Set Theory

Fan

2023.7.21

Contents

Abstract

This is a reading note for Robert's *Set Theory*. It is my first reading note written in English, so you may see many grammar mistakes. This note consists of some important point that I am not familiar with or considered worthing remembered and my answer to the question following each lesson, whose correctness are not guranteened, but I will point out where can be refined.

Table 1: various notation

notations	meanings
$\sim$	*not, or it is not the case that*
$\vee$	*or*
$\wedge$	*and*
$A \rightarrow B$	*if* A *then* B
$A \leftrightarrow B$	A *if and only if* B (Also:'iff')
$\forall x A$	*for all x such that* A
$\exists x A$	*there exists an x such that* A
$\exists! x A$	*there exists exactly one x such that* A
$\iota x A$	*the unique x such that* A
$x = y$	*x equals y, or x and y are identical*
$A)(B$	A *and* B *are disjointed*
$A \cup B$	$\{x : x \in A \,\mathrm{or}\, x \in B\}$
$A \cap B$	$\{x : x \in A \,\mathrm{and}\, x \in B\}$
$A - B$	$\{x : x \in A \,\mathrm{and}\, x \notin B\}$
$A \ominus B$	$(A - B) \cup (B - A)$
$\varnothing$	$\{x : x \neq x\}$
$A \times B$	$\{(a, b) : a \in A \,\mathrm{and}\, b \in B\}$
$f \restriction C$	the restriction of f to C

notations	meanings
$\breve{R}$	R converse
R/S	relative product
$R \circ S$	the composition of R and S
$R[U]$	the R-image of U
Id_A	the identity function for A
$A \underset{f}{\sim} B$	f is a one-to-one function on A onto B
$A \sim B$	A and B are equivalent
B^C	the set of all functions on C to B
$\prod_{i \in I} \mathfrak{a}_i$	Cartesian product
$P(A)$	power set of A
c_B	characteristic function of B
$\underline{A} \underset{f}{\cong} \underline{A}'$	an isomorphism between $\underline{A}$ and $\underline{A}'$
$\underline{A}|B$	the substructures of $\underline{A}$
$\sup A$	the least upper bound of A
$\inf A$	the greatest lower bound of A
$\bar{\bar{A}}$	the cardinal number of A
$\hat{n}$	hyperexponentiation to the base 2 at n

1 SETS AND RELATIONS AND OPERATIONS AMONG THEM

Logical symbols and abbreviations are easy to write, but they are not meant to use throughout the whole proof. Even mathematics only sometimes use them in theorems'writing. When writing a proof, it is recommended to use ordinary language to explain your idea whenever it is necessery.

1.1 Set algebra and the set-builder

In this textbook, we assume that non-set doesn't exists. In other words, we only consider what is so-called pure set.

Axiom 1 (Axiom of Extensionality)**.** If, for any x,$x \in A$ if and only if $x \in B$,then $A = B$.

All expression in language can be classified into 3 groups, namely asserting expression, naming expression and others. Asserting expression is a kind of expression that can specify the range or value of some variable, for example, an inequility. Name expression is a kind of expression that describe some forms, for example, a function. When using set builder $\{x : - - -\}$, —should always be replaced by asserting expression. When using set buider $\{... : - - -\}$,...should be replaced by a naming expression, and — should be replaced by a asserting expression.

We defined following Boolean operations:

$$
\begin{cases}
A \cup B & = \{x : x \in A \,\text{or}\, x \in B\}, \text{called the union of} A \text{and} B. \\
A \cap B & = \{x : x \in A \,\text{and}\, x \in B\}, \text{called the intersection of} A \text{and} B. \\
A - B & = \{x : x \in A \,\text{and}\, x \notin B\}, \text{called } A \text{minus} B. \\
A \ominus B & = (A - B) \cup (B - A), \text{called the symmetric difference of} A \text{and} B. \\
\varnothing & = \{x : x \neq x\}, \text{the empty set}
\end{cases}
$$

Particularly, $X - A$ is also written as $\tilde{A}^{(X)}$, called the complement of A with respect to X.

When we are discussing sets, we always assume that they are included in a set X called 'temporary universe'. In this case, we write $\tilde{A}^{(X)}$ as $\tilde{A}$. However, there is no absolute universe.

If a law only involves $\sim, \cup, \cap, \varnothing, X$,not $\ominus$,etc,its dual is obtained simply by replacing these,respectively by $\sim, \cap, \cup, X, \varnothing$.

theorem 1.1. Assume $A,B,C \subseteq X$ and write $\tilde{U}$ for $X - U$.

$$
\begin{cases}
A \cup B = B \cup A & \text{and dual} \\
A \cup (B \cup C) = (A \cup B) \cup C & \text{and dual} \\
A \cup \varnothing = A & \text{and dual}(A \cap X = A) \\
A \cap \varnothing = \varnothing & \text{and dual.} \\
\tilde{\tilde{A}} = A \\
A \subseteq B \text{ if and only if} \tilde{A} \supseteq \tilde{B} \\
A - B = A \cap \tilde{B} \\
A \cap B = \varnothing \text{ if and only if} A \subseteq \tilde{B}
\end{cases}
$$

A and B are called disjoint, written $A)(B$, if $A \cap B = \varnothing$.

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \text{and dual}$$

$$\widetilde{A \cup B} = \tilde{A} \cap \tilde{B}, \text{and dual}$$

$$A \cap (B - C) = (A \cap B) - (A \cap C)$$

theorem 1.2. The family of all subsets of X, under $\ominus$ for $+$, and $\cap$ for $\cdot$, with $\varnothing$ for 0, and X for 1, forms a communicative ring with unit. the ring also satisfies the two additional laws : $A + A = 0$ (every element is of order 2) and $A \cdot A = A$ ($\cdot$ is idempotent). (Such ring is called a Boolean ring with unit.)

remark. To remember this kind of equation, I think you can regarded them as difference translations for one same thing. For instance, $A - B = A \cap \tilde{B}$, this equation's both side means that remove B from A, or the part of A that doesn't belong to B.

1.2   Russell's paradox

remark. $\{x : x \notin x\}$ does not exist.

In our intuitive set theory, we now accept these two axiom, namely:

Axiom 2 (Separation Axiom)**.** $\{x : x \in B \text{ and} \mathfrak{S}x\}$ always exists.

Axiom 3 (Replacement Axiom)**.** $\{\mathfrak{C} : x \in B\}$ always exists.

theorem 1.3. There is no universe set, i.e., for any set C there exists t such that $t \notin C$.

1.3   Infinite unions and intersections

theorem 1.4. Assume $\mathfrak{G} \subseteq X$ for all $i \in I$, and write $\tilde{U}$ for $X - U$ and take any intersection of the form $\bigcap_{i \in \varnothing} B_i$ to be X. Then:

1. (de Morgan's law) $\widetilde{\bigcup_{i \in I} \mathfrak{G}_i} = \bigcap_{i \in I} \tilde{\mathfrak{G}}_i$ and $\widetilde{\bigcap_{i \in I} \mathfrak{G}_i} = \bigcup_{i \in I} \tilde{\mathfrak{G}}_i$

2. (distributive laws) $B \cap \bigcup_{i \in I} \mathfrak{G}_i = \bigcup_{i \in I}(B \cap \mathfrak{G}_i)$ and its dual

remark. The varible i in the expression $\bigcap_{i \in I} \mathfrak{G}_i$ is called bound variable, and this kind of notation with bound variable is called bound variable notation. For any family K of sets, we write $\bigcup(K)$ for $\bigcup_{A \in K} A$, which is free of bound variables. Although the notations without bound variables seem to be more elegent, but sometimes when we have to point out various property of one element, using bound varialbles may be more convenient.

1.4   Ordered couples and Cartesian products

We read $\{a\}$ the singleton of a.

definition. $(a, b) = \{\{a\}, \{a, b\}\}$

theorem 1.5. If $(a, b) = (c, d)$, then $a = c$ and $b = d$.

