Appendix A

Set-Theoretic Reconstruction of Number Systems

In this appendix we represent the structures of the natural numbers, the integers, and the rationals in pure set-theoretic terms. This set-theoretic representation of numbers gives us first of all a good impression of the power of set theory in representing other structures or mathematical systems. To represent a number structure in pure set-theoretic terms means to define its primitives, operations and relations in set-theoretic terms only. To define the notion number in terms of sets may seem strange at first, since we are so much more familiar with numbers than with sets. The set-theoretic representation of numbers is in fact quite artificial and and the one given here is also not the only conceivable one. It is sufficiently cumbersome that it is never used in practice for ordinary manipulation of numbers. So its function is purely theoretical: it is a necessary step in establishing the interesting claim that set theory is the universal foundation of all of mathematics.

A.1 The natural numbers

First we define 0 as the empty set:

$$0 =_{def} \emptyset$$

Then for the number 1 let us find a set with exactly one member which is built from sets already constructed, i.e. built from $\emptyset$. Such a set is $\{\emptyset\}$. So we define

$$1 =_{def} \{\emptyset\}$$

As a result of these two definitions we see that

$$1 = \{0\}$$

We continue in the same way

$$2 =_{def} \{\emptyset, \{\emptyset\}\} = \{0, 1\}$$

$$3 =_{def} \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} = \{0, 1, 2\}$$

We can proceed indefinitely in this way, defining each successive number as the set of all its predecessors. This can be expressed formally in either of two ways:

for all n (i) $n + 1 = \{0, 1, 2, \ldots, n\}$
or (ii) $n + 1 = n \cup \{n\}$

Given any set of finite elements of any sort, the way to tell how many elements it has is to compare it with each of these 'number' sets in turn until one is found whose members can be put in a one-to-one correspondence with the members of the set in question. An analogy can be drawn to the method of telling that something is a meter long by comparing it to the standard meter, a physical object preserved in Paris.

Each natural number has a unique representation in our scheme, but it remains to be shown that the numbers, as reconstructed, have the properties that we expect them to have. In particular, our reconstruction should exhibit the required behavior in relations such as equality and greater-than, and under operations such as addition and multiplication.

The notion of a *successor* of a natural number is defined as:

$$\text{successor of } x =_{def} x \cup \{x\}.$$

We indicate the successor of x by $s(x)$.

Equality between natural numbers is defined as set equality, i.e., having identical membership. Thus, 5 and $s(4)$ are the same number, each being $\{0, 1, 2, 3, 4\}$.

The linear *order* 'less than' is defined by set inclusion: $x < y$ iff $x \subset y$; also, $x \leq y$, 'less than or equal to,' iff $x \subseteq y$, and similarly for $x > y$ and $x \geq y$.

Addition can be defined by a pair of rules using the notion of successor:

for all x (i) $x + 0 = x$
(ii) $x + s(n) = s(x + n)$

For example, to add two numbers, the second part of the definition is repeated until the first part becomes applicable The steps for $4 + 3$ are:

$$
\begin{aligned}
4+3 &= 4+s(2) && \text{def. successor}\\
&= s(4+2) && \text{def. addition}\\
&= s(4+s(1)) && \text{def. successor}\\
&= s(s(4+1)) && \text{def. addition}\\
&= s(s(4+s(0))) && \text{def. successor}\\
&= s(s(s(4+0))) && \text{def. addition}\\
&= s(s(s(4))) && \text{def. addition}\\
&= s(s(5)) && \text{def. successor}\\
&= s(6) && \text{def. successor}\\
&= 7 && \text{def. successor}
\end{aligned}
$$

Subtraction can also be defined by a pair of rules, but it is only defined when a set is being subtracted from one which contains it:

for all x (i) $x - x = 0$
(ii) $s(x) - n = s(x - n)$

For example,

$$
\begin{aligned}
4-2 &= s(3)-2 && \text{def. of successor}\\
&= s(3-2) && \text{def. of subtraction}\\
&= s(s(2)-2) && \text{def. of successor}\\
&= s(s(2-2)) && \text{def. of subtraction}\\
&= s(s(0)) && \text{def. of subtraction}\\
&= s(1) && \text{def. of successor}\\
&= 2 && \text{def. of successor}
\end{aligned}
$$

