1.12.6** Let $f\colon A \to B$ be a map of sets. Prove that f is injective if and only if given any set C and any two set maps $g_i\colon C \to A$, $i = 1, 2$, with compositions $f \circ g_1 = f \circ g_2$, then $g_1 = g_2$.

Solution "$\implies$"

Let f be injective, C be a set, and g_1, g_2 be the functions described above.

By definition, f is injective means that for all $a, b \in A$, $f(a) = f(b) \implies a = b$.

Let $x \in C$. Then $g_1(x), g_2(x) \in A$, by definition. Hence, by injectivity of f,

$$f(g_1(x)) = f(g_2(x)) \implies g_1(x) = g_2(x).$$

Since x was arbitrary, it follows that $g_1(x) = g_2(x)$ for all x.

"$\impliedby$"

Let $a, b \in A$ such that $f(a) = f(b)$. We wish to show that this implies $a = b$.

Suppose that $a \neq b$. Then let $C = A$, and consider

$$g_1(x) = x \quad \text{and} \quad g_2(x) = \begin{cases} x & \text{if } x \neq b \\ a & \text{if } x = b. \end{cases}$$

Then if $x \neq b$, we have $g_1(x) = g_2(x)$, so $f(g_1(x)) = f(g_2(x))$. If $x = b$, then

$$f(g_1(b)) = f(b) = f(a) = f(g_2(b)),$$

so $f \circ g_1 = f \circ g_2$. Thus, by assumption, $g_1 = g_2$ for all $x \in A$. In particular, $g_1(b) = g_2(b)$, but then

$$b = g_1(b) = g_2(b) = a,$$

a contradiction. Thus, $a = b$.

1.12.7 Let $f\colon A \to B$ be a map of sets. Prove that f is surjective if and only if given any set C and any two set maps $h_i\colon B \to C$, $i = 1, 2$, with compositions $h_1 \circ f = h_2 \circ f$, then $h_1 = h_2$.

Solution "$\implies$"

Let f be surjective, C be a set, and h_1, h_2 be functions as described above.

Let $b \in B$. Since f is surjective, there exists $a \in A$ such that $f(a) = b$. Hence, evaluating $h_1 \circ f$ and $h_2 \circ f$ at a, we get

$$h_1(f(a)) = h_2(f(a)) \implies h_1(b) = h_2(b).$$

Since b was arbitrary, it follows that $h_1(b) = h_2(b)$ for all $b \in B$.

"$\impliedby$"

If B only has one element and A is non-empty, then f is clearly surjective by the pigeonhole principle. Assume from now on that B has at least two differing elements.

Suppose f were not surjective. Then there exists $b \in B$ such that $b \notin f(A)$

Choose $C = B$, let $h_1\colon B \to B$ be the identity function on B, and let $h_2\colon B \to B$ also be the identity, but with $h_2(b) \neq h_1(b)$, since B has at least two unique elements.

Since $f(a) \neq b$ for any $a \in A$, $f(a) = h_1(f(a)) = h_2(f(a)) = f(a)$, so by assumption $h_1 = h_2$. But $h_1(b) \neq h_2(b)$. Contradiction, so f must be surjective.

1.12.8** Show a subset of a countable set is either countable or finite.

Solution Let N be a countable set, and let $A \subseteq N$ be a subset. Then A is either finite or infinite. We only need to show that if A is infinite, then A is countable.

Let A be infinite. Since N is countable, we can order its elements via $N = \{a_1, a_2, \ldots\}$. We define $f\colon A \to \mathbb{Z}^+$ as follows:

Consider $B \coloneqq \{n \in \mathbb{Z}^+ \mid a_n \in A\}$. By the well-ordering principle, it contains a minimal element n_1. Take $f(a_{n_1}) = 1$.

Next, consider $B - \{n_1\} \subseteq \mathbb{Z}^+$. Again, by well-ordering, it contains a minimal element n_2. Define $f(a_{n_2}) = 2$.

We proceed by induction: Suppose we have $n_1, \ldots, n_k$ with $f(n_i) = i$, where n_i is the least element of $B - \{n_1, \ldots, n_{i-1}\}$, for every $1 \leq i \leq k$.

Consider $B - \{n_1, \ldots, n_k\} \subseteq \mathbb{Z}^+$, which has a least element n_{k+1} by well-ordering. Define $f(a_{k+1}) = k + 1$.

