Numbers, sets and axioms

THE APPARATUS OF MATHEMATICS

A.G.HAMILTON
Lecturer in mathematics at the University of Stirling

*The right of the
University of Cambridge
to print and sell
all manner of books
was granted by
Henry VIII in 1534.
The University has printed
and published continuously
since 1584.*

CAMBRIDGE UNIVERSITY PRESS
Cambridge
New York   Port Chester
Melbourne   Sydney

Published by the Press Syndicate of the University of Cambridge
The Pitt Building, Trumpington Street, Cambridge CB2 1RP
40 West 20th Street, New York, NY 10011-4211, USA
10 Stamford Road, Oakleigh, Victoria 3166, Australia

First published 1982
Reprinted 1989, 1992

Library of Congress catalogue card number: 82-4206

British Library cataloguing in publication data

Hamilton, A. G.
Numbers, sets and axioms: the apparatus of mathematics.

I. Set theory
I. Title
511.33 QA248

ISBN 0 521 24509 5 hardback
ISBN 0 521 28761 8 paperback

CONTENTS

1

NUMBERS

Summary

First we consider what are the basic notions of mathematics, and emphasise the need for mathematicians to agree on a common starting point for their deductions. Peano's axioms for the natural numbers are listed. Starting with a system of numbers satisfying Peano's axioms, we construct by algebraic methods the systems of integers, rational numbers, real numbers and complex numbers. At each stage it is made clear what properties the system constructed has and how each number system is contained in the next one. In the last section there is a discussion of decimal representation of rational numbers and real numbers.

The reader is presumed to have some experience of working with sets and functions, and to be familiar with the ideas of bijection, equivalence relation and equivalence class.

1.1 **Natural numbers and integers**

It is fashionable nowadays at all levels of study from elementary school to university research, to regard the notion of set as the basic notion which underlies all of mathematics. The standpoint of this book is that the idea of set is something that no modern mathematician can be without, but that it is first and foremost a *tool* for the mathematician, a helpful way of dealing with mathematical entities and deductions. As such, of course, it becomes also an object of study by mathematics. It is inherent in the nature of mathematics that it includes the study of the methods used in the subject; this is the cause of much difficulty and misunderstanding, since it apparently involves a vicious circle. The trouble is that most people (mathematicians included) try to regard mathematics as a *whole* – a logical system for proving true theorems based on indubitable principles. The present author believes that this is a misleading picture. Mathematics is rather a mixture of intuition, analogy and logic – a body of accepted knowledge based on perceived reality, together with tools and techniques for drawing analogies, making conjectures and providing logical justification for conclusions drawn.

The fundamental notions of mathematics now are the same as they were a hundred years ago, namely, numbers or, to be more specific, the number systems. Modern abstract mathematics (with the exception, perhaps, of geometry and topology) is based almost entirely on analogies drawn with properties of numbers. Here are some simple examples. The algebraic theory of fields arises from a generalisation of the properties of addition and multiplication of numbers. Real analysis is just the study of functions from real numbers to real numbers. Functional analysis applies the methods of algebra (themselves derived from methods used in concrete numerical situations) to mathematical systems which are generalisations of three-dimensional physical space (which can be represented, of course, via coordinate geometry, by means of ordered triples of real numbers).

Our knowledge of the number systems derives from our perception of the physical world. We count and we measure, and the origins of mathematics lie in these activities. Modern methods can help in writing down and working out properties of numbers and in clarifying relationships between these properties. Indeed, this process has reached an advanced stage. Most mathematicians now agree on what are the principles which it is proper to use in order to characterise the number systems. This is very significant, for it provides a common starting point for logical deductions. If all mathematicians based their deductions on their own personal intuitions then communication would be very difficult and the subject would not be very coherent. One purpose of this book is to expound and explain the common starting point. In the first chapter we deal with the number systems out of which mathematics develops, and in subsequent chapters we shall investigate some of the tools (notably set theory) and try to explain what modern 'foundations of mathematics' is all about.

Counting is the first mathematical activity that we learn. We learn to associate the objects in a collection with words (numbers) which mark them off in a sequence and finally indicate 'how many' there are in the collection. This experience gives us an intuition about an unending sequence of numbers which can be used to count in this way any finite collection of objects. It is assumed that the readers of this book will have a well-developed intuition about natural numbers, so we shall not go into the psychology behind it (this is not to imply that the psychology of mathematical intuition is not worthy of study – just that it is outside the scope of this book).

Notation The set of natural numbers will be denoted by $\mathbb{N}$. $\mathbb{N}$ is the collection $\{0, 1, 2, \ldots\}$. Notice that we include 0 in $\mathbb{N}$. This is merely a convention. It is common but not universal.

Let us list some properties of these numbers which accord with intuition.

Examples 1.1

(a) There is an addition operation (a two-place function on $\mathbb{N}$) which is commutative and associative.

(b) $0+n=n$, for every $n \in \mathbb{N}$.

(c) In the list $\{0, 1, 2, \ldots\}$, the number following n is $n+1$, for each n.

(d) $n+1 \neq n$, for every $n \in \mathbb{N}$.

(e) $m+1=n+1$ implies $m=n$, for every $m, n \in \mathbb{N}$.

(f) There is a multiplication operation (also a two-place function on $\mathbb{N}$) which is commutative and associative, and which distributes over addition.

(g) $0 \times n=0$, and $1 \times n=n$, for every $n \in \mathbb{N}$.

(h) $m \times n=p \times n$ implies $m=p$, for every $m, n, p \in \mathbb{N}$ $(n \neq 0)$.

