of, the latter equimultiples respectively taken in corresponding order.
> 6. Let magnitudes which have the same ratio be called **proportional.**

Briefly, 4 means you can't have a ratio between a line and a square: this may be one source of the concern expressed by Archimedes in the quote above. If a and b *are* magnitudes with a ratio, and so are c and d, then by 5, we may say variously

(1) a is to b in the same ratio that c is to d,
(2) a is to b as c is to d,
(3) $a : b :: c : d$,

provided that, whenever we take a multiple na of a, and the same multiple nc of c, and a multiple mb of b, and the same multiple md of d, then

$$\begin{aligned} na > mb &\text{ if and only if } nc > nd, \\ na = mb &\text{ if and only if } nc = nd, \\ na < mb &\text{ if and only if } nc < nd. \end{aligned}$$

In Books V and VI of the *Elements,* Euclid goes on to prove the properties of proportionality that we shall need.

To return to our problem. From L draw a straight line parallel to BC, meeting AD at Q and AC at R. Then by property 1 of the parabola given above,

$$LQ^2 : CD^2 :: AQ : AD.$$

Since $LQ = MD$, and triangle ACD is similar to NCM, while ARQ is similar to ACD, we can rewrite the proportion as

$$NA^2 : AC^2 :: AR : AC.$$

Therefore NA is a mean proportional of AC and AR (see Euclid's VI.13, 20, and 23), so

$$\begin{aligned} NA : AC &:: AR : NA \\ &:: NA + AR : NA + AC \\ &:: NR : NC \\ &:: NL : NM. \end{aligned}$$

Since $AC = AG$, and $MN = NP$, we obtain

$$\begin{gathered} NA : AG :: NL : NM, \\ AG - NA : AG :: NM - NL : NM, \\ NG : AG :: LM : NM, \\ NG : 2AG :: LM : 2NM, \\ NG : GC :: LM : MP, \\ NG : GH :: LM : MP, \end{gathered}$$

which is (1), as desired.

Archimedes works out a rigorous formulation of this argument in the *Quadrature of the parabola,* but I prefer now to look at the alternative proof, given for Proposition 24 of that work.

Start over from Figure 1, getting Figure 6. Here D is the midpoint of BC as before,

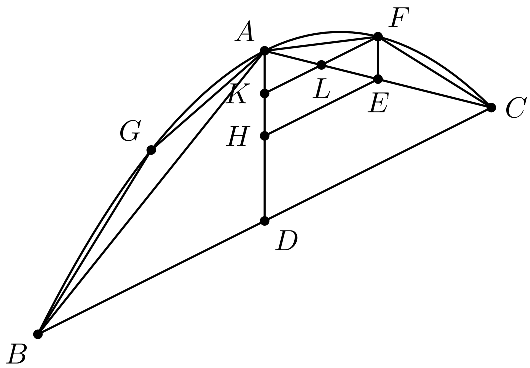


Figure 6

and E is the midpoint of AB. From E a straight line is drawn parallel to DA, meeting the parabola at F. Draw straight lines AF and FC. Then triangle ACF has the same altitude as the parabolic segment in which it is inscribed. Similarly we can find G on the parabola between A and B so that the inscribed triangle ABG has the same height as its parabolic segment. We show that triangles ACF and ABG are together one fourth of triangle ABC.

To this end, from E and F we draw parallels to BC, meeting AD at H and K respectively. Then

$$FK^2 : CD^2 :: AK : AD.$$

But $FK = EH$, and

$$EH : CD :: EA : CA :: 1 : 2.$$

Therefore AK is one fourth of AD. Consequently K is the midpoint of AH, and so L is the midpoint of AE. Hence triangle AKL is equal to triangle EFL. But EFL is one fourth of ACF, and AKL is one thirty-second of ABC. Therefore ACF is one eighth of ABC. Similarly, ABG is one eighth of ABC; so ABG and ACF together are one fourth of ABC.

We have started with the parabolic segment cut off by the chord BC, and we have removed from it the triangle ABC. Then we have removed triangles equal to a fourth of ABC. We can continue, removing triangles equal to a sixteenth of ABC, and so on. Moreover, at each step, we remove more than one half the remainder of the original parabolic segment (why?).

Therefore, if we continue long enough, we can make the remainder of the parabolic segment less than any pre-assigned area M. This is the conclusion of Euclid's Proposition X.1; let us note the proof. The pre-assigned area M is assumed to *have a ratio* with the parabolic segment, so that, by Definition V.4 above, some multiple nM of M exceeds the segment. Indeed, Archimedes himself makes the assumption explicit in the preface to the *Quadrature of the parabola;* it is what we may refer to as the **Archimedean axiom:**

> given [two] unequal areas, the exess by which the greater exceeds the less
> can, by being added to itself, be made to exceed any given finite area.
> [15, p.231]

If we take away at least half of the parabolic segment, and take M from nM, then in the latter case we are taking not more than half; so the former remainder is still less than the latter remainder. If we repeat this process $n-1$ times, then the remainder of the parabolic segment will be less than M.

Suppose we have an area that is a third again as large as triangle ABC. If we remove triangle ABC, what is left is one third. If we then remove one fourth of triangle ABC, then what is left is one twelfth of that triangle, which is one fourth of the previous remainder. Continuing, if we remove one fourth of what we last removed, then what remains is one fourth of the previous remainder. Therefore, continuing as far as necessary, we can make the remainder as small as we like. But this is the same process as we described in the original parabolic segment.

Suppose the original parabolic segment is *not* a third again as large as ABC, but is greater. Let the difference be M. We can inscribe in the parabolic segment a rectilinear figure which differs from the segment by less than M; so it is more than a third greater than ABC, which is absurd. There is a similar contradiction if the parabolic segment is less than a third again as large as ABC. Theorem 2 now follows.

2. Construction of the rational numbers

You know something about the chain

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \tag{2}$$

of number systems. Here $\mathbb{N}$ is the set $\{0, 1, 2, \dots\}$ of **natural numbers;** $\mathbb{Z}$ comprises the **integers;** $\mathbb{Q}$, the **rationals;** $\mathbb{R}$, the **real numbers.** What comes after $\mathbb{R}$ in (2)? It depends on how we think of $\mathbb{R}$. If we think of it as a *field,* then we might think of $\mathbb{R}$ as included in $\mathbb{C}$, the field of **complex numbers.** But what if we think of $\mathbb{R}$ as an *ordered field?* I postpone an answer until Section 4. Meanwhile I want to look at how we obtain (2) in the first place.

2.1. **The natural numbers.** We can understand $\mathbb{N}$ axiomatically. First of all,

(1) it has a distinguished **initial element** called 0 (**zero**);
(2) it has a distinguished singulary operation of **succession,** denoted by $n \mapsto n+1$: here $n+1$ is the **successor** of n.

I propose to refer to the ordered triple $(\mathbb{N}, 0, n \mapsto n+1)$ as an *iterative structure.* In general, by an **iterative structure,** I mean any set that has a distinuished element and a distinguished *singulary operation* (that is, a function from the set to itself). For example, modular arithmetic involves the iterative structures[4] $(\mathbb{Z}/n, 0, k \mapsto k+1)$. The iterative structure $(\mathbb{N}, 0, n \mapsto n+1)$ is distinguished among iterative structures for satisfying the following axioms.

(1) 0 is not a successor: $0 \neq n+1$.
(2) Succession is injective: if $m+1 = n+1$, then $m = n$.
(3) the structure admits **proof by induction,** in the sense that the only subset A with the following two closure properties is the whole set:
    (a) $0 \in A$;
    (b) for all n, if $n \in A$, then $n+1 \in A$.

These axioms seem to have been discovered originally by Dedekind [4, II, VI (71), p. 67], although they were also written down by Peano [12] and are often known as the **Peano axioms.** From these axioms, Landau develops the rational, real, and complex numbers rigorously, over the course of a book [10]. I want to do the same here, though more quickly and in a different style. Landau's natural numbers start with 1, not 0. Also, Landau does not use the following theorem. The proof is difficult, but the result is very useful.

Theorem 3 (Recursion)**.** *For every iterative structure (A, b, f), there is a unique* ***homomorphism*** *to this structure from $(\mathbb{N}, 0, n \mapsto n+1)$: that is, there is a unique function h from $\mathbb{N}$ to A such that*

(1) $h(0) = b$,
(2) $h(n+1) = f(h(n))$ for all n in $\mathbb{N}$.

Proof. I use the set-theoretic conception whereby a function g is just the set of ordered pairs (x, y) such that $g(x) = y$; so if (x, y) and (x, z) belong to g, then $y = z$. We now seek h as a particular subset of $\mathbb{N} \times A$.

[4]Some people might write these structures as $(\mathbb{Z}/n, \bar{0}, \bar{k} \mapsto \overline{k+1})$, to make sure that the reader distinguishes a natural number k from its congruence class *modulo n*.

Let B be the set whose elements are the subsets C of $\mathbb{N} \times A$ such that, if $(x, y) \in C$, then either

(1) $(x, y) = (0, b)$ or else
(2) C has an element (u, v) such that $(x, y) = (u + 1, f(v))$.

Let $R = \bigcup B$; so R is a subset of $\mathbb{N} \times A$. We may say R is a *relation* from $\mathbb{N}$ to A. If $(x, y) \in R$, we may write also

$$x \mathrel{R} y.$$

Since $(0, b) \in B$, we have $0 \mathrel{R} b$. If $n \mathrel{R} y$, then $(n, y) \in C$ for some C in B, but then $C \cup \{(n + 1, f(y))\} \in B$ by definition of B, so $(n + 1) \mathrel{R} f(y)$. Therefore R is the desired function h, provided it is a *function* from $\mathbb{N}$ to A. Proving this has two stages.

1. For all n in $\mathbb{N}$, there is y in A such that $n \mathrel{R} y$. Indeed, let D be the set of such n. Then we have just seen that $0 \in D$, and if $n \in D$, then $n + 1 \in D$. By induction, $D = \mathbb{N}$.

2. For all n in $\mathbb{N}$, if $n \mathrel{R} y$ and $n \mathrel{R} z$, then $y = z$. Indeed, let E be the set of such n. Suppose $0 \mathrel{R} y$. Then $(0, y) \in C$ for some C in B. Since 0 is not a successor, we must have $y = b$, by definition of B. Therefore $0 \in E$. Suppose $n \in E$, and $(n + 1) \mathrel{R} y$. Then $(n + 1, y) \in C$ for some C in B. Again since 0 is not a successor, we must have $(n+1, y) = (m+1, f(v))$ for some (m, v) in C. Since succession is injective, we must have $m = n$. Since $n \in E$, we know v is *unique* such that $n \mathrel{R} v$. Since $y = f(v)$, therefore y is unique such that $(n + 1) \mathrel{R} y$. Thus $n + 1 \in E$. By induction, $E = \mathbb{N}$.

So R is the desired function h. Finally, h is unique by induction. □

Corollary. *For every set A with a distinguished element b, and for every function F from $\mathbb{N} \times B$ to B, there is a unique function H from $\mathbb{N}$ to A such that*

(1) $H(0) = b$,
(2) $H(n + 1) = F(n, H(n))$ for all n in $\mathbb{N}$.

Proof. Let h be the unique homomorphism from $(\mathbb{N}, 0, n \mapsto n + 1)$ to $(\mathbb{N} \times A, (0, b), f)$, where f is the operation $(n, x) \mapsto (n + 1, F(n, x)))$. In particular, $h(n)$ is always an ordered pair. By induction, the first entry of $h(n)$ is always n; so there is a function H from $\mathbb{N}$ to A such that $h(n) = (n, H(n))$. Then H is as desired. By induction, H is unique. □

The proof of the Recursion Theorem used each of the three Peano axioms; induction alone would not enough. Indeed, if some iterative structure $\mathfrak{A}$ has the property that is guaranteed to $(\mathbb{N}, 0, n \mapsto n + 1)$ by the Recursion Theorem, then $\mathfrak{A}$ is **isomorphic** to $\mathbb{N}$ (why?), and consequently $\mathfrak{A}$ satisfies the Peano axioms.[5] But these axioms are independent. For example, $(\mathbb{Z}/n, 0, k \mapsto k + 1)$ satisfies axioms 2 and 3, but not 1; and there are examples satisfying 1 and 3, but not 2; and satisfying 1 and 2, but not 3 (can you find them?).

Moreover, it is possible to assume the Recursion Theorem and *prove* the Peano axioms from it.

[5]Here $\mathfrak{A}$ is the Fraktur version of A. The idea is that A is just a set, but $\mathfrak{A}$ is that set together with some other things—here a distinguished element and singulary operation. Then A is the **universe** of $\mathfrak{A}$. I shall not later distinguish notationally between structures and their universes. If I did want to make a distinction, I would use the letters depicted in Appendix B.

We can now use recursion to *define* the binary operation $(x, y) \mapsto x + y$ of **addition,** along with the binary operation $(x, y) \mapsto x \cdot y$ or $(x, y) \mapsto xy$ of **multiplication,** on $\mathbb{N}$. The definitions are:

$$n + 0 = n, \qquad n + (m + 1) = (n + m) + 1, \qquad n \cdot 0 = 0, \qquad n \cdot (m + 1) = n \cdot m + n.$$

Lemma. *For all n and m in $\mathbb{N}$,*

$$0 + n = n, \qquad (m + 1) + n = (m + n) + 1.$$

Proof. Induction. □

Theorem 4. *Addition on $\mathbb{N}$ is*
(1) ***commutative:*** *$n + m = m + n$; and*
(2) ***associative:*** *$n + (m + k) = (n + m) + k$.*

Proof. Induction and the lemma. □

Theorem 5. *Addition on $\mathbb{N}$ allows* ***cancellation:*** *if $n + x = n + y$, then $x = y$.*

Proof. Induction, and injectivity of succession. □

Lemma. *For all n and m in $\mathbb{N}$,*

$$0 \cdot n = 0, \qquad (m + 1) \cdot n = m \cdot n + n.$$

Proof. Induction. □

Theorem 6. *Multiplication on $\mathbb{N}$ is*
(1) *commutative: $nm = mn$;*
(2) ***distributive*** *over addition: $n(m + k) = nm + nk$; and*
(3) *associative: $n(mk) = (nm)k$.*

Proof. Induction and the lemma. □

Landau proves *using induction alone* that $+$ and $\cdot$ exist as given by the recursive definitions above. Note however that Theorem 5 needs more than induction (why?). Also, the existence of **exponentiation,** as an operation $(x, y) \mapsto x^y$ such that

$$n^0 = 1, \qquad n^{m+1} = n^m \cdot n,$$

requires more than induction.

The usual ordering $<$ of $\mathbb{N}$ is defined recursively as follows. First note that $m \leqslant n$ means simply $m < n$ or $m = n$. Then the definition of $<$ is:
(1) $m \not< 0$;
(2) $m < n + 1$ if and only if $m \leqslant n$.

In particular, $n < n + 1$. Really, it is the sets $\{x \in \mathbb{N} \colon x < n\}$ that are defined by recursion:
(1) $\{x \in \mathbb{N} \colon x < 0\} = \varnothing$;
(2) $\{x \in \mathbb{N} \colon x < n + 1\} = \{x \in \mathbb{N} \colon x < n\} \cup \{n\}$.

We now have $<$ as a binary relation on $\mathbb{N}$; we must *prove* that it is an ordering.

Theorem 7. *The relation $<$ is* ***transitive*** *on $\mathbb{N}$, that is, if $k < m$ and $m < n$, then $k < n$.*

Proof. Induction on n. □

Lemma. $m \neq m+1$.

Proof. The claim is true when $m = 0$, since 0 is not a successor. Suppose the claim is true when $m = k$, that is, $k \neq k+1$. Then $k+1 \neq (k+1)+1$, by injectivity of succession, so the claim is true when $m = k+1$. By induction, the claim is true for all m. □

Theorem 8. *The relation $<$ is **irreflexive** on $\mathbb{N}$: $m \nless m$.*

Proof. The claim is true when $m = 0$, since $m \nless 0$ by definition. Suppose the claim *fails* when $m = k+1$. This means $k+1 < k+1$. Therefore $k+1 \leqslant k$ by definition. By the previous lemma, $k+1 < k$. But $k \leqslant k$, so $k < k+1$ by definition. So $k < k+1$ and $k+1 < k$; hence $k < k$ by Theorem 7, that is, the claim fails when $m = k$. By induction, the claim holds for all m. □

Lemma. *(1) $0 \leqslant m$.*
(2) If $k < m$, then $k+1 \leqslant m$.

Proof. (1) Induction.
(2) The claim is vacuously true when $m = 0$. Suppose it is true when $m = n$. Say $k < n+1$. Then $k \leqslant n$. If $k = n$, then $k+1 = n+1 < (n+1)+1$. If $k < n$, then $k+1 < n+1$ by inductive hypothesis, so $k+1 < (n+1)+1$ by transitivity. Thus the claim holds when $m = n+1$. By induction, the claim holds for all m. □

Theorem 9. *The relation $\leqslant$ is **total** on $\mathbb{N}$: either $k \leqslant m$ or $m \leqslant k$.*

Proof. Induction and the lemma. □

Because of Theorems 7, 8, and 9, the set $\mathbb{N}$ is **(strictly) ordered** by $<$.

Theorem 10. *For all m and n in $\mathbb{N}$, we have $m \leqslant n$ if and only if the equation*

$$m + x = n \tag{3}$$

is soluble in $\mathbb{N}$.