Hence, for every $k \in \mathbb{Z}^+$, we have $a_k \in A$ and $f(a_k) = k$. Moreover, f is well-defined: Since A is a subset of N, each element of A can be written in the form a_ℓ for some $\ell \in \mathbb{Z}^+$, so $f(a)$ exists for every element in A.

Since A is infinite, f is surjective, by construction. All that's left is to show that f is injective.

Let $a_n, a_m \in A$. Then $f(a_n) = f(a_m) \implies n = m$, by definition. It follows that $a_n = a_m$, so f is injective.

Thus, f is a bijection from A to $\mathbb{Z}^+$, so A is countable, by definition.

2.17.1 Prove that the number of subsets of a set with n elements is 2^n.

Solution We show this by induction.

Base step:

Consder $N_1 \coloneqq \{1\}$. Then the subsets of N_1 are $\emptyset$ and N_1 itself, so there are $2 = 2^1$ subsets, so the base case holds.

Inductive step:

Suppose $N_k \coloneqq \{1, 2, \ldots, k\}$ has 2^k elements. We wish to show that $N_{k+1} \coloneqq \{1, 2, \ldots, k + 1\}$ has 2^{k+1} elements.

First notice that since $N_k \subseteq N_{k+1}$, all subsets of N_k are subsets of N_{k+1}, so we have 2^k subsets.

We want to show that if A is a subset of N_{k+1}, then A is either a subset of N_k or is a set of the form $B \cup \{k + 1\}$, where $B \subseteq N_k$.

If A is not a subset of N_k, then $k + 1 \in A$, since the only element in N_{k+1} that's not in N_k is $k + 1$. Then

$$A - \{k + 1\} \subseteq N_{k+1} - \{k + 1\} = N_k,$$

so $A = (A - \{k + 1\}) \cup \{k + 1\}$. Hence, subsets of N_{k+1} are subsets of N_k or subsets of N_k with $k + 1$. We get 2^k subsets from subsets of N_k, and the function

$$\mathcal{P}(N_k) \ni B \mapsto B \cup \{k + 1\} \in \{C \cup \{k + 1\} \mid C \in \mathcal{P}(N_k)\}$$

is a bijection (it has the inverse $B \mapsto B - \{k + 1\}$), so we have 2^k sets of the second form. Hence, we have $2^k + 2^k = 2 \cdot 2^k = 2^{k+1}$ subsets of N_{k+1}, so the inductive step holds.

Hence, by the principle of mathematical induction, the number of subsets of a set with n elements in 2^n.

2.17.3 The first nine Fibonacci numbers are $1, 1, 2, 3, 5, 8, 13, 21, 34$. What is the n-th Fibonacci number F_n? Show that $F_n < 2^n$.

Solution The n-th Fibonnaci number is given by the recursive formula $F_n = F_{n-1} + F_{n-2}$ for $n \geq 3$, where $F_1 = F_2 = 1$.

Notice that we can write

$$\begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} F_{n-1} \\ F_{n-2} \end{pmatrix}.$$

The characteristic polynomial of the matrix is $\lambda^2 - \lambda - 1$, and it has the roots

$$\lambda_1 = \frac{1+\sqrt{5}}{2} \quad \text{and} \quad \lambda_2 = \frac{1-\sqrt{5}}{2}$$

with eigenvectors

$$v_1 = \begin{pmatrix} \frac{1+\sqrt{5}}{2} \\ 1 \end{pmatrix} = \begin{pmatrix} \lambda_1 \\ 1 \end{pmatrix} \quad \text{and} \quad v_2 = \begin{pmatrix} \frac{1-\sqrt{5}}{2} \\ 1 \end{pmatrix} = \begin{pmatrix} \lambda_2 \\ 1 \end{pmatrix}.$$

Two useful properties of our eigenvalues are

$$\lambda_1 + \lambda_2 = 1 \quad \text{and} \quad \lambda_1\lambda_2 = \frac{1+\sqrt{5}}{2} \cdot \frac{1-\sqrt{5}}{2} = -1.$$

Thus, we can diagonalize our matrix via

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \lambda_1 & \lambda_2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \begin{pmatrix} \lambda_1 & \lambda_2 \\ 1 & 1 \end{pmatrix}^{-1} := SDS^{-1}.$$

