Set Theory

P. K. Tam

I. Sets

1. Simple Logic

We summon up here some working knowledge of simple logic. A ***statement*** (***assertion***, ***sentence***) is a collection of words which is either "true" or "false" but not both. When a statement is true we say that its ***truth-value*** is 1; when it is false, its truth value 0; the truth-value of a statement is therefore either 1 or 0, but not both. Logical constants $\sim$ (***negation***), $\vee$ (***disjunction***), $\wedge$ (***conjunction***), $\Rightarrow$ (***implication***) and $\Leftrightarrow$ (***equivalence***) are used to construct new statements from given statements. for statements p and q, the truth-values of $\sim p$, $p \wedge q$, $p \vee q$, $p \Rightarrow q$ and $p \Leftrightarrow q$ are determined by the following table:

p	$\sim p$
0	1
1	0

p	q	$p \wedge q$	$p \vee q$	$p \Rightarrow q$	$p \Leftrightarrow q$
0	0	0	0	1	1
0	1	0	1	1	0
1	0	0	1	0	0
1	1	1	1	1	1
verbally (we say)		p and q	p or q (in the inclusive sense)	p implies q (if p, then q)	p if and only if q

We often express the statement "For every x, p" by using the symbol $\forall$ (called the ***universal quantifier***): "$\forall x$, p" [more syntactically, $(\forall x)\,(p)$]. Similarly, the symbol $\exists$ (called the ***existential quantifier***) can be used to write "$\exists x$, p" [more syntactically, $(\exists x)(p)$] instead of "There exists x such that p". One should note carefully that the negation of $(\forall x)(p)$ is $(\exists x)(\sim p)$, and the negation of $(\exists x)(p)$ is $(\forall x)(\sim p)$.

2. Sets

Our goal is to acquire some working knowledge of the easier part of ZF set theory (ZF stands for Zermelo-Fraenkel). For an axiomatic (or "pro-axiomatic") approach, the following books are recommended:

(1) A.Hajnal and P.Hamburger, Set Theroy, Cambridge University Press, 1999.

(2) D. Goldrei, Classic Set Theory: a guided independent study, chapman & Hall, 1996.

(3) Y.N. Moschovakis, Notes on Set Theory, Springer-Verlag, 1994.

(4) K.T. Leung and Doris L.C. Chen, Elementary Set Theory, Hong Kong University Press, 1967.

We give below some explanation of the axioms without naming them. We believe that the ZF set theory is consistent (i.e. no contradiction will arise), and we can safely manipulate sets according to it. The concepts "***set***" and "***being an element of***" are primitive (undefined). For lucid expression, we often say/write "x contains u" or "u belongs to x" meaning "$u \in x$". Two sets x and y are equal, in symbol $x = y$, if they contain the same elements i.e., $(\forall u)(u \in x \Leftrightarrow u \in y)$. For our intuitive interpretation, a set may be regarded as an (intellectual or mathematical) object determined by its elements e.g., a set of people, a set of sheep, or a set of numbers. We write "$\sim (u \in x)$" simply as "$u \notin x$".

All positive integers constitute a unique set $\mathbb{N}$ i.e., $\mathbb{N}$ is the set which contains every positive integer and nothing else. We speak of $\mathbb{N}$ as the set of all positive integers (with

the expression "and nothing else" understood and suppressed), and write

$$\mathbb{N} = \{x \mid x \text{ is a positive integer}\}.$$

From $\mathbb{N}$ we can construct the sets $\mathbb{Z}$ (of all integers), $\mathbb{Q}$ (of all rational numbers), $\mathbb{R}$ (of all real numbers), and $\mathbb{C}$ (of all complex numbers), and introduce the usual operations "addition", "subtraction", "multiplication" and "division". In fact, we can construct the positive integers 1,2, ... from the ***empty set*** $\emptyset$ which is, by definition, the set containing no element:

$$\emptyset = \{x \mid x \neq x\}.$$

This story is however too long for us to go into; interested readers are referred to the references cited above.

Given $a_1, a_2, \cdots, a_n$, where n is any positive integer, there is a set which contains exactly these $a_1, a_2, \cdots, a_n$ as its elements (and nothing else); this unique set is denoted by: $\{x \mid x = a_1, a_2, \cdots, \text{ or } a_n\}$, or more simply $\{a_1, a_2, \cdots, a_n\}$.

More generally, given a set I and sets a_i for each $i \in I$, there is a set containing exactly the a_i, $i \in I$, as its elements; we denote this set simply as $\{a_i \mid i \in I\}$.

For sets x and y, y is said to be a ***subset*** of x, in symbol $y \subset x$, if each element of y is an element of x i.e., $(\forall u)(u \in y \Rightarrow u \in x)$. All subsets y of x constitute a unique set $\wp(x)$, called the ***power set*** of x:

$$\wp(x) = \{y \mid y \subset x\}.$$

For sets $a_1, a_2, \cdots, a_n$, where n is a positive integer, we can produce a set, called the ***union*** of $a_1, a_2, \cdots$, and a_n, in symbol $a_1 \cup a_2 \cup \cdots \cup a_n$ or more concisely $\bigcup_{j=1}^{n} a_j$, by the definition:

$$a_1 \cup a_2 \cup \cdots \cup a_n = \{x \mid x \in a_j \text{ for some } j = 1, 2, \cdots, n\}.$$

So $\bigcup_{j=1}^{n} a_j$ is the set which contains every element of each a_j, $j = 1, 2, \cdots, n$, and nothing else. More generally, for a set x, there exists a set, called the ***union of x***, in symbol $\bigcup x$,

which contains every element of each element of x (and nothing else):

$$\bigcup x = \{y \mid y \in u \text{ for some } u \in x\}.$$

So $\bigcup\{a_1, a_2\} = a_1 \cup a_2$, and $\bigcup \emptyset = \emptyset$.

