Chapter 2 - FUNCTIONS

2.1. FUNCTIONS & COMPOSITION

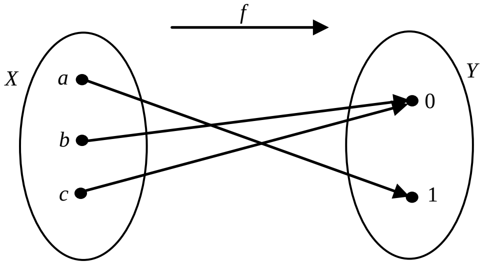
A *function* (a.k.a. *map*, *mapping*, *transformation*) consists of three "things":

1. A set *X*, called the *domain* of the function,
2. A set *Y*, called the *co-domain* of the function, and
3. A "*rule*" *f*, assigning to each $x \in X$ a unique element $y \in Y$.
   This *y* is denoted by $f(x)$, read as "*f* of *x*."

The notation we use for a function as defined above is $\boxed{f: X \to Y}$ or $\boxed{X \xrightarrow{f} Y}$. Thus, two functions $f: X \to Y$ and $g: U \to V$ are *identical* (*equal*, *the same*) if they have the same domain and co-domain, $X = U$ and $Y = V$, and the two rules are "equivalent," $f = g$. Formally, the last condition means: $\boxed{\forall x \in X \left[f(x) = g(x) \right]}$. The set of all functions from domain X to co-domain *Y* is defined and denoted by: $\boxed{Y^X \triangleq \left\{ f \,\middle|\, f: X \to Y \right\}}$.

Examples.

1. Let $f: X \to Y$ be a function with $X = \{a, b, c\}$ and $Y = \{0,1\}$ defined by $f(a) = 1$ and $f(b) = f(c) = 0$. This can be "pictured" as:



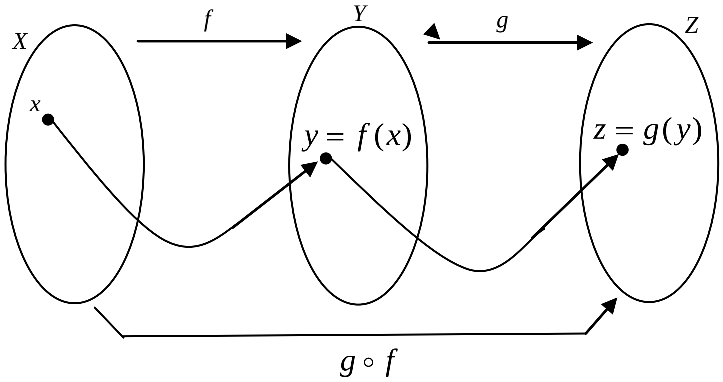
2. In Calculus you must have encountered many functions $f: \mathbb{R} \to \mathbb{R}$, for example $f(x) = x^2$ and $g(x) = e^x$, as well as a function like $\log_e : \mathbb{R}^+ \to \mathbb{R}$, the natural logarithm function.

3. A *Boolean function* (of *n* variables) is a function whose domain is the set of all bit-strings of length *n*, $\{0,1\}^n$, and whose co-domain is the set of bits $\{0,1\}$. Thus a Boolean function can be denoted by $f: \{0,1\}^n \to \{0,1\}$. A hardware designer might be interested in constructing Boolean circuits (logic gates) that compute Boolean functions.

4. For every set X there is a "special" function, called the ***identity function***, which we will denote by $1_X : X \to X$, defined by $\boxed{1_X(x) = x}$, for all $x \in X$.

Question. How many functions are there $X \to Y$, i.e. with finite domain X and finite co-domain Y? In other words, what is the cardinality of Y^X ? **Answer**. $|Y|^{|X|}$.

Let X, Y, and Z be sets with $f : X \to Y$ and $g : Y \to Z$. Then we can apply "first f and then g" and obtain a new function, denoted by $g \circ f : X \to Y$ and called the ***composition*** of the two functions. It is defined by: $\boxed{(g \circ f)(x) \triangleq g(f(x))}$. It can be depicted



N.B.1. Two functions, as in the figure above, can be composed even if the co-domain of the f is a subset of the domain of g. A more precise condition for "composability" will be given below.

Examples.

1. Let $A = \{a,b,c\}$, $B = \{u,v\}$, $C = \{x, y, z\}$ with functions $f : A \to B$ and $g : B \to C$ defined by $f(a) = f(c) = u$, $f(b) = v$, and $g(u) = y, g(v) = x$. Then $g \circ f : A \to C$ is the function whose values can be calculated as follows:

   $(g \circ f)(a) = g(f(a)) = g(u) = y$,
   $(g \circ f)(b) = g(f(b)) = g(v) = x$, and
   $(g \circ f)(c) = g(f(c)) = g(u) = y$.

2. **Claim**. $X \xrightarrow{f} Y \quad \Rightarrow \quad \boxed{1_Y \circ f = f = f \circ 1_X}$.

3. Let $X = Y = Z = \mathbb{N}$ and define two functions $f, g : \mathbb{N} \to \mathbb{N}$ as follows

$$f(n) = 2n \qquad \text{and} \qquad g(n) = n + 5\,.$$

Then, $\forall n \in \mathbb{N},\ (g \circ f)(n) = g(f(n)) = g(2n) = 2n + 5,$ whereas if we compose f and g in the opposite order we get $(f \circ g)(n) = f(g(n)) = f(n+5) = 2n + 10\,.$

<u>Corollary</u>. $f \circ g \neq g \circ f$, so, generally, <u>composition of functions is not commutative</u>!

We next show a very important (and very easy to prove) property of the composition operation: ***<u>composition of functions is associative</u>***.

Theorem 1. Let $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$, i.e. $f : A \to B,\ g : B \to C,$ and $h : C \to D.$ Then $\boxed{h \circ (g \circ f) = (h \circ g) \circ f}$. In picture:

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[rr, bend left, "g \circ f"] & B \arrow[r, "g"] \arrow[rr, bend right, "h \circ g"'] & C \arrow[r, "h"] & D
\end{tikzcd}$$

Proof. Clearly, $h \circ (g \circ f), (h \circ g) \circ f : A \to D$, and we need to show that the two functions have the same value on all elements in the domain *A*. Let $a \in A.$ Then,

$$\big[h \circ (g \circ f)\big](a) = h((g \circ f)(a)) = h(g(f(a))) = (h \circ g)(f(a)) = \big[(h \circ g) \circ f\big](a)\,. \qquad \blacksquare$$

Example. The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = \sqrt{e^{\cos x + 2} - 1}$ can be expressed as a composition of simpler functions. Define

$$f_1(x) \triangleq \cos x\,, \quad f_2(x) \triangleq x + 2\,, \quad f_3(x) \triangleq e^x\,, \quad f_4(x) \triangleq x - 1\,, \quad f_5(x) \triangleq \sqrt{x}\quad .$$

Then, taking into account that composition is associative (Theorem 1), we have

$$\begin{aligned}
\left[f_5 \circ f_4 \circ f_3 \circ f_2 \circ f_1\right](x) &= f_5(f_4(f_3(f_2(f_1(x))))) = f_5(f_4(f_3(f_2(\cos x)))) \\
&= f_5(f_4(f_3(\cos x + 2))) = f_5(f_4(e^{\cos x + 2})) = f_5(e^{\cos x + 2} - 1) = \sqrt{e^{\cos x + 2} - 1} = f(x)\ .
\end{aligned}$$

A function $f : X \to X$ is said to be *__idempotent__* if $f \circ f = f$. For example, the identity function $1_X : X \to X$ is idempotent. This is because $\forall x \in X$, we have

$$(1_X \circ 1_X)(x) = 1_X(1_X(x)) = 1_X(x).$$

Another, less trivial, example of an idempotent function is given by $f : \{a,b,c\} \to \{a,b,c\}$ defined by $f(a) = f(c) = c$ and $f(b) = b.$ Here we have

$$\begin{aligned} &f \circ f(a) = f(f(a)) = f(c) = f(a), \\ &f \circ f(b) = f(f(b)) = f(b), \text{ and} \\ &f \circ f(c) = f(f(c)) = f(c). \end{aligned}$$

For a function $f : X \to Y$ and a subset $A \subseteq X$ of the domain, the *__image of__* *A* *__under__* *f* is a subset of the co-domain defined by

$$\boxed{f(A) \triangleq \left\{ f(x) \middle| \, x \in A \right\}}.$$

For example, for $f : \{a,b,c\} \to \{a,b,c\}$ defined by $f(a) = f(c) = c$ and $f(b) = b,$ we have $f(\{a,b\}) = f(\{b,c\}) = f(\{a,b,c\}) = \{b,c\}$ and $f(\{a,c\}) = \{c\}$. The proof of the next claim follows immediately from the definitions. It expresses the "monotonicity" of function application: if the "input" gets larger so does the "output."

