

MAT 7003 : Mathematical Foundations

(for Software Engineering)

J Paul Gibson, A207

paul.gibson@it-sudparis.eu

<http://www-public.it-sudparis.eu/~gibson/Teaching/MAT7003/>

CountingNumbers

<http://www-public.it-sudparis.eu/~gibson/Teaching/MAT7003/L6b-CountingNumbers.pdf>

NATURAL NUMBERS

The **set** of natural numbers is either:

- the set of positive integers $\{1, 2, 3, \dots\}$ according to the traditional definition, or
- the set of non-negative integers $\{0, 1, 2, \dots\}$ according to a definition first appearing in the nineteenth century

They have two main purposes:

- counting, and
- Ordering

Properties of the natural numbers are studied in specialised fields such as:

- number theory, and
- combinatorics

NATURAL NUMBERS

Notation:

$$\mathbb{N}_0 = \{0, 1, 2, \dots\}; \quad \mathbb{N}^* = \mathbb{N}_1 = \{1, 2, \dots\}.$$

This set is *countably infinite*

This is also expressed by saying that the cardinal number (*cardinality*) of the set is:

aleph-null \aleph_0

NATURAL NUMBERS: Algebraic properties

The addition and multiplication operations on natural numbers have several algebraic properties:

- **Closure** under addition and multiplication: for all natural numbers a and b , both $a + b$ and $a \times b$ are natural numbers.
- **Associativity**: for all natural numbers a , b , and c , $a + (b + c) = (a + b) + c$ and $a \times (b \times c) = (a \times b) \times c$.
- **Commutativity**: for all natural numbers a and b , $a + b = b + a$ and $a \times b = b \times a$.
- Existence of **identity** elements: for every natural number a , $a + 0 = a$ and $a \times 1 = a$.
- **Distributivity** for all natural numbers a , b , and c , $a \times (b + c) = (a \times b) + (a \times c)$
- **No zero divisors**: if a and b are natural numbers such that $a \times b = 0$ then $a = 0$ or $b = 0$

We come back to algebraic properties when we consider algebraic structures later in the module

NATURAL NUMBERS: Peano axioms

The Peano axioms give a formal theory of the natural numbers. The axioms are:

- There is a natural number 0.
- Every natural number a has a natural number successor, denoted by $S(a)$. Intuitively, $S(a)$ is $a+1$.
- There is no natural number whose successor is 0.
- Distinct natural numbers have distinct successors: if $a \neq b$, then $S(a) \neq S(b)$.
- If a property is possessed by 0 and also by the successor of every natural number which possesses it, then it is possessed by all natural numbers. (This postulate ensures that the proof technique of mathematical induction is valid.)

It should be noted that the "0" in the above definition need not correspond to what we normally consider to be the number zero.

NATURAL NUMBERS: Peano axioms

We can use these axioms in a new RODIN context (*Peano*)

CONTEXT

Peano

SETS

Numbers

CONSTANTS

zero
s
equals

AXIOMS

```
axm1 : zero ∈ Numbers // There is a natural number zero
axm2 : s ∈ Numbers → Numbers // Every natural number a has a natural number successor,
// denoted by S(a).
axm3 : zero ∉ ran(s) // There is no natural number whose successor is zero
axm4 : equals ⊆ Numbers × Numbers
axm4a : ∀x,y. x∈Numbers ∧ y∈Numbers ∧ (x↔y) // Distinct natural numbers have distinct
// equals // successors: if a ≠ b, then S(a) ≠ S(b).
axm4b : (zero ↔ zero) ∈ equals // (When/why) Do we need this?
axm5 : ∀p. ( p ⊆ Numbers ∧ // If a property is possessed by 0 and also by the
zero ∈ p ∧ // successor of every natural number which possesses
(∀ n. n ∈ p ⇒ s // it, then it is possessed by all natural numbers.
(n) ∈ p ) ⇒ //
Numbers ⊆ p
```

END

NATURAL NUMBERS: construction using set theory

The standard construction is a special case of *von Neumann* ordinal construction

$$0 = \{ \}$$

$$1 = \{0\} = \{ \{ \} \}$$

$$2 = \{0, 1\} = \{0, \{0\}\} = \{ \{ \}, \{ \{ \} \} \}$$

$$3 = \{0, 1, 2\} = \{0, \{0\}, \{0, \{0\}\}\} = \{ \{ \}, \{ \{ \} \}, \{ \{ \}, \{ \{ \} \} \} \}$$

$$n = \{0, 1, 2, \dots, n-2, n-1\} = \{0, 1, 2, \dots, n-2\} \cup \{n-1\} = (n-1) \cup \{n-1\}$$

Although the standard construction is useful, it is not the only possible construction. For example:

one could define $0 = \{ \}$
and $S(a) = \{a\}$,
producing
 $0 = \{ \}$
 $1 = \{0\} = \{ \{ \} \}$
 $2 = \{1\} = \{ \{ \{ \} \} \}$, etc.

