Making up Numbers
A History of Invention in Mathematics

Ekkehard Kopp

Making up Numbers offers a detailed but accessible account of a wide range of mathematical ideas. Starting with elementary concepts, it leads the reader towards aspects of current mathematical research. Ekkehard Kopp adopts a chronological framework to demonstrate that changes in our understanding of numbers have often relied on the breaking of long-held conventions, making way for new inventions that provide greater clarity and widen mathematical horizons. Viewed from this historical perspective, mathematical abstraction emerges as neither mysterious nor immutable, but as a contingent, developing human activity.

Chapters are organised thematically to cover: writing and solving equations, geometric construction, coordinates and complex numbers, attitudes to the use of ‘infinity’ in mathematics, number systems, and evolving views of the role of axioms. The narrative moves from Pythagorean insistence on positive multiples to gradual acceptance of negative, irrational and complex numbers as essential tools in quantitative analysis.

Making up Numbers will be of great interest to undergraduate and A-level students of mathematics, as well as secondary school teachers of the subject. By virtue of its detailed treatment of mathematical ideas, it will be of value to anyone seeking to learn more about the development of the subject.

As with all Open Book publications, this entire book is available to read for free on the publisher’s website. Printed and digital editions, together with supplementary digital material, can also be found at www.openbookpublishers.com

Cover images from Wikimedia Commons. For image details see captions in the book.

Cover Design by Anna Gatti.
CHAPTER 7

Number Systems

If a man’s wit be wandering, let him study the mathematics; for in demonstrations, if his wit be called away never so little, he must begin again.

Sir Francis Bacon, ‘Of Studies’ in: Essays, 1597

Summary

Chapters 1-4 described key aspects of the historical evolution of the number concept up to the early nineteenth century, largely driven by the realisation that the solution of various problems (first posed verbally but increasingly expressed via various types of equation) would lead far beyond the Pythagorean concept of ‘multiples of the unit’ as the only entities regarded as ‘numbers’. By the early 1800s, these developments had led to the Fundamental Theorem of Algebra, clarifying the basic structure of polynomials. This had required the extension of the number concept to complex numbers.

Chapters 5 and 6 outlined two key episodes in the history of mathematicians’ struggle with the concept of infinity, arising in the analysis of ‘continuous magnitudes’ to understand the dynamics of instantaneous change and the summation of infinitely many terms. The development of Calculus techniques addressed both problems with a considerable measure of success, but only by postulating infinitesimal quantities whose existence could not be established convincingly. In the nineteenth century, these quantities were finally ‘banished’ through conceptual advances made mainly in Paris and Berlin, giving a central role to the notions of limit and continuity of functions. This, in turn, brought into much sharper focus the question of the nature of the underlying continuum, represented by the geometric ‘number line’ inherited from geometry.

The present chapter deals with several aspects of number systems. We review the familiar systems of numbers encountered on this journey. The natural (or counting) numbers are taken for granted, but we explore their structure a little further, highlighting, in particular, the Principle of Induction. Our initial interest in induction is as a proof technique; in Chapter 8 it will be seen as a fundamental property of the set of natural numbers. Next we outline the scheme devised by Richard Dedekind (1831-1916) to produce rigorous definitions of integers and rationals and their arithmetic, using only
the familiar properties of the natural numbers, while showing that these properties are inherited and extended in the new number systems.

The next two sections contrast the differing approaches of Dedekind and Georg Cantor (1845-1918) to the development of the real number system. Both started with the rationals. Dedekind emphasised the analogy with the order properties of the line, while Cantor employed (classes of) Cauchy sequences to define each real number, simplifying the extension of arithmetical properties from the rationals to the reals.

Finally, we consider infinite decimal expansions, a concept that, while familiar from ‘recurring’ decimal expansions encountered at school, has hidden depths that repay closer study on several counts. Rationals and irrationals give rise to two distinct (infinite) classes of expansions, and we indicate why the irrationals seem to be ‘more numerous’. We also identify constructible, algebraic and transcendental numbers, identifying how solutions of the ‘three famous problems’ of antiquity fit into these classes.

1. Sets of numbers

We have so far attached names to six different types of number, developed and explored over two millennia—albeit with rather variable degrees of precision. I will employ the language of sets to describe the collection of numbers in each category. This practice is of relatively recent origin, but is well-established in common parlance today—not least because of its (initially quite controversial) introduction into primary school teaching in many developed countries during the 1960s. I will use this ‘naive set theory’ informally, primarily to have a convenient notation and terminology, rather than engage with the logical formalities of any abstract theory of sets.

The six collections of numbers highlighted below are examples of sets whose members are various types of number. But we can imagine many different collections of objects, concrete or abstract, and it is convenient to have a simple terminology to identify them.\(^1\)

Here is a brief review of this terminology and notation:

By a set \(S\) we will understand any collection of distinct objects (mental or physical), together with a membership rule enabling us to decide whether a given object \(x\) is a member of the collection or not. If it is, we write \(x \in S\) (expressed variously as ‘\(x\) is an element (or member) of \(S\)’, or ‘\(x\) is in \(S\)’, or ‘\(x\) belongs to \(S\)’); if it is not, we write \(x \notin S\) (‘\(x\) is not in \(S\)’). The set \(S\) is an object in its own right—so \(S\) can itself be a member of some other set.

---

\(^1\)In 1895, Georg Cantor defined the term set as follows: ‘By a set \(M\) we understand every gathering together into a whole of definite, distinct objects \(m\) (which are called the ‘elements’ of the set) of our perception or of our thought.’
For a finite set $S$ one might simply list its elements—if these are $a, b, c$, write $S = \{a, b, c\}$. We write $\{x\}$ for the set containing just the element $x$. Such a set is called a singleton.

We define the empty set $\emptyset$ as a set that has no elements—this can be done by using a contradictory membership rule: for example, if $P(x)$ is a statement involving the variable $x$, then we may write $\{x : P(x)\}$ to specify the set of all possible elements $x$ for which the statement $P(x)$ is true. Then $\emptyset = \{x : x \neq x\}$, specifies ‘the set of all $x$ such that $x$ does not equal $x$’. Since there are no such $x$, the set $\emptyset$ has no elements. A set is non-empty if it is not the empty set.

Comparison of sets introduces further basic notation and terminology:

Given two sets $A, B$, they are equal (written $A = B$) if they contain exactly the same elements; that is, every element of $A$ is an element of $B$ and vice versa.

Call $A$ a subset of $B$ (and write $A \subseteq B$) if every element of $A$ is an element of $B$. This includes the possibility that the two sets are equal. The empty set $\emptyset$ is a subset of every set.

Call $A$ a proper subset of $B$ (written $A \subset B$) if every element of $A$ is an element of $B$, but not vice versa – so that $B$ contains elements that are not in $A$. In this case we write the set difference as $B \setminus A$. For example, $A = \{1, 2\}$ is a proper subset of $B = \{1, 2, 3\}$, and $B \setminus A = \{3\}$.

We write $A \cup B$ for the union of sets $A$ and $B$. This is the set whose elements belong to either $A$ or $B$ (or both). The set of all elements that $A$ and $B$ have in common is called their intersection, written as $A \cap B$. If two sets $A$ and $B$ have no elements in common (so that $A \cap B = \emptyset$) they are disjoint.

We also extend these definitions to a sequence $(A_n)_{n \geq 1}$ of sets, denoting the union by $\bigcup_{n \geq 1} A_n$ and the intersection by $\bigcap_{n \geq 1} A_n$.

The types of number encountered so far are:

Positive whole numbers—evolving from the ‘counting numbers’, or the unit and its multiples, and now known more formally as the natural numbers. The set of all natural numbers is denoted by $\mathbb{N}$.

Integers—extending the natural numbers to include zero and negative numbers. The resulting set of all integers is written as $\mathbb{Z}$.

Rational numbers—deriving from the Greek notion of ‘commensurable lengths’, these are expressed as ratios of integers without common factors; or more colloquially as ‘fractions in lowest form’. We write the set of all rational numbers as $\mathbb{Q}$.
Irrational numbers—deriving from ‘incommensurable lengths’ to distinguish them from the rationals. We have yet to give them a satisfactory definition as numbers.

Real numbers—described, until now, only by reference to points that can be marked on an unlimited geometric ‘number line’. We have claimed that this comprises all rational or irrational numbers, taken together. The set of all real numbers will be denoted by \( \mathbb{R} \).

Complex numbers—depicted, by analogy, as points in the plane, they may be regarded more formally as ordered pairs of real numbers, for which sums and products are formed by Hamilton’s explicit rules. Their full definition will therefore follow without difficulty once the concept of ‘real number’ has been defined consistently and independently of any geometric description. The set of all complex numbers is denoted by \( \mathbb{C} \).

The sets \( \mathbb{N} \), \( \mathbb{Z} \), \( \mathbb{Q} \), \( \mathbb{R} \) are today firmly embedded in our culture and daily experience. While the set \( \mathbb{C} \) may be less familiar, complex numbers have been central to many areas of mathematics and to progress in several areas of science and engineering, especially in applications of electromagnetism and in electronics, for at least the past 150 years. We will now look at these five sets more abstractly, as objects in their own right, and ask how they relate to each other.

Various examples have illustrated how the basic arithmetical operations (+, ×) and their inverses (−, ÷) are applied in computations and to obtain the solutions of various types of equations. We also know how the order relation (<) is applied to compare natural numbers, integers, and rational or real numbers, and how this ordering interacts with addition and multiplication. It will be shown (in the Appendix to Chapter 8) that the system of complex numbers as a whole cannot be ordered in a way that is compatible with addition and multiplication.

As far as the elements of the sets are concerned, we can ‘list’ the set of integers as a doubly infinite sequence \( \mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\} \), while the set \( \mathbb{Q} \) of rationals can, in turn, be regarded as the collection of all fractions \( \frac{m}{n} \), where \( m \) is any integer and \( n \) a natural number having no factors in common with \( |m| \), so that the fraction is expressed in its ‘lowest form’.

Observe that sums and products of natural numbers are again natural numbers (so that performing addition and multiplication in \( \mathbb{N} \) cannot take us beyond \( \mathbb{N} \)). The same is true for \( \mathbb{Z} \) and \( \mathbb{Q} \) : for example, the sum of two rational numbers, expressed as ratios (in lowest form) of integers, \( \frac{m}{n} \) and \( \frac{p}{q} \), is \( \frac{mq+np}{nq} \), which is again a ratio of two integers, as is their product \( \frac{mp}{nq} \). We say that both number systems are closed under addition and multiplication. Unlike \( \mathbb{N} \), the set of integers \( \mathbb{Z} \) is also closed under subtraction, but not under division (these are the inverse operations to addition and multiplication), while \( \mathbb{Q} \) is closed under subtraction, and \( \mathbb{Q} \setminus \{0\} \) is closed under division. All
this (though perhaps not the terminology) should be entirely familiar from schooldays.

However, the product of two irrational numbers need not be irrational – consider $(\sqrt{2})(\sqrt{2}) = 2$, for example. Since it is not closed under multiplication, the set of all irrational numbers will not be treated as a number system in the same fashion as $\mathbb{N}$, $\mathbb{Z}$, or $\mathbb{Q}$. A major task in this Chapter will be to incorporate this set, together with $\mathbb{Q}$, in the single number system $\mathbb{R}$, whose elements are described arithmetically. Two solutions to this occupy Sections 4 and 5, while in the final three short sections we briefly consider other methods of distinguishing between rationals and irrationals as well as between different types of irrational numbers.

2. Natural numbers

2.1. The principle of induction. We have treated the set of natural numbers $\mathbb{N} = \{1, 2, 3, \ldots\}$ as given: in other words, it simply exists and we can identify its elements successfully. This assumption is implicit in the process of counting, and corresponds to a perception of $\mathbb{N}$ that was universal from the time of the Pythagoreans until well into the nineteenth century. Until then, mathematicians saw no need to devise a more formal framework in which to derive elementary properties of the set $\mathbb{N}$. This point of view was perhaps expressed most bluntly in a famous phrase attributed to the influential Leopold Kronecker (1823-1891) in Berlin:

*Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk.*

(God created the natural numbers, all else is the work of man).

However, $\mathbb{N}$ is an infinite set, as every natural number $n$ has an immediate successor $n + 1$, as was observed in the Prologue. Therefore specific techniques are needed to analyse it (and its arithmetic) more fully to answer certain types of question. The most important of these is the Principle of Induction. Intuitively, this seeks to make the statement ‘and so on’ more precise. It can be pictured as consecutive dominoes falling in a never-ending row, or as climbing an infinite ladder step by step, from the bottom rung. Or simply by seeking to count numbers one-by-one ‘forever’.

As a method of proof this principle has a long history, but it was typically used implicitly, and often inconsistently.\(^2\) Perhaps the most explicit early example of its use can be found in the work of Levi ben Gershon (1288-1344) – see [25] for details. In the seventeenth century Blaise Pascal used induction explicitly when justifying the properties of his well-known Pascal

\(^2\)Mathematical induction concerns a specific method of proof, and should not be confused with inductive logic, which, in philosophy, is concerned with measures of evidential support for assertions (see the entry on Inductive Logic in the online Stanford Dictionary of Philosophy).
triangle (see Figure 30, page 122). Fermat frequently used the closely related method of ‘infinite descent’, using the fact that for any $n$ there are only finitely many different natural numbers less than $n$. However, it was only at the end of the nineteenth century that the Induction Principle was taken as an axiom in the work of Giuseppe Peano (1858-1932). This will be discussed in Chapter 8.

The basic idea is simple: suppose that we can verify that a given statement $P(n)$ about the natural number $n$ holds when $n = 1$ (i.e. $P(1)$ is true) and that we can prove the following inductive step: for any $n$, the truth of $P(n)$ implies the truth of $P(n + 1)$. Then the Principle claims that $P(n)$ must hold for all natural numbers.