Proof. By induction on k, if $m + k = n$, then $m \leqslant n$.
Conversely, if $m \leqslant 0$, then $m = 0$ (why?), so $m+0 = 0$. Suppose the equation $m+x = r$ is soluble whenever $m \leqslant r$, but now $m \leqslant r+1$. If $m = r+1$, then $m+0 = r+1$. If $m < r+1$, then $m \leqslant r$, so the equation $m+x = r$ has a solution k, and therefore $m + (k+1) = r+1$. Thus the equation $m+x = r+1$ is soluble whenever $m \leqslant r+1$. By induction, for all n in $\mathbb{N}$, if $m \leqslant n$, then (3) is soluble in $\mathbb{N}$. □

Theorem 11. *(1) If $k < \ell$, then $k+m < \ell+m$.*
(2) If $k < \ell$ and $m \neq 0$, then $km < \ell m$.

Here part 1 is a refinement of Theorem 5, and part 2 yields the following analogue of Theorem 5 for multiplication.

Corollary. *If $km = \ell m$ and $m \neq 0$, then $k = \ell$.*

Theorem 12. *$\mathbb{N}$ is **well ordered** by $<$: every nonempty set of natural numbers has a least element.*

Proof. Suppose A is a set of natural numbers with no least element. Let B be the set of natural numbers n such that, if $m \leqslant n$, then $m \notin A$. Then $0 \in B$, by the last lemma, since otherwise 0 would be the least element of A. Suppose $m \in B$. Then $m+1 \in B$, since otherwise $m+1$ would be the least element of A. By induction, $B = \mathbb{N}$, so $A = \varnothing$. □

2.2. **The positive rationals.** The integers can be constructed from the natural numbers; and the rationals, from the integers. Since the latter construction is probably more familiar than the former, I begin with it; rather, I construct the *positive* rational numbers from the **positive integers,** which we already have: the are just the non-zero natural numbers.

Let us denote the set of positive integers by $\mathbb{N}^+$, so

$$\mathbb{N}^+ = \mathbb{N} \smallsetminus \{0\}.$$

We want to define a set

$$\mathbb{Q}^+$$

of **positive rationals.** These are certain **fractions,** namely numbers of the form

$$\frac{a}{b}$$

or a/b. In particular, $a/b \in \mathbb{Q}^+$ if and only if a and b are in $\mathbb{N}^+$. But what does this *mean?*

One is taught in school that arithmetic of fractions obeys the following rules:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}. \tag{4}$$

However, in $\mathbb{Q}^+$, one must *prove* that these rules are valid, because the positive rational number a/b does not uniquely determine the ordered pair (a, b) of positive integers. For example, $1/2 = 2/4$, although $(1, 2) \neq (2, 4)$.

One might try defining a new operation $\oplus$ on $\mathbb{Q}^+$ by writing down a formula like[6]

$$\frac{a}{b} \oplus \frac{c}{d} = \frac{a+c}{b+d}. \tag{5}$$

But this implies $1/2 \oplus 1/3 = 2/5$, while $2/4 \oplus 1/3 = 3/7$. Since $1/2 = 2/4$, while $2/5 \neq 3/7$, we conclude that $\oplus$ is not *well defined.* This is a common loose way of speaking. The point is that there is no operation $\oplus$ on $\mathbb{Q}^+$ with the property required by (5).

On the set $\mathbb{N}^+ \times \mathbb{N}^+$ or $(\mathbb{N}^+)^2$, let $\sim$ be the relation given by

$$(a, b) \sim (c, d) \iff ad = bc. \tag{6}$$

One checks easily that $\sim$ is **reflexive** ($x \sim x$), **symmetric** ($x \sim y$ if and only if $y \sim x$) and **transitive** (if $x \sim y$ and $y \sim z$, then $x \sim z$). By definition therefore, $\sim$ is an **equivalence relation.** If a and b are in $\mathbb{N}^+$, we can now define a/b precisely: it is the set of elements of $(\mathbb{N}^+)^2$ that are equivalent to (a, b) with respect to $\sim$. Thus

$$\frac{a}{b} = \{(x, y) \in (\mathbb{N}^+)^2 \colon ay = bx\}.$$

[6] This example, and the difficulty it illustrates, are discussed on [Timothy] Gowers's Weblog at `http://gowers.wordpress.com/2009/06/08/why-arent-all-functions-well-defined/`.

Traditionally, a/b is therefore called the **equivalence class** of (a,b) with respect to $\sim$. Then $\mathbb{Q}^+$ is the set of such equivalence classes; we might write

$$\mathbb{Q}^+ = (\mathbb{N}^+)^2/{\sim}.$$

Now we can check that the rules in (4) are valid. Supposing $a/b = a'/b'$ and $c/d = c'/d'$, we have $ab' = ba'$ and $cd' = dc'$, so for example

$$acb'd' = ab'cd' = ba'dc' = bda'c',$$

and therefore $ac/bd = a'c'/b'd'$.

Considering (5) again, note that there is indeed a function f from $(\mathbb{N}^+)^2 \times (\mathbb{N}^+)^2$ to $\mathbb{Q}^+$ given by

$$f\big((x,y),(z,w)\big) = \frac{x+z}{y+w}.$$

There are just no functions g from $(\mathbb{N}^+)^2 \times (\mathbb{N}^+)^2$ to $\mathbb{Q}^+ \times \mathbb{Q}^+$ and h from $\mathbb{Q}^+ \times \mathbb{Q}^+$ to $\mathbb{Q}^+$ such that $f = h \circ g$.

By our construction, a positive integer is not literally a positive rational, because a positive rational is a class of pairs of positive integers. However, the positive integers embed in the positive rationals under the map

$$x \mapsto \frac{x}{1}.$$

This embedding respects arithmetic: $a/1 + b/1 = (a+b)/1$ and $(a/1)(b/1) = (ab)/1$. It also respects the ordering, where we define

$$\frac{a}{b} < \frac{c}{d} \iff ad < bc.$$

On $\mathbb{Q}^+$ there is a binary operation $(x,y) \mapsto x \div y$ of **division,** given by

$$\frac{a}{b} \div \frac{c}{d} = \frac{ad}{bc};$$

one checks that division is indeed well defined. In particular, we have

$$\frac{a}{1} \div \frac{b}{1} = \frac{a}{b}.$$

We usually confuse a positive integer a with the positive rational $a/1$, and for $x \div y$ we write x/y. For $1/a$, we write a^{-1}.

2.3. **The integers.** If a and b are in $\mathbb{N}^+$, then the equation

$$a = bx \tag{7}$$

may or may not have a solution in $\mathbb{N}^+$. Suppose it does have a solution; this solution is unique by the corollary to Theorem 11. If c and d are also in $\mathbb{N}^+$, and the equation

$$c = dx \tag{8}$$

has a solution in $\mathbb{N}^+$, then it is the *same* solution that (7) has if and only if

$$ad = bc \tag{9}$$

(why?). Then $\mathbb{Q}^+$ is defined to ensure two things:

(1) the equation (7) always has a solution in $\mathbb{Q}^+$;
(2) equations (7) and (8) have the same solution in $\mathbb{Q}^+$ if and only if (9) holds.

The integers can be understood to arise from the natural numbers in the same way, with addition taking the place of multiplication. If m and n are in $\mathbb{N}$ and $m \leqslant n$, then (3) has a solution by Theorem 10; moreover, this solution is *unique* (why?). In this case, the equation $k + x = \ell$ has the same solution if and only if $m + \ell = n + k$. We use this idea to define an equivalence relation $\approx$ on $\mathbb{N} \times \mathbb{N}$ or $\mathbb{N}^2$ by

$$(m, n) \approx (k, \ell) \iff m + \ell = n + k.$$

The equivalence class of (m, n) with respect to $\approx$ can be denoted by

$$m \mathbin{\dot{-}} n.$$

We denote the set of all such classes by $\mathbb{Z}$; this is the set of **integers.** So we have

$$\mathbb{Z} = \mathbb{N}^2/{\approx}.$$

One checks that arithmetic can be defined on $\mathbb{Z}$ by

$$(m \mathbin{\dot{-}} n) + (k \mathbin{\dot{-}} \ell) = (m + k) \mathbin{\dot{-}} (n + \ell), \quad (m \mathbin{\dot{-}} n) \cdot (k \mathbin{\dot{-}} \ell) = (mk + n\ell) \mathbin{\dot{-}} (m\ell + nk);$$

and a strict ordering, by

$$m \mathbin{\dot{-}} n < k \mathbin{\dot{-}} \ell \iff m + \ell < n + k.$$

We can embed $\mathbb{N}$ in $\mathbb{Z}$ by the map

$$x \mapsto x \mathbin{\dot{-}} 0.$$

For the class $0 \mathbin{\dot{-}} n$, we introduce the name

$$-n.$$

We identify $\mathbb{N}$ with its image in $\mathbb{Z}$. The function $(x, y) \mapsto x \mathbin{\dot{-}} y$ from $\mathbb{N}^2$ to $\mathbb{Z}$ extends to the binary operation of **subtraction** on $\mathbb{Z}$, given by

$$(m \mathbin{\dot{-}} n) - (k \mathbin{\dot{-}} \ell) = (m + \ell) \mathbin{\dot{-}} (n + k).$$

Theorem 13. *$\mathbb{Z}$ is an **integral domain,** that is,*

1. *it contains the additive identity 0 and the multiplicative identity 1,*
2. *addition is commutative and associative,*
3. *equations (3) are always soluble;*
4. *multiplication is commutative and associative;*
5. *multiplication distributes over addition,*
6. *if $x \cdot y = 0$, but $x \neq 0$, then $y = 0$.*

2.4. **The rationals.** The construction of the **rationals** in general proceeds just as for the positive rationals in 2.2, only now the relation $\sim$ defined in (6) must be understood as a relation on $\mathbb{Z} \times (\mathbb{Z} \smallsetminus \{0\})$. The set of classes m/n, where $m \in \mathbb{Z}$ and $n \in \mathbb{Z} \smallsetminus \{0\}$, is denoted by $\mathbb{Q}$; so

$$\mathbb{Q} = (\mathbb{Z} \times (\mathbb{Z} \smallsetminus \{0\}))/{\sim}.$$

Lemma. *$\mathbb{Q}$ is a **field,** that is,*

1. *it is an integral domain,*
2. *equations (7) are always soluble when $b \neq 0$.*

Theorem 14. *$\mathbb{Q}$ is an **ordered field,** that is,*

1. *it is both a field and an ordered set,*

(2) for all nonzero elements x, exactly one of x and $-x$ is positive,
(3) the the sum and product of two positive elements is always positive.

On any ordered field, there is an operation $x \mapsto |x|$, where

$$|a| = \begin{cases} a, & \text{if } a \geqslant 0; \\ -a, & \text{if } a < 0. \end{cases}$$

Here $|a|$ is the **absolute value** of a. An absolute value is always positive or 0.

Theorem 15. *$\mathbb{Q}$ embeds uniquely in every ordered field.*

Proof. Suppose K is an ordered field. Then K contains elements 0 and 1, and so there is a unique homomorphism h from $(\mathbb{N}, 0, n \mapsto n+1)$ to $(K, 0, x \mapsto x+1)$. By induction on n, if $m < n$ in $\mathbb{N}$, then $h(m) < h(n)$. Therefore h is injective. Hence we can treat $\mathbb{N}$ as a subset of K, and then we can construct $\mathbb{Q}$ inside K. □

We can now replace $\mathbb{Z}$ with its image in $\mathbb{Q}$.

Theorem 16. *The ordering of every ordered field is* ***dense,*** *that is, if x and y are elements of the field, and $x < y$, then there is z in the field such that $x < z < y$.*

Proof. Let $z = (x + y)/2$. □

An ordered set is **complete** if every nonempty subset with an upper bound has a *least* upper bound. If a subset does have a least upper bound, then it is unique and is called the **supremum** of the subset. A *greatest lower* bound is called an **infimum.**

Theorem 17. *In a complete ordered set, every nonempty subset with a lower bound has an infimum.*

Proof. Suppose A has an element b and a lower bound. Let C be the set of lower bounds of A. Then C is nonempty and has the upper bound b. A supremum of C is an infimum of A. Indeed, suppose d is a supremum of C. If $x < d$, then there is y in C such that $x < y \leqslant d$, so in particular $x \notin A$. Thus d is a lower bound of A. In particular, $d \in C$; so d is the greatest of the lower bounds of A. □

Even though $\mathbb{Q}$ is dense as an ordered set, we shall show that it is not complete.

Theorem 18. *The equation*

$$x^2 = 2 \tag{10}$$

has no solution in $\mathbb{Q}$.

Proof. We can use the method of **infinite descent.** Suppose there were a solution, n/m. We may assume m and n are positive integers. Then $n^2 = 2m^2$, so n must be *even:* say $n = 2k$. So $4k^2 = 2m^2$, hence $2k^2 = m^2$. Thus m/k is also a solution to (10). But $0 < m < n$. Thus there is no *least* n in $\mathbb{N}$ such that, for some m in $\mathbb{N}$, n/m solves (10). Therefore (10) has no solution, by Theorem 12. □

Theorem 19. *The set $\{x \in \mathbb{Q} \colon x^2 < 2\}$ has an upper bound in $\mathbb{Q}$, but no supremum.*

Proof. Call the set A. It has 2 as an upper bound. Suppose b is an upper bound. We show:

(1) $2 < b^2$;
(2) A has upper bounds less than b.

For 1, suppose $c \in \mathbb{Q}$ and $c^2 \leqslant 2$. We show c is *not* an upper bound of A by finding some positive h in $\mathbb{Q}$ such that $(c+h)^2 < 2$. For all h, we have
$$(c+h)^2 = c^2 + 2ch + h^2 = c^2 + (2c+h)h.$$
We have $c^2 < 2$ by Theorem 18, and moreover $c < 2$. If also $0 < h < 1$, then $2c + h < 5$, so
$$(c+h)^2 < c^2 + 5h.$$
Thus, if we require also $h < (2-c^2)/5$, then $(c+h)^2 < 2$. We can certainly find such h; just let h be the lesser of $1/2$ and $(2-c^2)/6$. Therefore c is not an upper bound of A. This proves 1.

For 2, since 2 is an upper bound for A, we may assume $b \leqslant 2$. If $k > 0$, then
$$(b-k)^2 = b^2 - 2bk + k^2 > b^2 - 2bk \geqslant b^2 - 4k.$$
Let also $k < (b^2-2)/4$; then $(b-k)^2 > 2$, so $b-k$ is an upper bound of A that is less than b. □

3. Construction of the real numbers

As a consequence of Theorem 19, we can write $\mathbb{Q}$ as the union of two nonempty disjoint sets A and B, where

(1) each element of A is less than each element of B;
(2) A has no greatest element;
(3) B has no least element.

Indeed, just let $A = \{x \in \mathbb{Q} \colon x < 0 \vee x^2 < 2\}$, and $B = \{x \in \mathbb{Q} \colon x > 0 \mathbin{\&} x^2 > 2\}$. See Figure 7. Here the pair (A, B) is an example of a *cut* in the sense of Dedekind [4, I, IV., pp. 12 f.]. Since B can be obtained from A as $\mathbb{Q} \smallsetminus A$, we may just refer to A as a cut. To be precise then, we define a **cut** of $\mathbb{Q}$ to be a nonempty proper subset A of $\mathbb{Q}$ such that

Figure 7

(1) every element of A is less than every element of $\mathbb{Q} \smallsetminus A$,
(2) $\mathbb{Q} \smallsetminus A$ has no least element, that is, if A has a supremum in $\mathbb{Q}$, then it belongs to A.

(Note that, in place of 2, one could require A to have no least element.) We denote the set of cuts of $\mathbb{Q}$ by

$$\mathbb{R}.$$

That is, a cut of $\mathbb{Q}$ is precisely a **real number.**

Dedekind [4, I] observes that this construction of $\mathbb{R}$ results in the complete ordered field that we want. Details are worked out in Landau [10], and also in Spivak's *Calculus* [14, ch. 28]. Spivak writes,

> The mass of drudgery which this chapter necessarily contains is relieved by one truly first-rate idea

—namely, the idea of what Dedekind calls a cut. My own view is that, in mathematics, if you think something is drudgery, then perhaps you are not looking at it the right way.

3.1. Cuts.

In the interest of finding some insight in the construction of $\mathbb{R}$, I note that the notion of a cut makes sense in any ordered set. Suppose A is an ordered set. A **cut** of A is a proper nonempty subset X of A such that

(1) every element of X is less than every element of $A \smallsetminus X$, that is, X is an **initial segment** of A, and
(2) if X has a supremum in A, then it belongs to X.

If $b \in A$, let

$$(b) = \{x \in A \colon x \leqslant b\};$$

this is an example of a cut of A. Let us denote by

$$\overline{A}$$

the set of all cuts of A. Then $\overline{A}$ is an ordered set when we define

$$X < Y \iff X \subset Y.$$

Also, A embeds in $\overline{A}$ under $x \mapsto (x)$; in particular, we have

$$x < y \iff (x) < (y).$$

Theorem 20. *Suppose A is an ordered set. Then $\overline{A}$ is a complete ordered set, and for all X in $\overline{A}$,*

$$X = \sup(\{(y) \colon y \in A \mathbin{\&} (y) \leqslant X\}). \tag{11}$$

*Hence $\overline{A}$ is a **completion** of A with respect to $x \mapsto (x)$, in that, if some B is also a complete ordered set, and some f embeds A in B, then $\overline{A}$ embeds in B under some g such that $g((x)) = f(x)$, that is, the following diagram* commutes:

$$\begin{tikzcd} A \arrow[r, "x\mapsto(x)"] \arrow[d, "f"'] & \overline{A} \arrow[dl, "g"] \\ B & \end{tikzcd}$$

If, further, B is a completion of A with respect to f, then g is an isomorphism from $\overline{A}$ to B.

