Set Theory Notes

by Tyler Wright

github.com/Fluxanoia fluxanoia.co.uk

These notes are not necessarily correct, consistent, representative of the course as it stands today, or rigorous. Any result of the above is not the author's fault.

These notes are in progress.

0 Notation

We commonly deal with the following concepts in Set Theory which I will abbreviate as follows for brevity:

Term	Notation
$\{0, 1, 2, \ldots\}$	$\mathbb{N}$

Contents

1 The Fundamentals

1.1 Axiom of Extensionality

For two sets a and b, we have that $a = b$ if and only if for all x we have that:

$$x \in a \Longleftrightarrow x \in b.$$

For two classes A and B, we have that $A = B$ if and only if for all x we have that:

$$x \in a \Longleftrightarrow x \in b.$$

1.2 Axiom of Pair Sets

For any sets x and y, there is a set $z = \{x, y\}$. This is the (unordered) pair set of x and y.

1.3 Axiom of the Powerset

For each set x, there exists a set which is the collection of the subsets of x, the powerset $\mathcal{P}(x)$.

For some set x, we have the powerset defined as follows $\mathcal{P}(x) = \{z \,:\, z \subseteq x\}$.

1.4 Axiom of the Empty Set

There exists a set with no members, the empty set $\varnothing$.

We have the empty set defined as follows $\varnothing = \{x \,:\, x \neq x\}$.

1.5 Axiom of Subsets

For some set x, we have that $\{y \in x \,:\, \Phi(y)\}$ is a set for some well-defined property of sets Φ.

1.6 Axiom of Unions

We have the basic union of two sets x_1 and x_2:

$$x_1 \cup x_2 = \{y : y \in x_1 \text{ or } y \in x_2\},$$

but for cases where we want to unify the members of the sets in a set X, we define:

$$\bigcup X = \{y : \exists x \in X, y \in x\}.$$

This axiom states that for a set X, $\bigcup X$ is a set.

1.7 Classes

We have that classes are collection of objects, these could also be sets. Classes that are not sets are called proper classes.

1.8 The Set ω

We have the set of natural numbers, $\mathbb{N} = \{0, 1, 2, \ldots\}$, and from this, we define ω:

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

where for some n in ω,

$$n = \{0, 1, 2, \ldots, n-1\},$$

with 0_ω being the empty set. We can go beyond this definition, defining:

$$\begin{aligned} \omega + 1 &= \{0, 1, 2, \ldots, \omega\}, \\ \omega + 2 &= \{0, 1, 2, \ldots, \omega, \omega + 1\}, \\ &\ldots \\ \omega + n &= \{0, 1, 2, \ldots, \omega, \omega + 1, \ldots \omega + n - 1\}. \end{aligned}$$

1.9 Russell's Theorem

We have that $R = \{x : x \notin x\}$ is not a set.

Proof. Suppose we have a set z such that $z = R$, is z in R? If we suppose z is in R, we have that z is not in z by the definition of R (as $z = R$) but z is R so z is not in R, a contradiction. Thus, we have that there is no set z equal to R, so R is not a set but a proper class. □

1.10 The Universe of Sets

We define the universe of sets as $V = \{x : x = x\}$. We have that V is a proper class.

Proof. If we suppose V is a set, we apply the axiom of subsets with $\Phi(x) = x \notin x$ and reach a contradiction via Russell's theorem. $\square$

2 Relations

We will first state the significant properties relations can have. Taking a relation R on X with x, y, z arbitrary in X:

Name	**Property**
Reflexive	xRx
Irreflexive	$\neg(xRx)$
Symmetric	$xRy \Rightarrow yRx$
Antisymmetric	$[xRy \text{ and } yRx] \Rightarrow [x = y]$
Connected	$[x = y]$ or $[xRy]$ or $[yRx]$
Transitive	$[xRy \text{ and } yRz] \Rightarrow [xRz]$

For example, equivalence relations must satisfy reflexivity, symmetry, and transitivity.

2.1 Partial Orderings

We say that a relation $\prec$ on a set X is a (strict) partial ordering if it is irreflexive and transitive.

Similarly, we say that a relation $\preceq$ on a set X is a non-strict partial ordering if it is reflexive, antisymmetric, and transitive.

A partial ordering $(X, \prec)$ is wellfounded if for any non-empty subset Y of X, Y has a least element under $\prec$.

2.2 Bounding

For a partially ordered set $(X, \prec)$:

- x_0 in X is the minimum of X if for all x in X, $x_0 \preceq x$,
- x' in X is minimal in X if for all x in X, $\neg(x \prec x')$,
- x_1 in X is the maximum of X if for all x in X, $x \preceq x_1$,
- x' in X is maximal in X if for all x in X, $\neg(x' \prec x)$.

Taking a non-empty subset Y of X, we consider the subordering $(Y, \prec)$ and for some α in X we say:

- α is a lower bound for Y if for all y in Y, $\alpha \prec y$,
- α is the infimum of Y if it's a lower bound and for all lower bounds λ of Y, $\alpha \preceq \lambda$,
- α is an upper bound for Y if for all y in Y, $y \prec \alpha$,
- α is the supremum of Y if it's an upper bound and for all upper bounds τ of Y, $\tau \preceq \alpha$.

2.3 Order Preserving Maps

We say that $f : (X, \prec_1) \to (Y, \prec_2)$ is an order preserving map if for each x_1, x_2 in X:

$$x_1 \prec_1 x_2 \Longrightarrow f(x_1) \prec_2 f(x_2).$$

Two orderings are (order) isomorphic if there is a bijective order preserving map between them.

2.4 Representation Theorem for Partially Ordered Sets

For a partially ordered set $(X, \prec)$, there is a set $Y \subseteq \mathcal{P}(X)$ which is such that $(X, \preceq)$ is order isomorphic to $(Y, \subseteq)$.

Proof. For some x in X, we set $X^x = \{x' \in X : x' \preceq x\}$, the set of elements preceding or equal to x. For x, y in X, $x \neq y$ implies that $X^x \neq X^y$ as these sets contain x and y (resp.) so $x \mapsto X^x$ is injective. This map is surjective trivially (mapping from X to $\{X^x : x \in X\}$). We have that:

$$x \preceq y \Longleftrightarrow X^x \subseteq X^y,$$

by our definition. Thus, $x \mapsto X^x$ is an order isomorphism. □

2.5 Total Orderings

A relation $\prec$ on a set X is a (strict) total ordering if it is a connected strict partial ordering.

