Introduction to Set Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 400

Subsection 1

Introduction to Natural Numbers

Natural Numbers and Sets

- To develop mathematics within axiomatic set theory, it is necessary to define natural numbers.
- Intuitively, natural numbers are $0, 1, 2, 3, \ldots$.
- We can easily give examples of sets having zero, one, two, or three elements:
  - $\emptyset$ has 0 elements;
  - $\{\emptyset\}$ or, in general, $\{a\}$ for any a, has one element;
  - $\{\emptyset, \{\emptyset\}\}$, or $\{\{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}\}$, or, in general, $\{a, b\}$, where $a \neq b$, has two elements, etc.
- We next supplement this intuitive understanding by a rigorous definition.

The First Natural Numbers as Sets

- To define the number 0, we choose a representative of all sets having no elements. This is easy, since there is only one such set: We define $0 = \emptyset$.
- Many sets have one element (singletons): $\{\emptyset\}, \{\{\emptyset\}\}, \{\{\emptyset, \{\emptyset\}\}\}$; How should we choose a representative? Since we already defined 0, a natural choice is $\{0\}$. So we define $1 = \{0\} = \{\emptyset\}$.
- Next we consider sets with two elements: $\{\emptyset, \{\emptyset\}\}$, $\{\{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$, etc. By now, we have defined 0 and 1, and $0 \neq 1$. We choose the set whose elements are the previously defined numbers 0 and 1: $2 = \{0, 1\} = \{\emptyset, \{\emptyset\}\}$.
- It should begin to be obvious how the process continues: $3 = \{0, 1, 2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$.
- $4 = \{0, 1, 2, 3\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}$.
- $5 = \{0, 1, 2, 3, 4\}$, etc.

Problem in General Definition of Natural Numbers

- We would like to define a natural number n as the set of all smaller natural numbers: $\{0, 1, \ldots, n-1\}$. So, n would be a particular set of n elements.
- The problem is that, even though we can define a specific natural number, there is no list of such definitions that tells us what a natural number is in general.
- To do this, we need a statement of the form: "A set n is a natural number if its elements are all the smaller natural numbers", but such a "definition" would involve the very concept being defined.
- Given a natural number n, we get the "next" number by adjoining one more element to n, namely, n itself. The procedure works for $1 = 0 \cup \{0\}$, $2 = 1 \cup \{1\}$, but not for 0, the least natural number.

The Successor of a Set

Definition (Successor)

The **successor** of a set x is the set $S(x) = x \cup \{x\}$.

- Intuitively, the successor $S(n)$ of a natural number n is the "one bigger" number $n + 1$.
- In the following we use the notation $n + 1 = S(n)$.
- We later define addition of natural numbers (using the notion of successor) in such a way that $n + 1$ indeed equals the sum of n and 1. But until then, it is just a notation, and no properties of addition are assumed or implied by it.
- We can now summarize the intuition behind natural numbers:
  (a) 0 is a natural number.
  (b) If n is a natural number, then its successor $n + 1$ is also a natural number.
  (c) All natural numbers are obtained by application of (a) and (b), i.e.. by starting with 0 and repeatedly applying the successor operation: $0, 0 + 1 = 1, 1 + 1 = 2, 2 + 1 = 3, 3 + 1 = 4, 4 + 1 = 5, \ldots$ etc.

Inductive Sets

Definition (Inductive Set)

A set I is called **inductive** if

(a) $0 \in I$.

(b) If $n \in I$, then $(n+1) \in I$.

- An inductive set contains 0 and, with each element, also its successor.
- According to (c) of the preceding slide, an inductive set should contain all natural numbers. The precise meaning of (c) is that the set of natural numbers is an inductive set which contains no other elements but natural numbers, i.e., it is the smallest inductive set.

Definition (Set of Natural Numbers)

The **set of all natural numbers** is the set

$$\mathbb{N} = \{x : x \in I, \text{ for every inductive set } I\}.$$

The elements of $\mathbb{N}$ are called **natural numbers**. Thus, a set x is a natural number if and only if it belongs to every inductive set.

Existence of $\mathbb{N}$

- The existence of $\mathbb{N}$ has to be justified on the basis of the Axiom of Comprehension: Let A be any particular inductive set; then clearly $\mathbb{N} = \{x \in A : x \in I \text{ for every inductive set } I\}$.
- The only remaining question is: Are there any inductive sets at all?
- Unfortunately, the existence of infinite sets (such as $\mathbb{N}$) cannot be proved from the axioms introduced so far.
- The reason is that these axioms have a general form: "For every set X, there exists a set Y such that ...", where, if the set X is finite, the set Y is also finite.
- Since the only set whose existence we postulated outright is $\emptyset$, which is finite, all the other sets whose existence is required by the axioms are also finite.

The Axiom of Infinity

The Axiom of Infinity

An inductive set exists.

- Some mathematicians object to the Axiom of Infinity on the grounds that a collection of objects produced by an infinite process (such as $\mathbb{N}$) should not be treated as a completed entity.
- Infinite sets are basic tools in mathematics and the essence of set theory. No contradiction resulting from their use has ever arisen.
- The Axiom of Infinity yields the set of natural numbers $\mathbb{N}$.

Lemma ($\mathbb{N}$ is Inductive)

$\mathbb{N}$ is inductive. If I is any inductive set, then $\mathbb{N} \subseteq I$.

- $0 \in \mathbb{N}$ because $0 \in I$ for any inductive I. If $n \in \mathbb{N}$, then $n \in I$ for any inductive I, so $(n+1) \in I$ for any inductive I, and consequently $(n+1) \in \mathbb{N}$. This shows that $\mathbb{N}$ is inductive.
  The second part follows from the definition of $\mathbb{N}$.

Ordering of Natural Numbers

- The next step is to define the ordering of natural numbers by size.
- Since the main idea was to define each natural number as a set of smaller natural numbers, we define the ordering as follows:

Definition (Ordering of $\mathbb{N}$)

The relation $<$ on $\mathbb{N}$ is defined by:

$$m < n \quad \text{if and only if} \quad m \in n.$$

- It is now necessary to prove that $<$ is indeed a linear ordering and that the ordered set $(\mathbb{N}, <)$ has the properties that are expected of the natural numbers.

Subsection 2

Properties of Natural Numbers

The Induction Principle

- In the preceding section we defined the set $\mathbb{N}$ of natural numbers to be the least set such that
  (a) $0 \in \mathbb{N}$;
  (b) If $n \in \mathbb{N}$, then $(n+1) \in \mathbb{N}$.
- We also defined $m < n$ to mean $m \in n$.

The Induction Principle

Let $\mathbf{P}(x)$ be a property (possibly with parameters). Assume that:

(a) $\mathbf{P}(0)$ holds.

(b) For all $n \in \mathbb{N}$, $\mathbf{P}(n)$ implies $\mathbf{P}(n+1)$.

Then $\mathbf{P}$ holds for all natural numbers n.

- This is an immediate consequence of our definition of $\mathbb{N}$. The assumptions (a) and (b) simply say that the set $A = \{n \in \mathbb{N} : \mathbf{P}(n)\}$ is inductive. Therefore, $\mathbb{N} \subseteq A$.

Using Proof by Induction

Lemma

(i) $0 \leq n$, for all $n \in \mathbb{N}$.

(ii) For all $k, n \in \mathbb{N}$, $k < n+1$ if and only if $k < n$ or $k = n$.

(i) We let $\mathbf{P}(x)$ be the property "$0 \leq x$" and proceed to establish the assumptions of the Induction Principle.

(a) $\mathbf{P}(0)$ holds. $\mathbf{P}(0)$ is the statement "$0 \leq 0$", which is certainly true $(0 = 0)$.

(b) $\mathbf{P}(n)$ implies $\mathbf{P}(n+1)$. Let us assume that $\mathbf{P}(n)$ holds, i.e., $0 \leq n$. This means, by definition of $<$, that $0 = n$ or $0 \in n$. In either case, $0 \in n \cup \{n\} = n+1$, so $0 < (n+1)$ and $\mathbf{P}(n+1)$ holds.

Having proved (a) and (b) we use the Induction Principle to conclude that $\mathbf{P}(n)$ holds for all $n \in \mathbb{N}$, i.e., $0 \leq n$, for all $n \in \mathbb{N}$.

(ii) This part does not require induction. It suffices to observe that $k \in n \cup \{n\}$ if and only if $k \in n$ or $k = n$.

Transitivity of $<$

Theorem

$(\mathbb{N}, <)$ is a linearly ordered set.

