Introduction to Set Theory

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 400

Subsection 1

Well-Ordered Sets

Extending Counting Beyond the Natural Numbers

- When we introduced natural numbers, we were motivated by the need to formalize the process of "counting":

  The natural numbers start with 0 and are generated by successively increasing the number by one unit: $0, 1, 2, 3, \ldots$ and so on.
- We defined "successor" by $S(x) = x \cup \{x\}$ and introduced natural numbers as elements of the smallest set containing 0 and closed under S.
- We want to be able to continue counting beyond natural numbers.
- The idea is that we can imagine an infinite number ω that comes "after" all natural numbers and then continue the counting process into the transfinite: $\omega, \omega + 1, (\omega + 1) + 1$, and so on.
- We formalize the process of transfinite counting, and introduce ordinal numbers as a generalization of natural numbers
- The theorems on induction and recursion are generalized to theorems on transfinite induction and transfinite recursion.

Transfinite Ordinal Generation

- Recall that each natural number is identified with the set of all smaller natural numbers: $n = \{m \in \mathbb{N} : m < n\}$.
- By analogy, we let ω, the least transfinite number, to be the set $\mathbb{N}$ of all natural numbers: $\omega = \mathbb{N} = \{0, 1, 2, \ldots\}$.
- It is easy to continue the process after this "limit" step is made. The operation of successor can be used to produce numbers following ω:

$$\begin{array}{rcl} S(\omega) & = & \omega \cup \{\omega\} = \{0, 1, 2, \ldots, \omega\}, \\ S(S(\omega)) & = & S(\omega) \cup \{S(\omega)\} = \{0, 1, 2, \ldots, \omega, S(\omega)\}, \text{ etc.} \end{array}$$

- We use the suggestive notation

$$S(\omega) = \omega + 1, S(S(\omega)) = (\omega + 1) + 1 = \omega + 2, \text{ etc.}$$

- In this fashion, we can generate greater and greater "numbers": ω, $\omega + 1$, $\omega + 2$, $\ldots$, $\omega + n$, $\ldots$, for all $n \in \mathbb{N}$.
- A number following all $\omega + n$ can again be conceived of as a set of all smaller numbers: $\omega \cdot 2 = \omega + \omega = \{0, 1, 2, \ldots, \omega, \omega + 1, \omega + 2, \ldots\}$.

Well-Ordered Sets

- We can introduce still greater numbers:

$$\omega \cdot 2 + 1 = \omega + \omega + 1 = \{0, 1, 2, \ldots, \omega, \omega + 1, \omega + 2, \ldots, \omega + \omega\},$$
$$\omega \cdot 3 = \omega + \omega + \omega = \{0, 1, 2, \ldots, \omega, \omega + 1, \omega + 2, \ldots, \omega + \omega, \omega + \omega + 1, \ldots\},$$
$$\omega \cdot \omega = \{0, 1, 2, \ldots, \omega, \omega + 1, \ldots, \omega \cdot 2, \omega \cdot 2 + 1, \ldots, \omega \cdot 3, \ldots, \omega \cdot 4, \ldots\}.$$

- The sets we generate are linearly ordered by $\in$, and every nonempty subset has a least element.

Definition (Well-Ordering)

A set W is **well-ordered** by the relation $<$ if

(a) $(W, <)$ is a linearly ordered set.

(b) Every nonempty subset of W has a least element.

- The sets above are all examples of sets well-ordered by $\in$.
- We will show that all well-orderings can be so represented.

Initial Segments of Well-Ordered Sets

- Let $(L, <)$ be a linearly ordered set. A set $S \subseteq L$ is called an **initial segment** of L if S is a proper subset of L (i.e., $S \neq L$) and if for every $a \in S$, all $x < a$ are also elements of S.
- Example: Both the set of all negative reals and the set of all nonpositive reals are initial segments of the set of all real numbers.

Lemma

If $(W, <)$ is a well-ordered set and if S is an initial segment of $(W, <)$, then, there exists $a \in W$, such that $S = \{x \in W : x < a\}$.

- Let $X = W - S$. As $S \neq W$, $X \neq \emptyset$. So X has a least element, say a, in the well-ordering $<$. If $x < a$, then x cannot belong to X, as a is its least member, so x belongs to S. If $x \geq a$, then x cannot be in S because otherwise a would also be in S as S is an initial segment. Thus, $S = \{x \in W : x < a\}$.
- If a is an element of a well-ordered set $(W, <)$, we call the set $W[a] = \{x \in W : x < a\}$ the **initial segment of W given by a**.

Increasing Functions

- A function f on a linearly ordered set $(L, <)$ into L is **increasing** if $x_1 < x_2$ implies $f(x_1) < f(x_2)$.
- An increasing function is one-to-one, and is an isomorphism of $(L, <)$ and $(\mathrm{ran} f, <)$.

Lemma

If $(W, <)$ is a well-ordered set and if $f : W \to W$ is an increasing function, then $f(x) \geq x$, for all $x \in W$.

- If the set $X = \{x \in W : f(x) < x\}$ is nonempty, it has a least element a. But, then, $f(a) < a$, and $f(f(a)) < f(a)$ because f is increasing. This means that $f(a) \in X$, which is a contradiction because a is least in X.

Isomorphisms Between Well-Ordered Sets

Corollary (Isomorphisms Between Well-Ordered Sets)

(a) No well-ordered set is isomorphic to an initial segment of itself.

(b) Each well-ordered set has only one automorphism, the identity.

(c) If W_1 and W_2 are isomorphic well-ordered sets, then the isomorphism between W_1 and W_2 is unique.

(a) Assume that f is an isomorphism between W and $W[a]$ for some $a \in W$. Then $f(a) \in W[a]$ and, therefore, $f(a) < a$, contrary to the lemma, as f is an increasing function.

(b) Let f be an automorphism of W. Both f and f^{-1} are increasing functions. So, for all $x \in W$, $f(x) \geq x$ and $f^{-1}(x) \geq x$, therefore, $x \geq f(x)$. It follows that $f(x) = x$, for all $x \in W$.

(c) Let f and g be isomorphisms between W_1 and W_2. Then $f \circ g^{-1}$ is an automorphism of W_1 and hence is the identity map. It follows that $f = g$.

Comparison of Well-Ordered Sets By "Length"

Theorem

If $(W_1, <_1)$ and $(W_2, <_2)$ are well-ordered sets, then exactly one of the following holds:

(a) Either W_1 and W_2 are isomorphic, or

(b) W_1 is isomorphic to an initial segment of W_2, or

(c) W_2 is isomorphic to an initial segment of W_1.

In each case, the isomorphism is unique.

- Let W_1 and W_2 be well-ordered sets.
  - The three cases (a), (b), and (c) are mutually exclusive: For example, if W_1 were isomorphic to $W_2[a_2]$ for some $a_2 \in W_2$ and at the same time W_2 were isomorphic to $W_1[a_1]$ for some $a_1 \in W_1$, then the composition of the two isomorphisms would be an isomorphism of a well-ordered set onto its own initial segment.
  - Uniqueness of the isomorphism in each case follows from the corollary.
  - We must show that one of the three cases (a), (b) and (c) always holds.

Continuing the Proof of the Comparison Theorem

- We define a set of pairs $f \subseteq W_1 \times W_2$ and show that either f or f^{-1} is an isomorphism attesting to (a), (b) or (c). Let
$$f = \{(x, y) \in W_1 \times W_2 : W_1[x] \text{ is isomorphic to } W_2[y]\}.$$
  - First, by the corollary, f is a one-to-one function: If $W_1[x]$ is isomorphic both to $W_2[y]$ and to $W_2[y']$, then $y = y'$; otherwise $W_2[y]$ would be an initial segment of $W_2[y']$ (or vice versa) while they are isomorphic, and that is impossible. Hence $(x, y) \in f$ and $(x, y') \in f$ imply $y = y'$. A similar argument shows that $(x, y) \in f$ and $(x', y) \in f$ imply $x = x'$.
  - Second, $x < x'$ implies $f(x) < f(x')$: If h is the isomorphism between $W_1[x']$ and $W_2[f(x')]$, then the restriction $h \restriction W_1[x]$ is an isomorphism between $W_1[x]$ and $W_2[h(x)]$. So $f(x) = h(x)$ and $f(x) < f(x')$.

Hence f is an isomorphism between its domain, a subset of W_1, and its range, a subset of W_2.