Similarly, we say that a relation $\preceq$ on a set X is a non-strict total ordering if it is a connected non-strict partial ordering.

2.6 Well-orderings

A relation $\prec$ on a set X is a well-ordering if it is a strict total ordering and for any non-empty subset Y of X, Y has a least element under $\prec$. We denote this with $(X, \prec) \in WO$.

2.7 Ordered Pairs

For x, y sets, the ordered pair of x and y is the set:

$$\langle x, y\rangle = \{\{x\}, \{x, y\}\}.$$

2.7.1 Uniqueness of Ordered Pairs

For x, y, u, v sets, we have that:

$$\langle x, y\rangle = \langle u, v\rangle \iff (x = u) \text{ and } (y = v).$$

Proof. Suppose the former, if $x = y$ then $\langle x, y\rangle = \{\{x\}, \{x, x\}\} = \{\{x\}\}$. Thus, $\langle u, v\rangle = \{\{u\}\}$ as it is equal to $\langle x, y\rangle$ which has one element, hence $u = v$. By the Axiom of Extensionality, we have that $x = u$ and so $y = x = u = v$.

If $x \neq y$, then $\langle x, y\rangle$ and $\langle u, v\rangle$ both have the same two elements by our assumption (so $u \neq v$). We cannot have $\{x\} = \{u, v\}$ so $\{x\} = \{u\}$ which means $x = u$ by the Axiom of Extensionality. Thus, $\{u, v\} = \{x, y\} = \{u, y\}$ so $y = v$.

Suppose the latter, then the former holds trivially. $\square$

2.7.2 The Ordered k-tuple

We define the k-tuple inductively. The 2-tuple is already defined. We define the 3-tuple:

$$\langle x_1, x_2, x_3\rangle = \langle\langle x_1, x_2\rangle, x_3\rangle,$$

and for k in $\{3, 4, \ldots\}$:

$$\langle x_1, x_2, \ldots, x_k\rangle = \langle\langle x_1, x_2, \ldots, x_{k-1}\rangle, x_k\rangle.$$

2.7.3 The Product of Sets

For A, B sets, we define:

$$A \times B = \{\langle a, b\rangle : a \in A, b \in B\}.$$

Similarly to k-tuples, for $A_1, A_2, \ldots, A_k$ sets, we have $A_1 \times A_2$ defined, so we define:

$$A_1 \times A_2 \times \cdots \times A_k = (A_1 \times A_2 \times \cdots \times A_{k-1}) \times A_k,$$

defining the k-product for k in $\{2, 3, \ldots\}$. This is not associative.

2.8 Binary Relations

A binary relation R is a class of ordered pairs. We write $R^{-1} = \{\langle y, x\rangle : \langle x, y\rangle \in R\}$.

2.8.1 Domain and Range

For a relation R, we define:

$$\begin{aligned}
\mathrm{dom}(R) &= \{x : \exists\, y \text{ where } \langle x, y\rangle \in R\},\\
\mathrm{ran}(R) &= \{y : \exists\, x \text{ where } \langle x, y\rangle \in R\},\\
\mathrm{Field}(R) &= \mathrm{dom}(R) \cup \mathrm{ran}(R).
\end{aligned}$$

2.9 Functions

A relation F is a function if for all x in $\mathrm{dom}(F)$, there is a unique y in $\mathrm{ran}(F)$ with $\langle x, y\rangle$ in F.

If F is a function, it is injective if and only if for all x, x':

$$(\langle x, y\rangle \in F \text{ and } \langle x', y\rangle \in F) \Rightarrow (x = x').$$

2.9.1 Ranges and Restrictions

For $F : X \to Y$:

- $F''A = \{y \in Y : \exists\, x \in A \text{ such that } F(x) = y\}$ the range of F on A,
- $F \restriction A = \{\langle x, y\rangle \in F : x \in A\}$ the restriction of F to A.

We can see that $F''A = \mathrm{ran}(F \restriction A)$.

2.9.2 The Set of Functions

For X, Y sets, we have that ${}^XY = \{F : F : X \to Y\}$.

2.9.3 Indexed Cartesian Products

For a set I with each i in I corresponding to a non-empty set A_i:

$$\prod_{i \in I} A_i = \{\text{functions } f : \text{dom}(f) = I \text{ and } f(i) \in A_i \text{ for all } i \in I\}.$$

3 Transitive Sets

A set x is transitive if and only if for all y in x, $y \subseteq x$. This can be abbreviated to $\cup x \subseteq x$.

3.1 The Successor Function

For a set x, $S(x) = x \cup \{x\}$ is the successor of x. $S(x) = x$ is equivalent to saying x is transitive.

3.2 Transitive Closure

For a set x, to find a superset of x which is transitive, the transitive closure TC of x, we recurse:

$$\bigcup^0 x = x,$$
$$\bigcup^{n+1} x = \bigcup \left(\bigcup^n x \right),$$

which we can write as:

$$TC(x) = \bigcup \left\{ \bigcup^n x : n \in \mathbb{N} \right\}.$$

The transitive closure is always transitive.

3.2.1 Properties of Transitive Closure

For a set x:

1. $x \subseteq TC(x)$,
2. If t is transitive and $x \subseteq t$ then $TC(x) \subseteq t$. $TC(x)$ is the smallest transitive set containing x,
3. By the above, $TC(x) = x$ if and only if x is transitive.

Proof. (1) This is true as $\bigcup^0 = x$.

(2) If $x \subseteq t$ then clearly $\bigcup^0 x \subseteq t$. We assume $\bigcup^k x \subseteq t$ and use the fact that:

$$\left[A \subseteq B \text{ with } B \text{ transitive} \right] \Rightarrow \bigcup A \subseteq B,$$

to deduce that $\bigcup^{k+1} x \subseteq t$. By induction we have that $TC(x) \subseteq t$ as required.

