The Natural Numbers

The Natural Numbers

The "counting numbers" $0, 1, 2, 3, \ldots$ are the basis of discrete mathematics. We refer to their totality as the set of ***natural numbers*** and denote it by $\mathbb{N}$. We have up to now used them to supply examples for our introduction to logic and to enumerate sets. It is time we briefly discuss how they can be formally defined.

We will represent the natural numbers as set of objects (denoted by $\mathbb{N}$) together with a relation called "succession": If n is a natural numbers, the "successor" of n, $\mathrm{Succ}(n)$, is defined and also in $\mathbb{N}$. In elementary terms, 1 is the successor to 0, 2 is the successor to 1, etc.

There is no unique set of natural numbers in the sense that we can exhibit "the" set $\mathbb{N}$. Rather, any pair $(\mathbb{N}, \mathrm{Succ})$, can qualify as a ***realization of the natural numbers*** if it satisfies certain axioms.

The Peano Axioms and the Induction Axiom

3.1. Definition. Let $\mathbb{N}$ be any set and suppose that the successor of any element of $\mathbb{N}$ has been defined. The ***Peano axioms*** are

1. $\mathbb{N}$ contains at least one object, called zero.
2. $\mathbb{N}$ is closed under the successor function, i.e., if n is in $\mathbb{N}$, the successor of n is in $\mathbb{N}$.
3. Zero is not the successor of a number.
4. Two numbers of which the successors are equal are themselves equal.
5. Induction axiom. If a set $S \subset \mathbb{N}$ contains zero and also the successor of every number in S, then $S = \mathbb{N}$.

Any set with a successor relation satisfying these axioms is called a realization of the natural numbers.

The von Neumann Realization

The Hungarian mathematician John von Neumann gave a very elegant realization of the natural numbers that is based on set theory:

Assume the empty set $\emptyset$ exists. Our idea is to define

$$
\begin{aligned}
0 &:= \emptyset, \\
1 &:= \{0\} = \{\emptyset\}, \\
2 &:= \{0, 1\} = \{\emptyset, \{\emptyset\}\}, \\
3 &:= \{0, 1, 2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}
\end{aligned}
$$

and so on. It is clear that we want 1 to be the successor of 0, 2 the successor of 1 and so on.

The set of natural numbers $\mathbb{N}$ is then defined as consisting of the element 0 as well as the successor of every element already known to be in $\mathbb{N}$.

The von Neumann Realization

Several questions arise:

- Is it possible to define a set $\mathbb{N}$ in this ***recursive*** way?
- Does the von Neumann realization actually satisfy the Peano axioms?

The answer to both questions is affirmative:

- The possibility of defining $\mathbb{N}$ in this way is taken as an ***axiom*** of set theory.
- The proof that Peano axiom (iv) is satisfied is much harder than it looks - try it!

For a discussion of both questions (and more) we refer to P.R. Halmos, ***Naive Set Theory*** (see Slide **??**). The relevant excerpt has been uploaded to SAKAI.

The von Neumann Realization

One interesting feature of this realization is that

$$n \in \mathrm{succ}(n) \qquad \text{and} \qquad n \subsetneq \mathrm{succ}(n).$$

Furthermore, we have a natural definition of the ordering relation "$<$" that does not require any concept of addition:

$$m < n \qquad :\Leftrightarrow \qquad m \subsetneq n.$$

Of course, we still need to check that the Peano axioms are satisfied:

1. $0 = \emptyset \in \mathbb{N}$ by definition.
2. For any $n \in \mathbb{N}$, $\mathrm{succ}(n) \in \mathbb{N}$ by definition.
3. $0 = \emptyset$ and for any n, $\mathrm{succ}(n) = n \cup \{n\} \neq \emptyset$, so 0 is not the successor of any number.
5. Any set S with the properties given is equal to $\mathbb{N}$ by the definition of $\mathbb{N}$.

The von Neumann Realization

We have skipped over the fourth Peano axiom: We need to show $\mathrm{succ}(m) = \mathrm{succ}(n)$ implies $m = n$. This is a little complicated and requires two further lemmas, which we discuss below.

3.2. Lemma. Let n be a natural number in the von Neumann realization (**??**). Then

$$\forall_{m \in \mathbb{N}} \quad m \in n \quad \Rightarrow \quad n \not\subset m, \tag{3.1}$$

or, equivalently,

$$\forall_{m \in \mathbb{N}} \quad n \subset m \quad \Rightarrow \quad m \notin n \tag{3.2}$$

Proof.