- We must show that $<$ is transitive, asymmetric and linear on $\mathbb{N}$.
  - (i) The relation $<$ is transitive on $\mathbb{N}$: We have to show that, for all $k, m, n \in N$, $k < m$ and $m < n$ imply $k < n$. We use induction on n. Let $\mathbf{P}(x)$ be "for all $k, m \in \mathbb{N}$, if $k < m$ and $m < x$, then $k < x$".
    - (a) $\mathbf{P}(0)$ holds. $\mathbf{P}(0)$ asserts: for all $k, m \in \mathbb{N}$, if $k < m$ and $m < 0$, then $k < 0$. By the lemma, there is no $m \in \mathbb{N}$ such that $m < 0$, so $\mathbf{P}(0)$ is trivially true.
    - (b) Assume $\mathbf{P}(n)$, i.e., for all $k, m \in \mathbb{N}$, if $k < m$ and $m < n$, then $k < n$. We have to prove $\mathbf{P}(n+1)$, i.e., we have to show that $k < m$ and $m < (n+1)$ imply $k < (n+1)$. But if $k < m$ and $m < (n+1)$, then by the lemma, $m < n$ or $m = n$. If $m < n$, we get $k < n$ by the inductive assumption $\mathbf{P}(n)$. If $m = n$, we have $k < n$ from $k < m$. In either case, $k < n+1$ by the lemma and, therefore, $\mathbf{P}(n+1)$.

  The Induction Principle now asserts the validity of $\mathbf{P}(n)$, for all $n \in \mathbb{N}$. This is precisely the statement of transitivity of $(\mathbb{N}, <)$.

Asymmetry of $<$

- We continue the proof by showing asymmetry:

  (ii) The relation $<$ is asymmetric on $\mathbb{N}$: Assume that $n < k$ and $k < n$. By transitivity, this implies $n < n$. So we only have to show that the latter is impossible.
  We proceed again by induction:

  - Clearly, $0 < 0$ is impossible (it would mean that $\emptyset \in \emptyset$).
  - Let us assume that $n < n$ is false and prove that $(n+1) < (n+1)$ is false. If $(n+1) < (n+1)$, were true, we would have either $n+1 < n$ or $n+1 = n$ by the preceding lemma. Since $n < n+1$ holds by the same lemma, and we have proved transitivity of $<$ previously, we conclude that $n < n$, thus contradicting our inductive assumption.

  We have now established both (a) and (b) in the Induction Principle (with $\mathbf{P}(x)$ being "$x < x$ is false"). We can conclude that $n < n$ is impossible for any $n \in \mathbb{N}$. We now know that $<$ is a (strict) ordering of $\mathbb{N}$.

It remains to prove $<$ is a linear ordering of $\mathbb{N}$.

$<$ is Linear

- It remains to prove that $<$ is a linear ordering.

  (iii) $<$ is a linear ordering of $\mathbb{N}$: We have to prove that for all $m, n \in \mathbb{N}$ either $m < n$ or $m = n$ or $n < m$. We proceed by induction on n.

  (a) For all $m \in \mathbb{N}$, either $m < 0$ or $m = 0$ or $0 < m$. This follows immediately from the preceding lemma.

  (b) Assume that for all $m \in \mathbb{N}$, either $m < n$ nor $m = n$ or $n < m$. We have to prove an analogous statement with $(n + 1)$ in place of n.
  If $m < n$, then $m < (n + 1)$ by the lemma and transitivity.
  Similarly, if $m = n$ then $m < (n + 1)$.
  Finally, if $n < m$, we would like to conclude that $n + 1 \leq m$. This would show that, for all $m \in \mathbb{N}$, either $m < (n + 1)$ or $m = (n + 1)$ or $(n + 1) < m$, establishing (b), and completing the proof.
  So we prove that if $n < m$, then $(n + 1) \leq m$ holds for all $m \in \mathbb{N}$ by induction on m (n is a parameter; that is, we are going to apply the Induction Principle to the property $\mathbf{P}(x)$: "If $n < x$, then $n + 1 \leq x$").
  We do this in the next slide and conclude that $\mathbf{P}(m)$ holds for all $m \in \mathbb{N}$, as needed.

  Finally, we finish the proof of (iii) by observing that the assumptions (a) and (b) of the Induction Principle have now been established.

Finishing Proof of Linearity of $<$

- We are going to apply the Induction Principle to the property $\mathbf{P}(x)$: "If $n < x$, then $n + 1 \leq x$".
  - If m $= 0$, the statement "if $n < 0$, then $n + 1 \leq 0$" is true (since its hypothesis must he false).
  - Assume $\mathbf{P}(m)$, i.e., if $n < m$, then $(n + 1) \leq m$. To prove $\mathbf{P}(m + 1)$, assume that $n < m + 1$. Then $n < m$ or $n = m$.
    If $n < m$, $n + 1 \leq m$ by the inductive assumption, and so $n + 1 \leq m + 1$.
    If $n = m$ then of course $n + 1 = m + 1$.
    In either case $\mathbf{P}(m + 1)$ is proved.

Induction Principle Second Version

- The preceding Proof of Part (iii) is an example of "double induction":
  - In order to prove a statement depending on two variables m and n, we proceed by induction on one of them (n).
  - But, then, the proof of the induction assumption (b) in itself requires induction on the other variable m (for fixed n).
- We state and prove another version of the Induction Principle that is often more convenient.

The Induction Principle, Second Version

Let $\mathbf{P}(x)$ be a property (possibly with parameters). Assume that, for all $n \in \mathbb{N}$,

$$\text{If } \mathbf{P}(k) \text{ holds for all } k < n, \text{ then } \mathbf{P}(n).$$

Then $\mathbf{P}$ holds for all natural numbers n.

I.e., in order to prove $\mathbf{P}(n)$, for all $n \in \mathbb{N}$, it suffices to prove $\mathbf{P}(n)$ (for all $n \in \mathbb{N}$) under the assumption that it holds for all smaller natural numbers.

Proof of the Second Version of the Induction Principle

- Assume that

$$\text{If } \mathbf{P}(k) \text{ holds for all } k < n, \text{ then } \mathbf{P}(n).$$

Consider the property $\mathbf{Q}(n)$: "$\mathbf{P}(k)$ holds for all $k < n$".

- Clearly $\mathbf{Q}(0)$ is true (there are no $k < 0$).
- If $\mathbf{Q}(n)$ holds, then $\mathbf{Q}(n+1)$ holds: If $\mathbf{Q}(n)$ holds, then $\mathbf{P}(k)$ holds for all $k < n$, and consequently also for $k = n$, by hypothesis. The preceding lemma shows that $\mathbf{P}(k)$ holds for all $k < n+1$, and therefore $\mathbf{Q}(n+1)$ holds.

By the Induction Principle, $\mathbf{Q}(n)$ is true for all $n \in \mathbb{N}$. Since for $k \in \mathbb{N}$ there is some $n > k$ (e.g., $n = k+1$), we have $\mathbf{P}(k)$ true for all $k \in \mathbb{N}$, as desired.

Well-Ordering

Definition (Well-Ordering)

A linear ordering $\prec$ of a set A is a **well-ordering** if every nonempty subset of A has a least element. The ordered set $(A, \prec)$ is then called a **well-ordered set**.

- Well-ordered sets form a backbone of set theory and we study them extensively later.

Theorem (Well-Ordering of $\mathbb{N}$)

$(\mathbb{N}, <)$ is a well-ordered set.

- Let X be a nonempty subset of $\mathbb{N}$. We have to show that X has a least element. So we assume that X does not have a least element and consider $\mathbb{N} - X$. The crucial step is to observe that if $k \in \mathbb{N} - X$, for all $k < n$, then $n \in \mathbb{N} - X$: otherwise, n would be the least element of X. By the second version of the Induction Principle we conclude that $n \in \mathbb{N} - X$ holds for all natural numbers n ($\mathbf{P}(x)$ is the property "$x \in \mathbb{N} - X$") and therefore that $X = \emptyset$, a contradiction.

Bounded Sets of Natural Numbers Have Maxima

Theorem

If a nonempty set of natural numbers has an upper bound in the ordering $<$, then it has a greatest element.

- Let $A \subseteq \mathbb{N}$, $A \neq \emptyset$ be given. Let $B = \{k \in \mathbb{N} : k \text{ is an upper bound of } A\}$. We assume that $B \neq \emptyset$. By the preceding theorem, B has a least element n, so $n = \sup(A)$. The proof is completed by showing that $n \in A$. Trivial induction proves that either $n = 0$ or $n = k + 1$ for some $k \in \mathbb{N}$. Assume that $n \notin A$. Then $n > m$, for all $m \in A$. Since $A \neq \emptyset$, this means that $n \neq 0$. Therefore, $n = k + 1$ for some $k \in \mathbb{N}$, which gives $k \geq m$ for all $m \in A$. Thus k is an upper bound of A and $k < n$, a contradiction.