Multiplication can be defined by a pair of rules involving addition, which has been already defined:

for all x (i) $x \cdot 1 = x$
(ii) $x \cdot s(n) = (x \cdot n) + x$

For example,

$$
\begin{aligned}
2 \cdot 3 &= 2 \cdot s(2) && \text{def. of successor} \\
&= 2 \cdot 2 + 2 && \text{def. of multiplication} \\
&= 2 \cdot s(1) + 2 && \text{def. of successor} \\
&= (2 \cdot 1 + 2) + 2 && \text{def. of multiplication} \\
&= (2 + 2) + 2 && \text{def. of multiplication} \\
&= 4 + 2 = 6 && \text{by addition, as previously defined}
\end{aligned}
$$

A.2 Extension to the set of all integers

Mathematicians (and scientists in general) strive to develop concepts with as wide a range of application as possible. Looking at the system above, one detects a gap: the concepts of equality, addition and multiplication are defined for any two natural numbers, but subtraction is not. It would desirable to extend the number system so as to have subtraction defined everywhere.

What does it mean to 'extend' a system? It means to create a new system with additional elements and possibly additional operations or relations in such a way that the new system contains a *subsystem which is isomorphic to the old system.* In other words, there is some subset of the elements, operations and relations of the new system which can be put in one-to-one correspondence with the elements, operations and relations of the old system, so that the corresponding operations on corresponding elements yield corresponding elements, and the corresponding relations contain corresponding ordered pairs of elements. This guarantees in effect that nothing of the old system has been lost in constructing the new one.

In this case, where we are concerned with an operation, subtraction, which is not defined on certain elements, we would much prefer, for purposes of conceptual economy, that the operation in the new system be given a single definition on all the elements. We will construct a new number system in which subtraction has a uniform definition on all elements, and which contains a subsystem which is isomorphic to the original system. The new number structure is called the *integers*. Remember that the set-theoretic representation of number structures is not in any sense a definition of what the numbers are in absolute terms, but rather of how they can be represented by set-theoretic constructions or *re*-constructions.

The representation of the integers does not bear any resemblance to the ordinary integers $\ldots -2, -1, 0, 1, 2, \ldots$. They are here defined in a special way so that the operations and relations on them can be defined in terms of the operations and relations already defined for the natural numbers.

DEFINITION A 1 *An integer is an ordered pair* $\langle a, b\rangle$ *of natural numbers.* ■

(Intuitively, the ordered pair $\langle a, b\rangle$ will correspond to the integer which is the difference $a - b$; i.e., $\langle 5, 3\rangle$ represents 2; $\langle 2, 4\rangle$ represents -2. Thus, many oredered pairs represent the same integer.)

Equality: $\langle a, b\rangle = \langle c, d\rangle$ if and only if $a + d = c + b$, using the definition of $+$ for the natural numbers. Note first that equality is an equivalence relation in the new system. Note also that under this definition $\langle a, b\rangle = \langle a + k, b + k\rangle$ for any k. Hence,

$$\begin{aligned} \langle 7,3\rangle &= \langle 6,2\rangle = \langle 5,1\rangle = \langle 4,0\rangle \\ \langle 3,7\rangle &= \langle 2,6\rangle = \langle 1,5\rangle = \langle 0,4\rangle \\ \langle 3,3\rangle &= \langle 2,2\rangle = \langle 1,1\rangle = \langle 0,0\rangle \end{aligned}$$

Every integer is therefore equal to some integer of one of these three forms:

1. $\langle a - b, 0\rangle$
2. $\langle 0, a - b\rangle$
3. $\langle 0, 0\rangle$

where a and b are natural numbers and '$-$' is as defined for the natural numbers. By convention, all integers equal to some integer of the first type will be called *positive integers*, the second type *negative integers* and the third type *zero*.

Ordering 'greater than': $\langle a, b\rangle > \langle c, d\rangle$ if and only if $a + d > c + b$ where $>$ on the right is the relation 'greater than' defined on the natural numbers. For example, $\langle 6, 3\rangle > \langle 2, 1\rangle$ (i.e., $3 > 1$) because $(6 + 1) > (2 + 3)$; similarly, $\langle 4, 4\rangle > \langle 2, 5\rangle$ (i.e., $0 > -3$) since $(4 + 5) > (2 + 4)$.