Let S be the set of natural numbers such that (3.1) holds,

$$S := \left\{ n \in \mathbb{N} : \forall_{m \in \mathbb{N}} \; m \in n \Rightarrow n \not\subset m \right\}.$$

The von Neumann Realization

Proof (continued).

Our goal is to show that $S = \mathbb{N}$, so that (3.1) is established for all $n \in \mathbb{N}$. Of course, at first it is possible that $S = \emptyset$.

We first show that $0 \in S$. Since $0 = \emptyset$, $m \in 0$ is false for all $m \in \mathbb{N}$ and so the implication

$$m \in 0 \quad \Rightarrow \quad 0 \notin m$$

is true for all $m \in \mathbb{N}$. Hence, $0 \in S$.

We next aim to show that if $n \in S$, then $\text{Succ}(n) \in S$. This then yields $S = \mathbb{N}$ by the induction axiom.

Let $n \in S$. We first derive a basic fact: since $n = n$, we have, in particular, that $n \subset n$ so $n \notin n$ by (3.2) for $m = n$. Then

$$\text{Succ}(n) = n \cup \{n\} \not\subset n.$$

The von Neumann Realization

Proof (continued).

Now suppose that $\text{Succ}(n) \subset m$ for some m. Then $n \subset \text{Succ}(n) \subset m$. Since $n \in S$, it follows that $m \notin n$. By contraposition, if $m \in n$, then $\text{Succ}(n) \not\subset m$.

Hence, $\text{Succ}(n) \not\subset n$ and $\text{Succ}(n) \not\subset m$ for all $m \in n$. Since the elements of $\text{Succ}(n)$ consist of n and the elements of n, it follows that

$$m \in \text{Succ}(n) \quad \Rightarrow \quad \text{Succ}(n) \not\subset m$$

Therefore, if $n \in S$, then $\text{Succ}(n) \in S$.

We have shown that the set S contains 0 and the successor of every element of S. By the induction axiom (which we have already established for the von Neumann construction) it follows that $S = \mathbb{N}$. $\square$

The von Neumann Realization

3.3. Definition. A set A is called transitive if

$$y \in x \wedge x \in A \quad \Rightarrow \quad y \in A.$$

In particular, a set A is transitive if and only if $x \subset A$ for all $x \in A$.

3.4. Lemma. Let n be a natural number in the von Neumann realization (**??**). Then n is transitive.

Proof.
We again proceed by induction. Let S be the set of transitive natural numbers. Then $0 \in S$ is vacuously true. Now let $n \in S$. If $x \in \mathrm{Succ}(n)$, then either $x \in n$ or $x = n$. If $x \in n$, then $x \subset n \subset \mathrm{Succ}(n)$, because $n \in S$. If $x = n$, then $x \subset n \cup \{n\} = \mathrm{Succ}(n)$. Hence, $\mathrm{Succ}(n) \in S$ and we again deduce $S = \mathbb{N}$ by the induction axiom. $\square$

The von Neumann Realization

Finally, we can prove that the von Neumann numbers satisfy the fourth Peano axiom:

3.5. Lemma. Let m and n be natural numbers in the von Neumann realization (**??**). Then n

$$\text{Succ}(m) = \text{Succ}(n) \quad \Rightarrow \quad m = n$$

Proof.
Let $n \cup \{n\} = m \cup \{m\}$. Then $n \in m$ or $n = m$. Similarly, $m = n$ or $m \in n$. Suppose that $m \neq n$. Then $n \in m$ and $m \in n$. By Lemma 3.4, $n \in n$. However, Lemma 3.2 then implies $n \notin n$, which is a contradiction. $\square$

Addition Once the set of natural numbers is established (e.g., through the Peano axioms), it is possible to define the operation of addition on $\mathbb{N}$,

$$+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \qquad (a, b) \mapsto a + b$$

We restrict ourselves to listing the properties that this operation then has.