Subsection 3

The Recursion Theorem

Finite and Infinite Sequences

- A **sequence** is a function whose domain is either a natural number or $\mathbb{N}$.
- A sequence whose domain is some natural number $n \in \mathbb{N}$ is called a **finite sequence of length** n and is denoted $\langle a_i : i < n \rangle$ or $\langle a_i : i = 0, 1, \ldots, n-1 \rangle$ or $\langle a_0, a_1, \ldots, a_{n-1} \rangle$.
- $\langle\rangle$ $(= \emptyset)$ is the unique sequence of length 0, the **empty sequence**.
- $\mathrm{Seq}(A) = \bigcup_{n \in \mathbb{N}} A^n$ denotes the set of all finite sequences of elements of A.
- If the domain of a sequence is $\mathbb{N}$, we call it an **infinite sequence** and denote it $\langle a_i : i \in \mathbb{N} \rangle$ or $\langle a_i : i = 0, 1, 2, \ldots \rangle$ or $\langle a_i \rangle_{i=0}^{\infty}$.
- So infinite sequences of elements of A are just members of $A^{\mathbb{N}}$.
- We also use the notation $\{a_i : i \in \mathbb{N}\}$, $\{a_i\}_{i=0}^{\infty}$, etc., for the range of the sequence $\langle a_i : i \in \mathbb{N} \rangle$.
- Similarly, $\{a_i : i < n\}$ or $\{a_0, a_1, \ldots, a_{n-1}\}$ denotes the range of $\langle a_i : i < n \rangle$.

Examples of Sequences

- We introduce two examples of sequences:
  (a) $s : \mathbb{N} \to \mathbb{N}$ is defined by $s_0 = 1$ and $s_{n+1} = n^2$, for all $n \in \mathbb{N}$.
  (b) $f : \mathbb{N} \to \mathbb{N}$ is defined by $f_0 = 1$ and $f_{n+1} = f_n \times (n+1)$, for all $n \in \mathbb{N}$.
- The two definitions exhibit a crucial difference.
  - The definition of s gives explicit instructions on how to compute s_x for any $x \in \mathbb{N}$. It enables us to formulate a property $\mathbf{P}$ such that $s_x = y$ if and only if $\mathbf{P}(x, y)$. $\mathbf{P}$ is "either $x = 0$ and $y = 1$ or, for some $n \in \mathbb{N}$, $x = n + 1$ and $y = n^2$". The existence and uniqueness of s satisfying (a) follows from our axioms: $s = \{(x, y) \in \mathbb{N} \times \mathbb{N} : \mathbf{P}(x, y)\}$.
  - The instructions supplied by the definition of f tell us only how to compute f_x provided that the value of f for some smaller number (namely, $x - 1$) was already computed. It is not immediately obvious how to formulate a property $\mathbf{P}$, not involving the function f being defined, such that $f_x = y$ if and only if $\mathbf{P}(x, y)$.
- The definition in (b) gives conditions f ought to satisfy: "f is a function on $\mathbb{N}$ to $\mathbb{N}$ which satisfies the "initial condition": $f_0 = 1$, and the "recursive condition": for all $n \in \mathbb{N}$, $f_{n+1} = f_n \times (n+1)$".

The Recursion Theorem

- A recursive definition of this kind is justified only if it is possible to show that there exists some function satisfying the required conditions, and that there do not exist two or more such functions.

The Recursion Theorem

For any set A, any $a \in A$, and any function $g : A \times \mathbb{N} \to A$, there exists a unique infinite sequence $f : \mathbb{N} \to A$ such that

(a) $f_0 = a$;

(b) $f_{n+1} = g(f_n, n)$, for all $n \in \mathbb{N}$.

- In Example (b), we had $A = \mathbb{N}$, $a = 1$, and $g(u, v) = u \times (v + 1)$.
- The set a is the "initial value" of f.
- The role of g is to provide instructions for computing f_{n+1} assuming f_n has already been computed.

Idea Behind the Proof of the Recursion Theorem

- The proof of the Recursion Theorem consists of devising an explicit definition of f.
- In Example (b), f_n is the n-factorial. An explicit definition of f is: $f_0 = 1$ and $f_m = 1 \times 2 \times \cdots \times (m-1) \times m$, if $m \neq 0$ and $m \in \mathbb{N}$.
- The problem consists in making "$\cdots$" precise. It can be resolved by stating that f_m is the result of a computation: $1, 1 \times 1, (1 \times 1) \times 2, (1 \times 1 \times 2) \times 3, \ldots, (1 \times 1 \times 2 \times \cdots \times (m-1)) \times m$.
- A computation is a finite sequence starting with the "initial value" of f and repeatedly applying g.
- In the example, the m-step computation t is a finite sequence of length $m+1$ where $t_0 = 1$ and $t_{k+1} = t_k \times (k+1) = g(t_k, k)$, for all $k < m$, $k \geq 0$.
- The rigorous explicit definition of f then is: $f_m = t_m$ where t is an m-step computation (based on $a = 1$ and g).
- The existence and uniqueness of f is reduced to showing that there is precisely one m-step computation for each $m \in \mathbb{N}$.

Proof of Existence I

- Existence of f: A function $t : (m+1) \to A$ is called an m-**step computation based on** a **and** g if $t_0 = a$, and, for all k such that $0 \leq k < m$, $t_{k+1} = g(t_k, k)$. Notice that $t \subseteq \mathbb{N} \times A$. Let

$$F = \{t \in \mathcal{P}(\mathbb{N}xA) : t \text{ is an } m\text{-step computation for some } m \in \mathbb{N}\}.$$

Let $f = \bigcup F$.

- Claim: f is a function.
  It suffices to show that the system of functions F is compatible. So let $t, u \in F$, $\mathrm{dom}t = n \in \mathbb{N}$, $\mathrm{dom}u = m \in \mathbb{N}$. Assume, e.g., $n \leq m$. Then $n \subseteq m$, and it suffices to show that $t_k = u_k$, for all $k < n$. This can be done by induction:
  - First, $t_0 = a = u_0$.
  - Next, let k be such that $k + 1 < n$, and assume $t_k = u_k$. Then $t_{k+1} = g(t_k, k) = g(u_k, k) = u_{k+1}$.

  Thus, $t_k = u_k$, for all $k < n$.

Proof of Existence II

- Existence of f (Cont'd):
  - Claim: $\mathrm{dom} f = \mathbb{N}$ and $\mathrm{ran} f \subseteq A$.
    We know that $\mathrm{dom} f \subseteq \mathbb{N}$ and $\mathrm{ran} f \subseteq A$. To show that $\mathrm{dom} f = \mathbb{N}$, it suffices to prove that for each $n \in \mathbb{N}$ there is an n-step computation t. We use the Induction Principle.
    - Clearly, $t = \{(0, a)\}$ is a 0-step computation.
    - Assume that t is an n-step computation. Then the following function t^+ on $(n+1)+1$ is an $(n+1)$-step computation:

$$\begin{aligned} t_k^+ &= t_k, \text{ if } k \leq n \\ t_{n+1}^+ &= g(t_n, n). \end{aligned}$$

    We conclude that each $n \in \mathbb{N}$ is in the domain of some computation $t \in F$, so $\mathbb{N} \subseteq \bigcup_{t \in F} \mathrm{dom} t = \mathrm{dom} f$.

Uniqueness of f

- We finish the proof of the existence of f:
  - Claim: f satisfies conditions (a) and (b).
    Clearly, $f_0 = a$ since $t_0 = a$, for all $t \in F$. To show that $f_{n+1} = g(f_n, n)$, for any $n \in \mathbb{N}$, let t be an $(n+1)$-step computation. Then $t_k = f$, for all $k \in \mathrm{dom} t$. So $f_{n+1} = t_{n+1} = g(t_n, n) = g(f_n, n)$.

  The existence of a function f with the properties required by the Recursion Theorem follows from the three claims.
- Uniqueness of f: Let $h : \mathbb{N} \to A$ be such that

  (a') $h_0 = a$;
  (b') $h_{n+1} = g(h_n, n)$, for all $n \in \mathbb{N}$.

  We show that $f_n = h_n$, for all $n \in \mathbb{N}$, again using induction.
  - First, $f_0 = a = h_0$.
  - If $f_n = h_n$, then $f_{n+1} = g(f_n, n) = g(h_n, n) = h_{n+1}$.

  Therefore, $f = h$.