(3) By (1), $x \subseteq TC(x)$. If x is transitive, we substitute it for t in (2) and get that $TC(x) \subseteq x$ as required. □

4 Number Systems

4.1 Von Neumann Numerals

We have the von Neumann numerals defined as:

$$\begin{aligned} 0 &= \varnothing, \\ 1 &= \{\varnothing\} = \{0\}, \\ 2 &= \{\varnothing, \{\varnothing\}\} = \{1, 2\}, \\ &\cdots \\ n+1 &= \{0, 1, \ldots, n\}. \end{aligned}$$

4.2 Inductive Sets

A set X is called inductive if $\varnothing$ is in X and for all x in X, $S(x)$ is in X.

4.3 Axiom of Infinity

There exists an inductive set.

4.4 Natural Numbers

We say that x is a natural number if for all X:

$$X \text{ is an inductive set} \Rightarrow x \in X.$$

We define ω as the class of natural numbers, $\omega = \cap\{X : X \text{ is an inductive set}\}$. We have that ω is the smallest inductive set.

Proof. Let z be an inductive set (by the Axiom of Infinity it exists). By the Axiom of Subsets, we define a set N:

$$N = \{x \in z : \forall Y, Y \text{ is inductive} \Rightarrow x \in Y\},$$

the elements of z in every inductive set. But $N = \omega$, so ω is a set.

We know that $\varnothing$ is in every inductive set by definition, so $\varnothing$ is in ω as it is the intersection of all inductive sets. For any x in ω, we know that for any inductive set Y that x is in Y (by the definition of ω) and thus $S(x)$ is also in Y (by the definiton of an inductive set). Thus, $S(x)$ is also in ω as Y was chosen arbitrarily. Hence, ω is an inductive set and the smallest such set by its definition. $\square$

4.5 Principle of Mathematical Induction

We suppose Φ is a well-defined property of sets, then we have that:

$$\Big[\Phi(0) \text{ and } \forall\, x \in \omega \text{ we have that } \Phi(x) \Rightarrow \Phi(S(x))\Big] \Rightarrow \Big[\forall\, x \in \omega \text{ we have that } \Phi(x)\Big].$$

Proof. We assume the antecedent, it suffices to show that the collection of x in ω where $\Phi(x)$ holds is inductive (as we assume $\Phi(0)$ holds).

Let $Y = \{x \in \omega : \Phi(x)\}$. As we assumed $\Phi(0)$, we know that 0 is in Y. Then, by the second half of our assumption, we can see that Y is closed under the successor function. Thus, Y is inductive and as ω is the smallest inductive set, $\omega \subseteq Y$ as required. $\square$

4.6 Representation of Natural Numbers

We have that every natural number is either 0 or $S(x)$ for some natural number x.

Proof. Let $Z = \{y \in \omega : y = 0 \text{ or } \exists\, x \in \omega \text{ such that } S(x) = y\}$. It suffices to show that Z is inductive. Clearly, 0 is in Z. Suppose we have some u in Z, then u is in ω. As ω is inductive, $S(u)$ is also in ω so $S(u)$ is in Z. Thus, Z is inductive as required. $\square$

4.7 Transitivity of ω

We have that ω is transitive.

Proof. Let $X = \{n \in \omega : n \subseteq \omega\}$. If $X = \omega$ then by definition ω is transitive. It suffices to show that X is inductive. We know that $\varnothing$ is in X as 0 is in ω. Taking n in X, then clearly $\{n\} \subseteq \omega$ as n is in ω. Furthermore, $n \subseteq \omega$ as n is in X. Thus, $n \cup \{n\} \subseteq \omega$ so $S(n) \in X$ which means X is inductive as required. $\square$

4.8 Ordering on the Naturals

For m, n in ω, we define:

$$m < n \iff m \in n,$$
$$m \leq n \iff m = n \text{ or } m \in n.$$

By definition, $n < S(n)$.

We have that:

1. This ordering is transitive,
2. For all n in ω and for all m we have that $m < n$ if and only if $S(m) < S(n)$,
3. For all n in ω, $n \not< n$.

Proof. (1) This follows from the transitivity of set inclusion.

(2) We take $\Phi(k) = [(m < k) \Rightarrow (S(m) < S(k))]$. We see $\Phi(0)$ holds. Supposing $\Phi(k)$ holds for some k, let $m < S(k)$ then m is in $k \cup \{k\}$. If m is in k then by $\Phi(k)$ we have that $S(m) < S(k) < S(S(k))$. If $m = k$ then $S(m) = S(k) < S(S(k))$. Thus, by induction, we have our result.

Assume $S(m) < S(n)$, m is in $S(m) = m \cup \{m\}$ which is in $S(n) = n \cup \{n\}$. If $S(m) = n$, then m is in n so $m < n$. If $S(m)$ is in n then m is in n as n is transitive.

(3) We know that $0 \not< 0$ as $0 \notin 0$. If $k \notin k$ then $S(k) \notin S(k)$ by Part (ii). Thus, $X = \{k \in \omega : k \notin k\}$ is inductive which makes it equal to ω as required. $\square$

4.9 Total Ordering on the Naturals

We have that $<$ is a (strict) total ordering on the naturals.

4.10 Well-ordering Theorem for ω

Let $X \subseteq \omega$, then either $X = \varnothing$ or there is some n_0 in X such that for any m in X either $n_0 = m$ or $n_0 < m$.

Proof. Suppose $X \subseteq \omega$ but has no least element. Let $Z = \{k \in \omega : \forall\, n < k, n \notin X\}$. We want to show Z is inductive, meaning $Z = \omega$ and so $X = \varnothing$.

Vacuously, 0 is in Z. Suppose we have k in Z, we let $n < S(k) = k \cup \{k\}$ and consider:

- If $n \in k$ then $n \notin X$ as $n < k \in Z$,
- If $n = k$ then $n \notin X$ because if n was in X then it would be the least element of X, a contradiction.

Thus, $S(k)$ is in Z so Z is inductive. $\square$

4.11 Recursion Theorem on ω

Let A be any set with a in A and $f : A \to A$ any function. There exists a unique function $h : \omega \to A$ such that for any n in ω:

$$h(0) = a,$$
$$h(S(n)) = f(h(n)).$$

Proof. We will find h as a union of k-approximations where u is a k-approximation if it is a function with $\mathrm{dom}(u) = k$ and for:

- If $k > 0$ then $u(0) = a$,
- If $k > S(n)$ then $u(S(n)) = f(u(n))$.