Then notice that

$$\begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix} = SDS^{-1} \begin{pmatrix} F_{n-1} \\ F_{n-2} \end{pmatrix} = \left[SDS^{-1}\right]^2 \begin{pmatrix} F_{n-2} \\ F_{n-3} \end{pmatrix} = \cdots = \left[SDS^{-1}\right]^{n-2} \begin{pmatrix} F_2 \\ F_1 \end{pmatrix} = SD^{n-2}S^{-1} \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Expanding, we get

$$\begin{aligned}
\begin{pmatrix} F_n \\ F_{n-1} \end{pmatrix} &= \begin{pmatrix} \lambda_1 & \lambda_2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \lambda_1^{n-2} & 0 \\ 0 & \lambda_2^{n-2} \end{pmatrix} \begin{pmatrix} \lambda_1 & \lambda_2 \\ 1 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \\
&= \begin{pmatrix} \lambda_1^{n-1} & \lambda_2^{n-1} \\ \lambda_1^{n-2} & \lambda_2^{n-2} \end{pmatrix} \left[\frac{1}{\lambda_1 - \lambda_2} \begin{pmatrix} 1 & -\lambda_2 \\ -1 & \lambda_1 \end{pmatrix} \right] \begin{pmatrix} 1 \\ 1 \end{pmatrix} \\
&= \frac{1}{\lambda_1 - \lambda_2} \begin{pmatrix} \lambda_1^{n-1} - \lambda_2^{n-1} & \lambda_1\lambda_2^{n-1} - \lambda_2\lambda_1^{n-1} \\ \lambda_1^{n-2} - \lambda_2^{n-2} & \lambda_1\lambda_2^{n-2} - \lambda_2\lambda_1^{n-2} \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix}
\end{aligned}$$

Thus, we get the famous formula

$$\begin{aligned}
F_n &= \frac{1}{\lambda_1 - \lambda_2} \left(\lambda_1^{n-1} - \lambda_2^{n-1} + \lambda_1\lambda_2^{n-1} - \lambda_2\lambda_1^{n-1} \right) \\
&= \frac{1}{\lambda_1 - \lambda_2} \left(\lambda_1^{n-1}(1-\lambda_2) - \lambda_2^{n-1}(1-\lambda_1) \right) \\
&= \frac{1}{\lambda_1 - \lambda_2} \left(\lambda_1^{n-1}\lambda_1 - \lambda_2^{n-1}\lambda_2 \right) \\
&= \frac{1}{\lambda_1 - \lambda_2} \left(\lambda_1^n - \lambda_2^n \right) \\
&= \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right].
\end{aligned}$$

Next, we'll prove the inequality by strong induction.

Base step:

$F_1 = 1 < 2 = 2^1$, so the base step holds.

Inductive step:

Assume $F_{n-2} < 2^{n-2} < 2^{n-1}$, $F_{n-1} < 2^{n-1}$. By definition,

$$F_n = F_{n-1} + F_{n-2} < 2^{n-1} + 2^{n-1} = 2 \cdot 2^{n-1} = 2^n,$$

so the inductive step holds.

By induction, $F_n < 2^n$.

2.17.5 Prove that the Well-Ordering Principle, the First Principle of Finite Induction, and the Second Principle of Finite Induction are all equivalent.

Solution We'll label the principles via their acronyms, i.e., WOP, FPFI, and SPFI. These are the implications we'll prove:

$$\text{WOP} \implies \text{FPFI} \implies \text{SPFI} \implies \text{WOP}.$$

WOP $\implies$ FPFI:

Let $P(n)$ be a statement about n, and suppose that $P(1)$ holds, and that $P(n) \implies P(n+1)$.

Consider $S = \{n \in \mathbb{Z}^+ \mid P(n) \text{ does not hold}\}$. If $S = \emptyset$, then we're done.

Suppose $S \neq \emptyset$. Then by the WOP, it has a least element $1 < n_0 \in S$. Since n_0 is the least element of S, $n_0 - 1$ is not in S, so $P(n_0 - 1)$ holds. But $P(n_0 - 1) \implies P(n_0)$ by assumption, which implies $n_0 \notin S$. This is a contradiction, so $S = \emptyset$ and the SPFI holds.

FPFI $\implies$ SPFI

Let $P(n)$ be a statemenet about n.

Suppose $P(1)$ holds. We want to show that if in addition, $P(1), \ldots, P(k) \implies P(k+1)$, then $P(n)$ holds for all $n \in \mathbb{Z}^+$. By the FPFI, since $P(1)$ holds and $P(k) \implies P(k+1)$, $P(n)$ holds for all n, so the SPFI holds.

SPFI $\implies$ WOP

Let $S \subseteq \mathbb{Z}^+$ with $S \neq \emptyset$.