Characterization of $(\mathbb{N}, <)$

- We use the Recursion Theorem to prove that some properties of the ordering of $\mathbb{N}$ by size uniquely characterize the ordered set $(N, <)$.

Theorem (Characterization of $<$)

Let $(A, \prec)$ be a nonempty linearly ordered set with the properties:

(a) For every $p \in A$, there is $q \in A$ such that $q \succ p$.

(b) Every nonempty subset of A has a $\prec$-least clement.

(c) Every nonempty subset of A that has an upper bound has a $\prec$-greatest element.

Then $(A, \prec)$ is isomorphic to $(\mathbb{N}, <)$.

- We construct the isomorphism f using the Recursion Theorem. Let a be the least element of A and let $g(x, n)$ be the least element of A greater than x (for any n). Then $a \in A$ and g is a function on $A \times \mathbb{N}$ into A: $g(x, n)$ is defined for any $x \in A$ because of (a) and (b) and does not depend on n.

Proof of the Characterization of $(\mathbb{N}, <)$

- a is the least element of A and $g(x, n)$ is the least element of A greater than x. The Recursion Theorem guarantees the existence of a function $f : \mathbb{N} \to A$, such that
  (i) $f_0 = a$, the least element of A.
  (ii) $f_{n+1} = g(f_n, n) =$ the least element of A greater than f_n.

  It is obvious that $f_n \prec f_{n+1}$, for each $n \in \mathbb{N}$. By induction, we get $f_n \prec f_m$, whenever $n < m$. Consequently, f is a one-to-one function.
  It remains to show that the range of f is A.
  If not, $A - \text{ran}f \neq \emptyset$. Let p be the least element of $A - \text{ran}f$. The set $B = \{q \in A : q \prec p\}$ has an upper bound p, and is nonempty (otherwise, p would be the least element of A, but then $p = f_0$). Let q be the greatest element of B (it exists by assumption (c)). Since $q \prec p$, we have $q = f_m$, for some $m \in \mathbb{N}$. However, it is now easily seen that p is the least element of A greater than q. Therefore, $p = f_{n+1}$, by the recursive condition (ii). Consequently, $p \in \text{ran}f$, a contradiction.

General Recursion

- In some recursive definitions, the value of f_{n+1} depends not only on f_n, but also on f_k for other $k < n$.
- A typical example is the Fibonacci sequence: $1, 1, 2, 3, 5, 8, 13, 21, \ldots$. Here $f_0 = 1$, $f_1 = 1$, and $f_{n+1} = f_n + f_{n-1}$, for $n > 0$.
- The following theorem formalizes this recursive construction:

Theorem (General Recursion)

For any set S and any function $g : \mathrm{Seq}(S) \to S$, there exists a unique sequence $f : \mathbb{N} \to S$ such that $f_n = g(f \restriction n) = g(\langle f_0, \ldots, f_{n-1} \rangle)$, for all $n \in \mathbb{N}$.

- Notice that, in particular, $f_0 = g(f \restriction 0) = g(\langle\rangle) = g(\emptyset)$.
- To obtain the Fibonacci sequence, we let

$$g(t) = \begin{cases} 1, & \text{if } t \text{ is a finite sequence of length 0 or 1} \\ t_{n-1} + t_{n-2}, & \text{if } t \text{ is a finite sequence of length } n > 1 \end{cases}$$

Proof of General Recursion

- The idea is to use the Recursion Theorem to define the sequence $\langle F_n : n \in \mathbb{N} \rangle = \langle f \restriction n : n \in \mathbb{N} \rangle$. So we define

$$F_0 = \langle\rangle \quad \text{and} \quad F_{n+1} = F_n \cup \{(n, g(F_n))\}, \text{ for all } n \in \mathbb{N}.$$

The existence of $\langle F_n : n \in \mathbb{N} \rangle$ follows from the Recursion Theorem with $A = \mathrm{Seq}(S)$, $a = \langle\rangle$ and $G : A \times \mathbb{N} \to A$ defined by

$$G(t, n) = \begin{cases} t \cup \{\langle n, g(t) \rangle\}, & \text{if } t \text{ is a sequence of length } n \\ \langle\rangle, & \text{otherwise} \end{cases}.$$

It is easy to prove by induction that each F_n belongs to S^n and that $F_n \subseteq F_{n+1}$, for all $n \in \mathbb{N}$. Therefore, $\{F_n : n \in \mathbb{N}\}$ is a compatible system of functions. Let $f = \bigcup_{n \in \mathbb{N}} F_n$. Then, clearly, $f : \mathbb{N} \to S$ and $f \restriction n = F_n$, for all $n \in \mathbb{N}$. Finally, $f_n = F_{n+1}(n) = g(F_n) = g(f \restriction n)$, as needed.

Parametric Version of the Recursion Theorem

- The following "parametric" version allows us to use recursion to define functions of two variables.

Theorem (Parametric Version of Recursion)

Let $a : P \to A$ and $g : P \times A \times \mathbb{N} \to A$ be functions. There exists a unique function $f : P \times \mathbb{N} \to A$, such that

(a) $f(p, 0) = a(p)$, for all $p \in P$;

(b) $f(p, n+1) = g(p, f(p, n), n)$, for all $n \in \mathbb{N}$ and $p \in P$.

The notation $f_{p,0}$ may be used in place of $f(p, 0)$, etc.

- Define an m-**step computation** to be a function $t : P \times (m+1) \to A$ such that, for all $p \in P$, $t(p, 0) = a(p)$ and

$$t(p, k+1) = g(p, t(p, k), k), \text{ for all } k, \text{ such that } 0 < k < m.$$

Then follow the steps in the proof of the Recursion Theorem, always carrying p along.

Subsection 4

Arithmetic of Natural Numbers

Definition of Addition

- We apply the Recursion Theorem to define addition of natural numbers; Then, we use Induction to prove basic properties of addition.

Theorem

There is a unique function $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that

(a) $+(m, 0) = m$, for all $m \in \mathbb{N}$;

(b) $+(m, n + 1) = +(m, n) + 1$, for all $m, n \in \mathbb{N}$.

- In the parametric version of the Recursion Theorem let $A = P = \mathbb{N}$, $a(p) = p$, for all $p \in \mathbb{N}$, and $g(p, x, n) = x + 1$, for all $p, x, n \in \mathbb{N}$.
- Notice that letting $n = 0$ in (b) leads to $+(m, 0 + 1) = +(m, 0) + 1$: Since, by (a), $+(m, 0) = m$ and, by the definition of the number 1, $0 + 1 = S(0) = 1$, we have $+(m, 1) = m + 1 = S(m)$, so the successor of $m \in \mathbb{N}$ is indeed the sum of m and 1.
- We write $m + n$ instead of $+(m, n)$ in the sequel. In this notation:
  - $m + 0 = m$;
  - $m + (n + 1) = (m + n) + 1$.

Commutativity of Addition

Theorem (Commutativity of Addition)

Addition is commutative; i.e., for all $m, n \in \mathbb{N}$, $m + n = n + m$.

- Let us say that n **commutes** if $m + n = n + m$ holds for all $m \in \mathbb{N}$. We prove that every $n \in \mathbb{N}$ commutes, by induction on n.
  - To show that 0 commutes, it suffices to show that $0 + m = m$ for all m (because, then, $0 + m = m + 0$ by definition). Clearly, $0 + 0 = 0$, and if $0 + m = m$, then $0 + (m + 1) = (0 + m) + 1 = m + 1$ (induction on m).
  - Assume that n commutes. We show that $n + 1$ commutes. We prove, by induction on m, that $m + (n + 1) = (n + 1) + m$ for all $m \in \mathbb{N}$.
    - If $m = 0$, then the equality has already been shown.
    - Assume that $m + (n + 1) = (n + 1) + m$.

$$
\begin{aligned}
(m+1)+(n+1) &= ((m+1)+n)+1 && \text{(by definition)}\\
&= (n+(m+1))+1 && \text{(since } n \text{ commutes)}\\
&= ((n+m)+1)+1 && \text{(by definition)}\\
&= ((m+n)+1)+1 && \text{(since } n \text{ commutes)}\\
&= (m+(n+1))+1 && \text{(by definition)}\\
&= ((n+1)+m)+1 && \text{(induction hypothesis)}\\
&= (n+1)+(m+1) && \text{(by definition).}
\end{aligned}
$$

Peano Arithmetic

- The theory of arithmetic of natural numbers can be developed axiomatically. The system of axioms is called **Peano arithmetic**:
  - The undefined notions of Peano arithmetic are the constant 0, the unary operation S, and the binary operations $+$ and $\cdot$.
  - The axioms of Peano arithmetic are:

    (P1) If $S(n) = S(m)$, then $n = m$.
    (P2) $S(n) \neq 0$.
    (P3) $n + 0 = n$.
    (P4) $n + S(m) = S(n + m)$.
    (P5) $n \cdot 0 = 0$.
    (P6) $n \cdot S(m) = (n \cdot m) + n$.
    (P7) If $n \neq 0$, then $n = S(k)$, for some k.
    (P8) **The Induction Schema**: Let **A** be an arithmetical property (i.e., a property expressible in terms of $+, \cdot, S, 0$). If 0 has the property **A** and if $\mathbf{A}(k)$ implies $\mathbf{A}(S(k))$ for every k, then every number has **A**.

