Module MA1S11 (Calculus)
Michaelmas Term 2016
Section 1: Sets and Number Systems

D. R. Wilkins

Contents

1 Sets and Number Systems

1.1 Sets

A *set* is a collection. The objects that belong to a set are referred to as the *elements* of the set. Those elements may for example be numbers, other sets, or other objects studied in a mathematical investigation.

We use the notation $p \in X$ to specify that an object p is an element of a set X.

We use the notation $p \notin X$ to specify that an object p is *not* an element of a set X.

When the number of elements in a set is sufficiently small, the set can be specified by listing those elements in braces.

Example Let X denote the set consisting of the first five prime numbers. This set can be specified as follows:

$$X = \{2, 3, 5, 7, 11\}.$$

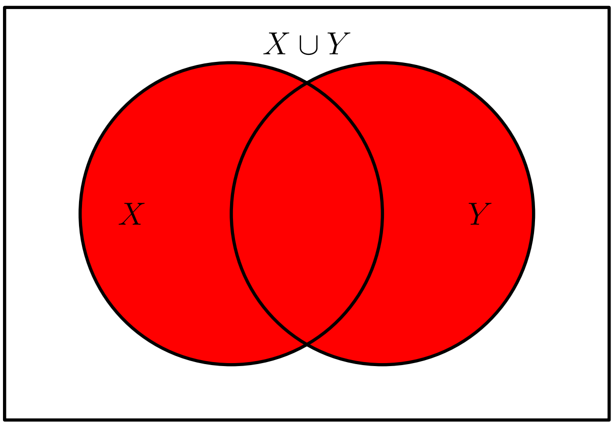
Then $3 \in X$ and $11 \in X$. But $42 \notin X$.

Let X and Y be sets. If the set X has the same elements as the set Y then the sets X and Y are equal (and are indeed the same set), and we may denote this by writing $X = Y$.

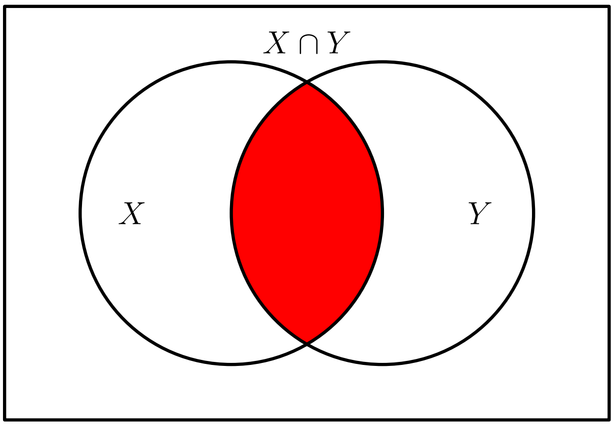
It follows that if sets X and Y satisfy $X \neq Y$, then either there exists an element of one of the two sets that is not an element of the other.

Example Let $X = \{1, 2, 3, 4, 5\}$ and $Y = \{5, 4, 3, 2, 1\}$. Then $X = Y$.

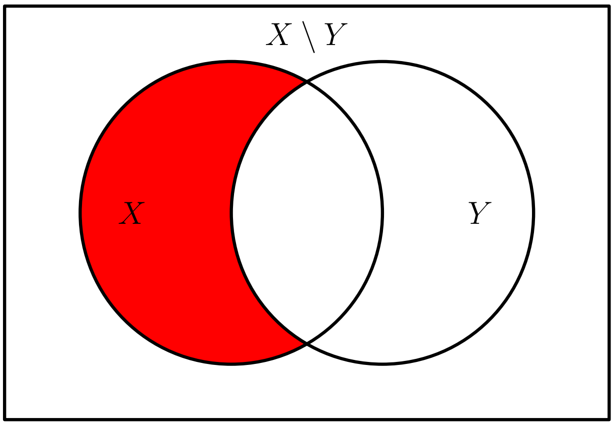
Given sets X and Y, we denote by $X \cup Y$ the *union* of the sets X and Y. This is the set consisting of those elements that belong either to X or else to Y. (This includes those elements that belong to both X and Y.)



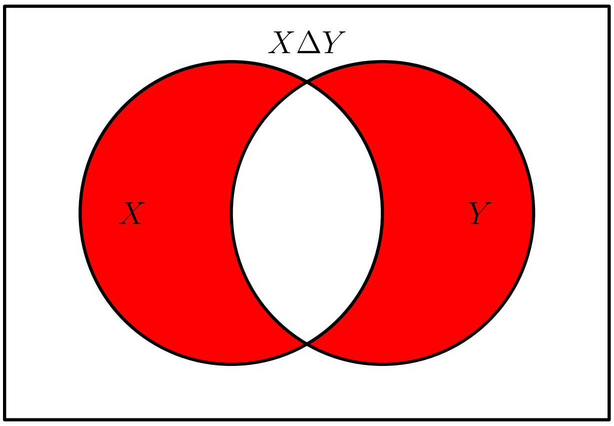
Given sets X and Y, we denote by $X \cap Y$ the *intersection* of the sets X and Y. This is the set consisting of those elements that belong to both X and Y.



Given sets X and Y, we denote by $X \setminus Y$ the *difference* of the sets X and Y. This is the set consisting of those elements that belong to the set X but not to the set Y.



The *symmetric difference* $X \Delta Y$ of sets X and Y is the union of the sets $X \setminus Y$ and $Y \setminus X$.



The definition of the symmetric difference $X \Delta Y$ of the sets X and Y ensures that

$$X \Delta Y = (X \setminus Y) \cup (Y \setminus X).$$

The symmetric difference $X \Delta Y$ of sets X and Y consists of all elements that belong to exactly one of the sets X and Y. One can verify that

$$X \Delta Y = (X \cup Y) \setminus (X \cap Y).$$

The set with no elements is referred to as the *empty set*, and is denoted by $\emptyset$.

Let X and Y be sets, and let p be an object. Then

- $p \in X \cup Y$ if and only if either $p \in X$ or $p \in Y$;
- $p \in X \cap Y$ if and only if both $p \in X$ and $p \in Y$;
- $p \in X \setminus Y$ if and only if $p \in X$ but $p \notin Y$.

Example Let

$$X = \{2, 4, 6, 8, 10\}$$

and

$$Y = \{6, 7, 8, 9, 10\}.$$

Then

$$\begin{aligned} X \cup Y &= \{2, 4, 6, 7, 8, 9, 10\}, \\ X \cap Y &= \{6, 8, 10\}, \\ X \setminus Y &= \{2, 4\}, \\ Y \setminus X &= \{7, 9\}. \end{aligned}$$

Unions and intersections of three or more sets can be defined and represented by notation analogous to that adopted for unions and intersections of two sets. For example, if W, X, Y, and Z are sets then the union

$$W \cup X \cup Y \cup Z$$

of the sets W, X, Y and Z consists of everything that belongs to at least one of the sets W, X, Y and Z, and the intersection

$$W \cap X \cap Y \cap Z$$

of the sets W, X, Y and Z consists of everything that belongs to every one of the sets W, X, Y and Z,

When constructing sets from others using the basic set operations of union, intersection and set difference, it is often necessary to specify the order of evaluation using parentheses $\bigl(\cdots\bigr)$.

Example Let W, X, Y and Z be sets. The set

$$(W \cup X) \cap (Y \cup Z)$$

is formed by first forming the union $W \cup X$ of the sets X and W, forming also the union $Y \cup Z$ of the sets Y and Z, and then forming the intersection of the resulting sets $W \cup X$ and $Y \cap Z$.