The following two simple examples illustrate the use of the Induction Principle:

(i) $1 + 3 + 5 + \ldots + (2n - 1) = n^2$ for every $n$ in $\mathbb{N}$. (Recall the ‘pebble proof’ of this claim in Chapter 1)

\[
\text{Proof: Let } P(n) \text{ be the statement: } 1 + 3 + 5 + \ldots + (2n - 1) = n^2. \text{ Then } P(1) \text{ becomes the statement } 1 = 1, \text{ which is true.}
\]

Next, take $n$ in $\mathbb{N}$ and assume that $P(n)$ holds. This implies $P(n + 1)$, because

\[
1 + 3 + \ldots + (2n - 1) + (2n + 1) = n^2 + (2n + 1) = (n + 1)^2 = P(n + 1).
\]

By the Induction Principle, $P(n)$ holds for every natural number.

(ii) Bernoulli’s inequality: Fix a real number $a > -1$. Then $(1+a)^k \geq 1+ka$ for every natural number $k$.

\[
\text{Proof: For each } k \geq 1, \text{ let } P(k) \text{ be the statement: if } a > -1, \text{ then } (1+a)^k \geq 1+ka.
\]

Again, $P(1)$ is true: $(1+a)^1 = 1+a$.

Assume that $P(k)$ holds. Note that $a > -1$ ensures that $(1+a)$ is positive. As $a^2 \geq 0$, we obtain

\[
(1+a)^{k+1} = (1+a)^k(1+a) \geq (1+ka)(1+a) = 1 + (k+1)a + ka^2 \geq 1 + (k+1)a,
\]

so that $P(k + 1)$ holds.

Again, by induction, $P(n)$ holds for every natural number $n$.

Bernoulli’s inequality enables us to verify formally that $\lim_{n \to \infty} x^n = 0$ when $|x| < 1$. (See Achilles and the Tortoise in Chapter 5.)
Proof: As $|x| < 1$, we can write $|x| = \frac{1}{1+b}$ for some $b > 0$. Let $\varepsilon > 0$ be given. By Bernoulli’s inequality,

$$|x|^n = \frac{1}{(1+b)^n} \leq \frac{1}{1+nb}.$$ 

Hence $|x^n| < \frac{1}{nb} < \varepsilon$ for all $n \geq N$, provided that we choose $N > \frac{1}{b\varepsilon}$.

So $\lim_{n \to \infty} x^n = 0$.

The Induction Principle implies another property of $\mathbb{N}$ that may seem blindingly obvious:

**Well-Ordering Property (WO) of $\mathbb{N}$**

Every non-empty subset of $\mathbb{N}$ has a least element.

Proof: We prove this by contradiction, using the Induction Principle. Suppose that (WO) is false for the set $\mathbb{N}$. Then it would have a non-empty subset $S$ with no least element. Let $P(n)$ be the statement “$i \notin S$ for all $i \leq n$”. In other words, $P(n)$ holds if $S$ does not contain any of the natural numbers $1, 2, 3, ..., n$. In particular, $1 \notin S$, since if it were in $S$ it would be its least element. Therefore $P(1)$ is true. For the inductive step, assume that $P(n)$ is true, so that none of $1, 2, 3, ..., n$ belong to $S$. In that case, $n + 1$ cannot belong to $S$, since otherwise it would be its least element. But this means that $P(n + 1)$ is true, and by induction, $P(n)$ holds for all $n$ in $\mathbb{N}$. This means that $S$ must be empty, contradicting our assumption that the (WO) is false. Therefore (WO) must hold for $\mathbb{N}$.

We have proved that the Induction Principle implies (WO). In fact the two are logically equivalent—we omit the other half of the proof.

In some contexts another version of induction is useful. The **Strong Induction Principle** uses the following induction step instead: assume that $P(m)$ is true for all $m \leq n$ and prove that $P(m + 1)$ is true. If this can be shown, then the Strong Induction Principle asserts that $P(n)$ holds for all $n$ in $\mathbb{N}$.

We will use this version of the Principle repeatedly below. The prefix ‘strong’ does not mean that we can prove more with this version than with that stated earlier. It refers to the fact that we make a stronger assumption in the induction step. The two versions of the Principle are logically equivalent (this is proved in MM). Note, however, that we have made no attempt to prove either version from earlier statements.

### 2.2. Prime numbers as building blocks.

The set $\mathbb{N} = \{1, 2, 3, ...\}$ is familiar from primary school. We learn early on that amongst the natural numbers there are some special ones: **prime numbers**. These are the natural numbers **greater than** 1 that have no proper divisors. In other words, a
prime number $p$ is divisible only by 1 and by itself. Dividing $p$ by 1 changes nothing, and dividing $p$ by itself results in 1.

All other natural numbers $n > 1$ are called composite. So a composite number $n$ has a proper divisor $a$, that is, a natural number greater than 1 but less than $n$ (written $1 < a < n$), such that $n = a \times b$ for some natural number $b > 1$. The divisors $a$ and $b$ are called factors of $n$.

For a long time 1 was treated as a prime number (since it certainly has no factors!) and this practice fits well with the use of the term in ordinary language. But this ended more than a century ago. A mathematical definition should be judged by its usefulness in identifying the nature of the objects being discussed. What we call the Fundamental Theorem of Arithmetic below will highlight one rather important reason why it is better not to include 1 among the prime numbers. So we will insist that a prime number must be greater than 1.

The first significant general result learnt at school about prime numbers is that any natural number greater than 1 has a prime divisor. If $n$ is prime, it is its own prime divisor. If $n$ is composite, then it must have at least one prime factor.

To see why this must be true we will use strong induction: suppose we have proved that every natural number less than some number $n$ has a prime divisor. If $n$ is prime there is nothing to prove. If $n$ is composite then $n = a \times b$, where both factors $a$ and $b$ are greater than 1. But this means that $a < n$, so that $a$ has a prime divisor by our inductive assumption. Call this divisor $p$. But if $p$ divides $a$, it also divides $a \times b = n$. This means that $n$ has a prime factor. Hence by strong induction every natural number, has at least one prime divisor.

This result illustrates how to decompose any natural number $n$ into prime factors. If $n$ is prime, nothing needs to be done. If $n$ is composite it has at least one prime factor, as shown above. Suppose now that $p_1$ is the smallest of these, so that we can write $n = p_1 \times n_1$ for some natural number $n_1$ strictly between 1 and $n$. If $n_1$ turns out to be prime, we are done. Otherwise, it has a smallest prime factor $p_2$ and $n_1 = p_2 \times n_2$ for some natural number $n_2$ strictly between 1 and $n_1$. Continuing in this way, we obtain a strictly decreasing sequence $n_1, n_2, \ldots$ of numbers between 1 and $n$ and, since $n$ is finite, this must be a finite sequence (Fermat’s method again): after finitely many steps ($k$ say) we will have $n_{k-1} = p_k \times n_k$ with $p_k$ prime and $n_k = 1$. It follows that $n = p_1 \times p_2 \times \ldots \times p_k$.

This simple procedure provides a prime factorisation of $n$.

Prime numbers are the basic building blocks of $\mathbb{N}$. The usefulness of this statement turns on the important question whether the above decomposition of $n$ into prime factors is unique. If we were to treat 1 as a prime, then there are obviously many prime factorisations of each natural number $n$,
since the factor $1$ can be included as many times as we like. Thus, to have any hope of obtaining uniqueness, $1$ must be excluded from the primes.

The factors can be shuffled without changing the product. This follows because multiplication in $\mathbb{N}$ is commutative: for any $m, n$ in $\mathbb{N}$ we have $n \times m = m \times n$.

Also, some of the factors might ‘repeat’, i.e. occur several times. To avoid such trivial variations in our representation we write the product of the prime factors of $n$ as follows from now on:

$$n = p_1^{k_1} p_2^{k_2} \ldots p_j^{k_j}.$$  

Here the prime factors are given in increasing order $p_1 < p_2 < \ldots < p_j$ with $k_l$ being the number of times that $p_l$ occurs in the product, for each $l = 1, 2, \ldots, j$. For example, $584 = 2^3 \times 73$, while $2520 = 2^3 \times 3^2 \times 5 \times 7$.

The claim, to be proved below, is that any natural number $n$ has a unique prime factorisation in this form.

First, however, we explore prime numbers a little further.

We might ask how many prime numbers there are. Here is the list of prime numbers below 100:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

These 25 numbers ‘thin out’ somewhat as the numbers grow: there are four primes below 10, but only two between 80 and 90, and one after that. Since it becomes ‘more difficult’ for a number to be prime as the number of possible divisors increases, it might be tempting to guess that the list of all primes could stop somewhere. But Euclid showed that this guess would be wrong.

We may paraphrase the statement of Euclid’s *Elements*, Book IX, Proposition 20) as follows:

*The number of primes is not finite.*

The proof is very simple. Take any finite collection of primes,

$$\{p_1, p_2, p_3, \ldots, p_k\}$$

and form the number $n = (p_1 \times p_2 \times p_3 \times \ldots \times p_k) + 1$. If $n$ is prime, it is a new prime greater than all the $p_i$. If $n$ is composite, it has a prime factor, $p$ say, as was shown above. This $p$ cannot be one of the $p_i$ ($i = 1, 2, \ldots, k$): if it were, it would divide both $n$ and the product $(p_1 \times p_2 \times p_3 \times \ldots \times p_k)$ and so $p$ would divide their difference $n - (p_1 \times p_2 \times p_3 \times \ldots \times p_k) = 1$, which is impossible. This shows that $p$ is a prime not in the above list, and therefore no finite collection of primes can exhaust the collection of all primes.

A remarkable, and much stronger, result was published in 1837 by Lejeune Dirichlet:
If \( a, d \) are natural numbers with no common factors, there are infinitely many primes in the infinite arithmetic progression

\[
a, a + d, a + 2d, a + 3d, \ldots, a + nd, \ldots
\]

See MM for examples and some consequences of this theorem. It represents most of what we know about infinite collections of primes that follow a given pattern—the search for a ‘formula’ that would provide the value of the \( n^{th} \) prime has long been abandoned as hopeless!

A less ambitious question is how the primes are distributed among the elements of \( \mathbb{N} \). Since we cannot expect a formula for the number \( \pi(N) \) of primes \( p \leq N \), mathematicians have sought, instead, to establish asymptotic estimates for \( \pi(N) \). These are estimates for \( \pi(N) \) when \( N \) grows very large. They included a correct conjecture made in the early 1790s by the teenage Gauss\(^a\), who had examined the list of primes below 3 million!

It was not until 1896 that Gauss’ conjecture was verified (independently) by two mathematicians: the French Jacques Hadamard (1865-1963) and the Belgian Charles de la Vallée Poussin\(^b\) (1866-1962). It remains one of the highlights of nineteenth century mathematics:

### The Prime Number Theorem

For large \( N \), \( \pi(N) \) behaves asymptotically like \( \frac{N}{\log N} \). More precisely,

\[
\lim_{N \to \infty} \frac{\pi(N)}{\left(\frac{N}{\log N}\right)} = 1.
\]

Loosely speaking, this says that, for large enough \( N \), the proportion \( \frac{\pi(N)}{N} \) of primes in \( \{1, 2, 3, \ldots, N\} \) is ‘close’ to \( \frac{1}{\log N} \). Here, as in Chapter 5, \( \log \) denotes the natural logarithm.

\(^a\)Near the end of his life Gauss stated that he had reached his conjecture in 1792 or 1793 (aged 15 or 16). But he did not publish his findings during his lifetime. His motto was *Pauca sed matura* (Few, but ripe) and he was unwilling to claim results for which he did not have a full proof. The first (slightly different) published conjecture of an asymptotic estimate for \( \pi(N) \) was given by the French mathematician Adrien-Marie Legendre in 1798.

\(^b\)He was ennobled by the King of Belgium for his feat, becoming *Charles-Jean Étienne Gustave Nicolas, baron de la Vallée Poussin*.

### 2.3. Uniqueness of prime factorisation.

We have shown that every natural number \( n \) can be represented as a product of its prime factors in the form

\[
n = p_1^{k_1} p_2^{k_2} \cdots p_j^{k_j}
\]

We now want to show that this representation is unique (up to shuffling of the factors). For this we prepare the ground a little, and show how a very familiar concept plays a crucial role. The greatest common divisor (gcd) of two
natural numbers \(a, b\) is the largest natural number \(d\) that divides both \(a\) and \(b\).

To show that the gcd \(d\) of two natural numbers \(a, b\) always exists we characterise it slightly differently.

Define \(d'\) as the smallest natural number such that there are integers \(s, t\) (positive or negative) such that

\[ d' = sa + tb. \]

For any pair of natural numbers \(a, b\) there is always at least one pair of integers \(s, t\) making \(sa + tb\) a natural number. Let \(L\) be the set of all natural numbers \(sa + tb\) found in this way. Therefore, \(d'\) exists by the Well-Ordering Principle, since it is the least member of the non-empty subset \(L\) of \(\mathbb{N}\).

Any common divisor of \(a\) and \(b\) clearly also divides \(d'\). We now show that \(d'\) is itself a common divisor of \(a\) and \(b\), which ensures that \(d'\) coincides with the greatest common divisor \(d\) of \(a\) and \(b\).