Proof. Suppose C is a subset of $\overline{A}$ with an upper bound. Then $\bigcup C$ is a cut of A, so $\bigcup C \in \overline{A}$. If $X \in C$, then $X \subseteq \bigcup C$; thus $\bigcup C$ is an upper bound of C. If Y is an upper bound of C, then for all X in C, we have $X \subseteq Y$: therefore $\bigcup C \subseteq Y$. Consequently,

$$\bigcup C = \sup(C).$$

So $\overline{A}$ is complete.

To show (11), let $X' = \sup(\{(x) \colon x \in A \mathbin{\&} (x) \leqslant X\})$. If $Y < X'$, then $Y < (x) \leqslant X$ for some x in A. Thus $X' \leqslant X$. Suppose now $X' < Y$. Then $Y \smallsetminus X'$ contains some x in A, so that $X' < (x) \leqslant Y$. But then $X < (x)$, so $X < Y$. Thus $X \leqslant X'$, and consequently $X = X'$.

Suppose B is a complete ordered set, and A embeds in B under f. Then $\overline{A}$ embeds in B under g, where for all X in $\overline{A}$,

$$g(X) = \sup\{f(x) \colon x \in A \mathbin{\&} (x) \leqslant X\}.$$

Then $g((x)) = f(x)$. Thus $\overline{A}$ is a completion of A.

Suppose further that B is also a completion of A, with respect to f. Then B embeds in $\overline{A}$ under some map h such that $h(f(x)) = (x)$. If $x \in A$, we have

$$h \circ g((x)) = h(f(x)) = (x);$$

thus $h \circ g$ is identical on $\{(x) \colon x \in A\}$. Let $X \in \overline{A}$. If $(x) \leqslant X$, then, since $h \circ g$ is order-preserving, we have

$$(x) = h \circ g((x)) \leqslant h \circ g(X).$$

By (11) then, we must have $X \leqslant h \circ g(X)$. Conversely, if $X < Y$, then $X \leqslant (x) < Y$, where $x \in Y \smallsetminus X$; hence $h \circ g(X) \leqslant (x) < Y$. Thus $h \circ g(X) \leqslant X$. Consequently, $h \circ g$ is identical on $\overline{A}$. □

An **ordered Abelian group** is an Abelian group that is ordered so that

$$x < y \implies x + z < y + z;$$

equivalently,

$$x > 0 \iff -x < 0, \qquad x > 0 \mathbin{\&} y > 0 \implies x + y > 0.$$

Here those x such that $x > 0$ are **positive.** As usual, we define

$$|x| = \begin{cases} x, & \text{if } x \geqslant 0; \\ -x, & \text{if } x < 0. \end{cases}$$

An ordered Abelian group is **complete** if it is complete as an ordered set. For example, $\mathbb{Q}$ is an ordered Abelian group, but is *not* complete, by Theorem 19. We shall observe below that $\mathbb{Z}$ is a complete ordered Abelian group. However, $\mathbb{Z}$ is **discrete,** because it has a least positive element (namely 1); but $\mathbb{Q}$ is not discrete.

Theorem 21. *Every ordered Abelian group that is not discrete is dense.*

Proof. Suppose G is an ordered Abelian group that is not discrete, and $a < b$ in G. Then $0 < c < b - a$ for some c, and then $a < a + c < b$. □

An ordered Abelian group is **Archimedean** if for every nonzero element a and element b there is an integer n such that $b < n\,|a|$. Then $\mathbb{Z}$ and $\mathbb{Q}$ are Archimedean. However, we can order the free Abelian group $\mathbb{Z} \oplus \mathbb{Z}$ by defining

$$(a, b) < (c, d) \iff (a < c \vee (a = c \mathbin{\&} b < d)),$$

so that

$$\cdots < (-1, 0) < (-1, 1) < \cdots < (0, -1) < (0, 0) < (0, 1) < \cdots < (1, -1) < (1, 0) < \cdots$$

The ordering is discrete, but non-Archimedean.

Theorem 22. *Every complete ordered Abelian group is Archimedean.*

Proof. In a non-Archimedean ordered Abelian group, there are two elements a and b such that a is positive, and b is an upper bound of $\{na \colon n \in \mathbb{Z}\}$. Then $b - a$ is also an upper bound of this set. Therefore this set has no supremum. Hence the ordered group is not complete. □

Theorem 23. *Every discrete complete ordered Abelian group is uniquely isomorphic to $\mathbb{Z}$.*

Proof. $\mathbb{Z}$ is complete by Theorem 12. Suppose A is a discrete Archimedean ordered Abelian group, and let a be its least positive element. If $b \in A$, then $|b| \leqslant na$ for some minimal n in $\mathbb{N}^+$, and then

$$(n-1)a < |b| \leqslant na, \qquad 0 < |b| - (n-1)a \leqslant a,$$

so $|b| = na$ by minimality of a. Thus a generates A. Then there is an isomorphism from A to $\mathbb{Z}$ taking a to 1, and this is the only isomorphism. □

Theorem 24. *If A and A_1 are dense complete ordered Abelian groups, and a and a_1 are positive elements of A and A_1 respectively, then there is a unique isomorphism from A to A_1 that takes a to a_1.*

Proof. Suppose $n \in \mathbb{N}^+$, and b in A is positive or 0. The set $\{x \in A\colon nx \leqslant b\}$ contains 0 and has b as an upper bound; so it has a supremum, which we may denote by b/n. We justify this notation by showing

$$n \cdot \frac{b}{n} = b. \tag{12}$$

Suppose $nu < b$. By density, there are x_k in A such that

$$nu = x_0 < x_1 < \cdots < x_{n-1} < x_n = b.$$

Let c be the least of the $x_k - x_{k-1}$. Then $n(u + c) = nu + nc \leqslant b$. Thus u is not an upper bound of $\{x \in A\colon nx \leqslant b\}$. Similarly, if $b < nu$, then u is not the supremum of $\{x \in A\colon nx \leqslant b\}$. So (12) follows.

If $b < 0$, we define $b/n = -|b|/n$. Note that the equation $nx = b$ has at most one solution in A, since of $x < y$, then $nx < ny$. Then b/n is that unique solution. Moreover, if $m/n = m'/n'$ in $\mathbb{Q}$, so that $mn' = m'n$, then

$$\frac{ma}{n} = \frac{m'a}{n'},$$

since if $ma = nx$, while $m'a = n'y$, then $m'nx = mn'y$, so $x = y$ as before. Thus we have a well-defined function $x \mapsto xa$, or

$$\frac{m}{n} \mapsto \frac{ma}{n},$$

from $\mathbb{Q}$ to A. This function is an embedding of ordered groups. We can denote the image of $\mathbb{Q}$ in A by $\mathbb{Q}a$.

If b is an arbitrary element of A, let

$$b' = \sup(\{xa\colon x \in \mathbb{Q} \mathbin{\&} xa \leqslant b\}).$$

If $c < b$, then $a < n(b - c)$ for some n in $\mathbb{N}^+$, and then there is m in $\mathbb{Z}$ such that

$$c < \frac{m}{n}a \leqslant b.$$

This shows $c \neq b'$. If $b < c$, then again $c \neq b'$. Therefore $b' = b$. Now the isomorphism from $\mathbb{Q}a$ to $\mathbb{Q}a_1$ that takes a to a_1 extends to an isomorphism

$$b \mapsto \sup(\{xa_1\colon x \in \mathbb{Q} \mathbin{\&} xa \leqslant b\})$$

from A to A_1; and this is the only way it can extend. □

Theorem 25. *Every Archimedean ordered Abelian group A has a completion; one such completion is $\overline{A}$.*

Proof. On $\overline{A}$ we define

$$X + Y = A \smallsetminus \{x + y\colon x \in A \smallsetminus X \mathbin{\&} y \in A \smallsetminus Y\}).$$

In particular, $(x)+(y) = (x+y)$. To check that $X+Y \in \overline{A}$ generally, suppose $x \in A \smallsetminus X$ and $y \in A \smallsetminus Y$. Since $A \smallsetminus X$ has no least element, there is z in $A \smallsetminus X$ such that $z < x$ and hence $z + y < x + y$. Thus $A \smallsetminus (X + Y)$ has no least element. The remaining conditions are easily met, and $X + Y \in \overline{A}$.

Since $+$ is commutative on A, it is commutative on $\overline{A}$ by its definition. Almost as easily, $+$ is associative on $\overline{A}$, since

$$\begin{aligned}X+(Y+Z) &= A\smallsetminus\{x+u\colon x\in A\smallsetminus X \mathbin{\&} u\in A\smallsetminus(Y+Z)\}\\ &= A\smallsetminus\{x+(y+z)\colon x\in A\smallsetminus X \mathbin{\&} y\in A\smallsetminus Y \mathbin{\&} z\in A\smallsetminus Z\}\\ &= A\smallsetminus\{(x+y)+z\colon x\in A\smallsetminus X \mathbin{\&} y\in A\smallsetminus Y \mathbin{\&} z\in A\smallsetminus Z\}\\ &= A\smallsetminus\{v+z\colon v\in A\smallsetminus(X+Y) \mathbin{\&} z\in A\smallsetminus Z\}\\ &= (X+Y)+Z.\end{aligned}$$

Also,

$$X+(0)=A\smallsetminus\{x+y\colon x\in A\smallsetminus X \mathbin{\&} y\geqslant 0\}=A\smallsetminus(A\smallsetminus X)=A$$

since if $x\in A\smallsetminus X$ and $y\geqslant 0$, then $x+y\in A\smallsetminus X$. Now we know that $\overline{A}$ is an ordered *monoid* in which A embeds.

To continue, we define

$$-X=\begin{cases}(-a), & \text{if } X=(a) \text{ for some } a \text{ in } A;\\ \{-x\colon x\in A\smallsetminus X\}, & \text{if } X\neq(a) \text{ for any } a \text{ in } A.\end{cases}$$

We have $(a)+(-a)=(0)$. Now suppose $X\neq(a)$ for any a in A. Say $x\in A\smallsetminus X$ and $y\in A\smallsetminus(-X)$. Then $-y\in X$, so $-y<x$, and hence $0<x+y$. Thus $(0)\leqslant X+(-X)$.

So far we have not used that A is Archimedean. But now suppose $(0)<x$. We still assume X is not any (a). There is some least integer n such that $nx\notin X$. Then $(n-1)x\in X$, so $(1-n)x\notin -X$, and hence $x\notin X+(-X)$. Thus $X+(-X)\leqslant(0)$, and therefore $X+(-X)=(0)$. So $\overline{A}$ is indeed a group. □

Recall that $\mathbb{R}=\overline{\mathbb{Q}}$. Let

$$\mathbb{R}^+=\{X\in\mathbb{R}\colon X\geqslant(0)\}.$$

Then there is an obvious isomorphism from $\mathbb{R}^+$ to $\overline{\mathbb{Q}^+}$, namely $X\mapsto X\cap\mathbb{Q}^+$.

Theorem 26. *$\mathbb{R}$ is a complete ordered field, and every complete ordered field is isomorphic to it.*

Proof. By Theorem 25, $\mathbb{R}$ has the structure of an ordered Abelian group. So does $\overline{\mathbb{R}^+}$, when we write the group operation multiplicatively. This multiplication extends in the standard way to $\mathbb{R}\smallsetminus\{(0)\}$, which is then an Abelian group, although not an ordered group. Finally, we define $X\cdot(0)=(0)$. Then $\mathbb{R}$ is an ordered field, provided multiplication distributes over addition.

Working first inside $\mathbb{R}^+$ or rather $\overline{\mathbb{Q}^+}$, we have

$$\begin{aligned}X\cdot(Y+Z) &= \mathbb{Q}^+\smallsetminus\{x\cdot u\colon x\in\mathbb{Q}^+\smallsetminus X \mathbin{\&} u\in\mathbb{Q}^+\smallsetminus(Y+Z)\}\\ &= \mathbb{Q}^+\smallsetminus\{x\cdot(y+z)\colon x\in\mathbb{Q}^+\smallsetminus X \mathbin{\&} y\in\mathbb{Q}^+\smallsetminus Y \mathbin{\&} z\in\mathbb{Q}^+\smallsetminus Z\}\\ &= \mathbb{Q}^+\smallsetminus\{x\cdot y+x\cdot z\colon x\in\mathbb{Q}^+\smallsetminus X \mathbin{\&} y\in\mathbb{Q}^+\smallsetminus Y \mathbin{\&} z\in\mathbb{Q}^+\smallsetminus Z\}\\ &\geqslant X\cdot Y+X\cdot Z.\end{aligned}$$

To prove the reverse inequality, suppose $a\in\mathbb{Q}^+$ and

$$(a)<X\cdot(Y+Z).$$

Then there is b in $\mathbb{Q}^+$ such that
$$\frac{(a)}{Y+Z} < (b) \leqslant X.$$
Then $(a/b) < Y + Z$, so there is c in $\mathbb{Q}^+$ such that
$$\left(\frac{a}{b}\right) - Z < (c) \leqslant Y.$$
Consequently,
$$\begin{aligned}(a) = \left(b \cdot \frac{a}{b}\right) = \left(b \cdot \left(c + \frac{a}{b} - c\right)\right) = \left(b \cdot c + b \cdot \left(\frac{a}{b} - c\right)\right)&\\ = (b)(c) + (b)\left(\frac{a}{b} - c\right) \leqslant X \cdot Y + X \cdot Z.&\end{aligned}$$
Since $X \cdot (Y + Z) = \sup(\{(a) \colon a \in \mathbb{Q}^+ \ \&\ (a) < X \cdot (Y + Z)\})$ (by (11) and density of $\mathbb{Q}^+$), we have
$$X \cdot (Y + Z) \leqslant X \cdot Y + X \cdot Z.$$
This establishes distributivity of multiplication over addition on $\mathbb{R}^+$ and then all of $\mathbb{R}$. Uniqueness of $\mathbb{R}$ as a complete ordered field follows from Theorem 24. □

Henceforth we may say $\mathbb{R}$ is *the* complete ordered field.

3.2. **Cauchy sequences.** Another way to construct $\mathbb{R}$ is by means of *Cauchy sequences.* First of all, a sequence $(a_n \colon n \in \mathbb{N})$ **converges** to the real number b if, for all positive real numbers ε, there is a natural number R such that, for all n in $\mathbb{N}$, if $n \geqslant R$, then
$$|a_n - b| < \varepsilon.$$
In this case, we write
$$\lim_{n\to\infty} a_n = b,$$
or perhaps $\lim(a_n \colon n \in \mathbb{N}) = b$.

Lemma. *A bounded monotone sequence in* $\mathbb{R}$ *converges.*

Proof. Let $(a_n \colon n \in \mathbb{N})$ be bounded an increasing, and let $b = \sup(\{a_n \colon n \in \mathbb{N}\})$. Suppose $\varepsilon > 0$. Then $b - \varepsilon$ is not an upper bound of $\{a_n \colon n \in \mathbb{N}\}$, so for some R in $\mathbb{N}$, we have
$$b - \varepsilon < a_R \leqslant b.$$
Since the sequence is increasing, if $n \geqslant R$, we have
$$b - \varepsilon < a_R \leqslant a_n \leqslant b,$$
and therefore
$$|a_n - b| = b - a_n < \varepsilon.$$
Thus $(a_n \colon n \in \mathbb{N})$ converges to b. Similarly, bounded decreasing sequences converge. □

A sequence $(a_n \colon n \in \mathbb{N})$ of real numbers is a **Cauchy sequence** if, for every positive real number ε, there is a natural number R such that, for all m and n in $\mathbb{N}$, if $m \geqslant R$ and $n \geqslant R$, then
$$|a_m - a_n| < \varepsilon.$$

For example, let sequences $(p_n : n \in \mathbb{N})$ and $(q_n : n \in \mathbb{N})$ be defined recursively by

$$p_0 = 1, \qquad q_0 = 1,$$
$$p_{n+1} = p_n + 2q_n, \qquad q_{n+1} = p_n + q_n.$$

Let $a_n = p_n/q_n$. Then

$$(a_n : n \in \mathbb{N}) = \Big(1, \frac{3}{2}, \frac{7}{5}, \frac{17}{12}, \frac{41}{29}, \dots\Big).$$

You can show that

$$p_n q_{n+1} - q_n p_{n+1} = (-1)^{n+1},$$

and hence

$$a_{n+1} - a_n = \frac{(-1)^n}{q_{n+1}q_n}.$$

Since $(q_n : n \in \mathbb{N})$ is increasing, it follows that

$$a_0 < a_2 < a_4 < \dots < a_5 < a_3 < a_1,$$

and moreover $(a_n : n \in \mathbb{N})$ is a Cauchy sequence. Finally,

$${p_n}^2 - 2{q_n}^2 = (-1)^{n+1},$$

so $(a_n : n \in \mathbb{N})$ converges to $\sqrt{2}$, which however is not in $\mathbb{Q}$, by Theorem 18.