Finishing the Proof of the Comparison Theorem

- We showed $f = \{(x,y) \in W_1 \times W_2 : W_1[x] \text{ is isomorphic to } W_2[y]\}$ is an isomorphism between its domain and its range.
    - If $\mathrm{dom} f = W_1$ and $\mathrm{ran} f = W_2$, then W_1 is isomorphic to W_2.
    - We show now that if the domain of f is not all of W_1 then it is its initial segment, and the range of f is all of W_2. (This suffices to complete the proof as the remaining case is obtained by interchanging the roles of W_1 and W_2.) So assume that $\mathrm{dom} f \neq W_1$.
        - We note that the set $S = \mathrm{dom} f$ is an initial segment of W_1: If $x \in S$ and $z < x$, let h be the isomorphism between $W_1[x]$ and $W_2[f(x)]$; then $h \restriction W_1[z]$ is an isomorphism between $W_1[z]$ and $W_2[h(z)]$, so $z \in S$.
        - To show that the set $T = \mathrm{ran} f = W_2$, we assume otherwise and, by a similar argument as above, show that T is an initial segment of W_2. But, then, $\mathrm{dom} f = W_1[a]$, for some $a \in W_1$, and $\mathrm{ran} f = W_2[b]$, for some $b \in W_2$. In other words, f is an isomorphism between $W_1[a]$ and $W_2[b]$. This means, by the definition of f, that $(a,b) \in f$. So $a \in \mathrm{dom} f = W_1[a]$, i.e., $a < a$, a contradiction.
- We say that W_1 has **smaller order type** than W_2 if W_1 is isomorphic to $W_2[a]$ for some $a \in W_2$.

Subsection 2

Ordinal Numbers

Ordinals as Order Types of Well-Ordered Sets

- Natural numbers were used to represent both the cardinality and the order type of finite sets. They were also used to prove theorems on induction and recursion.
- We now generalize this definition by introducing ordinal numbers.
  - Each ordinal is well-ordered by the $\in$ relation.
  - The collection of all ordinal numbers (which is not a set) is itself well-ordered by $\in$, and contains the natural numbers as an initial segment.
  - Ordinal numbers are representatives for all well-ordered sets, i.e., every well-ordered set is isomorphic to an ordinal number. Thus ordinal numbers can be viewed as order types of well-ordered sets.

Transitive Sets and Ordinal Numbers

Definition (Transitive Set)

A set T is **transitive** if every element of T is a subset of T.

- In other words, a transitive set has the property that $u \in v \in T$ implies $u \in T$.

Definition (Ordinal Number)

A set α is an **ordinal number** if

(a) α is transitive.

(b) α is well-ordered by $\in$.

- Lowercase Greek letters are used for ordinal numbers.
- Ordinal numbers are often simply called **ordinals**.

The Ordinal Number ω

- For every natural number m, if $k \in \ell \in m$ (i.e., $k < \ell < m$), then $k \in m$. Hence, every natural number is a transitive set.
- Also, every natural number is well-ordered by the $\in$ relation (because every $n \in \mathbb{N}$ is a subset of $\mathbb{N}$ and $\mathbb{N}$ is well-ordered by $\in$).

Theorem

Every natural number is an ordinal.

- The set $\mathbb{N}$ of all natural numbers is easily seen to be transitive, and is also well-ordered by $\in$. Thus $\mathbb{N}$ is an ordinal number.

Definition (ω)

$\omega = \mathbb{N}$.

Successor and Limit Ordinals, Ordering of Ordinals

Lemma

If α is an ordinal number, then $S(\alpha)$ is also an ordinal number.

- $S(\alpha) = \alpha \cup \{\alpha\}$ is a transitive set. Moreover, $\alpha \cup \{\alpha\}$ is well-ordered by $\in$, α being its greatest element, and $\alpha \subset \alpha \cup \{\alpha\}$ being the initial segment given by α. So $S(\alpha)$ is an ordinal number.
- We denote the successor of α by $\alpha + 1$:

$$\alpha + 1 := S(\alpha) = \alpha \cup \{\alpha\}.$$

- An ordinal number α is called a **successor ordinal** if $\alpha = \beta + 1$ for some β. Otherwise, it is called a **limit ordinal**.
- For all ordinals α and β, we define $\alpha < \beta$ if and only if $\alpha \in \beta$, thus extending the definition of the ordering of natural numbers.

The Ordering of the Ordinal Numbers I

Lemma

If α is an ordinal number, then $\alpha \notin \alpha$.

- Although $X \in X$ is not forbidden by the axioms, the sets which arise in mathematical practice do not have this peculiar property.
- If $\alpha \in \alpha$, then the linearly ordered set $(\alpha, \in_\alpha)$ has an element $x = \alpha$, such that $x \in x$, contrary to asymmetry of $\in_\alpha$.

Lemma

Every element of an ordinal number is an ordinal number.

- Let α be an ordinal and let $x \in \alpha$.
  - x is transitive: Let u and v be such that $u \in v \in x$. Since α is transitive and $x \in \alpha$, we have $v \in \alpha$ and therefore, also $u \in \alpha$. Thus, u, v and x are all elements of α and $u \in v \in x$. Since $\in_\alpha$ linearly orders a, we conclude that $u \in x$.
  - $\in$ is a well-ordering of x: By transitivity of α, we have $x \subseteq \alpha$. So, the relation $\in_x$ is a restriction of $\in_\alpha$. Since $\in_\alpha$ is a well-ordering, so is $\in_x$.

The Ordering of the Ordinal Numbers II

Lemma

If α and β are ordinal numbers such that $\alpha \subset \beta$, then $\alpha \in \beta$.

- Let $\alpha \subset \beta$. Then $\beta - \alpha$ is a nonempty subset of β. Thus, it has a least element γ in the ordering $\in_\beta$.

  Notice that $\gamma \subseteq \alpha$: If not, then any $\delta \in \gamma - \alpha$ would be an element of $\beta - \alpha$ smaller than γ (by transitivity of β).

  It suffices to show that $\alpha \subseteq \gamma$ (and, hence, $\alpha = \gamma \in \beta$): Let $\delta \in \alpha$. We show $\delta \in \gamma$. If not, $\gamma \in \delta$ or $\gamma = \delta$ (both γ and δ belong to β, which is linearly ordered by $\in$). But this implies that $\gamma \in \alpha$, since α is transitive. That contradicts the choice of $\gamma \in \beta - \alpha$.

The Ordering of the Ordinal Numbers is a Well-Ordering

Theorem

Let α, β and γ be ordinal numbers.

(a) If $\alpha < \beta$ and $\beta < \gamma$, then $\alpha < \gamma$.

(b) $\alpha < \beta$ and $\beta < \alpha$ cannot both hold.

(c) Either $\alpha < \beta$ or $\alpha = \beta$ or $\beta < \alpha$ holds.

(d) Every nonempty set of ordinal numbers has a $<$-least element. Consequently, every set of ordinal numbers is well-ordered by $<$.

(e) For every set of ordinal numbers X, there is an ordinal number $\alpha \notin X$ (i.e., "the set of all ordinal numbers" does not exist).

(a) If $\alpha < \beta$ and $\beta < \gamma$, then $\alpha < \gamma$ because γ is transitive.

(b) Assume that $\alpha < \beta$ and $\beta < \alpha$. By transitivity, $\alpha \in \alpha$, contradicting a preceding lemma.

Proof (Cont'd)

(c) If α and β are ordinals, $\alpha \cap \beta$ is also an ordinal (it is transitive and well-ordered) and $\alpha \cap \beta \subseteq \alpha$ and $\alpha \cap \beta \subseteq \beta$.
- If $\alpha \cap \beta = \alpha$, then $\alpha \subseteq \beta$ whence, by lemma, $\alpha \in \beta$ or $\alpha = \beta$.
- Similarly, $\alpha \cap \beta = \beta$ implies $\beta \in \alpha$ or $\beta = \alpha$.
- Finally $\alpha \cap \beta \subset \alpha$ and $\alpha \cap \beta \subset \beta$ is impossible: it implies $\alpha \cap \beta \in \alpha \cap \beta$, contradicting a preceding lemma.

(d) Let A be a nonempty set of ordinals. For $\alpha \in A$, consider $\alpha \cap A$.
- If $\alpha \cap A = \emptyset$, α is the least element of A.
- If $\alpha \cap A \neq \emptyset$, $\alpha \cap A \subseteq \alpha$ has a least element β in the ordering $\in_\alpha$. Then β is the least element of A in the ordering $<$.

(e) Let X be a set of ordinal numbers. Since all elements of X are transitive sets, $\bigcup X$ is also a transitive set. It follows from part (d) that $\in$ well-orders $\bigcup X$. Consequently, $\bigcup X$ is an ordinal number. Let $\alpha = S(\bigcup X)$. α is an ordinal number and $\alpha \neq X$. (Otherwise, we get $\alpha \subseteq \bigcup X$ and, by a preceding lemma, either $\alpha = \bigcup X$ or $\alpha \in \bigcup X$, and, in both cases, $\alpha \in S(\bigcup X) = \alpha$, contradicting the lemma.)