The set $A \times B = \{(a, b) : a \in A \text{ and } b \in B\}$ is called the Cartesian product of the arbitrary sets A and B.

theorem 1.6.   1. $A \times \bigcup_{i \in I} \mathfrak{B}_i = \bigcup_{i \in I}(A \times \mathfrak{B}_i)$

2. $\bigcup_{i \in I} \mathfrak{B}_i \times A = \bigcup_{i \in I}(\mathfrak{B}_i \times A)$

3. $A \times \bigcap_{i \in I} \mathfrak{B}_i = \bigcap_{i \in I}(A \times \mathfrak{B}_i)$

4. $A \times (B - C) = A \times B - A \times C$

5. $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$

1.5   Relations and functions

We say R is a relation if R is a set of ordered couples. We write Rxy (or xRy), and say R holds betweem x and y, if $(x, y) \in R$.

The domain of a relation R, Dom R, is defined to be $\{x : for some y, xRy\}$ and the range, Rng R, is $\{y : for some x, xRy\}$.

We say f is a function if f is a relation and for any x, y, z if $(x, y), (x, z) \in f$ then $y = z$.

'f is on A' means Dom $f = A$; 'f is to,or into B' means Rng $f \subseteq B$; 'f is onto B' means Rng $f = B$; '$f : A \to B$'means f is a function on A to B.

Taking $f = ((x, \mathfrak{a}x) : x \in A)$:

theorem 1.7. There exists exactly one function f on A such that for each $x \in A, f(x) \in \mathfrak{a}_x$.

For the unique function f on X such that, for all $x \in X$, $f(x) \in \mathfrak{a}_x$, all of the following are in use:

$$(\mathfrak{a}_x : x \in X) \quad (\lambda x \in X)\mathfrak{a}_x \quad x \in X \mapsto \mathfrak{a}_x.$$

The function $f = (\mathfrak{a}_x : x \in X)$ is sometimes called an indexed family (of sets). The (plain) family $\{\mathfrak{a}_x : x \in X\}$ has 'less information'.

If $C \subseteq \text{Dom } f$, we write $f \upharpoonright C$ (called the restriction of f to C) for the function g on C such that, for any $x \in C, g(x) = f(x)$.

We take $\check{R}$(R converse) to be the set of all (y, x) such that $(x, y) \in R$. The converse of a function which is not one-to-one is a relation but not a function. f is one-to-one if and onlly if $\check{f}$ is a function. In this case, the function $\check{f}$ is called the inverse function (of f) and written f^{-1}.

If R and S are relations, the relative product R/S is defined to be $\{(x, y) :$ for some $z, (x, z) \in R$ and $(z, y) \in S\}$. We also define $R \circ S$ to be S/R

theorem 1.8.
$$R/(S/T) = (R/S)/T$$

theorem 1.9.
$$\check{R/S} = \check{S}/\check{R}$$

We take $R[U]$ to be the set of all y such that for some $x \in U, (x, y) \in R$. A special case is the $f-$image of U, $f[U]$. Given a function f (not necessery one-to-one), we can form the relation $\check{f}$ and the image set $\check{f}[V]$; this set is called the $f-$ inverse image of V, and is written $f^{-1}[V]$.

theorem 1.10. Suppose for all $i \in I, \mathfrak{a}_i \subseteq X$. Then

1. $R[\bigcup_{i \in I} \mathfrak{a}_i] = \bigcup_{i \in I} R[\mathfrak{a}_i]$

2. $f^{-1}(A - B) = f^{-1}A - f^{-1}B.$

3. $f^{-1}(\bigcap_{i \in I} \mathfrak{a}_i) = \bigcap_{i \in I} f^{-1}\mathfrak{a}_i$, if $I \neq \varnothing.$

theorem 1.11. 1. $A \underset{Id_A}{\sim} A$

2. if $A \underset{f}{\sim} B$, then $B \underset{f^{-1}}{\sim} A$

3. if $A \underset{f}{\sim} B$ and $B \underset{g}{\sim} C$, then $A \underset{g \circ f}{\sim} C.$

We write $A \sim B$, if, for some f, $A \underset{f}{\sim} B.$

theorem 1.12. 1. $A \sim A$

2. if $A \sim B$, then $B \sim A$

3. if $A \sim B$ and $B \sim C$ then $A \sim C.$

A notion like $\sim$ for which satisfies previous three equations is called an 'equivalence'.

1.6   Sets of sets,power set, arbitrary Cartesian product

We denote by B^C the set of all function on C to B. We will prove that, if C has n elements and B has m, then B^C has m^n.

Cartesian product $\prod_{i \in I} \mathfrak{a}_i$ is defined to be the set of all f on I such that, for each $i \in I, f(i) \in \mathfrak{a}_i$.If $\mathfrak{a}_i = B$, then

$$\prod_{i \in I} \mathfrak{a}_i = \prod_{i \in I} B = B^I$$

The set $P(A)$ is the set of all subsets of the set A. It is also called the power set of A.

We form the 'characteristic function ' c_B of B as follows: c_B is the function on A such that, for any $x \in A, c_B(x) = u$ if $x \in B$, and $c_B(x) = v$ if $x \neq B$. Then define $H(B) = c_B$.

theorem 1.13.

$$P(A) \underset{H}{\sim} \{u, v\}^A$$

theorem 1.14. Consider sets $\mathfrak{a}_{ij} \subseteq X$ and take any $\bigcap_{t \in \varnothing} B_t = X$

$$\bigcap_{i \in I} \bigcup_{j \in J_i} \mathfrak{a}_{ij} = \bigcup_{f \in \prod_{i \in I} J_i} \bigcap_{i \in I} \mathfrak{a}_{if(i)}.$$

(The dual follows by applying de Morgan's law.)

Axiom 4 (The Axiom of Choice). Let F be a function on I such that for each $i \in I, F(i)$ is a non-empty set. Then there is a function f on I such that for each $i \in I, f(i) \in F_i$.

remark. Such an f is called a choice function (or selector) for the indexed family $(F(i) : i \in I)$.

remark. The Axiom of Choice is identical to the statement: If for each $i \in I, F(i) \neq \varnothing$, then $\prod_{i \in I} \neq \varnothing$.

When we are proving, we should try to avoid using the Axiom of Choice directly.

theorem 1.15. Assume all $\mathfrak{a}_{ij} \subseteq x$ and take $\bigcap_{t \in \varnothing} \mathfrak{B}_t = X$

$$\prod_{i \in I} \bigcup_{j \in J_i} \mathfrak{a}_{ij} = \bigcup_{f \in \prod_{i \in I} J_i} \prod_{i \in I} \mathfrak{a}_{if(i)}$$

1.7   Structures

We say $\circ$ is a binary operation over A if $\circ : A \times A \to A$. (As usual, $\circ((x,y))$ is written $x \circ y$). R is called a binary relation over A if $R \subseteq A \times A$. A typical (algebraic) structure is something of the form $\underline{A} = (A, R, \circ)$ where $\circ$ and R are over A. The set A is called the universe of $\underline{A}$. A structure can have any number of R's and $\circ$'s and these can have any number of places, and there cam also be distinguished elements.

Let $\underline{A} = (A, R), \underline{A}' = (A', R')$. We say that f is an $(\underline{A}, \underline{A}')-$ isomorphism (or isomorphism between $\underline{A}$ and $\underline{A}'$), provided that $A \underset{f}{\sim} A'$ for any $x, y \in A, xRy$ if and only if $f(x)R'f(y)$(If instead $\underline{A} = (A, \circ), \underline{A}' = (A', \circ')$,one has instead the familiar condition: $f(x \circ y) = f(x) \circ' f(y)$).

We write $\underline{A} \cong \underline{A}'$ and say that $\underline{A}$ is isomorphic to $\underline{A}'$ if for some $f, \underline{A} \underset{f}{\cong} \underline{A}'$.

theorem 1.16. The theorem 1.11 and 1.12 about $A \underset{f}{\sim} B$ and $A \sim B$ extend at once to $\underline{A} \underset{f}{\cong} \underline{B}$and $\underline{A} \cong \underline{B}$.

If $B \subseteq A$, we call $(B, R \cap (B \times B))$ the substructures of $\underline{A}$, written $\underline{A}|B$.

We say that f is an isomorphism of $\underline{A} = (A, R)$ into $\underline{A}' = (\underline{A}', \underline{R}')$ if f is one-to-one on A into A' and for any $x, y \in A$, xRy if and only if $f(x)R'f(y)$.

theorem 1.17. f is an isomorphism of $\underline{A}$ into $\underline{A}'$ if and only if f is an isomorphism between $\underline{A}$ and some substructures of $\underline{A}'$.