Lemma. *Every Cauchy sequence in $\mathbb{R}$ is bounded.*

Proof. Let $(a_n : n \in \mathbb{N})$ be a Cauchy sequence. Let R be such that, if $m \geqslant R$ and $n \geqslant R$, then $|a_m - a_n| \leqslant 1$. In particular, if $m \geqslant R$, then

$$|a_m| \leqslant |a_m - a_R| + |a_R| \leqslant 1 + |a_R|.$$

Thus each $|a_n|$ is bounded by $\max(|a_0|, \dots, |a_{R-1}|, 1 + |a_R|)$. □

Theorem 27. *Every Cauchy sequence in $\mathbb{R}$ converges.*

Proof. Let $(a_n : n \in \mathbb{N})$ be a Cauchy sequence. Then the sequence is bounded, by the last lemma. In particular, we can define

$$b_k = \sup(\{a_n : n \geqslant k\}).$$

Then $(b_k : k \in \mathbb{N})$ is bounded (why?) and decreasing, so it converges to some c by the next to last lemma. We have

$$|a_m - c| \leqslant |a_m - a_n| + |a_n - b_k| + |b_k - c|.$$

Let $\varepsilon > 0$. There is some R such that, if $k \geqslant R$, $m \geqslant R$, and $n \geqslant R$, then $|a_m - a_n| < \varepsilon/3$ and $|b_k - c| < \varepsilon/3$. For all k, there is n such that $n \geqslant k$ and $|a_n - b_k| < \varepsilon/3$. Therefore, if $m \geqslant R$, then $|a_m - c| < \varepsilon$. Thus $(a_n : n \in \mathbb{N})$ converges. □

For the alternative construction of $\mathbb{R}$, let us denote by

$$\mathbb{Q}^{\mathbb{N}}$$

the set of functions from $\mathbb{N}$ to $\mathbb{Q}$, that is, rational sequences. This becomes a commutative ring when, writing a for $(a_n : n \in \mathbb{N})$, we define

$$(a+b)_n = a_n + b_n, \qquad (-a)_n = -a_n, \qquad (ab)_n = a_n b_n.$$

Then $\mathbb{Q}$ embeds in this ring under the map that takes x to the sequence that is identically x. We may identify $\mathbb{Q}$ with its image in $\mathbb{Q}^{\mathbb{N}}$. Let S be the set of Cauchy sequences in $\mathbb{Q}^{\mathbb{N}}$. Then $\mathbb{Q} \subseteq S$.

Lemma. *S is a sub-ring of $\mathbb{Q}^{\mathbb{N}}$; that is, S contains 0 and 1 and is closed under $+$, $-$, and $\cdot$.*

Proof. The most difficult part is closure under multiplication. Let a and b be in S. By the previous lemma, there is R such that, for all n in $\mathbb{N}$, we have $|a_n| \leqslant R$ and $|b_n| \leqslant R$. Hence

$$\begin{aligned}|a_m b_m - a_n b_n| = |a_m b_m - a_n b_m + a_n b_m - a_n b_n| &\leqslant |a_m - a_n|\,|b_m| + |a_n|\,|b_m - b_n| \\ &\leqslant R(|a_m - a_n| + |b_m - b_n|).\end{aligned}$$

Then ab is Cauchy. □

By Theorem 27, we have a map $x \mapsto \lim x$, in fact a homomorphism, from S to $\mathbb{R}$. Let I be the kernel, namely the set of sequences in $\mathbb{Q}^{\mathbb{N}}$ that converge to 0. Then I is an *ideal* of S.

Theorem 28. *$S/I \cong \mathbb{R}$ under $x \mapsto \lim x$; in particular, I is a maximal ideal of S.*

Proof. We just have to show $x \mapsto \lim x$ is surjective. Let $a \in \mathbb{R}$. Then $a = \sup\{x \in \mathbb{Q} \colon x < a\}$. By the *Axiom of Choice,* there is a sequence b in $\mathbb{Q}^{\mathbb{N}}$ such that

$$b_0 < a, \qquad\qquad b_n + \frac{a - b_n}{2} < b_{n+1} < a.$$

Then $\lim b = a$. Thus S maps onto $\mathbb{R}$ under $x \mapsto \lim x$. □

4. Non-Archimedean fields

In moving from $\mathbb{N}$ to $\mathbb{Z}$ to $\mathbb{Q}$ to $\mathbb{R}$, we achieve the following. The formal sentence

$$\forall x\ \forall y\ \exists z\ x+z=y$$

is false in $\mathbb{N}$, but true in $\mathbb{Z}$. The sentence

$$\forall x\ \forall y\ \exists z\ (x\cdot z=y\lor x=0)$$

is false in $\mathbb{Z}$, but true in $\mathbb{Q}$. The sentence

$$\forall x\ \exists y\ (y^2=x\lor x<0)$$

is false in $\mathbb{Q}$, but true in $\mathbb{R}$ (why?). Thus, moving to $\mathbb{R}$ allows us to solve more equations. Is there any advantage to moving *beyond* $\mathbb{R}$?

In any case, we *can* move beyond $\mathbb{R}$. Let

$$\mathbb{R}[x]$$

denote the set of **polynomials** in x over $\mathbb{R}$: these have the form

$$a_0+a_1x+a_2x^2+\cdots+a_nx^n \tag{13}$$

or

$$\sum_{k=0}^{n}a_kx^k,$$

where the coefficients a_k are in $\mathbb{R}$. Then $\mathbb{R}[x]$ is an integral domain in which $\mathbb{R}$ embeds. Note that, if $m\leqslant n$, then

$$\sum_{k=0}^{m}a_kx^k=\sum_{k=0}^{n}b_kx^k\iff a_0=b_0\ \&\ \dots\ \&\ a_m=b_m\ \&\ b_{m+1}=0\ \&\ \dots\ \&\ b_n=0.$$

Thus, a polynomial is not simply an expression of the form in (13); it is an equivalence-class of such expressions. However, every polynomial in x can be written uniquely as an **infinite series**

$$\sum_{k=0}^{\infty}a_kx^k;$$

but here all but finitely many of the coefficients a_k are 0.

Just as we construct $\mathbb{Q}$ from $\mathbb{Z}$, so from $\mathbb{R}[x]$ we construct $\mathbb{R}(x)$, the set of **rational functions** in x over $\mathbb{R}$, consisting of the fractions

$$\frac{a_0+\cdots+a_nx^n}{b_0+\cdots+b_mx^m}. \tag{14}$$

Then $\mathbb{R}(x)$ is a field.

Theorem 29. *$\mathbb{R}(x)$ becomes a non-Archimedean ordered field when, for every element as in (14) such that $a_nb_m\neq 0$, that element is considered positive if and only if $a_nb_m>0$.*

Proof. Easily $\mathbb{R}(x)$ is an ordered field; it is non-Archimedean, since $-a+x>0$, that is, $x>a$, for all a in $\mathbb{Z}$. □

Suppose now K is an arbitrary ordered field that includes $\mathbb{R}$. Each element of K that is smaller (in absolute value) than *some* rational is called **finite;** each element that is smaller than *every* nonzero rational is called **infinitesimal.** Elements of K that are not finite are **infinite.**

For example, in $\mathbb{R}(x)$, for all a in $\mathbb{Q}$, we have

$$a < x < x^2 < x^3 < \cdots, \tag{15}$$

so the positive powers of x are infinite. Hence also, if a is a *positive* rational, we have

$$a > \frac{1}{x} > \frac{1}{x^2} > \frac{1}{x^3} > \cdots > 0, \tag{16}$$

so the negative powers of x are infinitesimal.

With K as before, let R be the set of finite elements of K, and let I be the set of infinitesimal elements. Then R is a sub-ring of K, and I is an ideal of R.

The **units** or multiplicatively invertible elements of a ring R compose a multiplicative group denoted by

$$R^\times. \tag{17}$$

In our situation, an element a of $K^\times$ is infinite if and only if $a^{-1} \in I$. In particular, either a or a^{-1} is finite—belongs to R. For this reason, R is called a **valuation ring;** the reason for the terminology will be seen below. It also follows that every element of $R \smallsetminus I$ is a unit of R. Consequently, I is a maximal ideal of R and is moreover the *unique* maximal ideal of R. For this reason, R is called a **local ring.** (So every valuation ring is a local ring.) Since I is maximal, we know R/I is a field.

Theorem 30. *Let K be an ordered field that includes $\mathbb{R}$, and let R be the ring of finite elements of K, with maximal ideal I of infinitesimals. Then the quotient map $x \mapsto x + I$ determines an isomorphism from $\mathbb{R}$ onto R/I.*

Proof. Let h be $x \mapsto x + I$ on $\mathbb{R}$. Then $\ker(h) = I \cap \mathbb{R}$, which is $\{0\}$. Thus h is injective. It remains to show h is surjective onto R/I.

Let $a \in R$. Since a is finite, the set $\{x \in \mathbb{R} \colon x < a\}$ has an upper bound in $\mathbb{R}$, hence a supremum, a'. We shall show $h(a') = a + I$. To this end, suppose $b \in \mathbb{R}$, but $h(b) \neq a + I$. This means $b - a$ is not infinitesimal. In particular, for some real number δ, we have

$$0 < \delta < |b - a|.$$

If $b < a$, then $b < b + \delta < a$, so b is not an upper bound of $\{x \in \mathbb{R} \colon x < a\}$. If $a < b$, then $a < b - \delta$, so b is not the supremum of $\{x \in \mathbb{R} \colon x < a\}$. In either case, $b \neq a'$. □

If a and b are arbitrary elements of K such that $a - b \in I$, then a and b are **infinitely close,** and we write

$$a \simeq b.$$

By the theorem, if a is finite, then a is infinitesimally close to some *unique* real number; this number is called the **standard part** of a. In particular, the infinisimals are the elements whose standard part is 0.

Let us see how this all works in $\mathbb{R}(x)$. The finite elements here are those of the form

$$\frac{a_n x^n + \cdots + a_0}{b_n x^n + \cdots + b_0},$$

where $b_n \neq 0$. The standard part of this element is a_n/b_n, since

$$\frac{a_nx^n + \cdots + a_0}{b_nx^n + \cdots + b_0} - \frac{a_n}{b_n} = \frac{(a_{n-1} - a_nb_{n-1}/b_{n-1})x^{n-1} + \cdots}{b_nx^n + \cdots + b_0}.$$

Using the division algorithm taught in school, we can formally compute the quotient of two nonzero elements of $\mathbb{R}[x]$, getting a possibly infinite series

$$c_0 + c_1x^{-1} + c_2x^{-2} + \cdots$$

or simply

$$\sum_{n=0}^{\infty} c_kx^{-k};$$

this is a **formal power series** in x^{-1} with coefficients from $\mathbb{R}$. For example, formally,

$$\frac{x}{x-1} = 1 + x^{-1} + x^{-2} + \cdots.$$

The set of all formal power series in x^{-1} over $\mathbb{R}$ is denoted by $\mathbb{R}[[x^{-1}]]$ or rather

$$\mathbb{R}[[t]],$$

where $t = x^{-1}$. This set is an integral domain in the obvious way, and its *quotient field* is denoted by

$$\mathbb{R}((t));$$

this is the field of **formal Laurent series** in t with coefficients from $\mathbb{R}$, namely series

$$\sum_{n=k}^{\infty} a_nt^n, \tag{18}$$

where $k \in \mathbb{Z}$, and each a_n is in $\mathbb{R}$. This field includes $\mathbb{R}(t)$, which is $\mathbb{R}(x)$.

The ordering of $\mathbb{R}(t)$ extends to $\mathbb{R}((t))$. Indeed, let a be the element in (18), and assume $a_k \neq 0$. Then a is

(1) positive if and only if $a_k > 0$,
(2) finite if and only if $k \geqslant 0$,
(3) infinitesimal if and only if $k > 0$.

If a is finite, then its standard part is a_0 (which is 0 if $k > 0$).

4.1. **Valuations.** The construction of $\mathbb{R}((t))$ as a field uses only that $\mathbb{R}$ is a field. Let K be an arbitrary field, not necessarily ordered; then we can form the field

$$K((t))$$

of formal Laurent series in t with coefficients from K. This has the sub-ring

$$K[[t]]$$

of formal power series in t with coefficients from K. This ring is a valuation ring, with unique maximal ideal (t); here (t) consists of the series $\sum_{n=1}^{\infty} a_nt^n$ with no constant term.

Theorem 31. *$K \cong K[[t]]/(t)$ under $\xi \mapsto \xi + (t)$.*

There is another quotient we can form, namely
$$K((t))^\times/K[[t]]^\times.$$
Here
$$K((t))^\times = K((t)) \smallsetminus \{0\}, \qquad K[[t]]^\times = K[[t]] \smallsetminus (t).$$
The quotient map $\xi \mapsto \xi K[[t]]^\times$ is the **t-adic valuation.** This can be understood by noting that, if $a_k \neq 0$, then
$$\frac{1}{t^k}\sum_{n=k}^{\infty} a_n t^n = \sum_{n=0}^{\infty} a_{k+n} t^n,$$
which is in $K[[t]]^\times$. We might write
$$\sum_{n=k}^{\infty} a_n t^n \equiv t^k \pmod{K[[t]]^\times}.$$
Thus the t-adic valuation maps $\langle t\rangle$ (that is, $\{t^n \colon n \in \mathbb{Z}\}$) onto $K((t))^\times/K[[t]]^\times$. If again $a_k \neq 0$, let
$$\left|\sum_{n=k}^{\infty} a_k t^k\right|_t = t^k;$$
define also
$$|0|_t = 0.$$
Suppose, as before, we order $\langle t\rangle \cup \{0\}$ so that
$$0 < \cdots < t^2 < t < 1 < t^{-1} < \cdots$$
Then

(1) $|ab|_t = |a|_t\,|b|_t$,
(2) $|a|_t = 0$ if and only if $a = 0$,
(3) $|a+b|_t \leqslant \max(|a|_t\,, |b|_t)$.

Compare these properties to the properties of absolute values in an ordered field, or on $\mathbb{C}$:

(1) $|ab| = |a|\,|b|$,
(2) $|a| = 0$ if and only if $a = 0$,
(3) $|a+b| \leqslant |a| + |b|$.

All of this can be done quite generally. Let $\mathfrak{O}$ be an arbitrary valuation ring with unique maximal ideal $\mathfrak{p}$ and and quotient field K. We order the multiplicative group $K^\times/\mathfrak{O}^\times$ by the rule
$$a\mathfrak{O}^\times \leqslant b\mathfrak{O}^\times \iff a/b \in \mathfrak{O},$$
and we say 0 is less than all elements of the group. Let the quotient map from $K^\times$ to $\mathfrak{O}^\times$, together with $\{(0,0)\}$ (the function taking 0 to 0) be denoted by
$$\xi \mapsto |\xi|_{\mathfrak{p}}\,;$$
this is the **$\mathfrak{p}$-adic valuation** on K, and with it, K becomes a **valued field.** The ordered group $K^\times/\mathfrak{O}^\times$ is the **value group,** and the field $\mathfrak{O}/\mathfrak{p}$ is the **residue field.** So $K((t))$, with the t-adic valuation, has the residue field K, by Theorem 31. For an arbitrary

ordered field extending $\mathbb{R}$, with valuation determined by the infinitesimals, the residue field is (isomorphic to) $\mathbb{R}$, by Theorem 30.

In the general situation,

$$\mathfrak{O} = \{x \in K : |x|_{\mathfrak{p}} \leqslant 1\}, \qquad \mathfrak{O}^{\times} = \{x \in K : |x|_{\mathfrak{p}} = 1\}, \qquad \mathfrak{p} = \{x \in K : |x|_{\mathfrak{p}} < 1\}.$$

In particular, the elements of the subgroup $\{n \cdot 1 : n \in \mathbb{Z}\}$ of K take values no greater than 1. But the elements of $K \smallsetminus \mathfrak{O}$ take values greater than 1. For this reason, if $\mathfrak{p} \neq (0)$, the $\mathfrak{p}$-adic valuation is **non-Archimedean.** By contrast, the absolute value function on a subfield of $\mathbb{R}$ or $\mathbb{C}$ is Archimedean.

Theorem 32. *Let $\mathfrak{O}$ be a valuation ring with maximal ideal $\mathfrak{p}$. On the quotient field of $\mathfrak{O}$,*

(1) $|ab|_{\mathfrak{p}} = |a|_{\mathfrak{p}} |b|_{\mathfrak{p}}$,
(2) $|a|_{\mathfrak{p}} = 0$ *if and only if* $a = 0$,
(3) $|a \pm b|_{\mathfrak{p}} \leqslant \max(|a|_{\mathfrak{p}}, |b|_{\mathfrak{p}})$,
(4) if $|a|_{\mathfrak{p}} \neq |b|_{\mathfrak{p}}$, *then* $|a \pm b|_{\mathfrak{p}} = \max(|a|_{\mathfrak{p}}, |b|_{\mathfrak{p}})$.

Proof. For 3, if $b \neq 0$, we have

$$|a \pm b|_{\mathfrak{p}} \leqslant |b|_{\mathfrak{p}} \iff \frac{a \pm b}{b} \in \mathfrak{O} \iff \frac{a}{b} \pm 1 \in \mathfrak{O} \iff \frac{a}{b} \in \mathfrak{O} \iff |a|_{\mathfrak{p}} \leqslant |b|_{\mathfrak{p}}.$$

For 4, suppose $|a|_{\mathfrak{p}} < |b|_{\mathfrak{p}}$. Since

$$|b|_{\mathfrak{p}} = |\pm b|_{\mathfrak{p}} = |a \pm b - a|_{\mathfrak{p}} \leqslant \max(|a \pm b|_{\mathfrak{p}}, |a|_{\mathfrak{p}}),$$

we have $|b|_{\mathfrak{p}} \leqslant |a \pm b|_{\mathfrak{p}} \leqslant |b|_{\mathfrak{p}}$, so $|b|_{\mathfrak{p}} = |a \pm b|_{\mathfrak{p}}$. □

In any valued field, there is the notion of **Cauchy sequence** and **convergent sequence:** the definitions are formally the same as for sequences in $\mathbb{R}$. A valued field is **complete** if every Cauchy sequence of its elements converges. Then $K((t))$ is complete with respect to the t-adic valuation. Also, $\mathbb{R}$ and $\mathbb{C}$ are complete with respect to the usual absolute value function.