Let X and Y be sets. If every element of the set X is an element of the set Y then we say that the set X is a *subset* of the set Y, and we denote this fact by writing $X \subset Y$.

If the set X is *not* a subset of the set Y, then we can denote this fact by writing $X \not\subset Y$.

Example Let $X = \{1, 3, 5\}$, $Y = \{1, 2, 3, 4, 5\}$ and $Z = \{2, 3, 4, 5\}$. Then $X \subset Y$ and $Z \subset Y$, but $X \not\subset Z$.

1.2 Determining Subsets by Conditionals

Let X be a set, and let $P(x)$ represent some conditional that may or may not be satisfied by elements x of the set X. The notation

$$\{x \in X \mid P(x)\}.$$

then specifies the subset of X consisting of those elements x of the set X that satisfy the condition $P(x)$.

Example Let

$$X = \{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\},$$

and let

$$W = \{x \in X \mid x^2 > 11\}.$$

Then

$$W = \{-5, -4, 4, 5\}.$$

Remark In the mathematical literature, it is commonplace to find notation of the form

$$\{x \in X : P(x)\}$$

in place of

$$\{x \in X \mid P(x)\}.$$

The set W is thus specified in this alternative notation as follows:—

$$W = \{x \in X : x^2 > 11\}.$$

1.3 Cartesian Products of Sets

Let X and Y be sets. The *Cartesian product* $X \times Y$ of the sets X and Y is the set consisting of all ordered pairs (x, y) for which $x \in X$ and $y \in Y$.

Example Let $X = \{1, 2, 3\}$ and $Y = \{8, 9\}$. Then

$$X \times Y = \{(1, 8), (2, 8), (3, 8), (1, 9), (2, 9), (3, 9)\}.$$

One may define in an analogous fashion the Cartesian product of three or more sets. Thus the Cartesian product $X \times Y \times Z$ of three sets X, Y and Z consists of all ordered triples (x, y, z) for which $x \in X$, $y \in Y$ and $z \in Z$.

Remark We have considered examples of sets whose elements are numbers. Provided that the set itself is a well-defined collection of elements, the definition of *sets* imposes no restriction on what those elements might be. The elements of the set might be numbers, or characters taken from some alphabet, or strings of characters, or colours, or molecules, or students registered for a particular module. For example, the following is a perfectly valid example of a set

$$\{1, 2, 59.7, \text{‘Dog’}, \text{‘Cat’}\}.$$

1.4 The System of Natural Numbers

The positive whole numbers $1, 2, 3, 4, 5, \ldots$ are referred to as *natural numbers*. They are also known as the *positive integers*.

The set consisting of all natural numbers is denoted by $\mathbb{N}$.

1.5 Summation of Finite Sequences of Numbers

Let $T_1, T_2, T_3, \ldots$ be an infinite seqeuence of real and complex numbers, and let

$$\begin{aligned} S_1 &= T_1, \\ S_2 &= T_1 + T_2, \\ S_3 &= T_1 + T_2 + T_3, \\ &\vdots \\ S_n &= T_1 + T_2 + T_3 + \cdots + T_n. \end{aligned}$$

Then S_n is the sum of the first n members of the infinite sequence $T_1, T_2, \ldots, T_n$.

The identity

$$S_n = T_1 + T_2 + T_3 + \cdots + T_n$$

is expressed more concisely in standard mathematical notation by writing

$$S_n = \sum_{j=1}^{n} T_j.$$

Similarly, we write

$$\sum_{j=p}^{q} T_j = T_p + T_{p+1} + \cdots + T_{q-1} + T_q.$$

We can read "$\sum_{j=p}^{q} T_j$" as specifying "the sum of the quantities T_j as j ranges over all integers between p and q inclusive".

Note that any letter may be used as the "index of summation" in place of index j of summation, other than those that are already in use, or appear in formulae for the "limits of summation" above and below the $\sum$ symbol. Thus

$$\sum_{j=1}^{n} T_j = \sum_{k=1}^{n} T_k = \sum_{m=1}^{n} T_m, \quad \text{etc.}$$

Note that

$$\sum_{j=1}^{n} T_j = \sum_{k=r+1}^{r+n} T_{k-r}$$

for all integers r, because both sums involve a summation of quantities T_j with $j = 1, 2, \ldots, n$. In particular,

$$\sum_{j=0}^{n-1} T_{j+1} = \sum_{j=1}^{n} T_j = \sum_{j=2}^{n+1} T_{j-1}.$$

1.6 The Principle of Mathematical Induction

For each natural number n, let $P(n)$ be some property, in general dependent on the value of the natural number n, that must be either true or false. The Principle of Mathematical Induction asserts that the property $P(n)$ must be true for all natural numbers n provided that the following two conditions are satisfied:—

(i) $P(1)$ is true;

(ii) if $P(k)$ is true for some natural number k, then so is $P(k+1)$.

In order to illustrate the procedure for setting out a proof using the Principle of Mathematical Induction, we establish the formula stated in the following proposition, which establishes a formula for the sum of the first n terms of an arithmetic sequence.

Proposition 1.1 *For each natural number n, let*

$$T_n = a + (n-1)d,$$

and let

$$S_n = \sum_{j=1}^{n} T_j = T_1 + T_2 + \cdots + T_n.$$

Then

$$S_n = \frac{n}{2}\left(2a + (n-1)d\right).$$

Proof using the Principle of Mathematical Induction Let

$$U_n = \frac{n}{2}\left(2a + (n-1)d\right)$$

for all natural numbers n. We must prove that $S_n = U_n$ for all natural numbers n.

Now $S_1 = T_1 = a$ and

$$U_1 = \frac{1}{2}(2a + 0 \times d) = a.$$

It follows that $S_1 = U_1$. Thus the identity $S_n = U_n$ we are seeking to prove is valid when $n = 1$. (We have now accomplished the *base step* of the induction proof.)

Now let k denote some natural number for which $S_k = U_k$, so that

$$S_k = \frac{k}{2}\left(2a + (k-1)d\right).$$

The definition of S_n for all natural numbers n ensures that $S_{k+1} = S_k + T_{k+1}$, and thus

$$S_{k+1} = S_k + a + kd.$$

The definition of U_n for all natural numbers n ensures that

$$\begin{aligned} U_{k+1} &= \frac{k+1}{2}\left(2a + ((k+1)-1)d\right) \\ &= \frac{k}{2}(2a + kd) + \frac{1}{2}(2a + kd) \\ &= \frac{k}{2}(2a + (k-1)d) + \frac{kd}{2} + \frac{1}{2}(2a + kd) \\ &= U_k + \frac{kd}{2} + \frac{1}{2}(2a + kd) \\ &= U_k + a + kd. \end{aligned}$$

Now k has been chosen subject to the requirement that $S_k = U_k$. It follows from the above calculations that

$$S_{k+1} = S_k + a + kd = U_k + a + kd = U_{k+1}.$$

We have thus shown that that if the identity $S_n = U_n$ holds when $n = k$, then this identity also holds for $n = k + 1$. (We have thus completed the *inductive step* of the induction proof.)

It now follows from the Principle of Mathematical Induction that $S_n = U_n$ for all natural numbers n, as required. ∎

Second Proof of Proposition 1.1 Let

$$U_n = \frac{n}{2}\left(2a + (n-1)d\right)$$

for all natural numbers. Then there is always an infinite sequence

$$T_1, T_2, T_3, T_4, \ldots$$

with the property that

$$T_1 + T_2 + T_3 + \cdots + T_n = U_n$$

for all natural numbers n. We simply have to identify what the sequence $T_1, T_2, T_3, \ldots$ is whose sums satisfy the above formula.