For any two natural numbers $a, b \in \mathbb{N}$ we can define the natural number $c = a + b \in \mathbb{N}$ called the ***sum*** of a and b. This addition has the following properties ($a, b, c \in \mathbb{N}$):

(i) $a + (b + c) = (a + b) + c$ (***Associativity***)

(ii) $a + 0 = 0 + a = a$ (***Existence of a neutral element***)

(iii) $a + b = b + a$ (***Commutativity***)

Multiplication

Similarly, we can define ***multiplication***, where $a \cdot b \in \mathbb{N}$ is called the ***product*** of a and b. We have the following properties ($a, b, c \in \mathbb{N}$):

(i) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (***Associativity***)

(ii) $a \cdot 1 = 1 \cdot a = a$ (***Existence of a neutral element***)

(iii) $a \cdot b = b \cdot a$ (***Commutativity***)

We also have a property that essentially states that addition and multiplication are ***consistent***,

$$a \cdot (b + c) = a \cdot b + a \cdot c. \qquad (\textbf{\textit{Distributivity}})$$

Note that we are not able to define subtraction or division for all natural numbers.

Notation for Addition and Multiplication

For any numbers $a_1, a_2, \ldots, a_n$ we define the notation

$$a_1 + a_2 + \cdots + a_n =: \sum_{j=1}^{n} a_j =: \sum_{1 \le j \le n} a_j$$

and

$$a_1 \cdot a_2 \cdots a_n =: \prod_{j=1}^{n} a_j =: \prod_{1 \le j \le n} a_j.$$

For $a, b \in \mathbb{N}$ define the statement

$$a \mid b \qquad \Leftrightarrow \qquad \exists c \in \mathbb{N} : c \cdot a = b,$$

read as "a divides b." If $a \mid b$, then a is called a ***divisor*** of b.

Mathematical Induction

Typically one wants to show that some statement frame $A(n)$ is true for all $n \in \mathbb{N}$ with $n \geq n_0$ for some $n_0 \in \mathbb{N}$. Mathematical induction works by establishing two statements:

(I) $A(n_0)$ is true.

(II) $A(n+1)$ is true whenever $A(n)$ is true for $n \geq n_0$, i.e.,

$$\forall_{\substack{n \in \mathbb{N} \\ n \geq n_0}} \big(A(n) \Rightarrow A(n+1)\big)$$

Note that (II) does not make a statement on the situation when $A(n)$ is false; it is permitted for $A(n+1)$ to be true even if $A(n)$ is false.

The principle of mathematical induction now claims that $A(n)$ is true for all $n \geq n_0$ if (I) and (II) are true. This follows from the fifth Peano axiom (the induction axiom).

Introductory Example

3.6. Example. Consider the statement

$$\sum_{k=1}^{n}(2k-1) = n^2 \qquad \text{for all } n \in \mathbb{N} \setminus \{0\}.$$

This is a typical example, in that $A(n)\colon \sum_{k=1}^{n}(2k-1) = n^2$ is a predicate which is to be shown to hold for all natural numbers $n > 0$.

We first establish that $A(1)$ is true:

$$\sum_{k=1}^{1}(2k-1) = 2\cdot 1 - 1 = 1 \qquad \text{and} \qquad 1^2 = 1,$$

so $A(1)\colon 1 = 1$ is true.

Introductory Example We next show that $A(n) \Rightarrow A(n+1)$ for all $n \in \mathbb{N} \setminus \{0\}$. This means we show that $\sum_{k=1}^{n+1}(2k-1) = (n+1)^2$ if $\sum_{k=1}^{n}(2k-1) = n^2$. Let n now be any n for which $A(n)$ is true. We then write

$$\sum_{k=1}^{n+1}(2k-1) = \sum_{k=1}^{n}(2k-1) + 2(n+1) - 1$$

If $A(n)$ is true for this specific n, we can replace the sum on the right by n^2, yielding

$$\sum_{k=1}^{n+1}(2k-1) = n^2 + 2n + 1 = (n+1)^2$$

But this is just the statement $A(n+1)$. Therefore, if $A(n)$ is true, then $A(n+1)$ will also be true. We have shown that $A(n) \Rightarrow A(n+1)$.

