

# Numbers and Sets

ADAM KELLY

October 22, 2020

This set of notes is a work-in-progress account of the course ‘Numbers and Sets’, originally lectured by Professor Imre Leader in Michaelmas 2020 at Cambridge. These notes are not a transcription of the lectures, but they do roughly follow what was lectured (in content and in structure).

These notes are my own view of what was taught, and should be somewhat of a superset of what was actually taught. I frequently provide different explanations, proofs, examples, and so on in areas where I feel they are helpful. Because of this, this work is likely to contain errors, which you may assume are my own. If you spot any or have any other feedback, I can be contacted at [ak2316@cam.ac.uk](mailto:ak2316@cam.ac.uk).

## Contents

<b>0</b>	<b>Introduction</b>	<b>2</b>
0.1	Structure of the Course . . . . .	2
0.2	Books . . . . .	2
0.3	Example Sheets . . . . .	3
0.4	A Brief Note About These Notes . . . . .	3
<b>1</b>	<b>Elementary Number Theory</b>	<b>4</b>
1.1	The Peano Axioms . . . . .	4
1.1.1	Addition . . . . .	5
1.1.2	Order . . . . .	5
1.1.3	Multiplication . . . . .	6
1.2	Strong Induction . . . . .	6
1.3	The Integers and Rationals . . . . .	7

## §0 Introduction

Numbers and sets is one of the first course in pure mathematics that you will take as an undergraduate at Cambridge. In a sense, it is the ‘starting course’, in that it will introduce you to the ‘pure maths’ way of thinking about things. This introduction will happen through the lense of thinking about objects, beginning with the natural and real numbers. You will be introduced to the ‘thoughtful way’ of thinking about such objects, that you can carry through to almost every other course in pure mathematics.

### §0.1 Structure of the Course

This course is divided into four sections.

1. *Elementary Number Theory*

This is a section that almost everybody enjoys. We deal with number theory first, which is elementary not in the sense that it is easy but in the sense that it is our ‘first steps’ in the subject. The main aim of this section is to get used to the additive and multiplicative structure of the natural numbers.

It is like that some of you will be familiar with this material already, but nothing in this section will be assumed, and everything will be built from the ground up.

2. *The Reals*

This section has a different perspective, centering on the questions of *what is a real number* and *what can we assume about them?* This is one of the harder parts of this course, and many of the definitions contain a subtlety that is not present in other sections.

3. *Sets and Functions*

This is a ‘terminology’ section. There is no exciting theorems, mostly notation, definitions, and so on. It is a short section, but it is somewhat boring in that sense.

4. *Countability*

This section is best described as ‘fun with infinite sets’. It is to do with the concepts introduced in section 3 (in the sense that we are thinking about sets and functions), but it has a very different flavour. You will find results in this section that are both interesting and surprising. Almost everyone likes this section.

Everything in the sections above makes up the ‘course’. If you are wondering what is examinable, it will be everything that was lectured. It is possible that this set of ‘lecture notes’ will contain additional content that was both not in lectures and not examinable. If you want to be sure whether something you are reading here or elsewhere is examinable, you can get a more formal answer in [the schedules](#).

### §0.2 Books

As with most mathematics courses in Cambridge, you will not need a textbook to follow this course. What is covered in lectures is enough to do both the example sheets and the examinations for this course. Still, you might find that a textbook can provide a different perspective, additional worked examples, and additional material that you may find informative, helpful or fun.

In particular, the following books are quite relevant/good, but there is no expectation that you will look at these.

- R. T. Allenby, *Numbers and Proofs*.

This book is readable, easy to understand and clear.

- A. G. Hamilton, *Numbers, Sets and Axioms*.

Another readable and clear book, but with a different flavour to the previous book.

- H. Davenport, *The Higher Arithmetic*.

This book can be thought of as showing ‘where things go next’. It is very interesting, and goes quite a bit beyond this course. It is worth noting however that this book contains no exercises.

You should be able to find all of these books in either your college library or the university library.

### §0.3 Example Sheets

As is normal for a 24 lecture course, there will be 4 example sheets. You should be able to have a good go at the first one after lecture 3 or 4.

### §0.4 A Brief Note About These Notes

This set of notes differs from what was lectured in a number of areas. I have attempted to briefly outline these changes below.

In the original lecture course, there was two lectures that (informally) introduced the idea of a proof, along with examples and non-examples of what a proof is. This material has been purposefully excluded, and familiarity with proofs (and common logical notation such as  $\forall$ ,  $\exists$ , and  $\implies$ ) is assumed. If you are interested in reading a brief introduction to proofs, I will direct you to this [quite readable introduction](#).

