PHIL 5506: Metalogic
T. Parent

SET THEORY PRIMER

1. Basics

$\{x \mid Cx\}$ is the set of all and only those things that satisfy condition C.
‘$x \in y$’ means that x is an **element** (a.k.a., a member) of y. (Note that x could itself be a set.)
‘$x \notin y$’ means that x is not an element of y.
$\emptyset$ or $\{\}$ is the **empty set**, where for any x, $x \notin \emptyset$. (Alternatively, $\emptyset = \{x \mid x \neq x\}$.)
$\{x\}$ is the **singleton** of x, i.e., the set whose only member is x.

Let A and B be sets. Then:
‘$A \subseteq B$’ means that A is a **subset** of B and that B is a **superset** of A—every element of A is an element of B.

I.e., for any x, if $x \in A$, then $x \in B$. (This does *not* mean that $A \in B$.)
The empty set is a subset of every set. (Do you see why?)

‘$A \subset B$’ means that A is a **proper subset** of B; A is a subset of B but $A \neq B$.

$A \cup B$ is the **union** of A and B: It is the set of all objects that belong to either A or B.

I.e., $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$.

$A \cap B$ is the **intersection** of A and B: It is the set of all objects which belong to both A and B.

I.e., $A \cap B = \{x \mid x \in A \text{ and } x \in B\}$.
A and B are called **disjoint** when their intersection is empty.

$\mathscr{P}A$ is the **power set** of A: It is the set of all subsets of A.

I.e., $\mathscr{P}A = \{x \mid x \subseteq A\}$.

$B - A$ or $B \setminus A$ is the **set difference** of B and A: It is the set $\{x \in B \mid x \notin A\}$. The order of B and A matters, since $\{x \in A \mid x \notin B\}$ is a different set (except when $A = B$). The set difference of B and A is also known as the **relative complement** of A in B—or if B is clear from context, we might just write ‘$\setminus A$’ or ‘$\bar{A}$’ and speak simply of the “complement” of A.[1]

$\langle a, b\rangle$ is an **ordered pair**. Unlike $\{a, b\}$, the order of the elements matters since $\langle a, b\rangle \neq \langle b, a\rangle$ (except when $a = b$).

$\langle a, b\rangle$ is usually defined as the set: $\{\{a\}, \{a, b\}\}$.

By extension, the ordered triple $\langle a, b, c\rangle$ is the ordered pair $\langle\langle a, b\rangle, c\rangle$; the ordered quadruple $\langle a, b, c, d\rangle$ is the ordered pair $\langle\langle a, b, c\rangle, d\rangle = \langle\langle\langle a, b\rangle, c\rangle, d\rangle$. And so on for any ***n*-tuple**, a.k.a. **sequence.** (Technically, an “n-tuple” can be a zero- or single-membered set, but normally the focus is on cases where $n \geq 2$.)

$\{\langle x_1, \ldots, x_n\rangle \mid Cx_1, \ldots, x_n\}$ is the set of n-tuples that satisfy condition C.
$A \times B$ is the **Cartesian product** of A and B: It is the set of all ordered pairs whose first member is in A and whose second member is in B.

I.e., $A \times B = \{\langle x, y\rangle \mid x \in A \text{ and } y \in B\}$

For $n \geq 2$, A^n is the **Cartesian power** of A; it is the set of n-tuples whose members are in A.

I.e., $A^n = \{\langle x_1, \ldots, x_n\rangle \mid x_1 \in A \text{ and} \ldots \text{and } x_n \in A\}$.

[1] But normally, $\bar{A}$ is *not* identified as the absolute complement of A, i.e., it is not identified with the set $\{x \mid x \notin A\}$, since that would create a Russell-like paradox.

Naïve Set Theory

Axiom of Extensionality: A = B iff: for any x, $x \in$ A iff $x \in$ B.

-This secures that {3, 4} = {4, 3}, and that {3, 3} = {3}.

Axiom of Comprehension: For any condition C, there is an A such that $x \in$ A iff x satisfies C.[2]

-The Russell set R shows that this "axiom" is false, where R = $\{x \mid x \notin x\}$

Zermelo-Frankel (ZF) Set Theory includes Extensionality, but instead of Comprehension…

Axiom of Separation: If A is a set, then so is any subset of A.

