Winter 2021 Math 61 Notes

Kyle Chui

2021-1-13

Contents

1 Sets and Functions **1**
1.1 Power Sets 1
1.2 Functions 1
1.3 Inverses of Functions 1

1 Sets and Functions

1.1 Power Sets

Definition. *Power Set*
If X is a set, the *power set* of X, denoted $\mathscr{P}(X)$, is the set of subsets of X.

Example. *Power Sets*

- $\mathscr{P}(\varnothing) = \{\varnothing\}$
- $\mathscr{P}(\{a, b\}) = \{\varnothing, \{a\}, \{b\}, \{a, b\}\}$
- $\mathscr{P}(\{a, b, c\}) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$

Definition. *Cardinality of Finite Sets*
If X has finitely many elements, then $|X|$ denotes the number of elements of X.

Theorem — *Cardinality of Power Sets*
If X is finite, then $|\mathscr{P}(X)| = 2^{|X|}$.

Proof. Let us induct on the cardinality of the set X. Suppose $|X| = 0$, so that $X = \varnothing$. Then $\mathscr{P}(X) = \{\varnothing\}$, so $|\mathscr{P}(X)| = 1 = 2^0$. Thus the statement is true when $|X| = 0$.

Suppose that the statement holds for some non-negative integer k. Let Y be a set such that $|Y| = k + 1$, and $y \in Y$. Observe that we may split $\mathscr{P}(Y)$ into two groups: the subsets containing y, and the subsets that do not contain y. A subset of Y that does not contain y is exactly $Y \setminus \{y\}$, which has k elements. By the inductive hypothesis, there exist 2^k such subsets. A subset of Y that does contain y is obtained by adding y to a subset of Y which does not contain y. Again, there are 2^k such subsets. Any subset of Y either does or does not contain y (but not both), so there are $2^k + 2^k = 2^{k+1}$ subsets of Y. Therefore $\mathscr{P}(X) = 2^{|X|}$ for all finite sets $|X|$. $\square$

1.2 Functions

Definition. *Function*
If X, Y are sets, a function f from X to Y, written $f : X \to Y$ is a subset of $X \times Y$ satisfying two properties:

- For all $a \in X$, there exists $b \in Y$ such that $(a, b) \in f$
  - Everything in the domain must get mapped to something in the codomain
- For all $a \in X$ and $b, b' \in Y$, if $(a, b), (a, b') \in f$, then $b = b'$
  - Every element in the domain can map to at most one element in the codomain

Note (Function Notation). If $(a, b) \in f$, we write $f(a) = b$.

Example. *Functions*

- $f: \mathbb{Z} \to \mathbb{N}$ such that $f(x) = x^2$
- $g: \mathbb{N} \to \mathbb{N}$ such that $g(x) = x^2$

Note that f and g are different functions.

Definition. *Domain and Codomain of a Function*
If $f: X \to Y$, X is the domain of f and Y is the codomain of f.

Definition. *Range of a Function*
For $f: X \to Y$, the range of f is:

$$\operatorname{range} f = \{y \in Y \mid y = f(x) \text{ for some } x \in X\}$$

Definition. *Surjectivity*
A function $f: X \to Y$ is *onto* or *surjective* if $\operatorname{range} f = Y$. In other words, a function is surjective if its range is equal to its codomain.

Example. *Surjective Functions*

- $f: \{a, b, c\} \to \{d, e, f\}$ defined by $f = \{(a, d), (b, e), (c, f)\}$
- $f: \mathbb{Z} \to \mathbb{N}$ defined by $f(x) = |x|$

Definition. *Injectivity*
A function $f: X \to Y$ is *one-to-one* or *injective* if, for all $x, y \in X$, $f(x) = f(y)$ implies that $x = y$. In other words, different elements in the domain map to different elements in the codomain.

Example. *Injective Functions*

- $g: \mathbb{N} \to \mathbb{N}$ defined by $g(x) = x^2$

Note (Properties of Functions). Observe that the both the domain and codomain of a function matter when it comes to determining whether the function satisfies certain properties. For instance, $f: \mathbb{Z} \to \mathbb{N}$ defined by $f(x) = x^2$ is not injective, but restricting the domain to $\mathbb{N}$ would make it injective. Similarly, a function $f: \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = x^2$ is not surjective, but restricting the codomain to $\mathbb{N}$ would make it surjective.