- It is not difficult to verify that natural numbers and arithmetic operations, as we defined them, satisfy the Peano axioms.

Subsection 5

Integers and Rational Numbers

Idea Behind Subtraction

- We defined natural numbers and their ordering and indicated how arithmetic operations on natural numbers can be defined.
- We now define integers and rational numbers.
- The idea is to convert an arithmetic operation that is only partially defined on natural numbers (subtraction in the case of integers, division in the case of rationals) into a total operation.
- We just outline the main ideas, and leave out almost all proofs.
- Subtraction may be defined for those pairs (n, m) of natural numbers where $n \geq m$. In this case, $n - m$ is the unique natural number k for which $n = m + k$. If $n < m$, no such natural number k exists, and $n - m$ is undefined.
- If $n - m$ is represented by the ordered pair (n, m), different ordered pairs represent the same integer, e.g., $(2, 5)$ and $(6, 9)$ both represent -3. In general, (n_1, m_1) and (n_2, m_2) represent the same integer if and only if $n_1 - m_1 = n_2 - m_2$. Rewritten as $n_1 + m_2 = n_2 + m_1$, it involves only addition of natural numbers.

Formal Construction of $\mathbb{Z}$

- Let $\mathbb{Z}' = \mathbb{N} \times \mathbb{N}$. Define a relation $\approx$ on $\mathbb{Z}'$ by

$$(a, b) \approx (c, d) \quad \text{if and only if} \quad a + d = b + c.$$

- The relation $\approx$ is an equivalence relation on $\mathbb{Z}'$.
- Let $\mathbb{Z} = \mathbb{Z}'/\approx$ be the set of all equivalence classes of $\mathbb{Z}'$ modulo $\approx$. We call $\mathbb{Z}$ be the **set of all integers**. Its elements are **integers**.
- Next, define a relation $<$ on $\mathbb{Z}$ by

$$[(a, b)] < [(c, d)] \quad \text{if and only if} \quad a + d < b + c.$$

Since (a, b) represents $a - b$ and (c, d) represents $c - d$, $a - b < c - d$ should mean $a + d < b + c$.

Representatives

- $<$ is well defined (i.e., truth or falsity of $[(a,b)] < [(c,d)]$ does not depend on the choice of representatives (a,b) and (c,d) but only on their respective equivalence classes).
- $<$ it is a linear ordering.
- For each integer $[(a,b)]$
  - either $a \geq b$, in which case $(a,b) \approx (a-b,0)$ ("-" is subtraction of natural numbers, which is defined in this case)
  - or $a < b$, in which case $(a,b) \approx (0,b-a)$.
- It follows that each integer contains a unique pair of the form $(n,0)$, $n \in \mathbb{N}$, or $(0,n)$, $n \in \mathbb{N} - \{0\}$. So $[(n,0)]$ are the positive integers and $[(0,n)]$ are the negative ones.
- The mapping $F : \mathbb{N} \to \mathbb{Z}$ defined by $F(n) = [(n,0)]$ is one-to-one and order-preserving, i.e., $m < n$ implies that $F(m) < F(n)$.
- We identify each integer of the form $[(n,0)]$ with the corresponding natural number n, and denote each integer of the form $[(0,n)]$ by $-n$, e.g., $-3 = [(0,3)] = [(2,5)] = [(6,9)]$.

Addition and Multiplication on $\mathbb{Z}$

- $(\mathbb{Z}, <)$ has no endpoints;
- $\{x \in \mathbb{Z} : a < x < b\}$, $a, b \in \mathbb{Z}$, $a < b$, has a finite number of elements.
- Every nonempty set of integers bounded from above has a greatest element, and every nonempty set of integers bounded from below has a least element.
- We can define **addition** and **multiplication** of integers by

$$\begin{aligned} [(a,b)] + [(c,d)] &= [(a+c, b+d)]; \\ [(a,b)] \cdot [(c,d)] &= [(ac+bd, ad+bc)]. \end{aligned}$$

- These operations satisfy the usual laws of algebra (commutativity, associativity, and distributivity of multiplication over addition).
- Moreover, for those integers that are natural numbers, addition and multiplication of integers agree with addition and multiplication of natural numbers.

Subtraction and Absolute Value

- We define **subtraction** by

$$[(a,b)] - [(c,d)] = [(a,b)] + (-[(c,d)]),$$

  where $-[(c,d)] = [(d,c)]$ is the **opposite** of $[(c,d)]$.
- Notice that $-[(n,0)] = [(0,n)] = -n$ and $-[(0,n)] = [(n,0)] = n$, in agreement with previous notation.
- The **absolute value** $|a|$ of an integer a is defined by

$$|a| = \begin{cases} a, & \text{if } a \geq 0 \\ -a, & \text{if } a < 0 \end{cases}$$

Fractions Over $\mathbb{Z}$

- We say that an integer a is **divisible** by an integer b if there is a unique integer x such that $a = b \cdot x$. This unique x is then called the **quotient** of a and b.
- We extend the system of integers so that any a is divisible by any b and all useful arithmetic laws remain valid in the extended system.
- Since the equation $a = 0 \cdot x$ bas either none or many solutions, the best we can hope for is an extension in which for all a and all $b \neq 0$, there is a unique x, such that $a = b \cdot x$.
- Let $\mathbb{Q}' : \mathbb{Z} \times (\mathbb{Z} - \{0\}) = \{(a, b) \in \mathbb{Z}^2 : b \neq 0\}$. We call $\mathbb{Q}'$ the **set of fractions over** $\mathbb{Z}$ and write a/b in place of (a, b) for $(a, b) \in \mathbb{Q}'$.
- We define an equivalence $\approx$ on the set $\mathbb{Q}'$ by
$$\frac{a}{b} \approx \frac{c}{d} \quad \text{if and only if} \quad a \cdot d = b \cdot c.$$
- Let $\mathbb{Q} = \mathbb{Q}'/\approx$ be the set of equivalence closes of $\mathbb{Q}$ modulo $\approx$. Elements of $\mathbb{Q}$ are called **rational numbers**; the rational number represented by a/b is denoted $[a/b]$.

Addition, Multiplication and Division in $\mathbb{Q}$

- There is an obvious one-to-one mapping i of the set $\mathbb{Z}$ of integers into the rationals: $i(a) = [\frac{a}{1}]$.
- We define **addition** and **multiplication** of rationals:

$$\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] = \left[\frac{a \cdot d + b \cdot c}{b \cdot d}\right], \quad \left[\frac{a}{b}\right] \cdot \left[\frac{c}{d}\right] = \left[\frac{a \cdot c}{b \cdot d}\right].$$

- One must now show:
  - (a) Addition and multiplication of the rationals are well defined (i.e., independent of the choice of representative).
  - (b) For integers, the new definitions agree with the old ones: i.e., $i(a + b) = i(a) + i(b)$ and $i(a \cdot b) = i(a) \cdot i(b)$, for all $a, b \in \mathbb{Z}$.
  - (c) Addition and multiplication of rationals satisfy the usual laws of algebra.
  - (d) If $A \in \mathbb{Q}$, $B \in \mathbb{Q}$, and $B \neq [0/1]$, then the equation $A = B \cdot X$ has a unique solution $X \in \mathbb{Q}$. Thus, **division** of rational numbers is defined, as long as the divisor is not zero; we denote this operation $\div$: $X = A \div B$.

Natural Ordering of Rationals

- Finally, we extend the ordering of integers to the rationals.
- First, notice that each rational can be represented by a fraction a/b where the denominator b is greater than 0:

$$\left[\frac{a}{b}\right] = \left[\frac{-a}{-b}\right] \text{ and either } b > 0 \text{ or } -b > 0.$$

- We now define the **natural ordering** of rationals:

$$\text{If } b > 0 \text{ and } d > 0, \text{ let } \left[\frac{a}{b}\right] < \left[\frac{c}{d}\right] \text{ if and only if } a \cdot d < b \cdot c.$$

- The definition does not depend on the choice of representatives as long as $b > 0$ and $d > 0$.
- $<$ is a linear ordering.
- For $a, b \in \mathbb{Z}$, $a < b$ if and only if $[a/1] < [b/1]$.
- The usual algebraic laws (e.g., if $a < b$ then $a + c < b + c$, etc.) hold.