I.e. If there is a set A, then there is a set $\{x \in A \mid Cx\}$, where C is any condition.

-This does not allow the Russell set. At most, it allows $\{x \in A \mid x \notin x\}$ which will be A itself (assuming that no x violates the Axiom of Regularity; see below).

Pair Axiom: For any x and y, there is a set $\{x, y\}$. (If $x = y$, then it will just be $\{x\}$.)

Union Axiom: If B = $\{A_1 \ldots A_n\}$, then the general union of B exists: $\bigcup B = A_1 \cup \ldots \cup A_n$.

Axiom of Infinity: There is a set $\mathbb{N} = \{x \mid x$ is a natural number$\}$. (See below for more.)

Powerset Axiom: If A is a set, then so is $\mathscr{P}$A.

Axiom of Regularity/Foundation: If A ≠ ∅, then for some $x \in$ A, there is no y is such that $y \in x$ and $y \in$ A.[3]

Axiom of Replacement: Suppose that for every $x \in$ A, there is a unique y such that Cxy. Then there is a set B of exactly these y.

Axiom of Choice: (ZF is often called "ZFC" due to the Choice Axiom.) Given a set of sets B = $\{A_1 \ldots A_n\}$, there is a function $g(x)$ such that for each $A_k \in B$, $g(A_k) = y$, where $y \in A_k$. (Basically, $g(x)$ "chooses" an element from each set in B.)

2. Set Theory and Number Theory

The set of **natural numbers** $\mathbb{N} = \{0, 1, 2, 3\ldots\}$

The set of **positive integers** $\mathbb{P} = \mathbb{N} \setminus \{0\} = \{1, 2, 3\ldots\}$

The set of **integers** $\mathbb{Z} = \{\ldots\text{-}3, \text{-}2, \text{-}1, 0, 1, 2, 3, \ldots\}$ = the union of $\mathbb{N}$ with its additive inverses.

The set of **rationals** $\mathbb{Q} = \{x \mid$ there is an $m \in \mathbb{Z}$ and an $n \in \mathbb{Z}$ such that $x = m/n\}$

The set of **reals** $\mathbb{R}$ = the union of $\mathbb{Q}$ with the set of irrationals.[4]

Zermelo's definition of $\mathbb{N}$:

1. Let ∅ define 0.
2. If a set A defines n, then {A} defines n+1.

   -Thus, {∅} defines 1, {{∅}} defines 2, {{{∅}}} defines 3, etc.

[2] Comprehension is not really an axiom but an axiom-*schema*: It implies a distinct axiom for each condition C that might occur in the schema. Ditto for the Separation "axiom" and the Replacement "axiom" in ZF.

[3] Regularity is often phrased instead as "each set A is disjoint with at least one of its own elements." But the drawback is that 'disjoint' applies only to sets; cf. Patrick Suppes (1971), *Axiomatic Set Theory*, Dover, p. 54. This means that "impure" sets like {Socrates} are ruled out, for Socrates is not "disjoint" with {Socrates}. Even so, ZF(C) is now standardly seen as concerned just with *pure* sets (∅ and sets that contain only sets). Yet in metalogic, we need sets *of formulae* to prove metatheorems. So I prefer Suppes' version of the Regularity Axiom, above.

[4] How to define the set of irrationals? Dedekind pioneered a partial definition using "cuts;" see Richard Dedekind, "Continuity and the Irrational Numbers," in *Essays on the Theory of Numbers*, New York: Dover, 1963. pp. 1-27.

Von Neumann's definition of $\mathbb{N}$:

1. Let ∅ define 0.
2. If a set A defines n, then $A \cup \{A\}$ defines $n+1$.
   -Thus, {∅} defines 1, {∅, {∅}} defines 2, {∅, {∅}, {∅, {∅}}} defines 3, etc.

Von Neumann's definition is equivalent to: Any natural number is the set of its predecessors. This claim can be extended to define transfinite numbers (which gives von Neumann's definition an advantage over Zermelo's).

3. Functions and Relations

Intuitively, a **function** F is an operation or rule which takes an element as input and associates it with an output or value such that **well-definedness** is satisfied: Each input is associated with a unique output. The set of inputs is the **domain** of F, written 'domF', whereas the set of outputs is its **range**, written 'ranF'. Take heed that a single "input" or "output" can be an n-tuple. Functions with n-tuple inputs are often our concern, and in such cases, we distinguish an input from its members by calling the latter the **arguments** of the function.