Definition. *Composition of Functions*
If $f: X \to Y, g: Y \to Z$ are functions, then $g \circ f: X \to Z$ is a function defined by $(g \circ f)(x) = g(f(x))$.

Theorem — *Composition of Injective/Surjective Functions is Injective/Surjective*
Let $f\colon X \to Y$, $g\colon Y \to Z$.

- If f, g are injective, so is $g \circ f$
- If f, g are surjective, so is $g \circ f$

Proof. Suppose f, g are injective functions. Let $x, x' \in X$ such that $(g \circ f)(x) = (g \circ f)(x')$. Then

$$\begin{aligned} g(f(x)) &= g(f(x')) \\ f(x) &= f(x') && \text{(Because } g \text{ is injective)} \\ x &= x' && \text{(Because } f \text{ is injective)} \end{aligned}$$

Therefore $g \circ f$ is injective. □

Proof. Suppose f, g are surjective functions. Let $z \in Z$. Because g is surjective, there exists some $y \in Y$ such that $g(y) = z$. Furthermore, because f is surjective, there exists some $x \in X$ such that $f(x) = y$. Thus, for every $z \in Z$, there exists some $x \in X$ such that $(g \circ f)(x) = g(f(x)) = g(y) = z$, so $g \circ f$ is surjective. □

Definition. *Bijectivity*
If a function is both injective and surjective, then we say that it is *bijective*.

Note (Cardinality and Bijections). If there is a bijection between two sets, they have the same number of elements.

1.3 Inverses of Functions

Definition. *Inverse of a function*
Suppose $f\colon X \to Y$, $g\colon Y \to X$ is an inverse to f (soon we'll prove that inverses are unique if they exist) if $f \circ g$ and $g \circ f$ are the identity. In other words, $(g \circ f)(x) = x$, $(f \circ g)(y) = y$ for all $x \in X$, $y \in Y$.

Theorem — *Bijective $\iff$ Inverse*
For $f\colon X \to Y$, f is a bijection if and only if f has an inverse.

Proof. Suppose f has an inverse function g. Then $f \circ g$ and $g \circ f$ are the identity. Suppose $f(a) = f(b)$. Then

$$\begin{aligned} f(a) &= f(b) \\ g(f(a)) &= g(f(b)) \\ (g \circ f)(a) &= (g \circ f)(b) \\ a &= b. \end{aligned}$$

Thus f is injective.

Suppose $b \in Y$. Since $f \circ g$ is the identity, we have that $(f \circ g)(b) = b$, so $f(g(b)) = b$. Thus f is surjective. Therefore f is a bijection.

Now suppose that f is a bijection. We define $f^{-1}(a)$ by $f^{-1}(a) = b$, where $a = f(b)$.

- Because f is surjective, we have that for all $a \in Y$, there exists some $b \in X$ such that $a = f(b)$.
- Because f is injective, any $a \in Y$ is *uniquely* mapped by some $b \in X$.

Thus f^{-1} is a function. We will now show that f^{-1} is the inverse of f. For all $x \in X$, $(f^{-1} \circ f)(x) = x$ by definition. For all $y \in Y$,

$$\begin{aligned} (f \circ f^{-1})(y) &= f(f^{-1}(y)) \\ &= f(f^{-1}(f(x))) && \text{(Because } f \text{ is surjective)} \\ &= f(x) && ((f^{-1} \circ f)(x) = x) \\ &= y. \end{aligned}$$

Therefore f^{-1} is the inverse of f. □

Theorem — *Uniqueness of Inverses*
Inverses of functions are unique, provided they exist.
Suppose $f\colon X \to Y$. If f has inverses $g, h\colon Y \to X$ such that $g \circ f = h \circ f = \mathrm{id}_X$, $f \circ g = f \circ h = \mathrm{id}_Y$, then $g = h$.

Proof. Let $y \in Y$. By the previous theorem we know that f is surjective, so $y = f(x)$, for some $x \in X$. Thus

$$\begin{aligned} g(y) &= g(f(x)) \\ &= x \\ &= h(f(x)) \\ &= h(y). \end{aligned}$$

Thus $g = h$ and the inverse is unique. □