Sets, Logic, Relations, and Functions

Andrew Kay

September 28, 2014

Abstract

This is an introductory text, not a comprehensive study; these notes contain mainly definitions, basic results, and examples.

Some parts are loosely adapted from the *Discrete Computing and Algorithms* and *Software Engineering* modules on the BSc Computer Science course at Birmingham City University. However, this text is neither a subset nor a superset of the syllabus of either module.

Other parts are loosely adapted from my notes from *Numbers and Sets* from Part IA of the Mathematical Tripos at the University of Cambridge, lectured by Prof. Imre Leader. This fills in the basic details which are omitted from my notes on *Numbers and Sets, Groups and Geometry*.

Z notation is used, but not exclusively; in particular, this text should not be used as a Z notation reference. Also, for clarity in some places I have used informal notations which are not strictly correct. Informal notations are marked as such.

Some examples and footnotes may reference concepts which have not (or have not yet) been formally defined, but which the reader is likely to have an informal understanding of. Otherwise, their definitions may be found in later sections, my other sets of notes, or external sources.

1 Sets

1.1 Sets

A **set** is a collection of items; an item in a set is called an **element**, and we say the set **contains** that item. A *set literal*[1] is written using curly braces, with the elements separated by commas.

Example 1.1.1.

1. $\{1, 2, 3, 4, 5\}$
2. $\{red^2, green, blue\}$
3. $\{newyork, paris, peckham\}$

> Informal
>
> Sometimes, where a set has too many elements to write out in full, it may be written implicitly, e.g. $\{1, 2, 3, \ldots 100\}$, or $\{1, 2, 3, \ldots\}$.

Some particulars about sets:

- Sets do not naturally have orderings; there is no canonical "first" or "last" element in a set.
- Sets do not contain duplicate elements; an item is either in a set, or is not in that set.
- Sets may be empty; $\emptyset$ is written to mean a set with no elements.
- Sets may have infinitely many elements.
- Sets may contain other sets.

Definition 1.1.2.

1. *If x is in a set S, we write $x \in S$, and say "x is an element of S".*
2. *If x is not in S, we write $x \notin S$,*[3] *and say "x is not an element of S".*
3. *$S \ni x$ means $x \in S$, and $S \not\ni x$ means $x \notin S$.*[4]

[1] For example, 23 is a *literal* number. Other expressions such as x, 7^n, or "the smallest prime number", may represent numbers, but are not "literal" numbers.

[2] Items such as *red* which are not constructed from other items or sets are called **atoms**.

[3] Generally, if a symbol for a relation like $\notin$ is another relation symbol $\in$ with a diagonal line through it, then the two relations are a *dichotomy* - either $x \in S$ or $x \notin S$.

[4] Generally, if a symbol for a relation like $\ni$ is the mirror image of another symbol $\in$, then it is the same relation in reverse. However, this is often not true for binary operators.

Definition 1.1.3.

1. *Two sets S and T are* ***equal*** *(i.e. $S = T$), iff*[5] *they contain the same elements; i.e. if x is an item, then $x \in S$ iff $x \in T$.*

2. *$S \neq T$ means that S and T are not equal.*

This gives us another perspective on sets: a set S is something of which we can only ask yes-or-no questions of the form "is x an element of S?". In particular, we can only distinguish between different sets by finding an element of one set which is not an element of the other.

Example 1.1.4.

1. $\{1, 2, 3, 4, 5\} = \{5, 4, 3, 2, 1\}$.

2. $\{1, 2, 3, 4, 5\} = \{1, 2, 2, 3, 3, 3, 4, 4, 4, 4, 5, 5, 5, 5, 5\}$.

3. $\{newyork, paris, peckham\} \neq \{milan, newyork, japan\}$.

> Informal
> To distinguish between an *expression* (a combination of items and connectives which produces a value) and a *statement* (an assertion that a particular thing is true), statements may end with full stops.

1.2 Subsets

Much like we have more relations between numbers, such as $\leqslant$ and $>$, we have more relations between sets.

Definition 1.2.1. *For sets S, T,*

1. *$S \subseteq T$ iff every element of S is also an element of T. We say "S is a* ***subset*** *of T".*

2. *$S \subset T$ iff $S \subseteq T$ and $S \neq T$. We say "S is a* ***proper subset*** *of T".*

Example 1.2.2.

1. $\{1, 2, 3\} \subseteq \{1, 2, 3, 4, 5\}$.

2. $\{1, 2, 3\} \supset \emptyset$.

[5] "Iff" is a mathematical shorthand for "if and only if"; it means that two things are logically equivalent, or alternatively, they are either both true or both false.

3. $\{hydrogen, helium, \ldots\} \nsubseteq \{earth, air, fire, water\}$.

4. $\{hydrogen, helium, \ldots\} \nsupseteq \{earth, air, fire, water\}$.

5. $\{red, green, blue\} \not\subset \{red, green, blue\}$.

Definition 1.2.3. *If S is a set, then $\mathbb{P}\,S$, the* ***power set*** *of S, is the set of all subsets of S; i.e. $A \in \mathbb{P}\,S$ iff $A \subseteq S$.*

Example 1.2.4.

1. $\mathbb{P}\{yellow, green\} = \{\emptyset, \{yellow\}, \{green\}, \{yellow, green\}\}$.

2. $\mathbb{P}\{1, 2, 3\} = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

3. $\mathbb{P}\,\emptyset = \{\emptyset\}$.

Definition 1.2.5. *If P is a set of non-empty subsets of S, then P is a* ***partition*** *of S if every element of S is in precisely one element of P.*

Example 1.2.6. $\{\{1, 2\}, \{3, 4\}, \{5\}\}$ *is a partition of* $\{1, 2, 3, 4, 5\}$.

1.3 Set Comprehensions

We wish to be able to construct sets without listing their members literally.

Example 1.3.1.

1. *The set of all square numbers. In this case we want to select all of the possible results of an expression, namely n^2.*

2. *The set of all prime numbers. In this case we want to select elements which satisfy a criterion, namely that the element is prime.*

> Informal
> Sometimes a set may be written as an English description of its contents, e.g. { all square numbers }, or { all prime numbers }.

The naive way to formally notate these would be $\{\ n^2\ \}$, or $\{\ p \mid p \text{ is prime}\ \}$. However, it is ambiguous what values n is meant to take - does $\{\ n^2\}$ contain the squares of all integers, or real numbers, or matrices?

Even worse, allowing constructions of this form leads to paradoxes:

Proposition 1.3.2 (Russell's Paradox)**.** *Let* $X = \{ x \mid x \notin x \}$*. Then* $X \in X$ *iff* $X \notin X$*.*

Proof. If $X \in X$, then $x = X$ satisfies the criterion $x \notin x$ and so $X \notin X$. Conversely,[6] if $X \notin X$, then $x = X$ must *not* satisfy the criterion $x \notin x$, and so $X \in X$. □

So, when we choose our notation, we should be careful to avoid these traps which might allow us to apparently construct sets which aren't really defined, or which might even be impossible.