Given a set u and a statement $p(x)$ involving (a free variable) x, there exists a set y which contains exactly those elements z of u such that $p(z)$ is true:

$$y = \{z \mid z \in u, \ \ p(z) \text{ is true } \}$$

is a set. As an example, for sets a_1, a_2 applying the above with a_1 as u, and "$x \in a_2$" as $p(x)$, we conclude that there is a set which contains exactly those elements z of a_1 such that $z \in a_2$, i.e. $\{z \mid z \in a_1, \ \ z \in a_2 \text{ is true } \}$ is a set. This set is denoted by $a_1 \cap a_2$, and is called the ***intersection*** of a_1 with a_2. Similarly we can define the ***intersection*** of a set a_1 with sets $a_2, a_3, \cdots, a_n$ (where n is a positive integer ≥ 2), denoted by $a_1 \cap a_2 \cap \cdots \cap a_n$ or $\bigcap_{j=1}^{n} a_j$, by:

$$\bigcap_{j=1}^{n} a_j = \{z \mid z \in a_1, \text{ "}z \in a_2, z \in a_3, \cdots, \text{ and } z \in a_n\text{" is true } \}.$$

Now it is easy to see that the set $a_1 \cap a_2 \cap \cdots \cap a_n$ is independent of the ordering of sets $a_1, a_2, \cdots, a_n$ e.g., $a_1 \cap a_2 = a_2 \cap a_1$, $a_1 \cap a_2 \cap a_3 = a_3 \cap a_1 \cap a_2$. Also we can define the ***intersection*** of a ***non-empty*** set x by:

$$\bigcap x = \{z \mid z \in u \text{ for every } u \in x\}$$

which is, we emphasize, a set. For example,

$$\bigcap\{a_1, a_2\} = a_1 \cap a_2.$$

Sets a_1 and a_2 are said to be ***disjoint*** if $a_1 \cap a_2 = \emptyset$; a set s of sets is said to be ***pairwise disjoint*** if for all distinct $a, b \in s$, $a \cap b = \emptyset$.

Let I be a set, and let a_i be a set for each $i \in I$. Then there exists a set which contains exactly the $a_i's$, and is denoted by: $\{u \mid u = a_i \text{ for some } i \in I\}$, or in short $\{a_i \mid i \in I\}$.

The set $\bigcup\{a_i \mid i \in I\}$ is also written as $\bigcup_{i\in I} a_i$; similarly the set $\bigcap\{a_i \mid i \in I\}$ is also written as $\bigcap_{i\in I} a_i$.

For sets a and b, there is a set, called the ***complement*** of b in a and denoted by $a \setminus b$, which contains exactly those elements of a which do not belong to b:

$$a \setminus b = \{x \mid x \in a,\ x \notin b\}.$$

Given a and b, we can define an ordered pair (a, b) ($oversetdef{=}\big\{\{a\}, \{a, b\}\big\}$) such that ordered pairs (a, b) and (c, d) are equal if and only if $a = c$ and $b = d$. For sets y and z there exists a set called the (***Cartesian***) ***product*** of y by z, denoted by $y \times z$, which contains exactly all ordered pairs (a, b) formed by $a \in y$ and $b \in z$:

$$y \times z = \{t \mid t = (a, b) \text{ for some } a \in y \text{ and } b \in z\}.$$

Similarly given sets $y_1, y_2, \cdots, y_n$, where $n \in \mathbb{N}$, we can form the (***Cartesian***) ***product*** of $y_1, y_2, \cdots, y_n$, denoted by $y_1 \times y_2 \times \cdots \times y_n$ or $\prod_{j=1}^n y_j$, which is the set containing exactly all ***ordered n-tuples*** $(a_1, a_2, \cdots, a_n)$ with $a_j \in y_j$, $j = 1, 2, \cdots, n$:

$$\prod_{j=1}^{n} y_j = \{t \mid t = (a_1, a_2, \cdots, a_n),\ \text{where } a_j \in y_j \text{ for } j = 1, 2, \cdots, n\};$$

we note that $(a_1, a_2, \cdots, a_n) = (b_1, b_2, \cdots, b_n)$ if and only if $a_j = b_j$ for $j = 1, 2, \cdots, n$. As examples we have $\mathbb{R}^n$ and $\mathbb{C}^n$:

$$\mathbb{R}^n = \underbrace{\mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R}}_{n \text{ terms}} \quad , \quad \mathbb{C}^n = \underbrace{\mathbb{C} \times \mathbb{C} \times \cdots \times \mathbb{C}}_{n \text{ terms}}.$$

The ***product*** of an arbitrary ***family*** of sets will be defined at the end of §5 below.