Foundations of Induction

Essentially, mathematical induction claims that for all $n_0 \in \mathbb{N}$,

$$\Big(A(n_0) \wedge \underset{\substack{n\in\mathbb{N}\\ n\geq n_0}}{\forall} (A(n) \Rightarrow A(n+1))\Big) \Rightarrow \underset{\substack{n\in\mathbb{N}\\ n\geq n_0}}{\forall} A(n). \tag{3.3}$$

To simplify the discussion, let us consider first the case $n_0 = 0$. Why is the conclusion (3.3) justified? Recall the 5th Peano axiom for the natural numbers:

> ***Induction axiom:*** *If a set $S \subset \mathbb{N}$ contains zero and also the successor of every number in S, then $S = \mathbb{N}$.*

Let us take $S = \{n \in \mathbb{N} : A(n)\}$. Then we first show that $A(0)$ is true, so $0 \in S$. Next we show that $A(n) \Rightarrow A(n+1)$ for all $n \in \mathbb{N}$. This means that if $n \in S$, then $n+1$ (the successor of n) is also in S. By the induction axiom, this means that $S = \mathbb{N}$. Thus, by showing the hypothesis in (3.3) we arrive at the conclusion, $A(n)$ is true for all $n \in \mathbb{N}$.

Foundations of Induction

To adapt the previous argument to the case where $n_0 > 0$, we can just take

$$S = \{n \in \mathbb{N} : n < n_0 \vee ((n \geq n_0) \wedge A(n))\}.$$

The details are left to you!

We observe that the 5th Peano axiom is basically tailor-made to ensure the validity of induction. We could paraphrase the axiom as "induction works!" In fact, there are alternative choices for the 5th axiom, such as the so-called

> ***Well-Ordering Principle:*** *Every non-empty set $S \subset \mathbb{N}$ has a least element.*

This axiom assumes that we know what "least", or, more precisely, "less than" means for the natural numbers. While we will discuss ordering relations in detail later, for now we make a provisional definition as follows.

Foundations of Induction

Let S_m be the set containing m as well as the successor of any element of S_m. Then

$$m < n \quad :\Leftrightarrow \quad (n \in S_m) \wedge (n \neq m).$$

Of course, if we use the von Neumann construction of the natural numbers, we simply have $m \leq n \Leftrightarrow m \subset n$.

We now take a "least element of a set M" to be an element $m_0 \in M$ such that $M \subset S_{m_0}$, or in other words, $m_0 \leq m$ for all $m \in M$. We then have the Well-Ordering Principle can then be written as

$$\forall_{M \subset \mathbb{N}} \; \exists_{m \in M} \; M \subset S_m.$$

(The Well-Ordering Principle is sometimes also called the Least Element Principle.)

Foundations of Induction

3.7. Theorem. Assume that a system of numbers satisfies the first four Peano axioms and the Well-Ordering Principle. Then the Induction Axiom holds.

Proof.
Let $S \subset \mathbb{N}$ satisfy the property that $0 \in S$ and that if $n \in S$, then $\text{Succ}(n) \in S$. We need to show that $S = \mathbb{N}$. Suppose that there exists an $n_0 \in \mathbb{N}$ such that $n_0 \notin S$. Then the set $M = \{n \in \mathbb{N} : n \notin S\}$ is non-empty. By the well-ordering principle, M must have a least element m_0. Since $0 \in S$, $m_0 \neq 0$. Since $m_0 > 0$ and $m_0 \in \mathbb{N}$, there exists a number $m_0 - 1$ preceding m_0. This number is not in M, because m_0 is the least element of M. Therefore, $m_0 - 1 \in S$. However, by the definition of S, the successor of $m_0 - 1$ must also be in S. Since the successor of every number is unique, $m_0 \in S$ and hence $m_0 \notin M$. We arrive at a contradiction. □

Foundations of Induction

In fact, the Induction Axiom and the Well-Ordering Principle are equivalent: you will prove in the assignments that the Induction Axiom also implies the Well-Ordering Principle. This means that if we take one of the two as an axiom, the other becomes a theorem that can be proven. It is a common situation in mathematics that we have several equivalent choices for a system of axioms.

Further Examples of Induction

Mathematical induction can be used to prove any sort of statement on the natural numbers in a variety of contexts. Some examples follow:

3.8. Examples.

1. $\forall_{n\in\mathbb{N}} (1+\frac{1}{2})^n \geq 1 + n/2.$
2. $\forall_{n\in\mathbb{N}} \forall_{a,b\in\mathbb{Q}} (a+b)^n = \sum_{k=0}^{n} \frac{n!}{(n-k)!k!} a^n b^{n-k}.$
3. $\forall_{n\in\mathbb{N}} \forall_{\substack{r\in\mathbb{Q} \\ r=p/q \\ q^2>p^2}} \sum_{k=0}^{n} r^k = \frac{r^{k+1}-1}{r-1}.$
4. Let $H_n = \sum_{k=1}^{n} \frac{1}{k}$ for $n \in \mathbb{N}\setminus\{0\}$. Then $\forall_{n\in\mathbb{N}} H_{2^n} \geq 1 + n/2.$
5. Let M be a set and $A_1, \ldots, A_n \subset M$. Then

$$\left(\bigcap_{i=1}^{n} A_i\right)^{\mathsf{c}} = \bigcup_{i=1}^{n} A_i^{\mathsf{c}}.$$