► Clearly, we can continue writing down such properties indefinitely. These are the kind of things we learn in elementary school. We learn them, discover that they work, and come to believe them as truths which do not require justification. However, the mathematician who is working in the theory of numbers needs a starting point in common with other mathematicians. *Peano's axioms* (listed first in 1888 by Dedekind, and not originating with Peano) are such a common starting point. They are five basic properties, all of them intuitively true, which serve as a basis for logical deduction of true theorems about numbers. They are as follows.

(P1) There is a number 0.

(P2) For each number n, there is another number n' (the *successor* of n).

(P3) For no number n is n' equal to 0.

(P4) If m and n are numbers and $m' = n'$, then $m = n$.

(P5) If A is a set of numbers which contains 0 and contains n' for every $n \in A$, then A contains all numbers.

(Note that we have used the word 'number' here as an abbreviation for 'natural number'.)

Remarks 1.2

(a) (P1) and (P2) provide the process for generating the sequence of natural numbers corresponding to the intuitive counting procedure. (P3) reflects the fact that the sequence has a beginning.

(b) (P4) is a more complicated property of the sequence of numbers: different numbers have different successors.

(c) (P5) is the principle of mathematical induction. This is the most substantial of the five, and is the basis of most proofs in elementary number theory. It may be more familiar as a method of proof rather than an axiom, and in a slightly different form: if $P(n)$ is a statement about a natural number n such that $P(0)$ holds, and $P(k+1)$ holds whenever $P(k)$ holds, then $P(n)$ holds for every natural number n. This can be seen to be equivalent to (P5) if we think of the set A and the statement $P(n)$ related by:

$n \in A$ if and only if $P(n)$ holds.

Thus, given a set A, a statement $P(n)$ is determined and vice versa.

► There is no mention in Peano's axioms of the operations of addition and multiplication. This is because these can be defined in terms of the other notions present.

The common starting point, therefore, *need not* mention these operations. However, it is quite difficult to carry out the procedure of defining them and justifying their existence (see Section 4.3) and, for our present purposes, it is certainly unnecessary. For our purposes we can broaden the common starting point, that is to say, we can include amongst our basic intuitive properties the following.

(A) There is a two-place function (denoted by $+$) with the properties:

$m + 0 = m$, for every number m.

$m + n' = (m + n)'$, for all numbers m, n.

(M) There is a two-place function (denoted by $\times$) with the properties:

$$m \times 0 = 0, \quad \text{for every number } m.$$

$$m \times n' = (m \times n) + m, \quad \text{for all numbers } m, n.$$

(Following the usual mathematical practice we shall usually omit multiplication signs, and write mn rather than $m \times n$. The exceptions will be when special emphasis is being placed on the operation of multiplication.)

We could also include amongst our basic intuitive properties the assertions that these operations satisfy the commutative, associative and distributive laws, but it is not difficult to prove, from the properties given above, that these hold. Let us carry out one such proof, as an example.

Theorem 1.3

Addition on $\mathbb{N}$ is commutative.

Proof

This is an exercise in proof by induction. We require two preliminary results:

(i) $0 + m = m$, for all $m \in \mathbb{N}$.

(ii) $m' + n = (m + n)'$, for all $m, n \in \mathbb{N}$.

For (i), we use induction on m. By property (A) we have $0 + 0 = 0$. Suppose that $0 + k = k$. Then $0 + k' = (0 + k)' = k'$ (using property (A) again).

Hence, by the induction principle, $0 + m = m$ holds for all $m \in \mathbb{N}$.

For (ii), we apply (P5) to the set

$$A = \{n \in \mathbb{N}\colon m' + n = (m + n)', \text{ for every } m \in \mathbb{N}\}.$$

First, $0 \in A$, since $m' + 0 = m'$ (by property (A)) and $(m + 0)' = (m)'$ (again by property (A)), and so $m' + 0 = (m + 0)'$, for any $m \in \mathbb{N}$. Second, suppose that $k \in A$, i.e. $m' + k = (m + k)'$ for every $m \in \mathbb{N}$. Then

$$\begin{aligned} m' + k' &= (m' + k)' && \text{(by property (A))},\\ &= ((m + k)')' && \text{(by our supposition that } k \in A),\\ &= (m + k')' && \text{(by property (A))}. \end{aligned}$$

This holds for every $m \in \mathbb{N}$, so $k' \in A$. We can therefore apply (P5) to deduce that $A = \mathbb{N}$, i.e., (ii) holds for all $m, n \in \mathbb{N}$.

Now to complete the proof of the theorem we need a further induction. Let B be the set $\{n \in \mathbb{N} : m + n = n + m, \text{ for every } m \in \mathbb{N}\}$.

First, $0 \in B$ since $m+0=m$ (by property (A)), and $0+m=m$ (by (i) above). Second, let us suppose that $k \in B$, i.e., $m+k=k+m$ for every $m \in \mathbb{N}$. Now

$$\begin{aligned} m+k' &= (m+k)' && \text{(by property (A))}, \\ &= (k+m)' && \text{since } k \in B, \\ &= k'+m && \text{(by (ii) above).} \end{aligned}$$

This holds for every $m \in \mathbb{N}$, so $k' \in B$. Applying (P5) to B we conclude that $B = \mathbb{N}$, i.e. $m+n=n+m$ for all $m, n \in \mathbb{N}$.

► It is not our purpose to develop elementary number theory, but there are some basic results which we should at least mention.

Remark 1.4

For every natural number n, either $n=0$ or $n=m'$ for some natural number m.

This may be proved using Peano's axioms. It is left as an exercise for the reader, with the hint that (P5) should be applied to the set $A = \{n \in \mathbb{N}: \text{either } n=0 \text{ or } n=m' \text{ for some } m \in \mathbb{N}\}$.