3. Some Simple Formulas

Theorem 1. *We have the following formulas for sets a, b, c:*

(i) $a \subset b$ *iff* $a \cup b = b$ *iff* $a \cap b = a$ *iff* $a \setminus b = \phi$ *iff* $b \setminus (b \setminus a) = a$;

(ii) $a \cup \phi = a$, $a \cap \phi = \phi$;

(iii) $a \cup b = b \cup a, \quad a \cap b = b \cap a;$

(iv) $(a \cup b) \cup c = a \cup (b \cup c), \quad (a \cap b) \cap c = a \cap (b \cap c);$

(v) $a \cup (b \cap c) = (a \cup b) \cap (a \cup c), \quad a \cap (b \cup c) = (a \cap b) \cup (a \cap c);$

(vi) (*De Morgan's rules*)

$$a \setminus (b \cup c) = (a \setminus b) \cap (a \setminus c), \qquad a \setminus (b \cap c) = (a \setminus b) \cup (a \setminus c);$$
$$(b \cup c) \setminus a = (b \setminus a) \cup (c \setminus a), \qquad (b \cap c) \setminus a = (b \setminus a) \cap (c \setminus a);$$

(vii) $a \cap (b \setminus c) = (a \cap b) \setminus (a \cap c), \qquad a \cup (b \setminus c) = (a \cup b) \setminus (c \setminus a);$

$(viii)$ *if* $a \subset c$, *then* $a \setminus b = a \cap (c \setminus b)$,

(ix) $a \subset b \Leftrightarrow c \setminus b \subset c \setminus a;$

(x)

$$a \cap (\bigcup c) = \bigcup\{a \cap x : x \in c\}, \qquad a \cap (\bigcap c) = \bigcap\{a \cap x : x \in c\},$$
$$a \cup (\bigcup c) = \bigcup\{a \cup x : x \in c\}, \qquad a \cup (\bigcap c) = \bigcap\{a \cup x : x \in c\},$$
$$a \setminus (\bigcup c) = \bigcap\{a \setminus x : x \in c\}, \qquad a \setminus (\bigcap c) = \bigcup\{a \setminus x : x \in c\};$$

(xi) $a \times b = \phi$ *iff either* $a = \phi$ *or* $b = \phi;$

(xii) $(a \cup b) \times c = (a \times c) \cup (b \times c), \qquad c \times (a \cup b) = (c \times a) \cup (c \times b);$

$(xiii)$ $(a \cap b) \times c = (a \times c) \cap (b \times c), \qquad c \times (a \cap b) = (c \times a) \cap (c \times b);$

(xiv) $(a \setminus b) \times c = (a \times c) \setminus (b \times c), \qquad c \times (a \setminus b) = (c \times a) \setminus (c \times b);$

(xv) $a \subset b \Rightarrow a \times c \subset b \times c,$

$(c \neq \phi$ *and* $a \times c \subset b \times c) \Rightarrow a \subset b,$

$(c \neq \phi$ *and* $c \times a \subset c \times b) \Rightarrow a \subset b.$

4. Mappings

A ***mapping*** from (or on) a set s to (or into) a set t is an ordered triple $f = (s, t, F)$ where $F \subset s \times t$ satisfies:

(i) for each $x \in s$, there exists $y \in t$ such that $(x, y) \in F$;

(ii) for each $x \in s$, and for $y, z \in t$,

$$\big((x, y) \in F \text{ and } (x, z \in F)\big) \Rightarrow y = z.$$

Very often we write "$f : s \to t$ (is a mapping)" or "f maps s to t" instead of "$f = (s, t, F)$ is a mapping", and write "$f : x \mapsto y$" or "y=f(x)" instead of "$(x, y) \in F$". In this notation, we express F by "$y = f(x),\ x \in s$". s is called the ***domain*** (or the **set of departure**) of f, denoted by $D(f)$; t is called the **target** (or the **set of destination**) of f, denoted by $R(f)$; y is called the ***image of*** x ***under*** f, f is said to map x onto y, and x is called a ***pre-image*** of y under f. Note that for an arbitrary $z \in t$, there may be distinct $x, w \in s$ satisfying $(x, z), (w, z) \in F$ i.e. $f(x) = z = f(w)$; on the other hand, there may not be any $x \in s$ satisfying $(x, z) \in F$ i.e. $f(x) = z$. f is said to be ***surjective*** (or f is a ***surjection***) if for each $z \in t$, there exists (at least one) $x \in s$ such that $f(x) = z$; f is said to be ***injective*** (or f is an ***injection***) if for any $x, w \in s$, $f(x) = f(w) \Rightarrow x = w$; f is said to be bijective (or f is a ***bijection***) if f is both surjective and injective.

We note that mappings $f : s \to t$ and $g : u \to v$ are equal if and only if $s = u$, $t = v$, and $f(x) = g(x)$ for every $x \in s$.

For $f : s \to t$ and $a \subset s$, we define $\boldsymbol{f(a)} = \{u \in t \mid u = f(x) \text{ for some } x \in a\}$, which is called the ***image*** of a under f. $f(s)$ is called the ***total image of*** f, or **range** of f, denoted by ***Im(f)***. For $b \subset t$, we define $\boldsymbol{f^{-1}(b)} = \{x \mid x \in s,\ f(x) \in b\}$, and call $f^{-1}(b)$ the ***pre-image*** of b under f. In case $b = \{z\}$ (where $z \in t$), we write $f^{-1}(z)$ instead of $f^{-1}(\{z\})$. We have the following

Theorem 2. *Let $f : s \to t$ be a mapping, $a_1, a_2 \subset s$, $A \subset \wp(a)$, $b_1, b_2 \subset t$, and $B \subset \wp(t)$. Then*

(i)

$$f(a_1 \cup a_2) = f(a_1) \cup f(a_2), \quad f(a_1 \cap a_2) \subset f(a_1) \cap f(a_2),$$
$$f(a_1 \setminus a_2) \supset f(a_1) \setminus f(a_2), \quad f\left(\bigcup A\right) = \bigcup \{f(a) : a \in A\},$$
$$f\left(\bigcap A\right) \subset \bigcap \{f(a) : a \in A\} \text{ (assuming } A \neq \emptyset \text{ for this formula);}$$