From this, we see that $\{\langle 0, a\rangle\}$ is a 1-approximation in particular. Furthermore, if u is a k-approximation and $l \leq k$ then $u \restriction l$ is an l-approximation, finally if $u(k-1) = c$ for some c, then $u' = u \cup \{\langle k, f(c)\rangle\}$ is a $(k+1)$-approximation.

Agreement on Domain
If u is a k-approximation and v is a k'-approximation for some $k \leq k'$ then $v \restriction k = u$ (hence $u \subseteq v$).

Proof. We appeal to the contrary with $0 \leq m < k$ being the least natural such that $u(m) \neq v(m)$. We know that $m \neq 0$ as $u(0) = a = v(0)$. So, $m = S(m')$ for some m'. As m is chosen minimally, $u(m') = v(m')$. We can then see that $u(m) = f(u(m')) = f(v(m')) = v(m)$, a contradiction. □

Uniqueness
If h exists, it is unique.

Proof. Suppose h and h' are two different functions with domain ω satisfying the theorem. We take $0 \leq m < \omega$ to be the least natural such that $h(m) \neq h'(m)$ and apply the same reasoning to the above. □

Existence
Let u be in B if and only if there exists k in ω such that u is a k-approximation. For any u, v in B either $u \subset v$ or vice-versa by our previous results. We take $h = \bigcup B$.

We have that h is a function:

Proof. We appeal to the contrary. If $\langle n, c\rangle$ and $\langle n, d\rangle$ are in h with $c \neq d$, then we have u, v in B with $u(n) = c$ and $v(n) = d$ but this is impossible by **Agreement on Domain**. □

We have that $\mathrm{dom}(h) = \omega$:

Proof. We appeal to the contrary and suppose $\varnothing \neq X = \{n \in \omega : n \notin \mathrm{dom}(h)\}$. By the definition of h this means that:

$$X = \{n \in \omega : \text{There's no } u\text{-approximation with } n \in \mathrm{dom}(u)\}.$$

We saw that there is a 1-approximation, so 0 is not the least element of X. We suppose $n_0 = S(m)$ is the least element of X. As m is not in X, there must be an n_0-approximation n with $n(m) = c$ for some c. But, we saw that we can extend k-approximations, so we can generate a $(n_0 + 1)$-approximation which is a contradiction. Thus, $X = \varnothing$. $\square$

Thus, we have that h exists and is a unique function as required. $\square$

5 Well-orderings and Ordinals

5.1 The Principle of Transfinite Induction

Let $\langle X, \prec \rangle$ be a well-ordering. We have that:

$$[\forall\, x \in X, (\forall\, y \prec x, \Phi(y)) \Rightarrow \Phi(x)] \Rightarrow \forall\, x \in X, \Phi(x).$$

Proof. We appeal to the contrary and assume the antecedent but suppose that $\varnothing \neq Z = \{x \in X : \neg\Phi(x)\}$. As $\langle Z, \prec \rangle$, there is $\prec$-least element z_0. But then for all $x \prec z_0$, $\Phi(x)$ holds. But, by the antecedent, this means $\Phi(z_0)$ holds, a contradiction. □

5.2 Initial Segments

For a well-ordering $\langle X, \prec \rangle$, the $\prec$-initial segment of some element z in X is the set of predecessors of z, denoted by X_z. Note that X_z does not contain z.

5.3 Order Preserving Maps on Well-orderings

For a well-ordering $\langle X, \prec \rangle$ with $f : \langle X, \prec \rangle \to \langle X, \prec \rangle$ an order preserving map, we have that for all x in X, $x \prec f(x)$.

Proof. We appeal to the contrary, that for some x in X, we have $f(x) \prec x$. As $\langle X, \prec \rangle$ is a well-ordering, there's a $\prec$-least x_0 in X with the property that $f(x_0) \prec x_0$. But $f(f(x_0)) \prec f(x_0)$ as f is order preserving. Thus, a contradiction to the minimality of x_0. □

5.3.1 Uniqueness of Order Isomorphisms

For well-orderings $\langle X, \prec_x \rangle$, $\langle Y, \prec_y \rangle$ with $f : \langle X, \prec_x \rangle \to \langle Y, \prec_y \rangle$ an order isomorphism. We have that f is unique.

Proof. Suppose we have two such isomorphisms f and g. We have that $(f^{-1} \circ g)$ is also an order isomorphism. Taking x arbitrary in X:

$$\begin{aligned} & x \preceq_x (f^{-1} \circ g)(x) \\ \Longrightarrow \quad & f(x) \preceq_y f(f^{-1} \circ g)(x) \\ \Longrightarrow \quad & f(x) \preceq_y g(x). \end{aligned}$$

By applying this argument again with the roles of f and g swapped, we can also see that $g(x) \preceq_y f(x)$. Thus, $f(x) = g(x)$.

In particular, if $\langle X, \prec_x \rangle = \langle Y, \prec_y \rangle$ then this isomorphism is the identity map. □

5.3.2 Non-existence of Order Isomorphisms to Segments

A well-ordered set is not order isomorphic to any segment of itself.

Proof. We appeal to the contrary and suppose there is such an order isomorphism on a well-ordering $\langle X, \prec\rangle$ to $\langle X_z, \prec\rangle$ for some z in X. But, we have that $x \preceq f(x)$ for any x in X and $f(z) \prec z$ as $f(z)$ is in X_z. Thus, we have that $z \preceq f(z)$ and $z \succ f(z)$, a contradiction. □

5.3.3 Order Isomorphism to Set of Segments

A well-ordered set $\langle X, \prec\rangle$ is order isomorphic to the set of its initial segments ordered by $\subset$.

Proof. We let $Y = \{X_a : a \in X\}$, we have that φ characterised by $a \mapsto X_a$ is an injective map as segments do not contain the element which determines it. As $a \prec b \Leftrightarrow X_a \subset X_b$, the mapping is order preserving. □

5.4 Ordinal Numbers

We say that $\langle X, \in\rangle$ is an ordinal if and only it X is transitive, and where $\prec = \in$, $\langle X, \prec\rangle$ is a well-ordering. We have that $\langle \omega, \in\rangle$ is an ordinal.