Every Set of Ordinals has a Supremum

- The ordinal number $\bigcup X$ used in the proof of Part (e) is called the **supremum** of X and is denoted $\sup X$.
- This is justified by observing that $\bigcup X$ is the least ordinal greater than or equal to all elements of X:
  (a) If $\alpha \in X$, then $\alpha \subseteq \bigcup X$, so, $\alpha \in \bigcup X$.
  (b) If $\alpha \leq \gamma$, for all $\alpha \in X$, then $\alpha \subseteq \gamma$, for all $\alpha \in X$, and so $\bigcup X \subseteq \gamma$, i.e., $\bigcup X \leq \gamma$.
- If the set X has a greatest element β in the ordering $<$, then $\sup X = \beta$. Otherwise, $\sup X > \gamma$, for all $\gamma \in X$ (and it is the least such ordinal). Therefore, every set of ordinals has a supremum in $<$.

Natural Numbers are Exactly the Finite Ordinals

- Ordinals are indeed a generalization of the natural numbers:

Theorem

The natural numbers are exactly the finite ordinal numbers.

- We already know that every natural number is an ordinal, and of course, every natural number is a finite set. So we only have to prove that all ordinals that are not natural numbers are infinite sets. If α is an ordinal and $\alpha \notin \mathbb{N}$, then, by a preceding theorem, it must be the case that $\alpha \geq \omega$ (because $\alpha \not< \omega$), so $\alpha \supseteq \omega$ because α is transitive. So α has an infinite subset and hence is infinite.
- Every ordinal is a well-ordered set, under the well-ordering $\in$.
- If α and β are distinct ordinals, then they are not isomorphic, as well-ordered sets because one is an initial segment of the other.
- Each ordinal number α bas the property that

$$\alpha = \{\beta : \beta \text{ is an ordinal and } \beta < \alpha\}.$$

Subsection 3

The Axiom of Replacement

Representation of Well-Ordered Sets by Ordinals

Theorem

Every well-ordered set is isomorphic to a unique ordinal number.

- The "proof" has a deficiency: it uses an assumption which does not follow from the axioms introduced so far.
- Let $(W, <)$ be a well-ordered set. Let A be the set of all those $a \in W$ for which $W[a]$ is isomorphic to some ordinal number. As no two distinct ordinals can be isomorphic (one is an initial segment of the other), this ordinal number is uniquely determined, and we denote it by α_a. Suppose that there exists a set S such that $S = \{\alpha_a : a \in A\}$. The set S is well-ordered by $\in$ as it is a set of ordinals. It is also transitive: If $\gamma \in \alpha_a \in S$, let φ be the isomorphism between $W[a]$ and α_a and let $c = \varphi^{-1}(\gamma)$. It is easy to see that $\varphi \upharpoonright c$ is an isomorphism between $W[c]$ and γ and so $\gamma \in S$. Therefore, S is an ordinal number, $S = \alpha$.

Representation by Ordinals II

- A similar argument shows that $a \in A$, $b < a$ imply $b \in A$: let φ be the isomorphism of $W[a]$ and α_a. Then $\varphi \restriction W[b]$ is an isomorphism of $W[b]$ and an initial segment I of α_a. By a preceding lemma, there exists $\beta < \alpha_a$, such that $I = \{\gamma \in \alpha_a : \gamma < \beta\}$, i.e., $\beta = \alpha_b$. This shows that $b \in A$ and $\alpha_b < \alpha_a$. We conclude, based on the same lemma, that either $A = W$ or $A = W[c]$, for some $c \in W$.

  We now define a function $f : A \to S = \alpha$ by $f(a) = \alpha_a$ From the definition of S and the fact that $b < a$ implies $\alpha_b < \alpha_a$ it is obvious that f is an isomorphism of $(A, <)$ and α. If $A = W[c]$, we would thus have $c \in A$, a contradiction. Therefore $A = W$, and f is an isomorphism of $(W, <)$ and the ordinal α.
- This would complete the proof if we were justified to make the assumption that the set S exists.

Example Illustrating Need for New Axiom

- To construct a sequence

$$\langle \emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}, \ldots \rangle$$

 we might define

$$\begin{aligned} a_0 &= \emptyset \\ a_{n+1} &= \{a_n\}, \text{ for all } n \in \mathbb{N} \end{aligned}$$

 following the general pattern of recursive definitions.
- The difficulty here is that to apply the Recursion Theorem we need a set A, given in advance, such that $g : \mathbb{N} \times A \to A$, defined by $g(n, x) = \{x\}$, can be used to compute the $(n+1)$-st term of the sequence from its n-th term.
- It is not obvious how to prove from our axioms that any such set A exists. It seems as if the definition of A itself required recursion.

Another Example Illustrating Need for New Axiom

- In Chapter 3, we have postulated existence of ω.
- From it, the sets $\omega+1=\omega\cup\{\omega\}$, $\omega+2=(\omega+1)\cup\{\omega+1\}$, etc., can easily be obtained by repeated use of operations union and unordered pair.
- We "defined" $\omega+\omega$ as the union of ω and the set of all $\omega+n$, for all $n\in\omega$, and passed over the question of existence of this set.
- Although it does not seem to be more questionable than the existence of ω, the existence of $\omega+\omega$ cannot be proved from the axioms we accepted so far.
- We know that, to each $n\in\omega$, there corresponds a unique set $\omega+n$; but, as yet, we do not have any axiom that would allow us to collect all these $\omega+n$ into one set.

The Axiom Schema of Replacement

The Axiom Schema of Replacement

Let $\mathbf{P}(x, y)$ be a property such that, for every x, there is a unique y for which $\mathbf{P}(x, y)$ holds. For every set A, there is a set B such that, for every $x \in A$, there is $y \in B$ for which $\mathbf{P}(x, y)$ holds.

- Let $\mathbf{F}$ be the operation defined by the property $\mathbf{P}$, i.e., let $\mathbf{F}(x)$ denote the unique y for which $\mathbf{P}(x, y)$. The corresponding Axiom of Replacement can then be stated as follows:

  > For every set A, there is a set B, such that for all $x \in A$, $\mathbf{F}(x) \in B$.

  Of course, B may also contain elements not of the form $\mathbf{F}(x)$ for any $x \in A$. An application of the Axiom Schema of Comprehension shows that $\{y \in B : y = \mathbf{F}(x), \text{ for some } x \in A\} = \{y \in B : \mathbf{P}(x, y) \text{ holds for some } x \in A\} = \{y : \mathbf{P}(x, y) \text{ holds for some } x \in A\}$ exists. We call this set the **image of A by $\mathbf{F}$**, written $\{\mathbf{F}(x) : x \in A\}$ or simply $\mathbf{F}[A]$.

More on The Axiom Schema of Replacement

- The Axiom Schema of Comprehension allows us to go through elements of a given set A, check for each $x \in A$ whether or not it has the property $\mathbf{P}(x)$, and collect those x which do into a set. In an entirely analogous way, the Axiom Schema of Replacement allows us to go through elements of A, take for each $x \in A$ the corresponding unique y having the property $\mathbf{P}(x, y)$, and collect all such y into a set. It is intuitively obvious that the set $\mathbf{F}[A]$ is "no larger than" the set A.
- Let $\mathbf{F}$ be the operation defined by $\mathbf{P}$. The Axiom of Replacement implies that the operation $\mathbf{F}$ on elements of a given set A can be represented, "replaced," by a function, i.e., a set of ordered pairs.

  > For every set A, there is a function f such that $\mathrm{dom} f = A$ and $f(x) = \mathbf{F}(x)$, for all $x \in A$.

  We simply let $f = \{(x, y) \in A \times B : \mathbf{P}(x, y)\}$, where B is the set provided by the Axiom of Replacement. We use notation $F \upharpoonright A$ for this uniquely determined function f and note that $\mathrm{ran}(F \upharpoonright A) = \mathbf{F}[A]$.

Completing the Proof of the Representation Theorem

- We have concluded earlier that in order to prove the theorem, we only have to guarantee the existence of the set $S = \{\alpha_a : a \in W\}$, where for each $a \in W$, α_a is the unique ordinal number isomorphic to $W[a]$.
- Let $\mathbf{P}(x, y)$ be the property:

  Either $x \in W$ and y is the unique ordinal isomorphic to $W[x]$, or $x \notin W$ and $y = \emptyset$.

  Applying the Axiom of Replacement with this $\mathbf{P}(x, y)$, we conclude that for $A = W$, there exists a set B such that for all $a \in W$ there is $\alpha \in B$ for which $\mathbf{P}(a, \alpha)$ holds. Then we let

  $$S = \{\alpha \in B : \mathbf{P}(a, \alpha) \text{ holds for some } a \in W\} = \mathbf{F}[W],$$

  where $\mathbf{F}$ is the operation defined by $\mathbf{P}$.