1.8   Partial orders and orders

Let $\underline{A} = (A, R)$ be a structure. $\underline{A}$ is called reflective if for any $x \in A, xRx$; otherwise it is called irreflective. $\underline{A}$ is transitive if xRz whenever xRy and yRz;symmetric if yRx whenever xRy; antisymmetric if $x = y$ whenever xRy and yRx and asymmetric if $y\not{R}x$ whenever xRy.Finally, $\underline{A}$ is connected if for any $x, y \in A, xRy$ or yRx or $x = y$.

Relation R is said to be equivalence if (A, R) is reflective,symmetric,and transitive.

A structure $\underline{A} = (A, R)$ is called a partial order if it is reflective, transitive,and antisymmetric; $\underline{A}$ is called a strict partial order(a variant) if $\underline{A}$ is irreflective and transitive. $\underline{A}$ is called an order if it is a partial order and is connected. As a variant, $\underline{A}$ is called a strict order if it is a strict partial order and is connected.

In a familiar way, we often use $\leq$ as a variable, instead of R, when (A, R) is reflective, and $<$ when (A, R) is irreflective. Moreover, if we start with $(A, <)$, then we write $x \leq y$ to mean : $x < y$ or $x = y$; and if we start with $(A, \leq)$, then we write $x < y$ to mean $x \leq y$ and $x \neq y$.

If $\underline{A} = (A, \leq)$ is a partial order (or order), then $(A, <)$ is a strict partial order (resp.,strict order). On the other hand, if $(A, <)$ is a strict partial order (or strict order), then $(A, \leq)$ is a partial order(resp., order).

For any family Q of sets, consider the inclusion relation cut down to Q, i.e., the relation $\subseteq_Q = \{(A, B) : A, B \in Q \text{ and } A \subseteq B\}$.

theorem 1.18. $(Q, \subseteq_Q)$ is a partial order.

A family Q of sets which is ordered by $\subseteq_Q$ is called a chain.

theorem 1.19. Suppose (A, R) and (A', R') are strict orders, f is on A onto A' and 'order preserving', i.e., $f(x)R'f(y)$ whenever xRy. Then $(A, R) \underset{f}{\cong}$ (A', R')

If $\underline{B}$ is a substructure of $\underline{A}$ and $\underline{A}$ is a partial order, strict partial order, order, ore strict order, then so is $\underline{B}$. If (A, R) is a partial order, etc., as above, then so is $(A, \breve{R})$.

If $B \subseteq A$ and $x \in A$, we say that x is a minimal element of B if $x \in B$ and for all $y \in B, y \not< x$. On the other hand, we say x is a minimum element if $x \in B$ and for all $y \in B, x \leq y$. Also, x is called a lower bound for B if for all $y \in B, x \leq y$. The notions maximal, maximum, upper bounde are obtained by passing $\leq$ to $\geq$.

theorem 1.20. Let $\underline{A} = (A, \leq)$ be a partial order, and $B \subseteq A$.

1. 'minimum' implies 'minimal'(i.e., if x is a minimum element of B, then x is a minimal element of B)

2. $\underline{B}$ has at most one minimum element.

3. If $\underline{A}$ is an order, then 'minimum' = 'minimal'.(i.e., x is a minimum element of B if and only if x is a minimal element of B).

remark. There are incredible number of synonyms for 'minimum' in common usage - for example, least, smallest, first, leftmost...

In a partial order $(A, \leq)$, one says that x precedes y(or y succeed x)if $x < y$. In an order $(A <\leq)$, to say that y is an immediate successor of x means of course that y is a minimum (or equivalently, minimal) element of the set B of all successors of x. If it exists, then it is unique and x is then the immediate predecessor of y. x is a least upper bound (also called a 'supremum' or 'sup' for B)means that x is a least member of the set C of all bounds for B. Such an x is unique if it exists. One also write $x = \sup B = \sup_{u \in B} u$. Similarly B may have a greatest lower bound, or infimum, called $\inf B$.

Let $\underline{A} = (A, \leq)$ be an order. By an initial segment of $\underline{A}$ we mean any subset B of A such that for any x, y, if $x < y$ and $x \in B$ then $y \in B$. Each element of a of A determines two initial segments of $\underline{A}$, namely Pred$a$(in full, Pred $\underset{\underline{A}}{<} a) = \{x : x < a\}$,and Pred$\underset{\underline{A}}{\leq} a = \{x : x \leq a\}$. The substructures of $\underline{A}$ whose universe is Pred a will be called $\underline{A}_a$. An inital segment is called proper if $B \neq A$.

Given $U, V \subseteq A$ we say that U and V are cofinal(or confinal or coterminal,or that U is cofinal with V or that V is with U,) all in the sense of the order $\underline{A}$, if for any $x \in U$ there is a $y \in V$ such that $x \leq y$ and if $x \in V$ then for some $y \in U$, $x \leq y$.

$\underline{A}$ is called dense if it has at least two elements and for any x an y, if $x < y$, then for some z: $x < z < y$. $\underline{A}$ is called discrete if every element not a last element has an immediate successor and every element not a first has an immediate predecessor. $\underline{A}$ is called a well-order if every non-empty subset of A has a first element. Any substructures of a well-order is a well-order.

theorem 1.21. Let $\underline{A} = (A, \leq)$ be a well-order

1. If A is not empty, there is a first element.

2. Every element not a last has an immediate successor

3. Every proper initaial segment is of the form Pred a(for some a)

2 CARDINAL NUMBERS AND FINITE SETS

2.1 Cardinal numbers,+,and $\leq$

Cardinals or cardinal numbers are denoted by κ, λ and μ. It is common to say sometimes 'the power of A' instead of 'the cardinal number of A'. We can now define $0, 1, 2$ by putting $0 = \bar{\bar{\varnothing}} = 0; 1 = \overline{\overline{\{x\}}}, 2 = \overline{\overline{\{x,y\}}}$ if $x \neq y$.

theorem 2.1. $\bar{\bar{A}} = \bar{\bar{B}}$ if and only if $A \sim B$.

theorem 2.2.   1. If $A \sim A', B \sim B', A)(B, and A')(B'$,then $A \cup B \sim A' \cup B'$

2. For any X, Y there exists X', Y', disjoint, such that $X \sim X'$ and $Y \sim Y'$.

definition. $\kappa + \lambda =$the unique μ such that for some $A, B, \bar{\bar{A}} = \kappa, \bar{\bar{B}} = \lambda, A)(B,$ and $A \bar{\cup} B = \mu$

theorem 2.3.   1. $\kappa + \lambda = \lambda + \kappa$

2. $\kappa + (\lambda + \mu) = (\kappa + \lambda) + \mu$

3. $\kappa + 0 = \kappa$

4. If $\kappa \neq 0$ then for some $\lambda, \kappa = \lambda + 1$

5. If $\kappa + 1 = \lambda + 1$, then $\kappa = \lambda$

definition. We say that $\kappa \leq \lambda$ if for some $\mu, \lambda = \kappa + \mu$

theorem 2.4. The following are equivalent:

1. $\kappa \leq \lambda$

2. For some A, B, $\bar{\bar{A}} = \kappa$, $\bar{\bar{B}} = \lambda$, and $A \subseteq B$

3. For any set B of power λ there exists $A \subseteq B$ of power κ

4. For any A, B of respective powers κ, λ, there exists f one-to-one on A to B

5. For any set A of power κ there exists $B \supseteq A$ of power λ

theorem 2.5 (Exchange Principle)**.** For any X, Y there exists Z)(X such that $Z \sim Y$.

theorem 2.6.   1. $\kappa \leq \kappa$

2. If $\kappa < \lambda$ and $\lambda \leq \mu$ then $\kappa \leq \mu$

3. If $\kappa \leq \lambda$ then $\kappa + \mu \leq \lambda + \mu$

4. $0 \leq \kappa$

5. If $\kappa < \lambda$, then $\kappa + 1 \leq \lambda$

theorem 2.7. For any $\kappa, \{\lambda : \lambda \leq \kappa\}$ exists.