A valuation is **discrete** if the value group is cyclic (hence isomorphic to $\mathbb{Z}$). The t-adic valuation of $K((t))$ is discrete.

Lemma. *In a field with a discrete valuation, the sequence of values of terms of a Cauchy sequence is eventually constant.*

Theorem 33. *Every field K with a discrete valuation $x \mapsto |x|$ has a **completion,** namely a complete valued field $\overline{K}$ in which K embeds, such that any embedding of K in a valued field extends to an embedding of $\overline{K}$ in that valued field.*

Proof. Let R consist of the Cauchy sequences of K, and let I consist of those sequences that converge to 0. Then R is a ring with maximal ideal I. Indeed, suppose $(a_n : n \in \mathbb{N})$ is in $R \smallsetminus I$. If n is large enough, then $a_n \neq 0$. Hence, for m and n large enough, we have

$$\left|\frac{1}{a_n} - \frac{1}{a_m}\right| = \left|\frac{a_m - a_n}{a_n a_m}\right| = \frac{|a_m - a_n|}{|a_n a_m|}.$$

By the lemma, $|a_n a_m|$ is eventually constant and nonzero. Therefore, if we define

$$b_n = \begin{cases} {a_n}^{-1}, & \text{if } a_n \neq 0, \\ 1, & \text{if } a_n = 0, \end{cases}$$

then $(b_n : n \in \mathbb{N}) \in R$. Now let

$$c_n = \begin{cases} 0, & \text{if } a_n \neq 0, \\ 1, & \text{if } a_n = 0. \end{cases}$$

Then $(c_n : n \in \mathbb{N}) \in I$, and $a_n b_n + c_n = 1$. Therefore I is indeed a maximal ideal of R. We can embed K in the field R/I under the quotient map. We extend the valuation to R/I by letting a Cauchy sequence have the value that its terms eventually reach. (Why is R/I complete, and the completion of K?) □

The field of rationals has a non-Archimedean completion $\mathbb{Q}_p$ for each prime p. Indeed, the **p-adic valuation** on $\mathbb{Q}$ is given by

$$\left|p^n \cdot \frac{a}{b}\right|_p = \frac{1}{p^n},$$

where $n \in \mathbb{Z}$, and a and b are integers indivisible by p. Then $\mathbb{Q}_p$ consists of the **p-adic numbers,** namely the formal sums

$$\sum_{n=k}^{\infty} a_n p^n,$$

where $k \in \mathbb{Z}$, and $a_n \in \{0, 1, \dots, p-1\}$. For example, in $\mathbb{Q}_p$,

$$-1 = \sum_{n=0}^{\infty} (p-1)p^k.$$

In sum:

(1) $\mathbb{R}$ is the unique complete ordered field;
(2) $\mathbb{R}$ is complete with respect to the absolute value function, but so is $\mathbb{C}$;
(3) there are many fields, even fields that include $\mathbb{Q}$, that are complete with respect to a non-Archimedean valuation.

5. Ultrapowers

5.1. **Algebra.** For notational convenience, if $n \in \mathbb{N}$, let us assume

$$n = \{x \in \mathbb{N} \colon x < n\} = \{0, \dots, n-1\}.$$

To be precise, we can define f on $\mathbb{N}$ by

$$f(0) = \varnothing, \qquad f(n+1) = f(n) \cup \{f(n)\}.$$

By induction, $f(n) = \{f(0), \dots, f(n-1)\}$. With more work, one shows f is injective. The image $f[\mathbb{N}]$ of $\mathbb{N}$ under f is denoted by

$$\omega.$$

So 0 in ω is $\varnothing$, and $n+1$ is $n \cup \{n\}$. It will be convenient to treat ω as $\mathbb{N}$.

Let Ω be a set, and $n \in \omega$. We define

$$\Omega^n$$

as the set of functions from n (that is, $\{0, \dots, n-1\}$) to Ω. In particular,

$$\Omega^0 = \{\varnothing\} = \{0\} = 1.$$

A subset of Ω^n is an **n-ary relation** on Ω. A typical element of Ω^n might be denoted by

$$(x^0, \dots, x^{n-1})$$

or more simply

$$\boldsymbol{x}.$$

On Ω there are just two 0-ary relations, namely $\varnothing$ and $\{\varnothing\}$, that is, 0 and 1.

Suppose now m and n are in ω, and

$$f \colon m \to n.$$

(If $n = 0$, then m must be 0.) Then a function from Ω^n to Ω^m is induced, namely

$$x \mapsto x \circ f.$$

Let us denote this function by

$$f^*$$

or more precisely f^*_Ω. Then[7]

$$f^*(x^0, \dots, x^{n-1}) = (x^{f(0)}, \dots, x^{f(m-1)}).$$

For example, if f is the inclusion of n in $n+1$, then $f^*(x^0, \dots, x^{n-1}, x^n) = (x^0, \dots, x^{n-1})$, or more simply $f^*(\boldsymbol{x}, y) = \boldsymbol{x}$.

In general, we get $X \mapsto f^*[X]$ from $\mathscr{P}(\Omega^n)$ to $\mathscr{P}(\Omega^m)$, where

$$\begin{aligned} f^*[A] &= \{f^*(\boldsymbol{x}) \colon \boldsymbol{x} \in A\} \\ &= \{\boldsymbol{y} \in \Omega^m \colon \exists (x^0, \dots, x^{n-1})\ ((x^0, \dots, x^{n-1}) \in A \ \&\ \boldsymbol{y} = (x^{f(0)}, \dots, x^{f(m-1)}))\}. \end{aligned}$$

[7] In the language of category theory, the pair $(m \mapsto \Omega^m, f \mapsto f^*)$ is a *contravariant functor* from the category $(\omega, \{\text{functions}\})$ to the category $(\{\text{sets}\}, \{\text{functions}\})$.

We also have a function $Y \mapsto f_*(Y)$ from $\mathscr{P}(\Omega^m)$ to $\mathscr{P}(\Omega^n)$ where

$$\begin{aligned} f_*(B) &= (f^*)^{-1}[B] \\ &= \{(x^0, \dots, x^{n-1}) \in \Omega^n \colon (x^{f(0)}, \dots, x^{f(m-1)}) \in B\}. \end{aligned}$$

If again f is the inclusion of n in $n+1$, then $f_*(B)$ can be understood as $B \times \Omega$. If f is a permutation of n, then

$$f^*[A] = (f^{-1})_*(A).$$

Now the statement of Theorem 38 below makes some sense.

So that the *proof* makes sense, suppose R is a commutative ring. As in § 3, we obtain the commutative ring

$$R^\omega.$$

If a is an element $(a_n \colon n \in \omega)$ of this ring, let

$$\operatorname{supp}(a) = \{n \in \omega \colon a_n \neq 0\},$$

the **support** of a. In one case of interest, R is $\mathbb{B}$, the two-element field $\{0, 1\}$.

If X and Y are subsets of some set, let

$$X \mathbin{\triangle} Y = (X \smallsetminus Y) \cup (Y \smallsetminus X),$$

the **symmetric difference** of X and Y.

Theorem 34. *The map $x \mapsto \operatorname{supp}(x)$ is a bijection from $\mathbb{B}^\omega$ onto $\mathscr{P}(\omega)$. Also*

$$\begin{aligned} \operatorname{supp}(0) &= \varnothing, \\ \operatorname{supp}(1) &= \omega, \\ \operatorname{supp}(xy) &= \operatorname{supp}(x) \cap \operatorname{supp}(y), \\ \operatorname{supp}(x+y) &= \operatorname{supp}(x) \mathbin{\triangle} \operatorname{supp}(y), \end{aligned}$$

Thus $\mathscr{P}(\omega)$ inherits from ω^ω the structure of a ring.

A ring (not necessarily commutative) is called **Boolean** if in it

$$x^2 = x. \tag{19}$$

So $\mathbb{B}$, $\mathbb{B}^\omega$, and $\mathscr{P}(\omega)$ are Boolean rings.

Theorem 35. *Let R be a Boolean ring. In R,*

$$2x = 0, \tag{20}$$

and hence

$$-x = x.$$

Also R is commutative, and R can be partially ordered by the rule

$$x \leqslant y \iff xy = x.$$

Then a nonempty subset I of R is an ideal of R if and only if

$$\begin{aligned} x \in I \mathbin{\&} y \in I &\implies x + y \in I, \\ x \in I \mathbin{\&} y \leqslant x &\implies y \in I. \end{aligned} \tag{21}$$

All prime ideals of R are maximal, and and ideal I is maximal if and only if

$$x \in I \iff x + 1 \notin I.$$

Proof. For (20), compute
$$2x = (2x)^2 = 4x^2 = 4x.$$
For commutativity then, compute
$$x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y,$$
$$0 = xy + yx.$$
Immediately from the definitions, $x \leqslant x$. If $x \leqslant y$ and $y \leqslant x$, then $x = xy = yx = y$. If $x \leqslant y$ and $y \leqslant z$, then $xz = xyz = xy = x$, so $x \leqslant z$. Thus $\leqslant$ partially orders R.

For the characterization of ideals, note that (21) is equivalent to $x \in I \implies xz \in I$.

From (19), we get
$$x(x - 1) = 0,$$
so in every Boolean integral domain, the only elements are 0 and 1. In short, every Boolean integral domain is a field, so prime ideals of R are maximal. Moreover, an ideal I of R is maximal if and only if R/I is the disjoint union of two cosets, I and $1 + I$; this yields the characterization of maximal ideals. □

Corollary. *A subset M of $\mathscr{P}(\omega)$ is a maximal ideal if and only if*

(1) $x \in M \mathbin{\&} y \in M \implies x \cup y \in M$,
(2) $x \in M \mathbin{\&} y \subseteq x \implies y \in M$,
(3) $x \in M \iff \omega \smallsetminus x \notin M$.

A ***principal*** *ideal $\mathscr{P}(A)$ of $\mathscr{P}(\omega)$ is maximal if and only if $A = \omega \smallsetminus \{n\}$ for some n in ω. A maximal ideal of $\mathscr{P}(\omega)$ is non-principal if and only if it contains all finite subsets of ω.*

For example, if $n \in \omega$, then the principal ideal $(\omega \smallsetminus \{n\})$, namely $\{x \in \mathscr{P}(\omega) : n \notin x\}$, is a maximal ideal of $\mathscr{P}(\omega)$.

Theorem 36. *Let K be a field. The function $X \mapsto \operatorname{supp}[X]$ gives a one-to-one correspondence between the ideals of K^ω and the ideals of $\mathscr{P}(\omega)$.*

Proof. We have
$$\operatorname{supp}(x) \cap \operatorname{supp}(y) = \operatorname{supp}(xy),$$
$$\operatorname{supp}(x) \mathbin{\triangle} \operatorname{supp}(y) \subseteq \operatorname{supp}(x + y) \subseteq \operatorname{supp}(x) \cup \operatorname{supp}(y) = \operatorname{supp}(x) \mathbin{\triangle} \operatorname{supp}(y) \mathbin{\triangle} \operatorname{supp}(xy).$$
Since $x \mapsto \operatorname{supp}(x)$ is surjective onto $\mathscr{P}(\omega)$, we can conclude that I is an ideal of K^ω if and only if $\operatorname{supp}[I]$ is an ideal of $\mathscr{P}(\omega)$. Moreover, if I is an ideal of K^ω, and $a \in I$, and $\operatorname{supp}(b) \subseteq \operatorname{supp}(a)$, then $b \in I$, since $b = ca$, where
$$c_n = \begin{cases} {a_n}^{-1}, & \text{if } a_n \neq 0, \\ 0, & \text{if } a_n = 0. \end{cases}$$
In particular, $\operatorname{supp}^{-1}[\operatorname{supp}[I]] = I$; so $X \mapsto \operatorname{supp}[X]$ is injective on ideals. □

Suppose M is a maximal ideal of $\mathscr{P}(\omega)$. Then $\operatorname{supp}^{-1}[M]$ is a maximal ideal of K^ω; let us denote this ideal also by M. We can form the quotient
$$K^\omega/M,$$

which must be a field; it is called an **ultrapower** of K. The **diagonal map**

$$x \mapsto (x\colon n \in \omega) + M$$

is an embedding of K in K^ω/M; we shall identify K with its image in K^ω/M.

If a and b are in K^ω, and $a + M = b + M$, let us write also

$$a \equiv b \pmod{M}, \tag{22}$$

or simply $a \equiv b$. The elements of M (as an ideal of $\mathscr{P}(\omega)$) can be thought of as **small.** Then (22) holds if and only if the set $\{n \in \omega\colon a_n \neq b_n\}$ of indices where a and b differ is small. This definition makes no use of the algebraic structure of K. So K can be just a set, although in § 6 we shall be interested only in the case where K is the complete ordered field $\mathbb{R}$.

Theorem 37. *Let K be an infinite set, and M a maximal ideal of $\mathscr{P}(\omega)$. Then the diagonal embedding of K in K^ω/M is surjective if and only if M is principal.*

Proof. Suppose the element a of K^ω is injective, so that, if $m \neq n$, then $a_m \neq a_n$. Then $a + M$ is in the image of the diagonal embedding if and only if M is principal. □

We may henceforth assume that M is a non-principal maximal ideal of $\mathscr{P}(\omega)$, though we shall not actually use the assumption until § 6. We have a bijection

$$((x^0_k\colon k \in \omega), \dots, (x^{n-1}_k\colon k \in \omega)) \mapsto ((x^0_k, \dots, x^{n-1}_k)\colon k \in \omega)$$

from $(K^\omega)^n$ onto $(K^n)^\omega$; we may write the bijection more simply as

$$(x^0, \dots, x^{n-1}) \mapsto (\boldsymbol{x}_k\colon k \in \omega).$$

So a plainface x or x^j, with a superscript at most, is an element of K^ω or K, while a boldface $\boldsymbol{x}_k$, with a subscript at most, is an element of K^n; but x^j_k, with both superscripts and subscripts, is in K. Instead of writing

$$(x^0 + M, \dots, x^{n-1} + M),$$

we may write simply

$$(x^0, \dots, x^{n-1}) + M;$$

and instead of

$$x^0 \equiv y^0 \mathbin{\&} \cdots \mathbin{\&} x^{n-1} \equiv y^{n-1} \pmod{M},$$

we may write

$$(x^0, \dots, x^{n-1}) \equiv (y^0, \dots, y^{n-1}) \pmod{M}.$$

If $S \subseteq K^n$, we define

$${}^*S = \{(x^0, \dots, x^{n-1}) + M\colon (\boldsymbol{x}_k\colon k \in \omega) \in S^\omega\}. \tag{23}$$

Thus we have a function $X \mapsto {}^*X$ from $\mathscr{P}(K^n)$ to $\mathscr{P}({}^*K^n)$ for each n in ω. Also

$${}^*K = K^\omega/M. \tag{24}$$

Lemma. *Let $S \subseteq K^n$. Then*

$$(x^0, \dots, x^{n-1}) + M \in {}^*S \iff \{k \in \omega\colon \boldsymbol{x}_k \notin S\} \in M.$$

Proof. Suppose $(x^0, \dots, x^{n-1}) + M \in {}^*S$. There is $(y^0, \dots, y^{n-1})$ in $(K^\omega)^n$ such that $(x^0, \dots, x^{n-1}) \equiv (y^0, \dots, y^{n-1})$ and each $\boldsymbol{y}_k$ is in S. Then

$$\begin{aligned}\{k \in \omega \colon \boldsymbol{x}_k \notin S\} &\subseteq \{k \in \omega \colon x^0_k \neq y^0_k \vee \dots \vee x^{n-1}_k \neq y^{n-1}_k\}\\ &= \{k \in \omega \colon x^0_k \neq y^0_k\} \cup \dots \cup \{k \in \omega \colon x^{n-1}_k \neq y^{n-1}_k\}.\end{aligned}$$

Each of the sets $\{k \in \omega \colon x^j_k \neq y^j_k\}$ is in M, so their union is, and therefore $\{k \in \omega \colon \boldsymbol{x}_k \notin S\} \in M$, by the corollary to Theorem 35.

Now suppose conversely $\{k \in \omega \colon \boldsymbol{x}_k \notin S\} \in M$. Then in particular $S \neq \varnothing$. Pick some $\boldsymbol{y}$ in S, and define

$$\boldsymbol{z}_k = \begin{cases} \boldsymbol{x}_k, & \text{if } \boldsymbol{x}_k \in S,\\ \boldsymbol{y}, & \text{if } \boldsymbol{x}_k \notin S.\end{cases}$$

Then $(x^0, \dots, x^{n-1}) + M = (z_0, \dots, z^{n-1}) + M$, which is in ${}^*S$. □

Theorem 38. *Let K be a set, and let the functions $X \mapsto {}^*X$ from $\mathscr{P}(K^n)$ to $\mathscr{P}({}^*K^n)$ be as given in* (23). *Then*

$$^*\{(x, x) \colon x \in K\} = \{(x, x) \colon x \in {}^*K\}; \tag{25}$$

for all n in ω and all subsets S and T of K^n,

$$^*S \cap K^n = S, \tag{26}$$
$$^*(K^n \smallsetminus S) = {}^*K^n \smallsetminus {}^*S, \tag{27}$$
$$^*(S \cap T) = {}^*S \cap {}^*T; \tag{28}$$

for all m and n in ω, all f from m to n, and all subsets S of K^n and T of K^m,

$$^*(f^*[S]) = f^*[{}^*S], \tag{29}$$
$$^*(f_*(T)) = f_*({}^*T). \tag{30}$$

(More precisely, the last equations are $^*(f^*_K[S]) = f^*_{^*K}[{}^*S]$ and $^*(f^K_*(T)) = f^{*K}_*({}^*T)$.)