Order Types

Definition (Order Type)

If W is a well-ordered set, then the **order type** of W is the unique ordinal number isomorphic to W.

- To accommodate the examples mentioned above, we need a more general Recursion Theorem than the one proved earlier:

The Recursion Theorem

Let $\mathbf{G}$ be an operation. For any set a there is a unique infinite sequence $\langle a_n : n \in \mathbb{N} \rangle$ such that

(a) $a_0 = a$.

(b) $a_{n+1} = \mathbf{G}(a_n, n)$, for all $n \in \mathbb{N}$.

- With this theorem, the existence of the sequence $\langle \emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \ldots \rangle$ and of $\omega + \omega$ follows .
- We prove this Recursion Theorem, as well as the more general Transfinite Recursion Theorem, in the next section.

Subsection 4

Transfinite Induction and Recursion

The Transfinite Induction Principle

- We show how the Induction Principle and the Recursion Theorem generalize to ordinal numbers.

The Transfinite Induction Principle

Let $\mathbf{P}(x)$ be a property (possibly with parameters). Assume that, for all ordinal numbers α,

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

Then $\mathbf{P}(\alpha)$ holds for all ordinals α.

- Suppose that some ordinal number γ fails to have property $\mathbf{P}$. Let S be the set of all ordinal numbers $\beta \leq \gamma$ that do not have property $\mathbf{P}$. The set S has a least element α. Since every $\beta < \alpha$ has property $\mathbf{P}$, it follows, by hypothesis, that $\mathbf{P}(\alpha)$ holds, a contradiction.

Second Version of the Transfinite Induction Principle

- The Transfinite Induction Principle has a form which resembles more closely the usual formulation of the Induction Principle for $\mathbb{N}$.

Second Version of the Transfinite Induction Principle

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

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

(b) $\mathbf{P}(\alpha)$ implies $\mathbf{P}(\alpha+1)$ for all ordinals α.

(c) For all limit ordinals $\alpha \neq 0$, if $\mathbf{P}(\beta)$ holds for all $\beta < \alpha$, then $\mathbf{P}(\alpha)$ holds.

Then $\mathbf{P}(\alpha)$ holds for all ordinals α.

- It suffices to show that the assumptions (a), (b) and (c) imply the hypothesis of the Original Version. So, let α be an ordinal such that $\mathbf{P}(\beta)$ for all $\beta < \alpha$.
  - If $\alpha = 0$, then $\mathbf{P}(\alpha)$ holds by (a).
  - If $\alpha = \beta + 1$ is a successor, $\mathbf{P}(\beta)$ holds, so $\mathbf{P}(\alpha)$ holds by (b).
  - If $\alpha \neq 0$ is limit, we have $\mathbf{P}(\alpha)$ by (c).

A Transfinite Recursion Theorem

- We generalize the Recursion Theorem: Functions whose domain is an ordinal α are called **transfinite sequences of length** α.

Theorem

Let Ω be an ordinal number, A a set, and $S = \bigcup_{\alpha<\Omega} A^\alpha$ the set of all transfinite sequences of elements of A of length less than Ω. Let $g : S \to A$ be a function. Then there exists a unique function $f : \Omega \to A$, such that

$$f(\alpha) = g(f \upharpoonright \alpha), \text{ for all } \alpha < \Omega.$$

- The proof is based on a more general Transfinite Recursion Theorem.
- If ϑ is an ordinal and f is a transfinite sequence of length ϑ, we use the notation $f = \langle a_\alpha : \alpha < \vartheta \rangle$.
- The theorem states that, if g is a function on the set of all transfinite sequences of elements of A of length less than Ω with values in A, then there is a transfinite sequence $\langle a_\alpha : \alpha < \Omega \rangle$ such that for all $\alpha < \Omega$, $a_\alpha = g(\langle a_\xi : \xi < \alpha \rangle)$.

The Transfinite Recursion Theorem

- For a given operation $\mathbf{G}$, t is a **computation of length α based on $\mathbf{G}$** if t is a function, $\mathrm{dom}t = \alpha + 1$ and, for all $\beta \leq \alpha$, $t(\beta) = \mathbf{G}(t \restriction \beta)$.

The Transfinite Recursion Theorem

Let $\mathbf{G}$ be an operation. Then, the property $\mathbf{P}(x, y)$

$$\begin{cases} x \text{ is an ordinal number and } y = t(x), \text{ for some computation } t \\ \qquad\qquad \text{of length } x \text{ based on } \mathbf{G}, \\ \text{or } x \text{ is not an ordinal number and } y = \emptyset. \end{cases}$$

defines an operation $\mathbf{F}$ such that $\mathbf{F}(\alpha) = \mathbf{G}(\mathbf{F} \restriction \alpha)$, for all ordinals α.

- $\mathbf{P}(x, y)$ defines an operation: If x is not an ordinal, this is obvious. To prove it for ordinals, it suffices to show by transfinite induction: For every ordinal α there is a unique computation of length α.
  The inductive assumption is that, for all $\beta < \alpha$, there is a unique computation of length β. We must prove the existence and uniqueness of a computation of length α.

The Existence Part

- According to the Axiom Schema of Replacement applied to the property "y is a computation of length x" and the set α, there is a set

$$T = \{t : t \text{ is a computation of length } \beta \text{ for some } \beta < \alpha\}.$$

Moreover, the inductive assumption implies that for every $\beta < \alpha$, there is a unique $t \in T$, such that the length of t is β. T is a system of functions. Set $\overline{t} = \bigcup T$. Finally, let $\tau = \overline{t} \cup \{(\alpha, \mathbf{G}(\overline{t}))\}$. We prove that τ is a computation of length α.

Claim: τ is a function and $\mathrm{dom}\tau = \alpha + 1$.

We have $\mathrm{dom}\overline{t} = \bigcup_{t \in T} \mathrm{dom} t = \bigcup_{\beta \in \alpha}(\beta + 1) = \alpha$. Consequently, $\mathrm{dom}\tau = \mathrm{dom}\overline{t} \cup \{\alpha\} = \alpha + 1$. Since $\alpha \notin \mathrm{dom}\overline{t}$, it is enough to prove that $\overline{t}$ is a function. This follows from the fact that T is a compatible system of functions: Let t_1 and $t_2 \in T$ be arbitrary, and let $\mathrm{dom} t_1 = \beta_1$, $\mathrm{dom} t_2 = \beta_2$. Assume that, $\beta_1 \leq \beta_2$. Then $\beta_1 \subseteq \beta_2$, and it suffices to show that $t_1(\gamma) = t_2(\gamma)$, for all $\gamma < \beta_1$. We do that by transfinite induction.

The Existence Part (Cont'd)

Assume that $\gamma < \beta_1$ and $t_1(\delta) = t_2(\delta)$, for all $\delta < \gamma$. Then $t_1 \upharpoonright \gamma = t_2 \upharpoonright \gamma$, and we have $t_1(\gamma) = \mathbf{G}(t_1 \upharpoonright \gamma) = \mathbf{G}(t_2 \upharpoonright \gamma) = t_2(\gamma)$. We conclude that $t_1(\gamma) = t_2(\gamma)$, for all $\gamma < \beta_1$.

Claim: $\tau(\beta) = \mathbf{G}(\tau \upharpoonright \beta)$, for all $\beta \leq \alpha$.