NATURAL NUMBERS: countability of other numbers

A set S is called **countable** if there exists an **injective** function

$$f: S \rightarrow \mathbb{N}$$

from S to the **natural numbers** $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.

If f is also **surjective**, thus making f **bijective**, then S is called **countably infinite**.

TO DO

Show that **integers are countable**

Show that **rationals are countable**

Show that **reals are not countable**

Georg Cantor (who introduced this branch of mathematics) showed that the real numbers cannot be put into one-to-one correspondence with the natural numbers ... see later slides

Theorem: The Cartesian product of finitely many countable sets is countable.

QUESTION: can you sketch a proof?

The integers, rationals and the reals

You're familiar with three other basic sets of numbers:

- the **integers** – natural numbers and their negatives (\mathbb{Z})
- the **rationals** - any number that can be expressed as the quotient a/b of two integers, with the denominator b not equal to zero (\mathbb{Q})
- the **reals** – « can be given by an infinite decimal representation, » -more formal definitions exist- (\mathbb{R})

The integers are obviously *discrete*, in that there's a big gap between successive pairs of integers.

To a first approximation, the rational numbers and the real numbers seem pretty similar.

The rationals and the reals

We know that the reals and the rationals are different sets, because we know that a few special numbers are not rational, e.g. π and the square root of 2. (Check on web for further details)

These irrational numbers may seem like isolated cases, but this intuition is entirely wrong: the vast majority of real numbers are irrational and the rationals are quite a small subset of the reals.

The rationals are *dense* in the reals: if I pick any real number x and a distance δ , there is always a rational number within distance δ of x . Between any two real numbers, there is always a rational number.

The rationals and the reals: Completeness

One big difference between the two sets is that the reals have a so-called “completeness” property:

*any subset of the reals with an upper bound has a smallest upper bound.
(And similarly for lower bounds.)*

So if I have a sequence of reals that converges, the limit it converges to is also a real number.

This isn't true for the rationals. For example, we can make a series of rational numbers that converge to π -

3, 3.1, 3.14, 3.141, 3.1415, 3.14159, 3.141592, 3.1415926, 3.14159265

But there is no rational number equal to π .

In fact, the reals are set up precisely to make **completeness** work. One way to construct the reals is to construct all convergent sequences of rationals and add new points to represent the limits of these sequences. (Most of the machinery of calculus depends on the existence of these extra points.)

Cantor's diagonal argument: uncountability of reals

The *diagonal method*, was published in 1891 by Georg Cantor as a proof that there are infinite sets which cannot be put into 1-1 correspondence with the infinite set of natural numbers.

Such sets are now known as *uncountable* sets, and the size of infinite sets is now treated by the theory of cardinal numbers which Cantor began.

Diagonalisation is a powerful and general technique that has been used in a wide range of proofs. Some relevant examples are:

- **Russell's paradox**,
- **the first of Gödel's incompleteness theorems**
- **Turing's answer to the Entscheidungsproblem of David Hilbert**

Cantor's diagonal argument

Proof by contradiction:

$E_0 =$	m	m	m	m	m	m	m	m	m	m	...
$E_1 =$	w	w	w	w	w	w	w	w	w	w	...
$E_2 =$	m	w	m	w	m	w	m	w	m	w	...
$E_3 =$	w	m	w	m	w	m	w	m	w	m	...
$E_4 =$	w	m	m	w	w	m	m	w	m	w	...
$E_5 =$	m	w	m	w	w	m	w	m	w	m	...
$E_6 =$	m	w	m	w	w	m	w	m	w	m	...
$E_7 =$	w	m	m	w	m	w	m	w	m	w	...
$E_8 =$	m	m	w	m	w	m	w	m	w	m	...
$E_9 =$	w	m	w	m	m	w	m	w	m	w	...
$E_{10} =$	w	m	w	m	w	m	w	m	w	m	...
$E_{11} =$	m	w	m	w	w	m	w	m	w	m	...
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\ddots
E_{\aleph}	w	m	w	w	m	w	m	m	m	w	...

If the reals are countable then we can enumerate/order them all in a list

But then we can *construct* a real that is not in the list.

This is a contradiction, so the original assumption is false, ie the reals are not countable

NOTE: This *construction* depends on some details concerning non-uniqueness of representations ...

Uncomputability: the number of functions is uncountable, whereas the number of programs is countably infinite... so there are uncomputable functions!

Largeness of sets and Cantor's theorem (for power sets)

NOTE: the notion of « relative largeness » is formalised by the definition of cardinality.

Two sets have the same cardinality if there is a bijection between the elements

The cardinality of the continuum (reals) is given by:

$$c = 2^{\aleph_0} > \aleph_0$$

The *continuum hypothesis* states that there is no cardinal number between the cardinality of the reals and the cardinality of the natural numbers

Cantor's Theorem: For every set S the power set of S, i.e., the set of all subsets of S (here written as P(S)), is *larger than* S itself.

Thus, P(\mathbb{R}) is larger than \mathbb{R} and P(P(\mathbb{R})) is larger than P(\mathbb{R}) and ...