Proof. For (25), we have

$$\begin{aligned}(x, y) + M \in {}^*\{(x, x) \colon x \in K\} &\iff \{k \in \omega \colon x_k \neq y_k\} \in M\\ &\iff x + M = y + M.\end{aligned}$$

For (26), we easily have $S \subseteq {}^*S \cap K^n$. Suppose conversely $(x^0, \dots, x^{n-1}) + M \in {}^*S \cap K^n$. Then

$$\{k \in \omega \colon \boldsymbol{x}_k \notin S\} \in M,$$

and also, for some $\boldsymbol{y}$ in K^n, we have $\{k \in \omega \colon \boldsymbol{x}_k \neq \boldsymbol{y}\} \in M$. Since

$$\{k \in \omega \colon \boldsymbol{y} \notin S\} \subseteq \{k \in \omega \colon \boldsymbol{y} \neq \boldsymbol{x}_k \vee \boldsymbol{x}_k \notin S\} = \{k \in \omega \colon \boldsymbol{y} \neq \boldsymbol{x}_k\} \cup \{k \in \omega \colon \boldsymbol{x}_k \notin S\},$$

we can conclude $\{k \in \omega \colon \boldsymbol{y} \notin S\} \in M$. (In particular, the set must be empty.) Hence $\boldsymbol{y} \in S$, so $(x^0, \dots, x^{n-1}) + M \in S$.

For (27), we have

$$\begin{aligned}(x^0,\dots,x^{n-1})+M\in{}^*(K^n\smallsetminus S)&\iff\{k\in\omega\colon\boldsymbol{x}_k\notin K^n\smallsetminus S\}\in M\\&\iff\{k\in\omega\colon\boldsymbol{x}_k\notin S\}\notin M\\&\iff(x^0,\dots,x^{n-1})+M\notin{}^*S\\&\iff(x^0,\dots,x^{n-1})+M\in{}^*K^n\smallsetminus{}^*S.\end{aligned}$$

For (28), we have

$$\begin{aligned}(x^0,\dots,x^{n-1})+M\in{}^*(S\cap T)&\iff\{k\in\omega\colon\boldsymbol{x}_k\notin S\cap T\}\in M\\&\iff\{k\in\omega\colon\boldsymbol{x}_k\notin S\}\cup\{k\in\omega\colon\boldsymbol{x}_k\notin T\}\in M\\&\iff\{k\in\omega\colon\boldsymbol{x}_k\notin S\}\in M\mathbin{\&}\{k\in\omega\colon\boldsymbol{x}_k\notin T\}\in M\\&\iff(x^0,\dots,x^{n-1})+M\in{}^*S\mathbin{\&}\\&\qquad(x^0,\dots,x^{n-1})+M\in{}^*T\\&\iff(x^0,\dots,x^{n-1})+M\in{}^*S\cap{}^*T.\end{aligned}$$

For (29), we may assume $S\neq\varnothing$, since ${}^*\varnothing=\varnothing$. Let $(x^0,\dots,x^{n-1})\in(K^\omega)^m$. There is $(\boldsymbol{y}_k\colon k\in\omega)$ in S^ω such that, for all k in ω, if $\boldsymbol{x}_k\in f^*[S]$, then $\boldsymbol{x}_k=f^*(\boldsymbol{y}_k)$. Hence

$$\begin{aligned}(x^0,\dots,x^{m-1})+M\in{}^*(f^*[S])&\iff\{k\in\omega\colon\boldsymbol{x}_k\notin f^*[S]\}\in M\\&\iff\{k\in\omega\colon\boldsymbol{x}_k\neq f^*(\boldsymbol{y}_k)\}\in M\\&\iff(x^0,\dots,x^{m-1})+M=f^*(y^0+M,\dots,y^{n-1}+M)\\&\iff(x^0,\dots,x^{m-1})+M\in f^*[{}^*S].\end{aligned}$$

Finally, for (30), we have

$$\begin{aligned}&(x^0,\dots,x^{n-1})+M\in{}^*(f_*(T))\\\iff&\{k\in\omega\colon\boldsymbol{x}_k\notin f_*(T)\}\in M\\\iff&\{k\in\omega\colon f^*(\boldsymbol{x}_k)\notin T\}\in M\\\iff&\{k\in\omega\colon f^*(\boldsymbol{x}_k)\neq\boldsymbol{y}_k\}\in M\text{ for some }(\boldsymbol{y}_k\colon k\in\omega)\text{ in }T^\omega\\\iff&f^*(x^0+M,\dots,x^{m-1}+M)=(y^0,\dots,y^{n-1})+M\text{ for some }(\boldsymbol{y}_k\colon k\in\omega)\text{ in }T^\omega\\\iff&(x^0,\dots,x^{m-1})+M\in f_*({}^*T).\end{aligned}$$

□

5.2. **Logic.** It will follow from Theorem 38 that K and ${}^*K$ agree on *sentences* of *first-order logic.* This result is stated formally as Theorem 41, in § 6 below, for the case $K=\mathbb{R}$; but the general claim has the same proof, and the preliminary work done now will be in terms of an arbitrary set K.

If $S\subseteq K^n$, then S can be understood as a *name* for:

(1) itself, in K,
(2) ${}^*S$, in ${}^*K$.

We can express this more symbolically by

$$S^K=S,\qquad\qquad S^{{}^*K}={}^*S.$$

An **atomic formula** is a string

$$St^0 \cdots t^{n-1},$$

where $S \subseteq K^n$, and each t^k is either a variable or an element of ${}^*K$. In case $n = 2$, we customarily write

$$t^0 \; S \; t^1$$

instead of St^0t^1.

The **formulas,** simply, are defined recursively:

(1) atomic formulas are formulas,
(2) if ϕ is a formula, then so is the **negation** $\neg\phi$,
(3) if ϕ and ψ are formulas, then so is the **conjunction** $(\phi \mathbin{\&} \psi)$,
(4) if ϕ is a formula, and x is a variable, then so is the **instantiation**[8] $\exists x\ \phi$ is a formula.

The following is sometimes overlooked in expositions of logic; but it is needed to allow recursive definitions on the set of formulas.

Theorem 39 (Unique Readability)**.** *Every formula is* uniquely *an atomic formula, a negation, a conjunction. or an instantiation. Every conjunction is* $(\phi \mathbin{\&} \psi)$ *for some* unique *formulas* ϕ *and* ψ*.*

We can introduce the other customary symbols as abbreviations:

(1) $(\phi \Rightarrow \psi)$ means $\neg(\phi \mathbin{\&} \neg\psi)$,
(2) $(\phi \lor \psi)$ means $(\neg\phi \Rightarrow \psi)$,
(3) $(\phi \Leftrightarrow \psi)$ means $((\phi \Rightarrow \psi) \mathbin{\&} (\psi \Rightarrow \phi))$,
(4) $\forall x\ \phi$ means $\neg\exists x\ \neg\phi$.

Whether a variable is **free** in a formula is defined recursively:

(1) all variables in an atomic formula are free,
(2) the free variables of $\neg\phi$ are those of ϕ,
(3) the free variables of $(\phi \mathbin{\&} \psi)$ are those of ϕ or ψ,
(4) the free variables of $\exists x\ \phi$ are those of ϕ, except x.

If the free variables of a formula are all on the list $(x^0, \dots, x^{n-1})$, then the formula can be called n**-ary.** In this case, if $n \leqslant r$, then the formula is also r-ary. If we want to understand a formula ϕ *as* n-ary, we may write it as $\phi(x^0, \dots, x^{n-1})$.

Suppose t^k is in ${}^*K$ or is a variable for each k in ω. For each n-ary formula θ, a formula $\theta(t^0, \dots, t^{n-1})$ is defined. The definition is recursive:

(1) If θ is atomic, then $\theta(\boldsymbol{t})$ is the result of replacing each x^k with t^k.
(2) If θ is $\neg\phi$, then $\theta(\boldsymbol{t})$ is $\neg\psi$, where ψ is $\phi(\boldsymbol{t})$.
(3) If θ is $(\phi \mathbin{\&} \psi)$, then $\theta(\boldsymbol{t})$ is $(\phi(\boldsymbol{t}) \mathbin{\&} \psi(\boldsymbol{t}))$.
(4) If θ is $\exists x^\ell\ \phi$, then we can understand ϕ as r-ary, where $r = \max(\ell + 1, n)$. In this case, $\theta(\boldsymbol{t})$ is $\exists x^\ell\ \psi$, where ψ is $\phi(\boldsymbol{u})$, where

$$u^k = \begin{cases} x, & \text{if } k = \ell, \\ t^k, & \text{if } k \neq \ell. \end{cases}$$

[8] I don't know of a common term for formulas $\exists x\ \phi$; *instantiation* seems to work, though, since the formula will be interpreted as saying that ϕ is true for some *instance* of x.

The case $n = 0$ is not excluded; in this case, $\theta(t^0, \dots, t^{n-1})$ is simply θ.

The **parameters** of a formula are the (names of) elements of ${}^*K$ that appear in the formula. A **sentence** is a formula with no free variables, namely a 0-ary or **nullary** formula.

A sentence σ with parameters from K may be **true** in K, in which case we write

$$K \vDash \sigma;$$

otherwise σ is **false** in K, and we write

$$K \nvDash \sigma.$$

The definition is recursive:

(1) $K \vDash Sa^0 \cdots a^{n-1}$ if and only if $(a^0, \dots, a^{n-1}) \in S$.
(2) $K \vDash \neg\sigma$ if and only if $K \nvDash \sigma$.
(3) $K \vDash (\sigma \mathbin{\&} \tau)$ if and only if $K \vDash \sigma$ and $K \vDash \tau$.
(4) $K \vDash \exists x\ \phi$ if and only if, assuming ϕ is n-ary, there is $\boldsymbol{a}$ in K^n such that $K \vDash \phi(\boldsymbol{a})$.

All of the foregoing holds also with K replaced by ${}^*K$.

The definition of truth shows why formulas as we have defined them are more precisely called formulas of **first-order logic.** In our formulas, variables stand only for *elements* of K. If we allowed variables standing for *relations* on K, then our formulas would be *second order.* The third of the Peano axioms in § 2.1 is second order; so is the definition of completeness of an ordered field. In § 6 we shall note that there is no first-order definition of $\mathbb{N}$ or $\mathbb{R}$.

If $S = \{(x, x) \colon x \in K\}$, then, instead of $t^0\ S\ t^1$, we may write

$$t^0 = t^1.$$

Then $K \vDash a^0 = a^1$ if and only if $a^0 = a^1$; and likewise in ${}^*K$, by (26). An n-ary formula ϕ **defines** an n-ary relation on ${}^*K$, namely $\{\boldsymbol{a} \in {}^*K^n \colon {}^*K \vDash \phi(\boldsymbol{a})\}$; this relation can be denoted by

$$\phi^{{}^*K}.$$

In case σ is nullary, we have $\sigma^{{}^*K} = \{x \in \{0\} \colon {}^*K \vDash \sigma\}$, so that

$${}^*K \vDash \sigma \iff \sigma^{{}^*K} = 1.$$

If the parameters of a formula all come from K, then the formula similarly defines a relation on K, denoted by ϕ^K.

Theorem 40. *Let θ be a formula with parameters from K. Then*

$${}^*(\theta^K) = \theta^{{}^*K}.$$

Proof. Since formulas are defined recursively, we can argue inductively. The claim is true when θ is atomic, by (26). If the claim is true when θ is ϕ, then by (27)

$$\begin{aligned} {}^*((\neg\phi)^K) &= {}^*(K^n \smallsetminus \phi^K) \\ &= {}^*K^n \smallsetminus {}^*(\phi^K) \\ &= {}^*K^n \smallsetminus \phi^{{}^*K} \\ &= (\neg\phi)^{{}^*K}, \end{aligned}$$

so the claim is true when θ is $\neg\phi$. Similarly, if the claim is true when θ is ϕ or ψ, then by (28) the claim is true when θ is $(\phi \mathbin{\&} \psi)$.

For the final case, let us first note that, if the claim is true when θ is considered as m-ary, and $m \leqslant n$, then the claim is still true when θ is considered as n-ary. Indeed, let f be the inclusion of m in n. Then

$$\theta(x^0, \dots, x^{n-1})^K = \theta(x^0, \dots, x^{m-1})^K \times K^{n-m} = f_*^K(\theta(x^0, \dots, x^{m-1})^K),$$

and likewise with ${}^*K$ in place of K. Now use (30).

To finish then, we suppose the claim is true when θ is ϕ, and we prove the claim when θ is $\exists x^\ell\ \phi$. We may assume ϕ and $\exists x^\ell\ \phi$ are both n-ary, where $\ell < n$. Then we can understand $(x^0, \dots, x^{n-1})$ as $(\boldsymbol{x}, y, \boldsymbol{z})$, where $\boldsymbol{x}$ is $(x^0, \dots, x^{\ell-1})$, and y is x^ℓ, and $\boldsymbol{x}$ is $(x^{\ell+1}, \dots, x^{n-1})$. Then

$$\begin{aligned}(\exists x^\ell\ \phi)^K &= \{(\boldsymbol{a}, b, \boldsymbol{c}) \in K^n \colon K \vDash (\exists x^\ell\ \phi)(\boldsymbol{a}, b, \boldsymbol{c})\} \\ &= \{(\boldsymbol{a}, b, \boldsymbol{c}) \in K^n \colon K \vDash \exists x^\ell\ \phi(\boldsymbol{a}, x^\ell, \boldsymbol{c})\} \\ &= f_*^K(\{(\boldsymbol{a}, \boldsymbol{c}) \in K^{n-1} \colon K \vDash \exists x^\ell\ \phi(\boldsymbol{a}, x^\ell, \boldsymbol{c})\}),\end{aligned}$$

where f is the function from $n-1$ to n given by

$$f(k) = \begin{cases} k, & \text{if } k < \ell, \\ k+1, & \text{if } \ell \leqslant k < n-1. \end{cases}$$

We have also that $K \vDash \exists x^\ell\ \phi(\boldsymbol{a}, x^\ell, \boldsymbol{c})$ if and only if $K \vDash \phi(\boldsymbol{a}, b, \boldsymbol{c})$ for some b in K. Then

$$\{(\boldsymbol{a}, \boldsymbol{c}) \in K^{n-1} \colon K \vDash \exists x^\ell\ \phi(\boldsymbol{a}, x^\ell, \boldsymbol{c})\} = f_K^*[\phi^K].$$

Combining these results, we have

$$(\exists x^\ell\ \phi)^K = f_*^K(f_K^*[\phi^K]).$$

By (29) and (30) then, the claim holds when θ is $\exists x^\ell\ \phi$. Therefore it holds generally. □

Theorem 41. *Let σ be a sentence with parameters from K. Then*[9]

$$K \vDash \sigma \iff {}^*K \vDash \sigma.$$

Proof. When $n = 0$, then equation (26) is simply ${}^*S = S$. □

5.3. **Mock higher-order logic.** If we want our logic to be able to refer generally to subsets of a set, to functions on the set of functions on the set, and so forth, then we can proceed as follows. First, we recursively define **types** as certain strings:

(1) 0 is a type,
(2) if $n \in \omega \setminus \{0\}$, and $(t_0, \dots, \tau_{n-1})$ is a list of n types, then the string

$$n\tau_0 \cdots \tau_{n-1}$$

is a type.

Note that the type 0 is also a type of the form $n\tau_0 \cdots \tau_{n-1}$, where $n = 0$.

Theorem 42 (Unique Readability)**.** *Every type has the form $n\tau_0 \cdots \tau_{n-1}$ for some* unique *n in ω and some* unique *list* $(\tau_0, \dots, \tau_{n-1})$ *of types.*

---

[9]In model-theoretic terms, the full structure on K is an *elementary substructure* of the structure induced on ${}^*K$ by $X \mapsto {}^*X$.

Given a set K, we can now define

(1) $K_0 = K$,
(2) if τ is a type $n\tau_0 \cdots \tau_{n-1}$, where $n > 0$, then

$$K_\tau = \mathscr{P}(K_{\tau(0)} \times \cdots \times K_{\tau(n-1)}).$$

Here $\tau(j)$ is just τ_j, when used as a subscript itself. The first condition is not a special case of the second: if τ is not 0, then elements of K_τ are *relations;* but elements of K_0 are just elements of K. Letting T be the set of types, we define

$$\tilde{K} = \bigcup_{\tau \in T} K_\tau.$$

Letting M be a maximal ideal of $\mathscr{P}(\omega)$ as before, we have a special case of (24):

$${}^*(\tilde{K}) = \tilde{K}^\omega/M.$$

This introduces a potential ambiguity, since $K \subseteq \tilde{K}$, but ${}^*K$ is not literally a subset of ${}^*(\tilde{K})$. Since a relation S on K is also a relation on $\tilde{K}$, its image ${}^*S$ is either a relation on ${}^*K$ or on ${}^*(\tilde{K})$, but these two relations called ${}^*S$ are not generally the same. This problem is taken care of by the following.

Theorem 43. *${}^*K$ embeds in ${}^*(\tilde{K})$ under*

$$\{x \in K^\omega \colon x \equiv a\} \mapsto \{x \in \tilde{K}^\omega \colon x \equiv a\}.$$

Then an embedding i of $\mathscr{P}({}^*K^n)$ in $\mathscr{P}({}^*(\tilde{K})^n)$ is induced, and the following diagram commutes.

$$\begin{array}{ccc}
\mathscr{P}(K^n) & \xrightarrow{\ *\ } & \mathscr{P}({}^*K^n) \\
{\scriptstyle\subseteq}\Big\downarrow & & \Big\downarrow{\scriptstyle i} \\
\mathscr{P}(\tilde{K}^n) & \xrightarrow[\ *\ ]{} & \mathscr{P}({}^*(\tilde{K})^n)
\end{array}$$

In particular, if $S \subseteq K^n$, then

$$i({}^*S) = {}^*S,$$

where ${}^*S$ is computed in ${}^*K$ and ${}^*(\tilde{K})$ respectively.