Theorem 1.5

Every non-empty set of natural numbers has a least member.

Before we prove this we require to give an explanation of the term 'least member'. Again this is an intuitive notion, but its properties can be derived from the definitions and properties of numbers already given. For $m, n \in \mathbb{N}$ we write $m<n$ if there is $x \in \mathbb{N}$, with $x \neq 0$, such that $m+x=n$. (We also use the notation $m \leqslant n$, with the obvious meaning.) A set A of natural numbers has a *least member* if there is an element $m \in A$ such that $m<n$ for every other element $n \in A$. The result of Theorem 1.5 is intuitively true when we think of the normal sequence $\{0, 1, 2, \ldots\}$ of natural numbers and note that the relation $<$ corresponds to the relation 'precedes'.

Proof (of Theorem 1.5)

Let A be a set of natural numbers which contains no least member. We show that A is empty. We apply (P5) to the set $B = \{x \in \mathbb{N}: x \leqslant n \text{ for every } n \in A\}$. Certainly $0 \in B$, since $0 \leqslant n$ for every $n \in A$. Suppose that $k \in B$. Then $k \leqslant n$ for every $n \in A$. But k cannot belong to A, since if it did it would be the least element of A. Hence

$k<n$ for every $n\in A$, and consequently $k+1\leqslant n$ for every $n\in A$, i.e. $k+1\in B$. By (P5), then, we have $B=\mathbb{N}$. By the definition of B, this means that $x\leqslant n$ holds for every $x\in\mathbb{N}$ and every $n\in A$. This is impossible unless A is empty, in which case it is vacuously true. The proof is now complete.

► The above theorem can be used to justify a slightly different version of the principle of mathematical induction.

(P5*) If A is a set of natural numbers which contains 0 and contains n' whenever $0, 1, \ldots, n$ all belong to A, then A contains all natural numbers.

Theorem 1.6

(P5*) holds (as a consequence of (P5), through Theorem 1.5).

Proof

Let $A\subseteq\mathbb{N}$, with $0\in A$ and such that $n'\in A$ whenever $0, 1, \ldots, n\in A$. We require to show that $A=\mathbb{N}$. Consider the set $\mathbb{N}\backslash A$ (the set of all elements of $\mathbb{N}$ which do not belong to A). Suppose that $\mathbb{N}\backslash A$ is not empty. Then by Theorem 1.5 it contains a least member, n_0, say. We have therefore $n_0\notin A$, and $x\in A$ for every x with $x<n_0$. Now $n_0\neq 0$, since $0\in A$, by our original hypothesis. Hence, $n_0=m'$ for some $m\in\mathbb{N}$ (by the result of Remark 1.4). So we have $m'\notin A$, but we have also $0, 1, \ldots, m\in A$. This is a contradiction since our hypothesis says that we have $n'\in A$ whenever $0, 1, \ldots, n\in A$. It follows that $\mathbb{N}\backslash A$ is empty, and consequently $A=\mathbb{N}$.

► The last of our basic results is one that we shall refer to when we discuss properties of the other number systems. It is the result which is commonly known as the *division algorithm*. Its proof is given here for the sake of completeness, and the reader may omit it.

Theorem 1.7

Let $a\in\mathbb{N}$, $b\in\mathbb{N}$, $b\neq 0$. There exist $q\in\mathbb{N}$, $r\in\mathbb{N}$ with

$$a=qb+r \quad\text{and}\quad r<b.$$

Moreover, the numbers q and r are uniquely determined.

Proof

Let $S=\{y\in\mathbb{N}: y+xb=a$, for some $x\in\mathbb{N}\}$. (S may be thought of as the set of differences $a-xb$ for all those $x\in\mathbb{N}$ such that $a\geqslant xb$.)

S is not empty, since $a \in S$ (corresponding to $x = 0$). Hence, by Theorem 1.5, S contains a least element, say r. Since $r \in S$, there is $q \in \mathbb{N}$ such that $r + qb = a$, i.e. $a = qb + r$. We must have $r < b$, for otherwise $b \leqslant r$, so that $r = b + r_1$, say, with $r_1 \in \mathbb{N}$, and $r_1 < r$, necessarily. Then $r + qb = a$ gives $r_1 + b + qb = a$, i.e. $r_1 + (q+1)b = a$, and this implies that $r_1 \in S$. This contradicts the choice of r as the least element of S.

It remains to show that q and r are unique. Suppose that $a = qb + r = q'b + r'$, with $r < b$, $r' < b$, and $r \leqslant r'$, say. Then there is $t \in \mathbb{N}$ such that $r + t = r'$, and we have $qb + r = q'b + r + t$, and hence $qb = q'b + t$. It follows that $q'b \leqslant qb$, so $q' \leqslant q$. Let $q = q' + u$, say, with $u \in \mathbb{N}$. Then $q'b + ub = qb = q'b + t$, giving $ub = t$. Since $r + t = r'$, then, we have $r + ub = r'$. Consequently $ub \leqslant r'$, which contradicts $r' < b$, unless $u = 0$. Thus we must have $u = 0$, and this implies that $r = r'$, $t = 0$, and $q = q'$, as required.

In the above proof we have used, besides Theorem 1.5, a few properties of addition, multiplication and inequalities which have not been explicitly derived from our basic assumptions. The most apparent, perhaps, is the cancellation law for inequalities: if $ax \leqslant bx$ and $x \neq 0$, then $a \leqslant b$. This may be treated as an exercise.