(ii)

$$f^{-1}(b_1 \cup b_2) = f^{-1}(b_1) \cup f^{-1}(b_2), \quad f^{-1}(b_1 \cap b_2) = f^{-1}(b_1) \cap f^{-1}(b_2),$$

$f^{-1}(b_1 \setminus b_2) = f^{-1}(b_1) \setminus f^{-1}(b_2)$, $\quad f^{-1}\left(\bigcup B\right) = \bigcup \{f^{-1}(b) : b \in B\}$,
$f^{-1}\left(\bigcap B\right) = \bigcap \{f^{-1}(b) : b \in B\}$ (*assuming* $B \neq \emptyset$ *for this formula);*

(*iii*) $f^{-1}(f(a)) \supset a$, $f(f^{-1}(b)) \subset b$;
(*iv*) *if* f *is injective, then*

$f(a_1 \cap a_2) = f(a_1) \cap f(a_2)$, $\quad f\left(\bigcap A\right) = \bigcap \{f(a) : a \in A\}$ *for* $A \neq \emptyset$,
$f(a_1 \setminus a_2) = f(a_1) \setminus f(a_2)$, $\quad f^{-1}(f(a)) = a$;

(*v*) *if* f *is surjective, then* $f(f^{-1}(b)) = b$.

For mappings $f : s \to t$, $g : u \to v$, the mapping $(f^{-1}(u), v, H)$ given by

$$H = \left\{(x, z) \in f^{-1}(u) \times v \mid z = g(y),\, y = f(x)\right\}$$

is called the ***composite*** of g by f, denoted by $g \circ f$. Thus $g \circ f$ maps $f^{-1}(u)$ (which may be empty) into v, and for each $x \in f^{-1}(u)$,

$$(g \circ f)(x) = g(f(x)).$$

Note that in general $g \circ f \neq f \circ g$, even if they have the same domain. For a set s, the mapping $\boldsymbol{i_s} : s \to s$ given by $\boldsymbol{i_s}(x) = x, x \in s$, is called the ***identity mapping*** on s. We can easily prove

Theorem 3. *We have the following.*
(*i*) *Let* $f : s \to t$, $g : t \to u$, *and* $h : u \to v$ *be mappings. Then* $h \circ (g \circ f) = (h \circ g) \circ f$.
(*ii*) *Let* $f : s \to t$ *be an injection. There exists uniquely a mapping* $\bar{f}^{1} : Im(f) \to s$, *called the* ***inverse*** (*mapping*) *of* f, *such that* $\bar{f}^{1} \circ f = i_s$. *Moreover we have:* $f \circ \bar{f}^{1} = i_{Im(f)}$.

We write f^{-1} *instead of* $\bar{f}^{1}$ *when it is more convenient to do so and when no confusion is likely to arise.*
(*iii*) *A mapping* $f : s \to t$ *is injective if and only if for any mappings* $p : w \to s$, $q : w \to s$,

$$f \circ p = f \circ q \Rightarrow p = q.$$

(*iv*) *The composite* $g \circ f$ *of injections* $f : s \to t$ *and* $g : t \to u$ *is an injection.*

(*v*) *A mapping* $f : s \to t$ *is surjective if and only if for any mappings* $k : t \to r$, $\ell : t \to r$,

$$k \circ f = \ell \circ f \ \Rightarrow k = \ell.$$

(*vi*) *The composite* $g \circ f$ *of surjections* $f : s \to t$ *and* $g : t \to u$ *is a surjection.*

(*vii*) *Let* $f : s \to t$, $g : t \to u$ *be mappings, let* $a \subset s$, *and let* $b \subset u$. *Then*

$$(g \circ f)(a) = g(f(a)), \qquad (g \circ f)^{-1}(b) = f^{-1}\left(g^{-1}(b)\right).$$

(*viii*) *Let* $f : s \to t$, $g : t \to u$ *be bijections. Then* $g \circ f$ *is bijective and the inverse mapping* $(g \circ f)^{-1}$ *of* $g \circ f$ *is equal to the composite of the inverse mapping* f^{-1} *by the inverse mapping* g^{-1} *:*

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Let I be a set and let a_i be a set for each $i \in I$, the mapping f on I to the set $\{a_i \mid i \in I\}$ given by $f(i) = a_i$ is denoted by $(a_i)_{i\in I}$, and is called a ***family*** of sets. When $I = \mathbb{N}$ (respectively, $\{1, 2, \cdots, n\}$ for some $n \in \mathbb{N}$), f is called a ***sequence*** (resp., ***finite sequence***). The set of all mappings g on I to the set $\bigcup_{i\in I} a_i$ such that $g(i) \in a_i$ for each $i \in I$ is called the ***product*** of $(a_i)_{i\in I}$, and is denoted by $\prod_{i\in I} a_i$:

$$\prod_{i\in I} a_i = \{g \mid g : I \to \bigcup_{i\in I} a_i \text{ is a mapping, } g(i) \in a_i \text{ for each } i \in I\}.$$

Note that when $I = \{1, 2, \cdots, n\}$(where $n \in \mathbb{N}$), this is essentially $\prod_{j=1}^{n} a_j$, as we may identify $n-$tuples with mappings on I.

Remark. By the axiom of choice (to be explained in §II.3 below) we can prove that: For a surjection $f : s \to t$, there exists a mapping $g : t \to s$ such that $f \circ g = i_t$. In general, such g is not unique and $g \circ f \neq i_s$.