5.4.1 Elements and Segments

For an ordinal $\langle X, \in\rangle$, then every element z in X is identical to X_z.

Proof. Suppose X is transitive and $\in$ well-orders X. Taking z in X:

$$\begin{aligned} w \in X_z \quad &\Longleftrightarrow \quad w \in X \text{ and } w \in z \\ &\Longleftrightarrow \quad w \in z, \qquad\qquad (\text{as } z \subseteq X) \end{aligned}$$

thus, $X_z = z$ as required. □

So, for any elements a, b of an ordinal:

$$a \in b \Longleftrightarrow a \subset b \Longleftrightarrow X_a \subset X_b.$$

5.4.2 Subsets and Segments

For an ordinal $\langle X, \in\rangle$ with $Y \subset X$, if $\langle Y, \in\rangle$ is also an ordinal, then Y is an $\in$-initial segment of X.

Proof. Taking a in Y as supposed, as Y is an ordinal so $Y_a = a$. As $Y \subset X$, a is in X so $X_a = a$. Thus, $X_a = Y_a$. Furthermore, as $Y \neq X$, we consider $c = \inf\{z \in X : z \notin Y\}$ which exists as the set is non-empty and $\langle X, \in\rangle$ is a well-ordering. Hence, $Y = X_c$. □

5.4.3 Segments

For an ordinal $\langle X, \in\rangle$ any $\in$-initial segment of $\langle X, \in\rangle$ is an ordinal.

Proof. We take some u in X and w in X_u. As $\in$ well-orders X, it well-orders any subset of X so $\langle X_u, \in\rangle$ is a well-ordering. We have that:

$$t \in w \in u \Longrightarrow t \in u = X_u,$$

thus X_u is transitive as required. □

5.4.4 The Intersection of Ordinals

For ordinals X, Y, $X \cap Y$ is also an ordinal.

Proof. We take $\in$ to be the ordering on X. We know that $X \cap Y$ is transitive as X and Y are transitive. Any subset of X is a well-ordering under $\in$, in particular $X \cap Y$ is well-ordered by $\in$. □

5.5 Classification Theorem for Ordinals

For two ordinals X, Y, either $X = Y$ or one is an initial segment of the other (or equivalently a member).

Proof. Suppose that $X \neq Y$. We know that $X \cap Y$ is an ordinal also. We have two cases.

If $X = X \cap Y$ or $Y = X \cap Y$, one must be an initial segment of the other as it must be a proper subset under our assumption $X \neq Y$.

If $X \cap Y$ is a proper subset of X and Y, it is an initial segment of X and Y simultaneously we set $X \cap Y = X_a = Y_b$ for some a in X and b in Y. But, we know that as X and Y are ordinals, $a = X_a = Y_b = b$. However, this means:

$$a = b \in X \cap Y = X_a,$$

but $a \notin X_a$, a contradiction. □

5.6 Equality under Isomorphisms

For two ordinals X and Y, if X is order isomorphic to Y then $X = Y$.

Proof. Suppose $X \neq Y$, then without loss of generality we take X to be an initial segment of Y. But, this would mean Y is order isomorphic to a segment of itself which is a contradiction. □

5.7 Bound on Isomorphisms

A well-ordering is order isomorphic to at most one ordinal.

Proof. If a well-ordering is isomorphic to more than one ordinals, then these ordinals are isomorphic to each other and thus, equal. $\square$

5.8 Criterion for Ordinals

If every segment of a well-ordered set $\langle A, \prec\rangle$ is order isomorphic to some ordinal, $\langle A, \prec\rangle$ itself is order isomorphic to an ordinal.

Proof. Each segment must be order isomorphic to at most one ordinal (thus exactly one). We define a function F from the segments of A to the ordinal $F(A_b)$ such that $\langle A_b, \prec\rangle \cong \langle F(b), \in\rangle$. We know that this ordinal is unique as non-identical segments have differing sizes. We let $Z = \mathrm{ran}(F)$:

$$Z = \{F(b) : \exists\, b \in A, \exists \text{ an isomorphism } g_b \text{ from } \langle A_b, \prec\rangle \text{ to } \langle F(b), \in\rangle\},$$

noting that the isomorphism between A_b and $F(b)$ is unique. If c, b are in A with $c \prec b$ then $A_c = (A_b)_c$ implying that $F(c) \neq F(b)$ so F is injective and thus bijective between A and Z. Continuing with $c \prec b$:

$$g_b \restriction A_c : \langle A_c, \prec\rangle \cong \langle (F(b))_{g_b(c)}, \in\rangle,$$

by the uniqueness of order isomorphisms $(g_b \restriction A_c) = g_c$ and $F(c) = (F(b))_{g_b(c)}$. Thus, $F(c) \in F(b)$.

We know that Z is well-ordered by $\in$ as A is well-ordered by $\prec$ and F is an order isomorphism. For $u \in F(b) \in Z$, as g_b is surjective, $u = g_b(c)$ for some $c \prec b$. Then, $u = F(b)_u = F(b)_{g_b(c)} = F(c)$. Hence, u is in Z, so Z is transitive. Thus, Z is an ordinal. $\square$

5.9 Representation Theorem for Well-orderings

Every well-ordering is order isomorphic to exactly one ordinal.

Proof. For a well-ordering $\langle X, \prec \rangle$, we know that if it is isomorphic to an ordinal, this is the only such ordinal. We take:

$$Z = \{v \in X : X_v \text{ is not isomorphic to an ordinal}\},$$

and want to show it's empty as this will suffice combined with our criterion. Supposing the contrary, we take v_0 to be the $\prec$-least element of Z. We have that $\langle X_{v_0}, \prec \rangle$ is a well-ordering with each element preceding v_0, as such $(X_{v_0})_w = X_w$ for each w in X_{v_0} is order isomorphic to an ordinal. Which means X_{v_0} must also be order isomorphic to an ordinal via our criterion, a contradiction. Thus, Z is empty, as required. □

5.10 Order Type of Well-orderings

For a well-ordering $\langle X, \prec \rangle$, the order type of $\langle X, \prec \rangle$ is the unique ordinal isomorphic to $\langle X, \prec \rangle$, written as $\mathrm{ot}(\langle X, \prec \rangle)$.