Using ‘long division’, write \(a = qd' + r\) for some integer \(q\) (the ‘quotient’) and an integer \(r\) with \(0 \leq r < d'\) (the ‘remainder’). Therefore

\[ r = a - qd' = a - q(sa + tb) = (1 - qs)a + (-qt)b = ua + vb, \]

where we have \(u = 1 - qs\) and \(v = -qt\). Here \(u\) and \(v\) are integers, so \(r\) has been written in the form \(ua + vb\) for some integers \(u, v\). By definition, \(d'\) is the smallest natural number that can be written in this form. On the other hand, by our construction, \(0 \leq r < d'\). This means that \(r = 0\). Hence \(a = qd'\), so \(d'\) divides \(a\). A similar argument holds if we reverse the roles of \(a\) and \(b\). Thus \(d' = d\) is the gcd of \(a\) and \(b\). This confirms that the gcd \(d\) of two natural numbers \(a\) and \(b\) always exists and can be written as \(d = sa + tb\) for some integers \(s, t\).

It follows, in particular, that if \(a\) and \(b\) are relatively prime (\(a\) and \(b\) have no common divisors other than 1), then we can always find integers \(s, t\) such that

\[ sa + tb = 1. \]

These simple facts are used to prove a key result due to Euclid. First observe that if a natural number \(n\) is a divisor of the product \(ab\) of two natural numbers, then \(n\) need not divide either \(a\) or \(b\). For example: 12 divides \(10 \times 6 = 60\), but it divides neither 10 nor 6. Euclid shows that this cannot happen for a prime.

**Euclid’s Lemma:**

If \(p\) is prime and divides the product \(ab\), then \(p\) divides at least one of \(a\) and \(b\).

**Proof:** Suppose that \(p\) is a prime divisor of the product \(ab\). If \(p\) does not divide \(a\), it has no factors in common with \(a\) (since \(p\) is prime). Therefore the gcd of \(a\) and \(p\) is 1, which means that we can find integers \(s, t\) satisfying \(sa + tp = 1\).
Multiply this equation by $b$ to obtain $sab + tpb = b$. But $p$ divides $ab$, so $ab = cp$ for some natural number $c$. Hence $b = (sc + tb)p$. We have shown that $p$ is a divisor of $b$ and this proves Euclid’s lemma.

Using induction, Euclid’s lemma can be extended to products of many factors:

**Corollary:**

If $p$ divides the product $a_1a_2\ldots a_k$, then $p$ must divide at least one of the factors $a_i$ for $i = 1, 2, \ldots, k$.

The simple proof is left to the reader. This completes the preliminaries.

**Uniqueness of prime factorisation:**

The prime decomposition $n = p_1^{a_1}p_2^{a_2}\ldots p_k^{a_k}$ of the natural number $n$ is unique.

**Proof:** Suppose that there are two such decompositions:

$$n = p_1^{a_1}p_2^{a_2}\ldots p_k^{a_k} = q_1^{b_1}q_2^{b_2}\ldots q_l^{b_l}$$

where the $p_i, q_j$ are primes, arranged in increasing order, for $i = 1, 2, \ldots k$ and $j = 1, 2, \ldots l$ respectively. Then each $q_j$ divides the product $p_1^{a_1}p_2^{a_2}\ldots p_k^{a_k}$, hence it divides one of the $p_i$, where $i \leq k$, and each $p_i$ divides the product $q_1^{b_1}q_2^{b_2}\ldots q_l^{b_l}$, hence divides one of the $q_j$. Since all are prime, it follows that each $p$ is one of the $q$ and vice versa. So $l = k$ and $p_j = q_j$ for each $j \leq k$, since the two products are in the given form.

It remains to show that the powers also correspond: if for some $j \leq k$ we have $a_j > b_j$, divide both expressions for $n$ by $p_j^{b_j}$ and compare the resulting products

$$p_1^{a_1}p_2^{a_2}\ldots p_{j-1}^{a_{j-1}}p_j^{a_j-b_j}p_{j+1}^{a_{j+1}}\ldots p_k^{a_k}$$

and

$$p_1^{b_1}p_2^{b_2}\ldots p_{j-1}^{b_{j-1}}p_j^{b_j-1}p_{j+1}^{b_{j+1}}\ldots p_k^{b_k}.$$

The two products are equal by assumption, but the first is divisible by $p_j$ (since $a_j > b_j$) while the second product is not divisible by $p_j$. The contradiction shows that $a_j > b_j$ is impossible, and reversing the roles of the two expressions shows that $b_j > a_j$ is also impossible. So each $a_j = b_j$ and the two prime factorisations of $n$ are identical, as claimed.

The uniqueness of prime factorisation is also known as the **Fundamental Theorem of Arithmetic**, since it gives us a complete description of the structure of the set $\mathbb{N}$ of natural numbers: each natural number can be obtained uniquely as a product of powers of primes, arranged in increasing order.

### 3. Integers and rationals

A trivial extension of set $\mathbb{N}$ of natural numbers results from adding the number 0 to it. We denote the result by $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$; alternatively, we list its
elements as the sequence \( \{0, 1, 2, 3, \ldots, n, \ldots\} \) where the difference between successive entries is always 1. Historically, 0 appeared much later than the ‘counting numbers’; but it feels more logical to include it at the outset if we wish to investigate the arithmetical structure of \( \mathbb{N} \): 0 is the neutral element for addition, since \( n + 0 = n \) for any natural number \( n \). In the same way, 1 is the neutral element for multiplication \( (n \times 1 = n \) for all natural numbers \( n \)). We will take for granted the number system \((\mathbb{N}_0, +, \times)\); that is, the set \( \mathbb{N}_0 \) together with the arithmetical operations of addition and multiplication. These are assumed to satisfy the following ‘laws of arithmetic’:

(i) **commutative:** \( n + m = m + n \), \( nm = mn \),

(ii) **associative:** \( (m + n) + p = m + (n + p) \),

(iii) **distributive:** \( m(n + p) = mn + mp \).

Moreover, the set \( \mathbb{N}_0 \) is ordered: write \( n < m \) if the equation \( n + k = m \) has a solution for some \( k \neq 0 \) in \( \mathbb{N}_0 \). Also write \( n \leq m \) if either \( n < m \) or \( n = m \). We could picture this on the ‘geometric’ number line by saying that either \( m \) and \( n \) coincide or \( m \) ‘lies to the right’ of \( n \).

In 1854 this represented the starting point for Richard Dedekind in his quest to show rigorously how the familiar number systems we have described can be constructed directly from \((\mathbb{N}_0, +, \times, <)\), in terms both of definition of their elements and extension of the arithmetical operations and the order relation. Dedekind viewed mathematical progress as arising from

---

3https://commons.wikimedia.org/wiki/File:Richard_Dedekind_1900s.jpg
'free creations of the human spirit and the constraints imposed by logical necessity', which, for him, meant that new mathematical objects should 'always arise in a natural way from the current state of mathematical knowledge' (the quotations are taken from [6]). In particular, extending numbers systems from $\mathbb{N}_0$ would, in the first place, require the 'unlimited completion' of the arithmetical operations $(+, -, \times, \div)$ plus powers and roots.

An exhaustive treatment of the extensions may be found in the classic text [30], published in 1930 by Edmund Landau (1877-1935), where the required constructions are undertaken with the utmost rigour. In fact, Landau goes further: he shows how—as we will consider in the next chapter—the natural numbers themselves can be defined abstractly, how each extension to the next larger class (integers, rationals, real numbers and complex numbers) proceeds, how the arithmetical operations and order relations can be extended consistently in each case and how everything fits together.

Landau's Preface makes clear that he regards the contents of his book as wholly elementary, and presents it as essential background training for any mathematics student, to be read carefully at least once—after which the details can be forgotten!

My book is written, as befits such easy material, in merciless telegram style ("Axiom," "Definition," "Theorem," "Proof," occasionally "Preliminary Remark")... I hope I have written this book in such a way that a normal student can read it in two days. And then (since he already knows the formal rules from school) he may forget its contents.

Owing to Landau’s highly ‘telegraphic’ and rigorous style, the book was received by his intended readership with rather less enthusiasm than he might have expected—perhaps for the reasons he mentions! Rather than repeat the exercise, I will largely omit detailed proofs in what follows below.

3.1. Dedekind on integers. To arrive at a number system that allows unlimited application of the four arithmetical operations $(+, -, \times, \div)$ the system $(\mathbb{N}_0, +, \times)$ must be extended twice: first, to allow us to *subtract* numbers without restriction, and then, from this extension, to allow *division* by any non-zero number. Dedekind’s approach to both extensions was essentially the same: the process of finding the *difference* or the *quotient* of two natural numbers can be represented by considering *pairs* of numbers, i.e. elements of the *Cartesian product*, much as Hamilton had done in extending addition and multiplication from $\mathbb{R}$ to $\mathbb{C}$.

---

4The Cartesian product of any two sets $A$ and $B$ is defined as the set of all ordered pairs $(a, b)$ of elements $a \in A$ and $b \in B$. We write this as $A \times B = \{(a, b) : a \in A, b \in B\}$. A non-empty subset of the Cartesian product $A \times B$ is called a *relation*, since it describes ways of associating elements of the two sets with each other.
In each case a novel aspect of Dedekind’s definitions was the explicit use of what is now called an equivalence relation.\(^5\) This enabled him to provide unambiguous definitions of the ‘new’ number concepts he wished to display, using only the familiar properties of natural numbers. While the idea underlying equivalence relations can be found in specific contexts well before Dedekind, the definitions given below—never published by him—probably constitute the first consistent use of the method in general (see [13], p. 371), helping to usher in what Bertrand Russell (1872-1970) would later call ‘definition by abstraction’.

To define the elements of the first extension of \(\mathbb{N}_0\) (to be denoted by \(\mathbb{Z}\), whose elements he called integers) Dedekind used ordered pairs of elements of \(\mathbb{N}_0\). He defined the operations of addition and multiplication for members of the set \(S\) of ordered pairs as follows:

\[
(m, n) + (p, q) = (m + p, n + q), \quad (m, n) \times (p, q) = (mp + nq, mq + np).
\]

We use the same symbols +, \(\times\) on both sides, but the pairs on the right define the sum and product on the left.

The choice of definitions may be puzzling at first glance. But remember that \(\mathbb{N}_0\) is being extended because it is not closed under subtraction. The pair \((m, n)\) is intended to help define the difference \(m - n\). For example, the above sum reflects the ‘sum of differences’ \((m + p) - (n + q) = (m - n) + (p - q)\).

Since we are working with elements of \(\mathbb{N}_0\) we can use its arithmetic and order properties. If \(n \leq m\) (so \(m\) ‘lies to the right of’ or equals \(n\)) the difference \((m - n)\) of the pair \((m, n)\) will be in \(\mathbb{N}_0\), so the pair will represent a familiar object. But if \(m < n\) the pair will represent a new object. We might wish to define (e.g.) the pair \((2, 5)\) as representing \(-3\), but this symbol will only be meaningful if we can extend the arithmetic of \(\mathbb{N}_0\) to deal with such pairs.

Now note that the sum of the pairs \((5, 2)\) and \((2, 5)\) is the pair \((7, 7)\), whose ‘difference’ is 0. This is so for any pairs \((m, n)\) and \((n, m)\). The ‘difference’ is not uniquely defined in this way: taking \(m = 5, n = 2\) produces this result, but so does \(m = 4, n = 1\), since \((4, 1) + (1, 4) = (5, 5)\), for example. There is ambiguity in these definitions.

Dedekind resolved this by defining an equivalence relation on the set \(S = \mathbb{N}_0 \times \mathbb{N}_0\). This would treat pairs with the same ‘difference’ as interchangeable:

\(^5\)Formally: an equivalence relation \(R\) on any set \(S\) is a subset \(R\) of the Cartesian product \(S \times S\). If \((a, b) \in R\) we write \(a \sim b\) (‘\(a\) is related to \(b\)’). An equivalence relation must be:

(i) reflexive: \(a \sim a\),

(ii) symmetric: if \(a \sim b\) then \(b \sim a\),

(iii) transitive: if \(a \sim b\) and \(b \sim c\) then \(a \sim c\).

Clearly the equality relation = has these properties. So an equivalence relation ‘generalises’ the concept of equality by partitioning the set \(S\) into equivalence classes. Members of the same class (representatives of the class) are treated interchangeably, and no two classes have any members in common (they are disjoint).
pairs \((m,n)\) and \((p,q)\) are related if \(m + q = n + p\). We write this as \((m,n) \sim (p,q)\).

To check that this defines an equivalence relation on \(S\), consider any pairs \(r = (m,n)\), \(s = (p,q)\), \(t = (u,v)\) in \(S\). Using the commutative and associative laws for addition, and cancellation in \(\mathbb{N}_0\), we have:

(i) \(r \sim r\) since \(m + n = n + m\),
(ii) \(r \sim s\) implies that \(s \sim r\), since \(m + q = n + p\) implies \(p + n = q + m\), and
(iii) if for pairs \(r, s, t\) we have \(r \sim s\) and \(s \sim t\) then also \(r \sim t\); for this note that \(m + q = n + p\) and \(p + v = q + u\). But then also \((m + q) + (p + v) = (n + p) + (q + u)\). So \(m + v = n + u\), hence \(r \sim t\).

Dedekind now defined the set \(\mathbb{Z}\) of integers as the collection of all equivalence classes of pairs (where related pairs belong to the same class) under the relation \(\sim\). Fortunately, it turns out that each class has exactly one representative which is either of the form \((n,0)\) or of the form \((0,n)\). The positive integer \(n\) is then the class containing \((n,0)\). If the pairs \((n,0)\) and \((p,q)\) are equivalent, then \(n + q = 0 + p\), so that the pair \((p,q)\) is equivalent to \((0,n)\), since \(q + n = p + 0\), and by the commutative law in \(\mathbb{N}_0\) these two identities are the same. So we can define \(-n\) as the class containing \((0,n)\). In this fashion we justify writing \(\mathbb{Z}\) as the sequence \{\(...,-2,-1,0,1,2,...\}\) from now on.