Now if

$$T_1 + T_2 + T_3 + \cdots + T_n = U_n$$

for all natural numbers n then $T_1 = U_1$ and $T_n = U_n - U_{n-1}$ whenever $n > 1$. It follows that

$$T_1 = U_1 = \frac{1}{2}(2a - 0 \times d) = a.$$

Moreover if $n > 1$ then

$$\begin{aligned} T_n &= U_n - U_{n-1} \\ &= \frac{n}{2}\,(2a + (n-1)d) - \frac{n-1}{2}\,(2a + (n-2)d) \\ &= \frac{n}{2}\Big((2a - (n-1)d) - (2a - (n-2)d\Big) \\ &\qquad + \frac{1}{2}(2a + (n-2)d) \\ &= \frac{nd}{2} + \frac{1}{2}(2a + (n-2)d) = \frac{1}{2}(2a + (2n-2)d) \\ &= a + (n-1)d. \end{aligned}$$

Thus if $T_1, T_2, T_3, \ldots$ is the infinite sequence characterized by the property that

$$T_1 + T_2 + T_3 + \cdots + T_n = \frac{n}{2}\,(2a + (n-1)d)$$

for all natural numbers n then

$$T_n = a + (n-1)d$$

for all natural numbers n. The result follows. ∎

It follows directly from Proposition 1.1 that

$$\sum_{j=1}^{n} j = \tfrac{1}{2}n(n+1),$$

for all natural numbers n, where

$$\sum_{j=1}^{n} j = 1 + 2 + 3 + \cdots + n.$$

Third Proof of Proposition 1.1 Let n be a natural number. Consider the following table with two rows and n columns:—

1	2	3	4	$\cdots$	$n-1$	n
n	$n-1$	$n-2$	$n-3$	$\cdots$	2	1

Each row of the table sums to V_n, where

$$V_n = \sum_{j=1}^{n} j = 1 + 2 + 3 + 4 + \cdots + n.$$

Moreover there are n columns, and each column sums to $n + 1$. It follows that $2V_n = n(n + 1)$. because each side of this equality is equal to the sum of the numbers appearing as entries in the table. Dividing by 2, we find that

$$\sum_{j-1}^{n} j = \tfrac{1}{2} n(n + 1).$$

Now let $T_n = a + (n - 1)d$, where a and d are the initial value and increment respectively of the arithmetic sequence, and let

$$S_n = \sum_{j=1}^{n} T_j = T_1 + T_2 + T_3 + \cdots + T_n$$

for all natural numbers n. Then

$$\begin{aligned} S_n &= \sum_{j=1}^{n} (a + (j - 1)d) = (a - d)n + d \times \sum_{j-1}^{n} j \\ &= (a - d)n + \frac{d}{2} n(n + 1) \\ &= \frac{n}{2} \left(2(a - d) + (n + 1)d\right) \\ &= \frac{n}{2} \left(2a + (n - 1)d\right), \end{aligned}$$

as required. ∎

Remark The formula proved in Proposition 1.1 appears on page 22 of the booklet *Formulae and Tables* published by the State Examinations Commission (*Foirmlí agus Táblaí*, Coimisiún na Scrúduithe Stáit, SEC/PO 100000555-V5-Jan2016, p.22).

The Principle of Mathematical Induction had manifold applications in mathematics. In particular its application is not restricted to problems concerned with summation of sequences of numbers.

Example We use the method of Proof by Mathematical Induction to prove that $9^n - 1$ is divisible by 8 for all natural numbers n. Now if $n = 1$ then $9^n - 1 = 8$, and thus $9^n - 1$ is divisible by 8. Thus the proposition that $9^n - 1$ is divisible by 8 holds for $n = 1$.

Suppose that this proposition holds for $n = k$, so that k is some natural number for which $9^k - 1$ is divisible by 8. Now

$$\begin{aligned} 9^{k+1} - 1 &= (9^{k+1} - 9^k) + (9^k - 1) \\ &= (9 - 1) \times 9^k + (9^k - 1) \\ &= 8 \times 9^k + (9^k - 1). \end{aligned}$$

now both 8×9^k and $9^k - 1$ are divisible by 8, and the sum of two integers divisible by 8 must itself be divisible by 8. It follows that $9^{k+1} - 1$ is divisible by 8. Thus if the proposition that $9^n - 1$ is divisible by 9 holds for $n = k$ then it also holds for $n = k + 1$. Thus the proposition that $9^n - 1$ is divisible by 8 is true for all natural numbers n, as claimed.

1.7 The System of Integers

The whole numbers are referred to as *integers*. An integer may be positive negative or zero. The positive integers are the natural numbers. The negative integers are the numbers that take the form $-n$ for some natural number n. And of course 0 is the unique integer that is zero. The set consisting of all integers is denoted by $\mathbb{Z}$.

1.8 The System of Rational Numbers

A *rational number* is a number that can be expressed in the form p/q where both p and q are integers and $q \neq 0$. The set consisting of all rational numbers is denoted by $\mathbb{Q}$.

1.9 The System of Real Numbers

The rational numbers are not sufficient for the purposes of representing lengths in Euclidean geometry. Additional numbers such as $\sqrt{2}$ and π are required in order that lengths, angles and other physical magnitudes can be represented as "numbers". Such numbers are referred to as *irrational numbers*. The union of the sets of rational and irrational numbers is the set of *real numbers*. The set of real numbers is denoted by $\mathbb{R}$. If x and y are real numbers then so are $x+y$, $x-y$ and xy. Also x/y is a real number, provided that $y \neq 0$. Each positive real number x has a positive nth root $\sqrt[n]{x}$ that is a positive real number with the property that $(\sqrt[n]{x})^n = x$.

1.10 The System of Complex Numbers

The system of real numbers can be embedded within a larger number system whose elements are referred to as *complex numbers*. Any complex number may be represented in the form $a + bi$ where a and b are real numbers and i is a particular complex number that satisfies the equation $i^2 = -1$.

The set consisting of all complex numbers is denoted by $\mathbb{C}$.

Remark We have briefly described the sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ that represent the elements of the corresponding number systems, i.e., the systems of *natural numbers*, *integers*, *rational numbers*, *real numbers* and *complex numbers*. These sets are of particular importance in mathematics. Accordingly, once the basic concepts of set theory had taken root in the mathematical literature, it become commonplace for printers to represent these sets with letters **N**, **Z**, **Q**, **R** and **C** printed in boldface, to emphasize the fact that these letters are being used to denote the sets representing the basic number systems of mathematics. Of course mathematics lecturers, writing with chalk on blackboards, were not in a position to "print in boldface". Accordingly they distinguished the letters denoting these sets by adding extra strokes. The resulting glyphs accordingly were said to be written in "blackboard bold".

But once this notation became commonplace amongst mathematicians, when writing on blackboards or in handwritten manuscripts, they came to expect to see these special sets of numbers represented in the same fashion in print. Accordingly fonts were developed containing uppercase versions of the letters N, Z, Q, R and C, in the "blackboard bold" or "openface" style that had become commonplace amongst mathematicians.

1.11 The Laws of Indices for Integer Powers of Real Numbers

Let a be a real number. The positive integer powers a^n of a are defined such that $a^1 = a$ and $a^n = a^{n-1}a$ for all natural numbers n satisfying $n > 1$. This definition of positive integer powers of a real number a is an example of a *recursive definition* in which, for example, a^8 is defined in terms of a^7, which in turn is defined in terms of a^6, and so on.