- We need to say what values our variables take. The most sensible way to do this is by specifying a set[7] of all possible values.
- We can't have a set S which contains itself, otherwise we can construct Russell's Paradox by letting x take values from S.
- We can't have a set E containing absolutely everything, otherwise E would contain E.

Definition 1.3.3.

1. *If* x *is a variable taking values from* S*, we write* $x : S$*.*
2. *If* x *is a variable taking only the values from* S *which satisfy some criterion, we write* $x : S \mid$ *criterion.*

The distinction between $x : S$ and $x \in S$ is subtle.[8] In other notations, $\in$ may be used interchangeably for both purposes.

> Informal
> In some circumstances, when it's obvious what S is, $x : S$ may be omitted.

Definition 1.3.4. *A* ***set comprehension*** *is an expression of the form* $\{$ *variables* $\bullet$ *expression* $\}$*.*

[6] The *converse* of a statement "if P, then Q" is the statement "if Q, then P".

[7] However, in some circumstances, it may not be possible to construct a set containing all of the intended values. In these cases, we might write $x : S$ even though S is not a set.

[8] In terms of computer programming, $x : S$ is like defining a variable (e.g. `int x;`), and we can't use a variable until we've specified what type it has. Also, while we can write $(n + 2) \in \mathbb{N}$, $(n + 2)$ is not a variable, so we can't write $(n + 2) : \mathbb{N}$.

Example 1.3.5.

1. *$\{ n : \mathbb{N} \bullet n^2 \}$.*
2. *Where $P(n)$ means "n is prime", $\{ p : \mathbb{N} \mid P(p) \bullet p \}$.*

> Informal
> When the expression in a set comprehension is simply the one variable, it is often omitted. For example, $\{ p : \mathbb{N} \mid P(p) \}$.

1.4 Set Operators

Much like we have operators such as $+$, $-$, and $\cdot$ which combine numbers, we have operators which combine sets.

Definition 1.4.1. *For sets S, T,*

1. *$S \cap T$ is the **intersection** of S and T.*

   $x \in (S \cap T)$ iff both $x \in S$ and $x \in T$.
2. *$S \cup T$ is the **union** of S and T.*

   $x \in (S \cup T)$ iff either $x \in S$ or $x \in T$, or both.
3. *$S \setminus T$ is S **minus** T.*

   $x \in (S \setminus T)$ iff $x \in S$ but $x \notin T$.
4. *$S \triangle T = (S \setminus T) \cup (T \setminus S)$ is the **symmetric difference** of S and T.*
5. *$\#S$ is the **cardinality** of S. If S has finitely many distinct elements, we say S is a **finite** set, and $\#S$ is the number of distinct elements.*[9]
6. *Where $S : \mathbb{P}\, E$ for some "universal set" E, $S^{\mathsf{c}} = E \setminus S$ is the complement of S.*

Example 1.4.2.

1. *$\{1, 2, 3\} \cap \{3, 4, 5\} = \{3\}$.*
2. *$\{1, 2, 3\} \cup \{3, 4, 5\} = \{1, 2, 3, 4, 5\}$.*
3. *$\{a, b, c, d\} \cap \{x, y, z\} = \emptyset$*

[9] If S is not finite, it is an **infinite set**, and $\#S$ is one of the infinite "cardinal numbers".

4. $\{red, yellow, blue\} \setminus \{red, green, blue\} = \{yellow\}$.

5. $\{red, yellow, blue\} \triangle \{red, green, blue\} = \{yellow, green\}$.

6. $\#\{red, green, blue\} = 3$, $\#\{a, b, c, d\} = 4$, *and* $\#\emptyset = 0$.

Definition 1.4.3. *If $S \cap T = \emptyset$, i.e. there is no element which is in both sets, then we say S, T are **disjoint**.*

Definition 1.4.4. *For $S : \mathbb{P}\,\mathbb{P}\,X$, i.e. S is a set of subsets of X,*

1. *$\bigcap S$ is a **generalised intersection**. $\bigcap S \subseteq X$.*
   For $x : X$, $x \in \bigcap S$ iff $x \in A$ for every $A : S$.[10]

2. *$\bigcup S$ is a **generalised union**. $\bigcup S \subseteq X$.*
   For $x : X$, $x \in \bigcup S$ iff $x \in A$ for some $A : S$.

Informal

We will write $\bigcap_{variables}$ *expression* to mean $\bigcap\{$ *variables* $\bullet$ *expression* $\}$. In particular, $\bigcap_{i=1}^{n}$ *expression* means $\bigcap\{\, i : \{1, \ldots n\} \bullet$ *expression* $\}$.
(Similarly for $\bigcup$).

1.5 Cartesian Products

Because sets are only defined by their elements, $\{x, y\} = \{y, x\}$.

Definition 1.5.1.

1. *(x, y) is an **ordered pair**, and $(x, y) = (y, x)$ iff $x = y$.*[11]

2. *$(x_1, \ldots x_k)$ is a **k-tuple**, and $(x_1, \ldots x_k) = (y_1, \ldots y_k)$ iff every $x_i = y_i$.*

Definition 1.5.2.

1. *If S, T are sets, $S \times T = \{\, s : S, t : T \bullet (s, t) \,\}$ is the **Cartesian product** of S and T.*

2. *If S is a set, and k is a natural number, $S^k = S \times \cdots S$ is a Cartesian product of k copies of S.*

Note that $\#(S \times T) = \#S \cdot \#T$, and $\#S^k = (\#S)^k$.

[10] Note that if $S = \emptyset$, $\bigcap S = X$.

[11] E.g. $(x, y) = \{\{x\}, \{x, y\}\} \neq \{\{y\}, \{x, y\}\} = (y, x)$, and $(x, x) = \{\{x\}, \{x, x\}\} = \{\{x\}, \{x\}\} = \{\{x\}\}$.

Example 1.5.3.

1. $\{red, blue\} \times \{hat, tie\} = \{(red, hat), (red, tie), (blue, hat), (blue, tie)\}$.

2. $$\begin{aligned}\{1,2,3\} \times \{a, b, c, d\} = \{&(1, a), (1, b), (1, c), (1, d),\\ &(2, a), (2, b), (2, c), (2, d),\\ &(3, a), (3, b), (3, c), (3, d)\}.\end{aligned}$$

3. $\{newyork, paris, peckham\} \times \emptyset = \emptyset$.

4. $$\begin{aligned}\{0,1\}^3 = \{&(0,0,0), (0,0,1), (0,1,0), (0,1,1),\\ &(1,0,0), (1,0,1), (1,1,0), (1,1,1)\}.\end{aligned}$$

By identifying e.g. $(x, y, z) = ((x, y), z) = (x, (y, z))$, we can write e.g. $(X \times Y) \times Z = X \times (Y \times Z)$. Therefore, Cartesian products are associative.

2 Logic

2.1 Propositions and Predicates

In natural language, a proposition is a statement of fact, which is either true or false.

Definition 2.1.1.