Having defined the elements of \(\mathbb{Z}\) and the operations of addition and multiplication, Dedekind proceeded to check that these operations inherit the properties stated above for \((\mathbb{N}_0, +, \times)\). Using the simplified notation, we can perform any addition (for \(a, b\) in \(\mathbb{Z}\), \(a+b\) is again in \(\mathbb{Z}\)). The neutral element 0 satisfies \(a + 0 = a\) for every \(a\) in \(\mathbb{Z}\) (adding 0 changes nothing). Every \(a\) has an inverse for addition: for any \(a \in \mathbb{Z}\) there is a unique element, which we denote by \(-a\), in \(\mathbb{Z}\), satisfying the identity \(a + (-a) = 0\). This enables us to define subtraction in \(\mathbb{Z}\) in terms of addition, since \(a - b\) is simply shorthand for the addition of \(a\) and \(-b\), that is: \(a - b = a + (-b)\).

In \(\mathbb{Z}\) we can multiply two numbers and stay within the set. The neutral element is 1: \(a \times 1 = a\) for each \(a\) in \(\mathbb{Z}\).

We extend the ordering \(a < b\), where the notation means that \(a\) is less than \(b\) if \(a\) occurs before \(b\) in the ordering. This is again defined to mean that \(b = a + k\) for some \(k \neq 0\) in \(\mathbb{N}\). The ‘non-strict’ order relation \(a \leq b\) again means that either \(a < b\) or \(a = b\). Both definitions extend those used in \(\mathbb{N}\). As usual, we also write \(a > b\) if \(b < a\) (and \(a \geq b\) if \(b \leq a\)).

As \(\mathbb{N}\) is closed under addition, the ordering is transitive: if \(a < b\) and \(b < c\) then \(a < c\).
We note (without proof) that we can compare any two integers (formally, the ordering is total), and that in \( \mathbb{Z} \) we have the

(iv) trichotomy: Given integers \( a, b \), exactly one of the following three possibilities occurs:

\[
\begin{align*}
&a < b, \\
&a = b, \\
&b < a.
\end{align*}
\]

We also omit proofs, for \( \mathbb{Z} \), of the familiar ‘laws of arithmetic’, listed as (i)-(iii) for \( \mathbb{N}_0 \) at the outset, as well as (iv) and the following simple consequences of the above:

The ordering of integers is compatible with addition and multiplication. In other words:

(v) if \( a < b \) then \( a + c < b + c \) for any integer \( c \);

(vi) if \( a < b \) then \( ac < bc \) if \( 0 < c \), and \( bc < ac \) if \( c < 0 \)

(the final inequality follows as multiplication by \(-1\) reverses the order).

Moreover, the familiar cancellation laws hold:

(vii) if \( a + b = a + c \) then \( b = c \);

(viii) if \( a \neq 0 \) and \( ab = ac \) then \( b = c \).

The first cancellation law confirms that subtraction (the opposite of addition) gives a unique answer:

if \( b + x = a \) and \( b + y = a \) then \( x = y \).

The use of all these properties will be familiar from school mathematics.

Given two pairs from \( \mathbb{N}_0 \), \((m, n)\) and \((p, q)\), representing negative integers, so that \( m < n \) and \( p < q \), their product \((mq + np, mq + np)\) will have its first term larger than its second. To see this, we use laws (i)-(iii) and (vi), and compute

\[
(mp + nq) - (mq + np) = m(p - q) + n(q - p) = (n - m)(q - p) > 0.
\]

In particular, this proves the claim (already used by Diophantus, see Chapter 1) that \((-1) \times (-1) = 1\).

In the Appendix to Chapter 8 the above laws will be used to verify our earlier claim that the system of complex numbers \((\mathbb{C}, +, \times)\) cannot be given an ordering that is similarly compatible with addition and multiplication.

3.2. Dedekind on rational numbers. Fitting fractions into an extended number system in which the laws of arithmetic remain valid also requires care. However, Dedekind’s solution of this issue may feel somewhat more familiar than the steps he needed to accommodate negative numbers. During the Renaissance, as we saw, the arithmetic of fractions became accepted earlier and with less hesitancy than did negative numbers. The practice of expressing a fraction \( \frac{m}{n} \) ‘in lowest form’ is familiar from school. We now express this by saying that we require \( m \) and \( n \) to be relatively prime. The
To define the number system \((\mathbb{Q}, +, \times, <)\) formally, Dedekind was able to start with \textit{pairs} \((a, b)\) of integers, using the arithmetic and order structure of \((\mathbb{Z}, +, \times, <)\), just as he had used \(\mathbb{N}_0\) when defining the integers. To arrive at the integers as a system closed under subtraction, whose elements were defined uniquely, he had needed the equivalence relation discussed above. His task now would be to accommodate another arithmetical operation, division, that was missing from \(\mathbb{Z}\), and to define the elements of the new set \(\mathbb{Q}\) uniquely. These constraints are again met by defining a suitable choice of equivalence relation, one that is based on what is familiar to us as cross-multiplication.

Dedekind began with the Cartesian product \(\mathbb{Z} \times \mathbb{Z}\). He then discarded all pairs whose second coordinate is zero, and imposed an equivalence relation on the remaining pairs:

\[
\text{If integers } b \text{ and } d \text{ are not } 0, \text{ then } (a, b) \text{ is related to } (c, d) \text{ whenever } ad = bc.
\]

This relation is written as \((a, b) \sim (c, d)\).

As we did for addition above, it is easy to check that \(\sim\) is reflexive, symmetric and transitive (see Footnote 4). For this we use the fact that multiplication in \(\mathbb{Z}\) is commutative and associative, and apply the second cancellation law. Moreover, for any \(a, b\) we have \(a(-b) = b(-a)\). Thus \((a, b) \sim (-a, -b)\). So in any equivalence class we can find a representative pair whose second element is in \(\mathbb{N}\).

In this way, Dedekind defined the set \(\mathbb{Q}\) of \textit{rational numbers} as the collection of all equivalence classes of pairs of integers \((a, b)\) with \(b \neq 0\). As Hamilton had done for the complex numbers, he needed to define the operations of addition and multiplication in \(\mathbb{Q}\), ensuring that these reflected the familiar arithmetic of fractions: for given fractions \(\frac{m}{n}, \frac{p}{q}\),

\[
\frac{m}{n} + \frac{p}{q} = \frac{mq + np}{nq}, \quad \frac{m}{n} \times \frac{p}{q} = \frac{mp}{nq}.
\]

Writing \([a, b]\) for the equivalence class of the pair \((a, b)\), Dedekind therefore defined the \textit{sum} of the two classes \([a, b]\) and \([c, d]\) as the equivalence class of the pair \((ad + bc, bd)\) :

\[
[a, b] + [c, d] = [ad + bc, bd],
\]

and their \textit{product} as:

\[
[a, b] \times [c, d] = [ac, bd].
\]

Recall that the representatives can be chosen with \(b, d\) as natural numbers (i.e. positive integers). As we saw for the integers, the classes on the right-hand side \textit{define} the symbols +, \(\times\) on the left, as addition and multiplication for rationals.
The resulting rules for the arithmetic of fractions can be derived from these definitions, and we will now revert to denoting the class \([a, b]\) (a rational number) by \(\frac{a}{b}\), where \(b > 0\) and \(a\) and \(b\) are relatively prime, to represent this equivalence class of fractions.

The algebraic operations in \(\mathbb{Q}\) are compatible with addition and multiplication in \(\mathbb{Z}\), which we identify with the subset of \(\mathbb{Q}\) where the denominators (second members of the pairs) are 1. Thus \(\mathbb{Z}\) may be regarded as a subset of \(\mathbb{Q}\), with the same algebraic operations, exactly as \(\mathbb{N}\) and \(\mathbb{N}_0\) are treated as subsets of \(\mathbb{Z}\).

For the ordering of members of \(\mathbb{Q}\) simply write: \([a, b] < [c, d]\) if and only if \(ad < bc\), where the latter inequality uses the ordering in \(\mathbb{Z}\). Here it is important that \(b\) and \(d\) are taken to be positive. In terms of fractions, this reads: \(\frac{m}{n} < \frac{p}{q}\) if and only if \(mq < np\), extending the ordering from \(\mathbb{Z}\) to \(\mathbb{Q}\). The trichotomy and the transitivity of the ordering also extend to \(\mathbb{Q}\).

Having defined \((\mathbb{Q}, +, \times, <)\), Dedekind had now arrived at a system of numbers in which addition and multiplication can be performed without restriction or moving outside \(\mathbb{Q}\) (in formal terms, the set \(\mathbb{Q}\) is closed under these operations). The laws of arithmetic remain true in the number system \((\mathbb{Q}, +, \times)\). We can reverse the arithmetical operations: rational numbers can be subtracted at will, and a rational number can be divided by any rational number other than 0, with the unique answer remaining an element of \(\mathbb{Q}\). Finally, the inherited ordering on \(\mathbb{Q}\) is compatible with the arithmetical operations on \(\mathbb{Q}\), exactly as described above (in (v) and (vi)) for \(\mathbb{Z}\).

However, unlike \(\mathbb{N}_0\), the larger sets \(\mathbb{Z}\), \(\mathbb{Q}\) do not have the Well-Ordering property (although it holds for subsets of \(\mathbb{Z}\) that are bounded below). Clearly, neither \(\mathbb{Z}\) nor \(\mathbb{Q}\) has a smallest element.

Moreover, in \(\mathbb{N}\) we identify \(n + 1\) as the successor of the natural number \(n\). This concept extends to members of \(\mathbb{Z}\), but it no longer makes sense in \(\mathbb{Q}\): given a rational number \(r\), there is no such thing as the ‘next greatest’ rational number. If such a number (say \(s\)) were to exist, it would obviously satisfy \(s > r\), so that \(s - r > 0\). But then their average \(\frac{r+s}{2}\) would also be rational, and greater than \(r\), but less than \(s\). So the assumption that such an \(s\) exists leads to a contradiction: hence there is no such \(s\). Similarly, \(\mathbb{Q}^+\), the set of all positive rationals, can have no least member.

In fact, given any two rational numbers \(r < s\) one can always find rationals (such as \(\frac{r+s}{2}\)) that lie strictly between them. Repeating this with \(r\) and \(\frac{r+s}{2}\) (or, alternatively, \(\frac{r+s}{2}\) and \(s\)) and continuing in this vein it becomes possible to insert an infinite number of distinct rationals between \(r\) and \(s\), however close together \(r\) and \(s\) may be. This shows that \(\mathbb{Q}\) is very different from the set of natural numbers \(\mathbb{N}\)—one can ‘pack in’ rational numbers on the ‘number line’ as closely as one pleases.
The set \( \mathbb{N} \) of natural numbers provides the ‘spine’ on which the other numbers systems are built.

The well-known *Archimedean property* holds in \( \mathbb{Q} \):

*Given any \( p \) in \( \mathbb{Q} \) there is a natural number \( n > p \).*

Archimedes uses an equivalent statement in his treatise *On Sphere and Cylinder*. However, calling it the ‘Archimedean property’ is really a misnomer; for line segments, such a statement already appears and plays a key role in the comprehensive study of incommensurable geometrical magnitudes that dominates Book X of Euclid’s *Elements*. This book was written before Archimedes was born.

For \( \mathbb{Q} \) the proof of the claim is trivial: since \( p \in \mathbb{Q} \) has (a representative of) the form \( \frac{a}{b} \), where \( a \) is an integer and \( b \) a natural number, the claim is equivalent to saying that we can find a natural number \( n \) such that \( nb > a \). This is obvious if \( a \leq 0 \), while if \( a \geq 1 \), we can take \( n = a + 1 \). Then, as \( b \geq 1 \), we have \( nb = (a + 1)b = ab + b \geq a + b > a \).

Although all the above properties of \( \mathbb{Q} \) had been tacitly assumed to hold for centuries, Dedekind had shown that one can derive this number system by logical reasoning alone, purely on the basis of properties of his starting point, the natural numbers. Just as Hamilton had done for ‘imaginary’ numbers, he was able to confirm the validity of the inherited arithmetical relationships of his number system, without needing to concern himself with explaining the nature of either negative numbers or fractions in terms of analogies with geometry or anything else. This approach differs sharply from earlier concerns about whether negative or imaginary numbers exist—or, indeed, whether ratios should be regarded as numbers. More important than the nature of the objects were the relationships between them that governed their interaction. In time, this abstract approach came to govern much thinking about mathematics. In the next section, we will see how it also led Dedekind to a rigorous arithmetical description of the ‘number line’.

### 4. Dedekind cuts

In 1858, when preparing an introductory lecture course on Calculus, Dedekind realised that he could not prove results such as the IVT without an arithmetical definition of the underlying continuum. As he points out in [8], one could not give a rigorous proof of much simpler results, such as \( \sqrt{2} \times \sqrt{3} = \sqrt{6} \), unless square roots were described by arithmetical means.\(^6\)

In keeping with his general programme of creating each extended number system from the previous one, Dedekind set out to define a new number system.
system, starting from \( \mathbb{Q} \), by means analogous to the extensions described in the previous section. While those extensions included abstract notions such as equivalence relations, neither had been technically difficult, and in each case the relationship between a number in the extended class and its antecedents in the former one was clear.

However, his current extension, beginning with the rationals, presented a more fundamental obstacle, as he discusses in detail in [8]. He realised in particular that, instead of using pairs of rationals, he would require an infinite number of rationals when filling a ‘gap’ in \( \mathbb{Q} \) with an arithmetically defined irrational number, in order that the new number system would have a new property, that he would call continuity. His project led him to consider sets of rational numbers more abstractly, and his final definition of elements of the real number system may seem some way removed from the general reader’s intuition of what numbers are. The brief summary we give below may therefore be somewhat more challenging conceptually than what has gone before. (More details are given in MM.)