We write $\kappa \leq^* \lambda$ if, for some A, B, $\bar{\bar{A}} = \kappa$, $\bar{\bar{B}} = \lambda$, and there is a funciton f on B onto A (A is 'an image of B')or else $\kappa = \varnothing$.

theorem 2.8.   1. If $\kappa < \lambda$ then $\kappa \leq^* \lambda$

2. If $\kappa \leq^* \lambda$ then $\kappa \leq \lambda$

3. Suppose $\bar{\bar{B}} = \lambda$ and some R well-orders A. Then $\kappa \leq^* \lambda$ implies $\kappa \leq \lambda$.

2.2   Natural numbers and finite sets

definition. κ is a natural number if κ belongs to every set X such that $0 \in X$ and, for any λ, if $\lambda \in X$ then $\lambda + 1 \in X$.

We say A is finite if $\bar{\bar{A}}$ is a natural number; A is infinite otherwise.

theorem 2.9.   1. 0 is a natural number.

2. If κ is a natural number so is $\kappa + 1$

3. (Induction) Suppose that $\mathfrak{p}0$ ('$\mathfrak{p} holds for 0$'); and that, for any n, if $\mathfrak{p}n$ then $\mathfrak{p}(n + 1)$. Then for every $n, \mathfrak{p}n$.

theorem 2.10.   1. $m + n$ is a natural number

2. If $\kappa < n$ then κ is a natural number

3. If $\kappa + n = \lambda + n$ then $\kappa = \lambda$

4. Corollaries:

    - If $m \leq n$ then there is exactly one k such that $m + k = n$
    - A finite set is not equivalent to a proper subset of itself
    - $n < n + 1$
    - If $m \leq n$ and $n \leq m$ then $m = n$

5. $\kappa \leq n$ or $n \leq \kappa$

6. Corollaries:

    - $\leq$ 'orders' the natural numbers. In this 'order':
    - 0 is the first element
    - for each $n, n + 1$ is the immediate successor of n , and
    - each $n \neq 0$ has an immediate predecessor.

7. Put $W_n = \{m : m < n\}$. Then $\bar{\bar{W}}_n = n$. So every finite set A can be ordered.

8. If (A, R) is any order, every finite subset of A has a first element

    remark. So also a last. Hence every finite order is a well-order.

9. Any two orders $(A, \leq), (A', \leq')$ each on an n-element set are isomorphic.

10. If $\kappa \leq^* n$ then $\kappa \leq n$

remark. When we use greek letter κ, λ etc., we don't guarantee that they are finite, but when we use letters like n,j,k etc., we assume that they are finite.

theorem 2.11.   1. (The least element principle). If for some n, $\mathfrak{p}n$, then there is ia a minimal(which is here the same as minimum) n such that $\mathfrak{p}$n.

2. (Course-of-values induction) If, for any n, if $\mathfrak{Q}m$ holds for all $m < n$, then $\mathfrak{Q}n$; then, for all n, $\mathfrak{Q}n$.

By an n-termed sequence or synonymously, an ordered n-tuple of elements of A we mean a function s on W_n to A. We may sometimes write s_i instead of $s(i)$. The length of s is n. We say that R is an $n-$ary relation for A if $R \subseteq A^{W_n}$. o is called an $n-$ary operation for A if $o : A^{W_n} \to A$

2.3 Multiplication and exponentiation

theorem 2.12. If $A \sim A'$ and $B \sim B'$ then $A \times B \sim A' \times B'$

definition. $\kappa \cdot \lambda$(or just $\kappa\lambda$)= the unique μ such that, for some A, B, $\bar{\bar{A}} = \kappa, \bar{\bar{B}} = \lambda$, and $\overline{\overline{A \times B}} = \mu$.

theorem 2.13.   1. $\kappa\lambda = \lambda\kappa$

   2. $\kappa(\lambda\mu) = (\kappa\lambda)\mu$

   3. $\kappa(\lambda + \mu) = \kappa\lambda + \kappa\mu$

   4. $\kappa \cdot 0 = 0; \kappa \cdot 1 = \kappa; \kappa \cdot 2 = \kappa + \kappa$

   5. If $\kappa\lambda = 0$ then $\kappa = 0$ or $\lambda = 0$.

   6. If $\kappa \leq \lambda$ then $\kappa\mu \leq \lambda\mu$.

   7. If $\kappa, \kappa \geq 2$ then $\kappa + \lambda \leq \kappa \cdot \lambda$

   8. $m \cdot n$ is a natural number

   9. If $m \neq 0$ and $n < p$ then $mn < mp$(so, if $m \neq 0$ and $mn = mp$ then $n = p$)

theorem 2.14. If $A \sim A'$ and $B \sim B'$, then $A^B \sim A'^{B'}$

definition. κ^λ= the unique μ such that for some $A, B, \bar{\bar{A}} = \kappa, \bar{\bar{B}} = \lambda$, and $\mu = \bar{\bar{A^B}}$.

theorem 2.15.   1. $(\kappa^\lambda)^\mu = \kappa^{\lambda\mu}$

   2. $\kappa^{\lambda+\mu} = \kappa^\lambda \kappa^\mu$

   3. $(\kappa\lambda)^\mu = \kappa^\mu \lambda^\mu$

   4. $\kappa^0 = 1; \kappa^1 = \kappa; \kappa^2 = \kappa\kappa$; and if $\kappa \neq 0$ then $0^\kappa = 0$

   5. If $\kappa \leq \lambda$ then $\kappa^\mu \leq \lambda^\mu$

   6. If $\kappa \leq \lambda$ then $\mu^\kappa \leq \mu^\lambda$ unless $\kappa = \mu = 0 < \lambda$

   7. If $\bar{\bar{A}} = \kappa$, the $\overline{\overline{P(A)}} = 2^\kappa$

   8. $\kappa \leq 2^\kappa$

   9. m^n is a natural number.

2.4 Definition by induction

theorem 2.16.   1. If f works for n and $k < n$, then $f \upharpoonright W_{k+1}$ works for k.

    remark. 'work for' means that it satisfy the condition in theorem 2.17.1

  2. If $\mathfrak{B}_0 = a$ and for all $n, \mathfrak{n} + \mathbf{1} = \mathfrak{a}_{\mathfrak{B}_n}$, then $(\mathfrak{B}_i : i \leq k)$ works for k.

definition. $D_x(\mathfrak{a}_x, a, n) = $ the unique z such that for some f on $W_{n+1}, f(0) = a, f(i+1) = \mathfrak{a}_{f(i)}$ for all $i < n$, and $f(n) = z$.

theorem 2.17 (Definition by induction).   1. There is exactly one f such that f is on $W_{q+1}, f(0) = a$, and $f(n+1) = \mathfrak{a}_{f(n)}$ for all $n < q$.

  2. $\mathfrak{B}_0 = a$ and for all $n, \mathfrak{B}_{n+1} = \mathfrak{a}_{\mathfrak{B}_n}$, and it also hold for $\mathfrak{C}$, then, for all $n, \mathfrak{B}_n = \mathfrak{C}_n$.

  3. $D_x(\mathfrak{a}, a, 0) = a.D_x(\mathfrak{a}, a, n+1) = \mathfrak{a}_{D_x(\mathfrak{a}_x, a, n)}$

theorem 2.18. We can justibly introduce by recursion a notion $\mathfrak{B}$ by requiring that

$$\mathfrak{B}_n = \mathfrak{C}((\mathfrak{B} : j < n))\text{for all } n$$

remark. It means that, we use some transformation $\mathfrak{C}$ on $(\mathfrak{B} : j < n)$ to give out $\mathfrak{B}_n$, which is a course-of-values form of recursion.

theorem 2.19. If N exists, then in fact there is exactly one function F on N such that $F(0) = c$. and for all $n, F(n+1) = \mathfrak{a}_{f(n)}$.