This is clear if $\beta = \alpha$, as $\tau(\alpha) = \mathbf{G}(\overline{t}) = \mathbf{G}(\tau \upharpoonright \alpha)$. If $\beta < \alpha$, pick $t \in T$ such that $\beta \in \operatorname{dom} t$. Since t is a computation, and $t \subseteq \tau$,

$$\tau(\beta) = t(\beta) = \mathbf{G}(t \upharpoonright \beta) = \mathbf{G}(\tau \upharpoonright \beta).$$

The Uniqueness Part

- Let σ be another computation of length α; we prove $\tau = \sigma$. As τ and σ are functions and $\text{dom}\tau = \alpha + 1 = \text{dom}\sigma$, it suffices to prove by transfinite induction that $\tau(\gamma) = \sigma(\gamma)$, for all $\gamma \leq \alpha$. Assume that $\tau(\delta) = \sigma(\delta)$, for all $\delta < \gamma$. Then

$$\tau(\gamma) = \mathbf{G}(\tau \restriction \gamma) = \mathbf{G}(\sigma \restriction \gamma) = \sigma(\gamma).$$

The assertion follows.
This concludes the proof that the property $\mathbf{P}$ defines an operation $\mathbf{F}$. Notice that for any computation t, $\mathbf{F} \restriction \text{dom}t = t$. This is because for any $\beta \in \text{dom}t$, $t_\beta = t \restriction (\beta + 1)$ is obviously a computation of length β, whence, by the definition of $\mathbf{F}$, $\mathbf{F}(\beta) = t_\beta(\beta) = t(\beta)$.
To prove that $\mathbf{F}(\alpha) = \mathbf{G}(\mathbf{F} \restriction \alpha)$, for all α, let t be the unique computation of length α; we have

$$\mathbf{F}(\alpha) = t(\alpha) = \mathbf{G}(t \restriction \alpha) = \mathbf{G}(\mathbf{F} \restriction \alpha).$$

The Transfinite Recursion Theorem, Parametric Version

- We prove a parametric version of the Transfinite Recursion Theorem.
- If $\mathbf{F}(z,x)$ is an operation in two variables, we write $\mathbf{F}_z(x)$ in place of $\mathbf{F}(z,x)$. For any fixed z, $\mathbf{F}_z$ is an operation in one variable.
- If $\mathbf{F}$ is defined by $\mathbf{Q}(z,x,y)$, the notations $\mathbf{F}_z[A]$ and $\mathbf{F}_z \restriction A$ mean

$$\begin{array}{rcl}\mathbf{F}_z[A] & = & \{y : \mathbf{Q}(z,x,y), \text{ for some } x \in A\};\\ \mathbf{F}_z \restriction A & = & \{(x,y) : \mathbf{Q}(z,x,y), \text{ for some } x \in A\}.\end{array}$$

- Call t a **computation of length α based on G and z** if t is a function, $\mathrm{dom}\, t = \alpha + 1$, and, for all $\beta \leq \alpha$, $t(\beta) = \mathbf{G}(z, t \restriction \beta)$.

The Transfinite Recursion Theorem, Parametric Version

Let $\mathbf{G}$ be an operation. The property $\mathbf{Q}(z,x,y)$

$$\left\{\begin{array}{c}x \text{ is an ordinal number and } y = t(x), \text{ for some computation } t\\ \text{of length } x \text{ based on } \mathbf{G} \text{ and } z,\\ \text{or } x \text{ is not an ordinal number and } y = \emptyset.\end{array}\right.$$

defines an operation $\mathbf{F}$ such that $\mathbf{F}(z,\alpha) = \mathbf{G}(z, \mathbf{F}_z \restriction \alpha)$, for all ordinals α and all sets z.

The Transfinite Recursion Theorem (Successor-Limit)

- To distinguish between successor ordinals and limit ordinals in various constructions, we reformulate the Transfinite Recursion Theorem:

The Transfinite Recursion Theorem (Successor-Limit)

Let $\mathbf{G}_1, \mathbf{G}_2$ and $\mathbf{G}_3$ be operations, and let $\mathbf{G}$ be the operation defined by

$$\begin{cases} \mathbf{G}(x) = y \text{ if and only if either} \\ \text{(a)} \quad x = \emptyset \text{ and } y = \mathbf{G}_1(\emptyset) \\ \text{(b)} \quad x \text{ is a function, } \mathrm{dom} x = \alpha + 1, \text{ for ordinal } \alpha, \text{ and } y = \mathbf{G}_2(x(\alpha)) \\ \text{(c)} \quad x \text{ is a function, } \mathrm{dom} x = \alpha, \text{ for limit ordinal } \alpha, \text{ and } y = \mathbf{G}_3(x) \\ \text{(d)} \quad x \text{ is none of the above and } y = \emptyset \end{cases}$$

Then, the property $\mathbf{P}$

$$\begin{cases} x \text{ is an ordinal number and } y = t(x), \text{ for some computation } t \\ \qquad\qquad \text{of length } x \text{ based on } \mathbf{G}, \\ \text{or } x \text{ is not an ordinal number and } y = \emptyset. \end{cases}$$

(based on $\mathbf{G}$) defines an operation $\mathbf{F}$ such that $\mathbf{F}(0) = \mathbf{G}_1(\emptyset)$, $\mathbf{F}(\alpha + 1) = \mathbf{G}_2(\mathbf{F}(a))$, for all α, $\mathbf{F}(\alpha) = \mathbf{G}_3(\mathbf{F} \restriction \alpha)$, for all limit $\alpha \neq 0$.

Proof of the Successor-Limit Version

- Consider the operation

$$\begin{cases} \mathbf{G}(x) = y \text{ if and only if either} \\ \text{(a)} \quad x = \emptyset \text{ and } y = \mathbf{G}_1(\emptyset) \\ \text{(b)} \quad x \text{ is a function, dom} x = \alpha + 1 \text{, for ordinal } \alpha \text{, and } y = \mathbf{G}_2(x(\alpha)) \\ \text{(c)} \quad x \text{ is a function, dom} x = \alpha \text{, for limit ordinal } \alpha \text{, and } y = \mathbf{G}_3(x) \\ \text{(d)} \quad x \text{ is none of the above and } y = \emptyset \end{cases}$$

and the property $\mathbf{P}$

$$\begin{cases} x \text{ is an ordinal number and } y = t(x) \text{, for some computation } t \\ \qquad\qquad \text{of length } x \text{ based on } \mathbf{G}, \\ \text{or } x \text{ is not an ordinal number and } y = \emptyset. \end{cases}$$

The operation $\mathbf{F}$ defined by $\mathbf{P}$ satisfies $\mathbf{F}(\alpha) = \mathbf{G}(\mathbf{F} \restriction \alpha)$, for all α. Using our definition of $\mathbf{G}$, we can verify that $\mathbf{F}$ has the required properties.

Proof of the Original Recursion Theorem

- Recall the Recursion Theorem:

The Recursion Theorem

Let $\mathbf{G}$ be an operation. For any set a there is a unique infinite sequence $\langle a_n : n \in \mathbb{N} \rangle$ such that

(a) $a_0 = a$.

(b) $a_{n+1} = \mathbf{G}(a_n, n)$, for all $n \in \mathbb{N}$.

- Let $\mathbf{G}$ be an operation. We want to find, for every set a, a sequence $\langle a_n : n \in \omega \rangle$ such that $a_0 = a$ and $a_{n+1} = \mathbf{G}(a_n, n)$, for all $n \in \mathbb{N}$. By the parametric version of the Transfinite Recursion Theorem, there is an operation $\mathbf{F}$, such that $\mathbf{F}(0) = a$ and $\mathbf{F}(n+1) = \mathbf{G}(\mathbf{F}(n), n)$, for all $n \in \mathbb{N}$. Now we apply the Axiom of Replacement: There exists a sequence $\langle a_n : n \in \omega \rangle$ that is equal to $\mathbf{F} \restriction \omega$. This proves the theorem.

Proof of the Generalization to Transfinite Sequences

- Recall also the following theorem:

Theorem

Let Ω be an ordinal number, A a set, and $S = \bigcup_{\alpha<\Omega} A^\alpha$ the set of all transfinite sequences of elements of A of length less than Ω. Let $g : S \to A$ be a function. Then there exists a unique function $f : \Omega \to A$, such that

$$f(\alpha) = g(f \upharpoonright \alpha), \text{ for all } \alpha < \Omega.$$

- Define an operation $\mathbf{G}$ by

$$\mathbf{G}(t) = \begin{cases} g(t), & \text{if } t \in S \\ \emptyset, & \text{otherwise} \end{cases}$$

The Transfinite Recursion Theorem provides an operation $\mathbf{F}$ such that $\mathbf{F}(\alpha) = \mathbf{G}(\mathbf{F} \upharpoonright \alpha)$ holds for all ordinals α. Let $f = \mathbf{F} \upharpoonright \Omega$.

Subsection 5

Ordinal Arithmetic

Addition of Ordinal Numbers

- We use the Transfinite Recursion Theorem to define addition, multiplication, and exponentiation of ordinal numbers.

Definition (Addition of Ordinal Numbers)

For all ordinals β,

(a) $\beta + 0 = \beta$.

(b) $\beta + (\alpha + 1) = (\beta + \alpha) + 1$ for all α.

(c) $\beta + \alpha = \sup\{\beta + \gamma : \gamma < \alpha\}$, for all limit $\alpha \neq 0$.

- If we let $\alpha = 0$ in (b), we have the equality $\beta + 1 = \beta + 1$;
  - the left-hand side denotes the sum of ordinal numbers β and 1;
  - the right-hand side is the successor of β.

Justification of the Definition

- This definition conforms with the formal version of the Transfinite Recursion Theorem:

  Consider operations $\mathbf{G}_1, \mathbf{G}_2$ and $\mathbf{G}_3$, where
  - $\mathbf{G}_1(z,x) = z$,
  - $\mathbf{G}_2(z,x) = x+1$, and
  - $\mathbf{G}_3(z,x) = \sup(\mathrm{ran} x)$, if x is a function (and $\mathbf{G}_3(z,x) = 0$, otherwise).