Density and Unboundedness of the Rational Ordering

Theorem

$(\mathbb{Q}, <)$ is a dense linearly ordered set and has no endpoints. In fact, for every $r \in \mathbb{Q}$ there exists $n \in \mathbb{N}$ such that $r < n$.

- $\mathbb{Q}$ is infinite: Since $\frac{a}{b} - 1 < \frac{a}{b} < \frac{a}{b} + 1$, $\mathbb{Q}$ has no endpoints.
- For the last statement:
  - If $r \leq 0$ we can taken $n = 1$.
  - If $r > 0$, we write $r = a/b$ where $a > 0, b > 0$, $a, b \in \mathbb{N}$ and take $n = a + 1$.
- It remains to show that $(\mathbb{Q}, <)$ is dense. Let r, s be rationals such that $r < s$ and assume that $r = a/b$ and $s = c/d$, where $b > 0$ and $d > 0$. Now we let

$$x = \frac{a \cdot d + b \cdot c}{2 \cdot b \cdot d},$$

i.e., $x = (r + s)/2$. Then $r < x < s$.

The Integer Part of a Rational Number

Lemma

Given a rational number r, there is a unique integer e such that $e \leq r < e + 1$. We call e the **integer part** of r, denoted $e = \lfloor r \rfloor$.

- Let $r = \frac{a}{b}$, $b > 0$.
  - Assume that $a \geq 0$, $1 \leq b$, so $a \leq a \cdot b$ and $r = \frac{a}{b} \leq a \in \mathbb{Z}$. It now follows that $S = \{x \in \mathbb{Z} : x \leq r\} \subseteq \mathbb{Z}$ has an upper bound $a \in \mathbb{Z}$.
  - If $a < 0$, then 0 is an upper bound on S.

  Therefore, S has a greatest element e. Then $e \leq r < e + 1$. Clearly, e is the unique integer with this property.

Expansion in Base p

- By the preceding lemma, $r = \lfloor r \rfloor + q$, where $\lfloor r \rfloor$ is an integer and $q \in \mathbb{Q}$, $0 \leq q < 1$. We concentrate on the expansion of q.
- Construct a sequence of digits $0, 1, \ldots, p-1$ by recursion as follows:
  - Find $a_1 \in \{0, \ldots, p-1\}$ such that $a_1/p \leq q < (a_1+1)/p$ (let $a_1 = \lfloor q \cdot p \rfloor$).
  - Then find $a_2 \in \{0, \ldots, p-1\}$ such that $a_1/p + a_2/p^2 \leq q < a_1/p + (a_2+1)/p^2$ (let $a_2 = \lfloor (q - a_1/p) \cdot p^2 \rfloor$).
  - In general, find $a_k \in \{0, \ldots, p-1\}$ such that

$$\frac{a_1}{p} + \cdots + \frac{a_k}{p^k} \leq q < \frac{a_1}{p} + \cdots + \frac{a_k + 1}{p^k}$$

(take $a_k = \left\lfloor \left(q - \frac{a_1}{p} - \cdots - \frac{a_{k-1}}{p^{k-1}} \right) \cdot p^k \right\rfloor$).

- We call the sequence $\langle a_i, i \in \mathbb{N} \rangle$ the **expansion of q in base p**.
- When $p = 10$, it is customary to write $q = 0.a_1 a_2 a_3 \ldots$.

Properties of Expansion in Base p

- It can be shown that:
  (a) There is no i such that $a_j = p - 1$, for all $j \geq i$.
  (b) There exist $n \in \mathbb{N}$ and $\ell > 0$ such that $a_{n+\ell} = a_n$, for all $n \geq n_0$ (the expansion is **eventually periodic**, with **period** ℓ).
- Moreover, if $q = \frac{a}{b}$, then we can find a period ℓ such that $\ell \leq |b|$.
- Conversely, each sequence $\langle a_n : n \in \mathbb{N} \rangle$ with the properties (a) and (b) is an expansion of some rational number q, with $0 \leq q < 1$.

Subsection 6

Operations and Structures

Binary Operations

- The functions $+, \cdot$, etc., are usually referred to as operations.
- Each of these operations assigns to a pair of objects (numbers, sets) a third object of the same kind (their sum, difference, union, etc.).
- The order may make a difference, e.g., $7 - 2$ and $2 - 7$ are different.

Definition (Binary Operation)

A **binary operation on** S is a function mapping a subset of S^2 into S.

- Nonletter symbols such as $+, \times, \cdot, \triangle$, etc., are often used to denote operations.
- The value (result) of the operation $*$ at (x, y) is then denoted $x * y$ rather than $*(x, y)$.
- There are also operations, such as square root or derivative, which are applied to one object rather than to a pair of objects.

More on Operations

Definition (Unary and Ternary Operation)

- A **unary operation on** S is a function mapping a subset of S into S.
- A **ternary operation on** S is a function on a subset of S^3 into S.

Definition (Closure Under an Operation)

Let f be a binary operation on S and $A \subseteq S$. A is **closed under the operation** f if for every $x, y \in A$ such that $f(x, y)$ is defined, $f(x, y) \in A$.

- Similar definitions apply in the case of unary or ternary operations.

Examples

(a) Let $+$ be the operation of addition on the set of all real numbers.
- Then $+$ is defined for all real numbers a and b.
- The set of all real numbers, as well as the set of all rational numbers and the set of all integers, are closed under $+$.
- The set of even natural numbers is closed under $+$, but the set of odd natural numbers is not.

(b) Let $\div$ be the operation of division on the set of all real numbers.
- $\div$ is not defined for (a, b) where $b = 0$.
- The set of all rational numbers is closed under $\div$, but the set of all integers is not.

(c) Let S be a set; define binary operations $\cup_S$ and $\cap_S$ on S ms follows:

(i) If $x, y \in S$ and $x \cup y \in S$, then $x \cup_S y = x \cup y$.

(ii) If $x, y \in S$ and $x \cap y \in S$, then $x \cap_S y = x \cap y$.

If we take $S = \mathcal{P}(A)$ for some A, $\cup_S$ and $\cap_S$ are defined for every pair $(x, y) \in S^2$.

Intuition Behind Structures

- A structure consists of a set A and of several relations and operations on A.
- For example, we consider structures with two binary relations and two operations, say a unary operation and a binary operation. Let
  - A be a set,
  - R_1 and R_2 be binary relations in A,
  - f be a unary operation and
  - g a binary operation on A.

  We make use of the five-tuple (A, R_1, R_2, f, g) to denote the structure.
- Example:
  (a) Every ordered set is a structure with one binary relation.
  (b) $(A, \cup_A, \cap_A, \subseteq_A)$ is a structure with two binary operations and one binary relation.
  (c) Let $\mathbb{R}$ be the set of all real numbers. $(\mathbb{R}, +, -, \times, \div)$ is a structure with four binary operations.

Requirement for Ordered n-tuples

- Recall that an ordered pair (a_0, a_1) has been defined as a set that uniquely determines its two coordinates a_0 and a_1, i.e., $(a_0, a_1) = (b_0, b_1)$ if and only if $a_0 = b_0$ and $a_1 = b_1$.
- We called a_0 the first coordinate of (a_0, a_1), and a_1 its second coordinate.
- In analogy, an n-tuple $(a_0, a_1, \ldots, a_{n-1})$ should be a set that uniquely determines its n coordinates $a_0, a_1, \ldots, a_{n-1}$, i.e., we want

$$(a_0, \ldots, a_{n-1}) = (b_0, \ldots, b_{n-1}) \\ \text{if and only if} \quad a_i = b_i, \text{ for all } i = 0, \ldots, n-1.$$

- We already introduced a notion that satisfies this condition: the sequence of length n, $\langle a_0, a_1, \ldots, a_{n-1} \rangle$
- The statement that $(a_0, \ldots, a_{n-1}) = (b_0, \ldots, b_{n-1})$ if and only if $a_i = b_i$, for all $i = 0, \ldots, n-1$, is just a reformulation of equality of functions.