Another ambiguity arises when we consider that some *elements* of $\tilde{K}$ are also *relations* on $\tilde{K}$. Indeed, every element S of $\tilde{K} \smallsetminus K_0$ is a relation on $\tilde{K}$, so it determines both the element $(S \colon k \in \omega) + M$ or S of ${}^*(\tilde{K})$ and the relation ${}^*S$ on ${}^*(\tilde{K})$, but these are not literally the same. This is taken care of by the following.

Theorem 44. *There is an embedding ι from the subset $\bigcup_{\tau \in T} {}^*(K_\tau)$ of ${}^*(\tilde{K})$ into $\widetilde{({}^*K)}$ such that*

(1) $\iota(x) = x$ when $x \in {}^*K$,
(2) $\iota(x) \in ({}^*K)_\tau$ when $x \in {}^*(K_\tau)$, and
(3) if $S \in \tilde{K} \smallsetminus K_0$, then

$$\iota(S) = \{(\iota(x^0), \dots, \iota(x^{n-1})) \colon \boldsymbol{x} \in {}^*S\}. \tag{31}$$

Proof. If τ is a type $n\tau_0\cdots\tau_{n-1}$, let

$$E_\tau = \{(\boldsymbol{x}, y) \in \tilde{K}^{n+1} \colon \boldsymbol{x} \in y \mathbin{\&} y \in K_\tau\}.$$

Then the sentence

$$\forall \boldsymbol{x}\ \forall y\ (E_\tau \boldsymbol{x} y \Rightarrow K_{\tau(0)} x^0 \mathbin{\&} \cdots \mathbin{\&} K_{\tau(n-1)} x^{n-1} \mathbin{\&} K_\tau y)$$

is true in $\tilde{K}$. By Theorem 41, it is true in ${}^*(\tilde{K})$. By Theorem 40,

$$(K_\tau x)^{{}^*(\tilde{K})} = {}^*(K_\tau).$$

Hence, if $S \in {}^*(K_\tau)$, then

$$(E_\tau \boldsymbol{x} S)^{{}^*(\tilde{K})} \subseteq {}^*(K_{\tau(0)}) \times \cdots \times {}^*(K_{\tau(n-1)}),$$

and the function that converts such S to $(E_\tau \boldsymbol{x} S)^{{}^*(\tilde{K})}$ is an embedding. We can now define ι recursively:

(1) $\iota(x) = x$ if $x \in {}^*(K_0)$,
(2) if $\tau = n\tau_0\cdots\tau_{n-1}$, and $R \in {}^*(K_\tau)$, then

$$\iota(R) = \{(\iota(a^0), \dots, \iota(a^{n-1})) \colon {}^*(\tilde{K}) \vDash E_\tau \boldsymbol{a} R\}. \tag{32}$$

By induction, ι maps ${}^*(K_\tau)$ into $({}^*K)_\tau$. Moreover, if again $\tau = n\tau_0\cdots\tau_{n-1}$, and $S \in K_\tau$, then the sentence

$$\forall \boldsymbol{x}\ (S\boldsymbol{x} \iff E_\tau \boldsymbol{x} S)$$

is true in $\tilde{K}$, so it is true in ${}^*(\tilde{K})$, which means in particular

$${}^*S = S^{{}^*(\tilde{K})} = (S\boldsymbol{x})^{{}^*(\tilde{K})} = (E_\tau \boldsymbol{x} S)^{{}^*(\tilde{K})}.$$

This and (32) establish (31). □

As we shall see in § 6, ι is not generally surjective. Also, even though every element of $\tilde{K}$ is an element of some K_τ, not every element of ${}^*(\tilde{K})$ is an element of some ${}^*(K_\tau)$.

6. Analysis

Let ${}^*\mathbb{R}$ be the ultrapower $\mathbb{R}^\omega/M$ of $\mathbb{R}$, where M is a *non-principal* maximal ideal of $\mathscr{P}(\omega)$. Then $\mathbb{R}$ embeds properly in ${}^*\mathbb{R}$, by Theorem 37. Everything we do now will be based on Theorem 41 in case $K = \mathbb{R}$ or $K = \tilde{\mathbb{R}}$.

If S is a relation on $\mathbb{R}$, then ${}^*S$ is a **standard** relation and is the **extension** of S. Also, elements of $\mathbb{R}^n$ are **standard.** Note then that a standard relation might have nonstandard elements.

Suppose $S \subseteq \mathbb{R}^n$, and f is a function from S to $\mathbb{R}$. Let

$$T = \{(\boldsymbol{x}, f(\boldsymbol{x}))\colon \boldsymbol{x} \in S\};$$

this is the **graph** of f. Then the sentences

$$\forall \boldsymbol{x}\ \exists y\ (S\boldsymbol{x} \Rightarrow T\boldsymbol{x}y),$$
$$\mathbb{R} \vDash \forall \boldsymbol{x}\ \forall y\ \forall z\ (S\boldsymbol{x}\ \&\ T\boldsymbol{x}y\ \&\ T\boldsymbol{x}z \Rightarrow y = z)),$$

are true in $\mathbb{R}$; by Theorem 40, they are true in ${}^*\mathbb{R}$. Therefore ${}^*T$ is the graph of a function from ${}^*S$ to ${}^*\mathbb{R}$. We may denote this function by

$${}^*f.$$

We have then

$${}^*f \restriction S = f. \tag{33}$$

In a formula, in place of $T\boldsymbol{x}y$, we may write

$$f(\boldsymbol{x}) = y.$$

Theorem 45. *${}^*\mathbb{R}$ is a non-Archimedean ordered field with respect to ${}^*{<}$, ${}^*{+}$, ${}^*{-}$, and ${}^*{\cdot}$, and $\mathbb{R}$ is an ordered subfield of ${}^*\mathbb{R}$.*

Proof. There is a first-order sentence σ saying that $\mathbb{R}$ is an ordered field; but then ${}^*\mathbb{R} \vDash \sigma$. By (26) and (33), $\mathbb{R}$ is an ordered subfield of ${}^*\mathbb{R}$. Since $\mathbb{R}$ is a *proper* subset of ${}^*\mathbb{R}$, the latter must be non-Archimedean. □

Corollary. *Being Archimedean is not a first-order property of fields.*

In the notation of the proof of Theorem 44, we have the sentence

$$\forall x\ (\exists y\ E_{10}yx\ \&\ \exists z\ \forall y\ (E_{10}yx \Rightarrow y \leqslant z) \Rightarrow$$
$$\exists w\ (\forall y\ (E_{10}yx \Rightarrow y \leqslant w)\ \&\ \forall z\ (\forall y\ (E_{10}yx \Rightarrow y \leqslant z) \Rightarrow w \leqslant z))),$$

which says in $\tilde{\mathbb{R}}$ that every subset x of $\mathbb{R}$ with an element y and an upper bound z has a least upper bound w. This is true, so the same sentence is true in ${}^*(\tilde{\mathbb{R}})$. But more precisely, in $\tilde{\mathbb{R}}$, the sentence is not about subsets of $\mathbb{R}$, but about elements of $\mathbb{R}_{10}$, which is $\mathscr{P}(\mathbb{R})$. In ${}^*(\tilde{\mathbb{R}})$, the sentence says that every element of ${}^*(\mathbb{R}_{10})$ with an upper bound has a least upper bound. We know that $\iota({}^*(\mathbb{R}_{10})) \subseteq ({}^*\mathbb{R})_{10}$, which is $\mathscr{P}({}^*\mathbb{R})$. Now we can conclude that the embedding is proper, not surjective.

Theorem 46. *$\mathbb{N}$ is a proper initial segment of ${}^*\mathbb{N}$. In particular, $\mathbb{N}$ consists of the finite elements of ${}^*\mathbb{N}$.*

Proof. For each n in $\mathbb{N}$, the sentence

$$\forall x\ (\mathbb{N}x \Rightarrow x = 0 \lor x = 1 \lor \cdots \lor x = n \lor x > n)$$

is true in $\mathbb{R}$, hence in ${}^*\mathbb{R}$, so that $\{0, 1, \ldots, n\}$ is an initial segment of ${}^*\mathbb{N}$. The sentence

$$\forall x\ \exists y\ (\mathbb{N}y \ \&\ x < y)$$

is true in $\mathbb{R}$ and hence in ${}^*\mathbb{R}$. In particular, let a be a positive infinite element of ${}^*\mathbb{R}$. Then there is n in ${}^*\mathbb{N}$ such that $a < n$. Such n must be infinite and so are not in $\mathbb{N}$. □

Corollary. *The Peano Axioms are not first order.*

Theorem 47. *A standard relation has nonstandard elements if and only if it is infinite.*

Proof. Suppose $S = \{\boldsymbol{a}_0, \ldots, \boldsymbol{a}_{n-1}\} \subseteq \mathbb{R}^m$. Then the sentence

$$\forall \boldsymbol{x}\ (S\boldsymbol{x} \Leftrightarrow \boldsymbol{x} = \boldsymbol{a}_0 \lor \cdots \lor \boldsymbol{a}_{n-1})$$

is true in $\mathbb{R}$ and ${}^*\mathbb{R}$, so ${}^*S = S$.

Now suppose f is an injective function from $\mathbb{N}$ into $\mathbb{R}$. Then ${}^*f$ is an injective function on ${}^*\mathbb{N}$. If ${}^*f(n)$ is an element a of $\mathbb{R}$ for some n in ${}^*\mathbb{N}$, then the sentence

$$\exists x\ (\mathbb{N}x \ \&\ f(x) = a)$$

is true in ${}^*\mathbb{R}$ and $\mathbb{R}$, so $n \in \mathbb{N}$. Thus, if $n \in {}^*\mathbb{N} \smallsetminus \mathbb{N}$, then ${}^*f(n) \in {}^*\mathbb{R} \smallsetminus \mathbb{R}$. □

6.1. Sequences.

Theorem 48. *Let a be a sequence $(a_n \colon n \in \mathbb{N})$ in $\mathbb{R}$. Then ${}^*a$ is a sequence $(a_n \colon n \in {}^*\mathbb{N})$ for some a_n in ${}^*\mathbb{R}$ (for n in ${}^*\mathbb{N} \smallsetminus \mathbb{N}$). Also a converges if and only if ${}^*a$ converges. If ${}^*a$ converges to b, then $b \in \mathbb{R}$.*

The following theorem can be understood as an alternative *definition* of convergence, if one does not want to bother with the traditional definition.

Theorem 49. *A standard sequence $(a_n \colon n \in {}^*\mathbb{N})$ converges to L if and only if, for all infinite n,*

$$a_n \simeq L.$$

Proof. Let a be the sequence, and suppose it converges to L. For every positive standard ε, there is a standard M such that the sentence

$$\forall x\ (\mathbb{N}x \ \&\ x \geqslant M \Rightarrow |a_n - L| < \varepsilon)$$

is true in $\mathbb{R}$ and ${}^*\mathbb{R}$. In particular, for every infinite n, we have $|a_n - L| < \varepsilon$ for every standard positive ε; but this just means $a_n \simeq L$.

Suppose a does not converge to L. Then there is some positive standard ε such that the sentence

$$\forall y\ \exists x\ (\mathbb{N}x \ \&\ x \geqslant y \ \&\ |a_n - L| \geqslant \varepsilon)$$

is true in $\mathbb{R}$ and ${}^*\mathbb{R}$. In particular, if M is infinite, then there is some n in ${}^*\mathbb{N}$ that is greater than M (and therefore infinite) such that $|a_n - L| \geqslant \varepsilon$. □

For example, $\lim_{n\to\infty} 1/n = 0$, simply because $1/n$ is infinitesimal when n is infinite.

Theorem 50. *Let a and b be standard convergent sequences, and $r \in \mathbb{R}$. Then*

$$\lim(a+b) = \lim(a) + \lim(b), \tag{34}$$

$$\lim(ra) = r\lim(a), \tag{35}$$

$$\lim(ab) = \lim(a)\lim(b). \tag{36}$$

Proof. Let R be the ring of finite members of ${}^*\mathbb{R}$, and let I be its ideal of infinitesimals. Suppose $a_n \simeq L$ and $b_n \simeq M$. Then $a_n - L$ and $b_n - M$ are in I, hence so are $(a_n + b_n) - (L + M)$ and $ra_n - rL$. This shows (34) and (35). For (36), note

$$|a_n b_n - LM| = |a_n b_n - a_n M + a_n M - LM| \leqslant |a_n|\,|b_n - M| + |a_n - L|\,|M|\,.$$

But the last is in I since $|a_n|$ and $|M|$ are in R (why?). □

Theorem 51. *A standard sequence is bounded if and only if every term is finite.*

Proof. That a is bounded means that, for some M, the sentence

$$\forall x\ (x \in \mathbb{N} \Rightarrow |a_x| < M)$$

is true in $\mathbb{R}$; then it is true in ${}^*\mathbb{R}$, so every entry in ${}^*a$ is bounded by M, hence finite.

Suppose a is unbounded. Then the sentence

$$\forall x\ \exists y\ (y \in \mathbb{N}\ \&\ |a_y| > x$$

is true in $\mathbb{R}$, hence in ${}^*\mathbb{R}$. Let L be positive and infinite; then there is n in ${}^*\mathbb{N}$ such that $|a_n| > L$. □

Compare the following with Theorem 27.

Theorem 52. *A standard sequence (a_n) converges if and only if, for all infinite m and n,*

$$a_m \simeq a_n.$$

Proof. If (a_n) converges to L, then $a \simeq L$ for all infinite n, and therefore $a_m \simeq a_n$ for all infinite m and n, since $\simeq$ is an equivalence relation.

Suppose conversely $a_m \simeq a_n$ for all infinite m and n. If each a_n is *finite*, and n is in particular infinite, then (a_n) converges to the standard part of a_n. Suppose some a_n is infinite. Then by Theorem 51, the sequence $(a_n \colon n \in \mathbb{N})$ is unbounded. Hence the sentence

$$\forall x\ \exists y\ (x \in \mathbb{N} \Rightarrow y \in N\ \&\ x \leqslant y\ \&\ |a_x| + 1 \leqslant |a_y|)$$

is true in $\mathbb{R}$ and ${}^*\mathbb{R}$, so a_m and a_n fail to be infinitely close for some infinite m and n. □

Traditionally, L is a **limit point** of (a_n) if for all positive ε and for all m in $\mathbb{N}$, there is n such that $m < n$ and $|L - a_n| < \varepsilon$. The following can be used as an alternative definition.

Theorem 53. *A finite number L is a limit point of the standard sequence (a_n) if and only if, for some infinite n,*

$$a_n \simeq L.$$

Proof. If L is a limit point of (a_n), then the sentence

$$\forall x\ \forall y\ \exists z\ (x > 0\ \&\ y \in \mathbb{N} \Rightarrow z \in N\ \&\ y < z\ \&\ |L - a_z| < x)$$

is true in $\mathbb{R}$ and ${}^*\mathbb{R}$, so for an infinitesimal ε there is an infinite n such that $|L - a_n| < \varepsilon$ and hence $a_n \simeq L$.

Suppose L is not a limit point of (a_n). Then there is some positive ε and some n in $\mathbb{N}$ such that the sentence

$$\forall x\ (x \in \mathbb{N} \Rightarrow |L - a_x| \geqslant \varepsilon)$$

is true in $\mathbb{R}$ and ${}^*\mathbb{R}$. This means $|L - a_n| \geqslant \varepsilon$ whenever n is infinite. □

The non-standard proof of the following should be compared with the traditional divide-and-conquer proof.

Theorem 54 (Bolzano–Weierstraß)**.** *Every bounded standard sequence has a limit point.*

Proof. Indeed, by Theorem 51, if (a_n) is bounded, then each a_n has a standard part when n is infinite, and that standard part is a limit point of the sequence by Theorem 53. □

6.2. **Continuity.** Suppose now f is a standard function defined on an interval $[a, b]$. If $c \in [a, b]$, we say, classically, that

$$\lim_{x \to c} f(x) = \lim_c(f) = L$$

if for all positive ε there is a positive δ such that, for all x in $[a, b]$,

$$0 < |x - c| < \delta \implies |L - f(x)| < \varepsilon.$$

Theorem 55. *If f is a standard function defined on an interval I that contains c, then $\lim_c f = L$ if and only if, for all x in I that are distinct from c,*

$$x \simeq c \implies f(x) \simeq L.$$

Theorem 56. *If $\lim_c f$ and $\lim_c g$ exist, then*

$$\lim_c(f + g) = \lim_c(f) + \lim_c(g),$$
$$\lim_c(fg) = \lim_c(f)\lim_c(g);$$

if also $\lim_c(f) \neq 0$, then

$$\lim_c \left(\frac{1}{f}\right) = \frac{1}{\lim_c(f)}. \tag{37}$$

Proof. For (37), if $f(x) \simeq L$, and $L \neq 0$, then $|f(x)| > |L|/2$, so that

$$\left|\frac{1}{f(x)} - \frac{1}{L}\right| = \frac{|L - f(x)|}{|f(x)L|} < \frac{2}{L^2}|L - f(x)| \simeq 0.$$ □

The function f is **continuous at** c, if $\lim_c(f) = f(c)$; **continuous on** $[a, b]$, if continuous at every point of $[a, b]$.