1. *$\top$ is taken to mean "true", $\bot$ is taken to mean "false", and $\top \neq \bot$.*[12]
2. *An **atomic proposition** is either $\top$, $\bot$, or a variable $P : \{\top, \bot\}$.*
3. *A **proposition** is an expression which results in one of the values $\top, \bot$.*
4. *A **propositional formula** is a proposition with only atomic propositions as variables.*
5. *The **truth value** of a proposition is the value of its result.*
6. *A **predicate** is a proposition with one or more variables.*[13]
7. *A proposition is a **tautology** if its truth value is always $\top$, a **contradiction** if its truth value is always $\bot$, and a **contingency** otherwise.*

Any statement of fact, mathematical or otherwise, is a proposition.

Example 2.1.2.

1. *"Earth is a planet"* $= \top$.
2. $(1 + 1 = 2) = \top$.
3. *"6 is a prime number"* $= \bot$.
4. $(5 > 4) = \top$.
5. $(\top = \bot) = \bot$.

The truth value of a predicate typically (but not necessarily) depends on the value of its variables.

[12] For example, define $\top = \{\emptyset\}$ and $\bot = \emptyset$.
[13] However, we normally don't consider propositional formulae to be predicates.

Example 2.1.3.

1. *prime*$(p : \mathbb{N})$ = *"p is a prime number".*
2. *small*$(n : \mathbb{N}) = (n < 14)$.
3. *immortal*$(x : \{$ *all animals* $\})$ = *"x lives forever".*

Because predicates give yes-or-no answers, they naturally correspond with sets. Given any predicate $P(x : X)$ we can form the corresponding set $S : \mathbb{P}\,X$ by taking $S = \{\, x : X \mid P(x) \,\}$, the set of elements x which satisfy[14] $P(x)$. Conversely, given a subset $S : \mathbb{P}\,X$, the predicate $P(x : X) = (x \in S)$ corresponds with S.

2.2 Propositional Calculus

As with numbers and sets, propositions can be combined using logical connectives.

Definition 2.2.1. *For propositions P, Q,*

1. *$P \wedge Q$ is* ***conjunction****, or "P and Q".*
   $(P \wedge Q) = \top$ *iff* $P = \top$ *and* $Q = \top$.
2. *$P \vee Q$ is* ***disjunction****, or "P or Q".*
   $(P \vee Q) = \top$ *iff* $P = \top$, *or* $Q = \top$, *or both.*[15]
3. *$\neg P$ is* ***negation****, or "not P".*
   $\neg P = \top$ *iff* $P = \bot$.
4. *$P \to Q$ is* ***implication****,*[16] *or "P implies Q" or "if P, then Q".*
   $(P \to Q) = \top$ *iff* $P = \bot$ *or* $Q = \top$.[17]
5. *$P \leftarrow Q$ is* ***converse implication****,*[18] *and means $Q \to P$.*

[14] A predicate is "satisfied" by a value if it is true for that value.

[15] In natural language, "would you like soup, or salad?" suggests that only one option may be selected. In propositional logic, however, you would be permitted to take both soup and salad, should you prefer.

[16] This is related to the $\Rightarrow$ relation, which means that one claim is a sufficient condition for another.

[17] If P implies Q, then when P is false, Q could be either true or false. It is only when P is true that we know Q must be true (by P's implication). Many find this confusing.

[18] This is related to the $\Leftarrow$ relation, which means that one claim is a necessary condition for another.

6. $P \leftrightarrow Q$ *is* ***equivalence***,[19] *or "P iff Q", and means* $P = Q$.

Example 2.2.2. *Let* $P =$ *"It is raining",* $Q =$ *"Alice will take an umbrella", and* $R =$ *"Alice will be soaked".*

1. $P \wedge R$ *means "It is raining and Alice will be soaked."*
2. $P \vee \neg Q$ *means "It is raining, or Alice will not take an umbrella."*
3. $\neg Q \rightarrow R$ *means "If Alice will not take an umbrella, then she will be soaked."*
4. $P \leftarrow (Q \vee R)$ *means "It is raining only if Alice either will take an umbrella or be soaked."*
5. $Q \leftrightarrow P$ *means "Alice will take an umbrella if and only if it is raining."*

2.3 Truth Tables

Given a propositional formula, all possible values for the atomic propositions may be exhausted in a **truth table**. For example, the following truth table gives the results of each connective defined in Definition 2.2.1.

P	Q	$P \wedge Q$	$P \vee Q$	$\neg P$	$P \rightarrow Q$	$P \leftarrow Q$	$P \leftrightarrow Q$
$\top$	$\top$	$\top$	$\top$	$\bot$	$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\top$		$\bot$	$\top$	$\bot$
$\bot$	$\top$	$\bot$	$\top$	$\top$	$\top$	$\bot$	$\bot$
$\bot$	$\bot$	$\bot$	$\bot$		$\top$	$\top$	$\top$

Truth tables can be used to calculate the result of a propositional formula, to determine if it is a tautology or a contradiction, or to prove that it is equivalent to another propositional formula.

Example 2.3.1.

1. $P \vee \neg P$ *is a tautology:*

P	$\neg P$	$P \vee \neg P$
$\top$	$\bot$	$\top$
$\bot$	$\top$	$\top$

[19] This is related to the $\Leftrightarrow$ relation, which means "iff" (or "if and only if").

2. *$P \wedge \neg P$ is a contradiction:*

P	$\neg P$	$P \wedge \neg P$
$\top$	$\bot$	$\bot$
$\bot$	$\top$	$\bot$

3. *$\neg P \vee Q$ is equivalent to $P \to Q$:*

P	Q	$\neg P$	$\neg P \vee Q$	$P \to Q$
$\top$	$\top$	$\bot$	$\top$	$\top$
$\top$	$\bot$	$\bot$	$\bot$	$\bot$
$\bot$	$\top$	$\top$	$\top$	$\top$
$\bot$	$\bot$	$\top$	$\top$	$\top$

2.4 Algebraic Identities

Propositional formulae in n variables require truth tables with 2^n rows. For complex formulae with many variables, it is unfeasible to prove by exhaustion.

When we do algebra with numbers, we make use of identities, such as $ax+bx = (a+b)x$, and $x^2-a^2 = (x+a)(x-a)$. Expressions and equations can be simplified by substituting expressions for other equivalent (but simpler) expressions. We will do the same with propositional formulae.

Proposition 2.4.1.