Dedekind’s definition of real numbers as produced by what he called cuts of the set \( \mathbb{Q} \) is today one of the standard ways of introducing the real numbers. Although completed in 1858, he did not publish his work for more than a decade. He only did so in 1872 when he became aware that a paper by Georg Cantor, defining real numbers in terms of Cauchy sequences of rationals, was soon to appear. Their papers were by no means universally appreciated at the time. As an example, we have the verdict of the outspoken Hermann Hankel (1839-1873):

Every attempt to treat the irrational numbers formally and without the concept of [geometric] magnitude must lead to the most abstruse and troublesome artificialities, which, even if they can be carried through with complete rigour, as we have every right to doubt, do not have a higher scientific value.

But in due course the constructions by Dedekind and Cantor were to become staples of undergraduate mathematics in the twentieth century – even if not always welcomed by that audience, either!

Dedekind’s elegant paper ([8]) is entitled Stetigkeit und Irrationale Zahlen (Continuity and irrational numbers). He lays great emphasis on continuity, which he regards as the key concept through which he links his reasoning explicitly to the properties of the geometric number line.

He compares the order properties of \( \mathbb{Q} \) with the positioning of points on a line \( L \):

1. For rational numbers, if \( b < a < c \), we say that \( a \) lies between \( b \) and \( c \); just as a point \( p \) on \( L \) lies between points \( q \) and \( r \) if \( r \) is to its right and \( q \) to its left.
2. Between any two distinct rational numbers \(a, b\) there are infinitely many other rational numbers; similarly, \(L\) contains infinitely many points between distinct points \(p, q\).

3. (a) Fix a rational number \(a\). Split \(\mathbb{Q} \setminus \{a\}\) into two classes, \(A_1\) and \(A_2\), where \(A_1\) contains all rational numbers \(b < a\), while \(A_2\) contains all rational numbers \(c > a\). This leaves us with choosing where to place \(a\). Placing \(a\) in \(A_1\) would make \(a\) the largest number of \(A_1\); placing \(a\) in \(A_2\) would make \(a\) the smallest number of \(A_2\). Either choice will ensure that each number in \(A_1\) is less than every number in \(A_2\). (Dedekind’s choice will become clear below.)

(b) Fix a point \(p\) on the line \(L\). Cut \(L\) into two pieces and place every point to the left of \(p\) into the line segment \(P_1\) and every point to the right of \(p\) into the line segment \(P_2\). We can either include \(p\) in \(P_1\) as its right-most point, or in \(P_2\) as its left-most point. Either choice ensures that every point of \(P_1\) lies to the left of every point of \(P_2\).

Thus, to ensure that rational numbers correspond uniquely to the ‘splits’ of \(\mathbb{Q}\) described in 3(a) requires a decision whether \(A_1\) should have a largest element or \(A_2\) a smallest. The possibility that \(A_1\) has greatest element \(b\) while \(A_2\) also has a least element \(c\) can be ruled out: in that case \(b < c\) and \(\frac{1}{2}(b + c)\) would belong to neither \(A_1\) nor \(A_2\) since it is larger than \(b\) and smaller than \(c\).

As Dedekind points out, to each number in \(\mathbb{Q}\) there corresponds one and only one point of \(L\). However, there is a crucial difference between \(\mathbb{Q}\) and \(L\), since \(L\) contains points describing ‘incommensurable lengths’ such as \(\sqrt{2}\):

‘Of the greatest importance, however, is the fact that in the straight line \(L\) there are infinitely many points which correspond to no rational number...The straight line \(L\) is infinitely richer in point-individuals than the domain \(\mathbb{Q}\) of rational number-individuals.’

If now, as we desire, we try to follow up arithmetically all phenomena in the straight line, the domain of rational numbers is insufficient...and it becomes absolutely necessary that...\([\mathbb{Q}]\)...be essentially improved by the creation of new numbers such that the domain of numbers shall gain the same completeness, or as we may say at once, the same continuity, as the straight line.’

His goal in providing a new description of the real numbers is that ‘arithmetic shall be developed out of itself’, mirroring the way that ‘negative and fractional numbers are formed by a new creation’. His method of creating this richer number system rests on understanding what the continuity of the line \(L\) means. His answer is that this lies in the converse of the ‘splitting’ of \(L\):

‘If the points of the straight line fall into two classes such that every point of the first class lies to the left of every point of the second class, then there exists one
and only one point which produces this division of all points into two classes, this severing of the straight line into two portions.'

He does not claim that he can prove this (seemingly obvious) assertion, but instead takes it as an assertion about the nature of the line \( L \) that will be taken as an unproven property. The task he now faces is to create a number system that ‘completes’ \( \mathbb{Q} \) by satisfying this continuity property.

4.1. Cuts and order properties. The above comparison of \( \mathbb{Q} \) and the line \( L \) shows that ‘splitting’ \( \mathbb{Q} \) at a rational number (such as 2) will provide a pair of \((A_1, A_2)\) of disjoint sets that together make up all of \( \mathbb{Q} \), such as \( A_1 = \{ r \in \mathbb{Q} : r < 2 \} \), \( A_2 = \{ r \in \mathbb{Q} : r \geq 2 \} \), where the number 2 provides the least element of \( A_2 \). But there are also quite different splittings of \( \mathbb{Q} \): for example, we might place all negative rationals as well as all other rationals whose square is less than 2 in \( A_1 \), while \( A_2 \) consists of the rest, i.e. the positive rationals whose square is greater than 2 (there is no rational whose square equals 2). In symbols:

\[
A_1 = \{ r \in \mathbb{Q} : r < 0 \} \cup \{ r \in \mathbb{Q} : r \geq 0, r^2 < 2 \}, \quad A_2 = \{ r \in \mathbb{Q} : r \geq 0, r^2 > 2 \}.
\]

Here \( A_1 \) has no largest element and \( A_2 \) no smallest.\(^7\) This differs fundamentally from splitting the line \( L \) into two pieces, and occurs precisely because \( \mathbb{Q} \) cannot fill the ‘gap’ at this point. Dedekind’s solution is to turn this fact into a definition – for him:

a (Dedekind) cut of \( \mathbb{Q} \) is a disjoint pair of non-empty sets \((A_1, A_2)\) making up all of \( \mathbb{Q} \) (that is, \( A_1 \cup A_2 = \mathbb{Q} \) and \( A_1 \cap A_2 = \emptyset \)), and such that \( A_1 \) has no largest element.

Following Landau, we will call \( A_1 \) the set of lower numbers, and \( A_2 \) the set of upper numbers for this cut.

When cutting \( \mathbb{Q} \) at a rational number \( r \), Dedekind’s choice ensures that the lower numbers have no largest element, while \( r \) becomes the smallest upper number for this cut. For any given cut, every lower number is less than every upper number.

To simplify the notation and terminology, we can focus on the set \( A_1 \) of lower numbers, since this determines \( A_2 \) completely as its complement \( A_2^c = \mathbb{Q} \setminus A_1 \). Writing \( \alpha \) instead of \((A_1, A_2)\) to denote the cut means that \( \alpha = A_1 \) and \( \alpha^c = A_2 \). We use Greek letters to denote cuts; the elements of any cut are rational numbers, denoted by letters such as \( p, q, r \), etc. We re-state the definition in these terms:

**Definition:**

Call a subset \( \alpha \) of \( \mathbb{Q} \) a cut if

(i) \( \alpha \) and \( \alpha^c = \mathbb{Q} \setminus \alpha \) are both non-empty sets of rationals,

\(^7\)The elementary calculations to prove this are left to the reader – they can be found (e.g.) on p.3 of [40], and in MM.
(ii) for rationals \(p, q\), if \(p \in \alpha\) and \(q < p\) then \(q \in \alpha\).

(iii) \(\alpha\) has no largest element: given \(q \in \alpha\), we can find \(p \in \alpha\) with \(q < p\).

Thus \(\alpha\) consists of the lower numbers for the cut, and \(\alpha^c\) of its upper numbers. Two cuts \(\alpha, \beta\) are said to be equal if they contain the same rational numbers. We write \(\alpha = \beta\). The set \(\mathbb{R}\) of all cuts comprises the real numbers; each real number is determined uniquely by a subset of \(\mathbb{Q}\), the set of its lower numbers.

The ordering of cuts \(\mathbb{R}\) is defined by set inclusion.

Definition:

Given two cuts \(\alpha, \beta\) write \(\alpha < \beta\) if \(\alpha\) is a proper subset of \(\beta\) i.e. \(\alpha \subset \beta\).

Hence \(\beta\) contains a lower number that is an upper number for \(\alpha\).

(i) This definition shows that the ordering is transitive: given cuts \(\alpha, \beta, \gamma\), if \(\alpha < \beta\) and \(\beta < \gamma\), then \(\alpha < \gamma\).

This follows as \(\beta\) has a lower number \(r\) that is an upper number for \(\alpha\), while \(\gamma\) has a lower number \(s\) that is an upper number for \(\beta\). But \(r < s\) (for \(\beta\), any upper number \(s\) is greater than any lower number). So \(\alpha < \gamma\), since \(s\) is a lower number for \(\gamma\) but an upper number for \(\alpha\).

(ii) The trichotomy holds for the ordering \(<\).

For any cuts \(\alpha, \beta\), exactly one of \(\alpha < \beta\), \(\alpha = \beta\), \(\beta < \alpha\) holds.

This is immediate from set inclusion, which defines \(<\).

We write \(\alpha \leq \beta\) if either \(\alpha = \beta\) or \(\alpha < \beta\). Thus \(\alpha \leq \beta\) means that \(\alpha \subseteq \beta\).

As for any (linearly) ordered set, we can define the following useful objects related to the order \(\leq\) on \(\mathbb{R}\):

- given a set \(B\) of cuts, the cut \(\alpha\) is an upper bound for \(B\) if \(\beta \leq \alpha\) for all \(\beta\) in \(B\). We say \(B\) is bounded above by \(\alpha\).

  The least upper bound (or supremum) of \(B\) is defined as an upper bound \(\alpha\) of \(B\) such that \(\alpha \leq \gamma\) for every upper bound \(\gamma\) of \(B\).

  Similarly, a cut \(\delta\) is a lower bound for \(B\) if \(\delta \leq \beta\) for all \(\beta\) in \(B\), and then \(B\) is bounded below by \(\delta\).

  The greatest lower bound (or infimum) of \(B\) is defined as a lower bound \(\delta\) of \(B\) such that \(\gamma \leq \delta\) for every lower bound of \(B\).

The crucial property of completeness (or ‘lack of gaps’) of the set of cuts is then given by the following result.

**Theorem:**

---

8Dedekind’s choice, expressed as requirement (iii), imposes an equivalence relation on the set of all pairs \((A_1, A_2)\) of disjoint subsets of \(\mathbb{Q}\) that satisfy \(A_1 \cup A_2 = \mathbb{Q}\). A cut is an equivalence class of such pairs, represented by its set of lower numbers.
Let $B$ be a non-empty subset of $\mathbb{R}$ for which there exists an upper bound $\theta \in \mathbb{R}$ under the ordering $<$. Then $B$ has a least upper bound in $\mathbb{R}$.

Proof: Each $\alpha \in B$ is a non-empty subset of $\mathbb{Q}$. Let $L(B)$ be the union of all the sets of lower numbers for cuts in $B$. Thus $r \in \mathbb{Q}$ belongs to $L(B)$ if and only if there is at least one cut $\alpha \in B$ such that $r$ is a lower number for $\alpha$. A rational number $r$ may be a lower number for many cuts in $B$, but we list it only once in forming $L(B)$. It is a straightforward exercise to show $L(B)$ satisfies the definition of a cut (see MM for details).

Next, $L(B)$ is an upper bound for $B$ since, by definition of $L(B)$, the set of lower numbers for any $\alpha$ in $B$ is a subset of $L(B)$. So $\alpha \leq L(B)$ holds for every $\alpha \in B$ by definition of the ordering (since $\leq$ means $\subseteq$).

Finally, $L(B)$ is the least upper bound for $B$: if a cut $\eta$ is an upper bound for $B$ we must show that $L(B) \leq \eta$. So we need to show that every lower number for $L(B)$ is also a lower number for $\eta$. But the lower numbers for every $\alpha$ in $B$ are lower numbers for $\eta$ (as $\eta$ is an upper bound for $B$). It follows that $L(B)$ is a subset of the set of lower numbers for $\eta$, i.e. $L(B) \leq \eta$. Hence $L(B)$ is the least upper bound for $B$. This completes the proof.

Rational cuts are easily identified:

**Theorem**

Given a rational $p$, define $\alpha_p = \{ r \in \mathbb{Q} : r < p \}$. Then $\alpha_p$ is a cut, and its smallest upper number is $p$.

Proof: Clearly $\alpha_p$ satisfies (i), (ii) of the definition of a cut. To see that $\alpha_p$ has no greatest lower number, let $q \in \alpha_p$ be arbitrary, so that $q < p$. But then $q < \frac{1}{2}(q+p) < p$ and (by definition of $\alpha_p$) we have $\frac{1}{2}(q+p) \in \alpha_p$, so (iii) is satisfied and $\alpha_p$ is a cut.

Equally, we cannot have $p < p$, so $p$ is not in $\alpha_p$, hence it is an upper number for $\alpha_p$. But $q < p$ implies $q \in \alpha_p$, so any upper number $q$ must satisfy $q \geq p$, hence $p$ is the smallest upper number for $\alpha_p$.

We call $\alpha_p$ the rational cut associated with $p$. We have a one-one correspondence $p \leftrightarrow \alpha_p = \{ r \in \mathbb{Q} : r < p \}$ between elements of $\mathbb{Q}$ and elements of $\mathbb{R}$. The correspondence preserves the ordering of $\mathbb{Q}$: $p < q$ if and only if

$$\{ r \in \mathbb{Q} : r < p \} \subset \{ r \in \mathbb{Q} : r < q \}.$$  

This indicates how the set $\mathbb{Q}$ can be embedded in the set $\mathbb{R}$ in a way that preserves the ordering. Moreover, it is not hard to show that between any two given cuts there is a rational cut.