5. Relations

For sets a and b, a ***relation*** from a to b is an ordered triple (a, b, R) where R is a subset of the product $a \times b$. When a and b are well understood (and no confusion is likely), we

sometimes say that R [instead of (a, b, R)] is a relation. For simplicity we write xRy in place of $(x, y) \in R$.

For us the most important relations are equivalence relations and partial orders.

A ***partial order*** in a set s is a relation (s, s, R) from s to s, which satisfies the following conditions:

(i) for each $x \in s$, xRx,

(ii) for all $x, y \in s$ (meaning $x \in s, y \in s$), (xRy and yRx) $\Rightarrow x = y$,

(iii) for all $x, y, z \in s$, (xRy and yRz) $\Rightarrow xRz$.

A partial order is often denoted by $\preceq$. If for every pair of $x, y \in s$, either $x \preceq y$ or $y \preceq x$ is true, then $\preceq$ is called a **total order** (or **linear order**) in s. A partial order need not be a total order.

Let $\preceq$ be a partial order in a set s. A subset t of s is said to be **bounded above** (relative to $\preceq$) if there is $y \in s$ such that for every $x \in s$, $x \preceq y$. And y is called an **upper bound** of t. Similarly we define the concepts of t being **bounded below**, and a **lower bound** of t. An $x \in t$ is called a **maximal element** of t if there does not exist a $u \in t \setminus \{x\}$ such that $x \preceq u$, i.e. for all $v \in t$, $x \preceq v \Rightarrow x = v$. Similarly we define the concept of a **minimal element** of t. An element $x \in t$ is called a **greatest element** of t if for all $v \in t$, $v \preceq x$. A greatest element is a maximal element, but a maximal element may not be a greatest element. Similarly, we define the concept of a **least element** of t, and show that a least element is a minimal element but a minimal element may not be a least element. Note that t may not be bounded above or/and below (hence does not have an upper and/or lower bound), may not have a maximal element and/or a minimal element, may not have a greatest element and/or a least element; t may have more than one maximal elements and/or more than one minimal elements; however, t has at most one greatest element, and/or at most one least element. t is called a **chain** in s if for every pair of $x, y \in t$, either $x \preceq y$ or $y \preceq x$ is true, i.e. if the restriction of $\preceq$ to t is a total order in t.

A partial order $\preceq$ in s is called a **well order** in s if every non-empty subset t of s has a least element (in t). Clearly, a well order is a total order.

We consider a simple example. Let $s = \{3, 1\} \times [0, 2]$, and define $\preceq$ in s by:

$$(a, b) \preceq (c, d) \text{ iff } a = c, b \leq d \text{ (as real numbers)}.$$

Let $t = \{3, 1\} \times [0, 2]$, $u = \{3\} \times (0, 1)$ Then

(i) $\preceq$ is a partial order, but not a total order, in s,

(ii) t is not a chain in s, but u is a chain in s,

(iii) t has two maximal elements $(1, 2), (3, 2)$, none of which is a greatest element, t has two minimal elements $(1, 0), (3, 0)$, none of which is a least element, but u has neither a maximal element nor a minimal element,

(iv) t has neither a greatest element nor a least element,

(v) t is neither bounded above nor bounded below, but u is bounded above and below.

An ***equivalence relation*** in a set s is a relation (s, s, R) from s to s, which satisfies the following conditions:

(i) for each $x \in s$, xRx,

(ii) for any $x, y \in s$, $xRy \Rightarrow yRx$,

(iii) for any $x, y, z \in s$, (xRy and $yRz \Rightarrow xRz$).

Let R be an equivalence relation in a set s [i.e. let (s, s, R) be an equivalence relation from s to s]. For $x \in s$, we define $\dot{x}$ to be the subset of s which contains all elements $y \in s$ satisfying yRx:

$$\dot{x} = \{y \mid y \in s \text{ and } yRx\}.$$

Theorem 4. *Let R be an equivalence relation in a set s. Then*

(i) for $x, z \in s$, $\dot{x} = \dot{z}$ if and only if xRz;

(ii) for $x, z \in s$, either $\dot{x} = \dot{z}$ or $\dot{x} \cap \dot{z} = \emptyset$;

(iii) $\bigcup\{\dot{x} \mid x \in s\} = s$, where $\{\dot{x} \mid x \in s\}$ is a short form of $\{u \mid u \in \wp(s),\ u = \dot{x}$ for some $x \in s\}$.

The set $\dot{x}$ is called the ***equivalence class*** containing x, and x is called a representative of the equivalence class $\dot{x}$. The set $\{\dot{x} \mid x \in s\}$ is denoted by s/R, and is called the ***quotient set*** induced by the equivalence relation R in s. The surjection $\pi : s \to t$ given by $\pi(x) = \dot{x}$ is called the ***quotient map*** induced by R.

The concept of an equivalence relation in a set s is closely related to the concept of a partition of the set s. By a ***partition*** of a set t we mean a subset p of $\wp(t)$ satisfying:

(i) for any $u, v \in p$, either $u = v$ or $u \cap v = \emptyset$,

(ii) $\bigcup p = t$.

Thus s/R is a partition of s. On the other hand, given a partition p of a set t, we can define

$$R = \{(x, y) \in t \times t : \text{there exists } u \in p, \text{ both } x \text{ and } y \text{ belong to } u\},$$

and prove that R is the unique equivalence relation in t satisfying $t/R = p$.