Further Examples of Induction

6. Let M be a set with cardinality $\operatorname{card} M = n$, $n \in \mathbb{N}$. Then $\operatorname{card} \mathscr{P}(M) = 2^n$.
7. Shootout at the O.K. Corral: an odd number of lawless individuals, standing at mutually distinct distances to each other, fire pistols at each other in exactly the same instant. Every person fires at their nearest neighbor, hitting and killing this person. Then there is at least one survivor.

The Shootout

Let us discuss the last example in more detail: Let $P(n)$ be the statement that there is at least one survivor whenever $2n+1$ people, fire pistols at each other in the same instant. Each person fires at his nearest neighbor, and all people stand at mutually distinct distances to each other.

For $n = 1$, there are three people, A, B and C. Suppose that the distance between A and B is the smallest distance of any two of them. Then A fires at B and vice-versa. C fires at either A or B and will not be fired at, so C survives.

Suppose $P(n)$. Let $2n+3$ people participate in the shootout. Suppose that A and B are the closest pair of people. The A and B fire at each other.

- If at least one other person fires at A or B, then there remain at most $2n$ shots fired among the remaining $2n+1$ people, so there is at least one survivor.
- If no-one else fires at A or B, then there are $2n+1$ shots fired among the $2n+1$ people and by $P(n)$, there is at least one survivor.

Pitfalls in Induction

While mathematical induction is an extremely powerful technique, it must be executed most carefully. In proceeding through an induction proof it can happen quite easily that implicit assumptions are made that are not justified, thereby invalidating the result.

3.9. Example. Let us use mathematical induction to argue that every set of $n \geq 2$ lines in the plane, no two of which are parallel, meet in a common point.

The statement is true for $n = 2$, since two lines are not parallel if and only if they meet at some point. Since these are the only lines under considerations, this is the common meeting point of the lines.

We next assume that the statement is true for n lines, i.e., any n non-parallel lines meet in a common point. Let us now consider $n + 1$ lines, which we number 1 through $n + 1$. Take the set of lines 1 through n; by the induction hypothesis, they meet in a common point. The same is true of the lines $2, \ldots, n + 1$. We will now show that these points must be identical.

Pitfalls in Induction

Assume that the points are distinct. Then all lines $2, \ldots, n$ must be the same line, because any two points determine a line completely. Since we can choose our original lines in such a way that we consider distinct lines, we arrive at a contradiction. Therefore, the points must be identical, so all $n + 1$ lines meet in a common point. This completes the induction proof.

Where is the mistake in the above "proof" of our (obviously false) supposition?

Strong (Complete) Induction

The method of induction can be strengthened. We can replace

(I) $A(n_0)$ is true.

(II) $A(n+1)$ is true whenever $A(n)$ is true for $n \geq n_0$.

with

(I) $A(n_0)$ is true.

(II') $A(n+1)$ is true whenever all the statements $A(n_0), A(n_0+1), \ldots, A(n)$ are true.

3.10. Example. We will show the following statement: ***Every natural number $n \geq 2$ is a prime number or the product of primes.***

Clearly the statement is true for $n = 2$, which is prime. Next assume that $2, 3, \ldots, n$ are all prime or the product of prime numbers. Then $n+1$ is either prime or not prime. If it is prime, we are finished. If it is not prime, it is the product of two numbers $a, b < n+1$. However, a and b are themselves products of prime numbers by our assumption, and hence so is $n+1 = a \cdot b$. Therefore, by the strong induction principle the initial statement is true.