Defining the sum and product of two cuts and checking that the arithmetical properties correspond takes somewhat more work, but clearly the
rational cut \( \{ r \in \mathbb{Q} : r < 0 \} \) is the neutral element for addition. This enables Dedekind to define positive and negative cuts, and check that the laws of arithmetic extend from \( \mathbb{Q} \) to \( \mathbb{R} \). Proofs of these claims can be found in MM and in (e.g.) [8], [10], [40]. (Also see [6]).

The steps outlined here enabled Dedekind to characterise real numbers directly in terms of rationals, showing that (as suspected) the real number \( \alpha \) can be regarded as the set of all rationals less than \( \alpha \). Although he avoided the logical trap that Cauchy fell into when defining irrationals as limits of rational sequences, Dedekind himself was somewhat hesitant about explicitly calling cuts numbers: for him, the set of lower numbers of a cut ‘produces’ a real number. Today, mathematicians generally do not share these qualms. A football analogy may be helpful here: when Manchester United play against Liverpool, the pitch will usually feature eleven players in the set comprising the Liverpool team, yet when the result of the match is recorded in the League Table, the team is regarded as a single unit (Liverpool). The set of players is treated as a single element of another set, namely the set of Premier League teams. Similarly, a cut is a set of rationals, but this set is equally regarded as an element of the set of real numbers.

The real number system that Dedekind defined fills in all the gaps of \( \mathbb{Q} \). The question now arose whether repeating the process would again generate new elements if one took cuts of the reals, as was done for the rationals. Dedekind’s key result shows that this would not happen—the analogy with the line had been ‘completed’ by defining the cuts.

**Dedekind’s Theorem:**

Given non-empty subsets \( A, B \) of \( \mathbb{R} \) such that \( A \cup B = \mathbb{R} \), \( A \cap B = \emptyset \) and \( a \in A, b \in B \) implies \( a < b \), there is a unique \( x \in \mathbb{R} \) such that for all \( a \in A, b \in B \) we have \( a \leq x \leq b \).

Consequently, either \( A \) has a largest element or \( B \) a smallest.

The proof can be found in MM.

5. Cantor’s construction of the reals

Georg Cantor expressed his admiration for the elegance and clear logic of Dedekind’s construction, but he was adamant that ‘numbers in analysis never present themselves as “cuts,” and therefore have first of all to be brought into this form by elaborate artifices’. His own construction, which he felt was the ‘most natural of all’, presenting the approach best suited to the analysis of functions, started from the Cauchy criterion (see Chapter 6) for convergence of sequences. In 1872 Cantor outlined his ideas in a paper dealing with trigonometric series, which he had sent to Dedekind prior to publication, thus prompting Dedekind to publish his long-held views. His was not the first publication using Cauchy sequences to define the irrationals—in 1869, the French mathematician Charles Meray (1835-1911) had published
an account in different terminology harking back to Cauchy. Eduard Heine (1821-1881), Cantor’s colleague at the University of Halle, who was motivated more directly by the need for clear foundations for Real Analysis, also published a version of Cantor’s arguments in a paper in 1872.

Cantor’s initial motivation differed substantially from that of other writers on the subject. His main interest, first encouraged by Heine, was to explore the way Fourier series were able to represent a wide class of functions. 9 Cantor addressed the problem of deciding for which functions the representing series is uniquely defined. He showed initially that this will be true if the series converges to \( f \) at all points. By 1872, he had succeeded in proving uniqueness even if the convergence failed at infinitely many points, provided that these points are distributed on the line in a specific fashion. It was this result that led him to consider how rational and irrational ‘points on the line’ are distributed, and thus drew his attention to the need for irrationals to be defined unambiguously as numbers.

Cantor was well aware that he could not define a real number as the limit of a sequence of rationals, since the definition of limit involves identifying the limit as a number. Cauchy sequences of rationals, however, only require us to know what rationals are and how to do arithmetic with them. Moreover, any rational number \( r \) has an obvious associated Cauchy sequence, namely the infinite constant sequence \( \{r, r, r, ... \} \). On the other hand, Cauchy sequences such as our old friend, the successive decimal approximations \( \{1, 1.4, 1.41, 1.414, ... \} \) to \( \sqrt{2} \), clearly lead to irrationals.

Cantor’s definition of irrationals was discursive, leaving many details to the reader. He considered Cauchy sequences of rationals, or, as he put it, ‘fundamental sequences of the first order’. To each such sequence, consisting of rationals \( (a_\nu) \) such that ‘after the choice of an arbitrarily small rational number \( \varepsilon \) a finite number of members can be separated off, so that those remaining have pairwise a difference which in absolute terms is smaller than \( \varepsilon' \), he attached a symbol \( b \). The real numbers would constitute the collection of all such first-order sequences. Cantor was aware that different Cauchy sequences can have the same limit, but it was his colleague Heine, who, in a paper also

---

9This had been a hot topic in analysis for some decades, ever since Joseph Fourier’s famous 1807 investigation on representing a general function \( f \) on the interval \([-\pi, \pi]\) by a trigonometric series of the form \( \frac{1}{2}a_0 + \sum_{n=1}^{\infty} [a_n \cos(nx) + b_n \sin(nx)] \). Fourier had calculated the coefficients in the series expansion as \( a_n = \frac{1}{\pi} \int_{-\pi}^{\pi} f(t) \cos(nt) dt \), \( b_n = \frac{1}{\pi} \int_{-\pi}^{\pi} f(t) \sin(nt) dt \), and claimed that, with these coefficients, the series would converge at each point \( x \) to the value \( f(x) \). The counter-example given by Niels Abel to Cauchy’s assertion that an infinite sum of continuous functions is always continuous used such a sequence. Abel also realised that his result illustrated deficiencies in various proofs given by Fourier. Over the next several decades a number of prominent mathematicians, including Dirichlet and Heine, had gradually succeeded in widening the range of situations for which uniqueness of the representation of \( f \) could be proved.
published around the same time, clarified explicitly that two such sequences should be considered equal if the sequence of their differences converges to 0. This requirement again introduces an equivalence relation on the set of rational Cauchy sequences. The fundamental sequences \((a_n), (b_n)\) belong to the same equivalence class if \(|a_n - b_n| \to 0\) when \(n \to \infty\).

Cantor was at pains to stress that \(b\) was in no sense assumed to be a ‘limit’, but served simply as a symbol representing the sequence. It was only after carefully defining the algebraic and order relations for fundamental sequences that he could make sense of the statement \(b = \lim_{\nu \to \infty} a_\nu\). He argued that irrationals, as a result of their definition, should have ‘as definite a reality in our mind’ as do rationals, and that this was what should convince one of the ‘evident admissibility of the limiting processes’. He then used the same construction, taking fundamental sequences of the second order, where each element was a fundamental sequence of the first order, to create the next level of abstraction. He continued this process indefinitely, but showed that nothing new would be created in any such repetition: they all ‘accomplish exactly the same thing for the determination of a real number \(b\) as the fundamental sequences of the first order’. This became his version of Dedekind’s ‘continuity’ property.

We summarise Cantor’s approach in current terminology:

**Definition**

\(^{10}\)https://commons.wikimedia.org/wiki/File:Georg_Cantor_(Porträt).jpg
(i) A Cauchy (or fundamental) sequence of rational numbers \((a_n)_{n \geq 1}\) is such that, for any given rational \(r > 0\), there is a natural number \(N\), depending on \(r\), such that \(|a_m - a_n| < r\) whenever \(m, n \geq N\). Denote the set of all rational Cauchy sequences by \(C\).

(ii) A null sequence \((a_n)\) of rational numbers is such that, for any rational \(r > 0\), there is a natural number \(N\), depending on \(r\), such that \(|a_n| < r\) for all \(n \geq N\). Denote the set of all rational null sequences by \(N\).

(iii) Two Cauchy sequences \((a_n), (b_n)\) of rational numbers are equivalent if the sequence \((a_n - b_n)\) of their differences is a null sequence. Write this as \((a_n) \sim (b_n)\), or \((b_n) \in (a_n) + N\). This defines an equivalence relation on \(C\).

Definition: The set \(\mathbb{R}\) of real numbers is the set of all equivalence classes of Cauchy sequences of rationals under the relation \(\sim\). In other words, for any sequence \(s = (s_n)\) in \(C\), the equivalence class of \(s\) is the subset of \(C\) given by

\[
[s] = \{s' \in C : s' \sim s\}.
\]

Any constant sequence \(r = r_n\) with \(r_n = r\) for all \(n\) is in \(C\). For two constant sequences the equivalence \(r \sim s\) means that \(r = s\). Thus \([r]\) is the only constant sequence in its class. We identify the rationals with the equivalence classes of constant sequences, i.e. embed \(\mathbb{Q}\) in \(\mathbb{R}\) by the correspondence \(r \leftrightarrow [r]\). So the rational number \(r\) is represented in \(\mathbb{R}\) by the class of the constant sequence \(r = \{r, r, r, ..., r, ...\}\).

To define the algebraic operations for the set of all equivalence classes, addition and multiplication of the representing sequences is done coordinate-wise – that is, individually for corresponding terms in the sequence. For given rational Cauchy sequences \(x = (x_n)_n\) and \(y = (y_n)_n\), the sum \([x] + [y]\) becomes the class of the sequence \(x + y = (x_n + y_n)_n\) and similarly for their product. The class \([0]\) of the constant sequence with \(r = 0\) is the neutral element for addition: it consists of all null sequences \((c_n)_n\) in \(C\). Hence \([a] + [0] = [a]\) for all classes \(a\). Similarly, the class \([1]\) is the neutral element for multiplication. Inverses are also simple to determine – note that to have a multiplicative inverse, the class \([a]\) must not contain null sequences.

This defines the algebraic system \((\mathbb{R}, +, \times)\), in which the rationals \(\mathbb{Q}\) are embedded by the correspondence \(r \leftrightarrow [r]\). We may now treat \(\mathbb{Q}\) as a subset of \(\mathbb{R}\), with + and \(\times\) extended from \(\mathbb{Q}\) to \(\mathbb{R}\).

This embedding allows Cantor to extend the modulus \(|\cdot|\) to \(\mathbb{R}\) by taking the modulus \(|[x]|\) of \(x = (x_n)\) as the class of \((|x_n|)_n\), and to define the set of (strictly) positive real numbers as

\[
\mathbb{R}_+ = \{[x] \in \mathbb{R} : [x] \neq [0], |[x]| = [x]\}.
\]

A real number \([y]\) is negative if its additive inverse \(-[y]\) is positive. Setting \([0] < [x]\) if \([x]\) belongs to \(\mathbb{R}_+\) defines the ordering \(<\) for \(\mathbb{R}\).
The proof of completeness of $\mathbb{R}$ uses the Cauchy Criterion for convergence – in Cantor’s approach this is the more technically challenging argument and will be omitted here. (Proofs can be found in MM and [10].)

Unlike Dedekind, Cantor emphasises the algebraic operations rather than the ordering. This makes his approach suitable for extensions of the completeness property to domains which have no linear ordering, such as the Cartesian plane $\mathbb{R}^2$ and its extensions to higher dimensions.

6. Decimal expansions

Having defined real numbers arithmetically, we can use the familiar concept of decimal expansions to highlight the difference between irrationals and rationals in another way that may feel more ‘concrete’ than Dedekind cuts or classes of Cauchy sequences of rationals. We will concentrate on positive numbers here. In our base-10 positional system of writing numbers, the decimal expansion of a real number is obtained by making successive choices from the set of single-digit (base 10) numbers $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, and combining them with the decimal point in order to separate the ‘integral’ and ‘fractional’ parts. The decimal point indicates where we leave the realm of natural numbers, so that what comes after the decimal point is intended to represent a number ‘lying between’ 0 and 1.

6.1. Expanding rationals. Write an infinite decimal expansion of a positive real number as

$$a_0.a_1a_2...a_m...$$

where $a_0$ is an element of $\mathbb{N}_0$, while, for $j \geq 1$, each $a_j$ is one of the digits 0, 1, 2, 3, 4, 5, 6, 7, 8 or 9. Here $a_0$ represents a finite sum of multiples (using these digits) of positive powers of 10. After the decimal point we add the infinite sum

$$\sum_{n=1}^{\infty} \frac{a_n}{10^n} = \frac{a_1}{10} + \frac{a_2}{10^2} + ... + \frac{a_k}{10^k} + ...$$

Finite, or ‘terminating’, decimal expansions are familiar, of course: we write $\frac{1}{8}$ as 0.125, for example. Nothing really changes if we write this as the infinite decimal expansion 0.12500000... instead, adding zeroes in all the decimal places after the third. Doing so brings the terminating expansion into line with ‘recurring’ expansions like $\frac{1}{3} = 0.3333... = 0.\overline{3}$ or $\frac{1}{7} = 0.142857$, where in both cases the upper bar denotes the indefinite repetition of the number or group of numbers concerned. (The recurrence need not start immediately after the decimal point: consider $\frac{8}{15} = 0.53333...$, for example.)

Any positive rational number, represented by $r = \frac{m}{n}$ (where the natural numbers $m, n$ have no common factors) will have decimal expansion of one of these two forms: if $n$ has no prime factors other than 2 and 5, its decimal...
expansion terminates, because the fraction \( \frac{m}{n} \) is equivalent to one of the form \( \frac{q}{10^k} \), for some natural number \( q \) and \( k \geq 1 \).