  We get an operation $\mathbf{F}$ such that for all z

$$
\begin{aligned}
\mathbf{F}(z,0) &= \mathbf{G}_1(z,0) = z \\
\mathbf{F}(z,\alpha+1) &= \mathbf{G}_2(z,\mathbf{F}_z(\alpha)) = \mathbf{F}_z(\alpha)+1, \text{ for all } \alpha. \\
\mathbf{F}(z,\alpha) &= \mathbf{G}_3(z,\mathbf{F}_z \restriction \alpha) = \sup(\mathrm{ran}(\mathbf{F}_z \restriction \alpha)) \\
&\qquad = \sup\{\mathbf{F}(z,\gamma) : \gamma < \alpha\}, \text{ for limit } \alpha \neq 0.
\end{aligned}
$$

  If β and α are ordinals, then we write $\beta + \alpha$ instead of $\mathbf{F}(\beta,\alpha)$ and these conditions are exactly the clauses of the definition.

Some Basic Properties of Addition

- Note, for all β, $(\beta+1)+1=\beta+2$, $(\beta+2)+1=\beta+3$, etc.
- Also, we have (if $\alpha=\beta=\omega$):

$$\begin{array}{rcl}\omega+\omega & = & \sup\{\omega+n : n<\omega\},\\ (\omega+\omega)+\omega & = & \sup\{(\omega+\omega)+n : n<\omega\}.\end{array}$$

- In contrast to these examples, consider the sum $m+\omega$ for $m<\omega$. We have $m+\omega=\sup\{m+n : n<\omega\}=\omega$, because, if m is a natural number, $m+n$ is also a natural number. We see that $m+\omega\neq\omega+m$; the addition of ordinals is not commutative.
- Notice that, while $1\neq 2$, we have $1+\omega=2+\omega$. Thus, cancelations on the right in equations and inequalities are not allowed.
- However, we will show that addition of ordinal numbers is associative and allows left cancelations.

Sums of Linear Orders and Ordinal Numbers

Theorem

Let $(W_1, <_1)$ and $(W_2, <_2)$ be well-ordered sets, isomorphic to ordinals α_1 and α_2, respectively, and $(W, <)$ the sum of $(W_1, <_1)$ and $(W_2, <_2)$. Then $(W, <)$ is isomorphic to the ordinal $\alpha_1 + \alpha_2$.

- Assume that W_1 and W_2 are disjoint, $W = W_1 \cup W_2$, and each element in W_1 precedes in $<$ each element of W_2, while $<$ agrees with $<_1$ and with $<_2$ on both W_1 and W_2. We prove the theorem by induction on α_2.
  - If $\alpha_2 = 0$, then $W_2 = \emptyset$, $W = W_1$, and $\alpha_1 + \alpha_2 = \alpha_1$.
  - If $\alpha_2 = \beta + 1$, then W_2 has a greatest element a, and $W[a]$ is isomorphic to $\alpha_1 + \beta$; the isomorphism extends to an isomorphism between W and $\alpha_1 + \alpha_2 = (\alpha_1 + \beta) + 1$.
  - Let α_2 be a limit ordinal. For each $\beta < \alpha_2$, there is an isomorphism f_β of $\alpha_1 + \beta$ onto $W[a_\beta]$, where $a_\beta \in W_2$; moreover, f_β is unique, a_β is the β-th element of W_2, and if $\beta < \gamma$, then $f_\beta \subseteq f_\gamma$. Let $f = \bigcup_{\beta<\alpha_2} f_\beta$. As $\alpha_1 + \alpha_2 = \bigcup_{\beta<\alpha_2}(\alpha_1 + \beta)$, it follows that f is an isomorphism of $\alpha_1 + \alpha_2$ onto W.

Ordering of Ordinals

Lemma

(a) If $\alpha_1, \alpha_2, \beta$ are ordinals, then $\alpha_1 < \alpha_2$ if and only if $\beta + \alpha_1 < \beta + \alpha_2$.

(b) For all ordinals α_1, α_2 and β, $\beta + \alpha_1 = \beta + \alpha_2$ if and only if $\alpha_1 = \alpha_2$.

(c) $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$, for all ordinals α, β and γ.

(a) We use transfinite induction on α_2 to show that $\alpha_1 < \alpha_2$ implies $\beta + \alpha_1 < \beta + \alpha_2$. Assume that α_2 is an ordinal greater than α_1 and that $\alpha_1 < \delta$ implies $\beta + \alpha_1 < \beta + \delta$, for all $\delta < \alpha_2$.

- If α_2 is a successor ordinal, then $\alpha_2 = \delta + 1$, where $\delta \geq \alpha_1$. By the inductive assumption in case $\delta > \alpha_1$, and trivially in case $\delta = \alpha_1$, we obtain $\beta + \alpha_1 \leq \beta + \delta < (\beta + \delta) + 1 = \beta + (\delta + 1) = \delta + \alpha_2$.
- If α_2 is a limit ordinal, then $\alpha_1 + 1 < \alpha_2$ and we have $\beta + \alpha_1 < (\beta + \alpha_1) + 1 = \beta + (\alpha_1 + 1) \leq \sup\{\beta + \delta : \delta < \alpha_2\} = \beta + \alpha_2$.

For the converse, assume $\beta + \alpha_1 < \beta + \alpha_2$. If $\alpha_2 < \alpha_1$, by the preceding part, $\beta + \alpha_2 < \beta + \alpha_1$. Since $\alpha_2 = \alpha_1$ is also impossible (it implies $\beta + \alpha_2 = \beta + \alpha_1$), the linearity of $<$ implies $\alpha_1 < \alpha_2$.

Ordering of Ordinals (Cont'd)

- Continuing with the proof:
  (b) This follows immediately from (a): If $\alpha_1 \neq \alpha_2$, then either $\alpha_1 < \alpha_2$ or $\alpha_2 < \alpha_1$ and, thus, either $\beta + \alpha_1 < \beta + \alpha_2$ or $\beta + \alpha_2 < \beta + \alpha_1$. If $\alpha_1 = \alpha_2$, then $\beta + \alpha_1 = \beta + \alpha_2$ holds trivially.
  (c) We proceed by transfinite induction on γ.
    - If $\gamma = 0$, then $(\alpha + \beta) + 0 = \alpha + \beta = \alpha + (\beta + 0)$.
    - Assume that equality holds for γ, and prove it for $\gamma + 1$: $(\alpha + \beta) + (\gamma + 1) = [(\alpha + \beta) + \gamma] + 1 = [\alpha + (\beta + \gamma)] + 1 = \alpha + [(\beta + \gamma) + 1] = \alpha + [\beta + (\gamma + 1)]$.
    - Let γ be a limit ordinal, $\gamma \neq 0$. Then $(\alpha + \beta) + \gamma = \sup\{(\alpha + \beta) + \delta : \delta < \gamma\} = \sup\{\alpha + (\beta + \delta) : \delta < \gamma\}$. We observe that $\sup\{\beta + \delta : \delta < \gamma\} = \beta + \gamma$ (the third clause in the definition of addition) and that $\beta + \gamma$ is a limit ordinal (if $\xi < \beta + \gamma$ then $\xi \leq \beta + \delta$ for some $\delta < \gamma$ and so $\xi + 1 \leq (\beta + \delta) + 1 = \beta + (\delta + 1) < \beta + \gamma$ because γ is limit). Finally, notice $\sup\{\alpha + (\beta + \delta) : \delta < \gamma\} = \sup\{\alpha + \xi : \xi < \beta + \gamma\}$ (because $\beta + \gamma = \sup\{\beta + \delta : \delta < \gamma\}$) and so we have $(a + \beta) + \gamma = \sup\{a + \xi : \xi < \beta + \gamma\} = \alpha + (\beta + \gamma)$.

Subtraction of Ordinals

Lemma (Definition of Difference)

If $\alpha \leq \beta$ then there is a unique ordinal number ξ, such that $\alpha + \xi = \beta$.

- As α is an initial segment of the well-ordered set β (or $\alpha = \beta$), the main theorem implies that $\beta = \alpha + \xi$, where ξ is the order type of the set $\beta - \alpha = \{\nu : \alpha \leq \nu < \beta\}$. By Part (b) of the preceding lemma, the ordinal ξ is unique.

Multiplication of Ordinal Numbers

Definition (Multiplication of Ordinal Numbers)

For all ordinals β,

(a) $\beta \cdot 0 = 0$.

(b) $\beta \cdot (\alpha + 1) = \beta \cdot \alpha + \beta$, for all α.