5.11 Classification Theorem for Well-orderings

For two well-orderings $\langle A, \prec_A \rangle$ and $\langle B, \prec_B \rangle$ we have that exactly one of the following holds:

- $\langle A, \prec_A \rangle \cong \langle B, \prec_B \rangle$,
- There exists b in B such that $\langle A, \prec_A \rangle \cong \langle B_b, \prec_B \rangle$,
- There exists a in A such that $\langle A_a, \prec_A \rangle \cong \langle B, \prec_B \rangle$.

Proof. We take $\langle X, \in \rangle$ and $\langle Y, \in \rangle$ to be the unique ordinals isomorphic to $\langle A, \prec_A \rangle$ and $\langle B, \prec_B \rangle$ (resp.) via maps:

$$\begin{aligned} f &: \langle X, \in \rangle \to \langle A, \prec_A \rangle, \\ g &: \langle Y, \in \rangle \to \langle B, \prec_B \rangle. \end{aligned}$$

We know that either these ordinals are order isomorphic or order isomorphic to an initial segment of the other. If the former is true, then we have that our well-orderings are isomorphic via f and g and their inverses. If the latter is true, we know that (without loss of generality) $\langle X, \in \rangle \cong \langle Y_y, \in \rangle$ for some y in Y. Thus:

$$f(\langle X, \in \rangle) \cong g(\langle Y_y, \in \rangle) \implies \langle A, \prec_A \rangle \cong \langle B_{g(y)}, \prec_B \rangle),$$

as required. □

6 Properties of Ordinals

We collate the properties of ordinals covered so far for some ordinals α, β, and γ:

- Ordinals are transitive,
- Ordinals are well-ordered by $\in$,
- $\alpha \in \beta \in \gamma$ implies that $\alpha \in \gamma$,
- If $X \in \alpha$ then X is an ordinal with $X = \alpha_X$,
- If $\alpha \cong \beta$ then $\alpha = \beta$,
- Exactly one of the following holds:
  - $\alpha = \beta$,
  - $\alpha \in \beta$,
  - $\beta \in \alpha$.

6.1 Principle of Transfinite Induction

For Φ a well-defined and definite property of ordinals, we have that for all ordinals α:

$$\big[\forall\, \beta < \alpha, \Phi(\beta) \Rightarrow \Phi(\alpha)\big] \Rightarrow \big[\Phi(\alpha)\big].$$

Hence, the class of ordinals is well-ordered.

Proof. We consider $C = \{\alpha \text{ an ordinal } : \neg\Phi(\alpha)\}$ and suppose it's non-empty. We take α_0 in C, if it is not the least element we have that $\alpha_0 \cap C$ is non-empty as there is some β in C with $\beta < \alpha$ which is equivalent to saying that $\beta \in \alpha$. As α_0 is an ordinal, we have that α_0 is well-ordered by $\in$, hence $C \cap \alpha_0 \subseteq \alpha_0$ has an $\in$-least element α_1 which is the least element of C.

Thus, we have that $\neg\Phi(\alpha_1)$ holds, but as this is the least element of C, for all ordinals β less than α_1 we have that $\Phi(\beta)$ holds. However, by our antecedent, this means $\Phi(\alpha_1)$ holds, a contradiction. Thus, C is empty as required.

Note that our argument showed than any non-empty class on the ordinals has a least element. Thus, the class of ordinals is well-ordered by $\in$. $\square$

6.2 The Class of Ordinals

The class of ordinals is a proper class.

Proof. Suppose the class of ordinals is a set z. We have that $\langle z, \in\rangle$ is transitive and well-ordered by $\in$. Thus, z is an ordinal, as such z is in z. But, this contradicts the strict ordering of $\in$. $\square$

6.3 Sum of Orderings

For $\langle A, R\rangle$ and $\langle B, S\rangle$ strict total orderings with $A \cap B$ empty, we define the sum ordering $\langle C, T\rangle$ as:

$$C = A \cup B,$$
$$xTy \Leftrightarrow \begin{cases} xRy & \text{for } x, y \in A \\ xSy & \text{for } x, y \in B \\ x \in A \text{ and } y \in B & \text{otherwise.} \end{cases}$$

We can avoid the disjoint constraint by taking the sum of $\langle A \times \{0\}, R\rangle$ and $\langle B \times \{1\}, S\rangle$. We can built this functionality into our operation. We name this operation $+'$ and for α, β ordinals:

$$\alpha +' \beta = \mathrm{ot}(\langle \alpha \times \{0\} \cup \beta \times \{1\}\rangle, T),$$
$$\langle \gamma, i\rangle T \langle \delta, j\rangle \Leftrightarrow (i = j \text{ and } \gamma < \delta) \text{ or } (i < j).$$

6.4 Product of Orderings

For $\langle A, R\rangle$ and $\langle B, S\rangle$ strict total orderings. We define the product of these orderings $\langle A, R\rangle \times \langle B, S\rangle$ to be the ordering $\langle C, U\rangle$:

$$C = A \times B$$
$$\langle x, y\rangle U \langle x', y'\rangle \Leftrightarrow (ySy') \text{ or } (y = y' \text{ and } xRx'),$$

taking the latter and replacing each member by the former. We can again construct an operation for ordinals α and β:

$$\alpha \cdot' \beta = \mathrm{ot}(\langle A \times B, U\rangle),$$

with U defined as above.

6.5 Supremum of Ordinals

For a set of ordinals A, $\sup(A)$ is the least ordinal γ such that for all δ in A, $\delta \leq \gamma$. Furthermore, we have the strict supremum $\sup^{+}(A)$ as the least ordinal γ^{+} such that for all δ in A, $\delta < \gamma^{+}$.

We can also write $\sup(A) = \bigcup A$.

Proof. If we suppose there isn't an ordinal which is an upper bound for A, there's some δ in A such that $\delta > \gamma$ for each ordinal γ. But, $\bigcup A$ must be a set and equal to the set of ordinals, a contradiction.