2.5 Axiom of infinity, Peano axioms, Dedekind infinite sets

An algebraic structure (A, S, z) where $z \in A, S : A \to A$ is called a Peano structure if (P1) for any $a \in A, Sa \neq z$;(P2) S is one-to-one; and (P3) for any subset B of A, if $z \in B$ and $Sa \in B$, whenever $a \in B$, then $B = A$.(These are the famous Peano axioms)

Axiom 5 (Axiom of Infinity). There exists a Peano structure.

theorem 2.20. The following are equivalent(forms of the Axiom of Infinity)

1. There exists a Peano structure;

2. There exists an infinite set;

3. N exists;

  We put $\aleph_0 = \bar{\bar{N}}$.

theorem 2.21. If κ is infinite, then $\aleph_0 \leq \kappa$

theorem 2.22. (A,S,z) is a Peano structure if and only if $(A, S, z) \cong (N, Sc, 0)$

A cardinal κ is called Dedekind infinite if $\kappa \geq \aleph_0$,

3 THE NUMBER SYSTEMS

3.1 Introductory remarks

We call structure $(N, +, \cdot, 0, 1, <)$ which we call $\underline{N}$. Let us say that $\underline{A} = (A, +, \cdot, 0, 1, <)$ is a Peano semiring if: $(A, S, 0)$ is a Peano system, where $Sa = a + 1$ for any $a \in A$; for any $a, b \in A, a < b$ if and only if for some $c \neq 0, b = a + c$, and also

$$\begin{cases} a + 0 = a \\ a + (b + 1) = (a + b) + 1 \end{cases} \text{and} \begin{cases} a \cdot 0 = 0 \\ a \cdot (b + 1) = a \cdot b + a \end{cases}$$

theorem 3.1. $\underline{A}$ is a Peano semiring if and only if $\underline{A}$ is isomorphic to $\underline{N} = (N, +, \cdot, 0, 1, <)$

It follows that any Peano semiring obeys the following rich list of laws (which should be taken as restricted to the natural numbers): 2.3.,2.4.1.,2.4.3.,2.10.3.-2.10.9. and 2.13.

3.2 Construction and characerization up to isomorphism of the integers, rationals, and reals

We define the notion $n \circ a$ by recursion, specifying that $0 \circ a = 0$ and $(n + 1) \circ a = n \circ a + a$, for any $a \in A$.

theorem 3.2. There exists one and up to isomorphism only one ordered intergral domain $\underline{Z} = (Z, +, \cdot, 0, 1, <)$ such that every element x of Z if of the form $n \circ 1$ or $-(n \circ 1)$ (where $n \in N$).

If $(A, +, \cdot, 0, 1, <)$ is an ordered integral domain, $a \in A$, and $i = n$ or $i = -n$ we put $i \circ a = n \circ a$ or $-(n \circ a)$,respectively.

theorem 3.3. There is one and up to isomorphism only one ordered field $\underline{Q} = (Q, +, \cdot, 0, 1, <)$ such that every element of Q is of the form $(i \circ 1)/(j \circ 1)$(where $i, j \in Z$ and $j \neq 0$.)

theorem 3.4. There is one and up to isomorphism only one Complete ordered field $\underline{R} = (R, +, \cdot, 0, 1, <)$

4 MORE ON CARDINAL NUMBERS

4.1 The Cantor-Bernstein Theorem

theorem 4.1 (Cantor-Bernstein)**.** If $\kappa \leq \lambda$ and $\lambda \leq \kappa$ then $\kappa = \lambda$

4.2 Infinite sums and products of cardinal

Axiom 6. Suppose for each $i \in I$, there is an x such that $\mathcal{P}(i, x)$. Then there exists f on I such that, for each $i \in I, \mathcal{P}(i, f(i))$.

theorem 4.2. Given $(\kappa_i : i \in I)$, there exists F on I such that $\overline{\overline{F(i)}} = \kappa_i$ for each $i \in I$.

theorem 4.3.   1. If F and G are both disjointed and on I and for each $i \in I, F(i) \sim G(i)$, then $\bigcup_{i \in I} F(i) \sim \bigcup_{i \in I} G(i)$

2. For any F on I there exists a disjointed G on I such that for each $i \in I, F(i) \sim G(i)$.

definition. $\sum_{i \in I} \kappa_i$ is the unique μ such that there exists a disjointed F on I such that, for each $i \in I, \overline{\overline{F(i)}} = \kappa_i$, and $\mu = \bigcup_{i \in I} F(i)$

theorem 4.4. If F and G are on I and for each $i \in I, F(i) \sim G(i)$, then $\prod_{i \in I} F(i) \sim \prod_{i \in I} G(i)$

definition. $\prod_{i \in I} \kappa_i$ is the unique μ such that there exists F on I such that for each $i \in I, \overline{\overline{F(i)}} = \kappa_i$, and $\overline{\overline{\prod_{i \in I} F(i)}} = \mu$.

theorem 4.5.   1. (General communicative law) Let $I \underset{f}{\sim} J$. Then $\sum_{j \in J} \kappa_j = \sum_{i \in I} \kappa_{f(i)}$(Likewise for $\prod$)

2. (General associative law)
$$\sum_{i \in I} \sum_{j \in J_i} \kappa_{ij} = \sum_{(i,j) \in W} \kappa_{ij},$$

where $W = \{(i, j) : i \in I \text{ and } j \in J_i\}$.(Likewise for $\prod$)

3. (General distributive law) $\kappa \cdot \sum_{i \in I} \lambda_i = \sum_{i \in I} (\kappa \lambda_i)$;
$$\prod_{i \in I} \sum_{j \in J_i} \kappa_{ij} = \sum_{h \in \prod_{i \in I} J_i} \prod_{i \in I} \kappa_{ih(i)}$$

4. $\sum_{i \in \{0,1\}} \kappa_i = \kappa_0 + \kappa_1$ and $\prod_{i \in \{0,1\}} \kappa_i = \kappa_0 \cdot \kappa_1$; $\sum_{i \in I} \kappa = \kappa \cdot \bar{\bar{I}}$ and $\prod_{i \in I} \kappa = \kappa^{\bar{\bar{I}}}$.
   remark. Thus $1 + 1 + 1 + \cdots = \sum_{n \in N} 1 = \aleph_0$ and $2 \cdot 2 \cdot 2 \cdots = 2^{\aleph_0}$.

5. If $J \subseteq I$ and $\kappa_i = 0$ for all $i \in I - J$, then $\sum_{i \in I} \kappa_i = \sum_{i \in J} \kappa_i$; and likewise for 1 and $\prod$

theorem 4.6.   1. If, for all $i \in I, \kappa_i \leq \lambda_i$, then $\sum_{i \in I} \lambda_i$ and $\prod_{i \in I} \kappa \leq \prod_{i \in I} \lambda_i$

17

2. If $\lambda \in Q$ then $\lambda \leq \sum_{\kappa \in Q} \kappa$

   remark. Hence every set of cardinals is bounded above.

3. $\kappa^{\sum_{i \in I} \lambda_i} = \prod_{i \in I} \kappa^{\lambda_i}$

4. $(\prod_{i \in I} \kappa_i)^{\lambda} = \prod_{i \in I} \kappa_i^{\lambda}$

theorem 4.7. If $\kappa_i \geq 2$ for all $i \in I$, then $\sum_{i \in I} \kappa_i \leq \prod_{i \in I} \kappa_i$.

4.3 Different kinds of infinity

theorem 4.8 (Cantor's Theorem). $\kappa < 2^{\kappa}$

theorem 4.9 (The Konig-Zermole Theorem). If, for each $i \in I, \kappa_i < \lambda_i$, then $\sum_{i \in I} \kappa_i < \prod_{i \in I} \lambda_i$

4.4 $\aleph_0, 2^{\aleph_0}$, and $2^{2^{\aleph_0}}$- the simplest infinite cardinals

A set A is called denumerable if $\bar{\bar{A}} = \aleph_0$, and countable if $\bar{\bar{A}} \leq \aleph_0$.

theorem 4.10. A is countable if and only if A is denumerable or finite.

theorem 4.11. If $\kappa \leq^* \aleph_0$, then κ ia countable.

theorem 4.12. The sets Z (of integers) and Q (of rationals) are denumerable. Also
$$\aleph_0 = \aleph_0 + \aleph_0 = \aleph_0 \cdot n = \aleph_0 \cdot \aleph_0 = \aleph_0^n = \overline{\overline{Sq}},$$
where $Sq = \bigcup_{n \in N} N^{W_n} =$ the set of all finite sequences of natural numbers.

A real number is called algebraic if it is a root of some polynomial with rational coefficients not all zero.

theorem 4.13. The set Alg of all real algebraic numbers is countable.

theorem 4.14. A countable union of countable sets is countable.