(c) $\beta \cdot \alpha = \sup \{\beta \cdot \gamma : \gamma < \alpha\}$, for all limit $\alpha \neq 0$.

- Examples:
  (a) $\beta \cdot 1 = \beta \cdot (0 + 1) = \beta \cdot 0 + \beta = 0 + \beta = \beta$.
  (b) $\beta \cdot 2 = \beta \cdot (1 + 1) = \beta \cdot 1 + \beta = \beta + \beta$; in particular, $\omega \cdot 2 = \omega + \omega$.
  (c) $\beta \cdot 3 = \beta \cdot (2 + 1) = \beta \cdot 2 + \beta = \beta + \beta + \beta$, etc.
  (d) $\beta \cdot \omega = \sup \{\beta \cdot n : n \in \omega\} = \sup \{\beta, \beta \cdot 1, \beta \cdot 2, \ldots\}$.
  (e) $1 \cdot \alpha = \alpha$ for all α, but this requires an inductive proof:
    - $1 \cdot 0 = 0$;
    - $1 \cdot (\alpha + 1) = 1 \cdot \alpha + 1 = \alpha + 1$;
    - If α is limit, $\alpha \neq 0$, $1 \cdot \alpha = \sup \{1 \cdot \gamma : \gamma < a\} = \sup \{\gamma : \gamma < a\} = \alpha$.
  (f) $2 \cdot \omega = \sup \{2 \cdot n : n \in \omega\} = \omega$. Since $\omega \cdot 2 = \omega + \omega \neq \omega$, we conclude that, in general, multiplication of ordinals is not commutative.

Products of Linear Orderings and Ordinal Multiplication

- Ordinal multiplication agrees with the general definition of products of linearly ordered sets:

Theorem

Let α and β be ordinal numbers. Both the lexicographic and the antilexicographic orderings of the product $\alpha \times \beta$ are well-orderings. The order type of the antilexicographic ordering of $\alpha \times \beta$ is $\alpha \cdot \beta$, while the lexicographic ordering of $\alpha \times \beta$ has order type $\beta \cdot \alpha$.

- Let $\prec$ denote the antilexicographic ordering of $\alpha \times \beta$. We define an isomorphism between $(\alpha \times \beta, \prec)$ and $\alpha \cdot \beta$ as follows: for $\xi < \alpha$ and $\eta < \beta$. let

$$f(\xi, \eta) = \alpha \cdot \eta + \xi.$$

The range of f is the set $\{\alpha \cdot \eta + \xi : \eta < \beta \text{ and } \xi < \alpha\} = \alpha \cdot \beta$. Moreover, f is an isomorphism (this part uses induction).

Exponentiation of Ordinal Numbers

Definition (Exponentiation of Ordinal Numbers)

For all β,

(a) $\beta^0 = 1$.

(b) $\beta^{\alpha+1} = \beta^\alpha \cdot \beta$, for all α.

(c) $\beta^\alpha = \sup\{\beta^\gamma : \gamma < \alpha\}$, for all limit $\alpha \neq 0$.

- Examples:
  (a) $\beta^1 = \beta$, $\beta^2 = \beta \cdot \beta$, $\beta^3 = \beta \cdot \beta \cdot \beta$, etc.
  (b) $\beta^\omega = \sup\{\beta^n : n \in \omega\}$;
  In particular, $1^\omega = 1$, $2^\omega = \omega$, $3^\omega = \omega$, ..., $n^\omega = \omega$, for any $n \in \omega$.
  $\omega^\omega = \sup\{\omega^n : n \in \omega\} > \omega$.
- Ordinal arithmetic differs substantially from the arithmetic of cardinals: For instance, $2^\omega = \omega$ and ω^ω are countable ordinals, while $2^{\aleph_0} = \aleph_0^{\aleph_0}$ is uncountable.

Subsection 6

The Normal Form

Continuity in the Second Variable

- Using exponentiation, one can represent ordinal numbers in a normal form analogous to the decimal expansion of integers.
- Observe that the ordinal functions $\alpha + \beta, \alpha \cdot \beta$ and α^β are continuous in the second variable: If γ is a limit ordinal and $\beta = \sup_{\nu<\gamma} \beta_\nu$,
  - $\alpha + \beta = \sup_{\nu<\gamma} (\alpha + \beta_\nu)$,
  - $\alpha \cdot \beta = \sup_{\nu<\gamma} (\alpha \cdot \beta_\nu)$,
  - $\alpha^\beta = \sup_{\nu<\gamma} (\alpha^{\beta_\nu})$.

Lemma

(a) If $0 < \alpha \leq \gamma$, then there is a greatest ordinal β, such that $\alpha \cdot \beta \leq \gamma$.

(b) If $1 < \alpha \leq \gamma$, then there is a greatest ordinal β, such that $\alpha^\beta \leq \gamma$.

- Since $\alpha \cdot (\gamma + 1) \geq \gamma + 1 > \gamma$, there exists a δ, such that $\alpha \cdot \delta > \gamma$. Similarly, because $\alpha^{\gamma+1} \geq \gamma + 1 > \gamma$, there is a δ with $\alpha^\delta > \gamma$. Because of continuity, the least δ such that $\alpha \cdot \delta > \gamma$ (or that $\alpha^\delta > \gamma$) must be a successor ordinal, say $\delta = \beta + 1$. Then β is the greatest ordinal such that $\alpha \cdot \beta \leq \gamma$ (respectively, $\alpha^\beta \leq \gamma$).

Division Algorithm for Ordinals

Lemma

If γ is an arbitrary ordinal and if $\alpha \neq 0$, then there exists a unique ordinal β and a unique $\rho < \alpha$ such that $\gamma = \alpha \cdot \beta + \rho$.

- Let β be the greatest ordinal such that $\alpha \cdot \beta \leq \gamma$ (if $\alpha > \gamma$, then $\beta = 0$), and let ρ be the unique ordinal, such that $\alpha \cdot \beta + \rho = \gamma$. The ordinal ρ is less than α, because otherwise we would have $\alpha \cdot (\beta + 1) = \alpha \cdot \beta + \alpha \leq \alpha \cdot \beta + \rho = \gamma$, contrary to the maximality of β.

  To prove uniqueness, let $\gamma = \alpha \cdot \beta_1 + \rho_1 = \alpha \cdot \beta_2 + \rho_2$, with $\rho_1, \rho_2 < \alpha$. Assume that $\beta_1 < \beta_2$. Then $\beta_1 + 1 \leq \beta_2$ and we have $\alpha \cdot \beta_1 + (\alpha + \rho_2) = \alpha \cdot (\beta_1 + 1) + \rho_2 \leq \alpha \cdot \beta_2 + \rho_2 = \alpha \cdot \beta_1 + \rho_1$, and, by a previous lemma, $\rho_1 \geq \alpha + \rho_2 \geq \alpha$, a contradiction. Thus $\beta_1 = \beta_2$. Now $\rho_1 = \rho_2$ follows by the subtraction lemma.

The Normal Form Theorem

- The normal form is analogous to the decimal expansion of integers, with the base for exponentiation being the ordinal ω:

Theorem (Normal Form)

Every ordinal $\alpha > 0$ can be expressed uniquely as

$$\alpha = \omega^{\beta_1} \cdot k_1 + \omega^{\beta_2} \cdot k_2 + \cdots + \omega^{\beta_n} \cdot k_n,$$

where $\beta_1 > \beta_2 > \cdots > \beta_n$, and $k_1 > 0, k_2 > 0, \ldots, k_n > 0$ are finite.

- Existence: By induction on α. The ordinal $\alpha = 1$ can be expressed as $1 = \omega^0 \cdot 1$. Now let $\alpha > 0$ be arbitrary. By the lemma, there exists a greatest β, such that $\omega^\beta \leq \alpha$ (if $\alpha < \omega$, then $\beta = 0$). Then, by the preceding lemma, there exist unique δ and ρ, such that $\rho < \omega^\beta$ and $\alpha = \omega^\beta \cdot \delta + \rho$. As $\omega^\beta \leq \alpha$, we have $\delta > 0$ and $\rho < \alpha$.

The Normal Form Theorem (Existence)

- We found unique $\delta > 0$ and $\rho < \alpha$, such that $\rho < \omega^\beta$ and $\alpha = \omega^\beta \cdot \delta + \rho$.

  Claim: δ is finite.

  If δ were infinite, then $\alpha \geq \omega^\beta \cdot \delta \geq \omega^\beta \cdot \omega = \omega^{\beta+1}$, contradicting the maximality of β.

  Thus let $\beta_1 = \beta$ and $k_1 = \delta$.