Take $S = \sup(A)$ and take u in $\bigcup A$. For some a in A, $u < a < A$, so $u < S$ and so u is in S, $\bigcup A \subseteq S$. Conversely, we consider s in S, then $s < S = \sup(A)$ so there is some a in A with $s < a \leq S$. Thus, s is in A so s is in $\bigcup A$, $S \subseteq \bigcup A$. Thus $S = \bigcup A$. $\square$

6.6 Types of Ordinals

We can consider three types of ordinals:

- The zero ordinal, 0,
- Successor ordinals, ordinals with immediate predecessors,
- Limit ordinals, ordinals that are not of the other types.

6.7 Transfinite Recursion Theorem on Ordinals

For $F : V \to V$ a function, there exists a unique function H from the ordinals to V such that for all α:

$$H(\alpha) = F(H \upharpoonright \alpha).$$

Proof. We define a function u to be a δ-approximation if $\mathrm{dom}(u) = \delta$ and for all $\alpha < \delta$, $u(\alpha) = F(u \upharpoonright \alpha)$.

Observations
We consider u to be a δ-approximation. For $\delta > 0$, we see that $u(0) = F(u \upharpoonright 0) = F(\varnothing)$ so a 1-approximation is equal to $\{\langle 0, F(\varnothing)\rangle\}$ with domain $\{0\} = 1$. Additionally, for some $\gamma < \delta$, $u \upharpoonright \gamma$ is a γ-approximation. Furthermore, $u \cup \{\langle \delta, F(u)\rangle\}$ is a $(\delta + 1)$-approximation. We take $B = \{u : \exists\, \delta$ such that u is a δ-approximation$\}$.

Agreement on Domain
For u a δ-approximation and v any γ-approximation with $\delta < \gamma$, $u = v \restriction \delta$.

Proof. We appeal to the contrary and take τ be the least value such that $u(\tau) \neq \gamma(\tau)$. Thus, $(u \restriction \tau = v \restriction \tau)$ but then:

$$u(\tau) = F(u \restriction \tau) = F(v \restriction \tau) = v(\tau),$$

which is a contradiction. $\square$

Uniqueness
If such H exists, it is unique.

Proof. We appeal to the contrary, taking H' to be some differing derivation of H. We consider the least τ such that $H(\tau) \neq H'(\tau)$ and apply the same reasoning to the above. $\square$

Limits
For some limit ordinal λ, if for all $\alpha < \lambda$ we have that u_α is an α-approximation, $\bigcup_{\alpha<\lambda} u_\alpha$ is a λ-approximation.

Proof. This union is a union of an increasing sequence of sets (so $\alpha < \beta < \lambda \Rightarrow u_\alpha \subseteq u_\beta$). As each element is a function, the union is also a function with domain λ. Thus, this union is a λ-approximation. $\square$

Existence
We define $H = \bigcup B$ which is a function with $\mathrm{dom}(H)$ being the set of ordinals.

Proof. We know that H is a function by **Agreement on Domain**. We take $C = \{\delta : \text{There's no } \delta\text{-approximation}\}$ and suppose C is non-empty. By the principle of transfinite induction on the ordinals, C has a least elememt ψ. We know that $\psi > 1$ as we defined a 1-approximation and by **Limits** it cannot be a limit ordinal. If $\psi = \mu+1$ then there's a μ-approximation v by the minimality of ψ. However, we can extend v to a ψ-approximation u by setting $u(\mu) = F(v)$. This is a contradiction. $\square$

Thus, we have that H exists and is a unique function as required. $\square$

6.8 Alternative Transfinite Recursion on Ordinals

For a in V and $F_0, F_1 : V \to V$ functions, there's a unique function H from the set of ordinals to V such that:

$$\begin{aligned} H(0) &= a, \\ \mathrm{succ}(\alpha) \implies H(\alpha) &= F_0(H(\beta)) \text{ where } \alpha = \beta + 1, \\ \lim(\alpha) \implies H(\alpha) &= F_1(H \restriction \alpha). \end{aligned}$$

Proof. We define $F : V \to V$ by:

$$F(u) = \begin{cases} a & \text{for } u = \varnothing \\ F_0(u) & \text{if } u \text{ is a function with a successor domain} \\ F_1(u) & \text{if } u \text{ is a function with a limit domain} \\ \varnothing & \text{otherwise,} \end{cases}$$

and apply the previous recursion theorem. □

6.9 Ordinal Addition

We define ordinal addition A_α for some successor ordinal $\beta + 1$ and limit ordinal λ as:

$$\begin{aligned} A_\alpha(0) &= \alpha + 0 = \alpha, \\ A_\alpha(\beta + 1) &= S(A_\alpha(\beta)) = A_\alpha(\beta) + 1, \\ A_\alpha(\lambda) &= \sup(\{A_\alpha(x) : x < \lambda\}). \end{aligned}$$

6.10 Ordinal Multiplication

We define ordinal multiplication A_α for some successor ordinal $\beta+1$ and limit ordinal λ as:

$$\begin{aligned} M_\alpha(0) &= 0, \\ M_\alpha(\beta + 1) &= M_\alpha(\beta) + \alpha, \\ M_\alpha(\lambda) &= \sup(\{M_\alpha(x) : x < \lambda\}). \end{aligned}$$

6.11 Ordinal Exponentiation

We define ordinal exponentiation A_α for some successor ordinal $\beta + 1$ and limit ordinal λ as:

$$\begin{aligned} E_\alpha(0) &= 1, \\ E_\alpha(\beta+1) &= E_\alpha(\beta) \cdot \alpha, \\ E_\alpha(\lambda) &= \sup(\{E_\alpha(x) : x < \lambda\}). \end{aligned}$$

6.12 Monotonicity of A_α

The functions A_α are strictly increasing and thus injective.