Claim 2. Let $f : X \to Y$ and let $A, B \subseteq X$. Then $A \subseteq B \Rightarrow f(A) \subseteq f(B).$

Proof. $f(A) = \left\{ f(x) \middle| \, x \in A \right\} \subseteq \left\{ f(x) \middle| \, x \in B \right\} = f(B).$ ■

The *__range of the function__* $f : X \to Y$ is the image $f(X)$ of the whole domain *X* under *f*. Thus the range of the function f defined above is $f(\{a,b,c\}) = \{b,c\}$. The range of the identity function 1_X is *X*. We sometimes write $\boldsymbol{range}(f)$ for the range of the function *f*.

N.B.2. A more precise condition for "composability" of two functions $f : X \to Y$ and $g : Y \to Z$ is: $\boxed{\boldsymbol{range}(f) \subseteq \text{ domain(g)}}$.

Claim 3. Let $f : X \to Y$. Then for all subsets $A, B \subseteq X$ we have

1. $f(A \cup B) = f(A) \cup f(B),$ and
2. $f(A \cap B) \subseteq f(A) \cap f(B).$
3. $f(A) - f(B) \subseteq f(A - B).$

Proof. (1) Since $A, B \subseteq A \cup B$, the $\supseteq$-inclusion follows from Claim 2. On the other hand, if $z \in f(A \cup B)$, then $z = f(x)$ with $x \in A \cup B$. So $x \in A$ or $x \in B$. Either way, $z \in f(A) \cup f(B)$.
(2) Follows immediately from Claim 2 since $A \cap B \subseteq A$ (and similarly for *B*).
(3) $z \in f(A) - f(B) \Rightarrow z \in f(A) \wedge z \notin f(B) \Rightarrow z = f(a)$ for some $a \in A$ and obviously $a \notin B$. Hence, $z = f(a)$ and $a \in A - B$, implying $z \in f(A - B)$. ■

2.2. PROPERTIES OF FUNCTIONS

We will define and discuss three pairs of properties of functions.

(A) **Onto and One-to-one functions**. These properties deal with the way a function operates on its “inputs” and the elements that the function yields as values.

Definition. [1st pair of properties] Let $f : A \to B$ be a function.

- *f* is *onto* if $\boxed{\boldsymbol{range}(f) = B}$. Using quantifiers we can express this property by the formula: $\boxed{\forall b \in B \exists a \in A[b = f(a)]}$.
- *f* is *one-to-one* (also written as 1-1) if $\boxed{\forall a, a' \in A[a \neq a' \;\Rightarrow\; f(a) \neq f(a')]}$.
  An equivalent condition is: $\boxed{\forall a, a' \in A[f(a) = f(a') \;\Rightarrow\; a = a']}$.
- *f* is a *correspondence* if it is both onto and one-to-one.

Examples.

1. The function $k : \{0,1\} \to \{a,b,c\}$ defined by $k(0) = b$ and $k(1) = c$ is 1-1 but not onto.
2. The function $\psi : \{0,1\} \to \{0,1\}$ defined by $\psi(b) = 1 - b$ for $b \in \{0,1\}$, is both onto and 1-1. Thus it is a correspondence.
3. The function $f(n) = n + 3 : \mathbb{Z} \to \mathbb{Z}$ is 1-1 and onto, thus a correspondence.
4. The function $f(n) = 5n + 3 : \mathbb{Z} \to \mathbb{Z}$ is 1-1 but not onto.

Claim 4. Let $f : X \to Y$ be a function with *X* and *Y* finite sets. Then,

1. $\forall A \subseteq X$, $|A| \geq |f(A)|$. In particular, $|X| \geq |f(X)| = |\boldsymbol{range}(f)|$.
2. f is 1-1 $\Leftrightarrow$ $\forall A \subseteq X[|A| = |f(A)|]$. In particular, if *f* is 1-1, $|X| = |f(X)|$.
3. f is 1-1 $\Rightarrow$ $|X| \leq |Y|$. [This follows immediately from part 2.]
4. f is onto $\Rightarrow$ $|X| \geq |Y|$. [This follows immediately from part 1.]

Corollary 5. If X and Y finite sets and $f : X \to Y$ is a correspondence, then $|X| = |Y|$.

Pigeonhole Principle [this is contrapositive of part 3, Claim 4]: If m pigeons are placed in n pigeonholes and $m > n$, then some pigeonhole contains more than one pigeon. In terms of functions, if $|X| > |Y|$, then any function $f : X \to Y$ cannot be one-to-one.

The following is a useful property of functions on finite sets.

Claim 6. Let X be a finite set and $f : X \to X$. Then, $\boxed{f \text{ is 1-1 } \Leftrightarrow f \text{ is onto}}$.

Proof. ($\Rightarrow$) If f is not onto, then $|f(X)| < |X|$, so by the Pigeonhole Principle, f is not 1-1.
($\Leftarrow$) Suppose f is not 1-1. By Claim 4, part 2, let $A \subseteq X$ be such that $|A| > |f(A)|$. Since by Claim 4, part 1, $|X - A| \geq |f(X - A)|$, we have

$$|X| = |A| + |X - A| > |f(A)| + |f(X - A)| \geq |f(A) \cup f(X - A)| \geq |f(X)| \ ,$$

implying that f is not onto. ■

Example. Claim 6 holds for finite sets only. For infinite sets neither of these properties implies the other.

- The function $f : \mathbb{N} \to \mathbb{N}$ defined by $f(n) \triangleq 2n$ is 1-1 but not onto.
- The function $g : \mathbb{N} \to \mathbb{N}$ defined by $g(n) \triangleq$ **if** (n even) **then** $n/2$ **else** n, is onto but not 1-1.

(B) **<u>Left- and right-invertible functions</u>**. These properties deal with invertibility of functions.

<u>Definition</u>.(2nd pair of properties) Let $f : A \to B$ be a function.

- f <u>*has a right inverse*</u> if $\exists g : B \to A\left[f \circ g = 1_B \right]$.
- f <u>*has a left inverse*</u> if $\exists h : B \to A\left[h \circ f = 1_A \right]$.
- f <u>*is invertible*</u> if has both a left and a right inverse.

Examples.