1. $P \vee \top = \top$, $P \wedge \top = P \vee \bot = P$, *and* $P \wedge \bot = \bot$.
2. *Double-negation:* $\neg\neg P = P$.
3. $P \vee \neg P = \top$, *and* $P \wedge \neg P = \bot$.
4. *Associativity of* $\vee$*:* $(P \vee Q) \vee R = P \vee (Q \vee R)$.
5. *Associativity of* $\wedge$*:* $(P \wedge Q) \wedge R = P \wedge (Q \wedge R)$.
6. *Commutativity of* $\vee$ *and* $\wedge$*:* $P \vee Q = Q \vee P$, *and* $P \wedge Q = Q \wedge P$.
7. *Distributivity of* $\wedge$ *over* $\vee$*:* $P \wedge (Q \vee R) = (P \wedge Q) \vee (P \wedge R)$.
8. *Distributivity of* $\vee$ *over* $\wedge$*:* $P \vee (Q \wedge R) = (P \vee Q) \wedge (P \vee R)$.
9. *De Morgan's law:* $\neg(P \wedge Q) = \neg P \vee \neg Q$.
10. *De Morgan's law:* $\neg(P \vee Q) = \neg P \wedge \neg Q$.
11. $P \to Q = \neg P \vee Q$, *and* $P \leftarrow Q = P \vee \neg Q$.

12. $P \leftrightarrow Q = (P \to Q) \wedge (P \leftarrow Q) = (P \wedge Q) \vee (\neg P \wedge \neg Q)$.

Proof. Exercise (using truth tables). $\square$

All identities in $\wedge$, $\vee$ and $\neg$ apply equivalently to the set operators $\cap$, $\cup$ and $^{\mathsf{c}}$ respectively.[20]

Example 2.4.2.

1. $$\begin{aligned} &\neg Q \to \neg P \\ &= \neg\neg Q \vee \neg P && (11) \\ &= Q \vee \neg P && (2) \\ &= \neg P \vee Q && (6) \\ &= P \to Q. && (11) \end{aligned}$$

2. $$\begin{aligned} &(P \wedge Q) \vee (P \wedge \neg Q) \\ &= P \wedge (Q \vee \neg Q) && (7) \\ &= P \wedge \top && (1) \\ &= P. && (1) \end{aligned}$$

[20] This follows by substituting $x \in S$, $x \in T$ for the atomic propositions P, Q respectively:

- $(x \in S) \wedge (x \in T) \Leftrightarrow x \in (S \cap T)$,
- $(x \in S) \vee (x \in T) \Leftrightarrow x \in (S \cup T)$, and
- $\neg(x \in S) \Leftrightarrow (x \in S^{\mathsf{c}})$.

3. $((P \to Q) \land (Q \to R)) \to (P \to R)$

$$
\begin{aligned}
&= \neg((\neg P \lor Q) \land (\neg Q \lor R)) \lor (\neg P \lor R) && (11)\\
&= (\neg(\neg P \lor Q) \lor \neg(\neg Q \lor R)) \lor (\neg P \lor R) && (9)\\
&= \neg(\neg P \lor Q) \lor \neg(\neg Q \lor R) \lor \neg P \lor R && (4)\\
&= (\neg\neg P \land \neg Q) \lor (\neg\neg Q \land \neg R) \lor \neg P \lor R && (10)\\
&= (P \land \neg Q) \lor (Q \land \neg R) \lor \neg P \lor R && (2)\\
&= \neg P \lor (P \land \neg Q) \lor R \lor (Q \land \neg R) && (6)\\
&= ((\neg P \lor P) \land (\neg P \lor \neg Q)) \lor ((R \lor Q) \land (R \lor \neg R)) && (8)\\
&= (\top \land (\neg P \lor \neg Q)) \lor ((R \lor Q) \land \top) && (1)\\
&= (\neg P \lor \neg Q) \lor (R \lor Q) && (1)\\
&= \neg P \lor \neg Q \lor R \lor Q && (4)\\
&= \neg P \lor R \lor Q \lor \neg Q && (6)\\
&= \neg P \lor R \lor \top && (1)\\
&= \top. && (1)
\end{aligned}
$$

2.5 Arguments

The most important purpose of logic is inferring new knowledge from existing (or hypothetical) knowledge. In mathematical logic, an **argument** is a statement of **premises** (existing knowledge) and a **conclusion** (to be inferred from the premises). By defining appropriate atomic propositions, we can translate arguments made in natural language into the language of propositional calculus. An **argument form** is an argument whose premises and conclusion are propositional formulae.

Example 2.5.1.
"If the apple is mouldy, it is not safe to eat."
"The apple is mouldy."
$\therefore$ *"The apple is not safe to eat."*

Let P = *"the apple is mouldy" and* Q = *"the apple is safe to eat". Then, the argument form is* $P \to \neg Q$, P, $\therefore \neg Q$.

		Premises		*Conclusion*
P	Q	P	$P \to \neg Q$	$\neg Q$
$\top$	$\top$	$\top$	$\bot$	$\bot$
$\top$	$\bot$	$\top^*$	$\top^*$	$\top^*$
$\bot$	$\top$	$\bot$	$\top$	$\bot$
$\bot$	$\bot$	$\bot$	$\top$	$\top$

Using a truth table, we see that for this argument form, whenever the premises are both true, the conclusion is true.

The $\therefore$ symbol means "therefore", and denotes the argument's conclusion. The * symbol is used to show where the premises are satisfied.

We wish to distinguish between valid arguments, where the inference is always logically sound, and invalid arguments, which might lead us to infer a false conclusion.

Definition 2.5.2.

1. *An argument form is **valid** if all possible values of its atomic propositions which satisfy the premises, also satisfy the conclusion.*
2. *An argument form is **invalid** if it is not valid; i.e. if its atomic propositions can take values such that the premises are satisfied, but the conclusion is false.*
3. *An argument is valid if the corresponding argument form is valid, and invalid if the corresponding argument form is invalid.*

Note that an argument form $P_1, \ldots P_k, \therefore Q$ is valid iff the propositional formula $(P_1 \wedge \cdots P_k) \to R$ is a tautology.[21]

Proposition 2.5.3. *The following argument forms are valid:*

1. *Modus ponens:* $P \to Q,\ P, \therefore Q$.
2. *Modus tollens:* $P \to Q,\ \neg Q, \therefore \neg P$.
3. *Disjunctive syllogism:* $P \vee Q,\ \neg P, \therefore Q$.
4. *Hypothetical syllogism:* $P \to Q,\ Q \to R, \therefore P \to R$.
5. *Principle of explosion:* $\bot, \therefore P$.

Proof.

1.

		Premises		Conclusion
P	Q	$P \to Q$	P	Q
$\top$	$\top$	$\top^*$	$\top^*$	$\top^*$
$\top$	$\bot$	$\bot$	$\top$	$\bot$
$\bot$	$\top$	$\top$	$\bot$	$\top$
$\bot$	$\bot$	$\top$	$\bot$	$\bot$

[21] This is the Deduction Theorem.

2. Premises / Conclusion

P	Q	$P \to Q$	$\neg Q$	$\neg P$
$\top$	$\top$	$\top$	$\bot$	$\bot$
$\top$	$\bot$	$\bot$	$\top$	$\bot$
$\bot$	$\top$	$\top$	$\bot$	$\top$
$\bot$	$\bot$	$\top^*$	$\top^*$	$\top^*$

3. Premises / Conclusion

P	Q	$P \lor Q$	$\neg P$	Q
$\top$	$\top$	$\top$	$\bot$	$\top$
$\top$	$\bot$	$\top$	$\bot$	$\bot$
$\bot$	$\top$	$\top^*$	$\top^*$	$\top^*$
$\bot$	$\bot$	$\bot$	$\top$	$\bot$

4. See Example 2.4.2.3.

5. $\bot \to P = \neg\bot \lor P = \top \lor P = \top$.