Lemma 1.2 *Let a be a real number and let p and q be natural numbers. Then $a^{p+q} = a^p a^q$.*

Proof The identity $a^{p+q} = a^p a^q$ can be proved by induction on q. The recursive definition of a^{p+1} ensures that, for fixed p, $a^{p+q} = a^p a^q$ when $q = 1$. Suppose that $a^{m+k} = a^m a^k$ for some natural number k. Then

$$a^{m+k+1} = a^{m+k}a = (a^m a^k)a = a^m(a^k a) = a^m a^{k+1}.$$

Thus if the identity $a^{m+n} = a^m a^n$ holds when $q = k$ for some natural number k, then it also holds for $q = k + 1$. It follows from the Principle of Mathematical Induction that the identity $a^{p+q} = a^p a^q$ holds for all real numbers a and for all natural numbers p and q, as required. ∎

Remark As an alternative to the reasonably elaborate induction argument, one can simply note that the product of p copies of the real number a and q copies of that same real number a will be the product of $p + q$ copies of that number.

The strategy of proof by induction comes into its own in areas of mathematics like group theory and linear algebra (especially in considering powers of square matrices), where is is appropriate to present a formal argument that demonstrates the role of the Associative Law for multiplication (of group elements, or of square matrices) in establishing the result.

Lemma 1.3 *Let a be a real number and let p and q be natural numbers. Then $a^{pq} = (a^p)^q$.*

Proof First we note that $a^p = (a^p)^1$, and thus, for fixed p, the identity $a^{pq} = (a^p)^q$ holds when $q = 1$. Suppose that this identity holds when $q = k$ for some natural number k, so that $a^{pk} = (a^p)^k$. Then, from Lemma 1.2,

$$a^{p(k+1)} = a^{pk+p} = a^{pk}a^p = (a^p)^k a^p = (a^p)^{k+1}.$$

Thus if the identity $a^{pq} = (a^p)^q$ holds for $q = k$, then it also holds for $q = k + 1$. It follows from the Principle of Mathematical Induction that the identity $a^{pk} = (a^p)^k$ holds for all real numbers a and for all natural numbers p and q. ∎

Given any real number a, we define $a^0 = 1$. With this definition, the identity $a^p = a^{p-1}a$ that defines a^p recursively for $p > 1$ is also valid when $p = 1$.

Note that $0^0 = 1$, according to the definition just adopted. (The identity $0^0 = 1$ is the standard definition of 0^0 that ensures that many formulae valid for non-zero values of a remain true when $a = 0$.)

Lemma 1.4 *Let a be a real number and let p and q be non-negative integers. Then $a^{p+q} = a^p a^q$.*

Proof In the case when p and q are both positive, this follows from Lemma 1.2. Otherwise at least one of the non-negative integers p and q is zero, and the identity follows from the convention that $a^0 = 1$ for all real numbers a. ∎

Lemma 1.5 *Let a be a real number and let p and q be non-negative integers. Then $a^{pq} = (a^p)^q$.*

Proof In the case when p and q are both positive, this follows from Lemma 1.3. Otherwise at least one of the non-negative integers p and q is zero, and therefore $a^{pq} = 1 = (a^p)^q$. ∎

If the real number a is non-zero then a^n is defined for negative integers n so as to ensure that if $n = -q$, where q is a natural number, then $a^n = (a^q)^{-1}$.

Lemma 1.6 *Let a be a non-zero real number and let p and q be natural numbers. Then $a^{p-q} = \dfrac{a^p}{a^q}$.*

Proof The proof breaks down into three cases depending on whether $p - q$ is zero, positive or negative.

Suppose that $p - q = 0$. Then $p = q$ and therefore

$$\frac{a^p}{a^q} = \frac{a^p}{a^p} = 1 = a^0 = a^{p-q}.$$

Thus the result is true when $p - q$ is zero.

Next suppose that $p-q > 0$. It then follows from Lemma 1.2 $a^p = a^{p-q}a^q$. Rearranging this inequality, we find that

$$a^{p-q} = \frac{a^p}{a^q}.$$

Finally suppose that $p - q < 0$. Then

$$a^{p-q} = \frac{1}{a^{q-p}} = \frac{1}{\dfrac{a^q}{a^p}} = \frac{a^p}{a^q}.$$

We have therefore verified the result in all three cases determined by the sign of $p - q$. ∎

Proposition 1.7 *Let a be a non-zero real number and let m and n be integers (which may be positive, negative or zero). Then $a^{m+n} = a^m a^n$.*

Proof Let a be a non-zero real number, let m and n be integers. Choose natural numbers p, q, r and s such that $m = p - q$ and $n = r - s$. Applying Lemma 1.6, we find that

$$a^m a^n = a^{p-q} a^{r-s} = \frac{a^p}{a^q} \times \frac{a^r}{a^s} = \frac{a^p a^r}{a^q a^s} = \frac{a^{p+r}}{a^{q+s}} = a^{p+r-q-s} = a^{m+n},$$

as required. ∎

Proposition 1.8 *Let a be a non-zero real number and let m and n be integers (which may be positive, negative or zero). Then $a^{mn} = (a^m)^n$.*

Proof In the cases where $m = 0$ and $n = 0$, both a^{mn} and $(a^m)^n$ are equal to 1, and therefore $a^{mn} = a^m a^n$ in these cases.

In the case where $m > 0$ and $n > 0$, the identity $a^{mn} = a^m a^n$ follows directly from Lemma 1.3.

Now let p and q be positive integers. Then

$$a^{-pq} = \frac{1}{a^{pq}} = \frac{1}{(a^p)^q} = \left(\frac{1}{a^p}\right)^q = (a^{-p})^q.$$

and

$$a^{-pq} = \frac{1}{a^{pq}} = \frac{1}{(a^p)^q} = (a^p)^{-q}.$$

Also

$$a^{pq} = (a^p)^q = \left(\frac{1}{a^p}\right)^{-q} = (a^{-p})^{-q}.$$

Substituting in $m = \pm p$ and $n = \pm q$ therefore yields the required identity in all cases where both m and n are non-zero. This completes the proof. ∎

Proposition 1.9 *Let a and b be real numbers. Then $(ab)^n = a^n b^n$ for all non-negative integers n. Moreover if a and b are both non-zero then $(ab)^n = a^n b^n$ for all integers n.*

Proof Let a and b be real numbers. The identity $(ab)^n = a^n b^n$ holds when $n = 0$ because $a^0 = 1$, $b^0 = 1$ and $(ab)^0 = 1$.

The required identity can be established for positive values of n, and for all real numbers a and b using the Principle of Mathematical Induction. Indeed the identity $(ab)^n = a^n b^n$ is true when $n = 1$.

Suppose that this identity is true when $n = k$, so that $(ab)^k = a^k b^k$. Then

$$(ab)^{k+1} = (ab)^k (ab) = a^k b^k ab = a^{k+1} b^{k+1}.$$

Thus if the identity $(ab)^n = a^n b^n$ is true when $n = k$ then it is also true when $n = k + 1$. It follows from the Principle of Mathematical Induction that $(ab)^n = a^n b^n$ for all positive integers n.

Now suppose that n is negative and that both a and b are non-zero. Let $p = -n$. Then $(ab)^p = a^p b^p$. Taking the reciprocal of both sides, we find that

$$(ab)^n = \frac{1}{(ab)^p} = \frac{1}{a^p} \times \frac{1}{b^p} = a^{-p} b^{-p} = a^n b^n.$$

This completes the proof that the identity $(ab)^n = a^n b^n$ holds for all non-zero real numbers a and b and for all integer values of n, whether they be positive, negative or zero. ∎

1.12 Factorials and Binomial Coefficients

Definition The *factorial* $n!$ of a positive integer n is defined by the formula

$$n! = 1 \times 2 \times 3 \times \cdots \times n.$$

It is thus the product of the positive integers from 1 to n. The factorial $0!$ of zero is defined so that $0! = 1$.