Notation: If d is an input to a function F, then 'F(d)' denotes the output of F on that input; e.g., if the successor function is $S(x) = x + 1$, then 'S(2)' denotes 3. Such a term can then indicate the input in further cases: Where $F(x) = x^2$, $F(S(2)) = 9$, $F(F(S(2))) = 81$, etc.

Mathematically, a function is defined *not* by specifying an operation or rule, but rather just by a set of input-output pairs of the form "⟨input, output⟩"

E.g., the squaring function on $\mathbb{Z}$ is {…⟨-2, 4⟩, ⟨-1, 1⟩, ⟨0, 0⟩, ⟨1, 1⟩, ⟨2, 4⟩…}, and the addition function on $\mathbb{P}$ is {⟨⟨1, 1⟩, 2⟩, ⟨⟨1, 2⟩, 3⟩…⟨⟨2, 1⟩, 3⟩, ⟨⟨2, 2⟩, 4⟩…}.

Accordingly, functions F and G are identical iff they have the same outputs on the same inputs (even if the operations/rules that characterize F vs. G are very different).

A function F **on A** is such that domF ⊆ A and ranF ⊆ A.[5] In cases where domF = A, we say it is **total function on A** (e.g., the successor function on $\mathbb{N}$). But if domF ⊂ A, then F is a **partial function on A** (e.g., the anti-successor function on $\mathbb{N}$).

If domF = A and ranF ⊆ B, we are able to say that F maps A **into** B, written 'F: A → B'. In cases where ranF = B, we can say more precisely that F maps A **onto** B. (Note that a function "on A" might not be *onto* A, e.g., the squaring function on $\mathbb{Z}$. This may be why 'over A' is sometimes used instead of 'on A'.)

A function F is **one-to-one** iff it never yields the same output on two different inputs.

I.e., F is one-to-one iff, for all x and y, $F(x) = F(y)$ only if $x = y$. (This is the converse of well-definedness.)

[5] Actually, mathematicians use the expression 'on A' more liberally. Consider that addition "on $\mathbb{P}$" does not have (any subset of) $\mathbb{P}$ as a domain, but rather $\mathbb{P} \times \mathbb{P}$. My guess is that we can say a function is "on A" anytime the function just relates members of A or members of some Cartesian power of A. (Ditto for relations.)

If F maps A onto B *and* is one-to-one, then there is a **1-1 correspondence between A and B**, sometimes written as '$A \asymp B$'.[6] This will be important in the next section.

A **binary relation** on sets A and B is a set of ordered pairs $\langle x, y\rangle$ where $x \in$ A and $y \in$ B. We speak here too of A as the domain and B as the range. Indeed, all functions are binary relations, but not vice-versa: Some binary relations pair an element of the domain with more than one member of the range. E.g., the relation $x < y$ on $\mathbb{Z}$ pairs any integer to infinitely many other integers. In the case of $x = 1$, the relation contains the pairs $\langle 1, 2\rangle$, $\langle 1, 3\rangle$, $\langle 1, 4\rangle$, etc.

Generalizing, if $A_1, \ldots, A_n$ are sets, then an ***n*-ary relation among $A_1 \ldots A_n$** is a set of n-tuples $\langle x_1, \ldots, x_n\rangle$ such that $x_1 \in A_1$ and…and $x_n \in A_n$.

Some sets—including many functions and relations—are characterized by a rule or operation that is an **effective method**, i.e., an **algorithm**. Roughly, this means that there is a finite series of well-defined, computer-implementable (or "mechanical") instructions, which can be completed in a finite amount of time, for identifying members of the set. Iff some algorithm correctly identifies that $x \in$ A, for any $x \in$ A, then A is **semi-decidable** or **effectively enumerable**. Whereas, iff some algorithm does this *and* correctly identifies that $y \notin$ A, for any $y \notin$ A, then A is **decidable** or **computable**. (N.B., Any decidable set is also "semi-decidable.")

Church's Thesis (CT), sometimes known as Turing's Thesis, says that any intuitively computable set is computable by a Turing Machine. CT is not believed to admit of strict mathematical proof, but it is useful in the attempt to make more precise our intuitive notions of "algorithm," "decidable," "computable," etc.