□

Beware that a "valid" argument from false premises may lead to a false conclusion. By the principle of explosion, if the premises form a contradiction, literally *any* conclusion can be drawn.

2.6 Quantifiers

Definition 2.6.1.

1. *$\forall$ is the* ***universal quantifier****, meaning "for all" or "for every".*

2. *$\exists$ is the* ***existential quantifier****, meaning "there exists" or "there is".*

A proposition of the form *quantifier variables • expression* is called a **quantified expression**.

Example 2.6.2. *If $P(x : X)$ is a predicate,*

1. *$\forall\, x : X \bullet P(x)$ means "for every $x : X$, $P(x)$ is satisfied".*

2. *$\exists\, x : X \bullet P(x)$ means "there is an $x : X$ which satisfies $P(x)$".*

> Informal
> We will write $\exists\, x : X$ to mean $\exists\, x : X \bullet \top$. This is equivalent to $X \neq \emptyset$.

Proposition 2.6.3.

1. $\big(\neg\,\forall\, x : X \bullet P(x)\big) \leftrightarrow \big(\exists\, x : X \bullet \neg P(x)\big)$.
2. $\big(\neg\,\exists\, x : X \bullet P(x)\big) \leftrightarrow \big(\forall\, x : X \bullet \neg P(x)\big)$.
3. $\forall\, x : \emptyset \bullet P(x)$ *is a tautology.*[22]
4. $\exists\, x : \emptyset \bullet P(x)$ *is a contradiction.*

Proof. Omitted. □

In particular, $\big(\forall\, x : X \bullet P(x)\big) \not\Rightarrow \big(\exists\, x : X \bullet P(x)\big)$, as $X = \emptyset$ is a counterexample.

Definition 2.6.4. $\exists!$ *means "there is a unique".*

$\exists!\, x : X \bullet P(x)$ *is equivalent to* $\exists\, x : X \bullet \forall\, x' : X \bullet P(x') \leftrightarrow x = x'$, *or "there is an* $x : X$ *which, for every* $x' : X$, $P(x')$ *is satisfied iff* $x' = x$*."*

[22] Statements of this form are "vacuously true", as they make no claims about any x.

3 Relations

3.1 Relations

Definition 3.1.1. $x \mapsto y = (x, y)$ *is a* ***maplet****.*

For $x : S, y : T$, a relation like $x > y$ or $x \trianglelefteq y$ tells us whether or not x and y are related in some way. Since this is a yes-or-no answer, it is natural to represent a relation using a set[23] which contains pairs of elements which are related.

Definition 3.1.2.

1. *R is a* ***relation*** *between S and T if $R \subseteq (S \times T)$.*

2. *$S \leftrightarrow T = \mathbb{P}(S \times T)$ is the set of all relations between S and T.*

3. *For $R : S \leftrightarrow T$, S is the* ***source*** *set, and T is the* ***target*** *set.*

I.e. a relation is a set of pairs (x, y) for which x is related to y, so a relation is a subset of $S \times T$, the set of all possible pairs. Hence, the set of all relations is $\mathbb{P}(S \times T)$, the set of all such subsets.

Example 3.1.3. *If $S = \{2, 3, 4, 5\}$, and $T = \{5, 6, 8\}$,*

1. $R_1 = \{2 \mapsto 5, 3 \mapsto 5, 3 \mapsto 8, 4 \mapsto 5, 5 \mapsto 6, 5 \mapsto 8\}$.

   $R_1 \subset (S \times T)$ *is the relation "x, y are coprime".*

   3 *and* 8 *are coprime, so* $3 \mapsto 8 \in R_1$.

2. $R_2 = \{3 \mapsto 2, 4 \mapsto 2, 4 \mapsto 3, 5 \mapsto 2, 5 \mapsto 3, 5 \mapsto 4\}$.

   $R_2 \subset (S \times S)$ *is the relation* $x > y$.

   $5 > 2$, *so* $5 \mapsto 2 \in R_2$.

3. $R_3 = \{\, n : \mathbb{N} \bullet n \mapsto (n^2 + 6) \,\}$.

   $R_3 \subset (\mathbb{N} \times \mathbb{N})$ *is the relation* $x^2 + 6 = y$.

   $4^2 + 6 = 22$, *so* $4 \mapsto 22 \in R_3$.

[23] However, some relations which we already defined, like $=$, $\in$, and $\subseteq$, cannot be represented as sets.

Informal

(x, y) is an expression, not a variable, so if $R = S \times T$, it's not strictly correct to write $(x, y) : R$. To resolve this, we can invent operators "first" and "second", where $\text{first}(a, b) = a$ and $\text{second}(a, b) = b$. Then we can write $p : S \times T$, $x = \text{first}\, p$, and $y = \text{second}\, p$.

However, this is messier and doesn't aid understanding, so we'll just write $(x, y) : R$, or equivalently $x \mapsto y : R$, as shorthand.

Relations are typically written in **infix** notation: if $R : S \leftrightarrow T$ then we write $\_R\_ : S \leftrightarrow T$, and for $x : S, y : T$, we write xRy to mean $x \mapsto y \in R$, and $x \not R y$ to mean $x \mapsto y \notin R$.

Informal

If R, S are relations then we will write $xRySz$ to mean that both xRy and ySz. For example, $3^2 = 9 > 5$.

This is not strictly correct, as generally neither $(xRy)Sz$ nor $xR(ySz)$ make sense.

3.2 Relation Operators

Definition 3.2.1. *For* $R : X \leftrightarrow Y, A : \mathbb{P}\, X, B : \mathbb{P}\, Y$,

1. $\text{dom}\, R = \{\, x \mapsto y : R \bullet x \,\}$ *is the **domain** of* R.

   $\text{dom}\, R \subseteq X$.

2. $\text{ran}\, R = \{\, x \mapsto y : R \bullet y \,\}$ *is the **range** of* R.

   $\text{ran}\, R \subseteq Y$.

3. *For* $S : Y \leftrightarrow Z$, $R \fatsemi S = \{\, x \mapsto y : R, y' \mapsto z : S \mid y = y' \bullet x \mapsto z \,\}$ *is the **relational composition** of* R *and* S.

   $R \fatsemi S \in X \leftrightarrow Z$*, and* $x(R \fatsemi S)z$ *iff* $\exists\, y : Y \bullet xRySz$.

4. $R^{\sim} = \{\, x \mapsto y : R \bullet y \mapsto x \,\}$ *is the **inverse** relation of* R.

   $R^{\sim} \in Y \leftrightarrow X$.

5. $R(\!|\, A \,|\!) = \{\, x \mapsto y : R \mid x \in A \bullet y \,\}$ *is the **relational image** of* A.