1. $f : A \to B$ may have no right inverse. For instance, when $A = \{a\}$, $B = \{1, 2\}$ and $f_1(a) = 1,$ f_1 does not have a right inverse. This is because any $g : B \to A$ must be $g(1) = g(2) = a,$ and $f_1 \circ g(2) = f_1(g(2)) = f_1(a) = 1 \neq 1_B(2).$
   On the other hand, in some cases *f* may have several right inverses: $A = \{a, b\},$ $B = \{1\}$ and $f_2(a) = f_2(b) = 1.$ Here f_2 has two right inverses, $g_1(1) = a$ and $g_2(1) = b.$
2. $f : A \to B$ may have no left inverse. E.g., the function f_2 from part (1) does not have a left inverse. And a function may have several left inverses. For example, take $A = \{a, b\}$, $B = \{x, y, z\}$ and define $f : A \to B$ by $f(a) = x$ and $f(b) = y.$ Then f has two left inverses $g_1(x) = g_1(z) = a,$ $g_1(y) = b$ and $g_2(x) = a,$ $g_2(y) = g_2(z) = b.$
3. $f : A \to B$ may have a left inverse but not right inverse and conversely. For example, the function f_1 from part (1) does not have a right inverse but does have a left one. And the function f_2 from part (1) does not have a left inverse but does have right ones.
4. Finally, $f : A \to B$ may have neither left nor right inverses. For example, let $A = \{a, b\},$ $B = \{x, y\}$ and $f(a) = f(b) = y.$ Take a function $g : B \to A$ that WLOG satisfies $g(y) = a.$ Then, $g \circ f(b) = g(f(b)) = g(y) = a \neq 1_A(b)$; hence *f* has no left inverse. And *f* has no right inverse because if $h : B \to A$ then $f \circ h(x) \neq x = 1_B(x).$

In light of these examples the following claim is interesting.

Claim 7. If a function $f : A \to B$ has a left inverse $g : B \to A$ and a right inverse $h : B \to A$, then $g = h.$

Proof.

$$\begin{aligned} g = g \circ 1_B = g \circ (f \circ h) & \qquad [h \text{ is a right inverse of } f] \\ = (g \circ f) \circ h & \qquad [\text{composition is associative}] \\ = 1_A \circ h & \qquad [g \text{ is a left inverse of } f] \\ = h & \qquad \blacksquare \end{aligned}$$

Consequence. According to the definition, a function is invertible *iff* it has a left inverse and a right inverse; from Claim 7 it follows that in this case there actually is a unique inverse (which is both left and right inverse). *This unique inverse is denoted by* f^{-1}.

Thus, f^{-1} is a function, $f^{-1} : B \to A$ (when $f : A \to B$). We now show that f^{-1} itself is also invertible. More precisely

Claim 8. Let $f : A \rightarrow B$ be an invertible function. Then $f^{-1} : B \rightarrow A$ is also invertible and the inverse of f^{-1} is f: $\boxed{(f^{-1})^{-1} = f}$.

Proof. If f^{-1} is a left inverse of f, then $f^{-1} \circ f = 1_A$, which in turn means that f is a right inverse of f^{-1}. And if f^{-1} is a right inverse of f, then $f \circ f^{-1} = 1_B$, which in turn means that f is a left inverse of f^{-1}. By Claim 7, f is the unique inverse of f^{-1} and the equality follows. ■

Example. Let $X = Y = \mathbb{N}$.

1. Consider the functions $f, g : \mathbb{N} \rightarrow \mathbb{N}$ defined by $g(x) \triangleq \textbf{if } (x \text{ even}) \textbf{ then } \frac{x}{2} \textbf{ else } x$ and $f(x) = 2x$. Then,

   $$\begin{aligned} f \circ g(x) &= f(g(x)) = f(\textbf{if } (x \text{ even}) \textbf{ then } \tfrac{x}{2} \textbf{ else } x) \\ &= 2(\textbf{if } (x \text{ even}) \textbf{ then } \tfrac{x}{2} \textbf{ else } x) = \textbf{if } (x \text{ even}) \textbf{ then } x \textbf{ else } 2x \\ &\neq 1_{\mathbb{N}}(x) \end{aligned}$$

   implying that g is not a right inverse of f. On the other hand,

   $$g \circ f(x) = g(f(x)) = g(2x) = \frac{2x}{2} = x = 1_{\mathbb{N}}(x)$$

   showing that g is a left inverse of f. This implies, by Claim 7, that f does not have a right inverse.

2. Now let $f, g : \mathbb{N} \rightarrow \mathbb{N}$ be defined as: $f(x) \triangleq x \dot{-} 1$ ($x \dot{-} 1$ is equal to 0 for $x = 0$, and $x - 1$ for $x > 0$) and $g(x) = x + 1.$ Then

   $f \circ g(x) = f(g(x)) = f(x+1) = x = 1_{\mathbb{N}}(x)$, whereas
   $g \circ f(x) = g(f(x)) = g(x \dot{-} 1) = (x \dot{-} 1) + 1 = \textbf{if } (x = 0) \textbf{ then } 1 \textbf{ else } x \neq 1_{\mathbb{N}}(x)$.

   Thus, g is a right (but not left) inverse of f; hence, f has no left inverse.

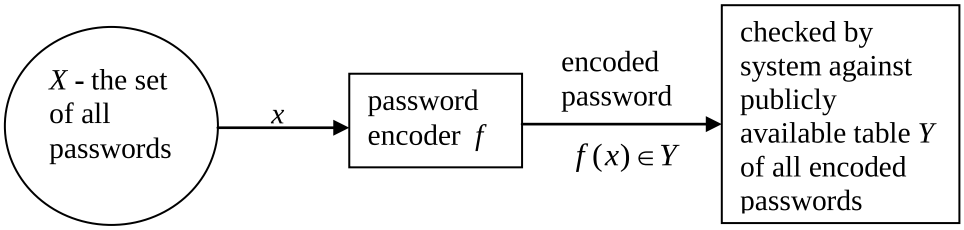
Examples.

1. A standard communication scheme has the following structure:

$$\boxed{sender}\xrightarrow[x\in X]{message}\boxed{encoder\ f}\xrightarrow[f(x)\in Y]{\substack{encoded\\ message}}\boxed{decoder\ g}\xrightarrow[g(f(x))\in X]{\substack{decoded\\ message}}\boxed{receiver}$$

   where X is the set of all possible messages and Y is the set of all encoded messages. In such a system it is imperative that $\forall x \in X,\ \ g(f(x)) = x.$ I.e., that g is a left inverse of f.

2. In a password identification scheme, the user types in a password x from some specific set of all possible passwords. This password is translated into an encoded password $f(x)$ which is then checked against a publicly available file Y of encoded passwords. The "picture" of this situation is given below



X - the set of all passwords
x
password encoder f
encoded password
$f(x)\in Y$
checked by system against publicly available table Y of all encoded passwords

   An adversary who might want to penetrate the system would have to find a password that would allow him to log-on. To do this he needs to find a right inverse $h: Y \to X$ of f. If the adversary has such an h in his possession then for any $y \in Y$ (which, recall, is publicly available) he can compute $h(y)$ and then type it into the system. This will allow the adversary to penetrate the system because $f(h(y)) = f \circ h(y) = 1_Y(y) = y$, which is included in the table.

(C) **Injective and Surjective functions**. These properties deal with the way other functions "interact" with the given function. They may be referred to as the "*categorical properties*" of functions.

Definition.(3rd pair of properties) Let $f : A \to B$ be a function.

- f is surjective (or is a surjection) if $\forall$set $S\,\forall g : S \to B\,\exists h : S \to A\left[g = f \circ h\right]$.
- f is injective (or is an injection) if $\forall$set $T\,\forall g : A \to T\,\exists h : B \to T\left[g = h \circ f\right]$.
- f is bijective (or is a bijection) if it is both surjective and injective.

For these properties a pictorial description might be helpful.

$\boxed{f \text{ surjectve}}$

$$\begin{tikzcd}
A \arrow[rr, "f"] & & B \\
& S \arrow[ul, dashed, "h"] \arrow[ur, "g"'] &
\end{tikzcd}$$

$\boxed{g = f \circ h}$

Here the broken arrow indicates that the existence of *h* is claimed: for every choice of a set *S* and for every choice of a function $g : S \to B$ there exists a function *h* that satisfies the compositional requirement: $g = f \circ h$.