Any other rational will have a non-terminating expansion. If, for example, \( \frac{1}{3} \) had a terminating decimal expansion, we would have \( \frac{1}{3} = \frac{q}{10^k} \) for some natural numbers \( q \) and \( k > 1 \). Hence \( 10^k = 3q \). But the uniqueness of prime factorisation shows that these numbers cannot be equal: on the left the prime factors are 2 and 5, while on the right 3 is a prime factor. A similar argument clearly applies to any rational \( \frac{m}{n} \) where \( n \) contains any prime factor other than 2 or 5.

We characterise recurring expansions of fractions \( \frac{m}{n} \) by using the pigeonhole principle:

Suppose there are \( k \) pigeonholes and \( n > k \) pigeons. Then at least one pigeonhole contains more than one pigeon.

For, if no pigeonhole contains more than one pigeon, and \( l \geq 0 \) pigeonholes are unoccupied, then \( k - l \) pigeonholes contain exactly one pigeon. The two finite sets, respectively of occupied pigeonholes and of pigeons, have the same number of elements, i.e. \( k - l = n \). This contradicts the fact that \( n > k \). So our assumption is false, and hence at least one pigeonhole contains more than one pigeon.

Now apply this to long division. If the decimal expansion of the rational number \( \frac{m}{n} \) is infinite, then dividing \( m \) by \( n \) must leave a non-zero remainder at infinitely many decimal places, as the expansion does not terminate. These remainders must be natural numbers less than \( n \), which means that there are at most \( n - 1 \) different choices. Hence within \( n \) successive decimal places some remainder \( r \) will occur a second time. As we are dividing \( m.000... \) by \( n \), the immediate successor of \( r \) will repeat exactly as before. In other words, the decimal expansion of any rational number either terminates or recurs with a finite period.

\(^a\)Also known as Dirichlet’s ‘drawer principle’ [Schubfachprinzip]. He used it in 1834, but its first known appearance is in a 1624 text by the French Jesuit priest Jean Leurechon.

We combine terminating and recurring expansions in the single phrase eventually periodic (with periodicity starting after a finite number \( k \geq 0 \) of places after the decimal point). We have shown that every rational number has an eventually periodic decimal expansion.

The converse is also true: if the decimal expansion of a real number \( x \) is eventually periodic, then \( x \) is rational.

To see this, we may assume that the periodicity begins at the first decimal place (if the expansion begins with \( m \) zeroes after the decimal point, we consider \( 10^m \cdot x \) instead). Thus \( x = a_0.a_1a_2...a_k \). This is the sum \( S \) of an infinite series with first term \( a_0 \). Let \( \sum_{n=0}^{\infty} a_n \) denote summation of all its terms, starting at \( n = 0 \), and set \( q = \)
\[
\frac{a_1}{10} + \frac{a_2}{10^2} + \ldots + \frac{a_k}{10^k}, \text{ then } S \text{ is the rational number}
\]
\[
S = a_0 + q \sum_{n=1}^{\infty} \frac{1}{(10^k)^n} = a_0 + q \left[ \frac{\frac{1}{10^k}}{1 - \left( \frac{1}{10^k} \right)} \right].
\]

Therefore the rational numbers are characterized as real numbers whose decimal expansions are eventually periodic. To know the infinite decimal expansion of a rational number \( r \) exactly, it suffices to know finitely many of its initial entries after the decimal point.

As we will see shortly, it is often helpful to express any terminating decimal expansion as an infinite expansion, in order to obtain a consistent set of entities. However, when doing this, the need to describe such a rational number uniquely as an infinite decimal expansion will require us to make a choice between using nines or recurring zeroes. Like Dedekind did for his cuts, we will opt for the former, as will be shown shortly.

### 6.2. Expanding irrationals.

Call an infinite decimal expansion aperiodic if it is not eventually periodic. Thus the irrational numbers can be characterised as real numbers whose decimal expansions are aperiodic. For these expansions we cannot determine the full expansion after only seeing finitely many decimal entries, since at each stage we have no \( \text{a priori} \) means of determining the next digit with certainty. An infinite sequence of digits chosen at random is highly likely to be aperiodic.

Imagine dipping a fishing net into a pond containing all infinite decimal expansions, and pulling out one of them, \( x \), at random. For \( x \) to be eventually periodic, it must have the property that there exists some finite \( M \) such that, having read the first \( M \) digits of \( x = a_0.a_1a_2a_3\ldots \), we will, from that point onward, know for certain what all its remaining digits are. A randomly selected infinite sequence of decimal digits is highly unlikely to have this property. At each point there are 10 choices for the next digit, which – in the absence of additional information – might reasonably be considered to be equally likely. They are chosen independently of each other. Under these assumptions the occurrence of any particular sequence of \( k \) digits in the infinite decimal expansion would have probability \( \frac{1}{10^k} \), unless we have extraneous information. This makes it highly implausible, if \( k \) is large, that our ‘randomly chosen’ expansion could be eventually periodic.

This suggests that the infinite decimal expansion of a real number is a more subtle concept than may at first appear to be the case. We will consider this (possibly disturbing) issue further in Chapter 10.

### 6.3. The Weierstrass-Stolz model.

Representing a positive real number \( x \) by an infinite decimal expansion \( a_0.a_1a_2a_3\ldots \) makes perfect sense once
the set $\mathbb{R}$ has been defined: for any $m \geq 1$, we call the \textit{finite} decimal expansion of order $m$, $x(m) = a_0.a_1a_2a_3 \ldots a_m$, the $m^{th}$ \textit{truncation} of this expansion (with the proviso, as indicated below, that a terminating expansion is shown in its ‘recurring nines’ form).

Then $x(m)$ represents the \textit{rational} number

$$x(m) = \frac{10^m a_0 + 10^{m-1} a_1 + \ldots + a_m}{10^m}.$$

The sequence of truncations $(x(m))_{m \geq 1}$ is non-decreasing (at each decimal place we add a non-negative term) and it is certainly bounded above by $a_0 + 1$. By the completeness of $\mathbb{R}$ this means that the sequence $(x(m))_m$ converges to a real number, namely the supremum of the sequence. Each $x(m)$ is a partial sum of the infinite series defining this supremum and writing $x = a_0.a_1a_2\ldots a_n\ldots$ is a short-hand notation for the sum of the series. In this sense we can now exhibit any irrational as the \textit{limit} of a sequence of rationals, as Cauchy wished to do.

This argument can be turned on its head, providing a more ‘concrete’ model of real numbers—although the above characterisation of irrationals as aperiodic expansions suggests that infinite decimal expansions are rather less familiar than they seem! The truncations of an arbitrary infinite decimal expansion define \textit{lower numbers} for a Dedekind cut that yields a real number $x$. Moreover, they will approach $x$ arbitrarily closely, as the series they define converges to it.

As we have observed, for certain \textit{rational} cuts there is ambiguity: for $r = \frac{q}{10^m}$ we can choose the infinite decimal expansion either in the form

$$a_0.a_1a_2\ldots a_m.0000$$

or, alternatively, as

$$a_0.a_1a_2\ldots (a_m - 1)999\ldots$$

since these two series have the same (rational) sum. For example, $\frac{1}{2} = 0.50000\ldots$ or $0.49999\ldots$. Dedekind’s choice that the lower numbers of a cut should \textit{not} have a greatest member is reflected by taking the ‘recurring nines’ expansion whenever this occurs—this choice constitutes an equivalence relation on the set of decimal expansions, just as Dedekind’s choice led to equivalence classes of cuts.

Thus, instead of using Dedekind cuts, we could begin with the set of positive infinite decimal expansions as defined above, impose the equivalence relation just described, and mimic the logic of Dedekind’s arguments.

First, define the order relation $<$ for infinite decimal expansions as follows: if $a = a_0.a_1a_2\ldots a_n\ldots$ and $b = b_0.b_1b_2\ldots b_n\ldots$, define $a < b$ if there is a $k \geq 0$ such that $a_i = b_i$ for all $i < k$ and $a_k < b_k$. 

6. \textbf{DECIMAL EXPANSIONS}
It is easy to see that the trichotomy holds for $<$, and we can define upper bounds as before. The key result is (again) that any set of infinite decimal expansions that is bounded above will have a least upper bound.

In other words, the set of positive infinite decimal expansions has the completeness property. Extending this to all expansions and, in particular, defining the arithmetical operations $(+,	imes)$ for negative numbers, is somewhat more intricate. Checking the arithmetical axioms can become tedious, so we will not pursue the matter here—an outline, including an elementary proof of completeness and the definition of arithmetical operations, can be found in MM. This approach is sometimes referred to as the Weierstrass-Stolz model of the reals—after Vorlesungen über Allgemeine Arithmetik, published in 1885 by Weierstrass’ former student Otto Stolz (1842-1905).

7. Algebraic and constructible numbers

Motivated by the solution of the ‘three famous problems’ of antiquity (see Chapter 3), we can identify various classes of real numbers in a different way. Recall that Plato reports the discovery by Thaeetetus that (in our terminology) positive square or cube roots of natural numbers are either natural or irrational numbers.

7.1. Roots. We place this in a more general setting: given any $m$ in $\mathbb{N}$, the positive $m^{th}$ root of a natural number $N$ is the unique positive solution of the equation $x^m = N$, and is written as $x = \sqrt[m]{N}$.

If $x = \sqrt[m]{N}$ is rational, then we can find relatively prime natural numbers $a,b$ such that $x = \frac{a}{b}$. Now solve the equation $(\frac{a}{b})^m = N$, so that $a^m = Nb^m$. Write the unique prime factorisation of $b$ as $b = p_1^{a_1} \ldots p_k^{a_k}$. Then every prime $p_i$ on the right divides $b$, so it must also divide $a^m$. Since $p_i$ is prime, it now divides $a$, using the extension of Euclid’s lemma we proved in Section 2. So $a$ and $b$ are relatively prime, yet have every $p_i$ as a common factor, which is impossible unless $b = 1$, so that $N = a^m$. Hence the Fundamental Theorem of Arithmetic immediately generalises Thaeetetus’ result, proving that:

$\sqrt[m]{N}$ is irrational unless $N = a^m$ for some natural number $a$.

This result provides us with an unlimited collection of different irrational numbers. In particular, this collection includes $\sqrt[3]{2}$, which, if it could

\[ \frac{1}{10} \text{ becomes } -\frac{1}{10}, \text{ which is less than } -\frac{1}{2}, \text{ in the ordering as defined here: the initial digits and the first decimal digits are equal, and in the second decimal place } 4 \text{ is less than } 5. \]

(We would also replace these terminating expansions by their ‘recurring nines’ version.)
be constructed by straightedge and compass, would solve the ancient problem of the duplication of the cube, considered in Chapter 3.

7.2. Algebraic numbers. The positive $m^{th}$ root of $N$ arises as the root of the polynomial $x^m - N = 0$. In Chapter 4, the Fundamental Theorem of Algebra showed that any polynomial of degree $m$ will have exactly $m$ (not necessarily distinct) roots belonging to the complex number system $\mathbb{C}$. This leads to a definition:

**Definition:**

An algebraic number is a solution of a polynomial equation of the form

$$c_m x^m + c_{m-1} x^{m-1} + \ldots + c_1 x + c_0 = 0,$$

where the $c_i$ are integers (or, equivalently, are rational numbers).

By the Fundamental Theorem of Algebra, this equation has $m$ solutions in $\mathbb{C}$.

In particular, the rational $r = \frac{a}{b}$ is an algebraic number, since it is the root of the equation $bx + (-a) = 0$.

We denote the set of all real algebraic numbers by $\mathbb{A}$. This includes $\mathbb{Q}$, but is considerably larger, as it includes all positive $m^{th}$ roots of natural numbers, for example. Sums and differences of square roots are similarly included. For example, if $a, b$ are natural numbers, then $x = \sqrt{a} + \sqrt{b}$ satisfies $x^2 = (\sqrt{a} + \sqrt{b})^2 = a + b + 2\sqrt{ab}$ and, collecting terms and squaring again, we obtain $(x^2 - (a + b))^2 = 4ab$ which becomes the polynomial

$$x^4 - 2(a + b)x^2 + (a - b)^2 = 0.$$

In fact, the set of real algebraic numbers includes all 23 classes of incommensurables identified (with considerably greater effort) by Euclid in Book X of the Elements: the surds he considered all lead to polynomial equations whose degree is a power of 2. So all Euclid’s classes of incommensurables belong to the set of real algebraic numbers.

7.3. Constructible numbers. The set of real algebraic numbers includes the solutions of the first two ‘famous problems’ of antiquity. First, the duplication of the cube involves constructing a length of $\sqrt[3]{2}$, which is a real algebraic number. Second, we saw in Chapter 3 that the trisection of the general angle, leads to the cubic equation $4z^3 - 3z - c = 0$, where $c = \cos \phi$ for the given angle $\phi$. If $c$ is rational, the three complex roots of the cubic are algebraic numbers. But the Intermediate Value Theorem ensures that any cubic has at least one real root, since the polynomial is negative for large negative $z$ and positive for large positive $z$. In our example, when $\phi = 60^\circ$ we know that $c = \frac{1}{2}$, so the cubic equation becomes $8z^3 - 6z - 1 = 0$, whose roots include the real algebraic number $z = \cos 20^\circ$.
But, although they are algebraic numbers, neither $\cos 20^\circ$ nor $\sqrt[3]{2}$ represent lengths that can be constructed by straightedge and compass alone. In 1837 the French mathematician Pierre Wantzel (1818-1848) defined the class of constructible numbers as numbers that correspond to lengths of such line segments. Using a method now known as field extensions, Wantzel proved that these are precisely the numbers that can be obtained by repeated use of the four arithmetical operations ($+, -, \times, \div$) and square root extraction. Obtaining a constructible length from a rational length by straightedge and compass therefore implies that this length represents the root of a polynomial equation with rational coefficients whose degree is a power of 2.

We know that $\sqrt[3]{2}$ and $\cos 20^\circ$ are roots of cubic equations, and one can prove that they cannot satisfy an equation whose degree is a power of 2. Thus neither is a constructible number.