The definition of factorials ensures that $n! = (n - 1)!n$ for all positive integers n.

Given non-negative integers n and r, where $0 \leq r \leq n$, the binomial coefficient $\begin{pmatrix} n \\ r \end{pmatrix}$ is defined by the formula

$$\begin{pmatrix} n \\ r \end{pmatrix} = \frac{n!}{r!(n-r)!}.$$

This definition ensures that

$$\begin{pmatrix} n \\ 0 \end{pmatrix} = \begin{pmatrix} n \\ n \end{pmatrix} = 1.$$

for all non-negative integers n.

Lemma 1.10 *Let n and r be positive integers, where $1 \leq r \leq n$. Then*

$$\begin{pmatrix} n \\ r \end{pmatrix} = \begin{pmatrix} n-1 \\ r-1 \end{pmatrix} + \begin{pmatrix} n-1 \\ r \end{pmatrix}$$

Proof Evaluating the right hand side, we see that

$$\binom{n-1}{r-1} + \binom{n-1}{r} = \frac{(n-1)!}{(r-1)!(n-r)!} + \frac{(n-1)!}{r!(n-r-1)!}.$$

Now the definition of factorials ensures that

$$\frac{1}{(r-1)!} = \frac{r}{r!} \quad \text{and} \quad \frac{1}{(n-r-1)!} = \frac{n-r}{(n-r)!}.$$

It follows that

$$\begin{aligned}\binom{n-1}{r-1} + \binom{n-1}{r} &= \frac{(n-1)!r}{r!(n-r)!} + \frac{(n-1)!(n-r)}{r!(n-r)!} \\ &= \frac{(n-1)!n}{r!(n-r)!} = \frac{n!}{r!(n-r)!} \\ &= \binom{n}{r}\end{aligned}$$

The result follows. ∎

1.13 The Binomial Theorem

Theorem 1.11 (Binomial Theorem) *Let x and y be real numbers. Then*

$$(x+y)^n = \sum_{r=0}^{n} \binom{n}{r} x^{n-r} y^r$$

for all natural numbers n.

Proof The definition of binomial coefficients ensures that the theorem is true when $n = 1$.

Suppose that the result holds for $n = k$, where k is some natural number, so that

$$(x+y)^k = \sum_{r=0}^{k} \binom{k}{r} x^{k-r} y^r.$$

Then

$$\begin{aligned}(x+y)^{k+1} &= (x+y)^k (x+y) = \sum_{r=0}^{k} \binom{k}{r} x^{k-r} y^r (x+y) \\ &= \sum_{r=0}^{k} \binom{k}{r} x^{k+1-r} y^r + \sum_{r=0}^{k} \binom{k}{r} x^{k-r} y^{r+1}\end{aligned}$$

Now, substituting in $r = j - 1$, where j ranges over integers from 1 to $k+1$, and then relabelling j as r, we find that

$$\begin{aligned}\sum_{r=0}^{k} \begin{pmatrix} k \\ r \end{pmatrix} x^{k-r} y^{r+1} &= \sum_{j=1}^{k+1} \begin{pmatrix} k \\ j-1 \end{pmatrix} x^{k+1-j} y^{j} \\ &= \sum_{r=1}^{k+1} \begin{pmatrix} k \\ r-1 \end{pmatrix} x^{k+1-r} y^{r}\end{aligned}$$

Therefore

$$\begin{aligned}&(x+y)^{k+1} \\ &\quad= \sum_{r=0}^{k} \begin{pmatrix} k \\ r \end{pmatrix} x^{k+1-r} y^{r} + \sum_{r=1}^{k+1} \begin{pmatrix} k \\ r-1 \end{pmatrix} x^{k+1-r} y^{r} \\ &\quad= x^{k+1} + y^{k+1} + \sum_{r=1}^{k} \left(\begin{pmatrix} k \\ r \end{pmatrix} + \begin{pmatrix} k \\ r-1 \end{pmatrix} \right) x^{k+1-r} y^{r}.\end{aligned}$$

Now

$$\begin{pmatrix} k \\ r \end{pmatrix} + \begin{pmatrix} k \\ r-1 \end{pmatrix} = \begin{pmatrix} k+1 \\ r \end{pmatrix}$$

for all non-negative integers k and positive integers r (see Lemma 1.10). It follows that

$$\begin{aligned}(x+y)^{k+1} &= x^{k+1} + y^{k+1} + \sum_{r=1}^{k} \begin{pmatrix} k+1 \\ r \end{pmatrix} x^{k+1-r} y^{r} \\ &= \sum_{r=0}^{k+1} \begin{pmatrix} k+1 \\ r \end{pmatrix} x^{k+1-r} y^{r}.\end{aligned}$$

Thus if the identity

$$(x+y)^n = \sum_{r=0}^{n} \begin{pmatrix} n \\ r \end{pmatrix} x^{n-r} y^{r}$$

holds for $n = k$, where k is some natural number, then it also holds for $n = k+1$. It follows from the Principle of Mathematical Induction that that this identity holds for all natural numbers n, as required. ∎

Remark The equation

$$(x+y)^n = \sum_{r=0}^{n} \begin{pmatrix} n \\ r \end{pmatrix} x^{r} y^{n-r}$$

that encapsulates the Binomial Theorem is reproduced in the booklet *Formulae and Tables* prepared for use in examinations in Ireland (on page 20 of the 2016 edition). The validity of this equation requires that $x^0 = 1$ and $y^0 = 1$, in order that the correct terms appear in the sum for $r = 0$ and $r = n$. Thus if this equation is to be true for all real values of x and y, be they positive, negative or zero, one must adopt the definition that $0^0 = 1$.

1.14 Intervals

A subset I of the set $\mathbb{R}$ of real numbers is said to be an *interval* if all real numbers that lie between two elements of the set I themselves belong to I. This requires that if u, v and w are real numbers satisfying $u < v < w$, and if $u \in I$ and $w \in I$ then also $v \in I$.

It can be shown that, in addition to the empty set $\emptyset$ and the whole set $\mathbb{R}$ of real numbers, there are eight types of integrals. Four types of integrals are bounded and are determined by their endpoints a and b.

Given real numbers a and b satisfying $a \leq b$, we denote by $[a, b]$ the set consisting of all real numbers x that satisfy $a \leq x \leq b$.

Given real numbers a and b satisfying $a < b$, we denote by $[a, b)$ the set consisting of all real numbers x that satisfy $a \leq x < b$, we denote by $(a, b]$ the set consisting of all real numbers x that satisfy $a < x \leq b$, and we denote by (a, b) the set consisting of all real numbers x that satisfy $a < x < b$.