Induction vs. Strong Induction

While induction is the principle that

$$\Big(A(n_0) \wedge \underset{\substack{n\in\mathbb{N}\\ n\geq n_0}}{\forall} \big(A(n) \Rightarrow A(n+1)\big)\Big) \Rightarrow \underset{\substack{n\in\mathbb{N}\\ n\geq n_0}}{\forall} A(n) \tag{3.4}$$

strong induction states

$$\Big(A(n_0) \wedge \underset{\substack{n\in\mathbb{N}\\ n\geq n_0}}{\forall} \big((A(n_0) \wedge \cdots \wedge A(n)) \Rightarrow A(n+1)\big)\Big) \Rightarrow \underset{\substack{n\in\mathbb{N}\\ n\geq n_0}}{\forall} A(n). \tag{3.5}$$

It is clear that (3.5) implies (3.4), since of course

$$\big((A(n_0) \wedge \cdots \wedge A(n)) \Rightarrow A(n+1)\big) \Rightarrow \big(A(n) \Rightarrow A(n+1)\big)$$

Thus the "usual" induction is a special case of strong induction. However, the converse is also true, as we shall see.

Induction vs. Strong Induction

We now show that (3.4) implies (3.5), i.e., strong induction follows from induction.

We fix $n_0 \in \mathbb{N}$ and define $B(n) : A(n_0) \wedge \cdots \wedge A(n)$ for $n \geq n_0$. Then $A(n_0) = B(n_0)$ and we can write strong induction as

$$\Big(B(n_0) \wedge \underset{\substack{n\in\mathbb{N}\\ n\geq n_0}}{\forall} \big(B(n) \Rightarrow A(n+1)\big)\Big) \Rightarrow \underset{\substack{n\in\mathbb{N}\\ n\geq n_0}}{\forall} A(n).$$

We can write

$$\big(B(n) \Rightarrow A(n+1)\big) \equiv \big(B(n) \Rightarrow (A(n+1) \wedge B(n))\big) \equiv \big(B(n) \Rightarrow B(n+1)\big)$$

so strong induction becomes

$$\Big(B(n_0) \wedge \underset{\substack{n\in\mathbb{N}\\ n\geq n_0}}{\forall} \big(B(n) \Rightarrow B(n+1)\big)\Big) \Rightarrow \underset{\substack{n\in\mathbb{N}\\ n\geq n_0}}{\forall} A(n). \tag{3.6}$$

Since $\underset{\substack{n\in\mathbb{N}\\ n\geq n_0}}{\forall} A(n) \equiv \underset{\substack{n\in\mathbb{N}\\ n\geq n_0}}{\forall} B(n)$ we see that (3.6) is just induction in B.

Recursive Definitions and the Factorial

The induction axiom also allows us to make ***recursive definitions***. For example, we wish to define a function (to be called the ***factorial***)

$$(\,\cdot\,)!\colon \mathbb{N} \to \mathbb{N}$$

having the properties that

$$0! := 1, \qquad n! := n \cdot (n-1)!, \qquad n \in \mathbb{N} \setminus \{0\}. \tag{3.7}$$

This is an example of a ***recursive definition*** and we may ask whether such a definition "makes sense", i.e., whether such a function exists and is unique.

That such recursive definitions define unique functions on $\mathbb{N}$ can be shown using the induction axiom. We refer again to Halmos's book for the details. In the present case, the function is simply

$$n! := \prod_{k=1}^{n} k, \qquad n \in \mathbb{N} \setminus \{0\}, \tag{3.8}$$

Recursive Definitions

The definition (3.7) is called an ***inductive*** or ***recursive formula*** for $n!$, while (3.8) is called a ***closed formula*** for $n!$. Recursive definitions often occur naturally in the formulation of a problem, and finding a closed formula can be extremely difficult. In some situations, a closed formula is highly desirable, while at other times, important properties are best expressed through recursive expressions.

For example, there exists a continuous extension of the factorial, given by the ***Euler gamma function***, defined for $t > 0$,

$$\Gamma(t) := \int_0^\infty z^{t-1} e^{-z}\, dz, \qquad t > 0.$$

It is possible to show that $\Gamma(1) = 1$ and that

$$\Gamma(t+1) = t\Gamma(t) = t\Gamma\big((t-1)+1\big) \qquad \text{for } t > 0.$$

Justification of Recursive Definitions

Comparing with (3.7), we see that

$$\Gamma(n+1) = n! \qquad \text{for } n \in \mathbb{N}.$$

Since the gamma function is defined for all strictly positive real numbers, we have a "continuous extension" of the factorial.

A slight modification allows for recursive definitions "starting" at $n = n_0$ instead of $n = 0$. Furthermore, we can define functions not just based on their preceding value, but on several such values.