► Natural numbers are a product of intuition. There is no need for a mathematical *definition* of natural numbers. Peano's axioms may be seen as an attempt to define, but they are in fact merely an attempt to characterise natural numbers. But immediately two questions arise. First, are Peano's axioms true of our intuitive natural numbers? And second, is there any collection of objects, essentially different from the set of natural numbers, for which Peano's axioms also hold true? The answer to the first question is clearly (intuitively) in the affirmative. The answer to the second is much harder to find, for it involves the mathematical abstractions: 'collection of objects for which Peano's axioms hold true', and 'essentially different'. We shall see in due course that the second answer is negative, but before that we must explain the abstractions.

Consider the set $2\mathbb{N} = \{2n : n \in \mathbb{N}\}$ of even natural numbers, and denote $k+2$ by k^*, for each $k \in 2\mathbb{N}$. Then the following are true:

(1) $0 \in 2\mathbb{N}$.

(2) For each $k \in 2\mathbb{N}$, $k^* \in 2\mathbb{N}$.

(3) For no $k \in 2\mathbb{N}$ is k^* equal to 0.

(4) If $k, l \in 2\mathbb{N}$, then $k^* = l^*$.

(5) If $A \subseteq 2\mathbb{N}$ is such that $0 \in A$ and $k^* \in A$ whenever $k \in A$, then $A = 2\mathbb{N}$.

In other words, Peano's axioms 'hold' for the set $2\mathbb{N}$ (together with the operation *). It is not difficult to conceive of other structures (i.e. sets together with unary operations) for which Peano's axioms also hold. We can say precisely what this means in general.

Definition

A *model* of Peano's axioms is a set N, together with a function f and an object e (a triple (N, f, e)) such that

(P1*) $e \in N$.

(P2*) The domain of f is N, and for each $x \in N$, $f(x) \in N$.

(P3*) If $x \in N$, then $f(x) \neq e$.

(P4*) If $x, y \in N$ and $f(x) = f(y)$, then $x = y$.

(P5*) If A is a subset of N which contains e and contains $f(x)$ for every $x \in A$, then $A = N$.

The function f is to act like the successor function and e is to act like 0. The reader should compare these conditions (P1*), . . . , (P5*) carefully with (P1), . . . , (P5).

► The model $(2\mathbb{N}, *, 0)$ given above, by its very existence, tells us that Peano's axioms do not characterise the set of natural numbers uniquely. But this new model has a *structure* which is identical to the structure of $(\mathbb{N}, ', 0)$. The two models are *isomorphic*, that is to say there is a bijection $\varphi : \mathbb{N} \to 2\mathbb{N}$ such that $\varphi(n') = (\varphi(n))^*$ for all $n \in \mathbb{N}$, and $\varphi(0) = 0$. (The function φ is given by $\varphi(n) = 2n$.) In general we can make the following definition.

Definition

Two models (N_1, f_1, e_1) and (N_2, f_2, e_2) of Peano's axioms are *isomorphic* if there is a bijection $\varphi : N_1 \to N_2$ such that

$$\text{(i)} \quad \varphi(f_1(x)) = f_2(\varphi(x)), \quad \text{for all } x \in N_1,$$

and

$$\text{(ii)} \quad \varphi(e_1) = e_2.$$

Such a function is said to be an *isomorphism*.

► Models of Peano's axioms exist which are different from, but isomorphic to, $(\mathbb{N}, ', 0)$. Mathematically, such models are essentially the same, and for mathematical purposes it really does not matter whether natural numbers are taken to be the elements of $\mathbb{N}$ or the elements of a different but isomorphic model. This will form the basis of our construction of natural numbers within set theory in Section 4.3. In a sense it is only a matter of labelling. If two models are isomorphic then their mathematical characteristics are the same but their elements may be objects of different sorts.

What makes the overall situation sensible, however, is the result of Corollary 1.9 below. It implies that there is no model of Peano's axioms which is not isomorphic to $(\mathbb{N}, ', 0)$. In other words, Peano's axioms do characterise the *structure* of $(\mathbb{N}, ', 0)$ completely.

Theorem 1.8 (definition by induction)

Let (N, f, e) be any model for Peano's axioms. Let X be any set, let $a \in X$ and let g be any function from X to X. Then there is a unique function F from N to X such that

$$F(e) = a,$$

and

$$F(f(x)) = g(F(x)), \quad \text{for each } x \in N.$$

► Theorem 1.8 legitimises what is probably a familiar process for defining functions with domain $\mathbb{N}$. This process was used on page 4 above in the properties (A) and (M). First specify the value of $F(0)$, and then, on the assumption that $F(n)$ has been defined, specify $F(n+1)$ in terms of $F(n)$. Here, of course, we are dealing with an arbitrary model of Peano's axioms, rather than $\mathbb{N}$. The proof of Theorem 1.8 is lengthy and technical, so we shall omit it at this stage. Theorem 4.15 is a particular case of Theorem 1.8, concerning that model of Peano's axioms (the set of abstract natural numbers) which is constructed in Section 4.3. The proof given there can be generalised in a straightforward way to apply to an arbitrary model, as required here.

Corollary 1.9

Any two models of Peano's axioms are isomorphic.

Proof

Let (N_1, f_1, e_1) and (N_2, f_2, e_2) be models of Peano's axioms. By Theorem 1.8, there is a unique function $F: N_1 \to N_2$ such that

$$F(e_1) = e_2,$$

and

$$F(f_1(x)) = f_2(F(x)), \quad \text{for each } x \in N_1.$$

This function F thus satisfies conditions (i) and (ii) required by the definition of an isomorphism. It remains only to prove that F is a bijection. Now applying Theorem 1.8 with N_1 and N_2 reversed will yield a unique function $G : N_2 \to N_1$ such that

$$G(e_2) = e_1,$$

and

$$G(f_2(y)) = f_1(G(y)), \quad \text{for each } y \in N_2.$$

We show that $G(F(x)) = x$ for every $x \in N_1$, by application of (P5*) to (N_1, f_1, e_1). Let $A = \{x \in N_1 : G(F(x)) = x\}$. Then $e_1 \in A$, since $G(F(e_1)) = G(e_2) = e_1$. Let $x \in A$. Then $G(F(x)) = x$, so that

$$G(F(f_1(x))) = G(f_2(F(x))) = f_1(G(F(x))) = f_1(x),$$

and consequently $f_1(x) \in A$. It follows, by (P5*), that $A = N_1$. Likewise, we can show that $F(G(y)) = y$ for every $y \in N_2$. Hence, F and G are bijections (and are inverses of each other) and the proof is complete.