Thus

$$\begin{array}{rcll} [a, b] & = & \{x \in \mathbb{R} \mid a \leq x \leq b\} & (a \leq b), \\ [a, b) & = & \{x \in \mathbb{R} \mid a \leq x < b\} & (a < b), \\ (a, b] & = & \{x \in \mathbb{R} \mid a < x \leq b\} & (a < b), \\ (a, b) & = & \{x \in \mathbb{R} \mid a < x < b\} & (a < b). \end{array}$$

In addition to the four types of bounded intervals just described, there are four types of unbounded intervals that do not include the whole of the set $\mathbb{R}$. An unbounded interval falling within one of these types is determined by a real number c representing an upper or lower endpoint:—

$$\begin{array}{rcl} [c, +\infty) & = & \{x \in \mathbb{R} \mid x \geq c\}, \\ (c, +\infty) & = & \{x \in \mathbb{R} \mid x > c\}, \\ (-\infty, c] & = & \{x \in \mathbb{R} \mid x \leq c\}, \\ (-\infty, c) & = & \{x \in \mathbb{R} \mid x < c\}. \end{array}$$

Example Let $I = [1,7]$, $J = (2,9)$, $K = [4,6)$ and $L = (5,+\infty)$, so that

$$\begin{aligned} I &= \{x \in \mathbb{R} \mid 1 \leq x \leq 7\}, \\ J &= \{x \in \mathbb{R} \mid 2 < x < 9\}, \\ K &= \{x \in \mathbb{R} \mid 2 \leq x < 6\}, \\ L &= \{x \in \mathbb{R} \mid x > 5\}. \end{aligned}$$

Examining the relevant definitions, we find that

$$\begin{aligned} I \cup J &= \{x \in \mathbb{R} \mid 1 \leq x < 9\} = [1,9), \\ I \cap J &= \{x \in \mathbb{R} \mid 2 < x \leq 7\} = (2,7], \\ I \setminus J &= \{x \in \mathbb{R} \mid 1 \leq x \leq 2\} = [1,2], \\ J \setminus I &= \{x \in \mathbb{R} \mid 7 < x < 9\} = (7,9), \end{aligned}$$

Also, with $K = [4,6)$ and $L = (5,+\infty)$, we find that

$$\begin{aligned} K \cup L &= \{x \in \mathbb{R} \mid x \geq 4\} = [4,\infty), \\ K \cap L &= \{x \in \mathbb{R} \mid 5 < x < 6\} = (5,6), \\ K \setminus L &= \{x \in \mathbb{R} \mid 4 \leq x \leq 5\} = [4,5], \\ L \setminus K &= \{x \in \mathbb{R} \mid x \geq 6\} = [6,+\infty). \end{aligned}$$

Also, with $I = [1,7]$, $J = (2,9)$ and $K = [4,6)$, we find that

$$\begin{aligned} I \setminus K &= \{x \in \mathbb{R} \mid 1 \leq x < 4 \text{ or } 6 \leq x \leq 7\} \\ &= [1,4) \cup [6,7], \\ J \setminus (I \setminus K) &= (2,9) \setminus ([1,4) \cup [6,7)) \\ &= [4,6) \cup [7,9). \end{aligned}$$

1.15 Least Upper Bounds

Let X be a subset of the set $\mathbb{R}$ of real numbers. A real number u is said to be an *upper bound* for the set X if $x \leq u$ for all $x \in X$. A real number s is said to be a *least upper bound* for the set X if s is an upper bound for the set X that is less than or equal to all other upper bounds for this set. Thus a real number s is an least upper bound for the set X if and only if the following two conditions are satisfied:—

(i) $x \leq s$ for all $x \in X$;

(ii) $s \leq u$ for all upper bounds u for the set X.

A subset X of the set $\mathbb{R}$ of real numbers is said to be *bounded above* if it has at least one upper bound.

A subset X of the real numbers can have at most one least upper bound. Indeed suppose that the real number s is a least upper bound for X and that the real number t is also a least upper bound for X. Then $s \leq t$, because s is less than or equal to all upper bounds for the set X. Similarly $t \leq s$, because t is less than or equal to all upper bounds for the set X. The inequalities $s \leq t$ and $t \leq s$ then together imply that $s = t$. Thus no subset of the real numbers can have more than least upper bound.

The least upper bound of a non-empty set X of real numbers, if it exists, is also referred to as the *supremum* of the set X. It is customarily denoted by $\sup X$. (The alternative notation $\operatorname{lub} X$ for the least upper bound of a set X is used in some mathematics textbooks.)

Example Let

$$X = \{q \in \mathbb{Q} \mid q < 1\}.$$

(In other words, X is the set consisting of all rational numbers q that satisfy $q < 1$.) We show that $\sup X = 1$.

Now it is clear from the definition of the set X that the number 1 is an upper bound for the set X. Let s be a real number satisfying $s < 1$. Then there exists a natural number n large enough to ensure that

$$1 - \frac{1}{n} > s.$$

Now

$$1 - \frac{1}{n} = \frac{n-1}{n},$$

and thus $1 - \dfrac{1}{n}$ is a rational number. It follows that

$$s < 1 - \frac{1}{n} \quad \text{and} \quad 1 - \frac{1}{n} \in X,$$

and therefore the real number s is not an upper bound for the set X.

We conclude from what we have just shown that every upper bound u for the set X must satisfy $u \geq 1$. Therefore the number 1 is the least upper bound for the set X, and thus $\sup X = 1$.

1.16 Greatest Lower Bounds

Corresponding to the definition of the concept of a *least upper bound* (or *supremum*) $\sup X$ of a set X that is non-empty and bounded above, there is an analogous definition of the concept of a *greatest lower bound* (or *infimum*) $\inf X$ of a set X of real numbers that is non-empty and bounded below.

Let X be a subset of the set $\mathbb{R}$. A real number l is a *lower bound* for the set X if $l \leq x$ for all $x \in X$. The set X is said to be *bounded below* if there exists a lower bound for the set. A real number l is said to be a *greatest lower bound* for the set X if l is a lower bound for this set that is greater than or equal to every other lower bound for this set.

The greatest lower bound of a set X, if it exists, is also referred to as the *infimum* of the set X, and is denoted by $\inf X$. (In some mathematical textbooks the greatest lower bound of a set X of real numbers may be denoted by $\operatorname{glb} X$.)

1.17 Bounded Subsets of the Real Numbers

A non-empty subset X of the set $\mathbb{R}$ of real numbers is said to be *bounded* if it is bounded above and below. It follows from this definition that a subset X of $\mathbb{R}$ is bounded if and only if there exist fixed constants A and B such that $A \leq x \leq B$ for all $x \in X$.

Let X be a subset of $\mathbb{R}$ with both a least upper bound $\sup X$ and a greatest lower bound $\inf X$, and let a and b be real numbers satisfying $a \leq b$ for which $X \subset [a, b]$, where

$$[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}.$$

Then the real number a is a lower bound for the set X and therefore $a \leq \inf X$. Similarly the real number b is an upper bound for the set X, and therefore $\sup X \leq b$. It follows that

$$[\inf X, \sup X] \subset [a, b].$$

Thus the interval $[\inf X, \sup X]$ is the smallest closed interval that contains the set X.

Example Let a and b be real numbers satisfying $a < b$. Then

$$\inf[a, b] = \inf[a, b) = \inf(a, b] = \inf(a, b) = a,$$

and

$$\sup[a, b] = \sup[a, b) = \sup(a, b] = \sup(a, b) = b.$$

where

$$[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}, \quad [a, b) = \{x \in \mathbb{R} \mid a \leq x < b\},$$

$$(a, b] = \{x \in \mathbb{R} \mid a < x \leq b\}, \quad (a, b) = \{x \in \mathbb{R} \mid a < x < b\}.$$

Example For each natural number n let

$$x_n = \frac{(n-1)^2}{n^2},$$

and let X be the set $\{x_n \mid n \in \mathbb{N}\}$ consisting of the members of the infinite sequence $x_1, x_2, x_3, x_4, \ldots$. Now

$$x_n = 1 - \frac{2}{n} + \frac{1}{n^2},$$

for all natural numbers n, and therefore

$$1 - \frac{2}{n} < x_n < 1$$

for all natural numbers n.