3.11. Example. The ***Fibonacci sequence*** is defined through

$$f_0 := 0, \qquad f_1 := 1, \qquad f_n := f_{n-1} + f_{n-2}, \qquad n \in \mathbb{N} \setminus \{0, 1\}.$$

This type of recursive definition also follows from the induction axiom, much as strong induction does.

Recursive Definitions of Sets

In the same manner, we can define subsets of $\mathbb{N}$ recursively. For example, consider the set $S \subset \mathbb{N}$ such that

$$3 \in S \qquad \text{and} \qquad x, y \in S \Rightarrow x + y \in S. \tag{3.9}$$

(The validity of such a recursive definition (that a set S with the properties (3.9) exists and is unique) is based on the induction axiom.) We know that $3 \in S$, so $3 + 3 = 6 \in S$, $3 + 6 = 9 \in S$, $6 + 6 = 12 \in S$ and so on. Our goal is to prove that

$$S = \{n \in \mathbb{N} : \exists k \in \mathbb{N} \setminus \{0\} : n = 3k\}.$$

However, this requires a little preparation.

Alphabets and Strings

We introduce an example from the theory of formal languages:

3.12. Definition. An ***alphabet*** Σ is a finite, non-empty set of elements called ***symbols***. We define the set Σ^* of ***strings*** (or ***words***) over Σ as follows:

(i) $\lambda \in \Sigma^*$, where λ is the ***empty string*** (***null string***) containing no symbols.

(ii) If $w \in \Sigma^*$ and $x \in \Sigma$, then $wx \in \Sigma^*$.

3.13. Example. Let $\Sigma = \{0, 1\}$. The elements of Σ are called ***bits*** and the words over Σ are called ***bit strings***. λ is a word, so also $\lambda 0 = 0$ is a word, as is $\lambda 1 = 1$. Since $\{0, 1\} \subset \Sigma^*$, the two-symbol words $01, 10, 11, 00 \in \Sigma^*$ and, continuing, $000, 001, 010, 011, 100, 101, 110, 111 \in \Sigma^*$. In this way, we inductively find all words over Σ.

We may interpret strings as tuples or finite sequences, but that is not necessary.

Bit Strings in Logic

Bit strings can be used in logic programming by replacing the values T and F by 1 and 0, respectively. Logical operations then become analogously defined ***bit operations***. In particular, $\neg$ becomes NOT, $\wedge$ becomes AND, $\vee$ becomes OR, where (for example)

b	NOT b
1	0
0	1

a	b	a AND b
1	1	1
1	0	0
0	1	0
0	0	0

a	b	a OR b
1	1	1
1	0	1
0	1	1
0	0	0

Given a bit string we then define corresponding ***bitwise operations*** recursively. For example,

$$\mathrm{NOT}(\lambda) := \lambda, \quad \mathrm{NOT}(wx) := \mathrm{NOT}(w)\,\mathrm{NOT}(x), \quad w \in \Sigma^*,\ x \in \Sigma.$$

Thus

$$\mathrm{NOT}(011) = \mathrm{NOT}(01)\,\mathrm{NOT}(1) = \mathrm{NOT}(0)\,\mathrm{NOT}(1)\,\mathrm{NOT}(1) = 100.$$

Concatenation of Strings

To denote a non-empty word $w \neq \lambda$, we often write wx, where $w \in \Sigma^*$ and $x \in \Sigma$.

3.14. Definition. We define ***concatenation of strings*** as follows:

(i) If $w \in \Sigma^*$, then $w \cdot \lambda = w$, where λ is the empty string.

(ii) If $w_1, w_2 \in \Sigma^*$, $x \in \Sigma$, then

$$w_1 \cdot (w_2 x) = (w_1 \cdot w_2)x.$$

This recursive definition is a bit difficult to read at first, so we give an example.

3.15. Example. Let $\Sigma = \{0, 1\}$. The concatenation of $110, 101 \in \Sigma^*$ according to Definition 3.14 is computed as follows:

$$\underset{w_1}{110} \cdot (\underset{w_2}{10}\,\underset{x}{1}) = (110 \cdot 10)1 = \big((110 \cdot 1)0\big)1$$
$$= \big(\big((110)1\big)0\big)1 = 110101.$$

Length of Strings

Definition 3.14 thus reduces the concatenation of strings to the concatenation of a string with a symbol, which we know how to do from Definition 3.12. In other words, we concatenate words by appending one symbol at a time. We make one more definition:

3.16. Definition. We define the ***length*** $l(w)$ ***of a string*** $w \in \Sigma^*$ as follows:

1. $l(\lambda) = 0$,
2. $l(wx) = l(w) + 1$, where $x \in \Sigma$.