  - If $\rho = 0$, then $\alpha = \omega^{\beta_1} \cdot k_1$ is in normal form.
  - If $\rho > 0$, then by the induction hypothesis, $\rho = \omega^{\beta_2} \cdot k_2 + \cdots + \omega^{\beta_n} \cdot k_n$, for some $\beta_2 > \cdots > \beta_n$ and finite $k_2, \ldots, k_n > 0$. As $\rho < \omega^{\beta_1}$, we have $\omega^{\beta_2} \leq \rho < \omega^{\beta_1}$ and so $\beta_1 > \beta_2$. It follows that

    $$\alpha = \omega^{\beta_1} \cdot k_1 + \omega^{\beta_2} \cdot k_2 + \cdots + \omega^{\beta_n} \cdot k_n$$

    is expressed in normal form.

The Normal Form Theorem (Uniqueness)

- Claim: If $\beta < \gamma$, then $\omega^\beta \cdot k < \omega^\gamma$ for every finite k.
  This is because $\omega^\beta \cdot k < \omega^\beta \cdot \omega = \omega^{\beta+1} \leq \omega^\gamma$.
  From this it easily follows that if
  $\alpha = \omega^{\beta_1} \cdot k_1 + \omega^{\beta_2} \cdot k_2 + \cdots + \omega^{\beta_n} \cdot k_n$ and $\gamma > \beta_1$, then $\alpha < \omega^\gamma$.
  We prove the uniqueness of normal form by induction on α.
  - For $\alpha = 1$, the expansion $1 = \omega^0 \cdot 1$ is clearly unique.
  - So let $\alpha = \omega^{\beta_1} \cdot k_1 + \cdots + \omega^{\beta_n} \cdot k_n = \omega^{\gamma_1} \cdot \ell_1 + \cdots + \omega^{\gamma_m} \cdot \ell_m$. The preceding observation implies that $\beta_1 = \gamma_1$. If we let $\delta = \omega^{\beta_1} = \omega^{\gamma_1}$, $\rho = \omega^{\beta_2} \cdot k_2 + \cdots + \omega^{\beta_n} \cdot k_n$ and $\sigma = \omega^{\gamma_2} \cdot \ell_2 + \cdots + \omega^{\gamma_m} \cdot \ell_m$, we have $\alpha = \delta \cdot k_1 + \rho = \delta \cdot \ell_1 + \sigma$, and since $\rho < \delta$ and $\sigma < \delta$, a preceding lemma implies that $k_1 = \ell_1$ and $\rho = \sigma$. By the induction hypothesis, the normal form for ρ is unique, and so $m = n$, $\beta_2 = \gamma_2, \ldots, \beta_n = \gamma_n$ $k_2 = \ell_2, \ldots, k_n = \ell_n$. If follows that the normal form expansion for α is unique.

Weak Goodstein Sequences

- We use the normal form to prove an interesting result on Goodstein sequences.
- Recall that for every natural number $a \geq 2$, every natural number m can be written in base a, i.e., as a sum of powers of a:
$$m = a^{b_1} \cdot k_1 + \cdots + a^{b_n} \cdot k_n,$$
with $b_1 > \cdots > b_n$, and $0 < k_i < a$, $i = 1, \ldots, n$.
- Example: The number 324 can be written as $4^4 + 4^3 + 4$ in base 4 and $7^2 \cdot 6 + 7 \cdot 4 + 2$ in base 7.
- A **weak Goodstein sequence** starting at $m > 0$ is a sequence $m_0, m_1, m_2, \ldots$ of natural numbers defined as follows:
    - Let $m_0 = m$, and write m_0 in base 2: $m_0 = 2^{b_1} + \cdots + 2^{b_n}$.
    - To obtain m_1, increase the base by 1 (from 2 to 3) and then subtract 1: $m_1 = 3^{b_1} + \cdots + 3^{b_n} - 1$.
    - In general, to obtain m_{k+1} from m_k (as long as $m_k \neq 0$), write m_k in base $k+2$, increase the base by 1 (to $k+3$) and subtract 1.

An Example of a Weak Goodstein Sequence

- The weak Goodstein sequence starting at $m = 21$ is as follows:

$$\begin{array}{rcl}
m_0 & = & 21 = 2^4 + 2^2 + 1 \\
m_1 & = & 3^4 + 3^2 = 90 \\
m_2 & = & 4^4 + 4^2 - 1 = 4^4 + 4 \cdot 3 + 3 = 271 \\
m_3 & = & 5^4 + 5 \cdot 3 + 2 = 642 \\
m_4 & = & 6^4 + 6 \cdot 3 + 1 = 1315 \\
m_5 & = & 7^4 + 7 \cdot 3 = 2422 \\
m_6 & = & 8^4 + 8 \cdot 2 + 7 = 4119 \\
m_7 & = & 9^4 + 9 \cdot 2 + 6 = 6585 \\
m_8 & = & 10^4 + 10 \cdot 2 + 5 = 10025 \\
\text{etc.} & &
\end{array}$$

Termination Theorem for Weak Goodstein Sequences

Theorem

For each $m > 0$, the weak Goodstein sequence starting at m eventually terminates with $m_n = 0$ for some n.

- We use the normal form for ordinals. Let $m > 0$ and $m_0, m_1, m_2, \ldots$ be the weak Goodstein sequence starting at m. Its ath term is written in base $a+2$: $m_a = (a+2)^{b_1} k_1 + \cdots + (a+2)^{b_n} k_n$. Consider the ordinal $\alpha_a = \omega^{b_1} \cdot k_1 + \cdots + \omega^{b_n} \cdot k_n$ obtained by replacing base $a+2$ by ω. It is easily seen that $\alpha_0 > \alpha_1 > \cdots > \alpha_a > \cdots$ is a decreasing sequence of ordinals, necessarily finite. Therefore, there exists some n such that $\alpha_n = 0$. But clearly $m_a \leq \alpha_a$ for every $a = 0, 1, 2, \ldots, n$. Hence $m_n = 0$.

Goodstein Sequences

- A number n is written in **pure base** $a \geq 2$ if it is first written in base a, then so are the exponents and the exponents of exponents, etc.
- Example: The number 324 written in pure base 3 is $3^{3+2} + 3^{3+1}$.
- The **Goodstein sequence** starting at $m > 0$ is a sequence $m_0, m_1, m_2, \ldots$ obtained as follows:
  - Let $m_0 = m$ and write m_0 in pure base 2.
  - To define m_1, replace each 2 by 3, and then subtract 1.
  - In general, to get m_{k+1}, write m_k in pure base $k+2$, replace each $k+2$ by $k+3$, and subtract 1.
- Example: The Goodstein sequence starting at $m = 21$ is as follows:

$$\begin{aligned} m_0 &= 21 = 2^{2^2} + 2^2 + 1 \\ m_1 &= 3^{3^3} + 3^3 \approx 7.6 \times 10^{12} \\ m_2 &= 4^{4^4} + 4^4 - 1 = 4^{4^4} + 4^3 \cdot 3 + 4^2 \cdot 3 + 4 \cdot 3 + 3 \approx 1.3 \times 10^{154} \\ m_3 &= 5^{5^5} + 5^3 \cdot 3 + 5^2 \cdot 3 + 5 \cdot 3 + 2 \approx 1.9 \times 10^{2184} \\ m_4 &= 6^{6^6} + 6^3 \cdot 3 + 6^2 \cdot 3 + 6 \cdot 3 + 1 \approx 2.6 \times 10^{36305} \end{aligned}$$

etc.

Termination Theorem for Goodstein Sequences

- Goodstein sequences initially grow even more rapidly than weak Goodstein sequences, but still:

Termination Theorem

For each $m > 0$, the Goodstein sequence starting at m eventually terminates with $m_n = 0$ for some n.

- We define a (finite) sequence of ordinals $\alpha_0 > \alpha_1 > \cdots > \alpha_a > \cdots$ as follows: When m_a is written in pure base $a+2$, we get α, by replacing each $a+2$ by ω.
- Example: For instance, in the example above, the ordinals are

$$\omega^{\omega^\omega} + \omega^\omega + 1,\ \omega^{\omega^\omega} + \omega^\omega,$$
$$\omega^{\omega^\omega} + \omega^3 \cdot 3 + \omega^2 \cdot 3 + \omega \cdot 3 + 3,\ \omega^{\omega^\omega} + \omega^3 \cdot 3 + \omega^2 \cdot 3 + \omega \cdot 3 + 2,$$
$$\omega^{\omega^\omega} + \omega^3 \cdot 3 + \omega^2 \cdot 3 + \omega \cdot 3 + 1,\ \text{etc.}$$

The ordinals α_a are in normal form, and again, it can be shown that they form a (finite) decreasing sequence. Therefore, $\alpha_n = 0$ for some n, and since $m_a \leq \alpha_a$, for all a, we have $m_n = 0$.