I have also included additional exposition on the Peano axioms, along with a more detailed look at how addition, multiplication, etc are defined. In the original lectures, this material was purposefully omitted. The exposition included in these notes closely follows the development in Tao’s *Analysis I* (see the bibliography).

## §1 Elementary Number Theory

Number theory is the branch of mathematics that studies the properties of *numbers*, with a particular emphasis on the natural numbers  $\mathbb{N}$ , the integers  $\mathbb{Z}$  and occasionally the rationals  $\mathbb{Q}$ . In this section, we will study some of the *additive* and *multiplicative* structure of the integers, looking at divisors, primes and tools such as modular arithmetic.

One of the aims of this course (and this section in particular) is to study numbers ‘from the ground up’, being quite careful about what we assume. This goal immediately presents us with a question: what exactly is a ‘number’?

### §1.1 The Peano Axioms

What are the natural numbers? Intuitively, we might say that they are a set<sup>1</sup>  $\mathbb{N} = \{1, 2, 3, \dots\}$ , created by starting at 1 and counting forward indefinitely, each time obtaining an object distinct from all of the previous ones. This does answer our question (a natural number is any element of  $\mathbb{N}$ ), but has created a series of other questions. For example, what does it mean to ‘count forward’, and how can it be done ‘indefinitely’? How are we allowed to use these natural numbers, in regard to defining things like addition and multiplication?

Instead of attempting to answer these questions using our informal, intuitive definition of the natural numbers, we will instead use a definition that is more precise. Namely, we will define the natural numbers using the Peano axioms. We will state the rules or *axioms* that natural numbers satisfy, which will define the natural numbers in terms of *how they work*, rather than *what they are*. After clearly setting out this definition, we will be in a much stronger position to write concrete mathematical proofs about the natural numbers.

#### Definition 1.1 (Peano Axioms)

The **natural numbers** are a set  $\mathbb{N}$ , along with a function  $S : \mathbb{N} \rightarrow \mathbb{N}$  and an object ‘1’ satisfying the following axioms:

1.  $1 \in \mathbb{N}$ .
2. If  $n \in \mathbb{N}$ , then  $S(n) \in \mathbb{N}$ .
3.  $S(n) \neq 1$  for every  $n \in \mathbb{N}$ .
4. If  $n, m \in \mathbb{N}$  and  $n \neq m$ , then  $S(n) \neq S(m)$ .
5. *Induction.* Let  $P(n)$  be any property about a natural number  $n$ . Suppose that  $P(0)$  is true, and suppose that whenever  $P(n)$  is true,  $P(S(n))$  is also true. Then  $P(n)$  is true for every natural number  $n$ .

This should match with our original, informal definition of the natural numbers. We have formalized the ‘counting forward’ process with the *successor function*  $s(n)$ .

**Remark.** We are going to assume various things about the way we write down natural numbers using the decimal system. You can assume that when we write something like  $n = 3$ , we really mean  $n = S(S(1))$  etc.

<sup>1</sup>We will look at sets later in the course, but an informal familiarity will be assumed from the beginning

### §1.1.1 Addition

Now we have defined natural numbers, but as of yet we can do nothing more look upon them fondly and increment them using the function  $S(n)$ . We will now begin to remedy that by defining addition and multiplication.

#### Definition 1.2 (Addition)

We define **addition** to be an operation  $+$  such that for  $m, n \in \mathbb{N}$ , we have  $m + 1 = S(m)$ , and  $m + (n + 1) = (m + n) + 1$ .

This definition defines addition for all natural numbers by induction. We are now able to state and prove various properties of addition.

#### Proposition 1.3 (Properties of Addition)

For all  $a, b, c \in \mathbb{N}$ . Then

- (i) *Addition is commutative.*  $a + b = b + a$ .
- (ii) *Addition is associative.*  $(a + b) + c = a + (b + c)$ .
- (iii) *Cancellation law.* If  $a + b = a + c$  then  $b = c$ .

*Proof Sketch.* Use induction.<sup>a</sup>

□

<sup>a</sup>The proofs for these sorts of statements tend to be slightly dull and laborious, and for this reason they have been excluded. If you wish to read them, I encourage you to consult a textbook/some other reference material.

### §1.1.2 Order

We can now use addition to define an ordering on the natural numbers.

#### Definition 1.4 (Ordering of the Natural Numbers)

Let  $n, m \in \mathbb{N}$ . We say that  $n$  is **greater than or equal to**  $m$ , written  $n \geq m$  if and only if  $n = m$  or  $n = m + a$  for some  $a \in \mathbb{N}$ . We say  $n$  is **strictly greater than**  $m$  if  $n \geq m$  and  $n \neq m$ .