Proof. We consider β, γ, δ ordinals with:

$$[\beta < \gamma] \implies [A_\alpha(\beta) < A_\alpha(\gamma)], \tag{1}$$

for all $\gamma \leq \delta$. The base case is trivial, we consider $\delta + 1$. For $\beta < \delta + 1$, if $\beta = \delta$, then:

$$\begin{aligned} A_\alpha(\delta) &= A_\alpha(\beta) \\ &< A_\alpha(\beta+1) \\ &= S(A_\alpha(\beta)) \\ &= S(A_\alpha(\delta)). \end{aligned}$$

Otherwise, $\beta < \delta$ so by our hypothesis:

$$\begin{aligned} A_\alpha(\beta) &< A_\alpha(\delta) \\ &< S(A_\alpha(\delta)) \\ &= A_\alpha(\delta+1). \end{aligned}$$

Now, we suppose (1) holds for all $\gamma < \lambda$ for some limit ordinal λ. For $\beta < \lambda$, clearly $\beta < \beta + 1 < \lambda$ as λ has no immediate predecessor. By the hypothesis:

$$\begin{aligned} A_\alpha(\beta) &< A_\alpha(\beta+1) \\ &\leq \sup(\{A_\alpha(\gamma) : \gamma < \lambda\}) \\ &= A_\alpha(\lambda), \end{aligned}$$

as required. $\square$

Similarly, both M_α and E_α are strictly increasing, for ordinals α, β, γ with $\beta > \gamma$:

- If $\alpha > 0$ then $M_\alpha(\beta) < M_\alpha(\gamma)$,
- If $\alpha > 1$ then $E_\alpha(\beta) < E_\alpha(\gamma)$.

6.13 Remainders

For α, β ordinals with $0 < \alpha \leq \beta$:

1. There's a unique ordinal γ such that $\alpha + \gamma = \beta$,
2. There's a unique pair of ordinals ζ, κ such that $\alpha \cdot \zeta + \kappa = \beta$ and $\kappa < \alpha$.

Proof. (i) As A_α is strictly increasing, we consider $Z = \{x : \alpha + x \geq \beta\}$ which must be non-empty as A_α is strictly increasing. We take $\gamma = \min(Z)$ and see that $\alpha + \gamma = \beta$ since if $\alpha + \gamma > \beta$ either:

- $\gamma = \delta + 1$ so $\alpha + \delta < \beta$ as δ is not in Z. But then, $(\alpha + \delta) + 1 = \alpha + \gamma \leq \beta$, a contradiction,
- γ is a limit ordinal, $\alpha + \gamma = \sup(\{\alpha + \delta : \delta < \gamma\})$. But, if $\alpha + \gamma > \beta$ then there's some $\delta < \gamma$ so that $\delta \geq \beta$. This contradicts $\gamma = \min(Z)$.

(ii) As M_α is strictly increasing, we again choose the least ζ such that $\alpha \cdot \zeta \leq \beta < \alpha \cdot (\zeta + 1)$. We apply part (i) to find κ such that $\alpha \cdot \zeta + \kappa = \beta$. We suppose ζ' and κ' also satisfy (ii), if $\zeta = \zeta'$ then by the uniqueness of part (i), $\kappa = \kappa'$. We suppose $\zeta < \zeta'$ so $\zeta + 1 \leq \zeta'$:

$$\begin{aligned}
\beta = \alpha \cdot \zeta + \kappa &< \alpha \cdot \zeta + \alpha \\
&= \alpha \cdot (\zeta + 1) \\
&\leq \alpha \cdot \zeta' \\
&\leq \alpha \cdot \zeta' + \kappa' \\
&= \beta,
\end{aligned}$$

a contradiction. Hence, $\zeta = \zeta'$. $\square$

7 Cardinality

7.1 Equinumerosity

We say that two sets, A and B, are equinumerous if there is a bijection between them, written as $A \approx B$.

We have that $\approx$ is an equivalence relation with equivalence classes as collections of all equinumerous sets of a size.

7.2 Finite Sets

A set is finite if it is equinumerous with a natural number. Sets that are not finite are infinite.

7.3 Pidgeon-hole Principle

No natural number is equinumerous to a proper subset of itself and thus:

- No finite set is equinumerous to a proper subset of itself,
- Any set equinumerous to a proper subset of itself is infinite,
- Any finite set is equinumerous to a unique natural number,
- ω is infinite.

Proof. We take $Z = \{n \in \omega : \forall f, (f : n \to n \text{ and injective}) \Rightarrow (\text{ran}(f) = n)\}$. Trivially, Z contains 0. For n in Z, we consider $f : (n+1) \to (n+1)$ an injective function.

Case 1 We suppose that $f \restriction n : n \to n$ is an injective function and by our inductive hypothesis, $\text{ran}(f \restriction n) = n$. Thus, $\text{ran}(f) = n + 1$.

Case 2 We suppose that $f(m) = n$ for some $m < n$. As f is injective, for some $k < n$, $f(n) = k$. We define g identically to f except $g(m) = k$ and $g(n) = n$ so that $g : (n+1) \to (n+1)$ and injective so **Case 1** applies to g. Hence, $\text{ran}(g) = n + 1 = \text{ran}(f)$. □

7.4 Cantor's Diagonal Argument

The natural numbers are not equinumerous with the real numbers.

Proof. We appeal to the contrary and suppose we have some injective map $f : \omega \to \mathbb{R}$:

$$\begin{aligned} f(0) &= 2.72938\ldots \\ f(1) &= 3.47000\ldots \\ f(2) &= 9.32789\ldots \\ &\vdots \end{aligned}$$

We can generate some x not in $\operatorname{ran}(f)$ by setting the i^{th} decimal place to the i^{th} decimal place of $f(i)$ mapped by:

$$k \mapsto \begin{cases} 1 & k \text{ even} \\ 2 & k \text{ odd.} \end{cases}$$

Thus, x would differ from every element of $\operatorname{ran}(f)$. A contradiction. $\square$

7.5 Infinite Infinities

No set is equinumerous to its powerset.

Proof. We appeal to the contrary and suppose $f : X \to \mathcal{P}(X)$ is a bijection for some set X. We set $Z = \{u \in X : u \notin f(u)\}$ and see that $Z \subseteq X$ so Z is in $\mathcal{P}(X)$. As such, $Z = f(u)$ for some u, but:

$$\begin{aligned} u \in Z &\implies u \notin f(u), \\ u \notin Z &\implies u \in f(u), \end{aligned}$$

which is a contradiction. $\square$