   $R(\!|\, A \,|\!) \subseteq Y$.

6. $A \lhd R = \{\, x \mapsto y : R \mid x \in A \,\}$ *is **domain restriction**.*

7. $R \rhd B = \{\, x \mapsto y : R \mid y \in B \,\}$ *is **range restriction**.*

8. $A \ntriangleleft R = \{ x \mapsto y : R \mid x \notin A \}$ *is **domain subtraction**.*
   $A \ntriangleleft R = R \setminus (A \lhd R)$.

9. $R \ntriangleright B = \{ x \mapsto y : R \mid y \notin B \}$ *is **range subtraction**.*
   $R \ntriangleright B = R \setminus (R \rhd B)$.

> Informal
> Where it is clearer, we will write e.g. $R(\!| \ x \ |\!)$, or $x \ntriangleleft R$, instead of $R(\!| \ \{x\} \ |\!)$, or $\{x\} \ntriangleleft R$.

3.3 Equivalence Relations

Definition 3.3.1. *Let $R : X \leftrightarrow X$.*

1. *R is **reflexive** if $\forall x : X \bullet xRx$.*
2. *R is **symmetric** if $\forall x, y : X \bullet xRy \Rightarrow yRx$.*
3. *R is **transitive** if $\forall x, y, z : X \bullet (xRy \wedge yRz) \Rightarrow xRz$.*
4. *R is an **equivalence relation** if R is reflexive, symmetric and transitive.*

Example 3.3.2. *Let $X = \{1, 2, 3\}$, and $R_1, \ldots R_8 : X \leftrightarrow X$.*

1. *$R_1 = \{1 \mapsto 2\}$ is neither reflexive, symmetric, nor transitive.*
2. *$R_2 = \{1 \mapsto 1, 2 \mapsto 2, 3 \mapsto 3, 1 \mapsto 2, 2 \mapsto 3\}$ is reflexive but neither symmetric nor transitive.*
3. *$R_3 = \{1 \mapsto 2, 2 \mapsto 1, 2 \mapsto 3, 3 \mapsto 2\}$ is symmetric but neither reflexive nor transitive.*
4. *$R_4 = \{1 \mapsto 2, 2 \mapsto 3, 1 \mapsto 3\}$ is transitive but neither reflexive nor symmetric.*
5. *$R_5 = R_2 \cup R_3$ is reflexive and symmetric but not transitive.*
6. *$R_6 = R_2 \cup R_4$ is reflexive and transitive but not symmetric.*
7. *$R_7 = \emptyset$ is symmetric and transitive but not reflexive.*
8. *$R_8 = \{1 \mapsto 1, 2 \mapsto 2, 3 \mapsto 3, 2 \mapsto 3, 3 \mapsto 2\}$ is reflexive, symmetric, and transitive. Hence, R_8 is an equivalence relation.*

Proposition 3.3.3. *If $R : X \leftrightarrow X$ is an equivalence relation, then*

$$\{ x : X \bullet R(\!|\ x\ |\!) \} = \{ x : X \bullet R^{\sim}(\!|\ x\ |\!) \}$$

and this set is a partition of X. Conversely, if P is a partition of X, then

$$\Big(\bigcup_{S:P} S \times S\Big) \in X \leftrightarrow X$$

is an equivalence relation.

Proof. $\forall\, x, y, z : X$,

1. $x \in R(\!|\ x\ |\!)$, so x is in at least one of the subsets.

2. $y \in R(\!|\ x\ |\!) \Leftrightarrow xRy \Leftrightarrow yRx \Leftrightarrow y \in R^{\sim}(\!|\ x\ |\!)$, hence $R(\!|\ x\ |\!) = R^{\sim}(\!|\ x\ |\!)$.

3. Suppose $x \in R(\!|\ y\ |\!)$. Then $yRx \wedge xRy$, and so $z \in R(\!|\ x\ |\!) \Leftrightarrow xRz \Leftrightarrow yRz \Leftrightarrow z \in R(\!|\ y\ |\!)$, so $R(\!|\ x\ |\!) = R(\!|\ y\ |\!)$, and therefore x is in at most one of the subsets.

Conversely, let R_P be the corresponding relation, and $S_x : P$ be the unique subset containing x.

1. $\forall\, x : X \bullet x \in S_x$, so $x \mapsto x \in R_P$ and R_P is reflexive.

2. R_P is trivially symmetric, as it is a union of symmetric relations.

3. $(x \in S_y \wedge y \in S_z) \Rightarrow (S_x = S_y = S_z) \Rightarrow x \in S_z$, so R_P is transitive.

Hence, R_P is an equivalence relation. □

Note also that $R_P(\!|\ x\ |\!) = S_x$. Therefore, there is a direct correspondence between partitions of X and equivalence relations on X.

Definition 3.3.4. *For an equivalence relation $R : X \leftrightarrow X$,*

1. *$X/R = \{ x : X \bullet R(\!|\ x\ |\!) \}$ is the **quotient** of X by R.*

2. *For $x : X$, $[x]_R = R(\!|\ x\ |\!) \in X/R$ is the **equivalence class** of x.*

By Proposition 3.3.3, X/R is a partition of X, and every partition of X is X/R for some equivalence relation R.

Example 3.3.5. *For R_8 defined in Example 3.3.2.8,* $X/R_8 = \{\{1\}, \{2, 3\}\}$.

Proposition 3.3.6.

1. *An intersection of reflexive relations is reflexive.*
2. *An intersection of symmetric relations is symmetric.*
3. *An intersection of transitive relations is transitive.*
4. *An intersection of equivalence relations is an equivalence relation.*

Proof. Let $S : \mathbb{P}(X \leftrightarrow X)$, i.e. S is a set of relations.[24]

1. $\forall\, x : X, R : S \bullet x \mapsto x \in R$, hence $\forall\, x : X \bullet x \mapsto x \in \bigcap S$.
2. If $x \mapsto y \in \bigcap S$, then $\forall\, R : S$, $x \mapsto y \in R$, so $y \mapsto x \in R$, so $y \mapsto x \in \bigcap S$.
3. If $x \mapsto y \in \bigcap S$ and $y \mapsto z \in \bigcap S$, then $\forall\, R : S$, $x \mapsto y \in R$ and $y \mapsto z \in R$, so $x \mapsto z \in R$, so $x \mapsto z \in \bigcap S$.
4. By (1), (2), and (3).

$\square$

Definition 3.3.7. *For $R : X \leftrightarrow X$, the equivalence relation **generated by** R is $\bigcap \{ R' : X \leftrightarrow X \mid (R \subseteq R') \wedge (R'$ is an equivalence relation$) \}$, i.e. the intersection of all equivalence relations containing R, or the "smallest" equivalence relation containing R.*

This is a superset of R, and by Proposition 3.3.6, an equivalence relation.

[24] Note that these proofs do work for $S = \emptyset$.

4 Functions

4.1 Functions

Definition 4.1.1. *For* $f : X \leftrightarrow Y$,

1. *If* $x \mapsto y \in f$, *we say "*f *maps* x *to* y*".*
2. f *is a* ***partial function*** *if* f *maps every* $x : X$ *to at most one* $y : Y$.