► The concept of a model of Peano's axioms which is different from, but isomorphic to, $(\mathbb{N}, ', 0)$ is the first stage of mathematical abstraction. Similar abstractions are made in the constructions of the systems of integers, rational numbers, real numbers and complex numbers. These constructions start from the basis of natural numbers and proceed using standard algebraic processes, but in the end they produce sets of mathematical objects which are exceedingly complex in themselves, but which have the necessary properties characterising the number systems in question. What are negative integers? There are some people who argue seriously that they do not exist. But they certainly exist for the mathematician. The mathematician can construct, using his abstract methods, a set which has the properties that the set of integers ought to have, starting from $\mathbb{N}$. We now proceed to do this in some detail. Rationals, reals and complexes will follow.

The way to construct the set of integers is to regard it as the set of all *differences* between ordered pairs of natural numbers. For example:

$(2, 3)$ gives rise to -1,

$(3, 2)$ gives rise to 1,

$(5, 31)$ gives rise to -26, etc.

Notice the significance of the order of the two numbers in the pair. The first problem is that different ordered pairs can give rise to the same integer, for example: $(2, 5)$ and $(7, 10)$ both give rise to -3. Thus we cannot define integers to *be* ordered pairs of natural numbers. What we do is take the collection of all ordered pairs (m, n) with $n-m=3$ to *represent* the integer -3. We do this via an appropriate equivalence relation, for which the above collection (and all other similarly defined collections) are equivalence classes.

(An equivalence relation on a set X is a binary relation on X which is reflexive, symmetric and transitive. The property which we use is that an equivalence relation gives rise to equivalence classes. An equivalence class consists of all elements of X which are related to a given element. Each element of X determines (and belongs to) one equivalence class. Indeed, X is partitioned into disjoint equivalence classes. We shall mention equivalence relations again in Section 3.1, with more details of the definition. Any standard text on beginning abstract algebra will provide further details if required.)

Now for the formal details of our construction of the integers.

Definition

Let a, b, c, $d \in \mathbb{N}$. We say that (a, b) is related to (c, d), written $(a, b) \diamond (c, d)$, if $a+d=b+c$. (Notice that we are unable to write '$a-b=c-d$' as we might have wished, because until we have defined negative numbers, differences of natural numbers may not exist.)

Now $\diamond$ is an equivalence relation. This is easily verified. For any pair (a, b) of natural numbers, $a+b=b+a$, so $(a, b) \diamond (a, b)$, and $\diamond$ is reflexive. If $(a, b) \diamond (c, d)$ then $a+d=b+c$, so $c+b=d+a$, i.e. $(c, d) \diamond (a, b)$, and $\diamond$ is symmetric. Lastly, if $(a, b) \diamond (c, d)$ and $(c, d) \diamond (e, f)$, then $a+d=b+c$ and $c+f=d+e$. We have

$$\begin{aligned} a+f+d &= a+d+f \\ &= b+c+f \\ &= b+d+e \\ &= b+e+d, \end{aligned}$$

and consequently $a+f=b+e$, so that $(a, b) \diamond (e, f)$, as required to show that $\diamond$ is transitive.

We define *integers* to be equivalence classes under the relation $\diamond$. As an example, the set $\{(a, b): a+1=b\}$ is an equivalence class (it is the class determined by (0, 1)), and we are *defining* the integer −1 to be this set. However, we shall not use normal notation for integers yet.

Let us denote the equivalence class determined by (a, b) by $\boldsymbol{(}a, b\boldsymbol{)}$. What we intend is that $\boldsymbol{(}a, b\boldsymbol{)}$ should be the integer that we intuitively think of as $a-b$.

► All we have so far is a set. It remains to describe the operations of addition and multiplication, to investigate the natural order of the integers and to examine in what way the newly defined set of integers 'contains' the set of natural numbers. This last reflects the way that we normally regard these sets – we do not normally distinguish between natural numbers and non-negative integers.

Definition

Addition and *multiplication* of integers are defined as follows. Let $a, b, c, d \in \mathbb{N}$.

$$\boldsymbol{(}a, b\boldsymbol{)} + \boldsymbol{(}c, d\boldsymbol{)} = \boldsymbol{(}a+c, b+d\boldsymbol{)},$$

$$\boldsymbol{(}a, b\boldsymbol{)} \times \boldsymbol{(}c, d\boldsymbol{)} = \boldsymbol{(}ac+bd, ad+bc\boldsymbol{)}.$$

Remarks 1.10

(a) These definitions have an intuitive basis.
$(a-b)+(c-d)=(a+c)-(b+d)$ lies behind the first.
$(a-b)\times(c-d)=(ac+bd)-(ad+bc)$ is the way to remember the second.