4. Sizes of Sets

The **cardinality** of A (or the cardinal number of A), written '$|A|$' or '$\overline{\overline{A}}$', indicates how many elements the set has.

$|A| = |B|$ iff there is a 1-1 correspondence between them. We then say that the sets are **equinumerous.**
$|A| > |B|$ iff, first, there is a 1-1 correspondence between B and a proper subset of A, and second, there is no 1-1 correspondence between B and A.

A set A is **finite** iff there is no 1-1 correspondence between A and any proper subset of A.
A set A is **infinite** iff there is a 1-1 correspondence between A and some proper subset of A.
-The 1-1 correspondence between $\mathbb{N}$ and its even members shows that $\mathbb{N}$ is infinite.
For any finite set A, $|A|$ is a natural number; whereas, $|\mathbb{N}| = \aleph_0$ (pronounced "aleph-nought"); this is the first transfinite cardinal number.

[6] Lots of people use the terms 'injection', 'surjection', and 'bijection' in this area, but I find that terminology confusing for more than one reason. I try to avoid it.

A set is **denumerable** or **countably infinite** iff it's equinumerous with $\mathbb{N}$.
A set is **enumerable** or **countable** iff it's either finite or denumerable.

N.B. This does not imply that the set is *recursively* enumerable.

A set is **nonenumerable** or **uncountable** iff it has a cardinality greater than $\aleph_0$.

Fun Facts:

1. $|\mathbb{N}| = |\mathbb{Q}| = \aleph_0$. That is so, even though $\mathbb{N} \subset \mathbb{Q}$.
2. For any set A, $|\mathscr{P}A| > |A|$. (Cantor's Theorem.) Thus, $|\mathscr{P}\mathbb{N}| > |\mathbb{N}|$.
3. $|\mathbb{R}| > \aleph_0$. I.e., $|\mathbb{R}|$ is infinite but there is no 1-1 correspondence between the natural numbers and the reals.
4. $|\mathbb{R}| = 2^{\aleph_0}$. That is, the cardinality of the reals = 2·2·2…

Are there are any infinite cardinals between $\aleph_0$ and $2^{\aleph_0}$? The **Continuum Hypothesis** (CH) says 'no'; it is expressed as the claim that $2^{\aleph_0} = \aleph_1$. It has been shown, however, that there is no proof of either CH or its negation in ZFC (assuming ZFC is consistent).

Cardinal Arithmetic[7]

Addition: For any cardinal numbers κ and λ, $\kappa + \lambda = |A \cup B|$, where $|A| = \kappa$ and $|B| = \lambda$, and where A and B are disjoint. Corollary:

-If $|A| \leq \aleph_0$, then $\aleph_0 + |A| = \aleph_0$. (Cf. Hilbert's Hotel). And in general, if at least one of $|A|$ and $|B|$ is infinite, then their sum is equal to whichever of $|A|$ or $|B|$ is greater. (If they are each equal to an infinite κ, then their sum is κ.)

Multiplication: $|A|\cdot|B| = |A \times B|$. I.e. The product of these cardinalities equals the cardinality of their Cartesian product. Corollary:

-If at least one of $|A|$ and $|B|$ is infinite, then their product equal to whichever of $|A|$ and $|B|$ is greater. (If they are each equal to an infinite κ, then their product is κ.)

Exponentiation: $|A|^{|B|}$ is the cardinality of the set of all functions from B into A.

I.e., $|A|$ to the power of $|B|$ equals the cardinality of the set E of all sets of pairs $\langle x, y\rangle$ such that $x \in B$ and $y \in A$ (where for any set $S \in E$, and given any $x \in B$, there is exactly one pair in S with x as its first member).

Other arithmetic operations are definable from these per usual. E.g., $|A| - |B| = |C|$ iff $|C| + |B| = |A|$, and if $|B| \neq 0$, then $|A| / |B| = |C|$ iff $|A| = |C|\cdot|B|$.

[7] Similar arithmetic operations exist for ordinal numbers, including the transfinite ordinals ω, ω^2, ω^ω, etc. But there are disanalogies, e.g., $2^\omega = \omega$, whereas $2^{\aleph_0} > \aleph_0$. Transfinite ordinal arithmetic also comes with other surprises, such as the fact that addition is not commutative, e.g., $2 + \omega \neq \omega + 2$.