Addition: $\langle a, b\rangle + \langle c, d\rangle = \langle a + c, b + d\rangle$ where addition on the right is addition as already defined on natural numbers. For example, $\langle 6, 3\rangle + \langle 4, 2\rangle = \langle 10, 5\rangle$ (i.e., $3 + 2 = 5$); also, $\langle 2, 5\rangle + \langle 2, 1\rangle = \langle 4, 6\rangle$ (i.e., $-3 + 1 = -2$).

Subtraction: $\langle a,b\rangle - \langle c,d\rangle = \langle a,b\rangle + \langle d,c\rangle = \langle a+d, b+c\rangle$. For example, $\langle 4,2\rangle - \langle 6,3\rangle = \langle 4,2\rangle + \langle 3,6\rangle = \langle 4+3, 2+6\rangle = \langle 7,8\rangle$ (i.e., $2-3=-1$). (To subtract, one adds the 'negative' of the subtrahend, i.e., $2-3 = 2+(-3)$.) Note further that $\langle a,b\rangle = \langle a,0\rangle - \langle b,0\rangle$. Since we call numbers of the form $\langle a,0\rangle$, $\langle b,0\rangle$ positive, we may now interpret this result as showing that any integer $\langle a,b\rangle$ can be represented as the difference of two positive integers $\langle a,0\rangle - \langle b,0\rangle$.

Multiplication: $\langle a,b\rangle \cdot \langle c,d\rangle = \langle (a\cdot c)+(b\cdot d), (a\cdot d)+(b\cdot c)\rangle$, where multiplication on the right side is multiplication as already defined on natural numbers. For example, $\langle 6,3\rangle \cdot \langle 4,2\rangle = \langle (6\cdot 4)+(3\cdot 2), (6\cdot 2)+(3\cdot 4)\rangle = \langle 24+6, 12+12\rangle = \langle 30,24\rangle$ (i.e., $3\cdot 2=6$); similarly, $\langle 2,5\rangle \cdot \langle 1,2\rangle = \langle (2\cdot 1)+(5\cdot 2), (2\cdot 2)+(5\cdot 1)\rangle = \langle 2+10, 4+5\rangle = \langle 12,9\rangle$ (i.e., $(-3)\cdot(-1)=3$). This definition has the desired result for positive integers: $\langle a,0\rangle \cdot \langle c,0\rangle = \langle a\cdot c, 0\rangle$; and for negative integers: $\langle 0,b\rangle \cdot \langle 0,d\rangle = \langle bd, 0\rangle$; $\langle a,0\rangle \cdot \langle 0,d\rangle = \langle 0, ad\rangle$.

The natural numbers are not themselves a subset of this set-theoretic representation of the integers. Rather, the set of all integers contains a subset consisting of the positive integers and zero which is isomorphic to the set of natural numbers. Although in many applications the distinction between natural numbers and non-negative integers is not important, the concepts can be seen to differ by virtue of the total systems of which they are part. For example, while the positive integer $+5$ can be subtracted from the positive integer $+3$, the corresponding natural number 5 cannot be subtracted from the natural number 3.

A.3 Extension to the set of all rational numbers

The operations of addition, subtraction and multiplication are now defined on all the integers. We have not said anything yet about division. The question 'What number multiplied by x gives y?' does not always have an answer in the integers. The next extension of this system will be to a number structure in which this question is always answered: the *rationals*. There is one notable exception: division by 0 is always impossible. (It is instructive to attempt to extend the system to one which includes division by 0 and observe the difficulties one encounters.) The elements of the new system will be defined in terms of integers, for convenience written as usual $\ldots -2, -1, 0, 1, 2, \ldots$ The operations and relations of the new system will be defined in terms of the operations and relations on the integers. An isomorphism can then be shown between the integers and a subsystem of the rationals.