The set R is sometimes called the continum, and its cardinal number is denoted by $\mathfrak{c}$.

theorem 4.15. $2^{\aleph_0} = \mathfrak{c}$

theorem 4.16. There exists transcendental real numbers.(i.e., reals which are not algebraic.)

theorem 4.17. $\mathfrak{c} = \mathfrak{c} + \mathfrak{c} = \mathfrak{c} \cdot \mathfrak{c} = \mathfrak{c}^n = \mathfrak{c}^{\aleph_0}$

theorem 4.18. $\mathfrak{c}^{\mathfrak{c}} = 2^{\mathfrak{c}}$

5 ORDERS AND ORDER TYPES

5.1 Ordered sums and products

The ordered sum of two orders can be defined in a natural way. If the orders $\underline{A} = (A, \leq)$ and $\underline{A}' = (A', \leq')$ are disjoint, then, their ordered sum $\underline{A} + \underline{A}'$ is the structure $(A \cup A', \leq'')$, where,

$$x \leq'' y \text{ if and only if } x \leq y \text{ or } x \leq' y \text{ or } (x \in A \text{ and } y \in A')$$

Let $\underline{I} = (I, \leq)$ be an order and suppose $(\underline{A_i} : i \in I)$ is a disjointed indexed family of orders (where each $\underline{A_i} = (A_i, \leq_i)$). Then, we defined the ordered sum $\sum_{i \in \underline{I}} \underline{A_i}$ to be $(\bigcup_{i \in I} A_i, \leq)$, where, $x \leq y$ if and only if for the determined i, j such that $x \in A_i$ and $y \in A_j$, either $i < j$ or else $(i = j$ and $x \leq_i y)$

If $\underline{A}$ and $\underline{B}$ are orders, the ordered product $\underline{A} \cdot \underline{B}$ can be defined to be $\sum_{b \in B} \underline{A}$

It is convenient to allow the case where the given $(\underline{A_i} : i \in I)$ is not disjointed. In this case, we put $\sum_{i \in \underline{I}} A_i = \sum_{i \in \underline{I}} A_i'$, where $\underline{A}' = (A_i', \leq_i')$, $A_i' = \{i\} \times A_i$, and of course, $(i, a) \leq_i' (i, b)$ if and only if $a \leq_i b$. Thus, $\underline{A} \cdot \underline{B}$ is just the the set $A \times B$ of "two letter words"(a,b) under the antilexograhic order.

* take A 'turn around', i.e., given $\underline{A} = (A, \leq)$, we have $A^* = (A, \geq)$

theorem 5.1. 1. If $\underline{I} = (I, \leq)$ is a well order and for each $i \in I, \underline{A_i}$ is a well order, then $\sum_{i \in \underline{I}} \underline{A_i}$ is a well-order.

2. If $\underline{A}$ and $\underline{B}$ are well-orders so are $\underline{A} + \underline{B}$ and $\underline{A} \cdot \underline{B}$.

5.2 Order types

Each order $\underline{A}$ corresponds something called Tp $\underline{A}$(the order-type of $\underline{A}$). Tp $\underline{A}$= Tp $\underline{B}$ if and only if $\underline{A} \cong \underline{B}$. Moreover, for convenience, we assume also that if the order $\underline{A}$ has finite cardinal n, then, Tp $\underline{A} = n$.

Order types are denoted by ρ, σ, τ. Order types of well-orders $\underline{A}$ are called ordinals and we write $\underline{A} =$Ord $\underline{A}$. We let $\omega =$Tp $(N, \leq); \eta =$Tp $(Q, \leq)$; and $\lambda =$Tp $(R, \leq)$.

theorem 5.2. If $\underline{A}, \underline{A}', \underline{B}, \underline{B}'$ are orders, $\underline{A} \cong \underline{A}'$ and $\underline{B} \cong \underline{B}'$, then $\underline{A} + \underline{B} \cong \underline{A}' + \underline{B}', \underline{A} \cdot \underline{B} \cong \underline{A}' \cdot \underline{B}'$, and $\underline{A}^* \cong \underline{B}^*$.(For +, assume $\underline{A})(\underline{B}$ and $\underline{A}')(\underline{B}')$

definition. $\sigma + \tau($ or $\sigma \cdot \tau)$ is the unique ρ such that for some (disjoint for +) orders $\underline{A}, \underline{B},$Tp $\underline{A} = \sigma,$Tp $\underline{B} = \tau$ and $\rho =$Tp$(\underline{A} + \underline{B})$(respectively, $\underline{A} \cdot \underline{B}).\sigma^*$ is defined similarly.

For any ordinal α and $\beta, \alpha + \beta$ and $\alpha \cdot \beta$ are ordinals.

theorem 5.3. Assume AC,

1. For any $(\sigma_i : i \in I)$ there exist orders $(\underline{A}_i : i \in I)$ such that Tp $\underline{A}_i = \sigma_i$ for each $i \in I$.

2. If the orders $\underline{A}_i$ and $\underline{A}'_i$ are isomorphic for each $i \in I$ and $\underline{I} = (I, \leq)$ is an order, then $\sum_{i \in \underline{I}} \underline{A}_i \cong \sum_{i \in \underline{I}} \underline{A}'_i$

definition. If $\underline{I}$ is an order, $\sum_{i \in \underline{I}} \sigma_i$ is the unique ρ such that for some orders $(\underline{A}_i : i \in I)$, Tp $\underline{A}_i = \sigma_i$ for each $i \in I$ and $\rho =$ Tp$(\sum_{i \in I} \underline{A}_i)$.

Here are some distinct ordinals:

$$0, 1, 2, \cdots, \omega, \omega + 1, \cdots, \omega \cdot 2 (= \omega + \omega), \cdots, \omega \cdot 3, \cdots, \omega \cdot \omega, \cdots$$

theorem 5.4. For $+, \cdot,$ and $\sum$ over order types,

1. Associative laws for $+$ and $\cdot$

2. communicative laws fail for $+$ and $\cdot$

3. $\sigma(\tau + \tau') = \sigma\tau + \sigma\tau'$

4. But the law $(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma$ fails, even for ordinals.

5. (1) and (3) extend suitably to $\sum$, assuming AC.

6. $(\sigma + \tau)^* = \tau^* + \sigma^*$ and $(\sigma \cdot \tau)^* = \sigma^* \cdot \tau^*$

If the order $\underline{A} = (A, \leq)$ and $\underline{A}' = (A', \leq')$ have the same type σ, then A and A' have the same cardinal; we define $\bar{\bar{\sigma}}$ to be this cardinal. Clearly $\overline{\overline{\sigma + \tau}} = \bar{\bar{\sigma}} + \bar{\bar{\tau}}$ and $\overline{\overline{\sigma \cdot \tau}} = \bar{\bar{\sigma}} \cdot \bar{\bar{\tau}}$

theorem 5.5.   1. Any two denumerable dense orders without first or last elements are isomorphic (and hence of type η)

2. Let $\underline{A}'$ have type η. Then, every countable order $(A, \leq)$ is isomorphic to a suborder (i.e., substructure) of $\underline{A}'$

6   AXIOMATIC SET THEORY

6.1   A formalized language

Axiom 7 (Empty Set Axiom)**.** There is exactly one x such that, for any $y, y \notin x$.

We take the following as convention

$$y = \iota x \mathcal{P} x \leftrightarrow [\exists! x \mathcal{P} x \wedge \mathcal{P} y] \vee [\sim \exists! x \mathcal{P} x \wedge \forall z (z \notin y)].$$

6.2 The axioms of set theory

We list the axioms of ZFC below.

1. (Empty Set Axiom) There is exactly one x such that, for any $y, y \notin x$

2. (Extensionality Axiom) If, for any x,$x \in A$ if and only if $x \in B$, then $A = B$.

3. (Separation Axiom) $\{x : x \in B \wedge \mathcal{P}x\}$exists

4. (Doubleton) $\{t : t = x \text{ or } t = y\}$exists.

5. (Union Axiom) $\{x : \text{for some } A, x \in A \text{ and } A \in W\}$exists.(That is, $\bigcup_{A \in W} A$exists)

6. (Power Set Axiom) $\{B : \text{for every } x \in B, x \in A\}$ exists.(That is, $P(A)$ exists)

   remark. The axioms listed so far constitue the theory of axiom system denoted by Z_0.