Now, given any real number s satisfying $s < 1$, there exists some positive integer n large enough to ensure that

$$1 - \frac{2}{n} > s,$$

and therefore the real number s cannot be an upper bound for the set X. But the number 1 is an upper bound for the set X. It follows that $\sup X = 1$. In this example there is no element of the set X that is equal to the least upper bound $\sup X$ of the set, and thus $\sup X \notin X$.

Now all elements of the set X are non-negative, and $x_1 = 0$. It follows that $\inf X = 0$. Moreover $\inf X \in X$.

Remark The above example demonstrates that there is no general principle requiring bounded sets to contain their least upper bounds or their greatest lower bounds. Some bounded sets contain their least upper bounds; others do not. Similarly some bounded sets contain their greatest lower bounds; others do not.

1.18 The Least Upper Bound Principle

The following property is a fundamental property of the system of real numbers.

> **The Least Upper Bound Principle.** Given any subset X of the set $\mathbb{R}$ of real numbers that is non-empty and bounded above, there exists a least upper bound for the set X.

Let X be a set of real numbers that is non-empty and bounded above. It follows from the Least Upper Bound Principle that the set X has a least upper bound. This least upper bound is unique. It is denoted by $\sup X$, and is often referred to as the *supremum* of the set X.

1.19 Existence of Greatest Lower Bounds

A natural complement to the *Least Upper Bound Principle* is a principle asserting the existence of greatest lower bounds. It follows easily from the Least Upper Bound Principle that any subset X of the set $\mathbb{R}$ of real numbers that is non-empty and bounded below must have a greatest lower bound. This follows on "reflecting" the set about the number zero, replacing each real number x in the set by $-x$. Specifically let X be a non-empty set of real numbers that is bounded below, and let R be the set consisting of all real numbers that are of the form $-x$ for some element x of X. (Thus a real number x satisfies $x \in R$ if and only if $-x \in X$.). Then the set R is non-empty and bounded above. It follows from the Least Upper Bound Principle that there exists a least upper bound $\sup R$ for the set R. Then $-\sup R$ is a greatest lower bound for the set X.

We now summarize the basic consequences of the Least Upper Bound Principle, as they apply to bounded sets.

Let X be a bounded set. Then there exist uniquely determined real numbers $\sup X$ and $\inf X$ that are the least upper bound and greatest lower bounds of the set X. Then $X \subset [\inf X, \sup X]$.

We recall that an interval is *closed* if and only if it contains its endpoints. In particular the interval $[\inf X, \sup X]$ is a bounded closed interval, and $X \subset [\inf X, \sup X]$.

Now let $[a, b]$ be any bounded closed interval for which $X \subset [a, b]$. Then b is an uppper bound for the set X, and a is a lower bound for the set X, and therefore

$$a \leq \inf X \leq \sup X \leq b.$$

It follows that

$$X \subset [\inf X, \sup X] \subset [a, b].$$

Thus $[\inf X, \sup X]$ is the smallest closed bounded interval that contains (as a subset) the set X.

Example Let

$$X = \{x \in \mathbb{R} \mid 0 \leq x < 1\}.$$

Then $\inf X = 0$ and $\sup X = 1$. Thus $X \subset [0, 1]$, where

$$[0, 1] = \{x \in \mathbb{R} \mid 0 \leq x \leq 1\}.$$

Moreover $[0, 1]$ is the smallest closed interval that contains the set X.

Example Let

$$X = \{x \in \mathbb{R} \mid x^2 < 2\}.$$

Then $\inf X = -\sqrt{2}$ and $\sup X = \sqrt{2}$. Thus $X \subset [-\sqrt{2}, \sqrt{2}]$. Moreover $[-\sqrt{2}, \sqrt{2}]$ is the smallest closed interval that contains the set X.

Example Let X be the set consisting of the reciprocals

$$1, \ \frac{1}{2}, \ \frac{1}{3}, \ \frac{1}{4}, \ \frac{1}{5}, \ldots$$

of the natural numbers. Then $\inf X = 0$ and $\sup X = 1$. Moreover $[0, 1]$ is the smallest closed interval that contains the set X.

1.20 Roots of Positive Real Numbers

Proposition 1.12 *Given any positive real number c, and given any natural number n, there exists a unique positive real number r with the property that $r^n = c$.*

We do not prove Proposition 1.12 formally here. A very formal and rigorous treatment of the real number system might establish the existence of the real number r by proving that if

$$r = \sup\{x \in \mathbb{R} \mid x > 0 \text{ and } x^n < c\},$$

(so that r is defined as the least upper bound of the specified set), then $r^n = c$. Alternatively, such a formal treatment might deduce Proposition 1.12 of a general theorem known as the Intermediate Value Theorem.

On the other hand, it is easy to prove that the positive real number r, assuming that it exists, is the only positive real number satisfying $r^n = c$. Indeed suppose that r and s are positive real numbers and that $r^n = c = s^n$. Were it the case that $r \neq s$, then either $r < s$ or $r > s$. If it were the case that $r < s$ then $r^n < s^n$ and therefore $r^n \neq s^n$, contradicting the requirement that $r^n = c = s^n$. If it were the case that $r > s$ then $r^n > s^n$ and therefore $r^n \neq s^n$, again contradicting the requirement that $r^n = c = s^n$. Thus the possibilities that $u < v$ and $u > v$ are ruled out, and the only remaining possibility is that $u = v$.

Given any positive real number c, and given any natural number n, the decimal expansion of a positive real number r satisfying $r^n = c$ may be found as follows. For each natural number k, let r_k be the largest multiple of 10^{-k} for which $r_k^n < c$. Then the number r_k is representable as a terminating decimal, with at most k decimal digits after the decimal point, and this number r_k is the unique number of this type for which both $r_k^n < c$ and $(r_k + 10^{-k})^n \geq c$. We obtain in this fashion an infinite sequence

$$r_1, r_2, r_3, r_4, \ldots$$

of terminating decimal approximations to the nth root of c.

Moreover if natural numbers k and m satisfy $k < m$, then the decimal expansions of r_k and r_m agree up to the kth decimal place. We can therefore determine the successive decimal digits of the decimal expansion of a real number r whose decimal expansion terminated after k decimal places is equal to r_k. This real number r satisfies $r^n = c$.

Example For example, if $c = 3$ and $n = 2$ then the procedure described above yields successive decimal approximations

$$1.7,\ 1.73,\ 1.732,\ 1.7320,\ 1.73205, \ldots$$

to a real number r satisfying $r^2 = 3$. This number r is the square root $\sqrt{3}$ of 3.

Example Also if $c = 4$ and $n = 2$ then the procedure yields successive decimal approximations

$$1.9,\ 1.99,\ 1.999,\ 1.9999,\ 1.99999, \ldots$$

to a real number r satisfying $r^2 = 4$. Of course $r = 2$.

1.21 Laws of Indices with Fractional Exponents

Let a be a positive real number, and let q be a positive integer. We define $a^{\frac{1}{q}} = \sqrt[q]{a}$, where $\sqrt[q]{a}$ denotes the unique positive real number with the property that $(\sqrt[q]{a})^q = a$.

Note that positive real numbers a and b satisfy $a^{\frac{1}{q}} = b$ if and only if $a = b^q$.

Note also that $(a^{pq})^{\frac{1}{q}} = a^p$ for all integers p and positive integers q. Indeed the definition of $(a^{pq})^{\frac{1}{q}}$ requires that $(a^{pq})^{\frac{1}{q}} = c$, where r is the unique positive real number satisfying $c^q = a^{pq}$. But $(a^p)^q = a^{pq}$ (see Proposition 1.8). $(a^{pq})^{\frac{1}{q}} = a^p$.