II. Infinite Arithmetic

1. Equinumerous sets

If there is an injection from a set s to a set t, we write $s \leq t$; the interpretation is that s has no more elements than t (i.e. s has at most as many elements as t). A set s is said to be ***equinumerous*** with (or ***equipotent*** to) a set t, in symbol $s \approx t$, if there exists a bijection from s to t; the interpretation is that s has exactly as many elements as t. We write $s < t$ if $s \leq t$ and $s \not\approx t$. Note that for sets s, t and u, we have

(i) $s \leq s$;

(ii) $s \leq t$, $t \leq u \ \Rightarrow \ s \leq u$; and

(iii) $s \leq t$, $t \leq s \ \Rightarrow \ s \approx t$.

While the first two assertions can be easily proved, the third is the content of the next theorem.

Theorem 1 (Schröder-Bernstein)**.** *If there are injections $f : s \to t$ and $g : t \to s$, then there is a bijection from s to t.*

Proof : First we consider the special case where sets $a \supset a_1 \supset a_2$, and a bijection $\varphi : a \to a_2$ is given. We want to show that there is a bijection from a to a_1. To this end, define $a_3 = \varphi(a_1)$, $a_4 = \varphi(a_2)$, and in general $a_{n+2} = \varphi(a_n)$ for each $n \in \mathbb{N}$; define $a_\infty = \bigcap\{a_j : j \in \mathbb{N}\}$. Then $a \supset a_1 \supset a_2 \supset a_3 \supset a_4 \supset a_5 \supset \cdots \supset a_\infty$, and there are bijections $\varphi_0 : a \setminus a_1 \to a_2 \setminus a_3$, $\varphi_n : a_{2n} \setminus a_{2n+1} \to a_{2n+2} \setminus a_{2n+3}$ (for each $n \in \mathbb{N}$) given by: $\varphi_0(x) = \varphi(x)$ for $x \in a \setminus a_1$, $\varphi_n(z) = \varphi(z)$ for each $z \in a_{2n} \setminus a_{2n+1}$. Since obviously $a_\infty \approx a_\infty$, $a_{2n-1} \setminus a_{2n} \approx a_{2n-1} \setminus a_{2n}$ for each $n \in \mathbb{N}$, and since

$$a_1 = a_\infty \cup (a_1 \setminus a_2) \cup (a_2 \setminus a_3) \cup (a_3 \setminus a_4) \cup (a_4 \setminus a_5) \cup \cdots \qquad \text{(disjoint union)},$$

$$a = a_\infty \cup (a_1 \setminus a_2) \cup (a \setminus a_1) \cup (a_3 \setminus a_4) \cup (a_2 \setminus a_3) \cup \cdots \qquad \text{(disjoint union)},$$

we see that there is a bijection from a to a_1.

Now consider the general case. Let $a = s$, $a_2 = (g \circ f)(a)$, let $\varphi : a \to a_2$ be given by $\varphi(x) = g\big(f(x)\big)$, $x \in a$, and let $a_1 = g(t)$. By the preceding paragraph, $a \approx a_1$. Since $a_1 \approx t$, we conclude that $s \approx t$ as desired. □

For sets s, t and u, we have:

(i) $s \approx s$,

(ii) $s \approx t \;\Rightarrow\; t \approx s$, and

(iii) $s \approx t$, $t \approx u \;\Rightarrow\; s \approx u$.

For sets s and t, we will denote by $\boldsymbol{t^s}$ the set of all mappings from s to t:

$$\boldsymbol{t^s} = \{f \mid f \text{ is a mapping from } s \text{ to } t\}.$$

We can easily prove the following

Theorem 2. *Let a_1, a_2, b_1, b_2 be sets such that $a_1 \approx a_2$, $b_1 \approx b_2$. Then*
(i) $a_1 \cup b_1 \approx a_2 \cup b_2$, *provided* $a_1 \cap b_1 = \emptyset$, *and* $a_2 \cap b_2 = \emptyset$,
(ii) $a_1 \times b_1 \approx a_2 \times b_2$,
(iii) ${b_1}^{a_1} \approx {b_2}^{a_2}$.

Proof : Exercises. □

2. Finite and Infinite Sets, Countable and Uncountable Sets

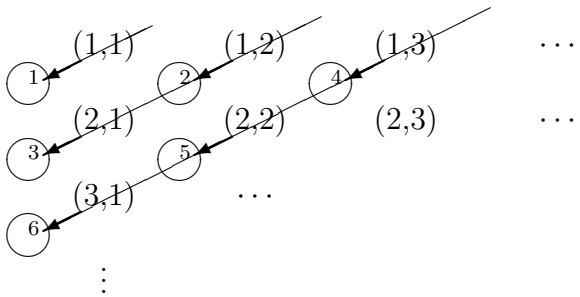
A set s is said to be ***finite*** if either $s = \emptyset$ or $s \approx \{1, 2, \cdots, n\}$ for some $n \in \mathbb{N}$; s is said to be ***infinite*** if it is not finite. s is said to be ***countably infinite*** if $s \approx \mathbb{N}$; s is said to be ***countable*** if it is finite or countably infinite; s is said to be ***uncountable*** if it is infinite but not countably infinite i.e. if $s \not\approx \{1, 2, \cdots, n\}$ for each $n \in \mathbb{N}$, and $s \not\approx \mathbb{N}$.