7. (Replacement Axiom) $\{\mathfrak{a}_x : x \in A\}$ exists.

8. (Axiom of Infinity)

9. (Axiom of Choice)

10. (Axiom of Regularity)

Thus the theory ZFC has been described. The theory Z consists of Z_0 plus Infiity and Regularity. ZF is Z plus F, meaning the Axiom of Replacement. ZFC is ZF plus Choice, 'C' standing for Choice.

theorem 6.1. One can drop from Z_0F both Separation and Doubleton and still derive them.

theorem 6.2. $\{x : \mathcal{P}x\}$ exists if there is a 'big enough B',i.e., a B such that $x \in B$ whenever $\mathcal{P}$x.

theorem 6.3. We establish the existence of the following sets: First, directly, from axioms: $\varnothing; \{x \in A : \mathcal{P}x\}; \{\mathfrak{a}_x : x \in A\}; \bigcup(W); \mathfrak{P}(A); \{x, y\}$. Hence easily $\{x\}, \bigcup_{i \in I} \mathfrak{a}_i, (x, y)$ and $(\mathfrak{a}_x : x \in X)$. Next: $A \cap B$ and $A - B; A \cup B = \bigcup(\{A, B\}); A \ominus B = (A - B)\bigcup(B - A); \bigcap_{i \in I} \mathfrak{a}_i$ if $I \neq \varnothing$. Now $A \times B$ and Dom R. Next, easily, Range $R, R[A]$. Then R/S, and $f \upharpoonright A$. Finally, A^B and $\prod_{i \in I} \mathfrak{a}_i$.

7 WELL-ORDERINGS,ORDINALS AND CAR-DINALS

7.1 Well-orders

In a well-order $\underline{A}$, every element x is clearly of just one of these three kinds: x is the first element; x is a successor element - i.e., x has an immediate predecessor.

Let $\underline{A} = (A, \leq)$ be any well-order and $u \notin A$. Let B be the ordered sum of $\underline{A}$ and the order with universe $\{u\}$. Then $\underline{B}$ is a well-order, and clearly $\underline{A} = \underline{B}_u$. We have the fact that every well-order $\underline{A}$ is of the form $\underline{B}_u$ for some well-order $\underline{B}$ and some u.

theorem 7.1. Suppose $\underline{A} = (A, \leq)$ is a well-order and $f : A \to A$ is increasing or, what is the same, order preserving(i.e., $f(x) < f(y)$ whenever $x < y$). Then for every $x \in A, f(x) \geq x$.

theorem 7.2. No well-order is isomorphic to (even a substructure of) a proper initial segment of itself.

An order (or indeed any structure) $\underline{A} = (A, \cdots)$ is called rigid if it has no automorphisms except Id_A.(An automorphism of $\underline{A}$ is an $(\underline{A}, \underline{A})-$isomorphism)

theorem 7.3. Any well-order $\underline{A} = (A, \leq)$ is rigid.

theorem 7.4. For any well-orders $\underline{A}$ and $\underline{B}$, at most one of the following holds:

1. $\underline{A}$ is isomorphic to a proper initial segment of $\underline{B}$

2. $\underline{B}$ is isomorphic to a proper initial segment of $\underline{A}$

3. $\underline{A} \cong \underline{B}$.

Moreover, in each of (1)=(3) the corresponding map is unique.

theorem 7.5 (Comparison Theorem for Well-orders)**.** Of any well-orders $\underline{A}$ and $\underline{B}$, one is isomorphic to an initial segment of the other.

theorem 7.6. Suppose $\underline{B}$ is any substructure of the well-order $\underline{A}$. Then $\underline{B}$ is isomorphic to an initial segment of $\underline{A}$.

Consider two assertion about an order $\underline{A} = (A, \leq)$

1. If B is any non-empty subset of A, then it has a minimal element.

2. If C is any subset of A, and, for each $a \in A$, if $x \in C$ for all $x < a$, then $a \in C$, then for all $a \in A, a \in C$.(Induction Principle)

According to these two assertion, we can prove that

theorem 7.7. Every well-order satisfies the induction principle(by the very definition of 'well-order').

Proof. Prove by contradiction. Suppose $\underline{A}$ is well-ordered and for each a in A, if $x \in C$, for all $x < a$ then $a \in C$. By the axiom of seperation, the set $B = \{x \in A : x \notin C\}$ exists, which is also a subset of A. Thus, B is also well-ordered and has a minimal element b. For any $a \in A, a < b, a \notin B$. Thus, $a \in C$ and $b \in C$, which is contrary to $b \in B$. Therefore $B = \varnothing$ and each $a \in A, a \in C$. $\qquad\square$

theorem 7.8 (Recursion over a fixed well-order)**.** ($\mathfrak{a}$ is given.)Let $\underline{A} = (A, \leq)$ be a well-order. Then, there is exactly one f such that f is a function on A and for each $a \in A$, $f(a) = \mathfrak{a}_{f \restriction \mathrm{Pred}\ a}$

theorem 7.9. We can introduce a notion $\mathfrak{O}(\underline{A})$(defined for all well-orders $\underline{A}$) by saying:"$\mathfrak{O}$ is defined recursively by requiring that: $\mathfrak{O}(\underline{A}) = \mathfrak{a}_{\{\mathfrak{O}(\underline{A}_a) : a \in A\}}$ for each well-order $\underline{A} = (A, \leq)$"

Let $\mathfrak{O}$ be defined recursively by previous way. If $\underline{A} \cong \underline{A}'$(both being well-orders) then $\mathfrak{O}(\underline{A}) = \mathfrak{O}(\underline{A}')$

7.2 Von Neumann ordinals

definition. We define Ord $\underline{A}$, for all well-order $\underline{A}$, by recursion,by requiring for any well-order $\underline{A} = (A, \leq)$:

$$\mathrm{Ord}\ \underline{A} = \{\mathrm{Ord}\ \underline{A}_a : a \in A\}.$$

theorem 7.10. If $\underline{A}$ and $\underline{B}$ are well-orders and $\underline{A} \cong \underline{B}$, then Ord $\underline{A} \cong=$ Ord $\underline{B}$.

$\alpha, \beta, \gamma, \epsilon$ range over ordinals.

theorem 7.11. $\alpha \notin \alpha$

theorem 7.12. If Ord $\underline{A} =$ Ord $\underline{B}$ ($\underline{A}, \underline{B}$ well-orders) then $\underline{A} \cong \underline{B}$.

definition. We say that $\alpha < \beta$ if for some well-orders $\underline{A}$ and $\underline{B}$, Ord $\underline{A} = \alpha$, Ord $\underline{B} = \beta$ and $\underline{A}$ is a proper initial segment of $\underline{B}$.

theorem 7.13. ¡'strictly orders' the ordinals. That is:

1. $\alpha \not< \alpha$;

2. If $\alpha < \beta$ and $\beta < \gamma$ then $\alpha < \gamma$;

3. $\alpha \leq \beta$ or $\beta \leq \alpha$

For any α, put $W(\alpha) = \{\beta : \beta < \alpha\}$. If $\alpha =$ Ord $\underline{A}$ then $W(\alpha)\{\mathrm{Ord}\ \underline{A}_a : a \in A\}$.Thus, by the Replacement Axiom:

theorem 7.14. $W(\alpha)$ exists.

Write $\underline{W}(\alpha) = (W(\alpha), \leq_{W(\alpha)})$.

theorem 7.15. $\underline{W}(\alpha)$ is a well-order and Ord $\underline{W}(\alpha) = \alpha$. Indeed, if Ord $\underline{A} = \alpha$, then $\underline{A} \cong_{f} \underline{W}(\alpha)$, where $f(a) = $ Ord $\underline{A}_a$ for each a in $\underline{A}$.

theorem 7.16. If for some $\alpha, \mathcal{P}\alpha$, then, there is a least α such that $\mathcal{P}\alpha$.

theorem 7.17 (Induction over all ordinals). Suppose that, for all α, if $\mathcal{P}\beta$ for all $\beta < \alpha$, then $\mathcal{P}\alpha$. Then, for all $\alpha, \mathcal{P}\alpha$.

theorem 7.18 (Recursion over all ordinals). We can (justifiably) introduce a notion $\mathfrak{O}(\alpha)$ (over all α) by saying that: $\mathfrak{O}(\alpha)$ is defined recursively by requiring that for each $\alpha, \mathfrak{O}(\alpha) = \mathfrak{a}_{\mathfrak{O}\beta:\beta<\alpha}$

theorem 7.19.   1. (Burali=Forti) The set of all ordinals does not exist.