(b) We are defining operations on equivalence classes. It is necessary in such a situation to verify that the operations are *well-defined.* We take the case of addition and leave multiplication as an exercise. What we must verify is that if $\boldsymbol{(}a, b\boldsymbol{)} = \boldsymbol{(}p, q\boldsymbol{)}$ and $\boldsymbol{(}c, d\boldsymbol{)} = \boldsymbol{(}r, s\boldsymbol{)}$, then $\boldsymbol{(}a+c, b+d\boldsymbol{)} = \boldsymbol{(}p+r, q+s\boldsymbol{)}$ (i.e. that the result of adding two classes does not depend on the pairs of natural numbers which are chosen to represent them). Suppose that $a+q=b+p$ and $c+s=d+r$. Then

$$\begin{aligned}(a+c)+(q+s) &= (a+q)+(c+s)\\ &= (b+p)+(d+r)\\ &= (b+d)+(p+r),\end{aligned}$$

and consequently $\boldsymbol{(}a+c, b+d\boldsymbol{)} = \boldsymbol{(}p+r, q+s\boldsymbol{)}$, as required.

(c) If (a, b) is an integer, and $c \in \mathbb{N}$, then $(a+c, b+c) = (a, b)$. To see this, just note that $(a+c, b+c) \diamond (a, b)$, since $(a+c)+b = (b+c)+a$.

(d) It is a straightforward exercise to verify that addition and multiplication satisfy the commutative, associative and distributive laws.

(e) Notice that, for any $a, b \in \mathbb{N}$,

$$(a, b) + (0, 0) = (a, b),$$

$$(a, b) \times (1, 0) = (a, b),$$

and

$$(a, b) \times (0, 0) = (0, 0).$$

Thus $(0, 0)$ behaves like zero, and $(1, 0)$ behaves like 1.

(f) For any $a, b \in \mathbb{N}$,

$$(a, b) + (b, a) = (0, 0).$$

To see this, we need to observe that $(a+b, a+b) = (0, 0)$, which is a special case of the result that $(m, m) = (0, 0)$, for every $m \in \mathbb{N}$.

We write $-(a, b)$ for (b, a), and we abbreviate $(a, b) + (-(c, d))$ by $(a, b) - (c, d)$. Thus we introduce *subtraction* as a legitimate operation on integers.

Exercise

$$(-(a, b)) \times (c, d) = -((a, b) \times (c, d)),$$

$$(-(a, b)) \times (-(c, d)) = (a, b) \times (c, d).$$

Notation

We denote the set of integers by $\mathbb{Z}$, and we shall use variables near the end of the alphabet for elements of $\mathbb{Z}$ (for the time being).

Definition

The order relation on $\mathbb{Z}$ is defined as follows. First we say that an element (a, b) of $\mathbb{Z}$ is *positive* if $b < a$ (as elements of $\mathbb{N}$). Again it must be shown that this is well-defined, i.e. that if $(a, b) = (c, d)$ and $b < a$ then $d < c$. If $a + d = b + c$ and $b < a$ then it certainly follows that $d < c$. $\mathbb{Z}^+$ denotes the set of positive integers. Now we define $<$, for

$x, y \in \mathbb{Z}$ by:

$$x < y \quad \text{if } y - x \in \mathbb{Z}^+.$$

We shall also use the symbol $\leqslant$ (less than or equal to) with its normal meaning.

Remarks 1.11

(a) For $x, y, z \in \mathbb{Z}$ we have $x < y$ if and only if $x + z < y + z$.

(b) For $x, y \in \mathbb{Z}$ and $z \in \mathbb{Z}^+$, we have $x < y$ if and only if $x \times z < y \times z$.

(c) For $x \in \mathbb{Z}$ and $y \in \mathbb{Z}^+$, we have $x < x + y$.

(d) If $x \in \mathbb{Z}^+$ and $y \in \mathbb{Z}^+$, then $x + y \in \mathbb{Z}^+$.

(e) If $x \in \mathbb{Z}^+$ and $y \in \mathbb{Z}^+$, then $x \times y \in \mathbb{Z}^+$.

(f) If $x \in \mathbb{Z}^+$, then $-x < x$.

(g) If $x \in \mathbb{Z}^+$, then $(0, 0) < x$.

(h) For any $x \in \mathbb{Z}$, $(0, 0) \leqslant x^2$.

We sketch proofs for (a) and (e). The others are left as exercises.

For (a), let $x = (a, b)$, $y = (c, d)$, $z = (e, f)$.

$$\begin{aligned}(y + z) - (x + z) &= ((c, d) + (e, f)) - ((a, b) + (e, f))\\ &= (c + e, d + f) - (a + e, b + f)\\ &= (c + e, d + f) + (b + f, a + e)\\ &= (c + e + b + f, d + f + a + e)\\ &= ((c + b) + (e + f), (d + a) + (e + f))\\ &= (c + b, d + a)\\ &= (c, d) + (b, a)\\ &= (c, d) - (a, b)\\ &= y - x.\end{aligned}$$

Thus $(y + z) - (x + z) \in \mathbb{Z}^+$ if and only if $y - x \in \mathbb{Z}^+$, i.e. $x + z < y + z$ if and only if $x < y$.

For (e), let $x = (a, b)$ and $y = (c, d)$, where $b < a$ and $d < c$.

$$x \times y = (ac + bd, ad + bc).$$

Now there exist $p, q \in \mathbb{N}\backslash\{0\}$ such that $a = b + p$ and $c = d + q$, so

$$\begin{aligned}ac + bd &= (b + p)(d + q) + bd\\ &= 2bd + pd + bq + pq,\end{aligned}$$

and

$$\begin{aligned} ad+bc &= (b+p)d+b(d+q) \\ &= 2bd+pd+bq. \end{aligned}$$

Therefore $ac+bd=ad+bc+pq$, so that

$$ad+bc<ac+bd \text{ in } \mathbb{N} \quad \text{(see Exercise 4 on page 18),}$$

and consequently $x\times y \in \mathbb{Z}^+$.