Theorem 3. *For every $n \in \mathbb{N}$, $\{1, 2, \cdots, n\} < \mathbb{N}$. Consequently a countably infinite set is infinite.*

Proof : In fact for each $n \in \mathbb{N}$, any map $f : \{1, 2, \cdots, n\} \to \mathbb{N}$ is not surjective. One can establish this last assertion by mathematical induction on n, or by considering $\sum_{j=1}^{n} f(j)$. □

Theorem 4. $\mathbb{N} \times \mathbb{N} \approx \mathbb{N}$. *Consequently if sets $s_1, s_2, \cdots, s_n$ are countably infinite (where $n \in \mathbb{N}$), then $s_1 \times s_2 \times \cdots \times s_n$ is countably infinite.*

Proof : A bijection $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ can be constructed according to the diagram:



e.g. $f(p,q) = \frac{1}{2}(p+q-1)(p+q-2)+p$. [One way to find an explicit expresion for f is to determine a function h such that $f(p,q) = h(p+q)+p$, where $h(2)=0$, $h(3)=1$, $h(4)=3$, $h(5)=6, \cdots$ $h(\ell+1) = p(\ell)+\ell-1$, $\ell \geq 2$.] Another bijection $g : \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ is given by $g(p,q) = 2^{p-1}(2q-1)$. (For the latter bijection g, note that each positive integer is the product of some non-negative integral power of 2 and an odd positive integer.)

By mathematical induction, we see that $\underbrace{\mathbb{N}\times\mathbb{N}\times\cdots\times\mathbb{N}}_{n\text{-times}} \approx \mathbb{N}$. The last assertion of the theorem then follows. □

Making use of Theorem 1 and Theorem 4 above, we can prove

Theorem 5. *We have:*

(*i*) *A subset of a finite* (*respectively, countable*) *set is finite* (*respectively, countable*);

(*ii*) *If sets* $s_1, s_2, \cdots, s_n$ *are finite* ($n \in \mathbb{N}$), *then* $\bigcup_{j=1}^{n} s_j$ *and* $\prod_{j=1}^{n} s_j$ *are finite;*

(*iii*) *If each* s_j, $j \in \mathbb{N}$, *is countable and if at least one of these* $s_j's$ *is infinite, then* $\bigcup_{j\in\mathbb{N}} s_j$ *is countably infinite;*

(*iv*) *If each* s_j, $j \in \mathbb{N}$, *is countable and non-empty, and if* $s_i \cap s_j = \emptyset$ *whenever* $i \neq j$, *then* $\bigcup_{j\in\mathbb{N}} s_j$ *is countably infinite.*

Proof : Exercise. □

Theorem 6. $\mathbb{N} < (0,1)$, *so* $(0,1)$ *is uncountable.*
(*As usual,* $(0,1) = \{x \in \mathbb{R} : 0 < x < 1\}$.)

Proof : Clearly the mapping $g : \mathbb{N} \to (0,1)$ given by $g(n) = \frac{1}{n+1}$ is injective. We will see that any mapping $f : \mathbb{N} \to (0,1)$ cannot be surjective. Indeed, for each $r \in f(\mathbb{N})$, there exists a $k \in \mathbb{N}$ such that $r = f(k)$. Now we can write r in a decimal expression e.g.

$$\begin{aligned} \frac{1}{2} &= 0.5\dot{0} = 0.4\dot{9}, \\ \frac{\sqrt{2}}{2} &= 0.70710678\cdots; \end{aligned}$$

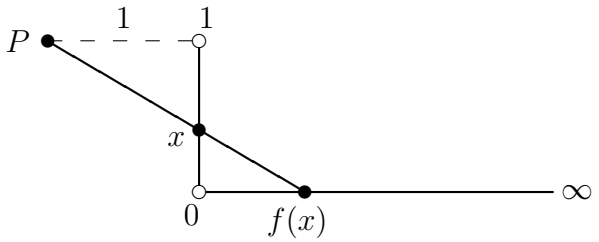
the decimal expression is unique if we discard those with recurring 9's. Thus $f(\mathbb{N})$ can be listed out as follows

$$\begin{aligned} f(1) &= 0.a_1^{(1)}a_2^{(1)}\cdots a_n^{(1)}\cdots \\ f(2) &= 0.a_1^{(2)}a_2^{(2)}\cdots a_n^{(2)}\cdots \\ &\vdots \\ f(k) &= 0.a_1^{(k)}a_2^{(k)}\cdots a_n^{(k)}\cdots \\ &\vdots \end{aligned}$$

where $a_j^{(k)} = 0, 1, 2, 3, 4, 5, 6, 7, 8$ or 9. For each $j \in \mathbb{N}$, let b_j be 2 if $a_j^{(j)} = 1$, let b_j be 1 if $a_j^{(j)} = 0, 2, 3, 4, 5, 6, 7, 8$ or 9, and let $c = 0.b_1b_2\cdots b_n\cdots$ (the real number whose decimal expression is $0.b_1b_2\cdots b_n$). Then $c \in (0, 1)$, yet for each $k \in \mathbb{N}$, $c \neq f(k)$, because $b_k \neq a_k^{(k)}$. Thus $f(\mathbb{N}) \neq (0, 1)$, and f is not surjective. □

Theorem 7. $(0, 1) \approx (0, \infty)$.
(*As usual,* $(0, \infty) = \{x \in \mathbb{R} : x > 0\}$.)