#### Proposition 1.5 (Properties of Ordering)

Let  $a, b, c \in \mathbb{N}$ . Then

- (i) *Order is reflective.*  $a \geq a$ .
- (ii) *Order is transitive.* If  $a \geq b$  and  $b \geq c$ , then  $a \geq c$ .
- (iii) *Order is anti-symmetric.* If  $a \geq b$  and  $b \geq a$ , then  $a = b$ .
- (iv) *Addition preserves order.*  $a \geq b$  if and only if  $a + c \geq b + c$ .
- (v)  $a > b$  if and only if  $a \geq b + 1$ .

**Proposition 1.6 (Trichotomy)**

Let  $a$  and  $b$  be natural numbers. Then exactly one of the following is true:  $a < b$ ,  $a = b$  or  $a > b$ .

**§1.1.3 Multiplication**

We can also define another familiar operation, multiplication, in the same inductive/recursive fashion that we defined addition.

**Definition 1.7 (Multiplication)**

We define **multiplication** to be an operation  $\times$  such that for  $m, n \in \mathbb{N}$ ,  $m \times 1 = m$ , and  $m \times (n + 1) = (m \times n) + m$ .

As before, induction implies that this is defined for all natural numbers. It also guarantees that multiplying two natural numbers is a natural number.

**Notation.** We will use  $a \times b = a \cdot b = ab$  when referring to multiplication.

**Proposition 1.8 (Properties of Multiplication)**

For all  $a, b, c \in \mathbb{N}$ . Then

- (i) *Multiplication is commutative.*  $a \times b = b \times a$ .
- (ii) *Multiplication is associative.*  $(a \times b) \times c = a \times (b \times c)$ .
- (iii) *Distributive law.*  $a \times (b + c) = a \times b + a \times c$ .
- (iv) *Cancellation law.* If  $a \times b = a \times c$  then  $b = c$ .
- (v) *Multiplication preserves order.* If  $a < b$ , then  $a \times c < b \times c$ .

**Remark.** The final two statements in the proposition above, the cancellation law and that multiplication preserves order, only hold because we are dealing with natural numbers. These properties do not hold in general if we allow  $a, b$  or  $c$  to be integers.

We could go further and define other common operations such as exponentiation, factorials and so on, all of which can be defined in the same fashion. However, in the interest of space, these definitions have been omitted.

**§1.2 Strong Induction**

There is a more useful form of induction that can be used, now that we have defined an ordering on the natural numbers.

**Proposition 1.9 (Strong Induction)**

Suppose that we have some property  $P(n)$  about a natural number  $n$ . If we have  $P(1)$ , and for all  $n \in \mathbb{N}$  we have that  $P(m)$  for  $m \leq n$  implies  $P(n + 1)$ , then  $P(n)$  holds for all  $n \in \mathbb{N}$ .

*Proof.* This follows from ordinary induction using the property “ $P(n)$  for all  $m \leq n$ ”.  $\square$

Informally, the principle of strong induction means that whenever we are proving some property  $P(n)$  holds for all  $n \in \mathbb{N}$  by induction, we can feel free to assume that  $P(m)$  holds for  $m \in \mathbb{N}$  with  $m < n$ .

**Remark** (For Pedants). Technically, we don’t need to check the case  $P(1)$  separately, as it is implied by the condition if suitably interpreted. Still, it’s safer to just check  $P(1)$ .

Some other equivalent but useful<sup>2</sup> forms of induction are listed below. Let  $P(n)$  be a property, then

- *Existence of a Minimal Counterexample*

If  $P(n)$  is false for some  $n \in \mathbb{N}$ , then there exists  $n_0 \in \mathbb{N}$  such that  $P(n_0)$  is false but  $P(m)$  is true for all  $m < n_0$ .

- *The Well-Ordering Principle*

If  $P(n)$  is true for some  $n \in \mathbb{N}$ , then there exists a minimal  $n_0$  such that  $P(n_0)$  is true.

### §1.3 The Integers and Rationals

The previous section defined the natural numbers, along with some ways that we can use them. We will now go one step further and define the *integers*, and the *rationals*.

#### Definition 1.10 (Integers)

The **integers** are a set  $\mathbb{Z}$  consisting of all symbols  $n$ ,  $-n$  and  $0$ , where  $n \in \mathbb{N}$ .

We can then define addition, multiplication and subtraction in (and subtraction) on the integers by extending our definition on the natural numbers in the obvious way. We can also check that the properties of addition we had before still hold. There are some additional properties that the integers have.