Ordered n-tuples

- We therefore define n-**tuples** as sequences of length n.
- For each i, $0 \leq i < n$, a_i is called the $(i+1)$-**st coordinate** of $\langle a_0, a_1, \ldots, a_{n-1} \rangle$. So a_0 is the first coordinate, a_1 is the second coordinate, ..., a_{n-1} is the n-th coordinate.
- The only 0-tuple is the empty sequence $\langle\rangle = \emptyset$, having no coordinates.
- 1-tuples are sequences of the form $\langle a_0 \rangle$, i.e., sets of the form $\{(0, a_0)\}$; it usually causes no confusion if one does not distinguish between a 1-tuple $\langle a_0 \rangle$ and an element a_0.
- If $\langle A_i : 0 \leq i < n \rangle$ is a finite sequence of sets, then the n-fold cartesian product $\prod_{0 \leq i < n} A_i$, as defined before, is just the set of all n-tuples $a = \langle a_0, a_1, \ldots, a_{n-1} \rangle$ such that $a_0 \in A_0$, $a_1 \in A_1$, ..., $a_{n-1} \in A_{n-1}$.
- If $A_i = A$, for all i, $0 \leq i < n$, then $\prod_{0 \leq i < n} A_i = A^n$ is the set of all n-tuples with all coordinates from A.
- $A^0 = \{\langle\rangle\}$ and A^1 can be identified with A.

n-ary Relations and n-ary Operations

- An **n-ary relation R in A** is a subset of A^n. We write $R(a_0, a_1, \ldots, a_{n-1})$ instead of $(a_0, a_1, \ldots, a_{n-1}) \in R$.
- An **n-ary operation F on A** is a function on a subset of A^n into A. We write $F(a_0, a_1, \ldots, a_{n-1})$ instead of $F(\langle a_0, a_1, \ldots, a_{n-1}\rangle)$.
- If $\mathbf{P}(x_0, x_1, \ldots, x_{n-1})$ is a property with parameters $x_0, x_1, \ldots, x_{n-1}$, we write

$$\{\langle a_0, \ldots, a_{n-1}\rangle : a_0 \in A_0, \ldots, a_{n-1} \in A_{n-1} \text{ and } \mathbf{P}(a_0, \ldots, a_{n-1})\}$$

to denote the set

$$\{a \in \textstyle\prod_{0\leq i<n} A_i : \text{for some } a_0, \ldots, a_{n-1}, \\ a = \langle a_0, \ldots, a_{n-1}\rangle \text{ and } \mathbf{P}(a_0, \ldots, a_{n-1})\}.$$

Pairs and 2-tuples

- 1-ary relations need not be distinguished from subsets of A.
- 1-ary operations are identified with functions on a subset of A into A.
- 0-ary relations ($\emptyset$ and $\{\langle\rangle\}$) do not have much use.
- 0-ary operations are objects of the form $\{(\langle\rangle, a)\}$ where $a \in A$. We call them **constants** and in the sequel identify them with elements of A, i.e., we do not distinguish between $\{(\langle\rangle, a)\}$ and a.
- Note that the ordered pair $(a_0, a_1) = \{\{a_0\}, \{a_0, a_1\}\}$, is generally a different set from the just-defined 2-tuple $\langle a_0, a_1\rangle = \{(0, a_0), (1, a_1)\}$.
- Consequently, we have two definitions of cartesian product, $A_0 \times A_1$ and $\prod_{0\leq i<2} A_i$, two definitions of binary relations and operations, etc.
- However, there is a canonical one-to-one correspondence between ordered pairs and 2-tuples that preserves first and second coordinates, defined by $\delta((a_0, a_1)) = \langle a_0, a_1\rangle$.
- Thus, for almost all practical purposes, it makes no difference which definition one uses.

Types and Structures

- A **type** τ is an ordered pair $(\langle r_0, \ldots, r_{m-1}\rangle, \langle f_0, \ldots, f_{n-1}\rangle)$ of finite sequences of natural numbers, where $r_i > 0$ for all $0 \leq i \leq m-1$.
- A **structure of type** τ is a triple $\mathfrak{A} = (A, \langle R_0, \ldots, R_{m-1}\rangle, \langle F_0, \ldots, F_{n-1}\rangle)$, where R_i is an r_i-ary relation on A for each $i \leq m-1$ and F_j is an f_j-ary operation on A for each $j \leq n-1$. In addition, we require $F_j \neq \emptyset$ if $f_j = 0$. (If $f_j = 0$, F_j is a 0-ary operation on A, whence, following earlier remarks F_j is a constant, i.e., just a distinguished element of A.)
- Example: $\mathfrak{N} = (\mathbb{N}, \langle < \rangle, \langle 0, +, \cdot \rangle)$ is a structure of type $(\langle 2 \rangle, \langle 0, 2, 2 \rangle)$. It carries one binary relation, one constant, and two binary operations.
- Example: $\mathfrak{R} = (\mathbb{R}, \langle\rangle, \langle 0, 1, +, -, \times, \div \rangle)$ is a structure of type $(\langle\rangle, \langle 0, 0, 2, 2, 2, 2\rangle)$, etc.
- We often present the structure as a $(1 + m + n)$-tuple, for example $(\mathbb{N}, <, 0, +, \cdot)$, when it is understood which symbols represent relations and which operations.
- We call A the **universe** of the structure.

Isomorphism of Structures

Definition (Isomorphism of Structures)

An **isomorphism** between structures $\mathfrak{A} = (A, \langle R_0, \ldots, R_{m-1}\rangle, \langle F_0, \ldots, F_{n-1}\rangle)$ and $\mathfrak{A}' = (A', \langle R'_0, \ldots, R'_{m-1}\rangle, \langle F'_0, \ldots, F'_{n-1}\rangle)$ of the same type τ is a one-to-one mapping h on A onto A' such that

(a) $R_i(a_0, \ldots, a_{r_i-1})$ if and only if $R'_i(h(a_0), \ldots, h(a_{r_i-1}))$ holds, for all $a_0, \ldots, a_{r_i-1} \in A$ and $i \leq m-1$;

(b) $h(F_j(a_0, \ldots, a_{f_j-1})) = F'_j(h(a_0), \ldots, h(a_{f_j-1}))$ holds, for all $a_0, \ldots, a_{f_j-1} \in A$ and all $j \leq n-1$, provided that either side is defined.

- The structures are called **isomorphic** if there is an isomorphism between them.

Abstract Example of Isomorphism of Structures

- Example: Let (A, R_1, R_2, f, g) and (A', R_1', R_2', f', g') be structures with two binary relations and one unary and one binary operation. Then h is an isomorphism of (A, R_1, R_2, f, g) and (A', R_1', R_2', f', g') if all of the following requirements hold:
  (a) h is a one-to-one function on A onto A'.
  (b) For all $a, b \in A$, $a \ R_1 \ b$ if and only if $h(a) \ R_1' \ h(b)$.
  (c) For all $a, b \in A$, $a \ R_2 \ b$ if and only if $h(a) \ R_2' \ h(b)$.
  (d) For all $a \in A$, $f(a)$ is defined if and only if $f'(h(a))$ is defined and $h(f(a)) = f'(h(a))$.
  (e) For all $a, b \in A$, $g(a, b)$ is defined if and only if $g'(h(a), h(b))$ is defined and $h(g(a, b)) = g'(h(a), h(b))$.

A Concrete Example

- Example: Let A be the set of all real numbers, $\leq_A$ be the usual ordering of real numbers, and $+$ be the operation of addition on A. Let A' be the set of all positive real numbers, $\leq_{A'}$, be the usual ordering of positive real numbers, and $\times$ be the operation of multiplication on A'. We show that the structures $(A, \leq_A, +)$ and $(A', \leq_{A'}, \times)$ are isomorphic.
  Let h be the function $h(x) = e^x$, for all $x \in A$. We prove that h is an isomorphism of $(A, \leq_A, +)$ and $(A', \leq_{A'}, \times)$. We have to prove:
  (a) h is a one-to-one function on A onto A': Clearly h is a function, $\mathrm{dom} h = A$, and $\mathrm{ran} h = A'$. Moreover, if $x_1 \neq x_2$, then $e^{x_1} \neq e^{x_2}$.
  (b) Let $x_1, x_2 \in A$; then $x_1 \leq_A x_2$ if and only if $h(x_1) \leq_{A'} h(x_2)$: Since the function e^x is increasing, $x_1 \leq x_2$ if and only if $e^{x_1} \leq e^{x_2}$ is indeed true.
  (c) Let $x_1, x_2 \in A$; then $x_1 + x_2$ is defined if and only if $h(x_1) \times h(x_2)$ is defined and $h(x_1 + x_2) = h(x_1) \times h(x_2)$: First, notice that both $+$ on A and $\times$ on A' are defined for all ordered pairs. Now, $h(x_1 + x_2) = e^{x_1 + x_2} = e^{x_1} \times e^{x_2} = h(x_1) \times h(x_2)$.