► The pattern that proofs take is well exemplified by the above. Results about elements of $\mathbb{Z}$ are re-stated in terms of equivalence classes of pairs of natural numbers and hence in terms of natural numbers themselves. Properties of $\mathbb{N}$ can then be used to justify properties of $\mathbb{Z}$. Care must be taken in such proofs to distinguish between elements of $\mathbb{Z}$ and elements of $\mathbb{N}$, and to make no assumptions about integers (and, moreover, to avoid treating elements of $\mathbb{N}$ as integers).

The above is a temporary warning only, however. Once the properties of integers have been derived from the properties of natural numbers, we can forget the apparatus of the construction, and treat integers in the intuitive way that we are accustomed to. Part of this intuition is the idea that $\mathbb{N}$ is a subset of $\mathbb{Z}$, i.e. that natural numbers are just non-negative integers. Our construction of $\mathbb{Z}$ renders this convenient idea false. However, we may recover the situation by the following process.

Consider the set S of integers of the form $(n, 0)$ $(n \in \mathbb{N})$. We have seen that $(0, 0)$ behaves like a zero. Let $f: S \to S$ be given by $f(n, 0) = (n+1, 0)$. Then $(S, f, (0, 0))$ is a model for Peano's axioms. This is left for the reader to verify. Moreover, $(S, f, (0, 0))$ is isomorphic to $(\mathbb{N}, ', 0)$, by Corollary 1.9 (the isomorphism associates each $n \in \mathbb{N}$ with $(n, 0) \in S$), and so S has the same mathematical structure as $\mathbb{N}$. Addition and multiplication bear this out, for we know that for $m, n \in \mathbb{N}$,

$$(m, 0)+(n, 0)=(m+n, 0),$$

and

$$(m, 0)\times(n, 0)=(mn, 0).$$

Consequently, we can take the elements of S to represent the natural numbers. This satisfies the formal mathematical requirements. In practice there is no need to do other than just imagine that $\mathbb{N}$ is a subset of $\mathbb{Z}$, in effect regarding n and $(n, 0)$ as different labels for the same object. From now on we actually do so. It should not lead to confusion.

Theorem 1.12

$\mathbb{Z}^+ \cup \{(0, 0)\}$, the set of non-negative integers, together with the successor function f given by $f(n, 0) = (n+1, 0)$ and the zero element $(0, 0)$, is a model for Peano's axioms.

Proof

The set S in the above argument is just $\mathbb{Z}^+ \cup \{(0, 0)\}$, so the proof is described above. Notice that the non-negative integers thus behave just as natural numbers do.

Theorem 1.13

(i) Given $x \in \mathbb{Z}$, we have *one* of the following: $x \in \mathbb{Z}^+$ or $x = 0$ or $-x \in \mathbb{Z}^+$.

(ii) If $x, y \in \mathbb{Z}^+$, then $x + y \in \mathbb{Z}^+$ and $x \times y \in \mathbb{Z}^+$.

Proof

(i) Let $x = (a, b)$. If $a = b$ then $(a, b) = (0, 0)$ and so $x = 0$. Now suppose that $a \neq b$. The set $\{a, b\}$ is a non-empty subset of $\mathbb{N}$, so contains a least member. If the least member is a, then $a < b$. If the least member is b then $b < a$. In the former case we have $-x \in \mathbb{Z}^+$, since $-x = (b, a)$. In the latter case we have $x \in \mathbb{Z}^+$. This proves (i).

(ii) These have already appeared as Remarks 1.11 (d) and (e).

► Our purpose here has been to develop the set $\mathbb{Z}$ of integers, and derive its basic properties, from our chosen starting point. This we have now done, and having done so we should forget the apparatus of the construction.

Our procedure merely gives a mathematical way of relating the set of integers to the set of natural numbers, and a demonstration that there is no need to make intuitive assumptions about integers, since our basic assumptions about natural numbers already implicitly contain the standard properties of integers.

With this in mind, from here on integers will be integers and natural numbers will be non-negative integers. The next stage in our development is a very similar construction, the construction of the set of rational numbers.

Exercises

1. Using (P5), prove the following: if $P(n)$ is a statement about the natural number n such that $P(0)$ holds and $P(n')$ holds whenever $P(n)$ holds, then $P(n)$ holds for every natural number n.

2. Verify that addition on $\mathbb{N}$ is associative.
3. Verify that multiplication on $\mathbb{N}$ is commutative and associative and that the usual distributive law holds.
4. Prove that for every natural number n, either $n = 0$ or $n = m'$ for some natural number m. Hence, show that the product of two non-zero natural numbers is non-zero.
5. Prove that for every pair of natural numbers m and n, either $m \leqslant n$ or $n \leqslant m$.
6. Let $m, n \in \mathbb{N}$, with $m \neq 0$. Prove that there exists $r \in \mathbb{N}$ such that $n < rm$. (Hint: use Theorem 1.7.)
7. Show that multiplication of integers is well-defined, i.e. that if $(a, b) = (p, q)$ and $(c, d) = (r, s)$ then $(ac + bd, ad + bc) = (pr + qs, ps + qr)$.
8. Verify the commutative, associative and distributive laws for addition and multiplication on $\mathbb{Z}$.
9. Prove Remarks 1.11(b), (c), (d), (f), (g) and (h).
10. Let a be a fixed element of $\mathbb{Z}$. Let A be a subset of $\mathbb{Z}$ such that $a \in A$ and $x + 1 \in A$ whenever $x \in A$. Prove that $\{x \in \mathbb{Z} : a \leqslant x\} \subseteq A$.
11. Prove that every non-empty set of integers which is bounded below has a least element.
12. Prove that every non-empty set of integers which is bounded above has a greatest element.
13. Prove that for any pair of integers a and b, either $a \leqslant b$ or $b \leqslant a$.
14. Let $x, y \in \mathbb{Z}$ be such that $xy = 0$. Prove that $x = 0$ or $y = 0$.