Proof : A bijection $f : (0, 1) \to (0, \infty)$ is constructed according to the diagram (by similar triangles):



e.g. $$f(x) = \frac{x}{1-x},\ x \in (0, 1).$$
(One checks easily that f is a bijection.) □

By similar methods one can prove

Theorem 8. *We have:*
(i) $\mathbb{Z} \approx \mathbb{N} \approx \mathbb{Q}$, *hence the set of all irrational numbers is uncountable;*

(*ii*) *For real numbers a and b satisfying $a < b$,*

$$(a, b) \approx (a, b] \approx [a, b) \approx (a, \infty) \approx (-\infty, b) \approx [a, \infty) \approx (-\infty, b] \approx \mathbb{R}.$$

Proof : Exercise. □

It is easy to see that

(i) $\{0, 1\}^s \approx \wp(s)$, and

(ii) $t^{\{1,2,\cdots,n\}} \approx \underbrace{t \times t \times \cdots \times t}_{n \text{ terms}}$,

where $n \in \mathbb{N}$; a proof of these is left to the reader as an exercise. A proof of the following theorem is a bit harder and will be omitted:

Theorem 9. *We have:*

(*i*) $\mathbb{N}^{\mathbb{N}} \approx (0, 1) \approx \wp(\mathbb{N})$*;*

(*ii*) *For each $n \in \mathbb{N}$, $\mathbb{R}^n \approx \mathbb{R}$;*

(*iii*) $\mathbb{R}^{\mathbb{N}} \approx \mathbb{R}$*;*

(*iv*) $\mathbb{R} < \wp(\mathbb{R}) \approx \mathbb{R}^{\mathbb{R}}$.

(These formulas also follow from some results of the next section.)

Thus, in a certain sense, $\mathbb{R}$ is infinite of a higher order than $\mathbb{N}$, and also $\mathbb{R}^{\mathbb{R}}$ is infinite of a higher order than $\mathbb{R}$. In fact we have

Theorem 10. *For any set s, $s < \wp(s)$.*

Proof : The proof is similar to that of Theorem 4. Clearly the mapping $g : s \to \wp(s)$ given by $g(x) = x, x \in s$, is injective. We will see that any mapping $f : s \to \wp(s)$ is not surjective. Indeed the set

$$t = \{x \in s \mid x \notin f(x)\}$$

belongs to $\wp(s)$, but for any $y \in s$, we have

$$\begin{cases} \text{either} & y \in f(y), \quad \text{which implies } y \notin t, \text{ hence } f(y) \neq t \\ \text{or} & y \notin f(y), \quad \text{which implies } y \in t, \text{ hence again } f(y) \neq t; \end{cases}$$

therefore we conclude that $t \notin f(s)$, and f is not surjective. □

3. The Axiom of Choice

The axiom of choice was introduced by E. Zermelo (1871-1953) in early 20th Century. Later, it is found to have many important equivalent statements and consequences, including the following.

Theorem 11. *The following statements are equivalent.*

(*i*) *The Axiom of Choice: if I is a nonempty set and if for each $i \in I$, a_i is a nonempty set, then the set $\prod_{i\in I} a_i$ is nonempty.*

(*ii*) *Zorn's Lemma: Let s be a non-empty set, and $\preceq$ a partial order in s. If every chain in s has an upper bound in s, then s has a maximal element.*

(*iii*) *The Well Order Theorem: Every set can be well-ordered, i.e. for each set s, there is a well order $\preceq$ in s.*

In 1938, K. Gödel proved that "ZF (the ZF set theory) + Axiom of Choice" is consistent if ZF is consistent. In 1963/64, P. J. Cohen proved that the Axiom of Choice is independent of ZF , i.e. the Axiom of Choice cannot be derived from ZF.

4. Cardinal Arithmetic

By using the axiom of choice, it can be proved that there exist sets , called ***cardinal numbers***, such that each set s is assigned with a cardinal number $|s|$, that equinumerous sets are assigned with one and the same cardinal number, that for each $n \in \mathbb{N}$, $|\{1, 2, \cdots, n\}| = n$, that $|\emptyset| = 0$, and that $s \approx |s|$. So cardinal numbers can be regarded as an extension of non-negative integers into the infinities. The cardinal number $|s|$ of a set s is also called the ***cardinality*** of s. Somewhat similar to Theorem 4 of §1 above, for cardinal numbers α and β we can form $\alpha + \beta$, $\alpha\beta$ and α^β, which observe the usual arithmetic (and partial order) rules for non-negative integers, e.g. $\alpha + \beta = \beta + \alpha$, $\alpha\beta = \beta\alpha$, $(\alpha+\beta)\gamma = \alpha\gamma+\beta\gamma$, $\alpha \le \beta \Rightarrow \alpha+\gamma \le \beta+\gamma$, etc. Thus arithmetic and partial order in $\mathbb{R}$ are extended to the infinities. Moreover we have the following theorem, of which a proof is not easy (c.f., for example, E. Hewitt and K. Stromberg, *Real and Abstract Analysis*, Springer-Verlag, 1969).

Theorem 12. *Let α, β be cardinal numbers. Then*

(i) *exactly one of the following holds:* $\alpha < \beta$, $\alpha = \beta$, $\beta < \alpha$;

(ii) $\alpha + \beta = \beta$, *if* $\alpha \leq \beta$ *and* β *is infinite ;*

(iii) $\alpha\beta = \beta$, *if* $0 < \alpha \leq \beta$ *and* β *is infinite;*

(iv) $\alpha^\beta = 2^\beta$, *if* $2 \leq \alpha \leq \beta$.

Using the axiom of choice we can also prove the following

Theorem 13. *For any infinite set s, $\mathbb{N} \leq s$. Consquently, $|\mathbb{N}|$ is the smallest infinite cardinal number.*