2. Every set K of ordinals is bounded above.

theorem 7.20. $\alpha = \{\beta : \beta < \alpha\}$

theorem 7.21.   1. $0 = \varnothing$

2. $\beta < \alpha$ if and only if $\beta \in \alpha$

3. Every member of an ordinal is an ordinal.

4. α is a transitive set - that is, for any x, y, if $x \in y \in \alpha$ then $x \in \alpha$)

theorem 7.22. x is an ordinal if and only if x is a transitive set and $(x, \in_x)$ is a well-order.

7.3   The well-ordering theorem

theorem 7.23 (Well-ordering Principle). Every set A can be well-ordered (that is, for some $\leq, (A, \leq)$ is a well-order). Obviously equivalent is: For any A there exists α such that $A \sim \alpha$.

theorem 7.24. The Well-ordering Principle implies AC.

theorem 7.25 (Zorn's Lemma). Ler $\underline{A} = (A, \leq)$ be a partial order, and suppose that every subset B of A which is ordered by $\leq$ has an upper bound. Then, $\underline{A}$ has a maximal member.

theorem 7.26. Zorn's Lemma is equivalent to AC.

7.4 Defining $\overline{\overline{A}}$ and Tp$\underline{A}$

definition. We put $\overline{\overline{A}}$ = the least ordinal α such that $A \sim \alpha$.

theorem 7.27. $\overline{\overline{A}} = \overline{\overline{B}}$ if and only if $A \sim B$.

An ordinal α is called an initial ordinal if α is not set-theoretically equivalent to any smaller ordinal. Obviously, α is a cardinal if and only if α is an initial ordinal.

It is clear that

$$\overline{\overline{\kappa}} = \kappa$$

theorem 7.28. Given $(\kappa_i : i \in I)$, there exists F on I such that for each $i \in I, \overline{\overline{F(i)}} = \kappa_i$. (take $f(i) = \kappa_i$)

definition. Let $\underline{A}$ be an order of power κ. If $\underline{A}$ is not a well-order, put Tp$\underline{A}$ = the set of all order (κ, R) isomorphic to $\underline{A}$; and if $\underline{A}$ is a well-order, put Tp $\underline{A}$ =Ord $\underline{A}$

theorem 7.29. For any orders $\underline{A}, \underline{B}$, Tp $\underline{A}$=Tp $\underline{B}$ if and only if $\underline{A} \cong \underline{B}$.

theorem 7.30. If $\underline{A} = (A, \leq)$ is an order and $\overline{\overline{A}} = n$, then Tp $\underline{A} = n$

7.5 Easy consequences for cardinals of the Well-ordering Principle

theorem 7.31. $\kappa \leq \lambda$(card) if and only if $\kappa \leq \lambda$(ord).

By theorem 7.31., the cardinals with their natural order are a 'suborder' of the usual ordering of the ordinals.

What's more, we see at once that: Every non-empty set (or even 'class') of cardinals has a least member. In particular, for any κ, since there is a larger cardinal, namely 2^κ, there is an immediate successor of κ (among cardinals); it is denoted by κ^+.

remark. Because every cardinal is a initial ordinal, by theorem 7.16., there is a least one. What's more, the initial ordinals that is greater than κ also has a least one, which is denoted by κ^+.

theorem 7.32 (Cantor-Bernstein)**.** If $\kappa \leq \lambda$ and $\lambda \leq \kappa$ then $\kappa = \lambda$.

theorem 7.33 (Comparability of cardinals)**.** $\kappa \leq \lambda$ or $\lambda \leq \kappa$

We define the cardinals $\aleph_\alpha$ for all α by recursion, putting

$\aleph_\alpha$ = the first infinite cardinal greater than $\aleph_\beta$ for all $\beta < \alpha$

theorem 7.34. Every infinite κ is an 'aleph'(i.e., is of the form $\aleph_\alpha$).

remark. To solve the ambiguity of cardinal + and ordinal +(and likewise for $\cdot$), we let $\aleph_\alpha + \aleph_\beta$ mean the cardinal sum, but $\omega_\alpha + \omega_\beta$ means the ordinal.

7.6 A harder consequences and its corollaries

theorem 7.35. If κ is infinite, then $\kappa \cdot \kappa = \kappa$

theorem 7.36. 1. If κ is infinite then $\kappa + \kappa = \kappa$

2. If at least one of κ and λ is infinite, then

$$\kappa + \lambda = \kappa \cdot \lambda = \max(\kappa, \lambda)$$

theorem 7.37. If κ is infinite, then

1. $(2^\kappa)^\kappa = 2^\kappa$

2. $\kappa^\kappa = 2^\kappa$

theorem 7.38. If κ is infinite, $\overline{\overline{I}} \leq \kappa$, and $\lambda_i \leq \kappa$ for each $i \in I$, then, $\sum_{i \in I} \lambda_i \leq \kappa$.

theorem 7.39. Let κ be infinite.

1. Suppose $\kappa = \sup_{\alpha \in Q} \alpha$ where $Q \subseteq \kappa$, (in other words, Q is a cofinal subset of κ)then $\kappa = \sum_{\alpha \in Q} \overline{\overline{\alpha}}$

2. Suppose $\sum_{i \in I} \lambda_i = \kappa$ where $\overline{\overline{I}} < \kappa$ and, for each $i \in I, \lambda_i < \kappa$. Put $Q = \{\lambda_i : i \in I\}$. Then $\kappa = \sup_{i \in I} \lambda_i$

An infinite cardinal λ is called regular if λ has no cofinal subset of power less than λ (otherwise, λ is singular). By theorem 7.39. we can also say: λ is regular if and only if λ cannot be expressed as a sum of fewer than λ cardinals each less than λ.

Then $\aleph_0$ is regular, and

theorem 7.40. If κ is infinite, then κ^+ is regular.

The remaining cardinals are the limit cardinals greater than $\aleph_0$. The first one $\aleph_\omega$ is singular, since $\aleph_\omega = \sum_{n \in \omega} \aleph_n$. In general, if α is a countable limit ordinal, then $\aleph_\alpha$ is singular.

Regular limit cardianls are also called weakly inaccessible. An infinite cardinal κ is called inaccessible if κ is regular and $2^\lambda < \kappa$ whenever $\lambda < \kappa$.

8 THE AXIOM OF REGULARITY

8.1 Partial universe and the axiom of regularity

By recursion, put

$$\begin{cases} V_0 = \varnothing \\ V_{\alpha+1} = P(V_\alpha) \text{ for any ordinal } \alpha \\ V_\delta = \cup_{\alpha < \delta} V_\alpha \text{ for any limit ordinal } \delta \end{cases}$$

Set of the form V_δ will be called partial universe. We write Vx to mean that for some $\alpha, x \in V_\alpha$.

theorem 8.1.   1. V_α is a transitive set (i.e., if $x \in y \in V_\alpha$ then $x \in V_\alpha$).

2. If $\alpha < \beta$ then $V_\alpha \subseteq V_\beta$.

3. V_α is supertransitive (i.e., transitive and if $x \subseteq y \in V_\alpha$ then $x \in V_\alpha$)

4. The predicate V is 'supertransitive'; i.e, if $x \in y$ or $x \subseteq y$, and Vy then Vx.

If Vx then we put Rk x, the rank of x, equal to the least α such that $x \in V_{\alpha+1}$(or, what is the same, $x \subseteq V_\alpha$).

theorem 8.2.   1. If Vx, Vy, and $x \in y$, then Rk $x <$ Rk y.

2. $V_\alpha = \{x : Vx \text{ and } \mathrm{Rk}x < \alpha\}$.

3. For any ordinal $\alpha, V\alpha$ and Rk $\alpha = \alpha$

theorem 8.3. If, for any $y \in x, Vy$, then Vx.