   Equivalently, $\forall x : \operatorname{dom} f \bullet \exists!\, y : Y \bullet x \mapsto y \in f$.

   Equivalently, $\forall x : X \bullet \# f(\!|\, x \,|\!) \leqslant 1$.

   $X \nrightarrow Y$ *is the set of all partial functions from* X *to* Y.
3. f *is a* ***function*** *if* f *maps every* $x : X$ *to exactly one* $y : Y$.

   Equivalently, $\forall x : X \bullet \exists!\, y : Y \bullet x \mapsto y \in f$.

   Equivalently, $\forall x : X \bullet \# f(\!|\, x \,|\!) = 1$.

   Equivalently, f *is a partial function, and* $\operatorname{dom} f = X$.

   $X \rightarrow Y$ *is the set of all functions from* X *to* Y.[25]
4. *If* f *is a function, then for* $x : X$, $f(x)$ *is the unique value* $y : Y$ *for which* $x \mapsto y \in f$.

   Equivalently, $f(x) = y$ *iff* $f(\!|\, x \,|\!) = \{y\}$.

   $f(x)$ *is the* ***evaluation*** *of* f *at* x.

Informal

For $f : X \rightarrow Y, A : \mathbb{P}\, X, B : \mathbb{P}\, Y$, we will write $f(A) = f(\!|\, A \,|\!)$, and $f^{-1}(B) = f^{\sim}(\!|\, B \,|\!)$. $f(A)$ is the "image" of A, and $f^{-1}(B)$ is the "pullback" of B.

Definition 4.1.2. *For a set* X, *and an equivalence relation* $R : X \leftrightarrow X$,

1. $\mathrm{id}_X = \{\, x : X \bullet x \mapsto x \,\}$ *is the* ***identity function*** *on* X.

[25] Another common notation is $Y^X = X \rightarrow Y$. This is very natural:

- $\# Y^X = (\# Y)^{\# X}$,
- There is a natural bijection between X^n and $X^{\{1,\ldots n\}}$,
- There is a natural bijection between $\mathbb{P}\, X$ and $\{0,1\}^X$, and $\# \mathbb{P}\, X = 2^{\# X}$.

2. *If $X : \mathbb{P}\,E$ for some "universal set" E, then $\mathbb{1}_X : E \to \{0,1\}$, given by $\mathbb{1}_X = \{\, x : X \bullet x \mapsto 1 \,\} \cup \{\, x : E \setminus X \bullet x \mapsto 0 \,\}$ is the* ***indicator function****, or* ***characteristic function****, of X.*

3. *$\pi_R : X \to X/R$, given by $\pi_R = \{\, x : X \bullet x \mapsto [x]_R \,\}$ is the* ***projection map****, or* ***quotient map****.*

$\forall\, x : X \bullet \mathrm{id}_X(x) = x$, and $\forall\, x : E \bullet (\mathbb{1}_X(x) = 1) \leftrightarrow (x \in X)$.

We often wish to define $f' : X/R \to Y$ by $f'([x]) = f(x)$ for $f : X \to Y$. However, we need to show that $\forall\, x, x' : X \bullet xRx' \Rightarrow f(x) = f(x')$ for this to be "well-defined".

Definition 4.1.3. *For $f : X \rightarrow\!\!\!\!\!+ \; Y, g : Y \rightarrow\!\!\!\!\!+ \; Z$, $g \circ f = f \mathbin{⨾} g$.*

$\circ$ is associative, i.e. $(f \circ g) \circ h = f \circ (g \circ h)$. Also, $(g \circ f)(x) = g(f(x))$. $\circ$ is generally not commutative, i.e. $(f \circ g) \neq (g \circ f)$ even when both are defined.

Informal
Where it is clearer, we will write gf to mean $g \circ f$.

4.2 Injections, Surjections and Bijections

Definition 4.2.1. *For $f : X \to Y$,*

1. *f is an* ***injection****, or is* ***injective****, if every $y : Y$ is mapped to by at most one $x : X$.*

   Equivalently, $\forall\, y : \mathrm{ran}\, f \bullet \exists!\, x : X \bullet f(x) = y$.

   Equivalently, $\forall\, x, x' : X \bullet f(x) = f(x') \Rightarrow x = x'$.

   Equivalently, $\forall\, y : Y \bullet \# f^{\sim}(\!|\, y \,|\!) \leqslant 1$.

   Equivalently, $f^{\sim}$ is a partial function.

   $X \rightarrowtail Y$ is the set of all injections from X to Y.

2. *f is a* ***surjection****, or is* ***surjective****, if every $y : Y$ is mapped to by at least one $x : X$.*

   Equivalently, $\forall\, y : Y \bullet \exists\, x : X \bullet f(x) = y$.

   Equivalently, $\forall\, y : Y \bullet \# f^{\sim}(\!|\, y \,|\!) \geqslant 1$.

   Equivalently, $\mathrm{ran}\, f = Y$.

   $X \twoheadrightarrow Y$ is the set of all surjections from X to Y.

3. *f is a* ***bijection****, or is* ***bijective****, if every $y : Y$ is mapped to by exactly one $x : X$.*

   Equivalently, $\forall\, y : Y \bullet \exists!\, x : X \bullet f(x) = y$.

   Equivalently, $\forall\, y : Y \bullet \# f^{\sim}(\!|\, y \,|\!) = 1$.

   Equivalently, $f^{\sim}$ is a function.

   $X \rightarrowtail\!\!\!\!\twoheadrightarrow Y$ is the set of all bijections from X to Y.

Note that $X \rightarrowtail\!\!\!\!\twoheadrightarrow Y = (X \rightarrowtail Y) \cap (X \twoheadrightarrow Y)$, i.e. f is bijective iff it is both injective and surjective.

Definition 4.2.2. *For $f : X \rightarrowtail\!\!\!\!\twoheadrightarrow Y$, $f^{-1} = f^{\sim}$ is the* ***inverse function*** *of f.*

If f is a bijection, f^{-1} is not only a function, but also a bijection. Also, id_X is a bijection, and $\mathrm{id}_X^{-1} = \mathrm{id}_X$.

For $f : X \rightarrowtail\!\!\!\!\twoheadrightarrow Y, g : Y \rightarrowtail\!\!\!\!\twoheadrightarrow Z$, $f^{-1} \circ f = \mathrm{id}_X$, $f \circ f^{-1} = \mathrm{id}_Y$, and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. Also, $\mathrm{id}_Y \circ f = f \circ \mathrm{id}_X = f$.

Proposition 4.2.3.

1. *$\forall\, f : X \nrightarrow Y, g : Y \nrightarrow Z \bullet gf \in X \nrightarrow Z$.*

   I.e. a composition of partial functions is a partial function.

2. *$\forall\, f : X \rightarrow Y, g : Y \rightarrow Z \bullet gf \in X \rightarrow Z$.*

   I.e. a composition of functions is a function.