The corresponding "injective picture" is

$\boxed{f \text{ injectve}}$

$$\begin{tikzcd}
A \arrow[rr, "f"] \arrow[dr, "g"'] & & B \arrow[dl, dashed, "h"] \\
& T &
\end{tikzcd}$$

$\boxed{g = h \circ f}$

We will now prove the remarkable result that the three pairs of properties are equivalent in the following sense:

f onto $\Leftrightarrow$ f has right inverse $\Leftrightarrow$ f surjective

and

f 1-1 $\Leftrightarrow$ f has left inverse $\Leftrightarrow$ f *in*jective

It obviously follows that the concepts of *correspondence*, *invertibility*, and *bijectivity* are equivalent as well.

Theorem 9. Let $f : A \to B$. TFAE

1. f is onto.
2. f has a right inverse.
3. f is surjective.

Proof. (1)$\Rightarrow$(2) Since *f* is onto, for each $b \in B$ there is an $a \in A$ such that $b = f(a)$. Pick one such *a* and denote it by a_b. I.e., $b = f(a_b)$. Define $g : B \to A$ by $g(b) \triangleq a_b$. Then, for each $b \in B$ we have $(f \circ g)(b) = f(g(b)) = f(a_b) = b = 1_B(b)$, implying $f \circ g = 1_B$, i.e. *g* is the right inverse of *f*.

(2)$\Rightarrow$(3) Let $s : B \to A$ be a right inverse of f, i.e. $f \circ s = 1_B$. Let S be an arbitrary set and $g : S \to B$ any function. Define $h : S \to A$ by $h \triangleq s \circ g$. Then,

$$f \circ h = f \circ (s \circ g) = (f \circ s) \circ g = 1_B \circ g = g \ .$$

(3)$\Rightarrow$(1) Let $b \in B$. We need to show that there is an $a \in A$ such that $b = f(a)$. By (3) we can pick $S = \{b\}$ and $g : S \to B$ defined by $g(b) = b$. Then, surjectivity of f gives a function $h : S \to A$ such that $g = f \circ h$. Define $a \triangleq h(b)$. Then $f(a) = f(h(b)) = (f \circ h)(b) = g(b) = b$. ■

Theorem 10. Let $f : A \to B$. TFAE

1. f is 1-1.
2. f has a left inverse.
3. f is injective.

Proof. (1)$\Rightarrow$(2) Let $B_1 = f(A)$ (the image of f) and let $B_0 = B - B_1$. Then every element $b \in B_1$ has exactly one pre-image $a_b \in A$ such that $f(a_b) = b$. (Elements of B_0 do not have a pre-image.) Obviously, $a_{f(a)} = a$ since the pre-image of $f(a)$ is a. Let $a_0 \in A$ and define a function $g : B \to A$ by : $g(b) \triangleq$ **if** $(b \in B_1)$ **then** a_b **else** $(b \in B_0)$ a_0. Then,

$$\forall a \in A, \ (g \circ f)(a) = g(f(a)) = a_{f(a)} = a = 1_A(a) \ \text{ i.e. } \ g \circ f = 1_A \, .$$

Thus, g is a left inverse of f.

(2)$\Rightarrow$(3) By assumption, let $k : B \to A$ be the left inverse of f, i.e. $k \circ f = 1_A$. For any set S and any function $g : A \to S$ define $h \triangleq g \circ k : B \to S$. Then,

$$h \circ f = (g \circ k) \circ f = g \circ (k \circ f) = g \circ 1_A = g \ ,$$

implying that f is injective.

(3)$\Rightarrow$(1) Suppose that $a \neq a'$ in A, but $f(a) = f(a')$. By (3) we pick $S = \{\alpha, \alpha'\}$ (with $\alpha \neq \alpha'$) and a function $g : A \to S$ defined by $g(a') = \alpha'$ and $g(a'') = a$, for all other elements $a'' \in A$. Let $h : B \to S$ be a function satisfying $h \circ f = g$ and whose existence is guaranteed by (3). Then a contradiction is reached as follows:

$$\alpha' = g(a') = (h \circ f)(a') = h(f(a')) = h(f(a)) = (h \circ f)(a) = g(a) = \alpha \qquad ■$$

Corollary 11. Let $f : A \to B$. TFAE

1. f is a correspondence.
2. f is invertible.
3. f is a bijection.

Convention: From now on we will use “onto” and “surjective” interchangeably, as is customary in mathematics and computer science. Similarly, we shall identify “1-1” and “injective.”

2.3. CARDINALITY, INFINITE SETS AND CANTOR’S THEOREM

The following very important definition is Georg Cantor’s[1] way to define the concept of cardinality (“number of elements”) of a set. Instead of formally defining what cardinality of a set is, Cantor formally defined when two sets have the same cardinality (regardless of whether the sets are finite or infinite).

Definition. Two sets X and Y *have the same cardinality*, denoted by $|X| = |Y|$, if there is a correspondence (equivalently, a bijection or an invertible function) between them; i.e., there is a function $f : X \to Y$ that is both 1-1 and onto.

In Cantor’s words, paraphrased, consider a “family” of all sets between any two of which there exists a bijection; i.e., a family of sets $\Im$ so that $\forall A, B \in \Im \left[\exists \text{ a bijection } f : A \to B \right]$. Then, informally, the cardinality of $S \in \Im$ is “what is common to all the sets in $\Im$”.

In the discussion of set theory we have defined the cardinality of a finite set to be “the number of elements” in the set. Expressed a little more formally this means that the cardinality of a set S is n, which we denoted by $|S| = n$, *precisely when there exists a bijection between the set S and the subset of natural numbers* $[n] \equiv \{1, 2, \ldots, n\} \subseteq \mathbb{N}$. Thus, a set S was defined as finite precisely when there is a bijection between S and some finite “initial segment” of natural numbers. We have then defined a set to be infinite if it is not finite. In the “functional” terminology this means that there is no bijection between S and any finite initial segment $[n]$ of natural numbers.

Theorem 12. The set of all natural numbers $\mathbb{N}$ is infinite.

Proof. Clearly $\mathbb{N} \neq \varnothing$ since $1 \in \mathbb{N}$. Suppose $\mathbb{N}$ is finite. Then there is a correspondence

[1] Georg Cantor was a mathematician who single-handedly created Set Theory. See a very interesting article in Wikipedia at http://en.wikipedia.org/wiki/Georg_Cantor

$v:[n]\to\mathbb{N}$ and hence $\mathbb{N}=\{v(1),v(2),...,v(n)\}$. Consider the integer $s\triangleq\sum_{i\in[n]}v(i)$. Obviously, $s\in\mathbb{N}$. However, $\forall i\in[n],\ v(i)<s$ and so $s\notin \boldsymbol{range}(v)$, contradiction. ■

Now that we know when two sets have the same cardinality (viz., when there exists a bijection between the two sets) the natural question is "when is the cardinality of one set larger than the cardinality of another set?" Again, for finite sets there is no problem, a set X with 10 elements has smaller cardinality than a set Y with 50 elements; this is denoted by $|X|<|Y|$. For infinite sets we base our definition on bijections, as in the case of equality of cardinalities. The definition is general and applies to both finite and infinite sets. Let X and Y be sets. We say that *the cardinality of* X *is strictly smaller than the cardinality of* Y, notation: $\boxed{|X|<|Y|}$, if the following two conditions hold

(a) there is a 1-1 mapping $f:X\to Y$, and
(b) there is no 1-1 mapping $g:Y\to X$.

Claim 13. Condition (a) and (b) are respectively equivalent to the conditions:

(a') there is an onto mapping $f':Y\to X$.
(b') there is no onto mapping $g':X\to Y$.

Proof. [a $\Leftrightarrow$ a$'$] Use Theorems 9 and 10. If $f:X\to Y$ is 1-1, then it has a left inverse $f':Y\to X$. This f' has a right inverse (actually the function f itself) so it is onto. Conversely, if $f':Y\to X$ is onto then it has a right inverse $f:X\to Y$ and this f has a left inverse (actually the function f' itself) so it is 1-1.
[b$\Leftrightarrow$ b$'$] Left as an exercise. ■

When condition (a), or equivalently (a'), holds we say that the cardinality of X is "smaller than or equal to" the cardinality of Y, notation: $\boxed{|X|\le|Y|}$. Note however, that the inequality signs "<" and "$\le$" are not the ones that we use in arithmetic; they reflect only the existence (and non-existence) of some kinds of mappings between the relevant sets, nothing more and nothing less.