Theorem 57 (Intermediate Value)**.** *If f is continuous on $[a, b]$, and d lies between $f(a)$ and $f(b)$, then for some c in (a, b),*

$$f(c) = d.$$

Proof. Suppose $f(a) < d < f(b)$. In $\mathbb{R}$, for all n in $\mathbb{N}^+$, there is some *least* j in $\mathbb{N}$ such that
$$f(a + \frac{j}{n}(b-a)) < d \leqslant f(a + \frac{j+1}{n}(b-a)). \tag{38}$$
Then the same is true in ${}^*\mathbb{R}$, with ${}^*\mathbb{N}$ replacing $\mathbb{N}$. In particular, we have (38) for some j in ${}^*\mathbb{N}$, where n is in ${}^*\mathbb{N} \smallsetminus {}^*\mathbb{N}$. Let c be the standard part of $a + (j/n)(b-a)$. Then
$$f(a + \frac{j}{n}(b-a)) \simeq f(c) \simeq f(a + \frac{j+1}{n}(b-a)).$$
Therefore $f(c) = d$. □

Theorem 58 (Extreme Value)**.** *If f is continuous on $[a,b]$, then it attains a maximum and minimum value on the interval.*

Proof. For all positive natural numbers n, for some natural number j such that $j \leqslant n$, the value of
$$f(a + \frac{j}{n}(b-a))$$
is maximized. In particular, this is so when n is infinite. If $i \leqslant n$, we now have
$$f(a + \frac{i}{n}(b-a)) \leqslant f(a + \frac{j}{n}(b-a)).$$
Let d be the standard part of $a + (j/n)(b-a)$. For every c in $[a,b]$, there is a natural number i such that
$$a + \frac{i}{n}(b-a) \leqslant c < a + \frac{i+1}{n}(b-a).$$
Then these three numbers are infinitely close, so
$$f(c) \simeq f(a + \frac{i}{n}(b-a)).$$
Therefore $f(c) \leqslant f(d)$. □

6.3. **Derivatives.** If
$$\lim_{x\to c} \frac{f(x) - f(c)}{x - c} = d,$$
then we write
$$f'(c) = d,$$
saying f is **differentiable** at c, with **derivative** d at c. So $f'(c) = d$ if and only if, whenever $c \simeq c$ but $x \neq c$, we have
$$\frac{f(x) - f(c)}{x - c} \simeq d.$$

Theorem 59. *If f is differentiable at c, then it is continuous at c.*

Proof. If f is differentiable at c and $x \simeq c$, then
$$f(x) - f(c) \simeq (x-c)f'(c) \simeq 0;$$
so f is continuous at c. □

Theorem 60. *If f and g are differentiable at c, then so are $f + g$ and fg, and*
$$(f+g)'(c) = f'(c) + g'(c), \qquad (fg)'(c) = f'(c)g(c) + f(c)g'(c).$$

Proof. If $x \simeq c$, then

$$\frac{(fg)(x) - (fg)(c)}{x - c} = \frac{f(x) - f(c)}{x - c} g(c) + f(x) \frac{g(x) - g(c)}{x - c} \simeq f'(c)g(c) + f(c)g'(c). \quad \square$$

The standard function f has a **local maximum** at c if, for some positive δ, the function f is defined on $(c - \delta, c + \delta)$ and on this interval is maximized at c.

Theorem 61. *A standard function f has a local maximum at c if and only if f is defined on $\{x : x \simeq c\}$ and on this interval is maximized at c.*

Proof. Necessity of the condition is immediate. To prove sufficiency, suppose f does not have a local maximum at c. Then for every positive δ, and in particular for δ that are infinitely close to c, either f is not defined on $(c - \delta, c + \delta)$, or else f is not maximized there at c. But that interval is a subset of $\{x : x \simeq c\}$. $\square$

Theorem 62. *If f has a local maximum and is differentiable at c, then $f'(c) = 0$.*

Proof. We assume that, if $x \simeq c$, but $x \neq c$, then $f(x) \leqslant c$, so

$$\frac{f(x) - f(c)}{x - c} \begin{cases} \geqslant 0, & \text{if } x < c, \\ \leqslant 0, & \text{if } x > c. \end{cases}$$

Since $(f(x) - f(c))/(x - c) \simeq f'(c)$, we can conclude that $f'(c) = 0$. $\square$

Theorem 63 (Rolle)**.** *If f is continuous on $[a, b]$ and differentiable on (a, b), and $f(a) = f(b)$, then, for some c in (a, b),*

$$f'(c) = 0.$$

Proof. Theorems 58 and 62. $\square$

6.4. **Integrals.** Classically, the integral of a bounded function f on an interval $[a, b]$ can be defined as follows. Suppose I is a number such that, for all positive ε, there is a positive δ such that, for all positive integers n, for all lists $(a_0, \dots, a_n)$ and $(\xi_1, \dots, \xi_n)$ of numbers such that

$$a = a_0 \leqslant \xi_1 \leqslant a_1 \leqslant \dots \leqslant a_{n-1} \leqslant \xi_n \leqslant a_n = b \tag{39}$$

and also

$$\min(a_1 - a_0, \dots, a_n - a_{n-1}) \leqslant \delta,$$

we have

$$\left| I - \sum_{i=1}^{n} f(\xi_i)(a_i - a_{i-1}) \right| < \varepsilon.$$

Then f is **integrable** on $[a, b]$, and

$$\int_a^b f = I.$$

This is not a first-order statement in $\mathbb{R}$, so we move to $\tilde{\mathbb{R}}$. Let $A_{[a,b]}$ be the set of finite sequences $(a_0, \xi_1, a_1, \dots, x_n, a_n)$ with entries from $\mathbb{R}$, where $n \in \mathbb{N}$ and (39) holds. Such sequences can be understood as binary relations on $\mathbb{R}$, so that $A_{[a,b]} \in \mathbb{R}_{200}$. If f is a bounded function on $[a,b]$, let $S_{f,a,b}$ be the function

$$(a_0, \xi_1, a_1, \dots, \xi_n, a_n) \mapsto \sum_{i=1}^{n} f(\xi_i)(a_i - a_{i-1})$$

on A. So $S_{f,a,b} \in \mathbb{R}_{22000}$. An element of ${}^*A_{[a,b]}$ also takes the form $(a_0, \xi_1, a_1, \dots, \xi_n, a_n)$, where again (39) holds; but now $n \in {}^*\mathbb{N}$. Such an element can be called **fine** if $a_{i-1} \simeq a_i$ for each i in $\{1, \dots, n\}$. It must be noted that fine elements of ${}^*A$ do exist: for example,

$$(a, a + \frac{1}{n}(b-a), a + \frac{1}{n}(b-a), \dots, a + \frac{n-1}{n}(b-a), a + \frac{n-1}{n}(b-a)),$$

where n is infinite.

Theorem 64. *Given a bounded function f on $[a,b]$, Then f is integrable on $[a,b]$ if and only if, for any two fine elements a and a' of ${}^*A_{[a,b]}$,*

$${}^*S_{f,a,b}(a) \simeq {}^*S_{f,a,b}(a').$$

In this case, $\int_a^b f$ is the standard part of either of these sums.

Theorem 65 (Fundamental, of Calculus)**.** *Suppose f is continuous on $[a,b]$. If $a \leqslant c \leqslant b$, then f is integrable on $[a,c]$. The function*

$$x \mapsto \int_a^x f$$

is differentiable on $[a,b]$, and its derivative is f.

Appendix A. The Greek alphabet

capital	minuscule	transliteration	name
A	α	a	alpha
B	β	b	beta
Γ	γ	g	gamma
Δ	δ	d	delta
E	ϵ	e	epsilon
Z	ζ	z	zeta
H	η	ê	eta
Θ	θ	th	theta
I	ι	i	iota
K	κ	k	kappa
Λ	λ	l	lambda
M	μ	m	mu
N	ν	n	nu
Ξ	ξ	x	xi
O	o	o	omicron
Π	π	p	pi
P	ρ	r	rho
Σ	σ, ς	s	sigma
T	τ	t	tau
Υ	υ	y, u	upsilon
Φ	ϕ	ph	phi
X	χ	ch	chi
Ψ	ψ	ps	psi
Ω	ω	ô	omega

The following remarks pertain to *ancient* Greek. The vowels are α, ε, η, ι, ο, υ, ω, where η is a long ε, and ω is a long ο; the other vowels (α, ι, υ) can be long or short. Some vowels may be given tonal accents (ά, ᾶ, ὰ). An initial vowel takes either a rough-breathing mark (as in ἁ) or a smooth-breathing mark (ἀ): the former mark is transliterated by a preceding h, and the latter can be ignored, as in ὑπερβολή hyperbolê *hyperbola,* ὀρθογώνιον orthogônion *rectangle.* Likewise, ῥ is transliterated as rh, as in ῥόμβος rhombos *rhombus.* A long vowel may have an iota subscript (ᾳ, ῃ, ῳ), especially in case-endings of nouns. Of the two forms of minuscule sigma, the ς appears at the ends of words; elsewhere, σ appears, as in βάσις basis *base.*

Appendix B. The German script

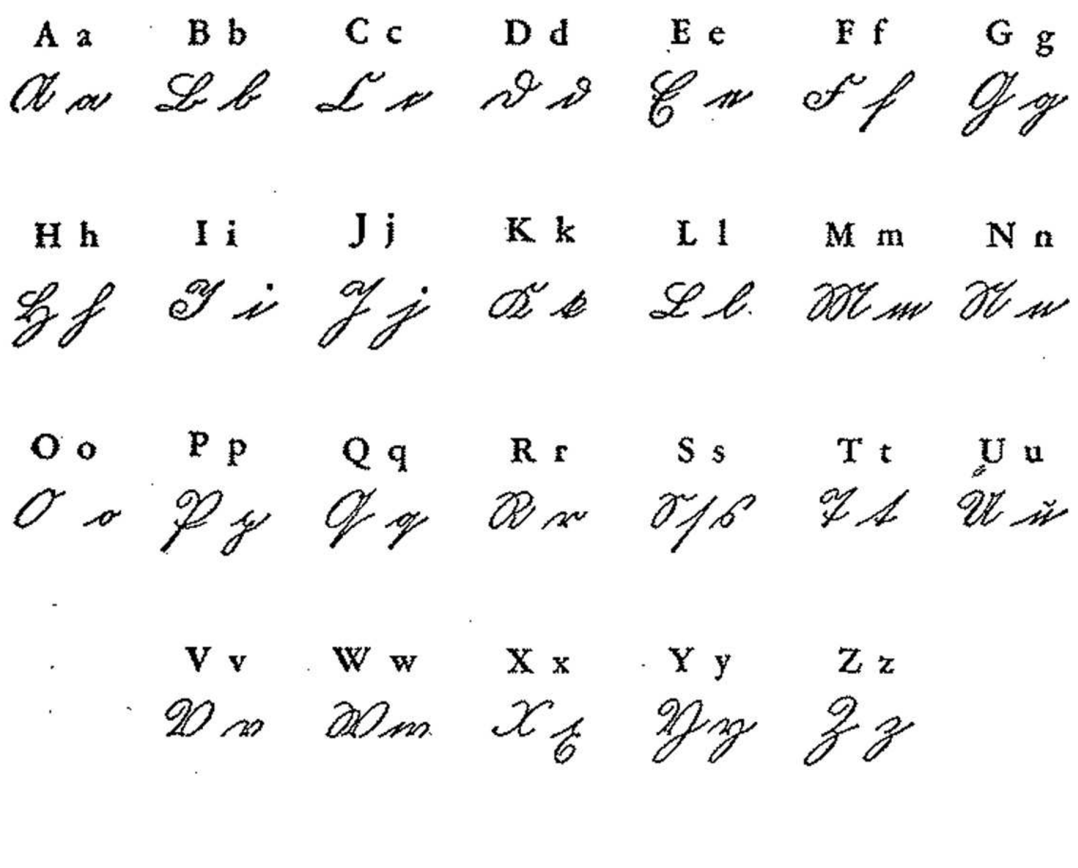
Writing in 1993, Wilfrid Hodges [8, Ch. 1, p. 21] observes

> Until about a dozen years ago, most model theorists named structures in horrible Fraktur lettering. Recent writers sometimes adopt a notation according to which all structures are named M, M', M^*, $\bar{M}$, M_0, M_i or occasionally N.

For Hodges, structures are A, B, C, and so forth; he refers to their universes as **domains** and denotes these by $\mathrm{dom}(A)$ and so forth. This practice is convenient if one is using a typewriter (as in the preparation of another of Hodges's books [9], from 1985). In 2002, David Marker [11] uses 'calligraphic' letters for structures, so that M is the universe of $\mathcal{M}$. I still prefer the Fraktur letters:

$$\begin{array}{ccccccccc} \mathfrak{A} & \mathfrak{B} & \mathfrak{C} & \mathfrak{D} & \mathfrak{E} & \mathfrak{F} & \mathfrak{G} & \mathfrak{H} & \mathfrak{I} \\ \mathfrak{J} & \mathfrak{K} & \mathfrak{L} & \mathfrak{M} & \mathfrak{N} & \mathfrak{O} & \mathfrak{P} & \mathfrak{Q} & \mathfrak{R} \\ \mathfrak{S} & \mathfrak{T} & \mathfrak{U} & \mathfrak{V} & \mathfrak{W} & \mathfrak{X} & \mathfrak{Y} & \mathfrak{Z} & \end{array} \qquad \begin{array}{ccccccccc} \mathfrak{a} & \mathfrak{b} & \mathfrak{c} & \mathfrak{d} & \mathfrak{e} & \mathfrak{f} & \mathfrak{g} & \mathfrak{h} & \mathfrak{i} \\ \mathfrak{j} & \mathfrak{k} & \mathfrak{l} & \mathfrak{m} & \mathfrak{n} & \mathfrak{o} & \mathfrak{p} & \mathfrak{q} & \mathfrak{r} \\ \mathfrak{s} & \mathfrak{t} & \mathfrak{u} & \mathfrak{v} & \mathfrak{w} & \mathfrak{x} & \mathfrak{y} & \mathfrak{z} & \end{array}$$

A way to write these by hand is seen in a textbook of German from 1931 [7]:



References

1. Apollonius of Perga, *Conics. Books I–III*, revised ed., Green Lion Press, Santa Fe, NM, 1998, Translated and with a note and an appendix by R. Catesby Taliaferro, With a preface by Dana Densmore and William H. Donahue, an introduction by Harvey Flaumenhaft, and diagrams by Donahue, Edited by Densmore. MR MR1660991 (2000d:01005)
2. Archimedes, *The works of Archimedes*, Dover Publications Inc., Mineola, NY, 2002, Reprint of the 1897 edition and the 1912 supplement, Edited by T. L. Heath. MR MR2000800 (2005a:01003)
3. ———, *The works of Archimedes. Vol. I*, Cambridge University Press, Cambridge, 2004, The two books on the sphere and the cylinder, Translated into English, together with Eutocius' commentaries, with commentary, and critical edition of the diagrams by Reviel Netz. MR MR2093668 (2005g:01006)
4. Richard Dedekind, *Essays on the theory of numbers. I: Continuity and irrational numbers. II: The nature and meaning of numbers*, authorized translation by Wooster Woodruff Beman, Dover Publications Inc., New York, 1963. MR MR0159773 (28 #2989)
5. Euclid, *The thirteen books of Euclid's Elements translated from the text of Heiberg. Vol. I: Introduction and Books I, II. Vol. II: Books III–IX. Vol. III: Books X–XIII and Appendix*, Dover Publications Inc., New York, 1956, Translated with introduction and commentary by Thomas L. Heath, 2nd ed. MR 17,814b
6. ———, *Euclid's Elements*, Green Lion Press, Santa Fe, NM, 2002, All thirteen books complete in one volume, the Thomas L. Heath translation, edited by Dana Densmore. MR MR1932864 (2003j:01044)
7. Roe-Merrill S. Heffner, *Brief German grammar*, D. C. Heath and Company, Boston, 1931.
8. Wilfrid Hodges, *Model theory*, Encyclopedia of Mathematics and its Applications, vol. 42, Cambridge University Press, Cambridge, 1993. MR 94e:03002
9. ———, *Building models by games*, Dover Publications, Mineola, New York, 2006, original publication, 1985. MR MR812274 (87h:03045)
10. Edmund Landau, *Foundations of analysis. The arithmetic of whole, rational, irrational and complex numbers*, third ed., Chelsea Publishing Company, New York, N.Y., 1966, translated by F. Steinhardt; first edition 1951; first German publication, 1929. MR 12,397m
11. David Marker, *Model theory: an introduction*, Graduate Texts in Mathematics, vol. 217, Springer-Verlag, New York, 2002. MR 1 924 282
12. Giuseppe Peano, *The principles of arithmetic, presented by a new method (1889)*, From Frege to Gödel (Jean van Heijenoort, ed.), Harvard University Press, 1976, pp. 83–97.
13. Abraham Robinson, *Non-standard analysis*, Princeton Landmarks in Mathematics, Princeton University Press, Princeton, NJ, 1996, Reprint of the second (1974) edition, With a foreword by Wilhelmus A. J. Luxemburg. MR MR1373196 (96j:03090)
14. Michael Spivak, *Calculus*, 2nd ed., Publish or Perish, Berkeley, California, 1980.
15. Ivor Thomas (ed.), *Selections illustrating the history of Greek mathematics. Vol. II. From Aristarchus to Pappus*, Harvard University Press, Cambridge, Mass, 1951, With an English translation by the editor. MR 13,419b

Mathematics Department, Middle East Technical University, Ankara 06531, Turkey
URL: `arf.math.metu.edu.tr/~dpierce/`
E-mail address: `dpierce@metu.edu.tr`