Properties of Isomorphic Structures

- Isomorphic structures have exactly the same properties as far as the relations and operations on the structures are concerned.
- Example: Let (A, R) and (B, S) be isomorphic (R and S are binary relations). R is an ordering of A if and only if S is an ordering of B. Moreover, A has a least element in R if and only if B has a least element in S.

  Let h be an isomorphism of (A, R) and (B, S). Assume that R is an ordering of A. We prove that S is an ordering of B. Let $b_1, b_2, b_3 \in B$ and $b_1 \ S \ b_2, b_2 \ S \ b_3$. Since h is onto B, there exist $a_1, a_2, a_3 \in A$, such that $b_1 = h(a_1)$, $b_2 = h(a_2)$, and $b_3 = h(a_3)$. Because $a_1 \ R \ a_2$ holds if and only if $h(a_1) \ S \ h(a_2)$ holds, i.e., if and only if $b_1 \ S \ b_2$ holds, we conclude that $a_1 \ R \ a_2$ and similarly $a_2 \ R \ a_3$. But R is transitive in A, so $a_1 \ R \ a_3$. But then $h(a_1) \ S \ h(a_3)$, i.e., $b_1 \ S \ b_3$. Reflexivity and antisymmetry are proven similarly.

Example (Cont'd)

- In an analogous way, it can be shown that, if S is an ordering of B, then R is an ordering of A.
  We show antisymmetry. Suppose that $a_1, a_2 \in A$, such that $a_1 \ R \ a_2$ and $a_2 \ R \ a_1$. Then $h(a_1) \ S \ h(a_2)$ and $h(a_2) \ S \ h(a_1)$. But, S is an ordering in B, whence, by antisymmetry, $h(a_1) = h(a_2)$. Now, since h is one-to-one, we get $a_1 = a_2$, proving antisymmetry of R in A.
- Finally, let A have a least element. We claim that B has a least element. Let a be the least element of A, i.e., $a \ R \ x$ holds for all $x \in A$. If $y \in B$, then $y = h(x)$ for some $x \in A$. But, for this x, $a \ R \ x$ holds. Correspondingly, $h(a) \ S \ h(x)$ holds. Hence, $h(a) \ S \ y$ holds for all $y \in B$. Thus $h(a)$ is the least element of B.

Automorphisms of Structures

- An isomorphism between a structure $\mathfrak{A}$ and itself is called an **automorphism** of $\mathfrak{A}$.
- The identity mapping on the universe of $\mathfrak{A}$ is trivially an automorphism of $\mathfrak{A}$.
- The structure $(\mathbb{N}, <)$ has no other automorphisms.
- On the other hand, the structure $(\mathbb{Z}, <)$, where $\mathbb{Z}$ is the set of all integers, has nontrivial automorphisms. In fact, they are precisely the functions f_h, $h \in \mathbb{Z}$, where

$$f_h(x) = x + h, \text{ for all } x \in \mathbb{Z}.$$

Closed Subsets of Structures

- Consider a fixed structure $\mathfrak{A} = (A, \langle R_0, \ldots, R_{m-1}\rangle, \langle F_0, \ldots, F_{n-1}\rangle)$. A set $B \subseteq A$ is called **closed** if the result of applying any operation to elements of B is again in B, i.e., if, for all $j \leq n-1$ and all $a_0, \ldots, a_{f_j-1} \in B$, $F_j(a_0, \ldots, a_{f_j-1}) \in B$ provided that it is defined. In particular, all constants of $\mathfrak{A}$ belong to B.
- Let $C \subseteq A$. The closure of C, denoted $\overline{C}$, is the least closed set containing all elements of C:

$$\overline{C} = \bigcap \{B \subseteq A : C \subseteq B \text{ and } B \text{ is closed}\}.$$

- Notice that A is a closed set containing C, so the system whose intersection defines $\overline{C}$ is nonempty.
- It is trivial to check that $\overline{C}$ is closed; by definition, then, $\overline{C}$ is indeed the least closed set containing C.

Examples

(a) Every set $B \subseteq A$ is closed if $\mathfrak{A}$ has no operations.

(b) Let $\mathbb{R}$ be the set of all real numbers and let $C = \{0\}$. The set of all natural numbers $\mathbb{N}$ is the closure of C in the structure $(\mathbb{R}, f)$ where f is the successor function defined by

$$f(x) = x + 1, \text{ for all real numbers } x.$$

(c) Let $C = \{0, 1\}$; the set of all integers $\mathbb{Z}$ is the closure of C in the structure $(\mathbb{R}, +, -)$ or in $(\mathbb{R}, +, -, \times)$.

(d) The set of all rationals $\mathbb{Q}$ is the closure of $\emptyset$ in $(\mathbb{R}, 0, 1, +, -, \times, \div)$.

- The notion of closure is important in algebra, logic, and other areas of mathematics.
- We now turn on how to construct the closure of a set "from below".

Construction of a Closure

Theorem (Construction of Closure)

Let $\mathfrak{A} = (A, \langle R_0, \ldots, R_{m-1}\rangle, \langle F_0, \ldots, F_{n-1}\rangle)$ be a structure and let $C \subseteq A$. If the sequence $\langle C_i : i \in \mathbb{N}\rangle$ is defined recursively by

$$\begin{aligned} C_0 &= C; \\ C_{i+1} &= C_i \cup F_0[C_i^{f_0}] \cup \cdots \cup F_{n-1}[C_i^{f_{n-1}}], \end{aligned}$$

then $\overline{C} = \bigcup_{i=0}^{\infty} C_i$;

- Of course, the notation $A_0 \cup \cdots \cup A_{n-1}$ is a shorthand for $\bigcup_{0 \le i < n} A_i$.
- Observe that $C_i \subseteq C_{i+1}$, for all i, so the sequence $\langle C_i : i \in \mathbb{N}\rangle$ is nondecreasing.

Proof of the Closure Theorem

- Let $\widetilde{C} = \bigcup_{i=0}^{\infty} C_i$.
  - We first prove that $\overline{C} \subseteq \widetilde{C}$:
    We must show that $\widetilde{C}$ is closed, because $\widetilde{C} \supseteq C_0 = C$. Let $j < n$ and $a_0, \ldots, a_{f_j - 1} \in \widetilde{C}$. From the definition of union we get that each a_r, $0 \leq r < f_j$, belongs to some C_i; let i_r be the least $i \in \mathbb{N}$ such that $a_r \in C_i$. By an easy inductive argument, the range of the finite sequence $\langle i_r : 0 \leq r < f_j - 1 \rangle$ of natural numbers contains a greatest element $\bar{\imath}$. Since $\langle C_i : i \in \mathbb{N} \rangle$ is nondecreasing, we have $a_r \in C_{i_r} \subseteq C_{\bar{\imath}}$, for all $0 \leq r < f_j - 1$. We conclude that, if $F_j(a_0, \ldots, a_{f_j - 1})$ is defined, then it belongs to $F_j[C_{\bar{\imath}}^{f_j}] \subseteq C_{\bar{\imath}+1} \subseteq \widetilde{C}$, so $\widetilde{C}$ is closed.
  - We prove, next, the reverse inclusion $\widetilde{C} \subseteq \overline{C}$:
    Clearly, $C_0 = C \subseteq \overline{C}$. If $C_i \subseteq \overline{C}$, then $F_j[C_i^{f_j}] \subseteq \overline{C}$, for each $j \leq n - 1$, because $\overline{C}$ is closed, and, therefore, also $C_{i+1} \subseteq \overline{C}$. We conclude using the Induction Principle that $C_i \subseteq \overline{C}$, for all $i \in \mathbb{N}$ and, finally, $\widetilde{C} = \bigcup_{i=0}^{\infty} C_i \subseteq \overline{C}$, as required.

Proving Properties of Closures

- The final theorem of this set is used to prove that all elements of a closure have some property **P**.

Theorem

Let $\mathbf{P}(x)$ be a property. Assume that

(a) $\mathbf{P}(a)$ holds for all $a \in C$.

(b) For each $j < n-1$, if $\mathbf{P}(a_0), \ldots, \mathbf{P}(a_{f_j-1})$ hold and $F_j(a_0, \ldots, a_{f_j-1})$ is defined, then $\mathbf{P}(F_j(a_0, \ldots, a_{f_j-1}))$ holds.

Then $\mathbf{P}(x)$ holds for all $x \in \overline{C}$.

- Hypotheses (a) and (b) ensure that $B = \{x \in A : \mathbf{P}(x)\}$ is closed and $C \subseteq B$. It follows that $\overline{C} \subseteq B$.
- The Induction Principle is a special case of the Theorem: Consider the structure $(\mathbb{N}, S)$ (S the successor operation) and $C = \{0\}$.