1.2 Rational numbers

There are four standard arithmetic operations: addition, subtraction, multiplication and division. In $\mathbb{N}$ only the first and third are permitted in general, since it need not be the case, for natural numbers a and b, that $a - b$ or a/b are natural numbers. The set $\mathbb{Z}$ of integers is such that subtraction is permitted, but it is still the case that division may not work in $\mathbb{Z}$. Just as we took differences of natural numbers to represent integers, here the essence of the process is to use ordered pairs representing quotients. The standard way of representing rational numbers is as quotients of integers. Of course, the same rational number may be represented thus in many different ways. Consequently, in our formal procedure, the pairs (2, 3), (8, 12), (−50, −75) and (1000, 1500) will all represent the same object. This makes sense intuitively if we think of them as representing the familiar object 2/3. The formal details are similar to those of the earlier construction of the integers.

Definition

Let $a, c \in \mathbb{Z}$, and let $b, d \in \mathbb{Z}\backslash\{0\}$. We say that (a, b) is related to (c, d), written $(a, b) \# (c, d)$, if $ad = bc$. (Notice that this expresses what we would like, namely $a/b = c/d$, but as yet we cannot write fractions since we do not have a division operation on $\mathbb{Z}$.) Intuitively we have $(a, b) \# (c, d)$ if a/b and c/d represent the same rational number.

Now $\#$ is an equivalence relation. First, for any $a, b \in \mathbb{Z}$ with $b \neq 0$, we have $ab = ab$, so $(a, b) \# (a, b)$, and so $\#$ is reflexive. Second, suppose that $(a, b) \# (c, d)$, so that $ad = bc$. Then $cb = da$ clearly, so $(c, d) \# (a, b)$, and we have shown that $\#$ is symmetric. Third, suppose that $(a, b) \# (c, d)$ and $(c, d) \# (e, f)$, where $a, c, e \in \mathbb{Z}$ and $b, d, f \in \mathbb{Z}\backslash\{0\}$. Then $ad = bc$ and $cf = de$. We have

$$afd = adf = bcf = bde = bed,$$

so since $d \neq 0$ we can deduce $af = be$. Hence, $(a, b) \# (e, f)$ as required to show that $\#$ is transitive.

We define the set of *rational numbers* to be the set of equivalence classes under $\#$. As an example, the set $\{(a, b) : a, b \in \mathbb{Z},\ b \neq 0,\ b = 2a\}$ is an equivalence class (it is the class determined by $(1, 2)$).

Let us denote the equivalence class determined by (a, b) by $a\,\boldsymbol{/}b$. What we intend is that $a\,\boldsymbol{/}b$ should be the rational number that we intuitively think of as a/b.

► Our exposition has been deliberately modelled on the previous description of the construction of the integers, so as to emphasise the analogy. In algebraic terms, the construction of the integers involved introducing 'additive inverses' for the natural numbers (namely, negative integers), and now the construction of the rational numbers involves the introduction of 'multiplicative inverses' for the non-zero integers. In this case, of course, we must also introduce other new objects; besides requiring rational numbers of the form $1/b (b \in \mathbb{Z}, b \neq 0)$ we also have rationals of the form a/b which cannot be reduced (by cancellation) to a fraction with numerator 1.

Again, all we have so far is a set. It remains to describe the operations of addition and multiplication (and subtraction and division), to investigate the natural order of the rational numbers, and to examine the way in which the newly-defined set of rational numbers contains the set of integers.

Definition

Addition and *multiplication* of rational numbers are defined as follows. Let $a, b, c, d \in \mathbb{Z}$, with $b \neq 0$, $d \neq 0$.

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

$$a/b \times c/d = ac/bd.$$

Remarks 1.14

(a) The above definitions reflect our intuitive basis for rational numbers. We think of

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}, \quad \text{and} \quad \frac{a}{b}\times\frac{c}{d}=\frac{ac}{bd}.$$

(b) We must verify that these operations are well-defined. This time we take the case of multiplication and leave addition as an exercise. Suppose that $a/b = p/q$ and $c/d = r/s$. We must show that $ac/bd = pr/qs$, i.e. that $(ac, bd) \# (pr, qs)$, i.e. that $acqs = bdpr$. Now we have supposed that $a/b = p/q$, and consequently that $aq = bp$, and similarly we have $cs = dr$. Thus

$$acqs = aqcs = bpdr = bdpr,$$

as required.

(c) If a/b is a rational number, and x is a non-zero integer, then $ax/bx = a/b$. To see this we just note that $(ax, bx) \# (a, b)$, since $axb = bxa$.

(d) Addition and multiplication of rational numbers are commutative and associative, and the distributive law holds. These results are easy consequences of the corresponding properties of integers. To illustrate, let us take the distributive law. Let $a, b, c, d, e, f \in \mathbb{Z}$, with $b \neq 0$, $d \neq 0$, $f \neq 0$.

$$\begin{aligned}
&(a/b)\times(c/d+e/f)\\
&\quad=(a/b)\times((cf+de)/df)\\
&\quad=a(cf+de)/bdf\\
&\quad=(acf+ade)/bdf.
\end{aligned}$$

Also

$$\begin{aligned}
&(a/b\times c/d)+(a/b\times e/f)\\
&\quad=(ac/bd)+(ae/bf)\\
&\quad=(acbf+bdae)/bdbf
\end{aligned}$$