Suppose the WOP does not hold, and that S does not have a least element. Then consider S^{c}.

We will prove by strong induction that $\mathbb{Z}^+ = S^{\mathrm{c}}$.

Base step:

$1 \in S^{\mathrm{c}}$. If not, then since 1 is the least element of $\mathbb{Z}^+$, this implies that 1 is the least element of S, which doesn't exist.

Inductive step:

Suppose $1, 2, \ldots, n \in S^{\mathrm{c}}$. Then $n+1 \in S^{\mathrm{c}}$. Otherwise, $n+1$ would be the least element of S^{c}, since S does not contain $1, 2, \ldots, n < n+1$. Thus, the inductive step holds.

By induction, $n \in S^{\mathrm{c}}$ for all $n \in \mathbb{Z}^+$, so $S^{\mathrm{c}} = \mathbb{Z}^+ \implies S = \emptyset$. This is a contradiction, so the WOP must hold.

Thus, all three principles are equivalent.

2.17.6 State and prove the binomial theorem. What algebraic properties do you need for your proof to work?

Solution For some numbers a, b and $n \in \mathbb{Z}^+$, the binomial theorem states

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

We first prove a lemma:

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}.$$

$$\begin{aligned}
\binom{n}{k} + \binom{n}{k-1} &= \frac{n!}{(n-k)! \cdot k!} + \frac{n!}{(n-(k-1))! \cdot (k-1)!} \\
&= \frac{n!}{(n-k)! \cdot k!} \cdot \frac{(n+1)-k}{(n+1)-k} + \frac{n!}{((n+1)-k)! \cdot (k-1)!} \cdot \frac{k!}{k!} \\
&= \frac{(n+1)! - n! \cdot k + n! \cdot k}{((n+1)-k)! \cdot k!} \\
&= \frac{(n+1)!}{((n+1)-k)! \cdot k!} \\
&= \binom{n+1}{k}.
\end{aligned}$$

We will prove the binomial theorem by induction on n.

Base step:

$(a+b)^1 = a + b = \binom{1}{0} a^{1-0} b^0 + \binom{0}{0} a^{1-1} b^1$, so the base step holds.

Inductive step:

Suppose the binomial theorem holds for $(a+b)^n$. Then by distributivity and commutativity of $\cdot$,

$$(a+b)^{n+1} = (a+b)^n (a+b) = a(a+b)^n + b(a+b)^n.$$

Expanding, we get

$$\begin{aligned}
(a+b)^{n+1} &= a(a+b)^n + b(a+b)^n \\
&= a \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k + b \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{n-(k-1)} b^k + \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^{k+1} \\
&= a^{n+1} + \sum_{k=1}^{n} \binom{n}{k} a^{n-(k-1)} b^k + \sum_{k=0}^{n-1} \binom{n}{k} a^{n-k} b^{k+1} + b^{n+1} \\
&= a^{n+1} + \sum_{k=1}^{n} \binom{n}{k} a^{n-(k-1)} b^k + \sum_{k=1}^{n} \binom{n}{k-1} a^{n-(k+1)} b^k + b^{n+1} \\
&= a^{n+1} + \sum_{k=1}^{n} \left[\binom{n}{k} + \binom{n}{k-1} \right] a^{n-(k-1)} b^k + b^{n+1} \\
&= \binom{n+1}{n+1} a^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} a^{n-(k-1)} b^k + \binom{n+1}{0} b^{n+1} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} a^{(n+1)-k} b^k,
\end{aligned}$$

so the inductive step holds.

By induction, the binomial theorem holds.

We needed distributivity, commutativity of multiplication, e.g., $b \cdot a^{n-k}b^k = a^{n-k}b^k \cdot b = a^{n-k}b^{k+1}$, and we also needed commutativity of addition.

Show that $\mathbb{Z}^+ \times \mathbb{Z}^+$ is countable.

Solution $(n, m) \mapsto 2^n 3^m$ is an injection from $\mathbb{Z}^+ \times \mathbb{Z}^+$ to $\mathbb{Z}^+$, by the unique prime factorization theorem.

$n \mapsto (n, 1)$ is also an injection from $\mathbb{Z}^+$ to $\mathbb{Z}^+ \times \mathbb{Z}^+$.

Thus, by Schröder-Bernstein, $|\mathbb{Z}^+ \times \mathbb{Z}^+| = |\mathbb{Z}^+|$, so by definition, the product is countable.