Next we look at an very important theorem of Cantor that had a major impact on the course of development of mathematics. One of its implications is that there does not exist a "largest set" (in the sense of cardinality): for any set whatsoever there exist sets that are larger than it. In particular, this is true for infinite sets! This implies that there is an infinite sequence of ever larger infinite sets. This was very surprising and disturbing to the mathematicians of Cantor's times and a source of much philosophical, metaphysical, and even theological debate. Leading mathematicians of Cantor's time expressed strong reservations and sometimes outright disdain for Cantor's new theory. Eventually, however, Set Theory was accepted by most mathematicians and nowadays constitutes a separate branch within "foundational" mathematics.

The proof of the theorem is very clever but (after the fact) not difficult. The proof method is itself quite important and often used, especially in Theoretical Computer Science.

Theorem 14 (**Cantor**). Let X be any set. <u>There is no onto function</u> $f : X \to \mathcal{P}(X)$.

Proof. Let $f : X \to \mathcal{P}(X)$ be an arbitrary function. It suffices to show that f is not onto. To achieve that it suffices to exhibit an element of $\mathcal{P}(X)$ (i.e., a subset of X) that is not the image of any element of X under f. This set is defined by $\boxed{B_f \triangleq \{x \in X \mid x \notin f(x)\}}$. Obviously, $B_f \subseteq X$ and hence $B_f \in \mathcal{P}(X)$. We will argue that $B_f \notin \boldsymbol{range}(f)$ thus showing that f is not onto. The argument is "by contradiction." Suppose f is onto so that, in particular, $B_f = f(y)$ for some $y \in X$. There are two cases to consider regarding this y:

- $y \in B_f \;\Rightarrow\; y \notin f(y) \;\Rightarrow\; y \notin B_f$, an impossibility!
- $y \notin B_f \;\Rightarrow\; y \in f(y) \;\Rightarrow\; y \in B_f$, also an impossibility!

It follows that f cannot be onto and the proof is complete. ■

Corollary 15. Let X be any set. Then, $|X| < |\mathcal{P}(X)|$.

Proof. Follows from the definition of "<" since there exists a 1-1 $f : X \to \mathcal{P}(X)$. ■

For finite sets Cantor's Theorem does not present surprises. For when X is finite, then $|\mathcal{P}(X)| = 2^{|X|} > |X|$, which is true because for every integer n, $2^n > n$. For infinite sets, e.g. the set $\mathbb{N}$ of natural numbers, Cantor's theorem says that the infinite set $\mathcal{P}(\mathbb{N})$ contains more elements (in the sense of cardinality) than the infinite set $\mathbb{N}$. And by the same argument, $\mathcal{P}(\mathcal{P}(\mathbb{N}))$ contains more elements than $\mathcal{P}(\mathbb{N})$, and so on:

$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < |\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))| < \ldots\ldots$$

The proof of Cantor's theorem uses the ***method of diagonalization***. Since this method is important we will illustrate it in a concrete example of a finite set $X = \{1,2,3,4\}$. For each candidate function $f : X \to \mathcal{P}(X)$ construct an f-table with rows labeled by the names $f(x)$, $x \in X$, plus one extra row for the counterexample set B_f. The columns of the table (except for the first) are labeled by (all) the elements of the set *X*. Each row represents a subset $f(x) \subseteq X$ using a bit vector representation (a.k.a. characteristic function). The method guarantees that the B_f row will always be different from all the other rows in the *f*-table. Here are two examples of possible functions *f*-tables.

f_1	1	2	3	4
$f_1(1)$	0	0	1	1
$f_1(2)$	1	0	0	1
$f_1(3)$	0	0	0	0
$f_1(4)$	1	1	1	1
B_{f_1}	1	1	1	0

f_2	1	2	3	4
$f_2(1)$	1	0	1	0
$f_2(2)$	0	1	0	1
$f_2(3)$	1	1	0	0
$f_2(4)$	1	1	1	0
B_{f_2}	0	0	1	1

When $|X| \le |\mathbb{N}|$, we say that *X* is ***countable***. Thus, a set is countable if either it is a finite set or it has the same cardinality as the set of natural numbers. A set is ***uncountable*** if it is not countable. By Corollary 15, $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$, hence $\mathcal{P}(\mathbb{N})$ is the first example of an uncountable set. Whenever we want to stress that a set is both countable and infinite, we may say that it is ***countably infinite***. The term ***denumerable*** is sometimes used for "countably infinite." Note that $|X| \le |\mathbb{N}|$ is just the condition (a), or (a'), with *Y* substituted by $\mathbb{N}$. A useful way to think about a countable set is that it is (in principle) possible to arrange its elements in a <u>*list*</u> or a <u>*sequence*</u> so that <u>every element of the set will eventually be encountered</u>, allowing repetitions.

Example. The set $X = \{1, 2, 3, 4, 5, 6, 7\}$ is countable because we can list its elements (in many ways, but one is sufficient for countability): 1,2,2,3,5,4,7,6,5. The set of natural numbers is countable as its elements can be listed in the natural order: 1, 2, 3, 4, 5, …

Example. The set of non-negative integers, $\mathbb{Z}^+$, can be listed: $0, 1, 2, 3, 4, \ldots$, so it is countable. The function $f : \mathbb{N} \to \mathbb{Z}$ defined by $f(n) \triangleq n - 1$ is a bijection between the two sets.

Example. The set of integers, $\mathbb{Z}$, can be listed: $0, 1, -1, 2, -2, 3, -3, 4, -4, \ldots.$, hence it also countable. In this case we can give a specific bijection $f : \mathbb{N} \to \mathbb{Z}$ as follows:

$$f(n) = \begin{cases} \frac{n}{2} & n \text{ even} \\ -\frac{n-1}{2} & n \text{ odd} \end{cases}$$

<u>Useful Observation</u>. Note that a listing of the elements of a set *X* in effect constitutes an onto function $f : \mathbb{N} \to X$, $f(1), f(2), f(3), \ldots$ By Claim 13, part (a), this implies that *X* is countable.

Corollary 16. A subset of a countable set is countable. Equivalently, a superset of an uncountable set is uncountable.

Proof. If a set is X countable, it can be listed, and so any subset $A \subseteq X$ can be listed by omitting the elements not in the set, i.e. the elements in $X - A$. If a superset Z of an uncountable set Y were countable, then Y would be a subset of a countable set and hence by the first part of the claim. ■

Claim 17. The set of prime numbers is countably infinite.

Proof. Being a subset of $\mathbb{N}$, the set of prime numbers is obviously countable.

Example. The set $\mathbb{N}\times\mathbb{N} = \{(i, j) \mid i, j \in \mathbb{N}\}$ is countable. To show that we need to show that there is a bijection between $\mathbb{N}\times\mathbb{N}$ and $\mathbb{N}$. Define $f : \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ by the following formula

$$f(m,n) \triangleq m + \frac{(m+n-1)(m+n-2)}{2}.$$

It is easy to compute: $f(1,1) = 1;\ f(1,2) = 2;\ f(2,1) = 3;$ e.t.c. Perhaps you should try to show that f is a bijection.

Example. An *infinite binary sequence* is an infinite sequence $b = \langle b_1, b_2, b_3, ..., b_n, ...\rangle$ where $\forall i \geq 1, b_i \in \{0,1\}$. Each such sequence defines a subset of natural numbers $A_b = \{n \mid b_n = 1\} \subseteq \mathbb{N}$. And conversely, each subset $A \subseteq \mathbb{N}$ defines an infinite binary sequence $b_A = \langle b_1, b_2, b_3, ..., b_n, ...\rangle$ by

$$b_n = \begin{cases} 1 & n \in A \\ 0 & n \notin A \end{cases}$$

Let $\mathbf{B_2}$ be the set of all infinite binary sequences. It is easy to see that each of the two mappings between $\mathbf{B_2}$ and $\mathcal{P}(\mathbb{N})$ is 1-1 and onto; in fact, they are inverses of each other. This shows that $|\mathcal{P}(\mathbb{N})| = |\mathbf{B_2}|$ and thus $\mathbf{B_2}$ is uncountable.

Example. Consider the function defined by the formula: $f(x) \triangleq \dfrac{x}{1+|x|}$. Obviously it is well-defined for all real numbers so we set its domain as $\mathbb{R}$. It is also easy to see that for all its arguments the values are in the open interval $(-1,1)$. Actually, this function $f:\mathbb{R}\to(-1,1)$ is a 1-1 and onto function. Hence, $|\mathbb{R}| = |(-1,1)|$.

We finally want to show that the set of real numbers $\mathbb{R}$ is uncountable. Actually, we will show a seemingly stronger result that the set of real numbers in the open interval $(0,1)$ is uncountable. By Corollary 16, it follows that $\mathbb{R}$ is uncountable as well. The proof uses a diagonal argument like in the proof of Cantor's theorem. We first note that every real number $r\in(0,1)$ can be written as an infinite decimal fraction $r = 0.r_1r_2r_3r_4r_5....$ where $\forall i\geq 1\left[0\leq r_i\leq 9\right]$. For example:

$\frac{1}{2} = 0.5000000\ldots$ $\qquad$ $e-2 = 0.7182818284590\ldots$

$\frac{1}{3} = 0.3333333\ldots$ $\qquad$ $\pi\text{-}3 = 0.14159\ 26535\ 89793\ldots$

$\frac{1}{10} = 0.1000000\ldots$ $\qquad$ $\frac{2}{11} = 0.181818181818181\ldots$

Now suppose that there is an onto mapping $\rho:\mathbb{N}\to(0,1)$. Just for illustrative purposes consider the infinite table with rows labeled by $\rho(1),\rho(2),\rho(3),\rho(4),\ldots$ with the *k*th row containing the infinite decimal expansion of the fraction $\rho(k)$. An example of such a table could be:

n	$\rho(n)$
---	-------------------------
1	0.66326432846084699919234...
2	0.87236481624123841297674...
3	0.99999421471247192477123...
4	0.12345678912345678912345...
5	0.80239487239471923874002...
6	0.18181818181818181818181...
7	0.32257876526578634957676...
	... ...

Denote by $\rho(k)_i$ the i^{th} digit of the fraction $\rho(k)$. E.g., $\rho(1)_2 = 6$ and $\rho(5)_9 = 2$. The digits $\rho(k)_k$ are indicated in red in the table given above. Given such a table representing the function ρ, we use the diagonal method to define a decimal fraction, B_ρ, which is in the interval $(0,1)$ but is not in the range of ρ. B_ρ is defined by $B_\rho \triangleq 0.d_1d_2d_3d_4d_5d_6\ldots$ where $d_k \triangleq \{0,1,2,3,4,5,6,7,8,9\}-\{0,9,\rho(k)_k\}$. Then, the fraction B_ρ does not occur in the ρ-table because it differs from row $\rho(k)$ in the k^{th} position.

2.4. DEDEKIND'S[2] AND TARSKI'S[3] DEFINITIONS OF FINITE SETS

We have defined a set to be finite when there is a bijection between the set and some finite "initial segment" of natural numbers. We have then defined a set to be infinite if it is not finite. This definition is quite adequate but it explicitly depends on the concept of "integer".

It may be of some interest to define "finite" (and hence "infinite') sets without referring to integers. One of the first such definitions was offered by Richard Dedekind: ***a set is finite if there is no bijection between it and any of its proper subsets***. By this definition, ***a set is infinite if there is a bijection between the set and one of its proper subsets***. Though relatively simple and not difficult to use, Dedekind's definition has a drawback in that it requires advanced methods to prove the equivalence between "Dedekind finite" sets and our original definition of finite sets[4].

Example. show that some our-finite set is Dedekind-finite
show that Z is infinite: n -> n+1
show that N is infinite:
show that R is infinite:

We will consider another, rather interesting, proposal of Tarski. Let $\Im$ be a family of sets. A set $A \in \Im$ is called *minimal* if $\Im$ does not contain a proper subset of *A* (put differently, no proper subset of *A* belongs to $\Im$). Tarski defines a set *S* to be *finite* if every non-empty family $\Im \subseteq \mathcal{P}(S)$ has a minimal element. Thus, contrapositively, a set *S* is *infinite* if there exists a non-empty family $\Im \subseteq \mathcal{P}(S)$ that does not have a minimal element. Note that Tarski's definition, unlike our own or Dedekind's, does not use the concept of bijection.

Example. Let $A = \{1, 2, 3\}$. Its power set is $\mathcal{P}(A) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, A\}$. For *A* to be finite it must be the case that every subset $\Im$ of $\mathcal{P}(A)$ must have a minimal element. Obviously, if $\varnothing \in \Im,$ then $\varnothing$ will be minimal. Here are some examples:

$\Im_1 = \{\{1\}, \{1, 3\}, \{3\}\}$	minimal elements (sets) are {1} and {3},
$\Im_2 = \{\{2\}, \{1, 2\}, A\}$	the only minimal element is {2}
$\Im_3 = \{\{1\}, \{2\}, \{3\}\}$	minimal elements are {1}, {2} and {3}.

[2] **Julius Wilhelm Richard Dedekind** (1831 – 1916) was a German mathematician who did important work in abstract algebra, algebraic number theory and the foundations of the real numbers.

[3] **Alfred Tarski** (1902, Warsaw, Poland – 1983, Berkeley, California) was a logician and mathematician who spent four decades as a professor of mathematics at the University of California, Berkeley. He wrote extensively on topology, geometry, measure theory, mathematical logic, set theory, metamathematics, and above all, model theory, abstract algebra, and algebraic logic.

[4] In fact, it seems that the, so called, ***Axiom of Choice*** is required.

Since similar arguments can be given to any (of the 2^8) subset $\Im$ of $\mathcal{P}(A)$, it follows that A is finite according to Tarski's definition. ■

Example. We will use Tarski's definition to show that the set of natural numbers $\mathbb{N}=\{0,1,2,...\}$ is infinite. We define a family $\Im$ of subsets of $\mathbb{N}$ (just a subset of $\mathcal{P}(\mathbb{N})$): $\Im=\{N_0,N_1,N_2,...\}$ where $N_k \triangleq \mathbb{N}-\{0,1,...,k-1\}$. According to this definition we have

$$N_0=\mathbb{N}; \quad N_1=\mathbb{N}-\{0\}=\{1,2,3,...\}; \quad N_2=\mathbb{N}-\{0,1\}=\{2,3,4,...\} \quad \text{etc.}$$

It should be easily seen that: $N_0 \supsetneq N_1 \supsetneq N_2 \supsetneq ... \supsetneq N_k \supsetneq N_{k+1} \supsetneq ....$, i.e. $\Im$ has no minimal element and consequently $\mathbb{N}$ must be infinite. ■

As a practice in using these concepts, we shall prove that every finite set according to Tarski is also finite according to Dedekind. Using the notation of Exercises 28 and 29, let $\mathcal{F}_D$ and $\mathcal{F}_T$ denote the collections of all finite sets according Dedekind and Tarski respectively.

Theorem. $\mathcal{F}_T \subseteq \mathcal{F}_D$.

Proof. Let $A\in\mathcal{F}_T$ and suppose that for some $A'\subsetneq A$ there is a bijection $f:A\to A'$. Define a family of sets $\Im=\{C\subseteq A \mid f(C)\subsetneq C\}$. Since $f(A)=A'\subsetneq A$, we have $A\in\Im$. It follows that $\varnothing\neq\Im\subseteq\mathcal{P}(A)$ and since A is finite (according to Tarski's definition), $\Im$ has a minimal element, say K. Since $K\in\Im$, $f(K)\subsetneq K$ and hence $f(K)\notin\Im$ (by the minimality of K). On the other hand, since f is 1-1, $f(K)\subsetneq K$ implies $f(f(K))\subsetneq f(K)$ (easy to verify), which in turn implies that $f(K)\in\Im$. This is a contradiction showing that $A\in\mathcal{F}_D$. ■

EXERCISES

(01) Express the function $f:\mathbb{R}\to\mathbb{R}$ defined by $f(x)=1+e^{2\sin^2 x+3}$ as a composition of simpler functions.

(02) Let $f:A\to B$ and $g:B\to A$ be two functions such that $g\circ f=1_A$. Show that the function $f\circ g$ is idempotent.

(03) Let $k:A\to A$ and let $A'\subseteq A$ be the range of *k*. Show that *k* is idempotent if, and only if, every $a'\in A'$ is a *fixpoint* of *k*, i.e. $k(a')=a'$.

(04) Suppose that the function $k:A\to A$ is idempotent. Define a domain *B* and functions $f:A\to B$ and $g:B\to A$ that satisfy: $f\circ g=1_B$ and $g\circ f=k$.

(05) Suppose $f:C\to D$ and $g:D\to C$ satisfy $f\circ g\circ f=f$.

(a) Prove or disprove: $f\circ g$ is idempotent.
(b) Prove or disprove: $g\circ f$ is idempotent.
(c) Use *f* and *g* to construct a mapping $g':D\to C$ that satisfies the following two identities: $f\circ g'\circ f=f$ and $g'\circ f\circ g'=g'$.

(06) Let $f:X\to Y$.

(a) Prove: f 1-1 $\Rightarrow$ $\forall A_1,A_2\subseteq X\left[f(A_1\cap A_2)=f(A_1)\cap f(A_2)\right]$.
(b) Prove: f 1-1 $\Rightarrow$ $\forall A_1,A_2\subseteq X\left[f(A_1-A_2)=f(A_1)-f(A_2)\right]$.
(c) Prove: f 1-1 $\Rightarrow$ $\forall A_1,A_2\subseteq X\left[f(A_1\oplus A_2)=f(A_1)\oplus f(A_2)\right]$.
(d) Which of the implications (a), (b), or (c) can be reversed?

(07) Define $f:[0,\infty)\to[0,1)$ by $f(x)=\frac{x}{1+x}$. Prove that f is a correspondence and find its inverse.

(08) Define $g:(-\infty,0]\to(-1,0]$ by $g(x)=\frac{x}{1-x}$. Prove that g is a correspondence and find its inverse.

(09) [*Preservation of properties under composition*] Let $f:A\to B$ and $g:B\to C$.

(a) Prove or disprove: *f* and *g* are 1-1 $\Rightarrow$ $g\circ f$ is 1-1.
(b) Prove or disprove: $g\circ f$ is 1-1 $\Rightarrow$ *f* and *g* are 1-1.
(c) Prove or disprove: *f* and *g* are onto $\Rightarrow$ $g\circ f$ is onto.
(d) Prove or disprove: $g\circ f$ is onto $\Rightarrow$ *f* and *g* are onto.

(10) Recall that $\mathbb{R}$ denotes the set of real numbers and define a function $f:\mathbb{R}\to\mathbb{R}$ by $f(x)=2x+7.$ Show that f is invertible by explicitly giving a furmula for the inverse map g and showing that $\forall x\in\mathbb{R}, (f\circ g)(x)=x$ and $(g\circ f)(x)=x.$

(11) Let $f:X\to Y$ and let $B\subseteq Y$. The *inverse image* of B is a subset of X defined by

$$f^{-1}(B) \triangleq \{x\in X \mid f(x)\in B\}.$$

In the following, A's with or without subscripts (respectively, B's with or without subscripts) are subset of X (respectively, Y). Prove the following claims.

(a) $B_1\subseteq B_2 \quad\Rightarrow\quad f^{-1}(B_1)\subseteq f^{-1}(B_2).$
(b) $f^{-1}(B_1\cup B_2)=f^{-1}(B_1)\cup f^{-1}(B_2).$
(c) $f^{-1}(B_1\cap B_2)=f^{-1}(B_1)\cap f^{-1}(B_2).$
(d) $f^{-1}(B_1-B_2)=f^{-1}(B_1)-f^{-1}(B_2).$
(e) $f^{-1}(B_1\oplus B_2)=f^{-1}(B_1)\oplus f^{-1}(B_2).$
(f) $\overline{f^{-1}(B)}=f^{-1}(\overline{B}).$
(g) $A\subseteq f^{-1}(f(A)).$
(h) $f(f^{-1}(B))\subseteq B.$
(i) $f(f^{-1}(B))=B \iff B\subseteq f(X).$
(j) $f(A)\cap B=f(A\cap f^{-1}(B)).$
(k) $f^{-1}(f(A_1))=A_1 \quad\Rightarrow\quad f(A\cap A_1)=f(A)\cap f(A_1).$

(12) Let $A=\{a,b,c\}.$

(a) Find an invertible function $f:A\to A,$ different from the identity 1_A.
(b) Find an idempotent function $e:A\to A,$ different from the identity 1_A.
(c) Find a set B and two functions $B\xrightarrow{s}A\xrightarrow{r}B$ such that $r\circ s=1_B$ and $s\circ r=e.$

(13) Let $f:X\to X$. (a) Prove or disprove: $\forall x\in X\left[f(x)=x\right] \iff \forall x\in X\left[f(f(x))=f(x)\right].$
(b) Prove or disprove: $\forall x\in f(X)\left[f(x)=x\right] \iff \forall x\in X\left[f(f(x))=f(x)\right].$

(14) Let X and Y be sets and let $\psi:\mathcal{P}(X)\to\mathcal{P}(Y)$. [Warning: ψ need not be a mapping induced by a function from X to Y (as defined in class); it is just an arbitrary function with domain and co-domain as specified.] Prove the following implication

$$\forall A,B\subseteq X\left[\psi(A\cup B)=\psi(A)\cup\psi(B)\right] \quad\Rightarrow\quad \forall A,B\subseteq X\left[\psi(A\cap B)\subseteq\psi(A)\cap\psi(B)\right].$$

(15) Let X and Y be sets and let $\varphi : \mathcal{P}(Y) \to \mathcal{P}(X)$ be a function satisfying the following two conditions:

(a) $\forall \Im \subseteq \mathcal{P}(Y)\left[\varphi(\bigcup \Im) = \bigcup_{S\in\Im} \varphi(S)\right]$, and
(b) $\forall S \in \mathcal{P}(Y)\left[\varphi(Y - S) = X - \varphi(S)\right]$.

Prove that there is a unique function $f : X \to Y$ such that $\forall S \in \mathcal{P}(Y)\left[\varphi(S) = f^{-1}(S)\right]$, where f^{-1} is the "inverse image" mapping as defined in Exercise 11.

(16) Let $\Im = \left\{A_i \middle| i \in I\right\}$ be a family of (not necessarily distinct) sets. The *Cartesian product* of $\Im$ is defined as a set of functions

$$\prod \Im \equiv \prod_{i\in I} A_i \triangleq \left\{ f : I \to \bigcup_{i\in I} A_i \middle| \forall i \in I\left[f(i) \in A_i \right]\right\}.$$

Thus, $A_1 \times A_2$ can be viewed as a set of functions $\left\{ f : \{1,2\} \to A_1 \cup A_2 \middle| f(i) \in A_i, i = 1, 2\right\}$, the idea being that each pair $(a,b) \in A_1 \times A_2$ is identified with the function f defined by $f(1) = a,\ f(2) = b.$ Let $\Im = \left\{A_i \middle| i \in I\right\}$ and $\Im' = \left\{B_i \middle| i \in I\right\}$ be two families of sets over the same index set I. Prove the equality $\prod_{i\in I} A_i \cap \prod_{i\in I} B_i = \prod_{i\in I} (A_i \cap B_i)$.

(17) Let $f : A \to B$ be 1-1. Prove that $\forall$set $S \forall g_1, g_2 : S \to A$, $f \circ g_1 = f \circ g_2 \Rightarrow g_1 = g_2$.

(18) Let $f : A \to B$ be onto. Show that $\forall$ set $S\ \forall g_1, g_2 : B \to S,\ g_1 \circ f = g_2 \circ f \Rightarrow g_1 = g_2$.

(19) How many bijections are there between the sets $\{a, b, c\}$ and $\{1, 2, 3\}$? List them all.

(20) For sets A and B define the set of bijections from A to B

$$\boldsymbol{B}(A,B) \triangleq \left\{ f \middle| f : A \to B \text{ is a bijection}\right\}.$$

Note that if $|A| \neq |B|$, then $\boldsymbol{B}(A,B) = \varnothing$. Prove: $\boldsymbol{B}(A,B) \neq \varnothing \Rightarrow |\boldsymbol{B}(A,B)| = |\boldsymbol{B}(A,A)|$.

(21) Let $f : A \to B$ be function that has a left inverse (equivalently, is 1-1). How many left inverses does f have?

(22) Show that the set of rational numbers (fractions) $\mathbb{Q}$, is countable.

(23) Find a bijection between the set of natural numbers $\mathbb{N}$ and the subset of positive even integers and prove that it is in fact a bijection.

(24) Show that for any real $a<b$ the function defined by the formula

$$g(x) \triangleq \frac{x}{1+|x|}\cdot\frac{b-a}{2} + \frac{b+a}{2}$$

is a bijection $g:\mathbb{R}\to(a,b)$. Conclude that for any real $a<b$, $|\mathbb{R}|=|(a,b)|$.

(25) Function $\beta:\mathcal{P}(X)\to\mathcal{P}(Y)$ is <u>*isotone*</u> if $\forall A,B\in\mathcal{P}(X)\left[A\subseteq B\Rightarrow\beta(A)\subseteq\beta(B)\right]$. Let $\varphi:\mathcal{P}(X)\to\mathcal{P}(Y)$ and $\psi:\mathcal{P}(Y)\to\mathcal{P}(X)$ be isotone and define $\theta:\mathcal{P}(X)\to\mathcal{P}(X)$ by $\theta(A)\triangleq\overline{\psi(\overline{\varphi(A)})}$.

(a) Prove that θ is isotone.

(b) Define a subset $\Im\triangleq\left\{A\in\mathcal{P}(X)\,\middle|\,\theta(A)\subseteq A\right\}\subseteq\mathcal{P}(X)$. Since clearly $X\in\Im$, we can define $X_1\triangleq\bigcap\Im\equiv\bigcap_{F\in\Im}F$. Prove that $X_1\in\Im$.

(c) Prove that $A\in\Im\Rightarrow\theta(A)\in\Im$.

(d) Prove $\theta(X_1)=X_1$.

(e) Define $X_2\triangleq\overline{X_1}\equiv X-X_1$, $Y_1\triangleq\varphi(X_1)$, and $Y_2\triangleq\overline{Y_1}\equiv Y-Y_1$. Clearly, $\{X_1,X_2\}$ and $\{Y_1,Y_2\}$ are partitions of X and Y respectively. Prove that $\psi(Y_2)=X_2$.

(f) <u>We have shown the following **Claim**</u>: Let X and Y be sets and $\varphi:\mathcal{P}(X)\to\mathcal{P}(Y)$ and $\psi:\mathcal{P}(Y)\to\mathcal{P}(X)$ be isotone. Then there exist partitions $X=X_1\uplus X_2$ and $Y=Y_1\uplus Y_2$ such that $Y_1=\varphi(X_1)$ and $X_2=\psi(Y_2)$.

(g) Prove the following result of Stefan Banach[5]: Let X and Y be sets and let $\alpha:X\to Y$ and $\beta:Y\to X$ be functions. Then there exist partitions $X=X_1\uplus X_2$ and $Y=Y_1\uplus Y_2$ such that $Y_1=\alpha(X_1)$ and $X_2=\beta(Y_2)$.

(26)[See Exercise (25)] In Exercise (25) we have defined a function $\theta:\mathcal{P}(X)\to\mathcal{P}(X)$ by $\theta(A)\triangleq\overline{\psi(\overline{\varphi(A)})}$ and in part (a) have shown that θ is isotone. This is assumed as given in this problem. Define a subset $\Re\triangleq\{A\subseteq X\,|\,A\subseteq\theta(A)\}\subseteq\mathcal{P}(X)$. Since $\varnothing\in\Re$, we can define $U\triangleq\bigcup\Re=\bigcup_{A\in\Re}A$.

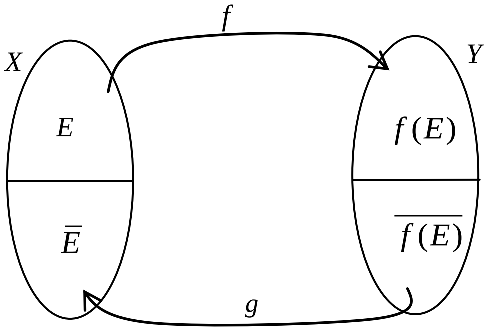
(a) Show that $U\in\Re$.

(b) Prove that $A\in\Re\Rightarrow\theta(A)\in\Re$.

(c) Prove $\theta(U)=U$.

[5] **Stefan Banach** (1892–1945) was a Polish mathematician who worked in interwar Poland and in Soviet Ukraine. A self-taught math prodigy, Banach was the founder of modern functional analysis (branch of analysis studying vector spaces and operators acting upon them) and a founder of the Lwów School of Mathematics.

(27) Let X and Y be sets and $f : X \to Y$ and $g : Y \to X$ two 1-1 mappings. Suppose there is a subset $E \subseteq X$ such that $\overline{E} = g(\overline{f(E)})$. Picture of the situation is:



Define a function $h : X \to Y$ by: $h(x) \triangleq$ <u>if</u> $x \in E$ <u>then</u> $f(x)$ <u>else</u> $g^{-1}(x)$. Prove that h is a bijection.

(28) Just in this exercise denote by $\mathcal{F}_D$ the collection of all finite sets according to Dedekind's definition. Prove, $B \in \mathcal{F}_D \wedge A \subseteq B \Rightarrow A \in \mathcal{F}_D$.

(29) Just in this exercise denote by $\mathcal{F}_T$ the collection of all finite sets according to Tarski's definition.

(a) Explain, very briefly, why $\varnothing, \{x\} \in \mathcal{F}_T$.

(b) Prove: $B \in \mathcal{F}_T \wedge A \subseteq B \Rightarrow A \in \mathcal{F}_T$.

(c) Use (b) to conclude that: A any set and $B \in \mathcal{F}_T \Rightarrow A \cap B \in \mathcal{F}_T$ & $A - B \in \mathcal{F}_T$.

(d) Prove: $A \in \mathcal{F}_T \wedge B \in \mathcal{F}_T \Rightarrow A \cup B \in \mathcal{F}_T$. [Challenging!]

(30) Recall that Tarski defines a set S to be <u>*finite*</u> if every non-empty family $\mathfrak{I} \subseteq \mathcal{P}(S)$ has a minimal element. Here we consider a "dual" approach. Let $\mathfrak{I}$ be a family of sets. A set $A \in \mathfrak{I}$ is called <u>*maximal*</u> if $\mathfrak{I}$ does not contain a proper superset of A (put differently, no proper superset of A belongs to $\mathfrak{I}$). Let us say that a set T is <u>*max-finite*</u> if every non-empty family $\mathfrak{I} \subseteq \mathcal{P}(S)$ has a maximal element. Prove that a set is Tarski-finite iff it is max-finite.