#### Proposition 1.11 (Algebraic Properties of the Integers)

Let  $a, b \in \mathbb{Z}$ . Then<sup>a</sup>

- (i) *Identity.*  $a + 0 = a$ .
- (ii) *Existence of an Additive Inverse.* For all  $a \in \mathbb{Z}$ , there exists  $b \in \mathbb{Z}$  such that  $a + b = 0$ .

<sup>a</sup>These properties imply that the integers are a *group*.

*Proof.*  $a + 0 = a$  holds automatically due to our definition of addition on the integers. Then, we always have a  $b \in \mathbb{Z}$  such that  $a + b = 0$ , as we can let  $b = -a$ .  $\square$

We also obtain another interesting property of multiplication.

<sup>2</sup>Some texts will claim that we can replace the induction axiom in Peano axioms with one of these other forms. This is incorrect, and typically one will need to add additional axioms alongside to keep the set of axioms equivalent.

**Proposition 1.12 (Zero Product Law)**

Let  $a$  and  $b$  be integers such that  $a \times b = 0$ . Then either  $a = 0$ ,  $b = 0$  or both.

*Proof.* Assume for the purposes of contradiction that both  $a \neq 0$  and  $b \neq 0$ . Then we must have either  $a > 0$  or  $a < 0$  by trichotomy. If  $a > 0$ , then  $a \times b > 0$  if  $b > 0$ , or  $a \times b < 0$  if  $b < 0$ . Otherwise, if  $a < 0$ , then  $a \times b < 0$  if  $b > 0$ , or  $a \times b > 0$  if  $b < 0$ . These are all possible cases, and thus we never have that  $a \times b = 0$ . Thus at least one of  $a$  and  $b$  must be zero.  $\square$

**Remark (Caveats).** We noted earlier that there were some properties of the natural numbers that don't hold over the integers. Specifically, if we have  $a < b$  for  $a, b \in \mathbb{Z}$ , and we multiply by a negative number, then the order is no longer preserved (it is switched). Also, the cancellation law only applies when we are cancelling a non-zero integer.

We can now use the integers to define the *rationals*.

**Definition 1.13 (Rationals)**

The **rationals** are a set  $\mathbb{Q}$  of expressions  $a/b$  for some  $a, b \in \mathbb{Z}$ , with  $b \neq 0$ . We will define equality between rationals such that  $a/b = c/d \iff ad = bc$ .

This definition implicitly defines  $\mathbb{Q}$  using *equivalence classes*, which will be discussed later. We need to be slightly more careful in defining addition on  $\mathbb{Q}$ , as we will need to ensure that it respects the equality relation between rationals.

**Definition 1.14 (Addition on  $\mathbb{Q}$ )**

For  $a/b$  and  $c/d \in \mathbb{Q}$ , we define addition such that

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.$$

We will now need to explicitly check that this definition is valid.

**Proposition 1.15**

Addition is well defined on  $\mathbb{Q}$ .

*Proof.* Let  $a/b = a'/b'$  and  $c/d = c'/d'$  be rationals. We show that

$$\begin{aligned} \frac{a}{b} + \frac{c}{d} &= \frac{a'}{b'} + \frac{c'}{d'} \\ \iff \frac{ad + bc}{bd} &= \frac{a'd' + b'c'}{b'd'} \\ \iff (ad + bc)(b'd') &= (a'd' + b'c')(bd) \\ \iff adb'd' + bcb'd' &= a'd'bd + b'c'bd \\ \iff (ab')dd' + (cd')bb' &= (a'b)d'd + (c'd)bb', \end{aligned}$$

which follows from  $ab' = a'b$  and  $cd' = c'd$ .  $\square$

To see why such a check was needed, consider the following example.



**Example 1.16**

We *cannot* define an operation on  $\mathbb{Q}$  sending  $a/b \rightarrow a^2/b^3$ , as we would have  $1/2 \rightarrow 1/8$  and  $2/4 \rightarrow 4/64 = 1/16$ , which is inconsistent.

We can then define multiplication in the same way as it was defined for integers, and we can check that all of the usual properties still hold. We can also define ordering, where  $a/b < c/d$  if  $ad < bc$ . The rules from ordering  $\mathbb{Z}$  still hold.

With all of these definitions in place, we can now start looking at some of the more interesting properties of numbers.

## Bibliography

- T. Tao, *Analysis I*

This book provides discussion of the Peano axioms, along with some relevant proofs that were (purposefully) excluded from the lectures. The treatment of the Peano axioms in these notes follow this exposition closely.