Lemma 1.13 *Let a be a positive real number, and let p, q, r and s be positive integers. Suppose that*

$$\frac{p}{q} = \frac{r}{s}.$$

Then

$$(\sqrt[q]{a})^p = (\sqrt[s]{a})^r.$$

Proof Basic algebra ensures that $ps = rq$. Let

$$u = (\sqrt[q]{a})^p \quad \text{and} \quad v = (\sqrt[s]{a})^r.$$

It then follows from Lemma 1.3 that

$$\begin{aligned} u^{rq} &= ((\sqrt[q]{a})^p)^{rq} = ((\sqrt[q]{a}))^{prq} = ((\sqrt[q]{a})^q)^{pr} = a^{pr}, \\ v^{ps} &= ((\sqrt[s]{a})^r)^{ps} = ((\sqrt[s]{a})^{rps} = ((\sqrt[s]{a})^s)^{pr} = a^{pr}. \end{aligned}$$

Therefore $u^{rq} = a^{pr} = v^{ps}$. But $rq = ps$, and there exists only one positive real number x satisfying the equation $x^{rq} = a^{pr}$ (see Proposition 1.12 and the remarks that follow it). Therefore $u = v$, and thus

$$(\sqrt[q]{a})^p = (\sqrt[s]{a})^r,$$

as required. ∎

Definition Let a be a positive real number, and let t be a rational number. We define

$$a^t = (\sqrt[q]{a})^p,$$

where p and q are integers for which $q > 0$ and $p/q = t$.

In the case where $t > 0$ it follows from Lemma 1.13 that the value of $(\sqrt[q]{a})^p$ does not depend on the choice of p and q, provided that $p/q = t$. Therefore a^t is well-defined in this case.

In the case where $t < 0$, we can write $t = -p/q$, where p and q are positive integers and, in that case

$$a^t = \frac{1}{(\sqrt[q]{a})^p}.$$

It follows that a^t is well-defined in this case also.

And $a^0 = 1$, and thus a^t is well-defined when $t = 0$. Thus a^t is well-defined for all *rational numbers* t.

Let a be a positive real number and let p and q be integers, where $q > 0$. The definition of $a^{\frac{p}{q}}$ ensures that

$$a^{\frac{p}{q}} = (\sqrt[q]{a})^p.$$

It then follows from Proposition 1.8 that

$$(a^{\frac{p}{q}})^q = ((\sqrt[q]{a})^p)^q = (\sqrt[q]{a})^{pq} = ((\sqrt[q]{a})^q)^p = a^p.$$

It then follows from the definition of $\sqrt[q]{a^p}$ that

$$\sqrt[q]{a^p} = a^{\frac{p}{q}} = (\sqrt[q]{a})^p.$$

Proposition 1.14 *Let a be a positive-zero real number and let t and u be rational numbers (which may be positive, negative or zero). Then $a^{t+u} = a^t a^u$.*

Proof Because t and u are rational numbers, and are thus representable as fractions where the numerators and denominators are integers, we can represent them as fractions over a common denominator. Therefore there exist integers p, q and r, where $q > 0$, such that $t = p/q$ and $u = r/q$. Then $t + u = (p + r)/q$. It then follows from Proposition 1.7 that

$$a^{t+u} = (\sqrt[q]{a})^{p+r} = (\sqrt[q]{a})^p (\sqrt[q]{a})^r = a^t a^u,$$

as required. ∎

Proposition 1.15 *Let a be a positive-zero real number and let t and u be rational numbers (which may be positive, negative or zero). Then $a^{tu} = (a^t)^u$.*

Proof The exponents t and u are rational numbers, and therefore there exist integers p, q, r and s, where $q > 0$ and $s > 0$, such that $t = p/q$ and $u = r/s$. Then

$$a = (a^{\frac{1}{qs}})^{qs}.$$

It therefore follows from Proposition 1.8 that

$$a^t = (a^{\frac{1}{q}})^p = (((a^{\frac{1}{qs}})^{qs})^{\frac{1}{q}})^p = ((a^{\frac{1}{qs}})^s)^p = (a^{\frac{1}{qs}})^{sp},$$

and therefore

$$(a^t)^u = ((a^t)^{\frac{1}{s}})^r = (((a^{\frac{1}{qs}})^{sp})^{\frac{1}{s}})^r = ((a^{\frac{1}{qs}})^p)^r = (a^{\frac{1}{qs}})^{pr} = a^{tu},$$

as required. ∎

Proposition 1.16 *Let a and b be positive real numbers. Then $(ab)^t = a^t b^t$ for all rational numbers t.*

Proof Let a and b be positive real numbers, and let t be a rational number. Then there exist integers p and q such that $q > 0$ and $t = p/q$. Then it follows from Proposition 1.9 that

$$(\sqrt[q]{a}\,\sqrt[q]{b})^q = (\sqrt[q]{a})^q\,(\sqrt[q]{b})^q = ab.$$

The definition of $\sqrt[q]{ab}$ as the unique positive real number u satisfying $u^q = ab$ then ensures that

$$\sqrt[q]{a}\,\sqrt[q]{b} = \sqrt[q]{ab}.$$

It then follows from Proposition 1.9 and the definitions of a^t, b^t and $(ab)^t$ that

$$a^t b^t = (\sqrt[q]{a})^p (\sqrt[q]{b})^p = (\sqrt[q]{a}\sqrt[q]{b})^p = (\sqrt[q]{ab})^p = (ab)^t,$$

as required. ∎

Remark Let a be a positive real number. At this stage we have defined and discussed the basic properties of a^x in all cases where x is a rational number. But what about $a^{\sqrt{2}}$ and a^π? How do we define a^x when x is an arbitrary real number that is not necessarily rational? This will be discussed in more depth when we come to discuss exponential and logarithm functions. We note here that, for all real numbers x, the real number a^x can be characterized as the unique real number with the property that $a^t \leq a^x \leq a^u$ for all rational numbers t and u satisfying $t \leq x \leq u$. It can then be shown that $a^{x+y} = a^x a^y$ and $(a^x)^y = a^{xy}$ for all real numbers x and y.

1.22 Summary of Laws of Indices

We have established the following results from the basic definitions:—

- if a is a real number, and if p and q are non-negative integers then $a^{p+q} = a^p a^q$ and $a^{pq} = (a^p)^q$ (see Lemma 1.4, and Lemma 1.5);
- if a is a *non-zero* real number, and if m and n are integers then $a^{m+n} = a^m a^n$ and $a^{mn} = (a^m)^n$ (see Proposition 1.7 and Proposition 1.15);
- if a is a *positive* real number, and if t and u are rational numbers then $a^{t+u} = a^t a^u$ and $a^{tu} = (a^t)^u$ (see Proposition 1.7 and Proposition 1.15);
- if a and b are real numbers, and if n is a non-negative integer, then $(ab)^n = a^n b^n$ (see Proposition 1.9);
- if a and b are non-zero real numbers, and if n is an integer, then $(ab)^n = a^n b^n$ (see Proposition 1.9);
- if a and b are positive real numbers, and if t is a rational number, then $(ab)^t = a^t b^t$ (see Proposition 1.16).

The following statement provides a summary of the laws of indices proved above that are applicable to powers of real numbers.

> *The "laws of indices" encapsulated in the formulae $a^{p+q} = a^p a^q$, $a^{pq} = (a^p)^q$ and $(ab)^p = a^p b^p$ are valid in the following situations:—*
>
> - *when a and b are real numbers and p and q are non-negative integers;*
> - *when a and b are non-zero real numbers and p and q are integers;*
> - *when a and b are positive real numbers and p and q are rational numbers.*