Therefore, the set $\mathbb{A}$ of real algebraic numbers includes all constructible numbers as a proper subset, and the set of constructible numbers includes the rationals as a proper subset. All three are of course infinite subsets of the real number system $\mathbb{R}$. We might reasonably ask if there are any irrationals, representable by aperiodic decimal expansions, that are not algebraic numbers?

8. Transcendental numbers

The third ‘famous problem’ of antiquity asked for the side of the square with area equal to that of a given circle—this is often called the quadrature of the circle. In the simplest case the circle has unit radius, so that its area is $\pi$, and the side of the square we seek is $\sqrt{\pi}$. It turns out that this number, and $\pi$ itself, are not algebraic numbers—and neither is the irrational number Euler had named $e$, the base of natural logarithms (see Chapter 5).

Real numbers that are not algebraic are called transcendental – the term was first used in this context by Euler, following Leibniz’ choice of this name for curves that Descartes had called ‘mechanical’. But at that stage no one had a proof that such numbers exist.

The earliest candidate to be examined closely was the familiar number $\pi$. In 1768 the Swiss polymath Johann Heinrich Lambert (1728-1777) proved that $\pi$ is irrational and conjectured (with a sketch plan for a possible proof) that it must be transcendental. Similarly, in 1806, Legendre, who had shown that $\pi^2$ is irrational, concluded about $\pi$:

\[\text{In the classic text [7] Courant and Robbins provide a fairly detailed description of Wantzel’s methods. Wantzel’s paper aroused little interest and was largely forgotten for nearly a century (see a recent account by Jesper Lützen in Historia Mathematica 36 (2009) pp. 374-394). Also see MM for a remarkable result concerning the construction of regular polygons inscribed in a circle, largely proved by Gauss and later completed by Wantzel.}\]
'It is probable that it is not even contained among the algebraic irrationals; in other words it cannot be the root of an algebraic equation with a finite number of terms, and rational coefficients. However, it seems difficult to prove this theorem rigorously.'

In antiquity, various attempts, some of them ingenious, were made to square the circle.

The quadratrix of Hippias, described in Chapter 3 as an angle trisector, provided an early ‘solution’ (based on Figure 16(b)) but this curve cannot be constructed by ruler and compass, as Euclid demands. Although no direct written account confirms it, most historians accept the report by the fourth century commentator Pappus that it was Menaechmus’ brother Dinostratus (about whom not much else is known) who made this discovery around 350 BCE. Pappus was well aware that this does not provide a straightedge-and-compass construction, as the quadratrix cannot be constructed by these means. But his report reflects the name that has survived for this curve, relating it to squaring the circle rather than trisecting the angle.

A different approach, unsuccessful but illustrating the level of sophistication achieved at that time, is preserved in an even earlier fragment by Hippocrates of Chios. He was able to square various types of lunes (crescent-shaped figures bounded by two circular arcs of unequal radii). He then noted that he would be able to square the circle if he could square the lunes created by a semicircle with half a regular inscribed hexagon and three semicircles with diameters equal to the sides of the hexagon. However, squaring these particular lunes proved elusive. (See MM for details of the above constructions.)

The spiral of Archimedes (see Chapter 5) provides a further quadrature of the circle. In Figure 37 the spiral starts at the point $O$, while $P$ is the
point reached at the first full turn of the circle. The tangent to $P$ meets the
line perpendicular to $OP$ at $T$. In Proposition 19 of his treatise *On Spirals*,
Archimedes shows that the line segment $OT$ equals the circumference of
the circle $OP$. If $OP = r$ this means that $OT = 2\pi r$, so that the area of
the right-angled triangle $TOP$ equals that of the circle $OP$. Constructing a
square with this area is then a simple matter.

These geometric constructions bring us no closer to a criterion for decid-
ing when a given number must be transcendental, or to define an example of
such a number arithmetically. This required a radically different approach,
developed in the mid-nineteenth century.

8.1. **Rapid approximation by rationals.** The breakthrough, showing
that transcendental numbers exist, was made in 1844 by the French mathe-
matician Joseph Liouville (1809-1882), who was the first to identify a specific
number that he could prove to be transcendental. His approach was to con-
sider ways in which one might distinguish between the two classes of alge-
bric and transcendental numbers by considering the speed with which such
numbers can be approximated by rationals.

It may seem counter-intuitive at first, but what separates the two classes
is that transcendental numbers allow rational approximations of greater ra-
pidity than algebraic numbers do! To make this statement more precise, con-
sider the approximation of an arbitrary real number by a rational number.$^{13}$

We can find infinitely many rationals between any two distinct real num-
bers. On the other hand, consider the distance between two distinct rational
numbers $r = \frac{a}{b}$ and $s = \frac{c}{d}$ (taking $b$ and $d$ as positive). We obtain

$$|r - s| = \left| \frac{a}{b} - \frac{c}{d} \right| = \frac{|ad - bc|}{bd} \geq \frac{1}{bd}.$$ 

The final inequality follows from Dedekind’s definition of rational numbers:
if we have $ad = bc$, then $r = s$. Thus, for distinct $r, s$, the distance $|ad - bc|$ is
at least 1, as $a, b, c, d$ are integers. In other words, if we try to approximate
$s = \frac{c}{d}$ by the rational $r$, we cannot get closer than the reciprocal of the product
of the denominators of the two fractions (in lowest form) representing these
rationals. We can approximate a fixed rational $s = \frac{c}{d}$ as closely as we please
by another rational, but to get very close to $s$ with $r = \frac{a}{b}$, we must expect
the denominator $b$ of $r$ to become very large.

Next, suppose that we wish to approximate a given real number $x$ by a
rational number $r = \frac{a}{b}$ in such a way that the distance between them is less
than the square of the denominator of $r$, that is

$$|x - r| < \frac{1}{b^2}.$$ 

$^{13}$We follow [18] pp.159-163, in the arguments given here. The approximation of real num-
bers by rationals is a much wider topic, discussed in more detail there.
If \( x = s = \frac{c}{d} \) is also rational, we have just seen that the distance is at least \( \frac{1}{bd} \), which is less than \( \frac{1}{b^2} \) only if \( b < d \). Hence, if \( x = s \) is rational, there can only be \( (d - 1) \) choices for the denominator \( b \) of the approximating rational \( r = \frac{a}{b} \) if the desired inequality is to hold. In other words, there are only finitely many (in fact, fewer than \( d \)) different rationals which lie closer to \( s = \frac{c}{d} \) than the square of their denominator.

This suggests the following definition.

**Definition:**

The real number \( x \) is **approximable by rationals to order** \( n \) if there is a number \( K \), depending only on \( x \), such that we can find infinitely many rationals \( \frac{a}{b} \) that satisfy the condition \( |x - \frac{a}{b}| < \frac{K}{b^n} \).

With this definition, any rational number is approximable by (other) rationals to order 1, since the identity \( |r - s| = \frac{|ad - bc|}{bd} \) shows that the rational \( s = \frac{c}{d} \) is approximated to within \( \left( \frac{|ad - bc|}{b^2} \right) \) by a rational \( r = \frac{a}{b} \), and for given \( c, d \) we can find infinitely many \( a, b \) to satisfy the equation \( ad - bc = 1 \) (since, with \( c, d \) known, this is a single linear equation in the two unknowns \( a, b \)). Since \( d \) is a natural number, \( \frac{1}{d} \leq 1 \), and it follows that, if we choose any \( K > 1 \), there are infinitely many rationals \( \frac{c}{d} \) such that \( |s - \frac{a}{b}| < \frac{K}{b^n} \).

However, the condition \( |s - \frac{a}{b}| < \frac{1}{b^2} \) is possible only if \( b < d \), so it follows that \( s \) is not approximable by rationals to order 2 (and hence to any order higher than 1). Whatever the choice of the constant \( K \) (which depends only on \( s \)) we have fewer than \( Kd \) different choices of \( r = \frac{a}{b} \), with \( a, b \) relatively prime, such that \( |s - \frac{a}{b}| < \frac{K}{b^n} \).

Recall that a real algebraic number \( a \) is the root of a polynomial with rational coefficients. We say that the **degree** of \( a \) is the **smallest** degree of a polynomial which has \( a \) as a real root. From the above, orders of approximation appear to be connected to the degree of the polynomial that defines a given algebraic number—after all, among algebraic numbers it is the **rationals** that are defined by polynomials of degree 1.

Liouville proved the following remarkable theorem:

**A real algebraic number of degree** \( n \) **is not approximable by rationals to any order greater than** \( n \).

(The proof makes more significant demands on the reader’s background and technical facility than we have done hitherto, and is omitted here. The interested reader can find a version of the proof in MM.)

He now had a criterion for determining that certain numbers must be transcendental:

**Corollary:** **Any real number approximable by rationals to all orders must be transcendental.**
Liouville proceeded to define a number that he could prove to be transcendental, based on the above theorem. He considered the sum of an infinite series of negative powers of $10$, using only $0$ or $1$ in the numerator, with the $k^{th}$ use of the digit $1$ occurring after $k!$ steps, that is, as $\frac{1}{10^k}$. Thus the first $1$ appears in the first decimal place, the second in the second place ($2! = 2$), the third in the sixth place ($3! = 6$), the fourth in the $24^{th}$ place, and so on. This leads to

Liouville’s constant: $L = \frac{1}{10^1} + \frac{1}{10^2} + \ldots + \frac{1}{10^{k!}} + \ldots$

The decimal expansion of $L$ starts with $0.1100010000000000000001000\ldots$

Notethatthenext$1$willoccuratthe$120^{th}$place after the decimal point, the one after that at the $720^{th}$ place, the next at the $5040^{th}$ place, and so on.

The series defining $L$ can easily be compared with a geometric one in order to prove that $L$ is a real number. Using the theorem Liouville proved, it is then easy to see that $L$ must be transcendental.

The $k^{th}$ partial sum of the series defining $L$ can be written as $r_k = \frac{p}{q_k}$, where

$p = 10^{k!-1} + 10^{k!-2} + 10^{k!-6} + 10^{k!-24} + \ldots + 10^{k!-l!} + \ldots + 1$

becomes the numerator when the first $k!$ terms are combined, since all other negative powers of $10$ up to $k!$ have numerator $0$. All terms of the series are positive, so $r_k < L$. The distance between $L$ and its $k^{th}$ truncation is

$L - r_k = \frac{1}{10^{(k+1)!}} + \frac{1}{10^{(k+2)!}} + \ldots$

How should we compute this infinite sum?

We can estimate the terms on the right by taking out the first term as a common factor and comparing the remaining terms with those of a geometric series:

$L - r_k = \frac{1}{10^{(k+1)!}} \{1 + \frac{1}{10^{(k+2)}} + \frac{1}{10^{(k+2)(k+3)}} + \ldots\}$

$< \frac{1}{10^{(k+1)!}} \{1 + \frac{1}{10} + \frac{1}{10^2} + \ldots\}$

$= \frac{1}{10^{(k+1)!}} \left(\frac{10}{9}\right)$

In each case we have replaced each of the exponents in the terms in the final brackets, replacing each of $(k + 2), (k + 2)(k + 3), \ldots$, by $1$, to obtain the second line, since $10^1 < 10^{k+2}, 10^2 < 10^{(k+2)(k+3)}, \ldots$. Since $\lim_{k \to \infty} \left(\frac{1}{10^{(k+1)!}}\right) = 0$, we conclude that $\lim_{k \to \infty} r_k = L$ is in $\mathbb{R}$.

To show that $L$ is approximable by rationals to all orders, fix a natural number $n$. For any $k \geq n$ we have found a rational $r_k = \frac{p_k}{q_k}$ where $q_k = \frac{1}{10^{k!}}$ and $p_k$ is the corresponding integer $p$, as above, such that, with $K = \frac{10}{9}$,

$\left|L - \frac{p_k}{q_k}\right| < K \frac{1}{10^{(k+1)!}} = K \frac{1}{q_k^{k+1}} < \frac{K}{q_k^n}$.
For arbitrary choices of \( n \), we always find infinitely many such rationals, namely the sequence \( r_{n+1}, r_{n+2}, \ldots, r_{n+m}, \ldots \). By the above theorem \( L \) is approximable by rationals to all orders, and therefore transcendental.

This proof is straightforward because the number \( L \) was chosen to make the application of the theorem as simple as possible. Liouville’s achievement was to find a workable criterion against which certain numbers could be tested for rapid approximation by rationals.

Proofs that the ‘well-understood’ numbers \( \pi \) (defined by a geometric relationship, or as the sum of Leibniz’ series \( 4(1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \ldots) \)) or \( e \) (defined as the sum of \( 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \ldots \), or as \( \lim_{n \to \infty} (1 + \frac{1}{n})^n \)), are transcendental, require much more advanced techniques that we cannot pursue here. The transcendence of \( e \) was proved by Charles Hermite (1822-1901) in 1873, and this was followed in 1882 by a proof of the transcendence of \( \pi \) by Ferdinand von Lindemann (1852-1939). He used Hermite’s approach to show that \( e^b \) is transcendental for any non-zero algebraic number (real or complex). By Euler’s identity \( e^{i\pi} = -1 \), this showed that \( i\pi \), and hence \( \pi \), must be transcendental.

The influential German mathematician David Hilbert famously posed a list of 23 problems at the meeting in Paris in 1900 of the International Congress of Mathematicians. The seventh problem asked whether, given algebraic numbers \( a, b \), with \( b \) irrational, the number \( a^b \) is always transcendental. In 1934, two mathematicians, Alexander Gelfond and Theodor Schneider, proved independently that this is true, providing a unified way of solving many problems that had been posed in number theory. Their result shows, for example, that \( 2^{\sqrt{2}} \) is transcendental.