DEFINITION A.2 *A rational number is an ordered pair $\langle a, b\rangle$ of integers where $b \neq 0$.* ■

The pair $\langle a, b\rangle$ may be interpreted in the language of ordinary arithmetic as the fraction $\frac{a}{b}$. Note that since each integer is defined as a pair of natural numbers a rational will be a pair of pairs of natural numbers.

Equality: $\langle a, b\rangle = \langle c, d\rangle$ if and only if $a \cdot d = c \cdot b$.

Ordering 'greater than': $\langle a, b\rangle > \langle c, d\rangle$ if and only if $a \cdot d > c \cdot b$.

Addition: $\langle a, b\rangle + \langle c, d\rangle = \langle a \cdot d + c \cdot b, b \cdot d\rangle$.

Subtraction: $\langle a, b\rangle - \langle c, d\rangle = \langle a \cdot d - c \cdot b, b \cdot d\rangle$.

Multiplication: $\langle a, b\rangle \cdot \langle c, d\rangle = \langle a \cdot c, b \cdot d\rangle$.

Division: $\langle a, b\rangle : \langle c, d\rangle = \langle a \cdot d, c \cdot b\rangle$.

(All operations on the right sides are as defined for the integers.)

It will be noted that attempting to divide by 0 yields an ordered pair whose second member is 0; by definition, such ordered pairs are not rational numbers and hence division by 0 is impossible within the system.

To define the isomorphism between the integers and a substructure of the rationals (except division), let the rational number $\langle x, 1\rangle$ correspond with the integer x, and all the operations for the rationals (except division) correspond to operations with the same name for the integers and similarly for the ordering. It can be verified that this is an isomorphism.

A.4 Extension to the set of all real numbers

This section does not actually come within the realm of discrete mathematics, which deals with set of cardinality no larger than $\aleph_0$. The real numbers, as we saw in Chapter 4, form a larger set, and its properties are different in many ways. Most of the subject of calculus, for example, depends on some of the essential properties of the real number system.

This extension of the number system in its set-theoretic representation allows us to obtain a system in which we always have an answer to a question like 'Which number multiplied by itself gives 2?'. There are two fundamental ways of constructing the real number system, one due to Cantor, the other to Dedekind. We give here Cantor's construction. Consider sequences

$A = \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{5}{6}, \frac{6}{7}, \ldots$

and

$B = \frac{2}{1}, \frac{3}{2}, \frac{4}{3}, \frac{5}{4}, \frac{6}{5}, \frac{7}{6}, \ldots$

Both of these sequences *converge to* 1; i.e., the more a sequence is developed, the closer one gets to 1, even though 1 is never actually reached. This is expressed more precisely by saying that a sequence $a_0, a_1, a_2, \ldots$ *converges to* x if for any positive number ϵ (epsilon), no matter how small, we can find an index N such that $|a_n - x| < \epsilon$ for all $n > N$. Some sequences of rational numbers converge to a number which is itself not representable as a rational number. The above definition cannot be used to test convergence in such cases, since we have no means of expressing the point of convergence. Another definition of convergence can be given which is equivalent to the former but which does not depend on the nature of x.

DEFINITION A.3 *A sequence $a_0, a_1, a_2, \ldots$ converges if for any positive number ϵ no matter how small we can find an index N such that $|a_n - a_m| < \epsilon$ for all $m > N$ and $n > N$.* ■

In other words, we are stating that the terms far out in the series must get closer and closer to each other, which has the same effect as saying that they must all get closer and closer to some particular point of convergence. Cantor defined a real number as a convergent sequence of rational numbers. The rational numbers themselves can be represented in this system as sequences of the form $r, r, r, \ldots$ where r is a rational number, since a sequence all of whose members are identical cerainly satisfies the definition of convergence. If one thinks of real numbers as infinite decimals, one way of representing real numbers would be as the limit of a sequence of finite decimals (which are rational numbers) of the form $x_1.$, $x_1.x_2$, $x_1.x_2x_3$, $x_1.x_2x_3x_4$, i.e., $\frac{x_1}{1}, \frac{x_1x_2}{10}, \frac{x_1x_2x_3}{100}, \ldots$ Operations must all be defined anew for the real numbers, but this is quite simple. To give just one example, addition is defined by: $a_0, a_1, a_2, \ldots + b_0, b_1, b_2, \ldots = a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots$