1. A Little Set Theory

I see it, but I don't believe it.

Cantor to Dedekind 29 June 1877

Functions are the single most important idea pervading modern mathematics. We will assume the informal definition of a function—a well-defined rule assigning to each element of the set A a unique element in the set B. We denote these data by $f\colon A \to B$ and the rule by $f\colon a \in A \mapsto f(a) \in B$. The set A is the **domain** of f and the receiving set B is its **codomain** (or range). We make an important distinction between the codomain and the **image** of a function, $f(A) = \{f(a) \in B \mid a \in A\}$ which is a subset contained in B.

When the codomain of one function and the domain of another coincide, we can compose them: $f\colon A \to B$, $g\colon B \to C$ gives $g \circ f\colon A \to C$ by the rule $g \circ f(a) = g(f(a))$. If $X \subset A$, then we write $f|_X\colon X \to B$ for the restriction of the rule of f to the elements of X. This changes the domain and so it is a different function. Another way to express $f|_X$ is to define the *inclusion function*

$$i\colon X \to A, \quad i(x) = x.$$

We can then write $f|_X = f \circ i\colon X \to B$.

Certain properties of functions determine the notion of equivalence of sets.

Definition 1.1. *A function $f\colon A \to B$ is* **one-one** *(or injective), if whenever $f(a_1) = f(a_2)$, then $a_1 = a_2$. A function $f\colon A \to B$ is* **onto** *(or surjective) if for any $b \in B$, there is an $a \in A$ with $f(a) = b$. The function f is a* **one-one correspondence** *(or bijective, or an equivalence of sets) if f is both one-one and onto. Two sets are* **equivalent** *or have the* **same cardinality** *if there is a one-one correspondence $f\colon A \to B$.*

If $f\colon A \to B$ is a one-one correspondence, then f has an inverse function $f^{-1}\colon B \to A$. The inverse function is determined by the fact that if $b \in B$, then there is an element $a \in A$ with $f(a) = b$. Furthermore, a is uniquely determined by b because $f(a) = f(a') = b$ implies that $a = a'$. So we define $f^{-1}(b) = a$. It follows that $f \circ f^{-1}\colon B \to B$ is the identity mapping $\mathrm{id}_B(b) = b$, and likewise for $f^{-1} \circ f\colon A \to A$ is the identity id_A on A.

For example, if we restrict the tangent function of trigonometry to $(-\pi/2, \pi/2)$, then we get a one-one correspondence $\tan\colon (-\pi/2, \pi/2) \to \mathbb{R}$. The inverse function is the arctan function. Furthermore, any open interval (a, b) is equivalent to any other (c, d) via the one-one correspondence $t \mapsto c + [d(t-a)/(b-a)]$. Thus the set of real numbers is equivalent as sets to any open interval of real numbers.

Given a function $f\colon A \to B$, we can define new functions on the collections of subsets of A and B. For any set S, let $\mathcal{P}(S) = \{X \mid X \subset S\}$ denote the **power set** of S. We define the **image** of a subset $X \subset A$ by

$$f(X) = \{f(x) \in B \mid x \in X\},$$

and this determines a function $f\colon \mathcal{P}(A) \to \mathcal{P}(B)$. Define the **preimage** of a subset $U \subset B$ by

$$f^{-1}(U) = \{x \in A \mid f(x) \in U\}.$$

The preimage determines a function $f^{-1}: \mathcal{P}(B) \to \mathcal{P}(A)$. This is a splendid abuse of notation; however, *don't confuse the preimage with an inverse function.* Inverse functions only exist when f is one-one and onto. Furthermore, the domain of the preimage is the set of subsets of B. We list some properties of the image and preimage functions. The proofs are left to the reader.

PROPOSITION 1.2. *Let $f: A \longrightarrow B$ be a function and U, V subsets of B. Then*
1) *If $U \subset V$, then $f^{-1}(U) \subset f^{-1}(V)$.*
2) *$f^{-1}(U \cup V) = f^{-1}(U) \cup f^{-1}(V)$.*
3) *$f^{-1}(U \cap V) = f^{-1}(U) \cap f^{-1}(V)$.*
4) *$f(f^{-1}(U)) \subset U$*
5) *For $X \subset A$, $X \subset f^{-1}(f(X))$.*
6) *If, for any $U \subset B, f(f^{-1}(U)) = U$, then f is onto.*
7) *If, for any $X \subset A, f^{-1}(f(X)) = X$, then f is one-one.*

EQUIVALENCE RELATIONS

A significant notion in set theory is the **equivalence relation**. A relation, R, is formally a subset of the set of pairs $A \times A$, of a set A. We write $x \sim y$ whenever $(x, y) \in R$.

DEFINITION 1.3. *A relation $\sim$ is an* **equivalence relation** *if*
1) *For all x in A, $x \sim x$. (Reflexive)*
2) *If $x \sim y$, then $y \sim x$. (Symmetric)*
3) *If $x \sim y$ and $y \sim z$. (Transitive)*

Examples: **(1)** For any set A, the relation of equality $=$ is an equivalence relation: No element is related to any other element except itself.

(2) Let $A = \mathbb{Z}$, the set of integers with the usual sense of divisibility. Given a nonzero integer m, write $k \equiv l$ whenever m divides $l-k$, denoted $m \mid l-k$. Notice that $m \mid 0 = k-k$ so $k \equiv k$ for any k and $\equiv$ is reflexive. If $m \mid l-k$, then $m \mid -(l-k) = k-l$ so that $k \equiv l$ implies $l \equiv k$ and $\equiv$ is symmetric. Finally, suppose for some integers d and e that $l-k = md$ and $j-l = me$. Then $j-k = j-l+l-k = me+md = m(e+d)$. This shows that $k \equiv l$ and $l \equiv j$ imply $k \equiv j$ and $\equiv$ is transitive. Thus $\equiv$ is an equivalence relation. It is usual to write $k \equiv l \pmod{m}$ to keep track of the dependence on m.

(3) Let $\mathcal{P}(A) = \{U \mid U \subset A\}$ denote the **power set** of A. Then we can define a relation $U \leftrightarrow V$ whenever there is a one-one correspondence $U \longrightarrow V$. The identity function $\mathrm{id}_U: U \to U$ establishes that $\leftrightarrow$ is reflexive. The fact that the inverse of a one-one correspondence is also a one-one correspondence proves $\leftrightarrow$ is symmetric. Finally, the composition of one-one correspondences is a one-one correspondence and so $\leftrightarrow$ is transitive. Thus $\leftrightarrow$ is an equivalence relation.

(4) Suppose $B \subset A$. Then we can define a relation by $x \sim y$ if x and y are both in B; otherwise, $x \sim y$ only if $x = y$. This relation comes in handy later.

Given an equivalence relation on a set A, say $\sim$, we define the **equivalence class** of an element a in A by

$$[a] = \{b \in A \mid a \sim b\} \subset A.$$

We denote the set of equivalence classes by $[A] = \{[a] \mid a \in A\}$. Finally, let p denote the mapping, $p: A \to [A]$ given by $p(a) = [a]$.

Proposition 1.4. *If a, $b \in A$, then as subsets of A, either $[a] = [b]$, when $a \sim b$, or $[a] \cap [b] = \emptyset$.*

Proof: If $c \in [a] \cap [b]$, then $a \sim c$ and $b \sim c$. By symmetry we have $c \sim b$ and so, by transitivity, $a \sim b$. Suppose $x \in [a]$, then $x \sim a$, and with $a \sim b$ we have $x \sim b$ and $x \in [b]$. Thus $[a] \subset [b]$. Reversing the roles of a and b in this argument we get $[b] \subset [a]$ and so $[a] = [b]$. ♢

This proposition shows that the equivalence classes of an equivalence relation on a set A partition the set into disjoint subsets. The canonical function $p: A \to [A]$ has special properties.

Proposition 1.5. *The function $p: A \to [A]$ is a surjection. If $f: A \to Y$ is any other function for which, whenever $x \sim y$ in A we have $f(x) = f(y)$, then there is a function $\overline{f}: [A] \to Y$ for which $f = \overline{f} \circ p$.*

Proof: The surjectivity of p is immediate. To construct $\overline{f}: [A] \to Y$ let $[a] \in [A]$ and define $\overline{f}([a]) = f(a)$. We need to check that this rule is well-defined. Suppose $[a] = [b]$. Then we require $f(a) = f(b)$. But this follows from the condition that $a \sim b$ implies $f(a) = f(b)$. To complete the proof, $\overline{f}([a]) = \overline{f}(p(a)) = f(a)$ and so $f = \overline{f} \circ p$. ♢

Of course, $p^{-1}([a]) = \{b \in A \mid b \sim a\} = [a]$ *as a subset of A, not as an element of the set* $[A]$. We have already observed that the equivalence classes partition A into disjoint pieces. Equivalently suppose $P = \{C_\alpha, \alpha \in I\}$ is a collection of subsets that partitions A, that is,

$$\bigcup\nolimits_{\alpha \in I} C_\alpha = A \ \text{ and } C_\alpha \cap C_\beta = \emptyset \ \text{ if } \alpha \neq \beta.$$

We can define a relation on A from the partition by

$$x \sim_P y \text{ if there is an } \alpha \in I \text{ with } x, y \in C_\alpha.$$

Proposition 1.6. *The relation $\sim_P$ is an equivalence relation. Furthermore there is a one-one correspondence between $[A]$ and P.*

Proof: $x \sim_P x$ follows from $\bigcup_{\alpha \in I} C_\alpha = A$. Symmetry and transitivity follow easily. The one-one correspondence required for the isomorphism is given by

$$f: A \longrightarrow P \ \text{ where } a \mapsto C_\alpha, \ \text{ if } a \in C_\alpha.$$

By Proposition 1.5 this factors as a mapping $\overline{f}: [A] \to P$, which is onto. We check that $\overline{f}$ is one-one: if $\overline{f}([a]) = \overline{f}([b])$ then $a, b \in C_\alpha$ for the same α and so $a {\sim_P} b$ which implies $[a] = [b]$. ♢

This discussion leads to the following equivalence of sets:

$$\{\text{Partitions of a set } A\} \Longleftrightarrow \{\text{Equivalence relations on } A\}.$$

Sets like the integers $\mathbb{Z}$ or a vector space V enjoy extra structure—you can add and subtract elements. You also can multiply elements in $\mathbb{Z}$, or multiply by scalars in V. When there is an equivalence relation on sets with the extra structure of a binary operation one can ask if the relation respects the operation. We consider two important examples and then deduce general conditions for this special property.

Example 1: For the equivalence relation $\equiv \pmod{m}$ on $\mathbb{Z}$ with $m \neq 0$ it is customary to write

$$[\mathbb{Z}] \quad =: \quad \mathbb{Z}/m\mathbb{Z}$$

Given two equivalence classes in $\mathbb{Z}/m\mathbb{Z}$, can we add them to get another? The most obvious idea to try is the following formula:

$$[i] + [j] = [i + j].$$

To be sure this makes sense, remember $[i] = [i']$ whenever $i \equiv i' (\bmod m)$ so we have to be sure any changes of representative of an equivalence class do not alter the sum equivalence classes. Suppose $[i] = [i']$ and $[j] = [j']$, then we require $[i + j] = [i' + j']$ if we want a definition of $+$ on $\mathbb{Z}/m\mathbb{Z}$. Let $i' - i = rm$ and $j' - j = sm$, then

$$i' + j' - (i + j) = (i' - i) + (j' - j) = rm + sm = (r + s)m$$

or $m \mid (i' + j') - (i + j)$, and so $[i + j] = [i' + j']$. Subtraction is also well-defined on $\mathbb{Z}/m\mathbb{Z}$ and the element $0 = [0]$ acts as an additive identity in $\mathbb{Z}/m\mathbb{Z}$. Thus $\mathbb{Z}/m\mathbb{Z}$ has the structure of a group. It is a finite group given as the set

$$\mathbb{Z}/m\mathbb{Z} = \{[0], [1], [2], \ldots, [m - 1]\}.$$

Example 2: Suppose W is a linear subspace of V a finite-dimensional vector space. Define a relation on V by $u \equiv v(\bmod W)$ whenever $v - u \in W$. We check that we have an equivalence relation:

reflexive: If $v \in V$, then $v - v = 0 \in W$, since W is a subspace.

symmetric: If $u \equiv v(\bmod W)$, then $v - u \in W$ and so $(-1)(v - u) = u - v \in W$ since W is closed under multiplication by scalars. Thus $v \equiv u(\bmod W)$.

transitive: If $u \equiv v(\bmod W)$ and $v \equiv x(\bmod W)$, then $x - v$ and $v - u$ are in W. Then $x - v + v - u = x - u$ is in W since W is a subspace. So $u \equiv x(\bmod W)$.

We denote $[V]$ as V/W. We next show that V/W is also a vector space. Given $[u], [v]$ in V/W, define $[u] + [v] = [u + v]$ and $c[u] = [cu]$. To see that this is well-defined, suppose $[u] = [u']$ and $[v] = [v']$. We compare $(u' + v') - (u + v)$. Since $u' - u \in W$ and $v' - v \in W$, we have $(u' + v') - (u + v) = (u' - u) + (v' - v)$ is in W. Similarly, if $[u] = [u']$, then $u' - u \in W$ so $c(u' - u) = cu' - cu$ is in W and $[cu] = [cu']$. The other axioms for a vector space hold in V/W by heredity and so V/W is a vector space. The canonical mapping $p: V \longrightarrow V/W$ is a linear mapping:

$$\begin{aligned} p(cu + c'v) &= [cu + c'v] = [cu] + [c'v] \\ &= c[u] + c'[v] = cp(u) + c'p(v). \end{aligned}$$

The kernel of the mapping is $p^{-1}([0]) = W$. Thus the dimension of V/W is given by

$$\dim V/W = \dim V - \dim W.$$

This construction is very useful and appears again in Chapter 11.

A general result applies to a set A with a binary operation $\mu\colon A \times A \to A$ and an equivalence relation on A.

Defintion 1.7. *An equivalence relation* $\sim$ *on a set A with binary operation* $\mu\colon A\times A \to A$ *is a* **congruence relation** *if the mapping* $\overline{\mu}\colon [A] \times [A] \to [A]$ *given by*

$$\overline{\mu}([a],[b]) = [\mu(a,b)]$$

induces a well-defined binary operation on $[A]$.

The operation of $+$ on $\mathbb{Z}$ is a congruence relation with respect to the equivalence relation $\equiv \pmod{m}$. The operation of $+$ is a congruence relation on a vector space V with respect to the equivalence relation induced by a subspace W. More generally, well-definedness is the important issue in identifying a congruence relation.

Proposition 1.8. *An equivalence relation* $\sim$ *on* A *with* $\mu\colon A \times A \to A$ *is a congruence relation if for any* $a, a', b, b' \in A$, *whenever* $[a] = [a']$ *and* $[b] = [b']$, *we have* $[\mu(a,b)] = [\mu(a',b')]$.

The Schröder-Bernstein Theorem

There is a marvelous criterion for the existence of a one-one correspondence between two sets.

The Schröder-Bernstein Theorem. *If there are one-one mappings*

$$f\colon A \to B \text{ and } g\colon B \to A,$$

then there is a one-one correspondence between A *and* B.

Proof: In order to prove this theorem, we first prove the following preliminary result.

Lemma 1.9. *If* $B \subset A$ *and* $f\colon A \to B$ *is one-one, then there exists a function* $h\colon A \to B$, *which is a one-one correspondence.*

Proof [Cox]*:* Take $B \subset A$ and suppose $B \neq A$. Recall that $A - B = \{a \in A \mid a \notin B\}$. Define

$$C = \bigcup\nolimits_{n\geq 0} f^n(A-B),$$

where $f^0 = \mathrm{id}_A$ and $f^k(x) = f\big(f^{k-1}(x)\big)$. Define the function $h\colon A \to B$ by

$$h(z) = \begin{cases} f(z), & \text{if } z \in C \\ z, & \text{if } z \in A - C. \end{cases}$$

By definition, $A - B \subset C$ and $f(C) \subset C$. Suppose $n > m \geq 0$. Observe that

$$f^m(A-B) \cap f^n(A-B) = \emptyset.$$

To see this suppose $f^m(x) = f^n(x')$, then $f^{n-m}(x') = x \in A - B$. But $f^{n-m}(x') \in B$ and so $x \in (A-B)\cap B = \emptyset$, a contradiction. This implies that h is one-one, since f is one-one.

We next show that h is onto:

$$\begin{aligned} h(A) &= f(C) \cup (A - C) \\ &= f\left(\bigcup\nolimits_{n\geq 0} f^n(A-B)\right) \cup \left(A - \bigcup\nolimits_{n\geq 0} f^n(A-B)\right) \\ &= \bigcup\nolimits_{n\geq 1} f^n(A-B) \cup \left(A - \bigcup\nolimits_{n\geq 0} f^n(A-B)\right) \\ &= A - (A-B) = B. \end{aligned}$$

So h is a one-one correspondence. $\diamondsuit$

Proof of the Schröder-Bernstein Theorem: Let $A_0 = g(B) \subset A$ and $B_0 = f(A) \subset B$. Then $g_0\colon B \to A_0$ and $f_0\colon A \to B_0$ are one-one correspondences, each induced by g and f, respectively. Let $F = f_0 \circ g_0\colon B \longrightarrow B_0$ denote the one-one function. Lemma 1.9 applies to (B, B_0, F), so there is a one-one correspondence $h\colon B_0 \to B$. The composition $h \circ f_0\colon A \to B_0 \to B$ is the desired equivalence of sets. $\diamondsuit$

The Problem of Invariance of Dimension

The development of set theory brought new insights about infinity. In particular, a set and its power set have different cardinalities. When a set is infinite, the cardinality of the power set is greater, and so there is a hierarchy of infinities. The discovery of this hierarchy prompted Cantor, in his correspondence with Richard Dedekind (1831–1916), to ask whether higher-dimensional sets might be distiguished by cardinality. On 5 January 1874 Cantor wrote Dedekind and posed the question:

> *Can a surface (perhaps a square including its boundary) be put into one-one correspondence with a line (perhaps a straight line segment including its endpoints) ...?*

He was soon able to prove the following positive result.

Theorem 1.10. *There is a one-one correspondence* $\mathbb{R} \longrightarrow \mathbb{R} \times \mathbb{R}$.

Proof: We apply the Schröder-Bernstein Theorem. Since the mapping $f\colon \mathbb{R} \to (0,1)$ given by $f(r) = \dfrac{1}{\pi}\left(\arctan(r) + \dfrac{\pi}{2}\right)$, is a one-one correspondence, it suffices to show that there is a one-one correspondence between $(0,1)$ and $(0,1)\times(0,1)$. We obtain one assumption of the Schröder-Bernstein theorem because there is a one-one mapping $f\colon (0,1) \longrightarrow (0,1)\times(0,1)$ given by the diagonal mapping, $f\colon t \mapsto (t,t)$.

To apply the Schröder-Berstein theorem we construct an injection $(0,1)\times(0,1) \longrightarrow (0,1)$. Recall that every real number can be expressed as a *continued fraction* ([Hardy-Wright]): suppose $r \in \mathbb{R}$. The **least integer function** (or *floor function*) is defined by

$$\lfloor r \rfloor = \max\{j \in \mathbb{Z} \mid j \leq r\}.$$

Since $0 < r < 1$, it follows that $1/r > 1$. Let $a_1 = \lfloor 1/r \rfloor$ and $r_1 = (1/r) - \lfloor 1/r \rfloor$. Then $0 \leq r_1 < 1$. We can write

$$r = \frac{1}{\frac{1}{r}} = \frac{1}{\frac{1}{r} - \left\lfloor \frac{1}{r} \right\rfloor + \left\lfloor \frac{1}{r} \right\rfloor} = \frac{1}{a_1 + r_1}.$$

If $r_1 = 0$ we can stop. If $r_1 > 0$, then repeat the process to r_1 to obtain a_2 and r_2 for which

$$r = \cfrac{1}{a_1 + \cfrac{1}{a_2 + r_2}}.$$

Continuing in this manner, we can express r as a continued fraction

$$r = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}} = [0; a_1, a_2, a_3, \ldots].$$

For example,

$$\frac{31}{127} = \cfrac{1}{4 + \cfrac{3}{31}} = \cfrac{1}{4 + \cfrac{1}{10 + \cfrac{1}{3}}} = [0; 4, 10, 3].$$

We can recognize a rational number by the fact that its continued fraction terminates after finitely many steps. Irrationals have infinite continued fractions, for example, $1/\sqrt{2} = [0; 1, 2, 2, 2, \ldots]$.

To prove Cantor's theorem, we first introduce an injection $I\colon (0,1) \to (0,1)$ defined on continued fractions by

$$I(r) = \begin{cases} [0; a_1 + 2, a_2 + 2, \ldots, a_n + 2, 2, 2, \ldots], & \text{if } r = [0; a_1, a_2, \ldots, a_n], \\ [0; a_1 + 2, a_2 + 2, a_3 + 2, \ldots], & \text{if } r = [0; a_1, a_2, a_3, \ldots]. \end{cases}$$

Thus I maps all of the real numbers in $(0,1)$ to the set $J = (0,1) \cap (\mathbb{R} - \mathbb{Q})$ of irrational numbers in $(0,1)$. We can define another one-one function, $t\colon J \times J \to (0,1)$ given by

$$t([0; a_1, a_2, \ldots], [0; b_1, b_2, \ldots]) = [0; a_1, b_1, a_2, b_2, \ldots].$$

The uniqueness of the continued fraction representation of a real number implies that t is one-one.

We finish the proof of the theorem by observing that the composition of one-one functions is one-one, and so the composition

$$t \circ (I \times I)\colon (0,1) \times (0,1) \to J \times J \to (0,1)$$

is one-one. The Schöder-Bernstein theorem applies to give a one-one correspondence between $(0,1)$ and $(0,1) \times (0,1)$. Thus there is a one-one correspondence between $\mathbb{R}$ and $\mathbb{R} \times \mathbb{R}$. ♢

Corollary 1.11. *There is a one-one correspondence between $\mathbb{R}^m$ and $\mathbb{R}^n$ for all positive integers m and n.*

The corollary follows by replacing $\mathbb{R}^2$ by $\mathbb{R}$ until $n = m$. A one-one correspondence is a relabelling of sets, and so as collections of labels we cannot distinguish between $\mathbb{R}^n$ and $\mathbb{R}^m$.

It follows that a function $\mathbb{R}^m \to \mathbb{R}$ could be replaced by a function $\mathbb{R} \to \mathbb{R}$ by composing with the one-one correspondence $\mathbb{R} \to \mathbb{R}^m$. A function expressing the dependence of a physical quantity on two variables could be replaced by a function that depends on only one variable. This observation calls into question the dependence on a certain number of variables as a physically meaningful notion—perhaps such a dependence can always be reduced to fewer variables by this mathematical slight-of-hand. In the epigraph, Cantor expressed his surprise in his proof of Theorem 1.10, not in the result.

If we introduce more structure into the discussion, the notion of dimension emerges. For example, from the point of view of linear algebra where we use the linear structure on $\mathbb{R}^m$ and $\mathbb{R}^n$ as vector spaces, we can distinguish between these sets by their linear dimension, the number of vectors in a basis.

If we apply the calculus to compare $\mathbb{R}^n$ and $\mathbb{R}^m$, we can ask if there exists a differentiable function $f\colon \mathbb{R}^n \to \mathbb{R}^m$ with an inverse that is also differentiable. At a given point of the domain, the derivative of such a differentiable mapping is a linear mapping, and the existence of a differentiable inverse implies that this linear mapping is invertible. Thus, by linear algebra, we deduce that $n = m$.

Between the realm of sets and the realm of the calculus lies the realm of topology—in particular, the study of continuous functions. The **main problem** addressed in this book is the following:

> **If there exists a continuous function $f\colon \mathbb{R}^n \to \mathbb{R}^m$ with a continuous inverse, then does $n = m$?**

This problem is called the question of the topological *Invariance of Dimension*, and it was one of the principal problems faced by the mathematicians who first developed topology. The problem was important because the use of dimension in the description of the physical space we dwell in was called into question by Cantor's discovery. The first proof of the topological invariance of dimension used new methods of a combinatorial nature (Chapters 9, 10, 11).

The combinatorial aspects of topology play a similar role that approximation does in analysis: by approximating with manageable objects, we can manipulate the approximations fruitfully, sometimes identifying properties that are associated to the combinatorics, but which depend only on the topology of the limiting object. This approach was initiated by Poincaré and refined to a subtle tool by L. E. J. Brouwer (1881–1966). It was Brouwer who gave the first complete proof of the theorem of the topological invariance of dimension and his proof established the centrality of combinatorial approximation in the study of continuity.

Toward our goal of a proof of invariance of dimension, we begin by expanding the familiar definition of continuity to more general settings.

Exercises

1. Let $f\colon A \to B$ be any function and U, V subsets of B, X a subset of A. Prove the following about the preimage operation:

a) $U \subset V$ implies $f^{-1}(U) \subset f^{-1}(V)$.

b) $f^{-1}(U \cup V) = f^{-1}(U) \cup f^{-1}(V)$.

c) $f^{-1}(U \cap V) = f^{-1}(U) \cap f^{-1}(V)$.

d) $f(f^{-1}(U)) \subset U$.
e) $f^{-1}(f(X)) \supset X$.
f) If for any $U \subset B, f(f^{-1}(U)) = U$, then f is onto.
g) If for any $X \subset A$, $f^{-1}(f(X)) = X$, then f is one-one.

2. Show that a set S and its power set, $\mathcal{P}(S)$ cannot have the same cardinality. (Hints to a difficult proof: Suppose there is an onto function $j\colon S \longrightarrow \mathcal{P}(S)$. Define the subset of S

$$T = \{s \in S \mid s \notin j(s)\} \in \mathcal{P}(S).$$

If j is surjective, then there is an element $t \in S$ with $j(t) = T$. Is $t \in T$?) Show that $\mathcal{P}(S)$ can be put in one-to-one correspondence with the set $\mathrm{map}(S, \{0, 1\})$ of functions from the set S to $\{0, 1\}$.

3. On the power set of a set X, $\mathcal{P}(X) = \{$ subsets of $X\}$, we have the equivalence relation, $U \cong V$ whenever there is a one-one correspondence between U and V. There is also a binary operation on $\mathcal{P}(X)$ given by taking unions:

$$\cup\colon \mathcal{P}(X) \times \mathcal{P}(X) \to \mathcal{P}(X), \quad \cup(U, V) = U \cup V,$$

where $U \cup V$ is the union of the subsets U and V. Show by example that the equivalence relation $\cong$ is not a congruence relation.

4. An equivalence relation, called the *equivalence kernel*, can be constructed from a function $f\colon A \to B$. The relation is on A and is defined by

$$x \sim y \Longleftrightarrow f(x) = f(y).$$

Show that this is an equivalence relation. Determine the relation that arises on $\mathbb{R}$ from the mapping $f(r) = \cos 2\pi r$. What equivalence kernel results from taking the canonical mapping $A \to [A]'$ where $\sim'$ is some equivalence relation on A?