3. *$\forall\, f : X \rightarrowtail Y, g : Y \rightarrowtail Z \bullet gf \in X \rightarrowtail Z$.*

   I.e. a composition of injections is an injection.

4. *$\forall\, f : X \twoheadrightarrow Y, g : Y \twoheadrightarrow Z \bullet gf \in X \twoheadrightarrow Z$.*

   I.e. a composition of surjections is a surjection.

5. *$\forall\, f : X \rightarrowtail\!\!\!\!\twoheadrightarrow Y, g : Y \rightarrowtail\!\!\!\!\twoheadrightarrow Z \bullet gf \in X \rightarrowtail\!\!\!\!\twoheadrightarrow Z$.*

   I.e. a composition of bijections is a bijection.

Proof. $\forall\, x : X, z : Z$,

1. $\# gf(\!|\, x \,|\!) = \# g(\!|\, f(\!|\, x \,|\!) \,|\!) \leqslant 1 \cdot \# f(\!|\, x \,|\!) \leqslant 1 \cdot 1$.

2. $\# gf(\!|\, x \,|\!) = \# g(\!|\, f(\!|\, x \,|\!) \,|\!) = 1 \cdot \# f(\!|\, x \,|\!) = 1 \cdot 1$.

3. $\#(gf)^{\sim}(\!|\, z \,|\!) = \# f^{\sim}(\!|\, g^{\sim}(\!|\, z \,|\!) \,|\!) \leqslant 1 \cdot \# g^{\sim}(\!|\, z \,|\!) \leqslant 1 \cdot 1$.

4. $\#(gf)^{\sim}(\!|\ z\ |\!) = \#f^{\sim}(\!|\ g^{\sim}(\!|\ z\ |\!)\ |\!) \geqslant 1 \cdot \#g^{\sim}(\!|\ z\ |\!) \geqslant 1 \cdot 1$.
5. $\#(gf)^{\sim}(\!|\ z\ |\!) = \#f^{\sim}(\!|\ g^{\sim}(\!|\ z\ |\!)\ |\!) = 1 \cdot \#g^{\sim}(\!|\ z\ |\!) = 1 \cdot 1$.

□

Proposition 4.2.4. $\forall f : X \to Y, g : Y \to Z$,

1. *$gf \in X \rightarrowtail Z \Rightarrow f \in X \rightarrowtail Y$.*
   I.e. if gf is an injection, then f is an injection.
2. *$gf \in X \twoheadrightarrow Z \Rightarrow g \in Y \twoheadrightarrow Z$.*
   I.e. if gf is a surjection, then g is a surjection.

Proof.

1. $\forall\, y, y' : Y \bullet f(y) = f(y') \Rightarrow gf(y) = gf(y') \Rightarrow y = y'$.
2. $\forall\, z : Z \bullet \exists\, x : X \bullet g(f(x)) = z$.

□

Proposition 4.2.5. *If X is a finite set, and $f : X \to X$, then f is injective iff it is surjective iff it is bijective.*[26]

Proof. $X = f^{\sim}(\!|\ X\ |\!)$, so $\#X = \#f^{\sim}(\!|\ X\ |\!) = \sum_{x:X} \#f^{\sim}(\!|\ x\ |\!) \leqslant \sum_{x:X} 1 = \#X$, with equality iff every term is 1; i.e. f is a bijection.

Similarly, if f is surjective, then $\sum_{x:X} \#f^{\sim}(\!|\ x\ |\!) \geqslant \sum_{x:X} 1 = \#X$ with equality iff every term is 1. □

Proposition 4.2.6. *For finite[27] sets X, Y,*

1. *$(\exists\, f : X \rightarrowtail Y) \Leftrightarrow \#X \leqslant \#Y$.*
2. *$(\exists\, f : X \twoheadrightarrow Y) \Leftrightarrow \#X \geqslant \#Y$.*
3. *$(\exists\, f : X \rightarrowtail\!\!\!\twoheadrightarrow Y) \Leftrightarrow \#X = \#Y$.*

Proof. $\forall\, f : X \to Y \bullet X = f^{\sim}(\!|\ Y\ |\!)$.

Let $m = \#X$, $n = \#Y$, $M = \{1, \ldots m\}$ and $N = \{1, \ldots n\}$, and let X and Y be enumerated by bijections $c_X : M \rightarrowtail\!\!\!\twoheadrightarrow X$ and $c_Y : N \rightarrowtail\!\!\!\twoheadrightarrow Y$ respectively.

---

[26] I.e. $X \rightarrowtail X = X \twoheadrightarrow X = X \rightarrowtail\!\!\!\twoheadrightarrow X$.

[27] For infinite sets, we will *define* cardinalities in this way.

1. $m = \#f^{\sim}\llparenthesis\ Y\ \rrparenthesis = \sum_{y:Y} \#f^{\sim}\llparenthesis\ y\ \rrparenthesis \leqslant \sum_{y:Y} 1 = n$.

   Conversely, if $\iota : M \rightarrowtail N$ is an injection[28], then $c_Y \iota c_X^{-1}$ is a composition of injections, so it is injective.

2. $m = \#f^{\sim}\llparenthesis\ Y\ \rrparenthesis = \sum_{y:Y} \#f^{\sim}\llparenthesis\ y\ \rrparenthesis \geqslant \sum_{y:Y} 1 = n$.

   Conversely, if $\pi : M \twoheadrightarrow N$ is a surjection[29], then $c_Y \pi c_X^{-1}$ is a composition of surjections, so it is surjective.

3. Any bijection is both an injection and a surjection, so by (1) and (2), $m \leqslant n$ and $m \geqslant n$. Therefore, $m = n$.

   Conversely, $c_Y c_X^{-1}$ is a composition of bijections, so it is bijective.

□

Corollary 4.2.7. *For finite*[30] *sets* X, Y,

1. $\exists f : X \rightarrowtail Y$ *iff* $\exists f' : Y \twoheadrightarrow X$.
2. *If* $\exists f : X \rightarrowtail Y$ *and* $\exists f' : Y \rightarrowtail X$, *then* $\exists f'' : X \rightarrowtail\!\!\!\!\twoheadrightarrow Y$.
3. *If* $\exists f : X \rightarrowtail Y$ *and* $\exists f' : X \twoheadrightarrow Y$, *then* $\exists f'' : X \rightarrowtail\!\!\!\!\twoheadrightarrow Y$.

Proof.

1. $\#X \leqslant \#Y$ iff $\#Y \geqslant \#X$.
2. If $\#X \leqslant \#Y$ and $\#Y \leqslant \#X$, then $\#X = \#Y$.
3. Follows immediately from (1) and (2).

□

[28] E.g. $\iota(k) = k$.

[29] E.g. for $k \leqslant n$, $\pi(k) = k$, and for $k > n$, $\pi(k) = n$.

[30] For infinite sets, (1) is the Partition principle and (2) is the Cantor-Bernstein-Schröder theorem. It follows that the ordering of infinite cardinalities is well-defined.