3.17. Remark. Since the set Σ^* is not a subset of the natural numbers, it may be asked whether a set with the properties of Definition 3.12 exists uniquely. That this is the case is an axiom of set theory, i.e., it is assumed that such recursive definitions "work".

Structural Induction

Structural induction is a useful variant of induction that allows us to prove properties for recursively defined objects, such as the strings we have just introduced.

Structural induction establishes a statement on a recursively defined set in two steps. We call those elements specifically included in the set (e.g., the empty string in Σ^*) the basis elements of the set.

1. Establish the statement for the basis elements.
2. Show that if the statement is true for each of the elements used to construct new elements in the recursive step of the definition, the statement holds for these new elements.

Structural Induction

As a first example, consider a proposition $P(w)$, where $w \in \Sigma^*$ is a string. In order to prove that $P(w)$ is true for all $w \in \Sigma^*$, we need to show

1. $P(\lambda)$, where λ is the empty string.
2. $\forall_{w \in \Sigma^*} \forall_{x \in \Sigma} P(w) \Rightarrow P(wx)$.

3.18. Example. We prove that $l(xy) = l(x) + l(y)$ for $x, y \in \Sigma^*$, where $l(w)$ is the length of a string $w \in \Sigma^*$, cf. Definition 3.16.

We need to formulate the statement in such a way that we can employ induction. Let us write it as

$$P(y): \forall_{x \in \Sigma^*} l(xy) = l(x) + l(y).$$

We first establish $P(\lambda)$. This is the statement

$$P(\lambda): \forall_{x \in \Sigma^*} l(x\lambda) = l(x) + l(\lambda).$$

Since $x\lambda = x$ and $l(\lambda) = 0$, $P(\lambda)$ is true.

Structural Induction

Next, assume that $P(y)$ is true. We must now show that $P(ya)$ is true for all $a \in \Sigma$, i.e.,

$$P(y) \Rightarrow \underset{a \in \Sigma}{\forall} P(ya)$$

or

$$\left(\underset{x \in \Sigma^*}{\forall} l(xy) = l(x) + l(y) \right) \Rightarrow \left(\underset{a \in \Sigma}{\forall} \underset{x \in \Sigma^*}{\forall} l(xya) = l(x) + l(ya) \right)$$

Since $l(xya) = l(xy) + 1$ and $l(ya) = l(y) + 1$ by Definition 3.16, the implication follows and the proof is complete.

The justification for structural induction lies in ordinary induction, applied to the statement

> $P(n)$: The claim is true for all elements of the set generated with n or fewer applications of the recursive rules for the set.

Structural induction first establishes $P(0)$ and then $P(n) \Rightarrow P(n+1)$.

Explicit Representation of Recursively Defined Sets

Let us return to our original example: Define $S \subset \mathbb{N}$ to be the set such that

(i) $3 \in S$,

(ii) $x, y \in S \Rightarrow x + y \in S$.

Then set

$$T = \left\{ n \in \mathbb{N} : \exists_{k \in \mathbb{N} \setminus \{0\}} \; n = 3k \right\}$$

We want to show that $S = T$.

First, we show $S \subset T$ by structural induction: $3 = 3 \cdot 1 \in T$, so the base case is established. Now for $x, y \in S$ suppose that $x, y \in T$ so that $x = 3k$ and $y = 3k'$ for $k, k' \in \mathbb{N} \setminus \{0\}$. Then

$$x + y = 3k + 3k' = 3(k + k')$$

so $x + y \in T$. This shows that $S \subset T$.

Explicit Representation of Recursively Defined Sets

Next, we show $T \subset S$ by (ordinary) induction. We claim that

$$\forall_{k \in \mathbb{N} \setminus \{0\}} \quad 3k \in S.$$

For $k = 1$, $3k = 3 \cdot 1 = 3 \in S$, so the base case is established. Now suppose that $3k \in S$. Since $3 \in S$ by definition, we can apply the recursive rule for S to deduce that

$$3(k+1) = 3k + 3 \in S.$$

This shows that $3(k+1) \in S$ if $3k \in S$. By the structural induction principle, $3k \in S$ for all $k \in \mathbb{N} \setminus \{0\}$. This established $T \subset S$.

We finally conclude that $S = T$.